Digitalizacija kao faktor rasta moderne ekonomije

Prateći rizici - sajber napadi i bezbednost podataka

Preventiva: šta preduzeća mogu da preduzmu?

Mogućnosti finansijske nadoknade štete

DIGITALIZACIJA I SAJBER SIGURNOST

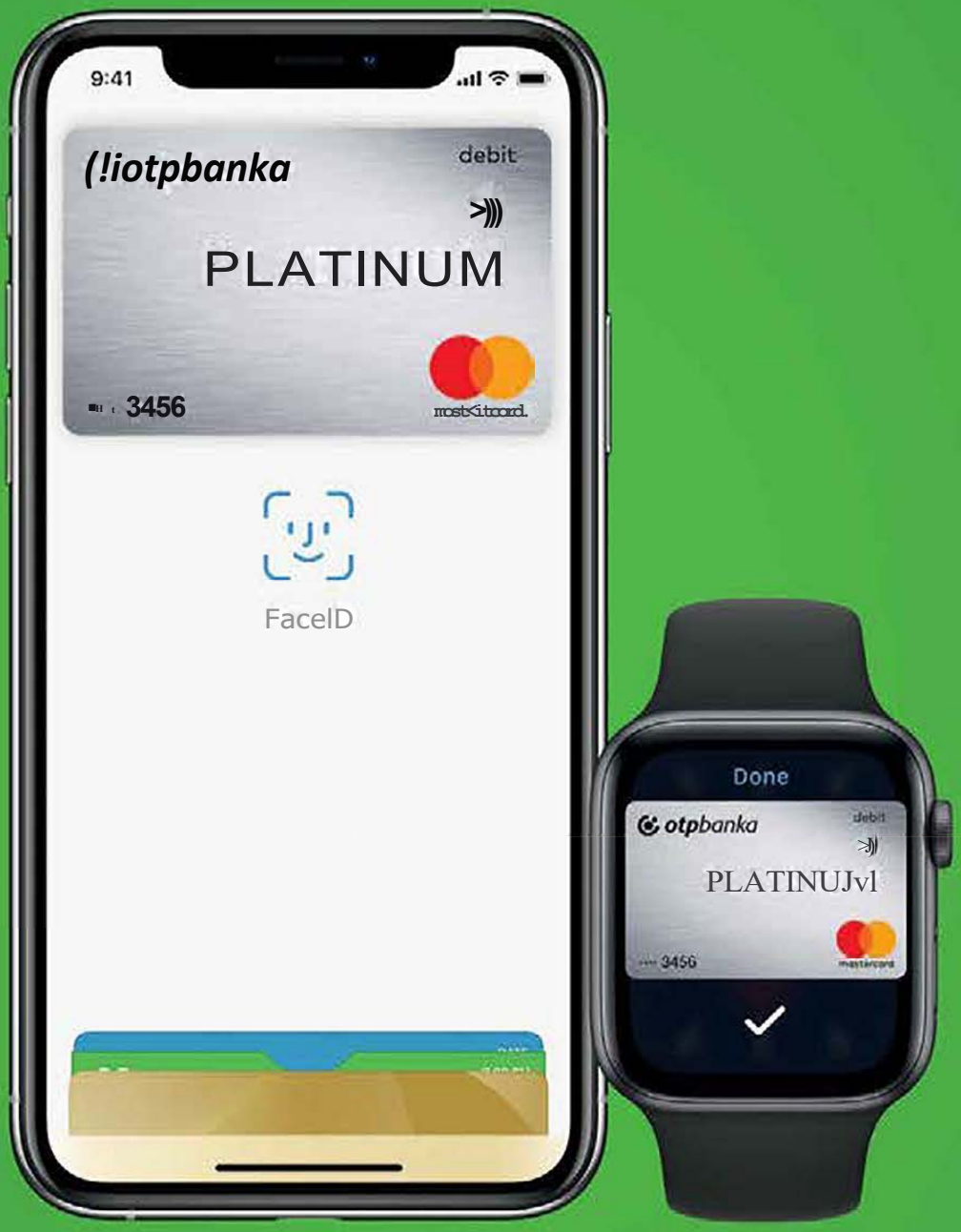
Kako da sačuvate biznis i imovinu

BE RISK PROTECTED.

Godina I, Broj 1
Mart 2021.

ISSN 278-179X

Mi koristimo Apple Pay



Biramo bezbedniji,
beskontaktni način plaćanja.

otpbanka | Pay

Da je digitalna transformacija u čitavom svetu postala sastavni deo života i poslovanja, pokazuju i podaci globalnih istraživanja po kojima 70 odsto preduzeća već ima digitalnu strategiju ili radi na njoj, da je takvu strategiju već usvojilo 55 odsto startapova, a da 39 odsto izvršnih direktora smatra da će ostvariti benefite od digitalne transformacije u narednih tri do pet godina.

U tom smeru krupnim koracima grabi i naša zemlja - preduzeća koja još nisu kročila u digitalizaciju u riziku su da u bliskoj budućnosti nestanu sa poslovne scene.

Ali, poslovanje u digitalnom okruženju nosi i svoje rizike – nikad nismo dovoljno mali i beznačajni da ne bismo bili meta hakerskih napada, bilo kroz blokadu poslovanja, kroz krađu podataka ili preko prevare zaposlenih.

Štete često mogu nadmašiti i vrednost čitavog našeg poslovanja: rizici od sajber napada su za svega sedam godina na listi rizika novog doba skočili sa 15. na prvo mesto prema procenama svetskih privrednika.

Upravo je sajber sigurnost bila jedna od centralnih tema na prošlogodišnjoj konferenciji „Rizici novog doba: uticaj na poslovanje i imovinu“, koju su pod sloganom BE RISK PROTECTED organizovali portali Sveosiguranju i Sveonovcu. Jedan od zaključaka bio je da je – u funkciji unapređenja bezbednosti poslovanja u digitalnom okruženju – neophodna sinergija IT i finansijskog sektora. U tom kontekstu, pod istim sloganom pokrenuta je i Inicijativa za jačanje bezbednosti podataka, a publikacija koja je pred vama – deo je ove Inicijative.

Cilj ove godišnje publikacije je da privrednicima i donosiocima odluka u javnom i privatnom sektoru pruži više informacija o načinima preventive/zaštite podataka i poslovanja u digitalnom okruženju, o regulativi i institucijama kojima je moguće obratiti se u kritičnim situacijama, o stepenu digitalizacije u finansijskom sektoru i prednostima po korisnike, ali i o mogućnostima finansijske nadoknade štete ukoliko se ona dogodi, kroz polise osiguranja.

Dugoročno, želja nam je da daljim aktivnostima, zajedno sa vama, doprinesemo da se naša zemlja što bolje kotira na svetskoj mapi kad je reč o bezbednom poslovanju u digitalnom okruženju.

Lela Saković
Vesna Lapčić

Broj 1, mart 2021. | **Izdavač:** NVO "Naše pravo"
Braće Jugovića 14, 11000 Beograd
Odgovorno lice: Lela Saković
Glavna urednica: Lela Saković
Izvršna urednica: Vesna Lapčić
Saradnici: Danijela Ilić, Danijela Nišavić, Olivera Bojić, Zlata Rakić, Marica Vuković, Snježana Davidović
Lektura: Stana Šehalić
Fotografije: Lična arhiva, Pixabay.com
Grafička priprema: Strudio Trid
Štampa: Caligraph d.o.o, Beograd
www.beriskprotected.rs | office@beriskprotected.rs

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

930.25:004.056.5

DIGITALIZACIJA i sajber sigurnost : kako da sačuvate biznis i imovinu / glavna urednica Lela Saković. - God. 1, br. 1 (mart 2021) - Beograd : NVO "Naše pravo", 2021- (Beograd : Caligraph). - 30 cm

Godišnje.
ISSN 2738-179X = Digitalizacija i sajber sigurnost
COBISS.SR-ID 34502665

DIGITALIZACIJA

OPASNOSTI I ŠTETE

PRAVA VLASNIKA PODATAKA

PREVENTIVA

OSIGURANJE

DIGITALIZOVANE FINANSIJE

Osiguranje za poslovanje u „oblaku“

Kompanije sve više koriste „oblak“ za čuvanje podataka. Vođena tim trendom, reosiguravajuća kompanija Munich Re je dogovorila saradnju sa Google Cloudom i Allianz Global Corporate&Specialty (AGCS) kako bi osmislili polisu sajber osiguranja namenjenu pokriću rizika poslovanja u „oblaku“. Inovativno sajber osiguranje nazvano je „Cloud Protection +“ i namenjeno je korisnicima Google Clouda.

Polisa osiguranja će inicijalno biti ponuđenja korisnicima Google Cloud u Sjedinjenim Američkim Državama i to onima sa prihodom od petsto miliona do pet milijardi dolara.

Kompanije su se udružile da bi objedinile stručnost Google Cloud-a za sigurnost specifičnu za oblak sa ekspertizom za preuzimanje rizika Münich Re-a i AGCS-a. Google Cloud će omogućiti organizacijama personalizovani izveštaj o njihovom sigurnosnom položaju na platformi pomoću novog alata Risk Manager. Tako dobijene podatke kompanije dele sa osiguravačem što im omogućava da imaju uvid u potpuno transparentan i efikasan proces procene i prihvatanje rizika osiguravača.

Sektor finansija i osiguranja treći je po curenju podataka

Broj podataka koji su procureli u svetu dostigao je neverovatnih 37 milijardi prošle godine, pokazuju podaci koje je tim Atlas VPN analizirao na osnovu izveštaja QuckView o kršenju zaštite podataka. Gotovo 60 odsto od ukupnog broja prijavljeno je unutar Sjedinjenih Država. Na globalnoj listi u ovoj oblasti, sektor finansija i osiguranja nalazi se na trećoj poziciji. Od pomenutih 37 milijardi, čak 82 odsto ili oko 30 milijardi podataka ugroženo je u samo pet velikih incidenata. Broj procurelih podataka u 2020. porastao je za čitavih 140 odsto u odnosu na 2019, kada je taj broj bio „svega“ 15 milijardi.

Zdravstvena industrija suočila se s najviše hakovanja – 484, što čini 12 odsto svih prošlogodišnjih kršenja. Informacioni sektor takođe je bio visoko ciljani i pretrpeo je 429 hakovanja, što je činilo 11 odsto povreda podataka prošle godine. Sektor finansija i osiguranja zauzima treće mesto na popisu: industrija je imala 382 hakerska napada – 10 odsto prošlogodišnjih kršenja.

Hakeri preuzeli kontrolu nad kamerama u kompaniji Tesla

Jedna hakerska grupa uspela je da preuzme kontrolu nad sigurnosnim kamerama koje su instalirane u kompaniji Tesla, te Equinox, bolnicama, zatvorima i bankama širom Sjedinjenih Američkih Država, objavio je Bleeping

Computer početkom marta ove godine. Osim što su podelili slike napravljene pogođenim kamerama, napadači su dokazali i da mogu da kompletno preuzmu kontrolu nad bezbednosnim sistemima koje koriste Cloudflare i Tesla. Pristup bezbednosnim sistemima bio je moguć zahvaljujući tome što je grupa iskoristila super admin nalog za kompaniju Verkada koja radi sa svim pogođenim sistemima. Kompanija je najpoznatija po tome što pruža usluge kompaniji Tesla, i snabdeva je IoT bezbednosnim kamerama.

Nakon prvih saznanja o napadu, bezbednosni eksperti su kontaktirali kompaniju Verkada, posle čega su napadači izgubili pristup super admin nalogu.
Na internetu se ubrzo pojavio haštag #OperationPanopticon koji se postavlja ispod vesti o ovim napadima, a odnosi se na koncept Panopticon kojim se opisuje dizajn zgrada u kojima oni koji u njima borave (obično zatvorenici) - ne mogu da budu sigurni da li ih neko posmatra ili ne.

Reinkarnacija ljudi kao čet botova

Tehnološki gigant Majkrosoft (Microsoft) podneo je patent koji omogućava „digitalnu reinkarnaciju“ preminulih u obliku čet botova (chatbot), kompjuterskih programa koji simuliraju razgovor ljudi, piše Forbs.

Umesto da koristi konvencionalni metod obuke čet botova, koristeći razgovore i materijale velikog broja korisnika, Majkrosoftov patent omogućava stvaranje čet bota od podataka i ranije komunikacije preminule osobe. Sistem bi koristio „društvene podatke“ kao što su slike, glasovne poruke, objave na društvenim mrežama i elektronsku pošta - za izgradnju profila osobe.

„Društveni podaci mogu se koristiti za stvaranje ili modifikovanje posebnog indeksa u temi ličnosti određene osobe. Posebni indeks se može koristiti za obuku čet bota za razgovore i interakciju u ličnosti određene osobe“, navodi se u objašnjenju.

„U nekim aspektima, glasovni snimak određene osobe se može generisati pomoću postojećih snimaka i zvučnih podataka određene osobe“

Majkrosoft za svoj izum tvrdi da nije važno o kojoj osobi se radi, navodeći da osoba čiji bot se izrađuje može biti „živa ili mrtva“.

U opisu tehnologije zaštićene ovim patentom pominje se i činjenica da bi čet bota mogli da „inspirišu“ preminuli prijatelji ili članovi porodice, što dovodi do zaključka da bi Majkrosoft želeo da koristi tehnologiju da „oživi“ preminule i omogući „razgovor“ sa njima.

Ideja o reinkarnaciji ljudi kao čet botova očigledno pokreće mnoštvo pitanja privatnosti, o kojima se ne govori u patentu.

Da li će ljudi dobiti pravo da se isključe iz takvog sistema? Da li bi rođaci poginulih mogli da spreče druge da svoje preminule članove porodice pretvore u čet botove?

Takva pitanja su, naravno, sporna dok Majkrosoft (ili neko drugi) ne isporuči radni prototip.

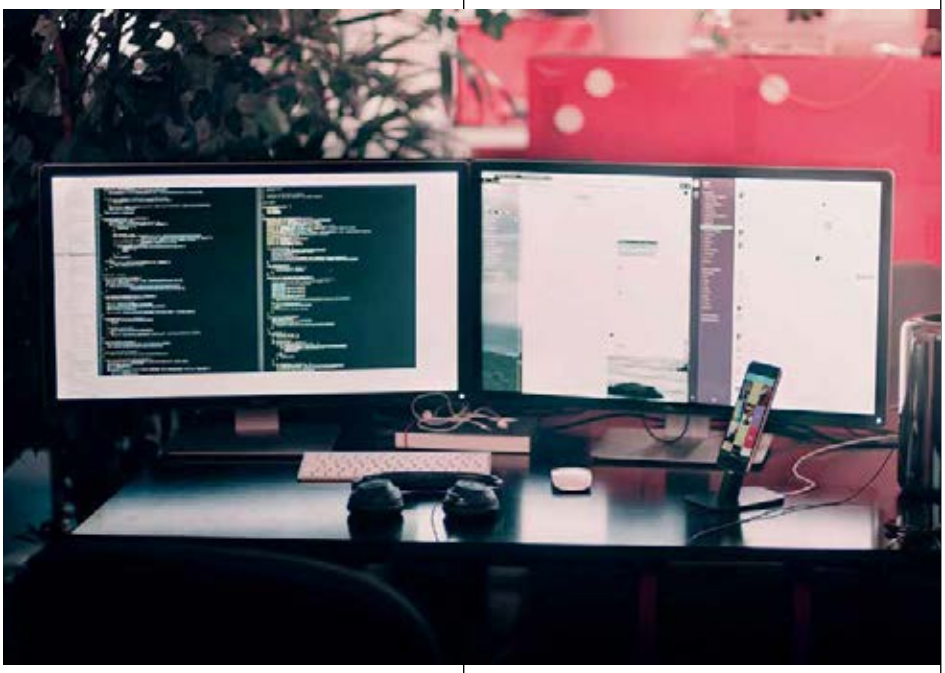
Hakerski napad na norveški parlament

Samo šest meseci od poslednjeg napada, hakeri su se ponovo infiltrirali u računarski sistem norveškog parlamenta i izvukli podatke, izjavili su norveški zvaničnici, a prenosi Tanjug.

Napad nepoznatih hakera povezan je sa ranjivošću Majkrosoftovog softvera Iksčejndž, saopštila je služba parlamenta, dodajući da je ovo međunarodni problem, preneo je Rojters.

Novi napad bio je žešći od prošlogodišnjeg, rekla je predsednica parlamenta Tone Vilhelmsen Troen na konferenciji za novinare.

„Ozbiljnost napada je posebno istaknuta činjenicom da se to događa uoči parlamentarnih izbora i da parlament rukovodi pandemijom“, istakla je ona, i dodala da je istraga o tome koje su informacije izvučene - u toku.



Raste izvoz kompjuterskih usluga iz Srbije

Izvoz kompjuterskih usluga iz Srbije iznosio je 1,37 milijardi evra u 2020. što je za 4,4 odsto više nego u 2019. godini, saopštio je Vojvođanski IKT klaster pozivajući se na podatke Narodne banke Srbije. Decembarski izvoz kompjuterskih usluga bio je čak za trećinu veći nego godinu dana ranije.

„Ovo nije rezultat na koji smo navikli proteklih godina kada je izvoz IT usluga rastao prosečnom stopom iznad 25 odsto, ali pandemija je učinila svoje. Januar i februar prošle godine pokazali su nastavak dugogodišnjeg trenda, no sa izbijanjem pandemije došlo je i do značajnog pada“, navodi se u saopštenju klastera koji okuplja najbolje domaće kompanije iz sektora informacionih tehnologija koje zapošljavaju više od 3.500 stručnjaka.

IT kompanije u Srbiji su, kako je rečeno, uspele da od marta 2020. godine kada je registrovan pad prihoda i broja projekata, očuvaju likvidnost i ljudske resurse „što je u datim okolnostima fantastičan podvig“.

„U poslednjem kvartalu ponovo je zabeležen uspon - kraj 2020. godine doneo je rast od iznad 30 odsto u poređenju sa decembrom prethodne godine“, kaže se u saopštenju i dodaje da oko 20.000 IT stručnjaka stoje iza ovog uspeha.

Građani žele da budu dobro informisani o zaštiti podataka o ličnosti

Građani Srbije žele da budu dobro informisani o zaštiti podataka o ličnosti, ali ne znaju dovoljno ni o svojim pravima, pokazalo je istraživanje javnog mnjenja o zaštiti ličnih podataka, čiji je rezultat predstavljen medijima u organizaciji Misije OEBS-a u Srbiji, a prenosi Beta. Pokazalo se da građani smatraju da su im najpotrebnije informacije o tome ko može da im traži lične podatke i kome da se obrate u slučaju zloupotrebe, ali su nepoverljivi prema primeni Zakona o zaštiti ličnih podataka.

Po rečima Slađane Brakus iz agencije TMG Insights koja je za OEBS sprovela to istraživanje, tek svaki treći građanin smatra da je dobro upoznat s ovom temom, dok polovini nisu dovoljno jasne informacije o tome.

„Kao najodgovorniji za zaštitu podataka o ličnosti percipiraju se država i zakonodavni okvir (73,8 odsto), a zatim sami pojedinci (65,3 odsto), što pokazuje da je jaka svest o ličnoj odgovornosti“, rekla je ona. Istraživanje je pokazalo i da građani mahom smatraju (76,5 odsto) da postoji visok rizik od ugrožavanja, odnosno zloupotrebe podataka o ličnosti.

„Skoro 40 odsto građana navodi da ne zna da li su njihovi podaci o ličnosti bili ugroženi, svaki drugi smatra da nisu, dok oko 12 odsto njih navodi da jesu“, rekla je ona.

Šef Misije OEBS u Srbiji, ambasador Jan Bratu, rekao je da je u savremenom dobu koje nosi rizike, istraživanje bilo nužno da bi se utvrdilo koliko građani znaju i da bi im se bolje zaštitilo to pravo.

„Ti podaci će pomoći Povereniku za informacije od javnog značaja i

zaštitu podataka o ličnosti da stvori nove politike koje će omogućiti zaštitu prava“, rekao je Bratu. Najavio je za naredne dve godine aktivnosti i kampanje radi obuke građana Srbije o zaštiti prava na privatnost.

Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti, Milan Marinović, rekao je da je s premijerkom Anom Brnabić razgovarao o izmeni strategije za tu oblast, kojom će se omogućiti Povereniku da ima organizacione jedinice van svog sedišta u Beogradu. „Posebno se to odnosi na obradu podataka o ličnosti zbog toga što je ona složenija i građani je ne razumeju“, rekao je Poverenik i najavio da će građani biti obaveštavani o zaštiti svojih ličnih prava.

Otvorena platforma za rešenja iz sajber bezbednosti

SHARE Fondacija je razvila Alate za digitalnu bezbednost – otvorenu platformu koja na jednom mestu daje uputstva i moguća rešenja problema sa radom sajtova, aplikacija ili uređaja, omogućava dodatno znanje o dobrim praksama zaštite informacionih sistema i digitalnih dobara i pruži savet ukoliko smo žrtva nasilja ili uznemiravanja posredstvom tehnologije.

Alati su namenjeni građanima, novinarima, aktivistima, ali i onima sa malo više tehničkih znanja ukoliko žele da se podsete. Cilj je, kako kažu iz Fondacije, da sopstvenim resursima i uz pomoć zajednice vremenom unapređuju bazu znanja, saveta i uputstava, kako bi Alati bili aktuelni i pratili promene u digitalnom okruženju.

DIGITALIZACIJA KAO GLOBALNI TREND I FAKTOR RASTA MODERNE EKONOMIJE

Biznisi idu tamo gde su kupci – a kupci su na digitalnim platformama

Kompanije koje posluju na digitalnim platformama, bilo da su velike ili male, povećavaju dostupnost svojih proizvoda većem broju potrošača, smanjuju troškove poslovanja, povećavaju efikasnost i konkurentnost. Digitalna nejednakost jedan je od najvećih rizika budućnosti, zajedno sa rizicima od klimatskih promena i propustima u sajber sigurnosti

Digitalizacija je najvažniji motor inovacija, konkurentnosti i ekonomskog rasta u svetu, navodi se u jednoj od stručnih studija „Digitalizacija kao globalni trend i faktor rasta moderne ekonomije“ grupe autora sa ukrajinskih univerziteta. Kao rezultat opsežnih istraživanja, oni dovode u direktnu vezu stepen digitalizacije i razvoja zemlje: prema njihovoj analizi, zemlje sa najvećim stepenom digitalnog razvoja su Norveška, Švedska, Švajcarska, Danska, Finska, Singapur. Jedan od osnovnih uslova digitalizacije jeste pristup kvalitetnom internetu, a budući da se najveći broj korisnika, prema podacima Svetske banke, nalazi u Evropi i centralnoj Aziji (75%), Srbija ima dobre predispozicije za razvoj digitalne ekonomije.

Osnovne prednosti ovog procesa su što kompanije koje posluju na digitalnim platformama, bilo da su velike ili male, povećavaju dostupnost svojih proizvoda većem broju potrošača, smanjuju troškove poslovanja, povećavaju efikasnost i konkurentnost, navode autori studije.

„Biznisi idu tamo gde su kupci - a kupci su na digitalnim platformama ili koriste digitalne uređaje da konzumiraju sadržaj i komuniciraju. Zato će poslovanje uz ignorisanje digitalnih platformi biti izuzetno teško u godinama koje dolaze”, kaže za naše čitaoce Vladimir Trkulja, osnivač Startita i ekspert za inovacije i razvoj biznis modela.

„Ulaganje u digitalnu transformaciju i dalje raste po godišnjoj stopi rasta od 15,5 odsto i očekuje se da će se 2023. približiti iznosu od 6,8 billiona dolara”, ocenila je kompanija za istraživanje tržišta digitalne transformacije, International Data Corporation (IDC) u svojoj analizi IDC FutureScape: Worldwide Digital Transformation 2021 Predictions.

Da je ova tvrdnja tačna pokazuje i USAID istraživanje „1000 preduzeća“ u kojem 80 odsto privrednika koji poseduju internet prodavnicu veruje da je prodaja putem interneta izuzetno važna, ako ne i važnija od tradicionalne prodaje.

Digitalna tehnologija i pristup obrazovanju

“Zapad koristi sve prednosti digitalne tehnologije, biznisi i pojedinci osećaju korist od ubrzane digitalizacije. Međutim, nerazvijene zemlje koje nemaju pristup digitalnoj tehnologiji (ili je ovaj pristup izuzetno limitiran) izopštene su iz ovog globalnog trenda. To negativno utiče na mogućnost obrazovanja, zapošljavanja i generalno stvaranja prilika za kvalitetniji život”, ističe Vladimir Trkulja.

Velike razlike mogu da se primete i među građanima pojedinačno. “Odlično je što postoji mogućnost da se koriste usluge eUprave, da se pretplatimo na digitalna izdanja časopisa, školujemo onlajn, naručujemo i plaćamo hranu digitalno – ali to ne mogu sebi da priušte svi građani naše zemlje. Da bi digitalizacija bila globalno pozitivan trend, moramo voditi računa da niko (ko želi da bude deo toga) ne bude izostavljen“.

Digitalna nejednakost jedan je od najvećih rizika budućnosti i prema Izveštaju o globalnim rizicima za 2021. Svetskog ekonomskog foruma (Global Risk Report 2021, WEF), koji analizira najveće svetske rizike na kraći i duži rok. Ovaj rizik nalazi se među onima koji su realni da se dogode u naredne dve godine.

Zajedno sa rizicima gubitaka nastalih usled ekstremnih vremenskih događaja, šteta na ekosistemima i propusta u sajber sigurnosti, u “top pet” našla se i digitalna nejednakost: jaz između onih kojima su digitalne tehnologije dostupne i onih kojima nisu i dalje se povećava među zemljama, ali i unutar samih država. To, posledično, ograničava ulaganje u digitalno obrazovanje, što vodi ka smanjenoj ekonomskoj mobilnosti pojedinca.

Ovaj rizik se, po rangiranju u ovom Izveštaju, nalazi među prvih pet kad je reč o najneposrednijim rizicima – onima koji su najverovatniji da svet zadese u naredne dve godine, zajedno sa krizom zapošljavanja i egzistencije, razočaranjem mladih, ekonomskom stagnacijom usled šteta po životnu sredinu koju je napravio čovek, i terorističkim napadima.

Ko može bez digitalizacije

Svet u kojem većina nas živi svakim danom postaje sve “digitalniji“, ali u određenim sferama života i poslovanja, može ostati stvar ličnog izbora.

Da li može „Samo bismo da probamo“?

“Najveća greška je odluka da se krene sa procesom digitalizacije pre nego što vlasnici i menadžment u potpunosti shvate šta sve to podrazumeva, koliko vremena i novca zahteva, i kakve će odluke (često i teške) morati da se donose. Ukoliko se ovaj proces započne bez čvrste rešenosti, već samo uz ideju da se ‘proba’ i ‘vidi kako to ide’, ceo proces digitalizacije (ili digitalne transformacije) je u najvećem broju slučajeva osuđen na propast. Takođe, bez jasno postavljenih ciljeva i definisanih metrika na osnovu kojih se njihovo postizanje prati – ne može se očekivati bilo kakav merljiv rezultat. I na kraju - potrebno je formirati kvalitetan tim koji će se dugoročno baviti procesom digitalizacije, sastavljen od zaposlenih i eksternih eksperata”, objašnjava Vladimir Trkulja.

Povratak na sadržaj


Vladimir Trkulja

"Kao što Vi kao pojedinac možete da izaberete da npr. slušate isključivo muziku na gramofonu, tako i određeni biznisi mogu da odluče da ne koriste bilo šta digitalno u svom poslovanju. Ali ako takav biznis funkcioniše u digitalizovanom društvu, takvom odlukom će smanjiti prihode – osim ukoliko se ne radi o nekim specifičnim biznisima čija je ključna vrednost zapravo oslanjanje na ne-digitalni pristup poslovanju. Ovakvih biznisa je sve manje, i sigurno je da će ih u budućnosti biti još manje", navodi on.

Najviše koristi digitalizacija je donela IT sektoru, jer ga je učinila nezaobilaznim delom svakog biznisa. Srbija na krilima tog globalnog trenda svake godine beleži rast izvoza IT usluga, a trend će se nastaviti jer su kompanije gladne za novim IT rešenjima, kao i za održavanjem i unapređivanjem postojećih rešenja. Značajno su digitalizovani i mediji, finansije i profesionalne usluge, ali se digitalizacija pozitivno reflektuje na sve sfere života: korišćenjem Internet of Things rešenja i mašinskog učenja, poljoprivreda beleži povećanje prinosa, proizvodni sektori veću efikasnost proizvodnje i manji škart, itd.

Kada kažemo da smo „digitalno transformisani"?

Direktor Centra za digitalnu transformaciju Predrag Nikolić kaže da nema preciznog odgovora na pitanje kada za jednu firmu možemo da kažemo da je digitalno transformisana. "Taj proces se nikad ne završava i neophodno je stalno hvatati korak sa savremenim trendovima. Pre 15 godina smo zamišljali da ekran reaguje na dodir, a sada već imamo kompjutere koji tako funkcionišu, imamo i mašine, robotiku, sve je to digitalna transformacija. Danas dronovima u poljoprivredi možemo da lociramo bolesnu biljku, ocenimo koji vremenski uslovi nas očekuju, pojava kojih štetočina. A uskoro će i roba da se isporučuje dronovima", objašnjava Nikolić.


Predrag Nikolić

Suština digitalne transformacije je, navodi on, da se uštedi vreme i novac. "Na taj način se ubrzavaju i poslovni procesi i poslovni modeli, obraća se više pažnja na e-komerc i e-marketing, naročito kroz društvene mreže".

Konsultanti i konsultacije za digitalnu transformaciju

Centar za digitalnu transformaciju - ćerka firma Privredne komore Srbije, organizuje obuke i sertifikaciju ljudi koji žele da budu konsultanti za digitalnu transofmaciju.

Šta je digitalizacija, a šta digitalna transformacija?

Termin „digitalizacija" poslednjih godina naročito je postao frekventan, ali i dalje mnogima nije jasno šta on tačno znači.

„Kada papirne fotografije prebacujemo u digitalne, kada muziku slušamo sa kompakt diskova umesto sa ploča, uopšte kada analogni signal prebacujemo u digitalni – reč je o informatizaciji", objašnjava za naše čitaoce Vladimir Trkulja.

Digitalizacija pak predstavlja upotrebu postojećih tehnologija i informacija za poboljšanje ili zamenu poslovnih procesa, stvaranje profita i stvaranje okruženja za digitalno poslovanje u kome informacija ima centralnu ulogu. "Najjednostavniji primer je upotreba gugl drajva za čuvanje i deljenje dokumenata umesto fioke zatrpane papirima, ili korišćenje neke platforme za internu poslovnu komunikaciju ili projektni menadžment. Primer su i mobilne aplikacije koje olakšavaju korisnicima pristup proizvodima ili uslugama, ubrzavaju ga i optimizuju digitalno poslovanje", kaže Trkulja.

Ono ka čemu se teži i što je kao proces najkompleksnije jeste digitalna transformacija - integracija digitalnih tehnologija u sva područja poslovanja tako da dovodi do njegovog transformisanja i kompletne promene poslovnih procesa. Primer su samohodna vozila koja će verovatno ostaviti bez posla veliki broj ljudi, ali će, s druge strane, povećati bezbednost vožnje a kompanijama smanjiti troškove.

Povratak na sadržaj

"Obučavamo ih po austrijskom modelu, a kasnije dovodimo i komisiju iz Austrije da ih sertifikuje po ISO standardu, da potom mogu da rade u celom svetu. Po završetku obuke, mi ih šaljemo u domaće firme gde započinju digitalnu transformaciju. Centar sufinansira 50 odsto troškova implementacije digitalne transformacije, do maksimalnog iznosa od 5.000 evra. Trudimo se da nađemo banke koje će ponuditi kredite za ove investicije", kaže Predrag Nikolić.

Dok su u 2018. godini digitalno transformisana preduzeća doprinela sa 13,5 biliona (13.500 milijardi) dolara globalnom nominalnom bruto domaćem proizvodu, za 2023. se predviđa da će ovaj iznos biti više od polovine ukupnog nominalnog BDP – 53,3 biliona dolara, najavljuje analitički portal Statista.com.

Jedan od prvih koraka ka uspostavljanju modela podrške digitalnoj transformaciji, posebno za mala i srednja preduzeća, bio je stvaranje mreže sertifikovanih konsultanata za digitalnu transformaciju sa znanjem i iskustvom u procesima povezanim sa digitalizacijom celokupnog poslovanja. CDT je u roku od dve godine obučio i sertifikovao (ISO 17024 standard) 43 konsultanta iz oblasti poslovnih modela i procesa, e-trgovine i društvenih medija, kao i IT bezbednosti i GDPR-a, i šest CDT trenera za buduće generacije sertifikovanih konsultanata. "Naš plan je da imamo oko 100 sertifikovanih konsultanata u naredne dve godine kako bismo dosegli 1.000 kompanija koje će proći kroz proces konsaltinga CDT- a, do kraja 2022. godine kroz Program podrške digitalnoj transformaciji za mikro, mala i srednja preduzeća", kaže Nikolić.

Daniela Ilić

INDEKS MREŽNE SPREMNOSTI

Koliko je Srbija spremna za "novo doba"?

Koliko je naša zemlja spremna za ulazak u novu eru pokazuju podaci Indeksa spremnosti mreže koje je uradila kompanija STL, jedan od vodećih integratora digitalnih mreža u svetu. Indeks spremnosti mreže (NRI) prepoznaje rasprostranjenost digitalnih tehnologija u današnjem umreženom svetu i fokusira se na četiri osnovne dimenzije, odnosno stuba: tehnologiju, ljude, upravljanje i uticaj. Obuhvata razna pitanja - od budućih tehnologija poput AI i Interneta stvari, do uloge digitalne transformacije u postizanju ciljeva održivog razvoja.

Indeks mrežne spremnosti 2020. rangira ukupno 134 ekonomije koje zajedno čine gotovo 98 procenata globalnog bruto domaćeg proizvoda (BDP). Švedska je i dalje najbolja. Najviše je napredovala Danska, koja je skočila sa šestog na drugo mesto u ovogodišnjem indeksu, pomerajući Singapur i Holandiju za po jedno mesto na treće, odnosno četvrto mesto. Švajcarska je, kao i prošle godine, zaokružila prvih pet. U prvih 10 ulaze još Finska, Norveška, Sjedinjene Države, Nemačka i Ujedinjeno Kraljevstvo.

Srbija se, sa proračunatim srednje visokim dohotkom, nalazi na 52. mestu: ispred nje su Slovenija (27), Mađarska (39), Hrvatska (43), Bugarska (46) i Rumunija (49), a iza nje je Crna Gora (58). Naša zemlja najviše je napredovala u digitalnoj transformaciji u oblasti ekonomije, ali bi se, kažu stručnjaci, moglo učiniti više za poboljšanje ekonomskih performansi kod zaposlenih. Takođe, dosta smo uradili kad su u pitanju propisi, odnosno, prilagođavanje zakonodavstva savremenim tokovima, tu se pre svega misli na Zakon o zaštiti podataka o ličnosti. Kad je u pitanju očekivani NRI rezultat s obzirom na nivo prihoda u ekonomiji, Srbija je znatno iznad linije trenda, što sugeriše da ima veću spremnost mreže nego što bi se očekivalo, s obzirom na nivo njenog dohotka. Srbija je rangirana na 6. mestu u grupi zemalja s višim srednjim dohotkom. Indikatori u kojima Srbija ima posebno dobre rezultate uključuju preduzeća sa veb sajtom, stopu pismenosti odraslih i IKT regulatorno okruženje. Najslabiji smo u oblastima vezanim za pristupačnost tehnologije, kao i za čistu energiju. Nesaglasnost u razvoju očituje se u ogromnoj razlici u ocenama stope digitalne pismenosti odraslih koja je izrazito niska, i aktivne pretplate na širokopojasne mobilne uređaje, koja je izuzetno visoka. Slične diskrepance nalazimo i pri ocenjivanju regulatornog okruženja za IKT koje je veoma nisko, i visokoj oceni za poslovnu upotrebu digitalnih alata. Prilično se visoko držimo kad je u pitanju broj zaposlenih u gig-ekonomiji, a loši smo kad su u pitanju ulaganja države u razvoj i istraživanje. Najbolje rezultate postižemo u korišćenju virtuelnih društvenih mreža i slobodi odlučivanja o životu, a loše nam idu ulaganja u visoke studije i plaćanje softvera.

Ivana Radoičić

Povratak na sadržaj

RIZICI DIGITALNOG POSLOVANJA

Loši momci dobro se kriju

Napadači su tihi, raspoređeni širom sveta, i izuzetno tehnički potkovani. S druge strane, stručnjake za odbranu teško je obezbediti i zadržati

Vest da je krajem prošle godine meta hakerskog napada bila i američka IT kompanija SolarWinds, što se odrazilo i na vladine agencije SAD i na brojne druge velike IT kompanije, ozbiljno je uzdrmala javnost. Napad je narušio lanac snabdevanja ove kompanije, čime je ugroženo oko 18.000 drugih kompanija!

Prema Izveštaju o globalnim rizicima Svetskog ekonomskog formuma za 2021, rizici od napada na digitalno poslovanje – sajber rizici i dalje su u vrhu globalnih rizika. Pandemija je ubrzala usvajanje tehnoloških dostignuća, ali i pokazala nespremnost na zaštitu, takozvanu "sajber ranjivost", i iznela "na sunce" tehnološke nejednakosti unutar, ali i između država.

Šta napadači žele, i kako mogu da nam naude?

Glavni razlog za sajber napade je finansijska korist kroz direktnu krađu: novca sa računa, podataka ili drugih informacija koje mogu da preprodaju na crnom veb tržištu, ili da ih zloupotrebe na drugi način. Zatim, mogu da nam blokiraju sistem i tako zaustave poslovanje – kako bi nam ponovo omogućili da radimo, obično traže otkup koji nije mali. Često, motiv može biti i samo da se nanese šteta konkurenciji, a javna je tajna da neke kompanije upravo u tom cilju iznajmljuju hakere, kako bi se domogle dela tržišnog kolača.

"Kao i bilo koji drugi strateški društveni izazov, i sajber bezbednost se ne može rešavati u zatvorenom sistemu: za to je neophodno partnerstvo između industrija, poslovnih lidera, regulatora i kreatora politika", stav je Svetskog ekonomskog foruma.

Top pet sajber izazova u 2021

Svetski ekonomski forum dao je i listu pet glavnih izazova u tekućoj godini, kad su u pitanju rizici po biznise u digitalnom okruženju.

Sve složeniji izazovi kad je reč o odbrani poslovanja u digitalnom svetu. Mašinsko učenje i veštačka inteligencija sve se brže prihvataju, i raste zavisnost od softvera, hardvera i infrastrukture u "oblaku". Čak i države vode međusobne bitke – od plasiranja lažnih vesti kako bi uticale na izbore u drugim zemljama, pa sve do napada na kritičnu infrastrukturu. U narednim mesecima riziku može biti izložena i isporuka vakcina, baš kao što su početkom pandemije bili ugroženi zdravstveni sistemi.

Zato bi, kako predlažu stručnjaci ove organizacije, svetski lideri morali da sajber bezbednost postave kao prioritet kad je reč o nacionalnoj bezbednosti. "Napadači su tihi, raspoređeni širom sveta, i izuzetno tehnički potkovani. Zato

Povratak na sadržaj

Veb kriminalac Džoker odlazi u penziju?!

Kriminalac koji stoji iza stranice Joker's Stash koja trguje ukradenim podacima sa kreditnih i debitnih kartica, sredinom februara je najavio da će svi serveri i rezervne kopije biti izbrisani, i ova stranica više neće moći da se otvori. Razlog je taj što ovaj kriminalac poznat kao Džoker - odlazi u penziju, prenosi Forbs.

U penziji će mu, kako se čini, biti prilično dobro ukoliko njega i njegove kolege ne uhvate Interpol ili FBI: imovina koju imaju procenjuje se na oko 2,1 milijardu dolara u bitkoinima. Zaradu su ostvarivali kroz proviziju na transakcije koje su se obavljale na ovoj platformi od 2014. godine, kada je pokrenuta. Naime, Joker's Stash je bilo najveće "crno" onlajn tržište ukradenih podataka sa kartica. Platforma nije služila samo za prodaju ukradenih podataka već je omogućavala kriminalcima da peru svoje nezakonito stečene kriptovalute. Sistem je funkcionisao tako da su se ukradeni podaci sa kartica koristili za kupovinu poklon kartica ili drugih predmeta kojima se lako trguje odnosno koji se lako mogu unovčiti. Prema pisanju Forbsa, još 2019. Prijavljeno je da se jedna baza platnih kartica, sa više od milion "sveže" ukradenih podataka, nudi na prodaju za 130 miliona dolara.

je neophodna saradnja javnog i privatnog sektora – privatnom sektoru će morati da bude na raspolaganju ono što je u domenu javnog sektora, a to je kreiranje politika, modela podsticaja tržišta, i masovne obuke", kaže se u Izveštaju Svetskog ekonomskog foruma.

Složeni propisi, različiti od zemlje do zemlje. Napadači se ne obaziru na granice, niti na lokalne zakone, a oni koji se bave odbranom morali bi da računaju na to da različite zemlje imaju različitu regulative. Kompanije, nasuprot, moraju da se bore u skladu sa svojim budžetima, a da se istovremeno pridržavaju propisa, što izaziva prilične napore posebno kad se posluje na globalnom tržištu. Kreatori politika trebalo bi da smanjuju regulatornu složenost, uz istovremeno povećanje zaštite, a posebno je važna međusobna saradnja između različitih kreatora politika.

Zavisnost od dobavljača. Očekuje se da će povezani uređaji već ove godine dostići brojku od 27 milijardi, zahvaljujući trendovima poput 5G, IoT i smart Sistema, a sve je dodatno podržano radom od kuće koji takve uređaje podrazumeva. Treba imati u vidu da većina tih uređaja zavisi od nekoliko globalnih proizvođača, a opasnost od prekida lanca nabavke kod pojedinačnih proizvođača pokazala se upravo prilikom nedavnog napada na SolarWinds.

Nedovoljno stručnjaka za sajber bezbednost. Prioriteti svakog preduzeća treba da uključuju proaktivni plan za usavršavanje sopstvenih kadrova u oblasti sajber bezbednosti: ovu vrstu stručnjaka prilično je teško obezbediti i zadržati, pa se predlaže "gajenje" sopstvenih kadrova, tao što će se znanje prenositi sa starijih na mlađe.

Teškoće u otkrivanju sajber kriminalaca. Bavljenje ovom vrstom kriminala prilično je lagodno, s obzirom na to da je do nedavno procenat otkrivenih kriminalaca u SAD bio svega 0,05 odsto, a u drugim zemljama čak i manje.

Crno internet tržište – šta se sve prodaje

Verovatno su sve ovo razlozi što crno internet tržšte cveta: oni koji su se odvažili da posete sajtove koji funkcionišu u paralelnom internet univerzumu kažu da se tamo može naći gotovo sve što nije legalno: od oružja, droge, pornografije, do kradenih podataka, kako o pojedincima tako i o čitavim kompanijama. Sredinom februara na crnom internet tržištu našle su se i vakcine protiv Covid-19, koje su se prema saopštenju kompanije Kaspersky koje je preneo Tanjug, prodavale po ceni od 250 do 1.200 dolara: i Fajzer, i AstraZeneka i Moderna, a reklamirane su i vakcine koje nisu odobrene od zvaničnih organa.

> Bavljenje sajber kriminalom prilično je lagodno, s obzirom na to da je do nedavno procenat otkrivenih kriminalaca u SAD bio svega 0,05 odsto, a u drugim zemljama čak i manje

Prošle godine jedna hakerska grupa ponudila je podatke o čak 73,2 miliona korisnika raznih sajtova, među kojima je najviše bilo onih sa sajta za upoznavanje Zoosk – oko 30 miliona, i sa servisa Chatbooks – 15 miliona. Na crnom tržištu našlo se i više od 600.000 naloga korisnika italijanskog provajdera Email.it, koji sadrže šifre korisnika, sigurnosna pitanja i odgovore, sadržaj mejlova isms poruka. Cene ovih podataka kretale su se od 0,5 do tri bitkoina, u zavisnosti od "odabranog paketa".

Tamo se, inače, mogu kupiti i Fejsbuk profili po prosečnoj ceni od 75 dolara, i Instagram i Tviter profili za dvadesetak dolara manje. Njih kupci koriste uglavnom radi povećanja broja lažnih pratilaca, ali i za krađu identiteta. Gugl nalozi su nešto skuplji – oko 200 dolara, ali donose i veću korist jer mnogi u prepisci čuvaju brojne lične i poslovne tajne. Najskuplji su nalozi za onlajn plaćanja koji, kažu, koštaju oko 350 dolara.

Selena Stanislavska

Povratak na sadržaj

ŠTA HAKERI NAPADAJU U SRBIJI

Domaći hakeri aktivni, stranima još nismo mnogo zanimljivi

U Srbiji je svake godine primetno sve više krivičnih dela visokotehnološkog kriminala, pre svega, napada zlonamernim računarskim programom „ransomware“. Žrtve ove specifične vrste sajber iznude uglavnom su male i srednje firme ali i javna preduzeća, pa i građani

Hakerski napadi, pretnje i uopšte svi oblici visokotehnološkog kriminala povećani su tokom pandemijske godine za 50 odsto, prema statističkim podacima Ministarstva unutrašnjih poslova (MUP). U 2019. godini bilo je ukupno 812 zahteva nadležnih tužilaštava za provere koje se odnose na krivična dela visokotehnološkog kriminala, dok ih je u istom periodu 2020. godine bilo ukupno 1203.

Štete od hakerskih napada kreću se od nekoliko stotina evra do nekoliko stotina hiljada evra, kad se koriste „Bussiness e-mail compromise“ (BEC) prevare ili „ransomware“ ucenjivački softver, kažu u MUP-u.

Tokom pandemije, povećan je, takođe, broj krivičnih prijava. Prema podacima MUP-a, u toku 2019. godine podneto je 168 krivičnih prijava protiv 153 osumnjičena, dok je prošle godine podneto 235 krivičnih prijava protiv 222 osumnjičena zbog sumnje da su počinili neko krivično delo visokotehnološkog kriminala.

U Srbiji je, kao i drugim državama, svake godine sve veća zastupljenost krivičnih dela visokotehnološkog kriminala, kako kažu u Ministarstvu unutrašnjih poslova, pre svega napada zlonamernim računarskim programom „ransomware“.

“Žrtve ove specifične vrste sajber iznude su uglavnom male i srednje firme, ali i javna preduzeća, pa i građani čiji računarski sistemi nisu dobro zaštićeni, tako da su njihove poslovne baze podataka bile izložene napadima. Nakon napada svi fajlovi su zaključavani (kriptovani), a kao otkup su zahtevane uplate isključivo u virtuelnim valutama (uglavnom bitkoin i monero)“, navode u MUP-u.

BEC prevara

U poslednjih nekoliko godina, u oblasti prevara na internetu uočen je kriminalni trend poznat kao „Kompromitovani poslovni e-mail“, odnosno tzv. BEC prevara („Bussiness e-mail compromise“).

“Suština ove finansijske prevare je da kriminalci na internetu pre-

Povratak na sadržaj

sretnu i preuzmu komunikaciju između poslovnih partnera, uglavnom preko elektronske pošte i da se novac namenjen plaćanju roba ili usluga, uz upotrebu falsifikovane dokumentacije, preusmeri na račune pod kontrolom kriminalaca. Nezakonito prikupljanje ličnih i poslovnih podataka, nakon kršenja mera zaštite, predstavlja sve veću pretnju i u Srbiji“, kažu u MUP-u.

Finansijske institucije su u odnosu na ostale sektore najprimamljivije za sajber kriminalce.

Vladislav Ujić, konsultant za IT bezbednost i zaštitu podataka Centra za digitalnu transformaciju potvrđuje da su najznačajnije oblasti poslovanja za napadače svakako sve finansijske institucije, telekom operateri, kao i osiguravajuće kuće.

Vladislav Ujić

“Osim njih, oblasti koje se napadaju više od ostalih su iz delatnosti konsaltinga odnosno usluga, kao i proizvodne delatnosti. Primarna meta napada su e-mail konverzacije i presretanje pisane komunikacije“, kaže Ujić.

Sajber napadima, prema njegovim rečima, pokušava se direktno ili indirektno ostvariti finansijska korist ili načiniti druga (ne)povratna šteta napadnutoj kompaniji.

Sajber-kriminalci često koriste dobijene podatke da bi olakšali dalju kriminalnu aktivnost, koja vrlo često izlazi izvan okvira krivičnih dela visokotehnološkog kriminala, pa se koriste za pranje novca, nezakonito organizovanje igara na sreću ili klađenje na internetu, kažu u MUP-u. “Nastavlja se trend da kriminalci koriste tzv. DDoS napade, odnosno distribuirano uskraćivanje usluge - Distributed Denial of Service, kao sredstvo za napade na kompanije u privatnom i javnom sektoru. Ovakvi napadi se rade ne samo zbog finansijske dobiti, već iz ideoloških, političkih ili čisto zlonamernih razloga“, kažu u MUP-u.

Ta vrsta napada nije samo jedna od najčešćih, već postaje sve pristupačnija i sve jeftinija za sve korisnike interneta, sa relativno niskim rizikom za otkrivanje. Već je postala popularna, i poznata kao „Kriminal kao servis“ (Crime-as-a-Service), saznajemo u Ministarstvu.

Darknet

Falsifikovanje i zloupotreba platnih kartica je i dalje vrlo prisutna u Srbiji, podaci o skimovanim („skimming“ - ilegalno prikupljanje podataka sa platnih kartica posebnim uređajima - skimerima) platnim karticama se vrlo često prodaju preko Darkneta, a kriminalci iz Srbije su često vrlo aktivni na ovim forumima, ukazuju u MUP-u.

Prema oceni Vladislava Ujića, posmatrajući globalne napade Srbija nije među zemljama koje su pre-

Zloupotrebe kriptovalutama

U poslednjih godinu dana, usled povećanja interesovanja građana za investiranje u kriptovalute (zbog njihovog naglog skoka vrednosti) često se dešavaju zloupotrebe digitalne imovine, kažu u Ministarstvu unutrašnjih poslova.

“Kriminalci koriste e-novac za finansiranje kriminalnih aktivnosti, pa se kriptovalute sve češće pojavljuju ne samo u krivičnim delima visokotehnološkog kriminala kao sredstvo za plaćanje, već i u klasičnim krivičnim delima organizovanog kriminala i korupcije, pranja novca, trgovine narkoticima i oružjem na Darknetu, iznudama i ucenama“, kažu u MUP-u.

Bitkoin i dalje predstavlja najčešću kriptovalutu sa kojom se suočavaju policijski službenici i tužioci u Srbiji, iako su na tržištu elektronskog novca sve popularnije i neke druge valute (Ethereum, Ripple, Litecoin, Stellar, Bitcoin Cash).

Zabeleženo je pojačano interesovanje u Srbiji za tzv. „rudarenjem“ kriptovaluta, postoji tržište na kome se e-valute kupuju, prodaju i razmenjuju za standardne valute (evre, dolare, dinare), određeni broj preduzeća aktivan je na tom tržištu, postavljen je veći broj ATM aparata na kojima je moguće kupovati i prodavati elektronski novac.

Novi trend visokotehnološkog kriminala „Cryptojacking“, koji se odnosi na neovlašćeno iskorišćavanje širokopojasnog interneta korisnika i iskorišćavanje procesorske snage njihovih računara za rudarenje kriptovaluta, još uvek nije zabeležen u Srbiji kroz krivične procese, što ne znači da nije već prisutan u Srbiji.

“Ono što je zabrinjavajuće je veliki porast prevara kod digitalne imovine, gde se prevaranti pojavljuju kao navodni investitori ili osnivači novih kriptovaluta, koji navodno garantuju određenu dobit za one koji ulažu u tu „novu“ e-valutu. U pitanju su klasične piramidalne prevare ali sada na novom terenu, u virtuelnom prostoru“, kažu u MUP-u.

Pored navedenog, sve su češće i krađe poseda nad kriptovalutama, jer građani koji investiraju u e-novac imaju malo tehničkih znanja o načinima kako to funkcioniše i kako da zaštite svoje privatne ključeve, odnosno posed nad kriptovalutama. Krađe digitalnog novca najčešće se dešavaju, kako kažu u MUP-u, kada hakeri zaraze malverom uređaj na kojima se nalaze novčanici sa privatnim ključevima.

Povratak na sadržaj

više interesantne svetskim hakerima, i po broju napada svih vrsta na godišnjem nivou nalazi se na 73. mestu na svetskoj rang listi, koju objavljuje kompanija Kaspersky.

"Štete koje se na godišnjem nivou proizvedu u Srbiji od hakerskih napada mere se u milionima evra", kaže Ujić.

Precizniji podaci o konkretnim napadima uglavnom se ne objavljuju javno jer sve napadnute kompanije pokušavaju da zaštite i svoju reputaciju i svoje klijente, pa zbog toga ne izlaze u javnost sa tim informacijama, napominje on.

"Svakako je kompanija koja pretrpi napad u obavezi da prijavi nadležnim institucijama sve detektovane upade u svoj informacioni sistem kao i sve vrste virusnih ili drugih problema koje u toku poslovanja ustanovi", kaže Ujić.

Ipak, iz iskustva na poljima IT bezbednosti i zaštite podataka i u radu sa kompanijama iz Srbije, on ocenjuje da se ne posvećuje dovoljno pažnje i ne odvaja dovoljno resursa, finansijskih i ljudskih, svim aspektima zaštite.

Veći broj krivičnih prijava

"Česte žrtve tehničkih napada različitih vrsta su novinari, onlajn mediji, ali i aktivisti i organizacije civilnog društva. Od 2014. godine Share fondacija je zabeležila više od 70 tehničkih napada na ove aktere. Pretpostavlja se da ih je bilo mnogo više jer se informacije o napadima često ne objavljuju", ukazuju u toj Fondaciji.

Građani bi trebalo da vode računa o tzv. „fišing" prevarama koje se šalju mejlom ili preko ili čet poruka, a u kojima se od njih traži da kliknu na određeni link ili otvore fajl poslat u prilogu, napominju u toj Fondaciji.

> U Ministarstvu unutrašnjih poslova kažu da su prošle godine podneli 235 krivičnih prijava protiv 222 osumnjičena zbog sumnje da su počinili neko krivično delo visokotehnološkog kriminala

Lokalni i globalni hakeri

Podatke o lokalno organizovanim hakerskim grupama teško je pronaći, ali takve grupe svakako postoje, kaže Ujić.

"Iako postoje, one na globalnom nivou ne predstavljaju neke značajne „igrače" koji bi na taj način bili zanimljivi široj javnosti. Opseg njihovog delovanja je više lokalno-regionalnog nego globalnog karaktera – napadi su uglavnom usmereni na web sajtove i portale u Hrvatskoj, Albaniji i okruženju", ocenjuje on.

Najnovije spominjanje „hakera iz Srbije" desilo se, kako on kaže, u vezi sa predsedničkim izborima u SAD i postojale su određene kontraverzne indikacije koje se odnose na daljinsku kontrolu sistema glasanja, a dovodile su se u vezu i sa pojedincima koji se nalaze i deluju u Srbiji.

"Nepisano pravilo je da hakerske grupe ne koriste lokalne servere i IP adrese kad kreiraju napade pa je samim tim neuporedivo teže odrediti odakle zapravo napadi dolaze i ko iza njih stoji", navodi Ujić.

Olivera Bojić

Povratak na sadržaj

KOJI SU KORACI U DIGITALNOJ TRANSFORMACIJI MSP

Uporedo razvijati i biznis i IT sistem

Piše: Miroslav Savanović, konsultant u oblasti digitalne transformacije, i član Savetodavnog odbora Inicijative za jačanje bezbednosti podataka

Kada preduzeće iz grupe MSP odluči - ili ga prilike na tržištu poput ovih u vreme pandemije - nateraju da počne da razmišlja kako da preživi ili čak unapredi svoje poslovanje, trebalo bi da napravi sveobuhvatno sagledavanje poslovanja, rizika i izazova koji mu prete, da ponderiše njihov uticaj, analizira poslovne procese i sopstveni informacioni sistem - ako ga uopšte ima. Zatim, da segmentira i analizira svoje kupce i njihove potrebe, kao i svoje dobavljače, i komunikaciju s njima. Dalje, da preispita načine upravljanja u preduzeću, analizira i pripremi svoje zaposlene, utvrdi na koga od njih se može osloniti u novoj realnosti koja zahteva novi pristup u angažovanju menadžera i zaposlenih koji mogu da osmisle i sprovedu disrupciju (raskrstiti sa starom praksom koja više ne funkcioniše, smisliti novi proizvod, uslugu, distribuciju, odustati od starih modela koji više ne funkcionišu).

Sve ovo treba staviti „na papir“, postaviti vremenski određene ciljeve, definisati mere, napraviti strategiju i operativni plan sprovođenja. Sve to nije nimalo lako. Oni koji to sve ne mogu sami, mogu pronaći konsultanta za digitalnu transformaciju, a dosta informacija dostupno je i besplatno preko različitih fondova i stimulacija koje daje Vlada. Ovo je samo deo onoga što čini digitalnu transformaciju.

Ukoliko Vaše preduzeće nema informacioni sistem, trebalo bi intenzivno da radite na tome da ga uvedete, i to prvo onaj segment koji se odnosi na odnose s kupcima, prodaju i povećanje prihoda, a to je CRM (Customer Relations Management), a tek nakon toga ERP (Enterprise Resource Planning) koji će omogućiti da se optimizuju unutrašnji procesi i smanje troškovi.

Da bi bilo koji aplikativni sistem funkcionisao, treba mu neka IT infrastruktura na kojoj će se te aplikacije izvršavati. Kod definisanja bilo kojeg IT sistema mora se voditi računa o potrebnoj procesorskoj snazi, memorijskom prostoru za bazu podataka, redundanciji, bekapima, sigurnosti podataka naročito, neprekinutom poslovanju i drugim performansama IT sistema. O svemu ovom brine dobar arhitekta sistema. Teško je sva znanja potrebna za kvalitetno funkcionisanje IT sistema smestiti u jednog čoveka, pa je najbolje angažovati kvalitetnu IT kompaniju koja će naći rešenje primereno potrebama i rizicima poslovanja MSP, bilo da je to izbor sopstvene IT infrastrukture ili cloud rešenja koje se sve više nameće kao budućnost zajedno s uslugama tipa IaaS, PaaS, SaaS, DaaS, FaaS.

Sve navedeno treba održavati, usavršavati pa i obnavljati ako se radi o sopstvenoj IT infrastrukturi. Čitav IT sistem treba da bude u funkciji biznisa koji podržava. Ako biznis ima nove zahteve, IT sistem mora da ima sposobnost i resurse da ga prati. Mnoge kompanije starog kova koje su imale stabilne tradicionalne biznise nisu menjale IT sisteme desetinama godina. Danas to više nije moguće jer se sve ubrzalo i digitalna transformacija podrazumeva brže odzive na turbulencije, vanredne situacije i zahteve tržišta, češće promene poslovnih modela, proizvoda i usluga, promene aplikacija koje ih prate, obradu sve većeg broja podataka itd. Trendove u IT-u ne treba pratiti radi samih trendova već u meri u kojoj ti novi trendovi pogoduju razvoju biznisa kojim se preduzeće bavi.

U takvoj situaciji jedno MSP bi trebalo da ima bar jednog IT stručnjaka u samom preduzeću i ozbiljnu IT kompaniju kao partnera koja će mu pružati potrebnu podršku. A može to biti i eksterno angažovan IT stručnjak.

Koliki su godišnji troškovi IT funkcije koja je u dobroj meri nosilac digitalne transformacije poslovanja? Teško je dati takvu procenu, ali u zavisnosti od industrijske oblasti u kojoj preduzeće radi, nivoa informatizacije i stvarno provedene digitalne transformacije, taj procenat se prema različitim izvorima kreće u rasponu 3-10 odsto od godišnjeg prometa.

Povratak na sadržaj

SOCIJALNI INŽENJERING:
NAJČEŠĆI OBLICI NAPADA

Prepoznajte da biste se odbranili

Zloupotrebe su najčešće usmerene na preduzeća, odnosno na zaposlene koji se navode da odaju lozinke i podatke o zaposlenima i IT sistemu, ili da prekrše bezbednosne mere tako što bi obavili određenu uplatu, omogućili ulaz u prostorije, i slično

Kao što se celokupno poslovanje seli u digitalni svet, tako ni prevaranti više ne koriste samo tradicionalne kanale komunikacije za ostvarivanje svojih ciljeva. Naravno, i dalje ima onih koji će pokušati da obmanu čuvara na ulazu u firmu i uvuku se u prostorije kako bi eventualno opljačkali pojedince ili ukrali imovinu, ali su u poslednje vreme sve popularnije "digitalne prevare" odnosno socijalni inženjering.

Digitalni prevaranti računaju na ljudske emocije, lakovernost ali i radoznalost, koja je naročito izražena baš u vreme vanrednih situacija. Mnogi su imali priliku da se u to uvere i tokom velikih "pikova" pandemije, kada su im stizali brojni linkovi "sa najnovijim informacijama" – što o vakcini, što o prirodnim lekovima, ali i "detalji o slepom mišu od kojeg je sve krenulo". U prvim mesecima pandemije, broj napada preko socijalnog inženjeringa rastao je munjevitom brzinom!

Oni se ne bave pretnjama, već često uspevaju da uspostave i prijateljski odnos sa žrtvom, pa ona uopšte nije svesna da je napadnuta - naprotiv, često se oseća srećnom i zadovoljnom jer misli da je nekome pomogla, ili da je uspešno odradila neki posao.

Zloupotrebe su najčešće usmerene na preduzeća, odnosno na zaposlene koji se navode da odaju lozinke i podatke o zaposlenima i IT sistemu, ili da prekrše bezbednosne mere tako što bi obavili određenu uplatu, omogućili ulaz u prostorije, i slično. Mete su i brojevi kartica i bankovnih računa, ali i podaci za koje se kasnije može tražiti otkupnina. U nastavku su najčešći oblici napada, a kao izvor smo koristili Nacionalni CERT.

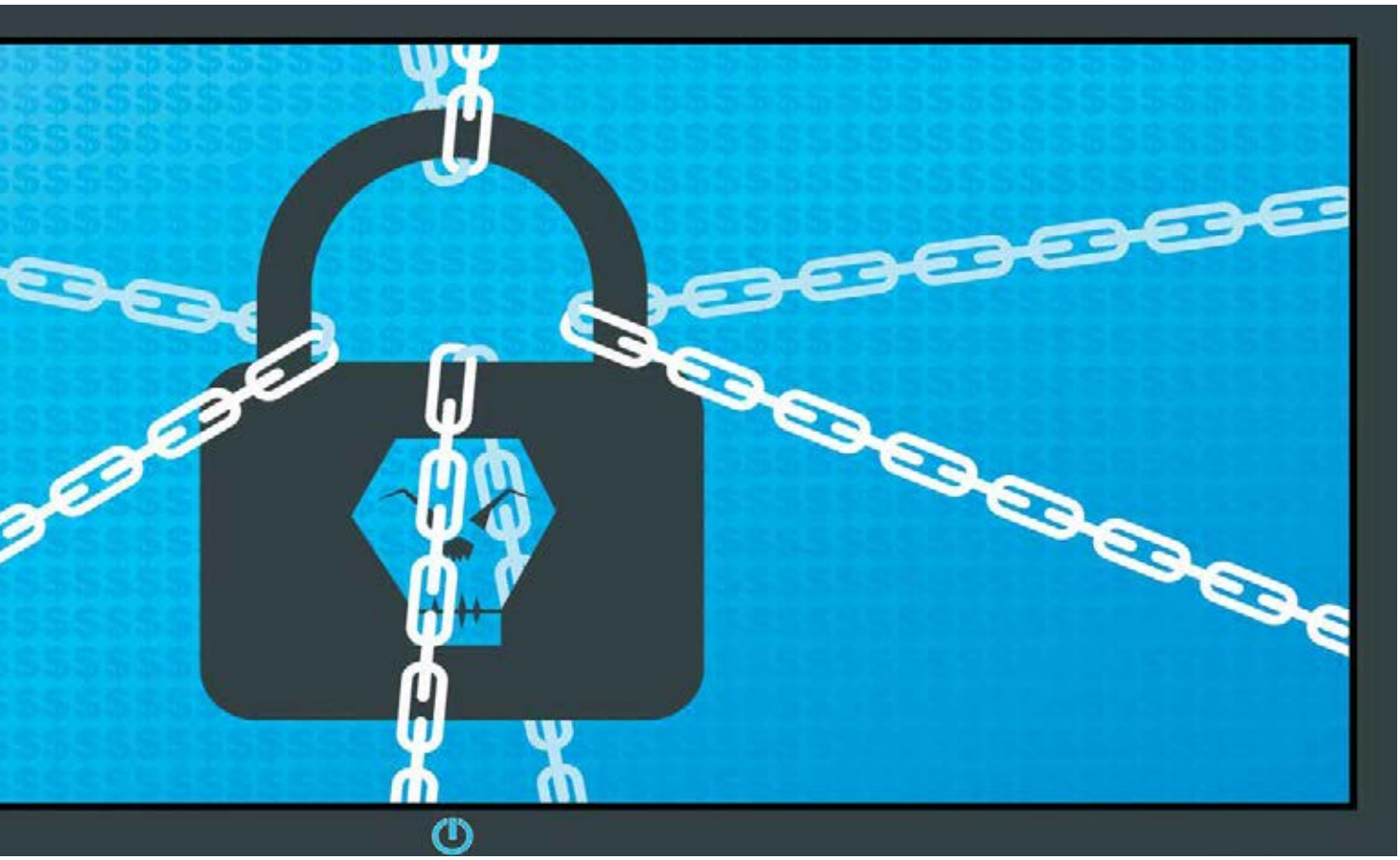
Phishing

Stiže nam poruka (mejl ili SMS) koja nam stvara osećaj straha, hitnosti ili radoznalosti - i navodi nas da kliknemo na priloženi link ili otvorimo prilog. Klik na link vodi na lažnu stranicu, koja liči na legitimnu, i kreirana je u cilju prikupljanja podataka kao što su e-adresa i lozinka. Klik na „Enable Content" ili „Enable Editing" u dokumentu iz priloga, automatski pokreće zlonamerni softver koji ubrizgava određene procese u operativni sistem primaoca, kako bi onemogućio detekciju od strane antivirusa i drugih bezbednosnih softverskih rešenja.

Spear phishing

Ciljana verzija phishing prevare kojom napadač bira određen osobu ili kompanije, kreira tekst poruke na osnovu njihovih karakteristika, radnih mesta i kontakata kako bi napad bio manje upadljiv. Ukoliko se napad vešto izvede, teško ga je detektovati a procenat uspešnosti je visok. Jedan od scenarija je onaj u kojem se napadač predstavlja kao kolega iz IT službe i šalje poruku e-pošte jednom ili više zaposlenih. Tekst poruke, potpis i način komunikacije je vrlo sličan uobičajenom načinu komunikacije sa IT službom što primaoce navodi da misle da je poruka autentična.

Povratak na sadržaj



Porukom se traži od primalaca da promene lozinku klikom na link, koji ih preusmerava na zlonamernu internet stranicu na kojoj napadač snima sve kredencijale koje unesu.

Baiting

Sadrži „mamac“ u vidu neke stvari koja će privući žrtvu, ili obećanje da će dobiti neku nagradu. Na primer, napadači ostavljaju USB sa zaraženim malverom na vidljivom mestu gde potencijalne žrtve mogu sigurno da ga vide (npr. toalet, lift, parking, hodnik). USB ima intrigantnu nalepnicu' kako bi ga žrtva iz radoznalosti ubacila u poslovni ili kućni računar i automatski instalirala zlonamerni softver. Onlajn baiting napad za mamac koristi oglase za besplatno preuzimanje muzike, filmova ili aplikacija sa internet stranica koje su zaražene zlonamernim softverom.

Pretexting

Podrazumeva prethodnu radnju sa dobro osmišljenim scenarijom kako bi se došlo do ličnih podataka žrtve, i obično se sprovodi telefonom ili u direktnom kontaktu. Podatke zatim koristi za krađu identiteta ili u za izvršenje nekog drugog krivičnog dela. Napadač se najpre lažno predstavlja ali bira identitet autoriteta (policajac, bankarski ili poreski službenik) kako bi uspostavio odnos poverenja, a zatim traži podatke radi navodne provere (JMBG, adresu stanovanja, telefonske brojeve, datum odmora, bankovne evidencije pa čak i podatke o merama zaštite i bezbednosti kompanije u kojoj je žrtva zaposlena. Napadač može da se predstavi kao spoljni revizor IT usluga i zatraži dozvolu za ulazak u zgradu. Dok fišing napadi uglavnom zloupotrebljavaju strah i hitnost, ovi napadi se oslanjaju na izgradnju lažnog osećaja poverenja sa žrtvom, kroz verodostojnu priču koja žrtvi ostavlja malo prostora za sumnju.

Scareware

Obuhvata lažne alarme ili upozorenja da nam je operativni sistem zaražen, i poziva da instaliramo softver koji će nam navodno pomoći da se rešimo zlonamernog softvera. Uobičajeni primer ovog napada su baneri koji se pojavljuju u veb pretraživaču dok, gde se obično prikazuje tekst poput „Računar može biti zaražen štetnim špijunskim softverom“, ili nam se nudi da instaliramo alat koji je zaražen, a često nas i usmerava na zlonamernu lokaciju na vebu. Može se sprovesti i preko neželjenih mejlova kojima se dostavljaju lažna upozorenja ili nam se nudi kupovina rizičnih usluga.

Tailgating

Podrazumeva fizičko prisustvo napadača u prostorijama firme gde je zabranjen pristup, tako što će pratiti zaposlenog koji ima autentifikaciju. Napadač se može predstavljati kao vozač, koji će uspostaviti komunikaciju sa nekim od zaposlenih koji ulaze u zgradu i ući sa njim, a zatim nastaviti u službene prostorije.

Povratak na sadržaj

GLOBALNE ŠTETE OD SAJBER NAPADA

Prognozira se rast šteta od 15 odsto godišnje

Prognozirani rast šteta od sajber napada od 15 odsto godišnje u narednih pet godina, ovu vrstu kriminala čini najvećim transferom ekonomskog bogatstva u istoriji - poslom isplativijim od ukupne globalne trgovine drogom i eksponencijalno većim rizikom po svetsku ekonomiju čak i od šteta nastalih usled prirodnih katastrofa

Da sajber kriminal ima svoju državu, bila bi to trenutno treća najjača ekonomija na svetu, nakon SAD i Kine - slikovito opisuje moć današnjih hakera Stiven Morgan, urednik Cybercrime magazina i osnivač Cybersecurity Ventures, vodeće svetske kompanije u oblasti istraživanja globalne sajber ekonomije. Stručnjaci upozoravaju da će ubrzan tehnološki razvoj i omasovljenje rada na daljinu usled pandemije koronavirusa dovesti do još većeg porasta sajber napada.

Globalni gubici mere se hiljadama milijardi dolara

McAfee, američki proizvođač bezbednosnih softvera, u analizi s kraja prošle godine navodi da je sajber kriminal svetsku ekonomiju u 2020. godini koštao više od bilion (hiljadu milijardi) dolara, što je nešto iznad jednog procenta globalnog BDP-a. Poređenja radi, visina globalnih gubitaka u 2018. godini bila je oko 600 milijardi dolara. „Nove tehnologije šire polje delovanja sajber kriminalaca, a tome pogoduje i prelazak na rad od kuće ili sa udaljenih lokacija", upozorava Stiv Grobman iz kompanije McAfee.

Rob Sobers, softverski inženjer specijalizovan za veb sigurnost u softverskoj kompaniji Varonis, smatra da će širenjem 5G mreže doći do povećanja propusnog opsega povezanih uređaja, pa će IoT uređaji postati još ranjiviji na sajber napade.

Stižu i upozorenja da pandemija koronavirusa koja još nije gotova, u kombinaciji sa rastućim sajber kriminalom preti da prouzrokuje još težu „kliničku sliku": Cybersecurity Ventures predviđa da će visokotehnološki kriminal već u toku druge pandemijske godine naneti štetu od šest hiljada milijardi dolara na globalnom nivou, a eksperti ove kompanije očekuju da će šteta od sajber napada rasti

Najveći sajber napadi u 2020.

Easy Jet
Britanska aviokompanija EasiJet bila je žrtva sajber napada u kojem su ukradeni podaci 9 miliona klijenata, uključujući i podatke sa kreditnih kartica. Klijenti su potom tužili kompaniju za štetu u visini od 23 milijarde dolara.

Zoom
Ogromna popularnost ove platforme za onlajn sastanke u toku prošle godine dovela je Zoom i na radar hakera. U aprilu je Zoom potreslo otkriće da se 500.000 ukradenih lozinki za pristup platformi prodaje na dark webu, što je omogućilo upade „prenkera" – nezvanih gostiju koji prave neslane šale, na onlajn sastanke.

Marriott
Lični podaci čak 5,2 miliona gostiju jednog od hotelskih lanaca kojim upravlja američka multinacionalna korporacija, ukradeni su početkom 2020. godine: reč je o podacima gostiju koji su koristili aplikaciju za lojalnost.

Nintendo
Nintendo, pionir onlajn igrica, pretrpeo je sajber napad na 160.000 naloga svojih korisnika preko kojih su hakeri kupovali digitalne proizvode sa Nintendo mreže.

Magellan Health
Američka zdravstvena kompanija Magellan Health u aprilu prošle godine postala je žrtva napada ransomvera, u kojem su ugroženi podaci 365.000 pacijenata uključujući i poverljive podatke o osiguranju.

Povratak na sadržaj

15 procenata godišnje u narednih pet godina, dostižući 10,5 hiljada milijardi dolara do 2025.

Ovo sajber kriminal čini najvećim transferom ekonomskog bogatstva u istoriji, isplativijim poslom od ukupne globalne trgovine drogom i eksponencijalno većim rizikom po svetsku ekonomiju čak i od šteta nastalih usled prirodnih katastrofa.

Uprkos rastu napada, kompanije i dalje nepripremljene

Rad od kuće koji podrazumeva daljinski pristup korporativnim mrežama učinio je biznise još ranjivijim, a na posebnom udaru bili su zaposleni – „fišing" prevare postale su najbrže rastuća vrsta sajber kriminala. Dodatno, zaposleni koji rade od kuće često dele kompjutere sa ukućanima i prijateljima, čineći time dostupnim login i druge poverljive podatke kompanije.

Stiv Morgan ocenjuje da bi samo zbog smanjenih resursa za sajber bezbednost prilikom rada na daljinu globalna šteta od sajber kriminala mogla da se duplira do kraja godine.

„Ako preduzeća obuče zaposlene kako da otkriju i reaguju na fišing prevare, troškovi štete od sajber kriminala mogu se zadržati na sadašnjem nivou. To je kao i sa virusom - što više znamo o njemu i što više činimo da bismo se zaštitili, to se smanjuje mogućnost štete koja će biti naneta društvu", kaže Morgan.

Međutim, kompanije su većinom nepripremljene na sajber incidente. Više od polovine kompanija učesnica McAfee istraživanja reklo je da nema plan za sprečavanje sajber napada, niti spreman odgovor ako se on dogodi; od 951 kompanije koja je imala neki plan, tek 32 odsto smatralo je da bi taj plan imao nekog efekta. Ovaj izveštaj pokazao je da kompanije i ne razumeju u potpunosti rizike koje nose sajber napadi, pa se može zaključiti da ih nedovoljna svest o problemu čini nezainteresovanim da unapred osmisle preventivne mere.

Nisu svi gubici odmah vidljivi

Sajber napadi ne izazivaju samo trenutne finansijske gubitke, već i one na dugi rok koji dolaze kao posledica: oštećenje ili uništavanje podataka zahteva dodatno vreme i angažman kako bi se do istih podataka ponovo došlo, troškove usled krađe intelektualne svojine, troškove usled prekida poslovanja, troškove istrage, angažman kompjuterskih forenzičara, i najzad – reputacioni rizik odnosno dugoročnu štetu po ugled kompanije.

Podaci kompanije McAfee pokazuju da je čak 92 odsto kompanija već imalo gubitke koji su prevazišli samo trenutno vidljivi trošak. Sa zastojem u poslovanju suočilo se oko dve trećine ispitanih organizacija, uz prosečnu štetu između 100.000 i 500.000 dolara. Zbog smanjenja efikasnosti usled zastoja poslovanja kompanije su u proseku gubile devet radnih sati nedeljno. Pritom, gotovo trećina ispitanika kao troškove je navela i angažovanje spoljnih konsultanata ili nova zapošljavanja radi očuvanja reputacije.

Ivana Radovanović

Hakerske mete tokom pandemije

U prošloj godini na udaru su dominantno bile one oblasti ekonomije koje su radile – zdravstvo, IT sektor, građevina, transport, ali i one koje su zbog zastoja poslovanja "spustile odbranu" – poput avioindustrije i hotelijerstva.

Tokom ove godine predviđa se pojačan broj napada na male biznise, koji svoje poslovanje sve više prenose na "cloud".

Aplikacije bez kojih bi rad od kuće bio nezamisliv, poput Skajpa i Zoom-a, takođe su na meti hakera kao mogućnost za krađu podataka. Kućne mreže izuzetno su ranjive jer su nedovoljno zaštićene. Dodatno, mnogi gotovo nikada ne menjaju šifre na ruterima, što olakšava pristup i laptopu i drugim uređajima nakačenim na kućnu mrežu.

Najzad, socijalni inženjering posebno je izražen u kriznim situacijama - sve su brojniji načini na koje sajber kriminalci biraju i mame žrtve "informacijama od značaja" poput onih o dostupnosti vakcina, ili pak zastrašivanjem nekom osetljivom informacijom iz privatnog života.

Povratak na sadržaj

DRAGAN PLESKONJIĆ, MEĐUNARODNI EKSPERT ZA SAJBER BEZBEDNOST, ČLAN SAVETODAVNOG ODBORA INICIJATIVE ZA JAČANJE BEZBEDNOSTI PODATAKA

Sajber ratovi „tinjaju velikim intenzitetom“

U nekoj meri napadi se mogu predvideti i to je „vruća“ oblast danas. Tu značajno pomažu nauka o podacima, mašinsko učenje i veštačka inteligencija

Da li stav „kod nas nema ničeg zanimljivog“ može da nas spase od sajber napada, ili je to samo loš izgovor i da li je skuplje ne preduzimati ništa, ili ulagati u sajber zaštitu? I gde je zapravo granica u pokušajima hakera – da li apetit zadovoljavaju napadima na preduzeća, ili im meta mogu biti i čitave države?

Za naše čitaoce o tome govori Dragan Pleskonjić, koji je osim angažmana na rukovodećim pozicijama u međunarodnim kompanijama sa globalnom pokrivenošću, u Srbiji fokusiran na svoje R&D projekte INPRESEC (Intelligent Predictive Security) i Glog. Ovi projekti donose novi pristup sajber bezbednosti korišćenjem mašinskog učenja i veštačke inteligencije za detek-

Povratak na sadržaj

ciju i sprečavanje sajber pretnji i napada, uz mogućnost predviđanja najverovatnijih napada i planiranja optimalnih proaktivnih odbrambenih mera, kao i unapređenja softverske i aplikacione sigurnosti.

Da li bi godišnje izdvajanje za sajber bezbednost trebalo da bude redovna stavka u budžetu svakog preduzeća?

Uvek me iznenadi kad vidim da neke firme ne vode računa o ovoj stavci u današnje vreme, kada je veći deo poslovanja baziran na računarskoj tehnologiji. Savetovao bih svima, koji još nemaju ovu stavku u svojim budžetima, da što pre o tome razmisle - pre nego što dožive štetu. Jedan jedini uspešan napad može značajno da ošteti firmu, pa čak i da je potpuno uništi.

Jedan od najopasnijih izgovora je „mi nemamo ništa interesantno“. A onda može da se desi da jednog dana dođu na posao i ne mogu da koriste računare - kad shvate da je u pitanju ransomware napad (napad ucenjivačkim softverom), obično „čupaju kosu sa glave“ i traže pomoć. Tada može biti već kasno, ako nisu prethodno preduzeli neophodne mere.

Kako se određuje visina iznosa koji treba ulagati u sajber bezbednost?

Iznosi se kreću u prilično širokom rasponu. Neka istraživanja kažu da idu ka 0,5 odsto bruto prihoda firme. Druga, koja ovaj budžet računaju u okviru IT budžeta, kažu da je to od 7 do 15 odsto IT budžeta. Trend je da ova stavka raste, usled povećanih opasnosti i rizika. Budžet za sajber bezbednost je najčešće deo ukupnog budžeta za informacione i komunikacione tehnologije (IKT). Mislim da to nije baš najsrećnije rešenje i da treba da bude poseban, jer ova oblast pokriva mnogo širi spektar od IKT. Dodao bih da je smeštanje ove funkcije u IKT sektor pomalo i konflikt interesa, ali o tome drugom prilikom.

Da li se neki period u prošlosti može smatrati prelomnim kada su preduzeća počela ozbiljno da shvataju sajber pretnje?

Nagli rast broja napada i štete koje su mnoga preduzeća pretrpela doveli su do toga da preduzeća ove pretnje uzmu ozbiljnije, da deluju preventivno. Rezultat su redovne procene rizika i upravljanje rizicima, a onda i određivanje balansa između uloženih sredstava u zaštitu i preuzetog rizika. Sa porastom potencijala industrije i mogućih finansijskog rezultata na jednoj strani i potencijalne štete od incidenata u računarskoj i informacionoj bezbednosti, rasla je potreba, a zatim i ulaganja.

Povratak na sadržaj

Značajan „motivator“ je i donošenje zakona, ali i kazni za nepreduzimanje potrebnih mera.

Obično se smatra da su napadači oni koji smišljaju modele napada, a odbrana ih prati. Da li postoji odbrana koja reaguje pre nego što se osmisli/pokrene napad?

Izgleda da su napadači obično korak ili dva ispred onih koji brane sisteme. Napadi su sve ređe nasumični, a sve češće ciljani, vrlo dobro promišljeni i planirani. Radi se ozbiljna analiza i procena gde napadi mogu da uspeju, koje ljude ili firme napasti, kako i kada ih napasti. Često je prednost na strani napadača. Oni biraju vreme, mesto, način i cilj napada. Odbrana mora da štiti sve vreme, na svim mestima, od svih načina napada. Borba je neravnopravna.

Od velike pomoći je, ako se može sprovesti preventiva, i ako se može bar u nekoj meri prognozirati ko će napasti, kada, gde i na koji način.

Tu spadaju i procena rizika i upravljanje rizicima, implementacija procesa i tehnologija za zaštitu i odgovarajuća podrška. Ukratko: ljudi, procesi, tehnologije u sadejstvu. Bezbednost je proces - nije proizvod, tačka u vremenu ili nešto što se uradi jednom; to je stalna aktivnost za koju treba biti spreman u svakom smislu.

Kako deluje predikcija napada – koja tehnologija se za to koristi?

U novije vreme je porastao značaj skupljanja podataka koji mogu pomoći da se predvide mogući napadi (neka vrsta obaveštajne aktivnosti, engl. threat intelligence), a tu su i mašinsko učenje i veštačka inteligencija (engl. machine learning and artificial intelligence) primenjeni u području predviđanja napada.

U nekoj meri napadi se mogu predvideti i to je „vruća“ oblast danas. Ovim se bavi jedan R&D projekat, koji sam pokrenuo i koji već pokazuje rezultate. Prema ovom što sam prethodno rekao, odbrana je razvučena na „širokom frontu“. Analiza i procena cilja, mesta, vremena i načina napada omogućava fokusiranje odbrane i uspeh sa manje uloženih sredstava i sa manjim rasipanjem snaga.

> Bezbednost je proces - nije proizvod, tačka u vremenu ili nešto što se uradi jednom; to je stalna aktivnost za koju treba biti spreman u svakom smislu

To znači da treba imati dobru procenu rizika, obaveštajne podatke i analize, moguće finansijske odnosno ekonomske efekte, kao i marketinšku, psihološku, društvenu, pa i političku komponentu, i još mnogo toga.

Sistem koji razvijam sa malim timom, uzima u obzir bezbednosne, tehnološke aspekte, ali takođe i psihološke, sociološke, etičke, finansijske, političke i geopolitičke, i neke druge.

Danas postoje posebni tokovi podataka, na koje se neki entiteti mogu pretplatiti i obrađivati ih sa ciljem da budu na vreme upozoreni i da podignu nivo pažnje (uzbune) na potreban nivo, fokusiraju odbranu na određene kritične segmente i uspešno se odbrane kad zatreba.

Uljuljkani u lične probleme, mnogi i ne znaju da se na globalnom nivou vode pravi mali hakerski ratovi?

Sajber ratovi „tinjaju velikim intenzitetom“, vrlo često je to daleko od očiju javnosti. Rekao bih čak da i ne prestaju i to traje već decenijama. Milijarde „sitnih“ sajber napada dešavaju se svakog meseca, a samo neki od njih izbiju na površinu po svojim posledicama i budu propraćeni u medijskim izveštajima.

Operativni centri za bezbednost (engl. Security Operations Centers) su vrlo zaposleni i njihove kontrolne table često „gore“ od signala koji stižu sa različitih tačaka informacionih i računarskih sistema i mreža.

Grad Oldsmar na Floridi nedavno je zamalo doživeo katastrofu - haker je uspeo da pristupi gradskom postrojenju za prečišćavanje vode preko softvera za daljinski pristup. Pokušao je da zatruje vodu u gradskom sistema za vodosnabdevanje, dodavanjem opasnog nivoa sredstava za čišćenje.

Zabeleženi su slučajevi napada na sisteme upravljanja električnom energijom, medicinskim sistemima, automobilima. Napadi na kritičnu infrastrukturu mogu dovesti do katastrofalnih posledica.

Da li je istina da klasični ratovi među državama uskoro neće ni postojati, i da se i na tom polju delovanje prebacuje u sajber prostor?

Itekako, to verujem da čak više i nije iznenađenje. Ciljevi su razni: otkrivanje poslovnih, finansijskih, privatnih, državnih i vojnih podataka i tajni, rezultata istraživanja, inovacija, intelektualne svojine, zatim onemogućavanje ili onesposobljavanje rada kritičnih infrastrukturnih i drugih sistema.

Neke zemlje imaju posebne jedinice za cyberwarfare i vrlo uspešno ih koriste. Nekada su te jedinice deo drugih vojnih snaga, recimo za elektronsko ratovanje, dok su u nekim zemljama uspostavljene posebne komande i cela struktura, kao što je recimo u kopnenoj vojsci, vazduhoplovstvu i mornarici. A brojni su i primeri pokušaja da se ukradu podaci o istraživanjima u vezi sa Covid-19 vakcinama.

Lela Saković

Povratak na sadržaj

HRVATSKA GOSPODARSKA KOMORA NA USLUZI GOSPODARSTVU U UVJETIMA EPIDEMIJE COVID-19 I NAKON POTRESA

„Digitalna komora“ – jedinstvena komunikacijska platforma za e-usluge

Piše: Dr Sc. Dražen Lučić, voditelj Odjela za informacijsku sigurnost, Hrvatska gospodarska komora

Hrvatska gospodarska komora (HGK) je krovna kuća poduzetništva u Republici Hrvatskoj (RH) koja usklađuje, promiče i zastupa zajedničke interese svih članica pred državnim i drugim tijelima u RH i inozemstvu. Tijekom proteklih godinu dana, unatoč epidemiji COVID-19 te nenadanim situacijama, izazvanim potresima u Zagrebu i bližoj okolici, HGK je bez prestanka obavljala sve redovite poslove i usluge za svoje članice, a ujedno je i provodila brojne aktivnosti u cilju digitalizacije usluga članicama i povišenja razine informacijske i kibernetičke sigurnosti.

Tijekom ovog kriznog razdoblja, HGK je organizirala redovito poslovanje radom od kuće. Radom na daljinu bitno je smanjen rizik obolijevanja ili stradanja djelatnika HGK, a učinkovitost i kvaliteta poslovanja se povećala, uz smanjenje ukupnih troškova poslovanja.

„Digitalna komora“ označava digitalnu preobrazbu poslovanja HGK kroz stvaranje jedinstvene komunikacijske platforme za e-usluge, koja je dostupna članicama HKG i poslovnoj zajednici te javnoj upravi i građanima. Uvođenjem „Digitalne komore“ veći dio komunikacije, koji se do sada odvijao putem telefona, sastanaka i dolazaka u HGK, obavlja se sada preko interneta. Projekt „Digitalna komora“ je sufinanciran s 85% sredstava iz fondova Europske unije (EU).

DIGITALNA KOMORA
Nova dimenzija usluge

Poslovanje HGK, kao i poduzetnika u RH, u potpunosti je usklađeno sa zakonskim i regulatornim okvirom EU, što, između ostalog, uključuje i područje informacijske i kibernetičke sigurnosti. Opća uredba o zaštiti osobnih podataka (GDPR), Zakon o kritičnim infrastrukturama (NIS direktiva), kao i sve druge zakonske odredbe EU u svezi zaštite podataka i privatnosti su pravovremeno uključene u zakonodavstvo RH. Danas nema razlike u obvezi obrade i čuvanja osobnih podataka od strane državnih institucija ili gospodarstva.

Središnji državni ured za razvoj digitalnog društva (SDU RDD), uz Agenciju za zaštitu osobnih podataka (AZOP) i još neke državne institucije, upravljaju i nadziru postupke uvođenja e-usluga i pravilne obrade osobnim podatcima. Poduzetnici su sve svjesniji rizika u digitalnom društvu, nažalost često kroz vlastita negativna iskustva. Zbog toga sve više ulažu u sprječavanje neželjenih incidenata, a u tome im pomaže i država kroz, na primjer, Zavod za sigurnost informacijskih sustava, već spomenuti SDU RDD, kao i HGK. HGK je, u suradnji s AZOP-om, tijekom proteklih šest mjeseci organizirala desetke besplatnih online tečajeva iz područja zaštite osobnih podataka, a HGK za sve vlastite djelatnike provodi redovitu izobrazbu iz područja informacijske i kibernetičke sigurnosti.

Svaka kriza je ujedno i točka preokreta u poslovanju ili prilika za novi početak. Tako će i ova kriza imati pozitivne učinke na upravljanje poslovanjem u digitalnom okruženju te prouzročiti znatan porast svijesti o značaju informacijske i kibernetičke sigurnosti. Brojni poduzetnici i institucije u RH, uključujući i HGK, dobar su primjer takve preobrazbe.

Povratak na sadržaj

KAKO SE DRŽAVE BRANE OD HAKERSKIH NAPADA

SAD najčešća meta, Grčka se najbolje brani

Svetski ekonomski forum savetuje da kreatori politika odmere svoje odluke imajući u vidu opasnost od sajber kriminala, te da budu kreativne u povećanju zaštite uz istovremeno smanjivanje regulatorne složenosti

Raznobojni snopovi svetlosti bez prestanka „pucaju" preko tamne podloge na ekranu gde je ucrtana mapa sveta. Sve deluje kao neka sajber igrica sa temom ratova zvezda. Ovakve interaktivne mape prikazuju širom sveta stacionirane hakere koji vode rat u sajber prostoru, udaljeni stotinama hiljada kilometara od svojih meta. A mete najbolje organizovanih i tehnički i tehnološki najopremljenijih sajber kriminalaca često su države i njima bliske organizacije i korporacije. Zato države razvijaju strategije u želji da se zaštite od sajber napada, a Evropska unija je tako krajem prošle godine usvojila Strategiju za sajber bezbednost.

Šta ugrožava nacionalnu sajber bezbednost?

Sistem je jak onoliko koliko i njegova najslabija karika, upozorava Svetski ekonomski forum, a najsvežiji neslavni primer ove tvdnje je sajber napad s kraja prošle godine na FireEye, američku kompaniju za sajber bezbednost čije sisteme koriste korporacije i vlade širom sveta upravo da bi se zaštitile od hakerskih napada.

Drugo „tupo oružje" u rukama država su nacionalni propisi koji su, navodi se u tekstu, gotovo uvek „iscepkani" i previše složeni, tako da širom otvaraju vrata sajber kriminalu koji nema nameru da poštuje granice i državne jurisdikcije. Organizacijama su, s druge strane, ruke vezane sve restriktivnijim propisima poput različitih nacionalnih, ali i nadnacionalnih uredbi o zaštiti podataka i propisa o privatnosti potrošača, što umanjuje šanse za odbranu.

Svetski ekonomski forum savetuje da kreatori politika odmere svoje odluke imajući u vidu opasnost od sajber kriminala, te da budu kreativni u povećanju zaštite uz istovremeno pojednostavljivanje regulativa.

Gde je Srbija?

Srbija se nalazi na 17. mestu od ukupno 160 država na listi NCSI indeksa, tik iza SAD, a ispred Velike Britanije, i to sa pozitivnom razlikom u odnosu na DDL od 16,30. Neki od nabrojanih indikatora korišćenih za analizu vrednosti ovog indeksa Srbije su razvoj politike sajber bezbednosti (100% ispunjenosti), zaštita digitalnih servisa (100%), zaštita ličnih podataka (100%) i odgovor na sajber incidente (100%), dok nam prosek kvare analiza sajber pretnji (samo 20%), doprinos globalnoj sajber bezbednosti (30%) i upravljanje sajber krizama (60%). Ako pogledamo susedne države, od Srbije je po NSCI indeksu bolja Hrvatska (11. pozicija), ali je naša država ispred Slovenije koja je na 40. mestu, BiH (58. mesto) i svih ostalih bivših YU republika, kao i ispred Rumunije (22. mesto), Mađarske (27. pozicija) i Bugarske (53. mesto).

Pandemija kao „so na ranu"

Sajber napadi u poslednje dve pandemijske godine usmereni su na trenutno najvitalnija polja za nacionalnu bezbednost država, poput isporuke vakcina protiv koronavirusa. Stoga ne čudi da su na listi najznačajnijih sajber incidenata u 2020. i na početku 2021. upravo napadi u vezi sa vakcinama, pokazuje lista vašingtonskog Centra za strategijske i međunarodne studije (CSIS). Među njima je krađa podataka o Oksfordskoj vakcini protiv koronavirusa od strane portugalskih hakera iz februara ove godine. Zatim, pokušaj severnokorejskih hakera u istom periodu da provale u kompjuterski sistem kompanije Fajzer, pokušaj neimenovanih hakera da ukradu podatke o vakcini istog proizvođača iz sistema Evropske medicinske agencije, pa malver severnokorejskih hakera uperen protiv proizvođača AstraZenekine vakcine.

Ko hakuje, a ko biva hakovan

Sjedinjene Države su prve među 20 zemalja sa najviše „značajnih" sajber napada u periodu od maja 2006. do juna 2020. godine, prema analizi Secops

Povratak na sadržaj

softvera, švedskog provajdera rešenja za bezbednost korisničkih naloga. To nije neobično s obzirom na koncentraciju moćnih finansijskih korporacija i kreatora globalnih politika na toj teritoriji. U analiziranom periodu Sjedinjene Države pretrpele su 156 značajnih sajber napada, dok je druga među državama na meti hakera bila Velika Britanija sa 47 napada, a treća Indija sa 23 incidenta. Prema listi američke Bedford biznis asocijacije SAD su među prvih 10 zemalja iz kojih hakerski napadi potiču (doduše, tek na 10. mestu - na prva dva su Rusija i Kina).

Zemlje sa najboljim mehanizmima odbrane

Prema listi „Nacionalni indeks sajber bezbednosti“ (NCSI), koji meri pripremljenost država da spreče sajber napade i nose se sa sajber incidentima, Grčka je najpripremljenija država. Slede Češka i Estonija, a u prvih pet su i Litvanija i Španija.

NCSI ističe da se u obzir uzimaju tri vrste sajber napada: DoS (zatrpavanje servera upitima kako bi im se onemogućio pristup), zatim, neautorizovana modifikacija podataka, i provaljivanje poverljivih podataka. Da bi procenio sposobnost odbrane države, indeks razmatra njenu regulativu, aktivnosti zvaničnih vladinih agencija, različitih komiteta i radnih grupa, kao i tehnologije koje se koriste, i sve to meri kroz veliki broj indikatora i drugih alata. Uz to, NCSI meri i nivo digitalnog razvoja - DDL, a razlika između ta dva pokazatelja je zapravo njihova usklađenost, odnosno indikator koliko sajber bezbednost zemlje prati njen digitalni razvoj. On se iskazuje u plusu ili u minusu.

Grčka je u tom smislu šampion, jer njen indeks sajber bezbednosti iznosi 96,10; DDL je 65,44, a razlika između njih je 30,66 u plusu.

Zemlja čiji tehnološki razvoj najmanje prati spremnost na odbranu od sajber napada je Sveti Kits i Nevis, kod kojih ova razlika ima negativan skor od 62,01 (doduše, postoje i zemlje u kojima DDL nije ni merljiv, verovatno jer nema dostupnih podataka, pa ovu razliku nije bilo moguće iskazati na listi NCSI). Ipak, Sveti Kits i Nevis nisu poslednji na listi. Ova zemlja nalazi se na 143. mestu po sposobnosti obrane od sajber terorizma, a poslednji, na 160. poziciji je Južni Sudan.

Ono što je zanimljivo je da na ovoj listi jake ekonomije i tehnološki razvijene države poput SAD i Japana ne zauzimaju očekivano visoke pozicije. Tako su Sjedinjene države na 16. mestu, Velika Britanija na 18. poziciji, Japan tek na 31, a Švedska na 42. Pritom SAD i Britanija imaju čak i negativan skor u razlici između vrednosti indeksa i DDL (prve dve -3,11, odnosno -6,04, Japan -19,81, a Švedska čak -26,34).

Takođe, ako dalje analiziramo ovu listu, primetno je da prve pozicije zauzimaju zemlje nekadašnjeg Istočnog bloka, Češka, Poljska (6. mesto na listi), ili bar one koje su se nalazile u sovjetskoj zoni uticaja: Estonija, Litvanija, Finska. S druge strane, Kina, koja je bez pogovora tehnološki tigar pati od istih „boljki” kao i zapadne „kolege” – neusklađenost digitalnog napretka sa odbranom od sajber terorizma (negativan skor od -22,94). I mada je NCSI svrstava na polovinu svoje liste po vrednosti indeksa, Kina je po jednom drugom indeksu (National Cyber Power Index) druga najmoćnija država na svetu koja, poluzvanično, ima čak i vojne jedinice specijalizovane za mrežni napad i odbranu koje broje oko 100.000 profesionalaca, kao i organizovane vladine i nevladine snage angažovane na istom zadataku.

Ivana Radovanović

Povratak na sadržaj

JOVAN MILOSAVLJEVIĆ, NACIONALNI CERT

Mete napada su i kompanije i fizička lica

Svaki korisnik interneta, bilo da govorimo o fizičkom ili pravnom licu, može biti potencijalna žrtva sajber napada. Na globalnom nivou, tokom pandemije virusa COVID-19, najveći broj sajber napada bio je usmeren na velike korporacije, kao i finansijski sektor i sektor zdravstva

Da li ste se nekad zapitali, kome da se obratite ako dođe do sajber napada u Vašoj firmi? Od koga nam prete najveće opasnosti, i koje firme su najčešća meta?

O tome specijalno za naše čitaoce govori Jovan Milosavljević, rukovodilac Službe za informacionu bezbednost u okviru Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL) - Nacionalni CERT.

„Od izbijanja pandemije, izazvane virusom COVID-19, broj incidenata na svetskom, ali i na regionalnom i lokalnom nivou bio je u konstantnom porastu. Najveći broj incidenata je bio usko povezan upravo sa temom COVID-19, a najzastupljeniji su bili napadi poput Phishing (fišing) i Ransomware (iznuđivački softver) kampanja“, kaže Jovan Milosavljević.

Da li napadi dolaze dominantno spolja, ili od domaćih hakera?

Građani, institucije i kompanije bili su žrtve sajber napada koji su organizovani i izvođeni kako iz inostranstva, tako i sa teritorije naše zemlje. Napadi iz inostranstva su bili zastupljeniji, dok su lokalni tipovi napada bili sofisticiraniji i prilagođeni zemljama u regionu, kako sa jezičkog tako i sa tematskog aspekta.

Ko su najčešće mete napada?

Definisanje ili određivanje mete napada može zavisiti od velikog broja faktora. Svaki korisnik interneta, bilo da govorimo o fizičkom ili pravnom licu, može biti potencijalna žrtva sajber napada. Na globalnom nivou, tokom pandemije virusa COVID-19, najveći broj sajber napada je bio usmeren na velike korporacije, kao i finansijski sektor i sektor zdravstva. Prethodnih godina broj napada je u određenoj meri više bio usmeren na mala i srednja preduzeća, ali i fizička lica.

Šta je uloga CERT-a?

Zakon o informacionoj bezbednosti prepoznaje Nacionalni CERT, CERT organa vlasti, samostalne CERT-ove i posebne CERT timove.

Uloga Nacionalnog CERT-a je prioritetno usmerena na koordinaciju prevencije i zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima (IKT sistemima), odnosno kritičnoj infrastrukturi, na nacionalnom nivou. Nacionalni CERT prikuplja i razmenjuje informacije o mogućim rizicima, na osnovu kojih obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima, kao i javnost Republike Srbije. Dodatno, Nacionalni CERT prati prijavljene incidente na nacionalnom nivou i na osnovu prikupljenih podataka analizira rizike i incidente, sa ciljem podizanja svesti opšte javnosti - kako građana, tako i privrednih subjekata i organa vlasti, o značaju informacione bezbednosti. Pored navedenog, Nacionalni CERT vodi i evidenciju posebnih CERT timova. To su timovi koji pružaju svim zainteresovanim korisnicima svoje usluge iz ove oblasti.

Povratak na sadržaj

Pored navedenog, Nacionalni CERT organizuje različite radionice za različite tipove korisnika. Najveći broj tehničkih obuka namenjen je pre svega zaposlenima u IKT sistemima od posebnog značaja, ali i drugim državnim institucijama. Postoje i teorijske obuke koje su usmerene na zaposlene u malim i srednjim preduzećima, pa sve do radionica koje su namenjene predstavnicima medija. Tehničke radionice se izvode na platformama za simulaciju sajber napada koje imaju više različitih, ali veoma realnih scenarija. Na ovaj način RATEL, kao Nacionalni CERT, umnogome doprinosi podizanju kadrovskih kapaciteta u oblasti informacione bezbednosti, na nacionalnom nivou.

Kakav je značaj članstva u međunarodnim CERT-ovima?

Aktivno članstvo u međunarodnim organizacijama, poput organizacije FIRST, od velikog je značaja za sve članice, uključujući i Nacionalni CERT Republike Srbije. Članstvo podrazumeva da je Nacionalni CERT legitimni prestavnik svoje države, da imate uređen interni sistem politika i procedura, da poštujete sve protokole za razmenu, rukovanje i čuvanje informacija i sl. Prisustvo na međunarodnoj sceni je veoma značajno i sa aspekta koji nam omogućava razmenu znanja sa eminentnim ekspertima iz ove oblasti.

Da li postoji obaveza da se napad prijavi i ko ima tu obavezu, a ko ne?

Svi IKT sistemi od posebnog značaja bi trebalo da prijave Nacionalnom CERT-u sve incidente koji se dogode u njihovom sistemu. Na sajtu Nacionalnoog CERT-a postoji elektronski formular preko kojeg je moguće prijaviti svaki incident. Pored navedenog, Zakon o informacionoj bezbednosti propisuje obavezu svih IKT sistema da Nacionalnom CERT-u Republike Srbije dostavljaju i prikupljene statističke podatke o svim incidentima koje su imali tokom prethodne godine, do 28. februara tekuće godine. U ovu svrhu kreirana je posebna aplikacija koje je dostupna svim IKT sistemima od posebnog značaja.

Nacionalni CERT ohrabruje i sve druge korisnike da prijave svoje incidente, kako bismo imali jasniji i realniji prikaz stanja informacione bezbednosti u Republici Srbiji.

Kada govorimo o definiciji incidenta, bilo bi dobro naglasiti da ona treba da govori i o pretnjama koje se odnosne na ključne principe - autentifikaciju, poverljivost, integritet i dostupnost. Na sajtu Nacionalnog CERT-a, u sekciji Često postavljena pitanja korisnici se mogu bliže upoznati sa kraćom definicijom incidenta, kao i definicijom šta se ne može smatrati incidentom.

Vesna Lapčić

Povratak na sadržaj

PRAVNI ASPEKT

Šta su podaci o ličnosti, i kako smeju da se obrađuju

Piše: Predrag Groza, partner u advokatskoj kancelariji Tomić Sinđelić Groza (TSG), član Savetodavnog odbora Inicijative za jačanje bezbednosti podataka

Svaka informacija na osnovu koje se može utvrditi, posredno ili neposredno, identitet fizičkog lica - predstavlja podatak o ličnosti, pa tako pored „tradicionalnih“ podataka (poput imena i prezimena, fotografije) podatkom o ličnosti može se smatrati i IP adresa, lokacijski identifikatori i slično

Zaštita podataka o ličnosti je ustavom zajemčeno pravo, te svako fizičko lice ima pravo da bude obavešteno o obradi podataka koji se na njega odnose, kao i pravo na delotvornu zaštitu u slučaju zloupotrebe tih podataka.

Šta se smatra podatkom o ličnosti? Zakon o zaštiti podataka o ličnosti ne daje taksativnu listu, već postavlja standard po kojem je podatak o ličnosti zapravo svaki podatak na osnovu kojeg je identitet fizičkog lica određen ili odrediv. Dakle, svaka informacija na osnovu koje se može utvrditi, posredno ili neposredno, identitet fizičkog lica predstavlja podatak o ličnosti, pa tako pored „tradicionalnih“ podataka (poput imena i prezimena, fotografije) podatkom o ličnosti može se smatrati i IP adresa, lokacijski identifikatori, itd.

Sistem zaštite podataka o ličnosti počiva na jasnim načelima koja svaki rukovalac (organ vlasti, javno preduzeće, kompanija...) mora da poštuje i primenjuje („odgovornost za postupanje“). Odgovornost za postupanje je univerzalno pravilo nezavisno od toga da li je reč o obradi podataka zaposlenih kod rukovaoca, podataka njegovih kupaca ili pak potencijalnih klijenata.

Obrada podataka mora biti zakonita (postoji odgovarajući pravni osnov za obradu), transparentna (lice mora biti obavešteno o obradi), srazmerna konkretnoj svrsi obrade, ograničena samo na bitne i neophodne podatke (minimizacija podataka), u svakom trenutku tačna i ažurna, i na kraju sigurna i poverljiva (zaštićena adekvatnim merama).

U pogledu zakonitosti obrade, pristanak lica je nekako ''najpoznatiji'' široj javnosti, možda zbog sveprisutnog direktnog marketinga koji često izlazi iz dozvoljenih okvira. Tako imamo situacije da se komercijalne transakcije (npr. apliciranje za potrošačke kredite) uslovljavaju pristajanjem na direktan marketing, koji zapravo nema puno veze sa primarnom i željenom transakcijom. Upravo zbog takvih zloupotreba, uslovi obrade podataka u svrhe direktnog marketinga su propisani posebnim zakonima - Zakonom o

Povratak na sadržaj

elektronskoj trgovini i Zakonom o oglašavanju – prema kojima je za obradu podataka u svrhe marketinga neophodan pristanak onoga ko prima oglasnu poruku. Dakle, „odsustvo pristanka“ je uvek prepreka za direktan marketing.

Međutim, pristanak je samo jedan od ukupno šest osnova za zakonitu obradu (a dovoljan je samo jedan!). S tim u vezi, osnov može biti i poštovanje pravnih obaveza rukovaoca (npr. poslodavac je dužan da vodi zakonom propisane evidencije u oblasti rada), zatim izvršavanje ugovora zaključenog sa licem čiji se podaci obrađuju (npr. banka obrađuje podatke klijenta u svrhe realizacije ugovora o kreditu), a pod određenim uslovima osnov obrade može biti i legitiman interes rukovaoca ili trećeg lica.

U slučaju da sumnjamo na neovlašćenu obradu ili zloupotrebu podataka o ličnosti, imamo određeni spektar prava prema konkretnom rukovaocu, i to: pravo na informacije o obradi, pravo na pristup podacima, pravo na ispravku ili dopunu podataka, pravo na zaborav (brisanje podataka), pravo na ograničenje obrade, itd. U slučaju da rukovalac ne postupi po opravdanom zahtevu u zakonskom roku, možemo se preko pritužbe obratiti Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti. Poverenik tada sprovodi postupak inspekcijskog nadzora radi utvrđivanja eventualne povrede, i može naložiti rukovaocu da postupi po zahtevu lica koje je uputilo pritužbu. Ostvarivanje ovih prava, po pravilu, ne kreira posebne troškove za lice koje se obraća rukovaocu odnosno Povereniku.

> Za obradu podataka u svrhe marketinga neophodan je pristanak onoga ko prima oglasnu poruku

Na kraju, u slučaju da je zloupotreba podataka prouzrokovala materijalnu ili nematerijalnu štetu licu čiji su podaci zloupotrebljeni, to lice ima pravo na naknadu štete koju ostvaruje u redovnom postupku pred nadležnim sudom.

Povratak na sadržaj

MILAN MARINOVIĆ, POVERENIK ZA INFORMACIJE OD JAVNOG ZNAČAJA I ZAŠTITU PODATAKA O LIČNOSTI

Kazne za kršenje propisa nisu dovoljno visoke

Za poslednjih desetak godina Poverenik je utvrdio više masovnih povreda podataka o ličnosti građana - incidenti su se dešavali upravo zbog neadekvatnih mera zaštite. Takođe, u više navrata je utvrđivao postojanje zloupotreba podataka koji se obrađuju na osnovu zakona od strane onih koji imaju pristup takvim podacima, što povlači krivičnu odgovornost lica, ali i odgovornost organizacija

Pre godinu i po dana u Srbiji je počeo da se primenjuje Zakon o zaštiti podataka o ličnosti, ali još postoje brojni problemi na terenu. Među njima su neusklađenost sa drugim propisima, nesprovodivost pojedinih odredbi, niske kazne za kršenje propisa, sporo usklađivanje kompanija sa propisom. Sam Zakon ima određene manjkavosti.

„Najveći broj subjekata u javnom i privatnom sektoru nije bio ispunio ni minimalne obaveze po ZZPL nakon njegovog stupanja na snagu. Te obaveze uglavnom su ispunila velika privredna društva, koja su povezana sa stranim kompanijama, koje su se godinama unazad pripremala za početak primene GDPR. Iz ovog razloga, Poverenik konstatno podseća na obaveze iz ZZPL i sprovodi edukacije“, kaže Milan Marinović, poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti.

Zakon o zaštiti podataka o ličnosti se primenjuje oko godinu i po dana. Dokle se stiglo sa primenom?

Poverenik je u poslednjih godinu i po dana sproveo niz postupaka u cilju primene Zakona o zaštiti podataka o ličnosti. Sačinjene su, i na sajtu Poverenika javno objavljene kontrolne liste koje sami rukovaoci mogu preuzimati u cilju samoprocene rizika i usklađenosti sa Zakonom. Poverenik sve ovo vreme sprovodi postupke redovnih i vanrednih nadzora, kao i postupke po pritužbama građana, daje mišljenja, analizira akte subjekata iz javnog i privatnog sektora, stara se o podizanju svesti u oblasti zaštite podataka o ličnosti. Tokom 2020. godine, koja je svima protekla u značajno otežanim uslovima, Poverenik je u korespondenciji sa velikim svetskim internet kompanijama izdejstvovao imenovanje njihovih predstavnika za Republiku Srbiju, pa danas svoje predstavnike ovde imaju Gugl, Jahu, Netfliks, Bukingkom, Alibaba, Vajber, Spotifaj...

Ostali zakoni trebalo je da se usklade sa ZZPL do kraja prošle godine. Da li je to učinjeno, i ako nije - kakve posledice izaziva?

Kako sve mogu da se zloupotrebe podaci građana i šta se od zloupotreba najčešće dešava u praksi?
Zloupotrebe podataka često se dešavaju u internetskom okruženju, posebno zbog činjenice da građani neoprezno postupaju sa sopstvenim podacima, olako ih dele i dostavljaju nepoznatim licima. U takvoj situaciji lako može doći do zloupotreba, kada se ta nepoznata lica mogu poslužiti Vašim podacima i preuzeti Vaš identitet, ulaziti u pravne poslove ili se na drugi način služiti njima. Takođe, Poverenik je u više navrata utvrđivao postojanje zloupotreba podataka koji se obrađuju na osnovu zakona od strane onih koji imaju pristup takvim podacima, što povlači krivičnu odgovornost lica, ali i odgovornost organizacije, tj. rukovaoca koji je, zbog neadekvatne zaštite podataka, omogućio takvu zloupotrebu.

Povratak na sadržaj

Ova zakonska obaveza nije ispunjena, što otvara niz problema u primeni kako ZZPL, tako i drugih zakona. ZZPL u članu 2. stav 2. propisuje da odredbe drugih zakona koji uređuju obradu podataka o ličnosti moraju biti u skladu sa ZZPL. Međutim, isti zakoni nikada nisu ni pobrojani, niti je izvršena njihova komparativna analiza sa ZZPL kako bi bili usklađeni. Iz ovog razloga ponovo je aktuelizovan problem nedostatka strateškog pristupa naše zemlje zaštiti podataka o ličnosti. Ovaj strateški deficit ne može se nadoknaditi samo donošenjem ZZPL, već najpre unutrašnjom harmonizacijom pravnih propisa.

U EU su institucije već počele da kažnjavaju kompanije na osnovu GDPR-a. Kolike su propisane kazne u Srbiji i da li su one uopšte motivišući faktor da se povede računa o zaštiti podataka o ličnosti?

Za razliku od kazni po GDPR, koje su drakonske i kreću se do 20 miliona evra ili do 4 odsto globalnog prihoda kompanije, kazne po ZZPL su neuporedivo niže, jer se izriču u prekršajnom postupku, pa su i sami zakonski iznosi kazni vezani opštim propisom o prekršajima. Kazne u EU predstavljaju glavni motivišući faktor za usklađivanje privrede sa GDPR, a iste obezbeđuju i specijalnu i generalnu prevenciju, što kod nas, objektivno, nije slučaj. Takođe, ostaje nejasno kako se kazne i mogu izreći za pojedine prekršaje. Tako, npr. kompanija Fejsbuk je u prekršaju, jer nije imenovala svog predstavnika u Republici Srbiji. Ovoj kompaniji, kao jednoj od najmoćnijih i najbogatijih na svetu, Poverenik bi trebalo da izrekne zbog ovoga prekršajni nalog od 100.000 dinara, a odgovornom licu 20.000 dinara. Pored činjenice da ovakva kazna svakako ne može biti srazmerna, delotvorna i preventivna, postavlja se pitanje kako uopšte sprovesti postupak inspekcijskog nadzora u kojem bi ovakva kazna bila izrečena.

Pandemija je ubrzala digitalizaciju. Da li ste u tom procesu negde uočili potencijalni problem po zaštitu podataka o ličnosti? Da li brzina razvoja digitalnog društva povećava i opasnost u tom smislu i kako „pomiriti“ ta dva procesa – digitalizaciju i sajber sigurnost?

Digitalizacija predstavlja neophodan proces u današnjem vremenu, kada je došlo do razvoja interneta neslućenih razmera. Međutim, upravo nužnost ovog procesa ukazuje na potrebe primene adekvatnih mera bezbednosti u obradi podataka. U tom smislu, svaka organizacija koja sprovodi proces digitalizacije mora posebnu pažnju da posveti ovom aspektu, kako ne bi došlo do kompromitovanja podataka. Za poslednjih desetak godina Poverenik je utvrdio više masovnih povreda podataka o ličnosti građana - incidenti su se dešavali upravo zbog neadekvatnih mera zaštite, koje moraju biti

Povratak na sadržaj

organizacionog, tehničkog i kadrovskog tipa. Tek preduzimanjem i konstantnim praćenjem i preispitivanjem ovih mera organizacija može obezbediti integritet i poverljivost podataka koje obrađuje. U tom smislu, lažna je dilema da li treba birati između digitalizacije i sajber bezbednosti, jer ta dva moraju da idu ruku pod ruku.

U EU je zaštita ličnih podataka jedno od osnovnih ljudskih prava. Da li se tako podaci o ličnosti tretiraju i u Srbiji?

Ustav Republike Srbije garantuje zaštitu podataka o ličnosti, kao jedno od ljudskih prava. Ova ustavna odredba garantuje da se obrada podataka o ličnosti uređuje zakonom, da je zabranjena i kažnjiva upotreba podataka o ličnosti izvan svrhe za koju su prikupljeni, u skladu sa zakonom, osim za potrebe vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom, kao i da svako ima pravo da bude obavešten o prikupljenim podacima o svojoj ličnosti, u skladu sa zakonom, i pravo na sudsku zaštitu zbog njihove zloupotrebe. Takođe, ovo pravo garantovano je i Konvencijom o zaštiti lica u odnosu na automatsku obradu podataka, koju je naša zemlja ratifikovala.

> “Lažna je dilema da li treba birati između digitalizacije i sajber bezbednosti, jer ta dva moraju da idu ruku pod ruku”

Koji su uočeni nedostaci postojećeg Zakona i hoće li oni biti ispravljeni najavljenim izmenama Zakona? Šta će biti predmet tih izmena?

Postojeći Zakon predstavlja kompilaciju prevoda GDPR i EU Direktive 680/16 (tzv. Policijska direktiva), u kojoj su potpuno zanemarene preambule ova dva, međusobno raznorodna dokumenta. Iz ovog razloga upotreba mnogih instituta i pravnih standarda koji nemaju uporište u domaćem pravu stvara prostor za proizvoljna tumačenja, dok su pojedine odredbe zaista neprimenljive.

Vesna Lapčić

JAVNA PREDUZEĆA – PODACI O GRAĐANIMA I KRITIČNA INFRASTRUKTURA

„Poslastica“ za hakere

Napadi na javna preduzeća prilično su učestali, a ponekad se dogode i tamo gde svet najmanje očekuje, i to zbog propusta odgovornih službi. Pandemija je hakerima dodatno išla na ruku, a preduzeća koja se računaju u kritičnu infrastrukturu pokazala su se posebno zanimljivim za sajber napade

Hakerski napad na gradske službe Novog Sada i javno preduzeće „Informatika“ pre godinu dana naveo je da se dobro zamisle čak i oni direktori i vlasnici firmi koji do tada nisu pridavali veliki značaj zaštiti podataka i informacionog sistema. Hakovano je 2.000 kompjutera i 120 servera, a gradskim službama je bilo potrebno više od mesec dana da se potpuno oporave. U svetu, napadi su svakodnevni, a u poslednjih godinu dana primećuje se da su hakeri izgleda među retkima kojima je pandemija išla na ruku: rad od kuće, često na privatnim računarima, njima je olakšao posao. Docent dr Bojan Jovanović, sa Katedre za informacione tehnologije Fakulteta organizacionih nauka u Beogradu napominje da je u celom svetu sajber kriminal tokom prošle godine procvetao.

„Redali su se napadi jedan za drugim širom sveta i to pre svega ciljano na institucije vlada mnogih zemalja, na javni sektor: školstvo, zdravstvo, i na finansijske institucije poput banaka i berzi“, kaže Jovanović. „Iako je većina napada bila bezuspešna, mnogo više znamo o uspešnim jer je medijska pažnja bila usmerena ka njima. Vektori napada na informacione

Povratak na sadržaj

sisteme firmi su se povećali, jer su, zahvaljujući radu od kuće, postali zanimljivi i kućni računari zaposlenih. Uz pomoć socijalnog inženjeringa na društvenim mrežama može se sakupiti mnoštvo podataka o identitetima pojedinaca. „Nemam ja šta da krijem" je najčešća rečenica prosečnog korisnika društvenih mreža. Ovakvim stavom narušavamo i sopstvenu privatnost, a možemo da ugrozimo i bezbednost firme u kojoj radimo".

Široko im polje

Napadi na javna preduzeća prilično su učestali, a ponekad se dogode i tamo gde svet najmanje očekuje: jedan od svežijih primera dogodio se nedavno u Holandiji, kada su ukradeni podaci iz zdravstvenih kartona građana koji su se testirali na kovid. Ispostavilo se da su hakerima informacije bile lako dostupne, jer je sistem podešen tako da podaci mogu da se izvezu jednim klikom.

Pre pet godina Ukrajinci su ostali bez struje, jer su hakeri napali elektromrežu i onesposobili isporuku električne energije.

U Venecueli je zbog sabotaže na elektromreži nestala električna energija u Karakasu, a bez struje je ostao i veći deo zemlje. Hakerski napad na hidroelektranu Guri koja proizvodi 80 odsto struje u toj južnoameričkoj državi dogodio se u aprilu 2019. godine. Ministar za komunikacije Venecuele Horhe Rodrigez je tada izjavio da će Venecuela podneti žalbu Visokom komesarijatu UN za ljudska prava zbog „sabotaže" na elektromreži, čiji je najverovatniji uzrok hakerski napad. On je nestanak električne energije ocenio kao „najbrutalniji napad na narod Venecuele u proteklih 200 godina". Mediji su tada objavili da je predsednik Venecuele Nikolas Maduro rekao kako je napad na nacionalnu električnu mrežu sproveden iz Čilea i Kolumbije uz podršku američke vlade.

Žrtva napada tokom 2019. bio je i Johanesburg, kada su inficirani računari provajdera električne energije, pa je deo grada ostao bez struje.


Dr Bojan Jovanović

Mediji su tada pisali da se napad na gradske javne institucije pokazao kao veoma unosan trend za sajber kriminalce. Veliki gradovi širom sveta pretrpeli su štete od „ransomware" napada, a prosečan iznos koji su plaćali da bi otkupili sopstvene podatke je oko 500.000 dolara. Neki od njih, poput Atlante i Baltimora, odbili su da plate napadačima za otključavanje podataka, ali ih je to na kraju koštalo mnogostruko skuplje, jer su na kraju potrošili desetine miliona dolara da ponovo aktiviraju i osposobe svoju mrežu.

Mađarska je pre nekoliko meseci jedva uspela da se odbrani od takozvanog DDoS napada, koji se odvija tako što hakeri preplavljuju mrežu neuobičajeno velikim internet prometom kako bi je blokirali. Napad je izveden u nekoliko talasa, a poremetio je usluge dela finansijskih institucija i prekinuo deo usluga „Magyar Telekom" u delovima Budimpešte, pre nego što je kompanija uspela da ga odbije. Iz ovog preduzeća su saopštili da je napad izveden sa kompjuterskih servera lociranih u Rusiji, Kini i Vijetnamu.

„Informatika" se oporavila

Gradski informacioni sistem Novog Sada je blokiran početkom prošlog marta, a nadležni su ucenjeni na 50 bitkoina, što je u tom trenutku bilo oko 400.000 evra. U međuvremenu je otkupnina smanjena na 20 bitkoina, ali je Grad odbio da plati i tu sumu, pa su podaci ostali zaključani. JKP je 24. aprila saopštilo da je u potpunosti otklonilo posledice teškog hakerskog napada. U pitanju je bio „ransomware" napad, odnosno kriptovanje podataka, koje je uzrokovalo da serveri budu neupotrebljivi. Automatizovani alati za otkrivanje i sprečavanje napada nisu ga prepoznali.

„Podaci građana nisu bili ugroženi, jer se čuvaju na platformi koja nije bila u fokusu napada. Podaci su bili kriptovani i samim tim nedostupni. Dekripcijom podataka i vraćanjem sistema u potpuno funkcionalno stanje za manje od mesec dana izbegnuta je šteta, svi podaci i korisnici su sačuvani", kaže za naše čitaoce Mirjana Beronja iz Službe za investicije, komercijalne poslove i marketing u „Informatici".

Posle napada sprovedena je detaljna analiza IT infrastrukture kako bi se uočile dobre, ali i slabe tačke postojećeg modela arhitekture. Uveli su sistem izbegavanja katastrofalnih događaja (Disaster Avoidance), koji omogućava potpuno integrisan oporavak servisa „skoro bez prekida" funkcionisanja. Implementirana su brojna nova rešenja, a uvedena je i nova politika kopija servera.

Najvažnije je obučavanje zaposlenih

Apsolutna zaštita ipak ne postoji. Dr Bojan Jovanović napominje da je sistem bezbednosti „živ" i da ga je potrebno stalno unapređivati.

„Svedoci smo da se svakog dana otkrivaju nove ranjivosti softvera, procedura i pravila. Cilj sistema bezbednosti je da se šteta koja može da nastane svede na minimum.

Povratak na sadržaj

Zakon o zaštiti podataka dobro pokriva ovu oblast. Preduzeća su dužna da svojim pravnim aktima regulišu organizaciju i aktivnosti koje je potrebno sprovesti. Ne postoji univerzalno rešenje. Svako preduzeće shodno tehničko - tehnološkim rešenjima koje koristi u radu treba da definiše kako će se to raditi“, objašnjava dr Jovanović.

Naš sagovornik napominje da je rizik veliki i da je od izuzetnog značaja permanentno obrazovanje zaposlenih, kao i da je to jedina prava aktivnost da se moguće neprepoznavanje lažnih mejlova svede na minimum.

„U riziku od sajber napada su sva preduzeća - i javna i privatna. Zaposleni moraju da budu spremni i obučeni - po mom saznanju i ubeđenju, obuke zaposlenih se ne sprovode dovoljno“, upozorava naš sagovornik.

Državna instuticija koja pohranjuje značajne baze podataka je Agencija za privredne registre. U njenoj IT službi priznaju da konstantno postoje pokušaji neovlašćenog pristupa, ali se oni na vreme detektuju i sprečavaju, pa do sada nije bilo upada u sistem.

> „Nemam ja šta da krijem“ je najčešća rečenica prosečnog korisnika društvenih mreža. Ovakvim stavom narušavamo i sopstvenu privatnost, a možemo i da ugrozimo bezbednost firme u kojoj radimo

„Najčešće potencijalne opasnosti su „phishing“ mailovi, „malware“, „ransomware“, DDoS napadi i „SQL injection“ napadi. Rizici uvek postoje ukoliko zaposleni nisu obučeni i zato smo u pristupili podizanju svesti o bezbednosti informacija i informacionog sistema. Sa jedne strane to smo uradili usklađivanjem sa Zakonom o informacionoj bezbednosti, a sa druge strane započeli smo implementaciju kontrola i zahteva definisanih standardom ISO/IEC 27001:2013. Takođe, postoji i uspostavljena adekvatna tehnička zaštita od lažnih mailova. Uspostavljena je organizaciona struktura, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru IKT sistema APR-a“.

Zlata Rakić

Povratak na sadržaj

MAJO MIĆOVIĆ, PREDSEDNIK ŠVAJCARSKO-SRPSKE TRGOVINSKE KOMORE, ČLAN SAVETODAVNOG ODBORA INICIJATIVE ZA JAČANJE BEZBEDNOSTI PODATAKA

Kako odabrati sajber zaštitu

Zainteresovanost kompanija, iako u blagom porastu, ne prati u potpunosti trendove sajber bezbednosti, ali odgovornost za to ne treba tražiti samo u kompanijama

Koliko je Srbija zanimljiva svetskim hakerima i kako oni biraju svoje mete, da li su naša preduzeća osposobljena ali i zainteresovana za odbranu i da li su im na raspolaganju adekvatni alati za to? O tome, ali i o konkretnim koracima koje treba da preduzme preduzeće koje želi da postane „sajber bezbednije“, za naše čitaoce govori Majo Mićović, investitor i osnivač lokalnih i regionalnih kompanija, direktor ICT kompanije Sky Express iz Beograda, koja je lider u oblasti bezbednosti digitalnih podataka u regionu, i distributer više od deset svetski priznatih softverskih rešenja za zaštitu podataka, implementiranih u vodećim regionalnim kompanijama.

„Podaci i dosadašnje iskustvo govore nam da Srbija i građani Srbije nisu u grupi visoko pozicioniranih ciljeva napadača, ali je evidentno i da je broj i sofisticiranost napada u stalnom rastu. Uzroke za to možemo pronaći u poboljšanju ekonomskih parametara, čime potencijalni napadač može ostvariti finansijsku satisfakciju, a donekle i u značajnijoj geopolitičkoj poziciji, što za sobom povlači pojačano interesovanje i angažovanje „nation-state“ sponzorisanih napadača. U ovom slučaju, primarni cilj napadača nije sticanje finansijske koristi, već prikupljanje i analiza poverljivih i poslovnih podataka, sa ciljevima od kojih su najznačajniji uticaj na kreatore državnih i poslovnih strategija, uticaj na javno mnjenje ili sticanje kompetitivne prednosti“, kaže Majo Mićović.

Koliko Srbija prati trendove kad je u pitanju sajber zaštita?

Ukoliko sajber bezbednost posmatramo na tradicionalan način, i ukoliko se ograničimo na proizvode, ponuda je bogata i raznovrsna. Nažalost, savremeni napadi su neuporedivo sofisticiraniji, a potrebe kompanija značajno kompleksnije. Tradicionalna rešenja jesu adekvatna, ali samo za ograničen skup potencijalnih problema.

Fokus zaštite ne može više biti samo resurs, poput servera, rutera ili radne stanice; na kraju krajeva, poslovanje jedne kompanije i ne zavisi od pojedinačnog resursa, već od njenih podataka i zaposlenih koji tim podacima pristupaju.

Savremena poslovna rešenja i savremeni informacioni sistemi zahtevaju savremena bezbednosna rešenja. Na sreću, na našem tržištu postoje kompanije koje to prepoznaju i koje mogu na pravi način da odgovore na savremene bezbednosne potrebe, ne samo u pogledu proizvoda, već i u pogledu usluga koje pružaju.

Koliko su domaća preduzeća svesna rizika, i koliko su zainteresovana za sajber bezbednost?

Poslovna svest o informacionoj bezbednosti je najčešće direktno proporcionalna segmentu poslovanja, kao i pokrivenošću domaćim i međunarodnim regulatornim zahtevima. Kao primer možemo uzeti kompanije u oblasti bankarskog i finansijskog poslovanja, kod kojih je stepen razvijenosti programa informacione bezbednosti (maturity level) na veoma visokom nivou, dok sa druge strane kao primer možemo uzeti proizvodna, i mala i srednja preduzeća kod kojih se problemu informacione bezbednosti uglavnom pristupa na tradicionalan način, čime se povećava izloženost savremenim tehnikama i metodama napada.

Zainteresovanost kompanija, iako u blagom porastu, ne prati u potpunosti trendove sajber bezbednosti, ali odgovornost za to ne treba tražiti samo u kompanijama, već je to najčešće posledica nedovoljne informisanosti o pretnjama, mogućim uticajima i posledicama napada, na čemu svi zajedno moramo u narednom periodu mnogo više da radimo.

Kako preduzeće da odabere pravi sistem za sajber zaštitu?

Tako što će upotrebiti pravi pristup rešavanju ovog problema. Svako preduzeće je specifično, bez obzira na to što na tržištu postoji mnogo preduzeća koja se bave istim poslom. Kao što ne postoji „one size fits all“ rešenje, isto tako nije ni moguće bukvalno prekopirati nečije rešenje. Najjednostavniji i najefikasniji način adresiranja problema informacione bezbednosti je da se prvo utvrde regulatorne i tržišne potrebe, sagleda postojeće stanje, na to se dodaju specifične želje u pogledu bezbednosti i kao rezultat ćemo dobiti jasnu analizu

Povratak na sadržaj

na osnovu koje kreiramo precizan plan unapređenja, u skladu sa prioritetima i mogućnostima.

Ovaj proces je moguće uraditi interno, u okviru kompanije, ali se rezultati mnogo brže i preciznije ostvaruju angažovanjem kompanija čija je oblast poslovanja informaciona bezbednost, zbog toga što u tom slučaju posao prepuštate nekom ko poseduje neophodno znanje i iskustvo, dovoljan broj obučenih kadrova i kontinuirano prati najnovije trendove pretnji.

Koja država prednjači u sajber bezbednosti kad je o preduzećima reč, a koja kad je reč o proizvodnji bezbednosnih sistema?

Preduzeća odavno ne poznaju pojam državnih granica, poslovanje se odvija na teritoriji više država, i podleže odredbama najrazličitijih regulativa. Svaka razvijena država, bilo zapadna ili istočna, nastoji da što preciznije reguliše i ustanovi bezbednosne minimume koji moraju biti zadovoljeni u poslovnim procesima, ne bi li time zaštitila i preduzeća, i svoje informacione sisteme. Naravno, regulative same po sebi nisu dovoljne, već je neophodno primeniti i adekvatne mere kontrole kojima se obezbeđuje kontinuitet u održanju zadovoljavajućeg nivoa bezbednosti. Moglo bi se reći da u Evropi po tome prednjače preduzeća iz UK i Nemačke, a svakako u svetskim razmerama iz SAD i Izraela.

Kad je reč o proizvodnji bezbednosnih sistema, međunarodni investicioni fond čiji sam član - Evolution Equity Partners, investirao je od 100 odsto portfolija koji čine software security kompanije - više od 80 odsto svojih sredstava u američke proizvođače rešenja, što dovoljno govori o stanju među vendorima na svetskom tržištu, bar iz naše perspektive. Uz SAD, tu su svakako i Izrael, Nemačka, Kina i Velika Britanija.

Nadamo se da će interesovanje za razvoj sigurnosnih softverskih rešenja i u našoj zemlji znatnije porasti, jer Srbija ima potencijale, koje već iskazuje u drugim granama IT industrije. Kao predstavnik Fonda za ovaj region, pažljivo pratim te promene.

Da li u Srbiji ima dovoljno edukovanih kadrova za posao u oblasti sajber bezbednosti, i ako nema, kako rešiti situaciju?

U Srbiji imamo neke od najbriljantnijih ljudi u sajber bezbednosti, prepoznate i priznate na globalnom nivou. Imamo i jako talentovane mlade ljude koji su tek zakoračili u svet informacione bezbednosti. Ono što nemamo je jasna i primenljiva strategija kojom ćemo te eksperte zadržati u Srbiji, i kojom ćemo talente ranije prepoznavati i pretvarati u eksperte. Edukacija jeste jedan od bitnih činilaca u razvoju znanja, ali je neuporedivo važnije kreirati programe razvoja koji će mladim kolegama omogućiti primenu stečenih znanja u praksi. Time ćemo obezbediti kraći period razvoja, uporedo sa poboljšanjem poslovne efikasnosti i upotrebljivosti. Jedan od načina je primena dualnog sistema obrazovanja, u šta se možemo uveriti posmatrajući najrazvijenije države sveta.

U međuvremenu, najsigurniji način rešavanja problema sajber bezbednosti je angažovanje domaćih firmi koje su kvalifikovane i dokazane u oblasti informacione bezbednosti, jer u ovom trenutku jedino one raspolažu dovoljnim brojem osposobljenih i kvalifikovanih kadrova.

Lela Saković

Povratak na sadržaj

Autor: Mikica Ivošević, Co-founder & CTO, Abstract

DA LI SU PREDUZEĆA SA KOJIMA SARAĐUJETE OTPORNA NA SAJBER NAPADE

Podaci mogu iscuriti i preko poslovnih partnera

Postoje metode i servisi koji nam omogućavaju da utvrdimo da li naši poslovni partneri imaju svest o informacionoj bezbednosti i šta su uradili da se zaštite, odnosno da budu digitalno bezbedni. Za korisnički orijentisane kompanije, možda najveći problem predstavlja šteta po reputaciju firme i gubitak poverenja korisnika, koji je veoma teško ponovo zadobiti

Danas gotovo da nema biznisa ili organizacije koja bar neki deo svog poslovanja nije digitalizovala. Prednosti onlajn poslovanja su brojne. Efikasnost, dostupnost, kvalitet korisničke usluge, smanjenje troškova poslovanja - samo su neke od prednosti. Posledično, količina podataka na webu se dramatično uvećava. Najveći broj firmi drži bar deo svojih poslovnih ili privatnih korisničkih podataka na internetu. Naličje digitalizacije je rizik kojem se firme izlažu, ukoliko sve podatke kojima raspolažu, ne zaštite na adekvatne načine.

Brojne regulative (od kojih je najpoznatija i najstroža GDPR) izdate sa ciljem da ovu dinamičnu oblast pravno urede, uvele su striktne kazne za nemar i propuste prilikom rukovanja privatnim podacima. Regulative su dale vetar u leđa promociji adekvatne informacione bezbednosti i zaštite korisničkih privatnih podataka. Tako i firme sve više vode računa o bezbednosti sistema i uspostavljanju procedura koje uređuju aktivnosti od obuka zaposlenih, do formiranja specijalizovanih odeljenja za informatičku bezbednost.

S kim imamo posla?

Premda svest o važnosti zaštite sopstvenih sistema raste, nedovoljno se govori i veoma malo radi na tome da se kompanije informišu i sistematski zaštite od rizika koji dolazi kroz saradnju sa trećim licima: partnerima, dobavljačima, kupcima... Koliko je ovo previđanje opasno svedoče neki od najvećih bezbednosnih propusta poslednjih godina, praćeni rekordno visokim kaznama regulatornih tela, koja su bila izazvana upravo nemarnim odnosom prema riziku od trećih lica, tj. poslovnih partnera.

Ko su etički hakeri?

Etičko hakovanje je termin skovan kada su neki hakeri počeli da zloupotrebljavaju svoje znanje o informacionoj bezbednosti. Hakovanje postoji od kada postoji internet - a cilj etičkih hakera je povećanje njegove bezbednosti i podizanje svesti o važnosti brige za bezbednost podataka na njemu.
HackerOne, BugCrowd i Synac su primeri platformi koje okupljaju etičke hakere sa ciljem pronalaska sigurnosnih propusta na aplikacijama. Postoje i forumi gde se okupljaju etički hakeri, a postoje i firme koje neguju i podržavaju te vrednosti.
Razlika između “dobrih” (etičkih) i “loših” hakera je u nameri - i vuče se po moralnoj liniji, ali su u smislu znanja i tehničkih veština razlike minimalne, te se i jedni i drugi mogu naći na istim mestima u potrazi za znanjem i materijalima za učenje.

Povratak na sadržaj

Kompleksnost poslovnog okruženja nameće saradnju kao neminovnost, jer se mnogi poslovni procesi danas mogu mnogo efikasnije obaviti prenošenjem na druge specijalizovane firme (onlajn naplata je sjajan primer). Ali, to pored brojnih prednosti, donosi i rizike po bezbednost podataka koje sa tim partnerima delimo.

Ovo je globalni problem sa kojim se posebno teško nose srednja i mala preduzeća, koja nemaju dovoljno znanja i veština ili dovoljno visok nivo svesti o informatičkoj bezbednosti. Zato se, uplašeni kompleksnošću ove oblasti, često obeshrabreni okreću od nje, na sopstvenu štetu. Srbija nije izuzetak.

Kako da proverimo poslovne partnere

Postoje metode i servisi koji nam omogućavaju da utvrdimo da li naši poslovni partneri imaju svest o informacionoj bezbednosti i šta su uradili da se zaštite, odnosno da budu digitalno bezbedni.

U zavisnosti od oblasti rada, neke firme imaju obavezu ili potrebu da svoje bezbednosne aktivnosti sertifikuju - prvo treba proveriti da li vaš potencijalni partner ima neki od sertifikata za bezbednost podataka poput ISO 27001. Drugi važan korak je procena sajber rizika kroz rezultate upitnika i direktnu komunikaciju sa nadležnim osobljem.

Ni sertifikacija ni procena oslonjena na upitnike ne garantuje da je preduzeće digitalno bezbedno, jer ISO 27001 ne garantuje da se sve propisane procedure sprovode, ali nas obaveštava da je preduzeće svesno važnosti bezbednosti podataka i da preduzima korake da ih zaštiti.

Zbog toga je veoma važno sprovesti proveru realnog stanja, korišćenjem servisa za upravljanje sajber rizikom trećih lica. Ovi servisi skeniraju, evidentiraju i u kontinuitetu prate i mere bezbednosne performanse trećih lica, upozoravajući pravovremeno na promene koje mogu predstavljati rizik po naše poslovanje.

Dalje, potrebno je da se uspostavi efikasna komunikacija između poslovnih partnera o svakom propustu, i saradnja na uklanjanju problema i smanjenju rizika na najmanju meru.

Ukoliko nakon svega neko od trećih lica ne ispuni minimalne bezbednosne standarde potrebne za sigurnu saradnju, okretanje drugim pružaocima tih usluga je poslednje rešenje.

Važan princip koji može značajno doprineti bezbednosti podataka je i minimalno izlaganje, u smislu organizovanog i sistematičnog rada na deljenju isključivo neophodnih podataka sa trećim licima.

Pored visokih novčanih kazni, bezbednosni propusti mogu dovesti i do prekida saradnje sa drugim kompanijama, te pada obima poslovanja.

Za korisnički orijentisane kompanije, možda najveći problem predstavlja šteta po reputaciju firme i gubitak poverenja korisnika, koji je veoma teško ponovo zadobiti. Dobar primer koliko je sve to opasno je WhatsApp koji je zanemario privatnost podataka i zbog toga u nekoliko dana ostao bez nekoliko stotina hiljada korisnika. Bezbednost podataka je velika i teška tema i korisnici će kazniti zanemarivanje bezbednosti njihovih privatnih i poverljivih podataka.

Povratak na sadržaj

KAKO DA SAČUVATE SVOJ NAZIV DOMENA I ZAŠTO

Auto zaključavate. A naziv domena?

Cena jednog automobila jeste veća od cene jednog naziva internet domena, ali ne i njegova vrednost, jer na nazivu domena se bazira čitavo internet poslovanje vaše firme. Ophodite se prema nazivu domena kao prema važnom poslovnom resursu, jer on to i jeste

Piše: Predrag Milićević, Fondacija „Registar nacionalnog internet domena Srbije“ (RNIDS)

Ugledati nečiju zastavu ili logo hakerske grupe na naslovnoj strani vlastitog sajta jeste vrlo neprijatno, ali nije pogubno po biznis. Osim toga, odmah se vidi i brzo se uklanja. Mnogo je gore ako je sajt napadnut a da se to ne vidi.

Kad vam „ukradu“ naziv domena, ukrali su vam korisnike

Koliko god veb sajt bio obezbeđen sa svih strana, po pitanju transakcija i sigurnosti podataka, prečesto se zaboravlja naziv domena na kome taj sajt „stoji“. Naziv domena ukazuje na server na kome se nalazi vebsajt i server preko koga ide elektronska pošta. „Krađom“ kompanijskog naziva domena hakeri preusmeravaju internet korisnike na servere koji su pod njihovom kontrolom i onda mogu da pristupe porukama vaše poslovne e-pošte (čime ugrožavaju poslovanje firme), kao i da na svoje sajtove preusmere vaše korisnike (čime ugrožavaju njihove podatke). Hakovan naziv domena može ozbiljno da ugrozi kredibilitet vlasnika sajta i naruši teško stečeno poverenje, i poslovnih partnera i korisnika.

„Ukradeni“ domen je prilično lako vratiti uz pomoć ovlašćenog registra kod kog je naziv domena registrovan, ali mogu proći meseci pre nego što se krađa otkrije, a u međuvremenu hakeri mogu doći do mnoštva osetljivih poslovnih informacija i privatnih podataka.

Povratak na sadržaj

Bolje sprečiti nego lečiti

RNIDS je obezbedio tri različita načina zaštite naziva naših nacionalnih domena .rs i .srb, od kojih prva dva ne naplaćuje. Prva vrsta zaštite je „Siguran režim“ (Secure Mode), koji ne dozvoljava da se promena bilo kog kritičnog podatka o nazivu domena izvrši bez posebnog odobrenja njegovog korisnika. Ovaj tip zaštite korisnik najčešće može sam da aktivira. „Zaključavanje na strani klijenta“ (Client Side Lock) podrazumeva zabranu izmena svih podataka o nazivu domena osim produženja registracije, a za unošenje promena neophodna je dozvola ovlašćenog registra kod kog je naziv domena registrovan. „Zaključavanje na strani registra“ (Registry Lock) je najviši nivo zaštite koji za svaku izmenu u vezi sa podacima o nazivu domena predviđa dodatnu proveru autentičnosti zahteva od strane RNIDS-a.

Uostalom, ako automobil zaključavate, zašto ne biste i naziv domena? Cena jednog automobila jeste veća od cene jednog naziva internet domena, ali ne i njegova vrednost, jer na nazivu domena se bazira čitavo internet poslovanje vaše firme. Ophodite se prema nazivu domena kao prema važnom poslovnom resursu, jer on to i jeste. On malo košta, ali puno vredi.

Izbegnite „greške u koracima“

Nazivom domena raspolaže onaj na koga je naziv registrovan (registrant), bez obzira na to ko je vlasnik veb-sajta na tom nazivu domena. Stoga je sasvim moguće da vaš sajt nestane sa interneta ako je na tuđem nazivu domena, i njegov registrant odluči da ga preusmeri ili deaktivira. Zato naziv domena ne treba da bude registrovan na ime nekog od zaposlenih u firmi, niti na veb agenciju koja je pravila sajt pa registrovala i naziv domena, već isključivo na vašu firmu, jer to je vaš poslovni resurs.

Svom nazivu domena treba redovno da obnavljate registraciju, jer se on ne registruje „zauvek“, već na određeni period. Redovnim obnavljanjem taj vremenski period može da bude praktično neograničen. Međutim, ako registracija istekne, i vaš naziv domena registruje neko drugi, na njemu se mogu naći razni nepoželjni sadržaji – od neistinitih, preko falsifikovanih, do pornografskih. Ako pretraživači i internet korisnici taj naziv domena i dalje vide kao vaš, to se može negativno odraziti na vaše poslovanje.

Povratak na sadržaj

DNEVNIK DIGITALNOG DOSELJENIKA

Rizici digitalizovanog poverenja

Poslali ste robu stalnom kupcu – kao i obično. On je uplatio – kao i obično. Ali vama novac nije legao na račun... Šaljete vašoj banci pitanje šta je sa uplatom, ona šalje taj dokument korespondentskoj banci, jednoj od najvećih na svetu. Najzad vam stiže odgovor – ta transakcija ne postoji!

Piše: Vojislav Rodić, direktor I Net, Beograd

Jednog dana, kao što je i uobičajeno, otpremite kamion sa narudžbinom vašem dugogodišnjem kupcu. Uvek ste slali predračun e-poštom i dok bi se roba tovarila, a pre nego što bi kamion krenuo, uplata bi legla na vaš račun. Ovog puta, a bio je petak, roba je bila natovarena, ali uplate još nije bilo na računu. Kamion je bio spreman, ali imate predosećaj da nešto nije u redu. Ne pada vam na pamet da sumnjate u poslovnu korektnost vašeg partnera, ali opet.....Pošaljete e-mail kupcu da pitate šta je bilo sa uplatom. Malo vas je i sramota što posle 10 (20, 30...) godina besprekorne saradnje izražavate sumnju u uvek korektnog kupca. Partner, pomalo ozlojeđeno, potvrđuje da je uplata izvršena i moli vas da roba krene u subotu jer je zbog tendera na kojem učestvuje neophodno da stigne do srede, ako čekate ponedeljak njima je već kasno. Pošto ste dobili pisanu potvrdu da je uplata po predračunu već izvršena, mirno potpisujete sve dokumente i roba kreće na put. U ponedeljak još nema uplate, ali to pripisujete uobičajenom toku međunarodnih bankarskih transakcija. Kada popodne vidite da i dalje nema uplate, zamolite partnera da vam pošalje SWIFT dokument sa svim parametrima transakcije i posle par sati stiže vam dokument koji vas smiruje, naravno da su uplatili, mora da je neko usporenje u banci. U utorak šaljete pdf vašoj banci da pitate šta je sa uplatom. Vaša banka šalje taj dokument korespondentskoj banci, jednoj od najvećih na svetu. U četvrtak stiže odgovor – ta transakcija ne postoji! Sada vas hvata panika, pomisao da ste ostali bez petocifrenog iznosa u evrima i da ne samo da niste ostvarili uobičajeno malu zaradu, nego ste izgubili iznos koji vas vraća nekoliko meseci unazad. Konačno zovete partnera i obaveštavate ga o tome šta se desilo, a onda vas čeka još veće iznenađenje. Oni vam kažu da od njih niste tražili SWIFT dokument, a oni su uplatu izvršili, kao i uvek, istog dana kada su dobili predračun. Zahvaljuju se što je kamion sa robom stigao na vreme. Iz njihove prespektive sve je urađeno po uobičajenoj proceduri, samo što je na predračunu bio vaš novi devizni račun, istina ne u vašoj, već u jednoj drugoj zemlji, ali njima je bilo nezgodno da vas ispituju zašto ste otvorili novi račun, pa još u drugoj zemlji. Nisu ni pomislili da budu toliko indiskretni da vas ispituju o vašoj poslovnoj politici, poznajete se toliko godina i saradnja je uvek bila besprekorna. Isporučili ste robu ugovorenog kvaliteta, potrudili se da stigne na vreme, nemaju nikakvu primedbu, ali shvataju da nešto nije u redu. Tada prvi put počinjete da pažljivije pregledate vašu elektronsku korespondenciju i shvatate da je prepiska između komercijalista sa obe strane, na prvi pogled potpuno uobičajena, isti službe-

Povratak na sadržaj

nici, ista terminilogija, ovog puta se pojavio novi detalj – u adresi e-pošte u nekim porukama (ne u svim) je u nazivu internet domena (desno od @) umesto latiničnog slova „l“ bio broj „1“. Kako je to moguće? Angažujete konsultanta u koga imate poverenja, u nadi da će dati savet ili ispostaviti rešenje koje će poništiti sve posledice. Umesto dijagnoze i lečenja, dobićete izveštaj o autopsiji. Prvi savet je da obavezno prijavite slučaj Posebnom odeljenju za visokotehnološki kriminal. Ne očekujte da ćete za koji dan ugledati hapšenje u medijima, a uskoro i povratiti vaš novac, ali neophodno je da imate odgovarajući zapisnik, kako biste u eventualnim budućim pravnim radnjama mogli ispravno da se identifikujete kao oštećena strana. Istovremeno kontaktirajte sve banke koje su mogle da budu uključene u „put vašeg novca“, a posebno banku u koju su otišla sredstva namenjana vama. Ko je vlasnik računa na koji su uplaćena vaša sredstva? Kako je moguće da je neko u toj zemlji otvorio račun sa imenom vaše firme? Nemojte da se iznenadite ako se ustanovi da ni taj račun uopšte nije na ime vaše firme. Kada ustanovite da je vlasnik računa preduzetnička radnja sa sedištem u toj zemlji, sledeće pitanje je - kako je moguće da je neki službenik banke uspešno obradio uplatu koja je glasila na ime vaše firme, a imala račun koji glasi na drugo pravno lice? Ovde se krije (veoma mala) mogućnost za eventualnu vansudsku (kod nekih banaka) ili sudsku naplatu štete. Ako ste reagovali veoma brzo (u satima, ne u danima) možda ćete uspeti da zaustavite transakciju kod korespondentske banke. Banke po pravilu reaguju veoma brzo na prijave ovakve vrste, tako što odmah zamrznu transakciju, ako nije sprovedena do kraja. To ne znači da ćete odmah dobiti sredstva nazad, ali bar neće nepovratno otići na račun u odredišnoj banci na egzotičnim ostrvima. Nije za utehu ali saznaćete i kako se zove ova vrsta prevare „man-in-the-middle“ – „posrednik u prepisci“

Gde je “ključ” prevare?

Kako je ovo uopšte moglo da se desi? Tehnički deo se obično realizuje tako što napadač prvo dođe u posed pristupnih podataka za administraciju servera e-pošte.

> Svaki put kad primetite bilo šta „sumnjivo“ (neuobičajena hitnost, ili promena broja računa) odmah kontaktirajte partnera, ali ne e-poštom koja je možda već kompromitovana, već telefonom - ma koliko da ste se odvikli od razgovora i pripadajućih troškova

Da li se radilo o ubačenom virusu (keylogger), nekoj psihološkoj manipulaciji zaposlenih ili možda čak i o unutrašnjem proboju, manje je važno. Ono što se dešava potom je ključ ove prevare – sveukupna elektronska korespondencija je pristupačna neautorizovanim osobama. Ponekad mesecima prate vašu korespondenciju, vredno uče terminologiju vašeg poslovanja, uobičajene aktere i stil njihovog ophođenja. Kada odluče da je trenutak za akciju, ubaciće se u prepisku, a onda se prepiska nastavlja sa naizgled istom osobom. Sve vam izgleda uobičajeno, samo će vaš partner u jednom trenutku biti obavešten o „novom“ broju vašeg računa. Pri tom se računa na vaše poverenje u dugogodišnjeg partnera, čime se „kupuje“ dovoljno vremena da se transakcija realizuje pre nego što postanete svesni da nešto ozbiljno nije u redu.

Kako sprečiti ovakve prevare?

Ne postoji univerzalno rešenje („savršeni“ antivirusni program) koje će vas sačuvati od ovakvih napada. Primenićete uobičajene mere – standardni antivirisuni programi na svim radnim stanicama, autorizacija vaših poruka primenom SSL sertifikata, DKIM i SPF alatima za autentifikaciju vaše e-pošte. Zatražite da se na vašem c-Panelu (najpopularniji program za upravljanje veb sajtom i nalozima e-pošte) aktivira standardna opcija da svaki put kada neko pristupi c-Panelu vi, ili neko koga ovlastite, dobije obaveštenje da je pravi ili ubačeni „administrator“ pristupio vašem sistemu. Prvo obaveštenje u kojem se vidi da je neko pristupio sa nepoznate IP adrese već je dovoljan znak za uzbunu. Najvažnije, svaki put kada primetite bilo šta „sumnjivo“ (neuobičajena hitnost, ili promena broja računa) odmah kontaktirajte partnera, ali ne e-poštom (koja je možda već kompromitovana) već telefonom, ma koliko da ste se odvikli od razgovora i pripadajućih troškova ako su partneri u nekoj dalekoj (skupoj) zoni. Eventualni troškovi zbog realizovane prevare će biti za više redova veličine veći od bilo kakvog troška za proveru.

Čuvajte vaše dugogodišnje partnere, ali proveravajte vaše poverenje prema njima, a i njima najavite da reaguju na bilo kakve promene u vezi sa finansijskim transakcijama sa vaše strane.

Povratak na sadržaj

SANJA KEKIĆ, PREDSEDNICA UDRUŽENJA ISACA BEOGRAD I POTPREDSEDNICA WOMEN4CYBER SERBIAN CHAPTER

Sistem kontrole je potreba, a ne obaveza

Jedan od osnovnih izazova u uspostavljanju sistema kontrole je jačanje svesnosti vlasnika domaćih kompanija o potrebi za tim sistemom i za zaštitom od rizika, posebno kada kompanija naglo poraste i prevaziđe vlasnika

Malo domaćih kompanija vidi potrebu za ozbiljnim i adekvatnim pristupom proceni rizika i uspostavljanju sistema kontrole. Uglavnom se ta tema posmatra u kontekstu regulatornih zahteva, ili radi dobijanja određenog posla ili neke vrste finansijske pomoći. Kad se uvodi „pod teretom obaveze“, sistem kontrole obično nije adekvatno urađen, kaže Sanja Kekić, predsednica Udruženja ISACA Beograd i potpredsednica Women4Cyber Serbian Chapter, i jedna od 50 najuticajnijih žena u oblasti bezbednosti prema rangiranju vodećeg britanskog časopisa za sajber bezbednost - SC Media UK.

„Jedan od osnovnih izazova je podizanje svesti vlasnika domaćih preduzeća o potrebi za sistemom kontrole i zaštitom od rizika, što postaje još značajnije kad preduzeće naglo poraste i prevaziđe vlasnika“.

U kom smislu je značajna sertifikacija kompanija za bezbednost, i koje sve sertifikate u toj oblasti kompanije mogu da pribave?

Osnovni cilj sertifikacije se odnosi na podizanje nivoa bezbednosti poslovanja procenom bezbednosnih rizika i uspostavljanjem sistema kontrola za preventivu rizičnih događaja, odnosno za ublažavanje posledica od nastanka rizičnih događaja.

Povratak na sadržaj

Krovni široko poznati sertifikati u oblasti bezbednosti informacija su sertifikati koji pripadaju ISO/IEC 27000 familiji, dok bi ona preduzeća koja u svom poslovanju imaju napredno poslovanje platnim karticama trebalo da budu usklađena sa PCI DSS standardom.

Važno je da i zaposleni u preduzećima koji su odgovorni za bezbednost informacija budu sertifikovani u ovoj oblasti, pa tako u zavisnosti od aktivnosti koje obavljaju to mogu biti ISACA sertifikati CISA, CISM, CRISC, CDPSE, CGEIT i ITCA, zatim to su (ISC)² sertifikati CISSP, SSCP, CCSP, CAP, CSSLP i HCISPP, pa i CompITA grupa sertifikata.

Sa druge strane uz pomoć NIST okvira za sajber bezbednost, COBIT okvira za sajber bezbednost odnosno ISACA-ine CMMI® Cyber maturity Platforme ili kontrolnih okvira kao što su NIST i CIS, preduzeća mogu sagraditi sajber zrelost u smislu upravljanja otpornošću na sajber napade i spremnosti da odgovore na eventualne sajber napade.

Šta je uloga Udruženja ISACA Beograd i u čemu se ogleda značaj članstva u toj međunarodnoj organizaciji?

Osnovna uloga Udruženja ISACA Beograd je podizanje svesti o važnosti sigurnosti i upravljanja rizicima i uspostavljanja adekvatnog sistema kontrole u digitalnom okruženju, kao i obrazovanje i kontinuirana edukacija profesionalaca u navedenim oblastima. Cilj je efikasnije i bezbedno korišćenje IT resursa i digitalnih podataka. Udruženje ISACA Beograd je nezavisni član globalne asocijacije ISACA, jedne od najpoznatijih stručnih organizacija na svetu u oblasti sigurnosti, rizika i kontrola u digitalnom okruženju.

Nezavisna međunarodna istraživanja pokazuju da članstvo u ISACA i/ili posedovanje ISACA sertifikata poboljšava profesionalno priznavanje, kredibilitet i potencijal za napredak. Takođe, daje pojedincu mogućnost besplatnog pristupa kvalitetnim materijalima koji se odnose na najsavremenije pristupe i metodologije iz oblasti koju pokriva ISACA asocijacija, kao i dostupnost najkvalitetnijih stručnjaka i iz Srbije ali i širom sveta.

Čini se kao da u oblasti sajber bezbednosti ima više muškaraca nego žena. Da li je to pogrešna percepcija?

Nije da se samo čini, tako je i u praksi. Prema izveštaju koji je (ISC)² izdao 2018. godine, zastupljenost žena u sajber bezbednosti na globalnom nivou je 11 odsto, dok je taj procenat u Evropi samo sedam odsto.

Lara Vučetić

Povratak na sadržaj

GLOBALNO SAJBER OSIGURANJE

Najbrže rastuće legalno tržište

Uporedo sa rastom opasnosti, raste i tržište sajber osiguranja – procenjuje se da će njegova vrednost 2025. godine prebaciti iznos od 20 milijardi dolara

Tržište sajber osiguranja dostići će vrednost veću od devet i po milijardi dolara u 2021. godini, što je 20 odsto veći rast u odnosu na prošlu godinu, a i u narednom periodu može se očekivati rast od po čak 25 odsto godišnje, procenjuju svetski analitičari.

Poslednjih godina promenila se percepcija privrednika kad je reč o sajber opasnostima: u brojnim anketama koje su se sprovodile među privrednicima na globalnom nivou, strah od sajber napada se sa šestog mesta tokom 2018. godine prebacio na prvo i premašio čak i strah od rizika izazvanih klimatskim promenama, koji je godinama držao ubedljivo prvo mesto.

"Udruženim snagama" sa pandemijom, sajber napadi su tokom prošle godine nadmašili sva očekivanja. Istovremeno sa rastom sajber kriminala, i rastom ulaganja u IT bezbednost za koje se procenjuje da će u 2025. godini biti u vrednosti oko 400 milijardi dolara – raste i vrednost tržišta osiguranja: prema procenama Minhen Re, ono će do 2025. dostići vrednost veću od 20 milijardi dolara. Najjače tržište trenutno je Severna Amerika (vrednost veća od 5,3 milijarde dolara), a snažan rast se predviđa i u Aziji, kao i u Evropi gde je vrednost ovog tržišta u 2020. bila oko milijardu dolara.

Izveštaj o pripremljenosti na sajber napade Hiscox Cyber Readiness Report pokazao je da je u 2019. godini 41 odsto kompanija iz SAD i Evrope pribavilo sajber osiguranje, a da još 30 odsto njih planira da to učini tokom 2020.

"Iako su sve industrije pod rizikom, najveća zainteresovanost je prepoznata u sektorima kao što su zdravstvo - zbog raspolaganja brojnim osetljivim podacima o ličnosti), farmacija - imajući u vidu da i proizvodni pogoni fabrika mogu biti pogođeni i dovesti do prekida rada, naftna industrija koja je trpela napade koji su recimo danima onemogućavali benzinskim pumpama da funkcionišu, hotelijerstvo - kako zbog podataka o ličnosti, tako i šteta usled napada koji dovode do prekida rada, finansijski sektor koji je jedan od najugroženijih zbog svoje prirode posla, i naravno sektor IT-a jer je on najsvesniji opasnosti koja postoji", kaže Bojan Jovanović iz kompanije Marsh.

Zdravstvena industrija bila je očigledno i najviše pogođena, bar sudeći po podacima Instituta Ponemon koji se bavi nezavisnim istraživanjima o zaštiti podataka i sajber politikama: tokom 2020. godine zdravstvena industrija našla se na vrhu liste najskupljih povreda podataka sa prosečnim troškom od 7,13 miliona dolara, što je 84 odsto više od globalnog proseka po industrijama.

Da je praktično nemoguće predvideti koje sve industrije mogu biti pogođene sajber napadom, pokazuje i jedan od najpoznatijih - "Petya" - koji je pogodio i reklamne,

Povratak na sadržaj

farmaceutske, građevinske, špediterske, logističke, konsultantske, naftne kompanije, pa čak i jednu multinacionalnu advokatsku kancelariju.

Šta u svetu pokriva polisa sajber osiguranja?

"Polise odnosno uslovi sajber osiguranja generalno su koncipirani tako da imaju nekoliko modula tj. vrsta pokrića: modul koji štiti sam sistem i potencijalno uništenje odnosno zaključavanje datoteka, zatim onaj koji se odnosi na krađu podataka o ličnosti, modul koji se odnosi na tzv. prekid rada usled sajber napada kao i modul koji pokriva tzv. sajber iznudu. U tom smislu svakoj kompaniji stoji na raspolaganju izbor između ovih modula, mada je preporuka da se svi osnovni moduli ugovore jednom istom polisom, jer po pravilu jedan sajber napad biva okidač za štete po više modula. Primera radi, sajber napadom se mogu zaključati datoteke pojedine kompanije, što može dovesti do prekida rada klijenta, a istovremeno dovesti i do curenja podataka o ličnosti - te bi praktično jednim napadom bila iscrpljena naknada štete po tri napred navedena modula", kaže Bojan Jovanović.

Prema njegovom iskustvu, zaštita podataka o ličnosti se prepoznaje kao najveći rizik za mnoge kompanije, imajući u vidu da je finansijska posledica štete teško predvidiva, kako u smislu samih kazni, zahteva trećih lica za naknadom štete, tako i posledica po sam brend kompanije. Kompanije ipak ne segmentiraju rizike kako bi se zaštitile samo od najvećih, već ugovaraju osiguranje tako da pokriju sve realno ostvarive sajber rizike koje mogu imati kao posledicu finansijsku štetu.

Promene izazvane pandemijom

Interesovanje kompanija za sajber osiguranjem od početka pandemije znatno je poraslo, prven-


Bojan Jovanović

stveno zbog rasta sajber napada koji je uslovljen globalnom zdravstvenom krizom. "Ipak, srazmerno interesovanju klijenata porastao je i oprez osiguravajućih društava, kao što je zbog pojedinih šteta koje su pogodile osiguravajuća društva na globalnom nivou došlo do ukupnog smanjenja kapaciteta i limita pokrića koje su osiguravači u mogućnosti da pruže za ovu vrstu osiguranja", kaže Jovanović, napominjući da govori o globalnim osiguravačima i globalnim klijentima koji imaju potrebu za limitima od više desetina miliona evra.

"Na lokalnom tržištu sve ovo je u znatno manjem obimu. Rast potražnje jeste zabeležen u određenom procentu, ali ne srazmerno riziku koji postoji. S druge strane, niža je i spremnost i kapaciteti osiguravača da pruže potrebna pokrića svojim klijentima, koja se za sada nisu smanjila uprkos pandemiji", kaže naš sagovornik.

Ukupne štete koje su pogodile osiguravače u "pandemijskoj" godini još nisu izbrojane.

"Za sada nemamo poseban podatak o procentualnom rastu broja šteta, a i iznosi šteta i posledice napada koji su se desili u 2020. godine biće poznati tek nakon dužeg vremena. Mnoge kompanije često zbog reputacionog rizika odlučuju da zataškaju sajber napade i da interno reše problem, pa je zato još teže doći do stvarnih podataka o štetama koje kompanije trpe na godišnjem nivou baš po ovom osnovu", kaže Jovanović.

On podseća i na neke od najvećih šteta koje su se desile u 2020. – jedna od njih, IT kompanija Technology Solutions Corp, javno je objavila da je na ime iznude platila iznos od oko 60 miliona dolara.

Neki napadi još nisu valorizovani, poput onih na neke od najvećih svetskih kompanija - ZOOM, Marriot, Twitter, Garmin, pa čak i na jednu od najvećih svetskih sajber sekjuriti kompanija, FireEye".

Trendovi za napadače

Izveštaj o globalnoj bezbednosti Trustwawe za 2020. godinu pokazao je da je regija koja je najčešće napadana u smislu krađe i zloupotrebe podataka Azijski Pacifik gde se u 2019. godini dogodilo 37 odsto svih sajber napada. Drugo mesto zauzela je Severna Amerika sa 33 odsto sajber napada, slede Evropa, Bliski Istok i Afrika sa ukupnim udelom od 25 odsto.

Među evropskim zemljama, Nemačka prednjači po prosečnim troškovima kompanija usled povrede podataka - 4,45 miliona dolara u 2020. godini, što je pad od sedam odsto u odnosu na godinu pre.

„Osiguranjem se trenutno mogu pokriti gotovo svi poznati tipovi šteta koje su kompanije trpele u prethodnim godinama usled sajber napada. Ono što je u poslednje vreme generalan trend je rast zahteva za plaćanjem otkupnina usled ransomware-a, odnosno malvera koji zaključava računar, te je to rizik koji postaje vrlo realan, ali daleko od toga da je i jedini koji može pogoditi kompaniju", kaže Bojan Jovanović.

Osiguravajuća društva u svetu prate „želje" klijenata, ali i dešavanja u ovoj oblasti, pa u slučaju pojedinih nedostataka nadograđuju i upotpunjuju svoju ponudu rizicima koje smatraju novom realnošću – objašnjava naš sagovornik iz kompanije Marsh.

Selena Stanislavski

Povratak na sadržaj

SAJBER NAPADI I OSIGURANJE U SRBIJI

Mnogo meta, a polise još u začetku

IT stručnjaci dele kompanije na “one koje su već bile meta sajber napada, i na one koje su bile, ali to još ne znaju”. Ponuda polisa sajber osiguranja tek počinje da se razvija, a potražnja od strane preduzeća sigurno će taj razvoj ubrzati

“Imamo problema sa vašim bankovnim podacima. Molimo vas da nam pošaljete vašu bankovnu karticu. Slikajte obe strane i kažite nam koliko novca imate na kartici. Pozdrav, vaša banka”.

Ovakvu poruku su početkom marta dobijali klijenti Banke Inteza sa lažne Fejsbuk stranice, a slični pokušaji prevara i krađe podataka svakodnevno kruže internetom.

U Mreži za poslovnu podršku kažu da je broj sajber napada u svetu povećan 620 odsto u odnosu na period pre 2012. godine, a broj spamova (neželjene elektronske pošte) raste na mesečnom nivou više od 1.100 odsto. Zbog tolikog broja pokušaja elektronskih prevara i krađa podataka IT stručnjaci dele kompanije samo na “one koje su već bile meta sajber napada, i na one koje još ne znaju da su bile takva meta”.

Dragoljub Rajić, konsultant Mreže, za naše čitaoce kaže da su u Srbiji sajber napadima najviše izložene banke i finansijske institucije, ali, ipak, značajno manje nego u Evropi. Razlog za to je i manji obim domaćeg tržišta i daleko niži nivo obrta ukupnih finansijskih sredstava, ali i nepostojanje mogućnosti za čitav niz online transakcija i usluga. I nivo industrijske špijunaže daleko je manji u Srbiji nego u razvijenim zemljama sveta, zato što su odeljenja razvoja i inovacija većine stranih kompanija koje nešto proizvode u Srbiji pretežno van zemlje, a ta odeljenja su obično mete hakerskih napada.

Po podacima RATEL-a, na svakih 39 sekundi u Srbiji dogodi se jedan sajber napad, kojeg nisu pošteđene ni računarske mreže lokalnih samouprava. Istraživanje o bezbednosti informacionih sistema koje je Nacionalna alijansa za lokalni ekonomski razvoj (NALED) sprove-

Povratak na sadržaj

la u 69 gradova i opština pokazuje da 58 odsto lokalnih samouprava nije proveravalo bezbednost mreže, a nijedna od anketiranih nije u poslednjih godinu dana testirala plan oporavka u slučaju kolapsa sistema.

Meta sajber napada bilo je čak 47 odsto lokalnih samouprava, a njih 12 odsto ne zna da li su bili hakovani. U petini samouprava ne postoji zaposleni zadužen za IT, a ostale tek na svaka 62 službenika imaju jednog specijalizovanog za ovu oblast. Svaka druga ne menja redovno pristupne lozinke, a u velikom broju su i službenici nedovoljno obučeni.

Ivan Živković, šef radne grupe za informacionu bezbednost u NALED-ovom Savezu za eUpravu i rukovodilac prodaje za javni sektor u Majkrosoftu ističe da se zaštita podataka ne može posmatrati kao jednokratna aktivnost već kao konstantan proces koji zahteva permanentno unapređivanje, nadogradnju, praćenje, a pre svega prevenciju.

„Neadekvatna primena odbrane od sajber opasnosti, odnosno nepostojanje strategije i alata za odbranu uglavnom dovode do toga da organizacija nije ni svesna da je bila predmet napada. Postoji dosta primera organizacija u Srbiji koje imaju uspostavljena izuzetno uspešna odeljenja koja se bave informacionom bezbednošću, ali je takođe veliki broj organizacija još na samom početku, a postoje i one koje nisu svesne važnosti ove teme“, kaže Živković za naše čitaoce.


Ivan Živković

Postojanje strategije ili internog akta o informacionoj bezbednosti kao i njegova primena je po njegovoj oceni pravi pokazatelj zrelosti neke organizacije. Adekvatno adresiranje ove teme unutar organizacije je, kako je rekao, pokazatelj svesnosti organa upravljanja o tome da u doba digitalizacije i informacionih tehnologija nije dovoljno imati samo aparat za gašenje požara u firmi već je podjednako važno imati i adekvatne alate za zaštitu od sajber napada.

Šta pokriva polisa osiguranja od sajber rizika

Porast sajber rizika u čitavom svetu gotovo da je “iznudio” i ponudu sajber osiguranja – polisa osiguranja od sajber rizika. Predviđanja su da će u narednih pet godina tržište osiguranja od sajber rizika, koje je sada vredno oko sedam milijardi dolara, dostići vrednost od preko 20 milijardi dolara.

Polisu za pokriće štete od sajber napada za sada u Srbiji nudi samo Wiener Städtische osiguranje, a drugi osiguravači poput kompanije Đenerali – aktivno razmatraju pokretanje ove usluge.

Prema njihovom iskustvu, o sajber rizicima najviše vode računa IT kompanije, jer njihovi ljudi i najviše znaju o ovoj vrsti rizika, ali ih ugovaraju i druge kompanije koje raspolažu velikim brojem ličnih podataka trećih lica, poput velikih trgovinski lanaca, medicinskih ustanova, banaka...

Da bi neka firma mogla da ugovori polisu osiguranja od sajber rizika, ona najpre mora da popuni upitnik u kojem daje osnovne podatke o svom kompjuterskom sistemu, primenjenoj zaštiti, načinu prenosa i skladištenja podataka, ali i finansijske podatke, informacije o uticaju na redovno poslovanje, o broju i prirodi ličnih podataka trećih lica. Podrazume-

Sajber osiguranje traže strani partneri

Saša Atanacković, direktor kompanije “Gecko” kaže da već pet godina ima polisu koja, između ostalog, pokriva i štete nastale usled sajber napada, ali i razne vrste odgovornosti povezane sa sajber rizicima. Ova polisa im je neophodna da bi uopšte obavljali poslove u inostranstvu.

„Mi smo domaća firma ali radimo na inostranim tržištima, i naši partneri zahtevaju da posedujemo takvu polisu. Osigurana suma naše polise je šest miliona evra. Za inostrana tržišta to nije veliki iznos. Veliki problem na domaćem tržištu je što je teško nabaviti polise sa većim osiguranim sumama koje bi pokrivale i zemlje van Srbije. Potreba postoji, ali bi osiguravači trebalo da se otvore ka ovoj vrsti osiguranja i da polise prilagode potrebama kompanija. Na zapadu su takve polise, koje imaju velika pokrića, dosta zastupljene i nisu čak ni skupe za kompanije“, rekao je Atanacković.


Dragoljub Rajić

Povratak na sadržaj

va se da je na svakom kompjuteru instaliran anti-virus softver koji se ažurira najmanje jednom sedmično, da se najvažniji podaci kopiraju i skladište na drugoj bezbednoj lokaciji najmanje istom dinamikom, da postoji kontrola mrežnog saobraćaja kao i kompanijska sigurnosna politika, i da je omogućeno njeno sprovođenje.

Polisa osiguranja sajber rizika pokriva direktne finansijske posledice sajber incidenta. Osim troškova angažmana IT stručnjaka, gubitka podataka trećih lica i odbrane u slučaju sudskih tužbi, jednom kupljena polisa osiguranja od sajber rizika podrazumeva pokriće i za tzv. multi-medijalnu odgovornost, kojoj su kompanije bile više nego uobičajeno izložene tokom vanrednog stanja.

Polisa sajber osiguranja nadoknađuje i iznose novčanih kazni izrečenih na osnovu prekršajnih naloga ovlašćenog državnog organa, a u takvim okolnostima se neretko javljaju i troškovi upravljanja kriznom situacijom kao i troškovi obaveštavanja korisnika i troškovi podrške klijentima.

Kompanije koje ne dolaze u kontakt sa velikim brojem ličnih podataka trećih lica, prvenstveno strahuju od gubitaka poslovnih prihoda usled nemogućnosti poslovanja nakon sajber incidenta. Uzročnik takvog prekida rada može biti, kako širenje zlonamernog koda ili virusa postavljenog samo sa željom da se nanese šteta, tako i nemogućnost pristupa kompjuterskim sistemima i podacima usled želje da se izvrši iznuda finansijskih sredstava da bi se pristup omogućio. Polisa sajber osiguranja u oba slučaja reaguje, tj. nadoknađuje utvrđenu izgubljenu dobit: plaća troškove iznude ukoliko angažovani IT stručnjaci utvrde da je neophodno, a pod uslovom da su učinjeni svi razumni napori da se utvrdi da sajber iznuda nije sama po sebi prevara, a nadoknađuje i napore da se izbegnu i umanje gubici, ukazuju u Wiener Städtische osiguranju.

I drugi osiguravači u vreme kad je zbog pandemije Covid 19, da bi se obezdedila fizička distanca, rad iz kancelarija premešten „po kućama“ a informacioni sistemi postali manje zaštićeni - razmatraju ponudu nove polise.

„Uveliko razmišljamo o izlasku na tržište sa ponudom usluge sajber osiguranja. Naši timovi rade na prikupljanju podataka i kreiranju uslova za stvaranje proizvoda koji će na najbolji način odgovoriti na potrebe klijenata. Očekujemo da ćemo u narednom periodu doći do adekvatnog rešenja koje ćemo ponuditi klijentima“, kažu u Đenerali osiguranju.

Marica Vuković

Povratak na sadržaj

DIGITALNA PONUDA OSIGURANJA

Polisa, prijava i rešavanje štete „na klik“

Osiguravajuće kompanije u Srbiji ubrzano prilagođavaju svoje usluge digitalnim trendovima, pa je danas moguće onlajn ugovoriti većinu vrsta osiguranja, i prijaviti štetu preko posebnih aplikacija na telefonu

Mladi, urbani, zaposleni i porodični ljudi koji nemaju mnogo vremena da čekaju u redu, najčešće kupuju polise osiguranja onlajn na iPad-u ili android telefonu. Ponuda, logično, prati trendove u potražnji, pa tako većina domaćih osiguravajućih kuća nudi onlajn polise za osiguranje domaćinstva, putno osiguranje i pomoć na putu. Osim toga i šteta može da se prijavi preko aplikacija.

U poslednjih godinu dana, „zahvaljujući“ pandemiji, i klijenti skloni tradicionalnoj kupovini u filijalama shvatili su prednost veb kanala u prodaji polisa. Domaće tržište osiguranja prati svetske trendove i primetan je napredak u pogledu digitalizacije, a kako ukazuju poznavaoci ovog tržišta - postoji potencijal i za primenu još modernijih usluga.

Inovacije u prodaji polisa

Iako se na prvi pogled digitalizacija poistovećuje sa prodajom preko interneta, Miodrag Jovanović, direktor direkcije za IT i integrisani sistem menadžmenta u kompaniji Đenerali osiguranje kaže da je suština u tome da se klijentima obezbedi kompletno korisničko iskustvo koje, osim prodaje uključuje i ispunjenje obaveza po osnovu ugovora o osiguranju, odnosno rešavanje šteta.

“Pravi period digitalne transformacije dolazi zajedno sa pristupačnim internetom i širokom rasprostranjenošću pametnih telefona. Đenerali je bio pionir na domaćem tržištu kada je 2017. godine ponudio prve mobilne aplikacije, kako za klijente, tako i za svoje agente prodaje“, kaže Jovanović.

Autoodgovornost mora da pređe na onlajn

Najveći potencijal za digitalnu prodaju je osiguranje od autoodgovornosti. „Prema zakonskoj regulativi AO nije moguće prodavati u digitalnom obliku - dokle god bude tako, ne možemo očekivati veliki napredak onlajn prodaje“, kaže Miloš Mamula iz Osiguranik.com.

Ratko Živković iz Wiener Städtische osiguranja se slaže da bi polise autoodogovornosti mogle da se prodaju onlajn. „Kod te vrste osiguranja je značajna činjenica što su klijenti navikli da prilikom registracije vozila sve obave na jednom mestu, kupe osiguranje, uplate troškove registracije i dobiju registarske nalepnice“, kaže Živković.

Povratak na sadržaj


Miodrag Jovanović

I ostale kompanije na tržištu osiguranja, podseća on, veoma ozbiljno rade na digitalizaciji i stvara se konkurentsko okruženje koje podstiče ubrzanje ukupne digitalne transformacije.

“Naša kompanija pruža digitalno iskustvo svojim klijentima preko mobilnih aplikacija, web shop-a i portala za klijente, ali takođe i preko mreže partnera, pre svega banaka, telekomunikacionih operatera i digitalnih zastupnika u osiguranju“, navodi Jovanović.

Trenutno, klijenti mogu samostalno da zaključe preko ove kompanije osiguranje domaćinstva i hitnih intervencija u objektu, putno osiguranje, osiguranje kućnih ljubimaca i osiguranje pomoći na putu.

Klijente, kako napominje, možda ipak najviše zanima prijava i rešavanje šteta.

“Na primer, kod putnog osiguranja omogućili smo besplatne govorne pozive ili čet preko interneta sa asistencijom, a kod osiguranja motornih vozila klijenti mogu samostalno da snime oštećenje na vozilu i dostave prateću dokumentaciju preko najsavremenije mobilne softverske platforme“, kaže on.

Njegov kolega, Alen Žagar, menadžer za digitalizaciju u kompaniji Đenerali osiguranje, ističe da je posebno u periodu korona krize kompanija klijentima omogućila ugovaranje i rešavanje šteta na daljinu.

Uloga veštačke inteligencije

Alen Žagar dodaje da iako klijenti na našem tržištu dobijaju sve kompletniju ponudu digitalnih proizvoda i usluga, na razvijenijim tržištima postoje i radikalnija digitalna rešenja.

„Ulogu ljudi preuzimaju softverska rešenja koja se zasnivaju na analitici podataka i veštačkoj inteligenciji, biometrijskim i drugim tehnologijama“, kaže on.

Takođe, osiguravajuće kuće imaju sve većeg konkurenta u malim start-up kompanijama koje nude inovativna rešenja, ukazuje on.

“Pored njih, veliki tehnološki giganti kao što su Gugle i Amazon, takođe, najavljuju ozbiljan ulazak u biznis osiguranja“, kaže Žagar.

Nove platforme

Digitalna tehnologija omogućava da se poveća fleksibilnost, preciznost i usmerenost osiguranja na kupca, kaže Đorđo Markeđani, predsednik Izvršnog odbora DDOR osiguranja: „Lakša povezanost izvora podataka omogućava precizniju i fleksibilniju kvantifikaciju rizika. Na primer, pokriće imovine zavisi od lokacije, vrste i preferencija klijenta“.

Ivan Grujić


Đorđo Markeđani

Markeđani kaže da je Srbija, sa tačke gledišta uređaja koji se koriste, digitalna zemlja, dok posmatrajući zrelost klijenata i finansijsku kulturu - još treba da se razvija.

Tržište Srbije je stoga spremno da iskoristi prednosti digitalizacije kod nekih vrsta proizvoda, na primer, putnog osiguranja, zdravstvenog osiguranja, asistencije, koji se i češće kupuju. Međutim, u drugim oblastima, kako dodaje, i dalje prevladava potreba da se objasni smisao i obim pokrića.

“Mi smo na digitalnoj platformi, ali neki od naših procesa završavaju se ipak ljudskim uticajem. Naša veb prodavnica pruža mogućnost kupovine proizvoda poput putnog osiguranja i osiguranja pomoći na putu. U oblasti prijave i procene šteta, tehnologija omogućava bolje i brže usluge. Planiramo uvođenje novih digitalnih rešenja za poljoprivredu i dobrovoljno zdravstveno osiguranje. Opcija prijave šteta preko veba ili aplikacije takođe će učiniti da osiguranje bude privlačnije jer će biti dostupno 24 sata dnevno, sedam dana u nedelji“, navodi Markeđani.

Ratko Živković, rukovodilac službe za razvoj i podršku prodaji u kompaniji Wiener Städtische osiguranje kaže da imaju u ponudi onlajn platformu (Moj Wiener portal) koja osiguranicima nudi uvid u ugovore o osiguranju, pla-

Povratak na sadržaj


Ratko Živković

ćenu premiju, dugovanja, kao i mogućnost onlajn plaćanja premije za dinarske ugovore.

"Uskoro će na portalu biti omogućena i prijava šteta, kao i uvid u odštetne zahteve. Preko mobilne aplikacije "Wiener zdravlje" može se poslati zahtev za pregled u zdravstvenim ustanovama. Na našem web shop-u moguće je kupiti putno osiguranje i osiguranje domaćinstva. Digitalni agent (WIDA) daje informacije i pristup veb kalkulatorima za životno i kasko osiguranje, kao i osiguranje domaćinstva", kaže Živković.

U Wiener Städtische osiguranju zabeležili su, kako kaže, značajan rast interesovanja klijenata koji su koristili veb kalkulator.

"Takođe, značajno je povećan broj info ponuda preko veb platformi i mobilnih aplikacija, a preko nekih je i ugovarano osiguranje „na daljinu". Uglavnom onlajn se mogu kupovati polise kod kojih se može automatizovati proces procene rizika. To su, na primer, putna osiguranja i osiguranja domaćinstva", kaže Živković.

Digitalno vs. tradicionalno

Miloš Brusin, predsednik Izvršnog odbora Sava životnog osiguranja kaže da je pandemija doprinela ubrzanom rastu broja ponuda "na klik" i ubrzavanju procesa digitalizacije u poslovanju.

"Većinu polisa kod neživotnih osiguranja moguće je ugovoriti i kupiti na daljinu. Registrovano je značajno povećanje onlajn ponuda i polisa koje se ugovaraju na daljinu", kaže Brusin.

Sava osiguranje u svom web shopu ima kombinovano osiguranje domaćinstva kao i putno zdravstveno osiguranje i paket putnih osiguranja.

Pandemija je svakako ubrzala pokretanje digitalnih rešenja, ali prema oceni Ivana Grujića, pomoćnika izvršnog direktora Triglav osiguranja, najveći broj usluga i dalje se sprovodi na tradicionalan način. Triglav osiguranje već nekoliko godina u svojoj ponudi ima


Miloš Brusin

mogućnost ugovaranja putnog zdravstvenog osiguranja preko web shop-a, a od 2019. godine na ovaj način se može ugovoriti i osiguranje stanova, kuća i stvari domaćinstva. Takođe, omogućili su i plaćanje premija putem platnih kartica na portalu.

Internet pomaže jačanju svesti o značaju osiguranja

Ako se, pak, poredimo sa zemljama u regionu, Miloš Mamula, direktor portala Osiguranik smatra da po pitanju digitalne transformacije još pomalo kaskamo za njima. Mnogi su, ipak, shvatili potencijal i prednosti digitalnih kanala u prodaji osiguranja što dovodi do većeg broja aktivnosti na internetu nego ranije. To je dobro zbog širenja svesti o značaju osiguranja. Pre pandemije, onlajn se najviše prodavalo putno zdravstveno osiguranje, čija je prodaja sada pala jer nema putovanja.

„Internet tržište osiguranja nije potpuno uređeno jer postoje sajtovi koji nude razne usluge osiguranja, a nije jasno koje tačno društvo za zastupanje ili posredovanje stoji iza tih portala. Takođe, ne postoje pravilnici o pravima korisnika i politike za obradu podataka o ličnosti, što su elementarni preduslovi za poslovanje u oblasti osiguranja na internetu", zaključuje Mamula.

Olivera Bojić

Može li životno osiguranje da se ugovori onlajn?

Kupovina preko različitih veb platformi je pogodna za jednostavne i standardizovane proizvode namenjene klijentima. Na domaćem tržištu nije uobičajena onlajn prodaja životnog osiguranja, ukazuju sagovornici. Zakonska regulativa zahteva da klijent potpiše ponudu osiguranja, postoje stroga pravila u vezi sa identifikacijom klijenta, a postoji i druga dokumentacija u skladu sa Zakonom o sprečavanju pranja novca i finansiranja terorizma. Ipak, u poslednje vreme radi podsticaja digitalizacije u finansijskom sektoru Narodna banka Srbije omogućila je video identifikaciju klijenata. Tako je pokrenuta mogućnost onlajn savetovanja, i ugovaranja ponude između klijenta i osiguravajuće kuće, uz pomoć video-identifikacije.

"Sava životno osiguranje je prvo predstavilo mogućnost savetovanja i ugovaranja ponude životnog osiguranja na ovaj način. Inače, klijenti koji dominantno kupuju polise onlajn su mlađi ljudi, iz urbanih sredina, „familijarni" sa novim tehnologijama, koji žele da realizuju svoju kupovinu sada i odmah, bez čekanja, na jednostavan i brz način", kaže Miloš Brusin.

Povratak na sadržaj

SKY EXPRESS

Da li je digitalizacija

Sajber napadi su u porastu. Jaz između broja napada i spremnosti adekvatnog odgovora na napade se svakodnevno produbljuje. Hakeri sve više žele da iskoriste sigurnosne propuste za krađu dragocenih podataka, uključujući finansijske detalje i osetljive lične podatke. Za korporacije, uticaj ovih napada prevazilazi finansijski gubitak. Od problema u odnosima s javnošću i gubitka poverenja kupaca do oštrih kazni regulatora, jedan uspešan sajber napad može paralisati poslovanje korporacije i naštetiti njenoj reputaciji i profitabilnosti u godinama koje dolaze.

Svaki napredak je sa sobom, osim benefita, donosio i prateće rizike. Digitalna revolucija, kao možda najveći događaj nakon vatre, točka i električne energije, takođe donosi brojne rizike, ali to ni u kom slučaju ne znači da smemo da se distanciramo od napretka, jer ćemo time SIGURNO načiniti nepopravljivu štetu za poslovanje.Jedini pravi odgovor je kreiranje adekvatnog odgovora na rizike, čime stvaramo dodatnu vrednost našeg poslovanja.
Za industriju osiguranja, tržišna prilika je ogromna. Upravljanje rizikom informacionih tehnologija postaje prioritet za preduzeća širom sveta, bez obzira na veličinu. A s obzirom na to da se očekuje da će globalno tržište sajber osiguranja dostići 433,6 milijardi dolara do 2030. godine, u poređenju sa 119,9 milijardi dolara u 2019*, sada je vreme za akciju.

*Cyber Security Market to Cross $433.6 Billion Revenue by 2030: P&S Intelligence (prnewswire.com)

Poslovna prilika je nesumnjivo atraktivna, no, to sa sobom nosi i određene, ne baš jednostavne izazove. Pre svega, kao relativno novi podsektor, malo je istorijskih podataka o sajber osiguranju.
Nemogućnost prikupljanja i analize relevantnih podataka otežava iskorišćavanje potencijala sektora, pa će u narednom periodu razmena podataka biti od vitalnog značaja.
Procena rizika i izloženosti digitalnim pretnjama takođe je teška, jer su mnogi osiguravači opterećeni složenošću određivanja cena proizvoda sajber osiguranja.

Za osiguravajuće kompanije je veoma važno da kreiraju široku paletu proizvoda dizajniranih tako da odgovaraju svim vrstama preduzeća i njihovim raspoloživim budžetima.
Strategiju razvoja proizvoda osiguranja namenjenih adresiranju sajber pretnji je neophodno bazirati na sledeća četiri stuba:

USPOSTAVLJANJE SISTEMA RANGIRANJA

Proaktivnim i kontinuiranim merenjem nivoa informacionog rizika klijenta, osiguravači će moći da na pouzdan način procene potencijalne uticaje sajber napada na preduzeće, pre nego što se napad dogodi. Ovaj neizostavan korak, ne samo da pomaže u oblikovanju strukture i cena proizvoda sajber osiguranja, već i samim klijentima pruža precizne informacije šta je to što utiče na ocenu njihovog rizika i ukazuje na korake koje je neophodno preduzeti da bi svoj rejting popravili.

osigurana?

Većina cyber security kompanija poseduje neophodan “know how” potreban za procenu informacionog rizika, ali, proces koji je potrebno preduzeti da bi se na pravi način izvršila procena rizika zahteva vreme i ljudske resurse i to u praksi predstavlja izuzetno limitirajući faktor.
Kreiranjem jedinstvenog sistema rangiranja rizika, koji kontinuirano prikuplja, prati i analizira raspoložive podatke koji utiču na ocenu rizika, baziranog na ustanovljenim i nepobitnim pravilima, relevantnim za oblast poslovanja klijenta, i sa mogućnošću dobijanja izveštaja u izuzetno kratkom vremenskom periodu, osiguravači dobijaju najbitniji ulazni parametar neophodan za kreiranje ponude.

PODIZANJE SVESTI

Uprkos rastućoj stopi sajber napada, kod većine potencijalnih klijenata ne postoji svest o postojanju rizika i mogućih posledica. Jasne i ciljane obrazovne i informativne kampanje koje su usredsređene na sajber rizike i strategije odgovora na rizike pomažu klijentima da se bolje upoznaju sa potrebama i mogućim odgovorima.
Podsticaj potražnje za sajber osiguranjem kroz kampanje javnog informisanja je od vitalnog značaja. Osnivanje lokalnih i regionalnih inicijativa za podizanje svesti biće ključno za povećanje svesti o sajber rizicima, kao i adekvatnim odgovorima na uočene rizike.
Takođe, neophodno je sprovesti edukaciju brokera tako da oni tačno znaju šta prodaju i koji proizvodi su najprikladniji za koju vrstu poslovanja. Štaviše, standardizacija formulacije olakšala bi razumevanje ponude. Doslednost i jednostavnost su ključni za uspeh proizvoda sajber osiguranja.

RAZMENA PODATAKA

Radeći zajedno, osiguravajuće kuće, bezbednosne kompanije i zakonodavci moraju razviti sistem prikupljanja i razmene podataka potrebnih za kreiranje odgovarajuće strukture, cene i plasmana sajber osiguranja kao osnovnog dela ukupnog portfolia osiguranja bilo koje kompanije.
Saradnja osiguravača sa zakonodavnim organima i kompanijama koje se bave bezbednošću je ključna, na nacionalnom i globalnom nivou.

FOKUS

Sajber napadi mogu pogoditi organizacije svih profila i veličina, kao i pojedine profesionalce poput advokata i lekara koji svakodnevno koriste osetljive lične informacije. Proizvodi sajber osiguranja za manje igrače ogromno su i uglavnom neiskorišćeno tržište.

Nekada posmatrani kao dve potpuno odvojene grane industrije, ponekad i suprotstavljene, sektori sajber sigurnosti i sajber osiguranja postaju sve bliži. Ovo već sada stvara zanimljive mogućnosti za obe strane, a u budućnosti će nesumnjivo konvergencija biti još intenzivnija.

OTPORNOST BANAKA NA SAJBER NAPADE

Odbrana jača od napada

Pandemija Covid-19 stavila je pred bankarski sektor nove izazove po pitanju sajber sigurnosti: napadi na banke u poslednjih godinu dana povećani su za oko 35 odsto, procene su Evropske centralne banke. Banke se uspešno brane dobro uspostavljenim sistemima za detekciju i brzo reagovanje na incidente

Darko Šehović

Bankarski sektor u Srbiji pokazao je veliku otpornost na sajber napade, koji su postali učestaliji, naročito tokom pandemije virusa Covid-19. Banke se uspešno brane upravo dobro uspostavljenim sistemima za detekciju i brzim reagovanjem na incidente, slažu se naši sagovornici. Veliku ulogu igraju i klijenti i zbog toga je potrebno da daju svoj dopinos i da prate uputstva koja im banka dostavlja. Izazovi očekuju bankarski sektor i u 2021. godini, jer će i dalje raditi u izmenjenim uslovima poslovanja.

"Sve banke u Srbiji poštuju postojeće propise koji važe u našoj zemlji, ali i svetske standarde iz ove oblasti. Rezultat toga je najbolja praksa i veoma visok nivo zaštite", kaže Darko Šehović, rukovodilac službe za bezbednost informacija u Udruženju banaka Srbije. Banke imaju složene sisteme zaštite, koji sadrže više nivoa i segmenata: to su, kako kaže, različita hardverska i softverska rešenja za otkrivanje, analizu i prevenciju sajber napada.

Napadi češći tokom pandemije

Procene Evropske centralne banke pokazuju povećanje napada za 35 odsto tokom pandemije na globalnom nivou, a slično stanje je i u Srbiji. "Napadači su kao mamac koristili visoku zainteresovanost za pandemiju i virus SARS-COV2 i varali su građane nudeći im navodno informacije u vezi sa aktuelnom zdravstvenom situacijom", dodaje Šehović.

Aleksandar Bratić, stručnjak za sajber bezbednost, kaže da je bankarski sektor uvek atraktivan za napade, a da je Covid-19 doveo do toga da su banke promenile

> Kako će pandemija očigledno biti aktuelna i u 2021. godini potrebno je redefinisati strategiju zaštite u skladu sa nastalim promenama

operativno delovanje i operativne procedure, kao i klijenti banaka.

„Kada posmatramo metodologiju napada sajber kriminalaca, uočavamo da se napadi najčešće dešavaju kad su zaposleni u bankama pod pritiskom ili menjaju način rada. Tokom cele 2020. godine zaposleni i klijenti banaka morali su menjati način života i poslovanja, tako da je

Bezbedno korišćenje bežičnih mreža (WiFi)

1. Uvek postavite snažne lozinke na svoj bežični uređaj (za pristup uređaju i za povezivanje sa bežičnom mrežom) - uređaji koje kupite obično imaju podrazumevane lozinke koje se mogu pogoditi.
2. Ukoliko obavljate transakcije preko bežičnih mreža, proverite da li to radite preko bezbednog komunikacijskog kanala (npr. https).
3. Budite oprezni kada pristupate nepoznatim bežičnim mrežama, koristite savete iz sekcije Bezbednost vašeg računara.

Izvor: Udruženje banaka Srbije

Povratak na sadržaj

2020. godina bila idealna za takve napade. Relativno stabilno poslovanje banaka bez velikih promena je u toku pandemije promenjeno, tako da su vektori napada koji su nekada bili prilično neefikasni, ponovo postali aktuelni“, objašnjava Bratić.

Najčešći napadi su i dalje, kako kaže, „phising“ napadi kojima kriminalci pokušavaju da dođu do korisničkog imena i lozinke, kao i napadi na korisničke sesije.

Kako se banke brane?

Banke bi, kako ocenjuje Bratić, trebalo da se prilagode novonastaloj situaciji, da urade analizu rizika u novim okolnostima i da na osnovu toga promene fokus i način zaštite svojih informacionih sistema.

„Svakako je potrebno da podignu nivo komunikacije sa klijentima i zaposlenima po pitanju informacione bezbednosti. Ove mere bi na kratak rok donele najviše rezultata, a kako će pandemija očigledno biti aktuelna i u 2021. godini potrebno je redefinisati strategiju zaštite i odrediti akcione planove za novonastali model rada“, ocenjuje Bratić.

Aleksandar Bratić

Darko Šehović kaže da banka u celini mora da ima svest o sajber rizicima, odnosno da top menadžment banke pruža podršku programima zaštite. “Ovo je nužno zbog obezbeđenja budžeta, ali i zbog strateškog opredeljenja i definisanja jasnih ciljeva. Poverenje je jedan od osnovnih elemenata na kojem se zasniva odnos između klijenata i banaka, pa je visok nivo bezbednosti u svakom pogledu prioritet banaka“, navodi on. Napadači u sajber prostoru ne poznaju radno vreme, tako da se napadi događaju praktično 365 dana u godini. „U najvećem broju to su napadi na klijente i njihovu infrastrukturu, kao najslabiju kariku u lancu finansijskih transakcija. Banke se uspešno brane upravo dobro uspostavljenim sistemima za detekciju i brzo reagovanje na incidente“, dodaje on.

Šta klijenti mogu da urade?

Za klijenta je, kaže Šehović, najbolje da prati uputstva koja mu dostavlja njegova banka. Osim toga, korisne informacije se mogu pronaći na sajtu Udruženja banaka Srbije, Nacionalnog CERT-a i drugim.

Aleksandar Bratić takođe smatra da je potrebno da klijenti koriste sve ponuđene mere zaštite koje banke nude tokom transakcije, a naročito da se informišu o preporukama banaka za obavljanje transakcija. Tako bi rizik prilikom obavljanja transakcija sveli na minimum.

Sajber pretnje ostaju i u 2021.

Pred nama je po svoj prilici još jedna godina izazova, koja može biti i teža od prethodne. Portal Securelist.com by Kasperski u analizi “Sajber pretnje finansijskim institucijama” navodi da će većina pretnji iz 2020. godine, postojati i u narednih godinu dana. Pandemija Covid-19 će, kako kažu, verovatno prouzrokovati masovni talas siromaštva, a to će uticati da se poveća broj onih koji pribegavaju kriminalu, uključujući i sajber kriminal.

Snježana Davidović

Kakav računar Vam je potreban za sigurno obavljanje transakcija?

1. Vaš računar uvek treba da bude ažuriran, sa najnovijim ispravkama za operativni sistem i aplikacije koje koristite.
2. Instalirajte i konfigurišite antimalver program.
3. Instalirajte ili uključite zaštitni zid (firewall) kako biste se zaštitili od neautorizovanih pristupa ka Vašem računaru.
4. Za rad na računaru koristite nalog koji nema administratorske privilegije.
5. Kreirajte snažnu lozinku za Vaš nalog.
6. Redovno pravite kopije svih bitnih podataka u sistemu.
7. Posebno osetljive podatke možete dodatno osigurati tako što ćete ih enkriptovati na vašem računaru.
8. Uvek se izlogujte pre nego napustite svoj računar.

Izvor: Udruženje banaka Srbije

Bezbedno korišćenje elektronske pošte

Elektronska pošta je sastavni deo svakog poslovanja, što potencijalnim napadačima predstavlja jednu od osnovnih tačaka za pokušaj prevara ili kompromitavanja vašeg računara. Poruke, čiji je predmet prevara, mogu izgledati kao da dolaze sa prave elektronske adrese banke. Onima koji se bave nezakonitim radnjama je relativno jednostavno da kreiraju lažni upis u polju „Od“ (From). Adresa elektronske pošte koja se pojavljuje u polju „Od“ u poruci NIJE garancija da dolazi od lica ili organizacije navedene u adresi elektronske pošte. Banke Vam nikada neće tražiti lozinku ili druge poverljive podatke preko imejla!

Izvor: Udruženje banaka Srbije

Povratak na sadržaj

DIGITALIZACIJA U BANKARSTVU OLAKŠAVA POSLOVANJE

Sve više onlajn servisa za preduzeća

Iako možda sad izgleda nezamislivo, ide se ka budućnosti u kojoj će gotovina biti istisnuta. Pravi bum u razvoju digitalnog bankarstva očekuje se saradnjom banaka sa startap kompanijama koje razvijaju aplikacije koje mogu da olakšaju poslovanje kompanijama

Broj ljudi koji plaćaju onlajn povećao se za 15 odsto u odnosu na period pre izbijanja pandemije Covid-19, pokazalo je prošlogodišnje MasterIndex Srbija istraživanje. Onlajn plaćanja koristi 81 odsto ispitanika, od čega 10 odsto plaća onlajn makar jednom nedeljno, dok 45 odsto koristi onlajn plaćanja makar jednom mesečno.

Osim plaćanja, i klasični bankarski proizvodi se menjaju i sve se seli na mreže. Bankari kažu da rastu i krediti ugovoreni na daljinu, mada su podaci još u obradi.

Iako možda sad izgleda nezamislivo, naši sagovornici kažu da sve ide ka budućnosti u kojoj će gotovina biti istisnuta. U nekim zemljama poput Švedske takav scenario se takoreći već ostvario.

Plaćanja su, ipak, samo deo digitalne transformacije banaka koju čine brojni procesi. Pravi bum u razvoju digitalnog bankarstva očekuje se saradnjom banaka sa startap kompanijama koje razvijaju brojne aplikacije koje mogu da olakšaju poslovanje kompanijama.

Pametno bankarstvo

Prednosti digitalne transformacije u bankarstvu su brojne: automatizacija procesa, povećanje sigurnosti podataka, brži transfer, kraće vreme čekanja kao i bolje analiziranje i upravljanje podacima i rizikom, kažu u AIK banci.

„Savremeno poslovanje banke nezamislivo je bez kontinuiranog ulaganja i razvijanja digitalnih kanala i njima prilagođenih proizvoda i usluga, sa ciljem da se svakom klijentu ponudi personalizovano rešenje“, kažu u AIK banci.

Kod svih banaka onlajn bankarstvo je ključni korak u procesu digitalizacije. Klijenti NLB banke mogu preko eBanking i mBanking aplikacije da proveravaju stanje na računu, plaćaju račune, kupuju i prodaju devize, dobijaju druge informacije koje su za njih značajne.

„Uvođenjem NLB Pay digitalnog novčanika, omogućili smo

Svetski trendovi stižu iz Azije

U Mobi banci kažu da kada razmišljaju o novim proizvodima, budućnosti, inovacijama - gledaju i u pravcu Azije, gde njihova PPF grupa uspešno posluje. „Tamo je sve vrlo jednostavno jer je prilagođeno preferencijama lokalnih potrošača. Zato je i naša vizija za Mobi Banku da nastavimo sa inovacijama i transformišemo bankarstvo tako da bude mobilno, direktno i lako za rad“, kaže Bogdanović.

U ovoj banci očekuju da će 2021. godina biti godina velikih promena na bolje. Prvenstveno zahvaljujući zalaganju Vlade, eUprave i NBS sa kojima trenutno rade na značajnom projektu koji će, kako kažu, promeniti budućnost bankarstva u Srbiji zauvek.

Povratak na sadržaj


Aleksandar Bogdanović, Mobi banka


Branko Gregranović, NLB banka

plaćanje na prodajnom mestu bez korišćenja gotovine i kartica, dovoljno je da sa sobom imate svoj pametni telefon i možete da platite prislanjanjem telefona na POS terminal na kasi. Takođe, omogućili smo i plaćanje QR kodom u našoj mobilnoj banci. Više ne morate da popunjavate uplatnicu i čuvate šablone, dovoljno je da skenirate grafički kod na računu. Najzad, i procesi u vezi sa kreditiranjem su u velikoj meri digitalizovani, pa klijenti troše mnogo manje vremena za rad sa svojom bankom“, ukazuje Branko Gregranović, predsednik Izvršnog odbora NLB banke.

Na srpskom tržištu postoji i potpuno digitalna, Mobi banka, čiji direktor prodaje Aleksandar Bogdanović kaže da „njihovi korisnici imaju banku u džepu“.

„Oni mogu da plaćaju račune, šalju novac u zemlji i inostranstvu, podižu i uplaćuju evre i dinare na našim bankomatima. Tu smo da ljudima olakšamo, a ne otežamo život redovima i „fali ti jedan papir“ filozofijom. Primer za to je i onlajn zaključenje ugovora za keš kredite do 600.000 dinara. Ovo je moguće zahvaljujući NBS koja zaista svojom regulativom pomera klatno digitalizacije na pravu stranu istorije“, kaže Bogdanović.

Digitalizacija je, kako kaže, omogućila bezgotovinske transakcije, potpunu transparentnost, brzo i lako upravljanje ličnim i kompanijskim finansijama. I to sve 24/7, uz uštedu vremena i novca.

Manja preduzeća se lakše prilagođavaju

Nemanja Ranđelović, ekspert za digitalne kanale za pravna lica OTP banke Srbija, ističe da digitalizacija preduzeća u Srbiji predstavlja kompleksan proces koji zavisi od mnogo faktora kao što su veličina preduzeća, biznis model, trenutni stepen digitalizacije i slično. Bankari su zapazili u praksi da manja preduzeća lakše prihvataju digitalizaciju i promene nego veliki robusni sistemi. Glavni pokretač novih trendova su upravo mala i srednja preduzeća.

„Digitalni kanali, prvenstveno eBanking, kod velikih sistema i dalje je na nivou osnovnih, dok manja preduzeća koriste sve funkcionalnosti pa i mBanking. Ono što se ističe kao sledeći korak u digitalizaciji je korišćenje e-faktura koje su u Srbiji još na minimumu iako postoje zakonski okviri, tehničke mogućnosti i ponuda usluge kod više banaka u Srbiji, uključujući i OTP banku“, ukazuje Nemanja Ranđelović.

Sve više će se, kako kaže, pojavljivati aplikacije „trećih strana“ koje će se povezivati sa bankom koristeći „Open API“ koncept.

„Primer je Paušal aplikacija koja već radi sa našom bankom i pruža dodatnu vrednost u poslovanju ove grupe“, kaže on.

> Prednosti digitalne transformacije u bankarstvu su brojne: automatizacija procesa, povećanje sigurnosti podataka, brži transfer, kraće vreme čekanja, kao i bolje analiziranje i upravljanje podacima i rizikom

Povratak na sadržaj

Aleksandra Ognjanović, Erste banka

Nemanja Ranđelović, OTP banka

Uloga startapova u digitalizaciji

Pokretač digitalnih personalizovanih servisa će upravo biti startapovi sa aplikacijama koje će ispunjavati različite potrebe nezavisno od veličina preduzeća i biznis modela. Finansijske transakcije i razmena podataka će se obavljati preko Open API tehnologije. U Evropi je već napravljen pomak u ovoj sferi, dok u Srbiji postoje projekti nekoliko banaka i startap aplikacija, ali puna primena i veliki broj servisa očekuju se u narednim godinama.

„Naša banka je najviše radila na unapređenju servisa za trgovce koji svoj biznis model vide u onlajn prodaji te smo u ovom segmentu i najviše odmakli poredeći se sa bankama na tržištu. Ponudu smo zaokružili postavkom Developer Cornera, gde nudimo bazu znanja ali i mogućnost da se probaju sve funkcionalnosti u testnom okruženju bez dolaska u banku. Sledeća platforma koju lansiramo ove godine je shipping platforma koja će povezati kurirske službe i onlajn prodavnice tako da banka radi podelu transakcije za koju je zadužen korisnik a koja sadrži cenu robe i isporuke. Na ovaj način se olakšava i onlajn prodavnici i kurirskim službama i samom korisniku koji će moći transaprentno da predvidi troškove i olakša kupovinu“, najavljuje Nemanja Ranđelović.

I u Erste banci iz godine u godinu je dostupan sve veći broj digitalnih usluga i proizvoda. Klijenti ove banke mogu digitalne usluge da ugovore ili aktiviraju bez dolaska u filijalu, što je uticalo i na povećanje broja digitalno aktivnih klijenata za gotovo 40 odsto.

„Kompanijama smo omogućili e-commerce uslugu, kao i najsavremeniji servis bezbedne i brze razmene eDokumenata, koji snižava troškove poslovanja i omogućava bržu naplatu i likvidnost. Uskoro ćemo kompanijama ponuditi i aplikaciju za mobilno bankarstvo, kao i redizajnirano elektronsko bankarstvo“, ističe Aleksandra Ognjanović, direktorka Sektora razvoja za stanovništvo, mala preduzeća i preduzetnike Erste banke.

Danijela Nišavić

Kakva je budućnost gotovine?

Pored svih promena i rastuće popularnosti digitalnog bankarstva, gotovina neće prestati da se koristi tako brzo, bar ne u Srbiji, mišljenja je Aleksandra Ognjanović.

„Važno je imati na umu preferencije građana, kao i činjenicu da nemaju svi mogućnost da koriste druge opcije plaćanja“, smatra ona.

Sa njom se slaže i Aleksandar Bogdanović iz Mobi banke koji kaže da za mlađe generacije gotovina postaje sve više zastarela. „Keš ne treba potpuno otpisati, kao što ni radio nije potpuno nestao nastankom televizije“, kaže on.

Branko Greganović ipak misli da će u jednom trenutku doći do potpunog ukidanja korišćenja gotovog novca, jer su sve druge opcije za transakcije jednostavnije, efikasnije i komfornije.

„To se neće dogoditi sutra, i zbog čvrsto ukorenjenih navika nekih segmenata klijenata i zbog okruženja u kome još nisu stvoreni preduslovi za to. Ali sam uveren da će u jednom trenutku doći vreme kada se gotovina više neće koristiti“, kaže Greganović.

Povratak na sadržaj

Piše: Goran Kunjadić, CISO NLB Banka

BEZBEDNO KORIŠĆENJE DIGITALNIH BANKARSKIH USLUGA

Snažna lozinka, i oprezno sa otvaranjem linkova

Ne treba koristiti lično ime za lozinku, kako svoje tako ni članova porodice, a ne savetuje se ni korišćenje datuma rođenja. I nikako ne treba držati papirić sa lozinkom uz telefon ili u novčaniku

Vreme kada su banke napadane od strane naoružanih pljačkaša odavno je prošlo. Danas je u porastu sajber kriminal, a napadači koriste metode koje se u osnovi sastoje iz dva koraka: prikupljanje informacija, i sam napad odnosno preuzimanje novca sa računa. Očigledno je da bez prikupljenih informacija napad ne bi mogao biti izveden.

Sistemi banaka su tehnološki veoma dobro obezbeđeni sofisticiranim tehnologijama i tehnikama nadzora nad sistemom, a najslabija karika u sistemu je opet čovek. Posebno ranjiva grupa su korisnici digitalnih bankarskih usluga, pa je neophodna kontinuirana edukacija o bezbednosti u korišćenju digitalnih usluga.

Korisnici bankarskih usluga, a posebno milenijalci, ne žele da posluju sa bankom na način koji zahteva dolazak u ekspozituru, a mobilni telefon postaje najčešće korišćen kanal komunikacije sa bankom. Mobilni uređaji bezbednosno su ranjivi sami po sebi, a samim tim su ranjive i aplikacije i servisi koji omogućavaju digitalne usluge. Jedan od mehanizama zaštite je korišćenje multifaktorske autentifikacije. Potreban je mobilni telefon na kome je instalirana i aktivirana registrovana aplikacija, PIN za ulazak u mBanking aplikaciju i na kraju, prilikom samog plaćanja, OTP (One Time Password - lozinka za jednokatnu upotrebu) koju dobijamo putem SMS poruke na registrovani telefon. Na taj način se napadačima znatno otežava posao. Pored toga, komunikacija između

mobilnog uređaja i sistema koji obrađuje zahteve za transakcije ili neke druge zahteve je šifrovana SSL (Secure Socket Layer) protokolom koji onemogućava presretanje komunikacije i zloupotrebu podataka koji se koriste za prenos novca.

Pored svih tehnoloških zaštita, mnogo je jednostavnije prevariti čoveka nego sistem zaštitnih mera. Najčešće korišćeni metod je “phishing”, odnosno slanje lažne mejl ili SMS poruke sa linkom ka zlonamernoj lokaciji. Ako korisnik klikne na ponuđenu URL (Uniform Resource Locator) lokaciju, omogućava napadaču da preuzme podatke sa uređaja. Zato je izuzetno važno da kada dobijemo poruku sa nepoznate ili sumnjive adrese nikako ne kliknemo na ponuđene linkove.

Osnovna stvar koju bi korisnici trebalo da preduzmu je korišćenje snažne lozinke, koja sadrži veći broj karaktera i to ne samo alfa numeričkih već i specijalnih karaktera. Ne treba koristiti lično ime, kako svoje tako ni članova porodice. Korišćenje datuma rođenja se takođe ne savetuje. Postoje softverska rešenja koja omogućavaju „razbijanje“ lozinke te je važno poštovati pomenuta pravila kako bi se korisnici zaštitili. Držanje papirića sa PIN-om ili lozinkom uz sam telefon ili u novčaniku uz karticu je krajnje neoprezno jer se čak i klasičnim džeparošima omogućava jednostavno kompromitovanje kredencijala za izvršenje plaćanja.

Redovno ažuriranje softvera za zaštitu i poštovanje bezbednosnih pravila učiniće naše korišćenje digitalnih usluga bezbednim.

Povratak na sadržaj

KOMPANIJA VISA SAVETUJE

Osam koraka do bezbedne prodaje na internetu

Nedavno globalno istraživanje koje je Visa sprovela pokazuje da skoro polovina kompanija smatra da je primena tehnologija koje garantuju sigurnost najvažniji faktor uspeha poslovanja za 2021. godinu. Ipak, za mnoga mala i srednja preduzeća ovaj proces često iziskuje dodatne resurse kako personalne, tako i finansijske. U slučaju nedostatka internih stručnjaka, potrebno je obratiti se pouzdanim partnerima, čija ekspertiza može da doprinese unapređenju mehanizama za prevenciju zloupotreba

Kriza izazvana pandemijom uticala je i na povećan broj zloupotreba u onlajn svetu, te je sajber bezbednost postala veoma značajna tema za preduzeća širom sveta. Kompanije su od pojave virusa COVID-19 prijavile u proseku 4.000 sajber napada dnevno, što predstavlja rast od 400 odsto u odnosu na period pre pandemije.[1] Iz tog razloga, za preduzeća je važno da primene mere koje obezbeđuju otpornost njihovih poslovnih sistema na sve učestalije online pretnje.

Sa ciljem da doprinese sprečavanju sajber zloupotreba i pruži podršku prilikom prilagođavanja uslovima poslovanja u „novom normalnom“, kompanija Visa, svetski lider u digitalnim plaćanjima predstavlja niz bezbednosnih preporuka za mala i srednja preduzeća koja tek razvijaju internet prodavnice, kao i one sa postojećim onlajn šopovima.

1 **Snažne lozinke** - Napadači često koriste automatizovani softver za pogađanje i probijanje lozinki, te je važno da se kreira složena šifra, koja sadrži velika i mala slova, brojeve i posebne znakove. Takođe, preporuka je da se promene lozinke koje dolaze sa softverskim paketima.

2 **Ažuriranje softvera** - Sajber kriminalci obično pokušavaju da ukradu podatke sa veb stranica trgovaca kojima kupci veruju, te redovno ažuriranje instaliranih platformi i aplikacija pomaže sprečavanju napada. Određeni alati će sami poslati podsetnik da su na raspolaganju nove verzije, pa je važno aktivirati notifikacije.

3 **Zaštita stranice za prijavu** - Na stranicama za prijavu kupaca treba da se primenjuje *Secure Sockets Layer* sigurnosni protokol, koji omogućava bezbedan prenos osetljivih informacija poput broja platne kartice i drugih podataka za prijavu. Ovaj korak pruža dodatnu zaštitu potrošača.

4 **Rezervna kopija podataka** - Poželjno je kreiranje rezervnih datoteka koje će obezbediti nastavak poslovanja u slučaju da dođe do kvara ili zaključavanja sistema. Pojedini programi nude automatsko stvaranje rezervnih kopi-

1 Izvor: Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic. Prnewswire. Avgust 2020.

Povratak na sadržaj

ja, te daju dodatnu dozu sigurnosti korisnicima.

Redovna provera bezbednosti veb stranice je važna, kako na kvartalnom nivou, tako i nakon bilo kakvih promena. Ovaj proces omogućava da se prepoznaju sigurnosne ranjivosti sajta, kao i procena rizika, što je veoma značajno za pravovremeno reagovanje.

Pouzdan hosting provajder - Firme koje pružaju ovu uslugu mogu da kreiraju rezervne kopije podataka na udaljenim serverima, kao i da pruže efikasan sistem zaštite koji nadgleda dolazne podatke i sprečava neovlašćene upade.

Održavanje veb stranice - Neophodno je obrisati sve datoteke koje se više ne koriste. Svaka baza podataka ili aplikacija na veb stranici predstavlja dodatnu ranjivu tačku i moguću metu napada sajber kriminalaca. Preporuka je i da se datoteke organizuju na jednostavan način, koji omogućava efikasnije praćenje promena i brisanje starih fajlova.

Ulaganje u nove tehnologije koje unapređuju internet kupovinu, ali i obezbeđuju veću zaštitu potrošača je od izuzetne važnosti. Jedan od takvih programa je Visa Secure, koji uz pomoć EMV 3-D Secure standarda sprečava neautorizovane transakcije i štiti trgovce od zloupotreba prilikom online naplate. U cilju bolje analize rizika, tehnologija omogućava da trgovac i izdavalac razmenjuju i do deset puta više podataka.

Nedavno globalno istraživanje koje je Visa sprovela pokazuje da skoro polovina kompanija smatra da je primena tehnologija koje garantuju sigurnost najvažniji faktor uspeha poslovanja za 2021. godinu. Ipak, za mnoga mala i srednja preduzeća ovaj proces često iziskuje dodatne resurse kako personalne, tako i finansijske. U slučaju nedostatka internih stručnjaka, potrebno je obratiti se pouzdanim partnerima, čija ekspertiza može da doprinese unapređenju mehanizama za prevenciju zloupotreba.

Do tada, praćenjem navedenih preporuka, mala i srednja preduzeća mogu da zaštite svoje poslovne sisteme i potrošače i tako doprinesu naporima koje Visa u saradnji sa finansijskim institucijama ulaže u stvaranje sigurnog platnog okruženja.

Povratak na sadržaj

ALEKSANDAR MATANOVIĆ, OSNIVAČ I SUVLASNIK ECD, ONLAJN PLATFORME ZA PRODAJU I OTKUP KRIPTOVALUTA

Digitalni keš ili digitalno zlato?

Iako je bitkoin zamišljen kao digitalni keš, ljudi ga zapravo više doživljavaju kao digitalno zlato. Odnos između mogućeg dobitka i rizika kod kriptovaluta je, prema mom mišljenju, izuzetno dobar

Kriptovalute su postale pravi mamac za investitore, ali i obične ljude. Mnogi veruju da je reč o valuti budućnosti koja će zameniti tradicionalni novac. Aleksandar Matanović, osnivač i suvlasnik platforme ECD.rs za prodaju i otkup kriptovaluta, misli da su kriptovalute sledeći evolutivni korak u razvoju novca, ali da će to biti dugačak proces.

„Tako korenite promene su retke i moraju da traju. Verovatno su decenije u pitanju da bi se tranzicija do kraja završila. Naravno, to ne znači da se u nekim segmentima ili u nekim državama to neće desiti i ranije. Mislim da je to jednako neizbežno kao i proces zamene postojećih automobila električnim, ali isto kao i taj proces, traži strpljenje“, kaže Matanović koji je ECD platformu osnovao 2012. godine kada je u timu bilo troje ljudi – danas ih je u timu više od 20. Poznati su i po tome što razvijaju mrežu automata za kriptovalute po Srbiji.

Koliko su kriptovalute poznate u Srbiji i koje?

Prilično su poznate, mislim da bi do sada trebalo da su svi čuli za njih, mada ih većina nije koristila. Kriptovalute su u principu globalnog karaktera, tako da popularnost neke kriptovalute vrlo malo varira od države do države. To znači da su pojedinačne kriptovalute uglavnom ili popularne svuda ili nisu popularne nigde. Kao što je bitkoin na ubedljivom prvom mestu, tako je i ethereum na ubedljivom drugom. Sve ostale su daleko iza, kako u svetu tako i kod nas.

Po kom principu funkcionišu kriptovalute, može li se njima kupovati?

Iako je bitkoin zamišljen kao digitalni keš, ljudi ga zapravo više doživljavaju kao digitalno zlato. Više gledaju na to kao na investiciju nego kao ne sredstvo plaćanja. Slično je i sa većinom drugih kriptovaluta. To naravno ne znači da se njima ne može ništa kupiti. Naprotiv, kriptovalutama možete kupiti praktično sve što možete i tradicionalnim novcem, s tim da je izbor značajno manji jer većina trgovaca i dalje ne prihvata kriptovalute.

O kakvoj zapravo tehnologiji je reč?

Većina kriptovaluta je bazirana na blockchain tehnologiji, mada ima i drugačijih pristupa. Specifičnost blockchain tehnologije je što samim svojim dizajnom sprečava nekontrolisano umnožavanje digitalnog sadržaja, bez obzira na to da li je taj digitalni sadržaj novac ili bilo šta drugo. Na taj način mi uvek možemo biti sigurni koja tačno količina određene kriptovalute je u opticaju, možemo biti sigurni i da se ta kriptovaluta neće nekontrolisano doštampavati, a sve to bez potrebe za centralnim autoritetom koji bi kontrolisao ceo proces.

U kojoj meri su digitalne valute sigurna investicija? Šta su potencijalni rizici?

Ne postoji sigurna investicija. Svaka investicija nosi određenu dozu rizika. Digitalne valute svakako spadaju među rizičnije investicije, ali uz potencijal za neverovatno visoku zaradu. Odnos između mogućeg dobitka i rizika kod kriptovaluta je, prema mom mišljenju, izuzetno dobar. Osim rizika od pada vrednosti, koji je prisutan kod svake vrste investicije, postoji i rizik od gubitka digitalnih valuta, odnosno od gubitka pristupa digitalnom

Povratak na sadržaj

novčaniku na kojem se te digitalne valute nalaze.

Dešava se da vlasnici kriptovaluta izgube lozinku za pristup, pa njihov digitalni novac ostane zarobljen. Da li je na pomolu rešenje za takve situacije?

Potpuno rešenje verovatno nikad neće postojati, jer prosto nije realno očekivati da će se svi ljudi bez izuzetka pridržavati protokola za bezbedno čuvanje. Karakteristika kriptovaluta je da je sam vlasnik jedini odgovoran. Postoje alati i smernice koje omogućuju bezbednije čuvanje, ali ljudi prave propuste. S druge strane, postoje servisi koji za korisnike čuvaju kriptovalute. Kako vreme prolazi, oni su sve bezbedniji i sigurniji, ali ne mogu reći da su 100 odsto sigurni niti da će ikada biti. To je cena koju plaćamo za slobodu da imamo potpunu kontrolu nad svojim novcem.

Kako komentarišete tvrdnje da digitalne valute potpomažu kriminalcima širom sveta za „pranje novca“?

Iako se o tome dosta priča, postoji upadljivo malo konkretnih slučajeva gde je to zaista i dokazano. Verujem da je procenat transakcija u kriptovalutama povezanih sa ilegalnim aktivnostima manji nego procenat transakcija u dolarima (ili bilo kojoj drugoj tradicionalnoj valuti) povezanih sa ileganlnim aktivnostima. Te priče plasiraju uglavnom ili oni koji ne razumeju previše svet kriptovaluta ili oni koji imaju interes u tome da se kriptovalute što manje koriste.

Koliko se kriptovalute rudare u Srbiji?

Vrlo je teško proceniti, ali verujem da se radi o par desetina hiljada ljudi. Naravno, većina njih to radi više na nivou hobija nego ozbiljnog posla. Kod nas je struja prilično jeftina, pa je kod nas ru-

darenje oduvek popularno, imajući u vidu da je struja glavni trošak kod rudarenja.

Kakva su dalje predviđanja u pogledu kretanja cena kriptovaluta, pre svega, najpopularnijeg bitkoina, pa i ostalih?

Vrlo teško pitanje. Dugoročno sam optimista, ali ne bih se usudio da dam bilo kakve preciznije prognoze. Cena direktno zavisi isključivo od odnosa ponude i potražnje, mada na taj odnos utiče puno parametara čije pojavljivanje i uticaj često nije moguće predvideti, tako da indirektno na cenu utiče veoma veliki broj faktora. Slično kao i na tradicionalnim tržištima, na cenu mogu uticati razne vesti, glasine, manipulacije od strane „krupnih igrača“. Trgovanje na berzama je često vođeno emocijama, a ne samo razumom, tako da se cene na berzama (pa i na kripto berzama) često kreću na načine koje nije lako objasniti. Bitna specifičnost kripto berzi u odnosu na tradicionalne je što one rade 24/7. Nema odmora, pauze, vikenda, praznika i to je svakako jedan od razloga što su varijacije cena na kripto berzama često ekstremnije nego na tradicionalnim, jer ne postoji period kad trejderi mogu malo da zastanu i razmisle i onda je emotivna komponenta trgovanja izraženija, a upravo emotivna komponenta je ta koja dominantno utiče na volatilnost tržišta.

Da li neko može da nam „ukrade“ digitalne valute? I koje je zaštite najbolje koristiti?

Može, ako nismo pažljivi. Za početak, treba pažljivo izabrati gde i kako čuvati kriptovalute, izbor digitalnih novčanika je prilično veliki. Treba praviti kopije pri instalaciji novčanika i treba koristiti lozinke koje nisu jednostavne. Naravno, treba voditi računa i o tome da niko osim vas ili nekoga kome verujete nema pristup ni novčaniku ni kopiji. Ovde je specifično to što kada izgubite pristup novčaniku ne postoji niko ko može da vam pomogne da povratite pristup. Nije kao kod kartica, gde kada izgubite PIN, banka vam izda novi.

U kom smislu bi nedavno usvojeni Zakon o digutalnoj imovini mogao da unapredi tržište u Srbiji? Kakva mislite da će biti dalja regulacija u svetu?

Zakon predstavlja solidnu osnovu, ali će mnogo zavisiti od podzakonskih akata i same primene, tako da je rano reći u kojoj meri će zakon to tržište unaprediti. Lično sam optimista, ali ostaje da vidimo kako će se stvari odvijati.

U svetu je trend da se kriptovalute legitimizuju i tradicionalne finansijske institucije polako ulaze na to tržište. Postoje i države koje ne gledaju baš blagonaklono na kriptovalute, čak ih i zabranjuju. Međutim, bitno je napomenuti da među državama koje zabranjuju kriptovalute nema onih država koje važe za najrazvijenije.

Povratak na sadržaj

IVAN PAUNOVIĆ, RUKOVODILAC ZA BEZBEDNOST INFORMACIJA (CISO) MOBI BANKE

Naš prioritet je sigurnost svakog klijenta

Mobi Banka na prvo mesto stavlja sigurnost svakog individulnog klijenta u sistemu i na aplikacijama banke. Kako bi zaštitila podatke svojih klijenata, Mobi Banka koristi razne bezbednosne mehanizme na sistemskom, kao i na nivou aplikacija

Mobi Banka je nedavno proslavila šesti rođendan sa pola milionitim korisnikom, a sada već ima više od 550 hiljada korisnika. Razgovarali smo sa Ivanom Paunovićem, rukovodiocem za bezbednost informacija (CISO) Mobi banke o tome da li to što je Mobi banka potpuno digitalizovana olakšava ili otežava posao očuvanja bezbednosti klijenata i same banke, i na koji način brinu o sigurnosti svojih klijenata.

„Kao prva srpska i regionalna digitalna banka, izuzetno smo posvećeni očuvanju bezbednosti klijenata i same banke. Zalaganjem svih kolega u ovih šest godina nije bilo značajnih slučajeva zloupotrebe ličnih podataka. Tako da, rekao bih da nam digitalizacija olakšava posao, ali da digitalno okruženje svakako predstavlja izazov za svaku banku, kompaniju, instituciju.

U cilju zaštitite klijenata i njihovih sredstava, pratimo transakcije na osnovu indikatora neobičnog ponašanja koji bi ukazali na eventualnu zloupotrebu podataka. U slučaju sumnje u autentičnost neke transakcije, klijent se odmah kontaktira radi provere, i po potrebi blokiramo karticu, račun ili onlajn i mobilne kanale, čime pravovremeno sprečavamo zloupotrebe“, kaže Ivan Paunović.

Na koji način sve brinete o sigurnosti vaših klijenata, njihovih računa, transakcija? Imaju li uopšte klijenti razloga za brigu?

Mobi Banka na prvo mesto stavlja sigurnost svakog individulnog klijenta u sistemu i na aplikacijama banke. Kako bi zaštitila podatke svojih klijenata, Mobi Banka koristi razne bezbednosne mehanizme na sistemskom, kao i na nivou aplikacija. Dodatno, jedan od načina obezbeđenja sigurne onlajn trgovine i transakcija je dvojni faktor autentifikacije gde se transakcija potvrđuje kroz drugi kanal, obično SMS kod, koji stiže na registrovani broj telefona klijenta. Pored toga, tokom pandemije, Banka je pojačala monitoring onlajn transakcija kao i kreditnih zahteva.

Kako nekada i pojedinačni slučaj može da bude posledica većeg incidenta, trudimo se da svakom pojedinačnom slučaju

Povratak na sadržaj

pristupimo kao da se radi o većem incidentu. Do sada nismo imali slučajeva sa incidentima koji značajno ugrožavaju bezbednost. Ti slučajevi podrazumevaju hakerske upade u mrežu, kompromitaciju baze podataka ili korisnika sa povlašćenim pravima pristupa.

Da li imate obuke za zaposlene kako da prepoznaju fišing napade?

Mobi Banka je izuzetno posvećena bezbednosti svojih klijenata, te zato postoje i obuke za zaposlene i poseban tim koji vodim, a koji se bavi pitanjima informacione bezbednosti. Održavamo obuke zaposlenih po pitanjima informacione bezbednosti. Obuke se održavaju sa praktičnim primerima i uputstvima kako zaposleni treba da se ponašaju u slučaju povrede informacione bezbednosti. U

> U slučaju sumnje u autentičnost neke transakcije, klijent se odmah kontaktira radi provere, i po potrebi blokiramo karticu, račun ili onlajn i mobilne kanale, čime pravovremeno sprečavamo zloupotrebe

prošloj godini održan je veliki broj obuka, a neke od tema uključuju spam i phishing mejlove, ransomware, zaštitu podataka i sigurno pretraživanje sadržaja na Internetu.

Da li imate i uputstva za klijente s obzirom na to da sigurnost transakcija često zavisi i od njih samih?

Mobi Banka radi na prevenciji i edukaciji svojih klijenata. Kroz različite kanale, od sajta do sms poruka, redovno upozoravamo klijente na moguće prevare, kako da ih prepoznaju i izbegnu. Zatim, edukujemo korisnike o bezbednom korišćenju kartica, mobilne i onlajn aplikacije. Dodatno, klijentima omogućavamo da sami povećaju bezbednost svojih sredstava kroz napredne funkcionalnosti u samoj aplikaciji, kao što su blokada kartica, podešavanje željenih limita za isplatu, promena PIN-a i kredencijala, promena ličnih podataka i uređaja, kao i aktivacija svih raspoloživih notifikacija za sve tipove transakcija. Tako klijent ima potpunu kontrolu nad svojim računima i sredstvima.

Povratak na sadržaj

VIDEO-IDENTIFIKACIJA KLIJENATA

Izazovi u zaštiti podataka o ličnosti

Piše: Zlatko Petrović, pomoćnik Generalnog sekretara Službe Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti

Video-identifikacija, kao oblik utvrđivanja i provere identiteta klijenata, sve je prisutnija kako u našoj zemlji tako i širom sveta. Ovaj oblik komunikacije znatno olakšava i ubrzava poslovanje, ali nosi i određene rizike, posebno u oblasti zaštite podataka o ličnosti.

U Srbiji je mogućnost video-identifikacije uvedena Zakonom o sprečavanju pranja novca i finansiranja terorizma, kojim je propisano da obveznik takvu vrstu provere identiteta sprovodi uz pristanak lica čiji se identitet utvrđuje i proverava, kao i da je dužan da čuva video-zvučni zapis koji je nastao u toku tog postupka.

U skladu sa ovim ovlašćenjem iz istog Zakona, Narodna banka Srbije donela je Odluku o uslovima i načinu utvrđivanja i provere identiteta fizičkog lica korišćenjem sredstava elektronske komunikacije sa vrlo detaljnim upustvima.

Razmatranjem navedenog zakonskog rešenja, kao i Odluke NBS, inicira se niz pitanja koja se tiču zaštite podataka o ličnosti. Posebno je važna zakonska obaveza propisana Zakonom o zaštiti podataka o ličnosti da odredbe posebnih zakona kojima se uređuje obrada podataka o ličnosti moraju biti u skladu sa ovim zakonom. Rok za usklađivanje tih zakona sa ZZPL istekao je završetkom 2020. godine, a usklađivanje ovog, kao ni drugih zakona nije izvršeno.

Video-identifikacija nosi nove rizike

Utvrđivanje i provera identiteta lica na navedeni način predstavlja jednu od radnji i mera poznavanja i praćenja stranke, u svrhu sprečavanja pranja novca i finansiranja terorizma. Ovako regulisana obrada podataka o ličnosti, u skladu sa ZZPL, predstavlja obradu u posebne svrhe, koju mogu obavljati samo tzv. nadležni organi, i to: a) organi vlasti koji su nadležni za sprečavanje, istragu i otkrivanje krivičnih dela, kao i gonjenje učinilaca krivičnih dela ili izvršenje krivičnih sankcija, uključujući i zaštitu i sprečavanje pretnji javnoj i nacionalnoj bezbednosti; b) pravno lice koje je za obavljanje ovih poslova ovlašćeno zakonom.

Ovakvo zakonsko rešenje izaziva nedoumice, jer je bez razrade preuzeto iz Direktive EU 680/16 (tzv. Law Enforcement Directive), u postupku usklađivanja ZZPL sa evropskim propisima u ovoj oblasti (što je potvrdila i Evropska ko-

> Odluka NBS propisuje obavezu obveznika koji već poseduje određene podatke o stranci, da njegov zaposleni upoređuje te podatke s podacima koje je pribavio u toku postupka video-identifikacije

Povratak na sadržaj

misija u svojoj Studiji iz jula 2019. godine). Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti je još oktobra 2019. godine podneo inicijativu Ministarstvu pravde za pokretanje postupka za autentično tumačenje ove zakonske odredbe, po kojoj do danas nije odgovoreno.

Iz ovog razloga, obrada podataka obveznika Zakona o sprečavanju pranja novca i finansiranja terorizma (ZSPNFT), u svrhe ispunjavanja obaveza iz istog Zakona, spada u poseban režim obrade podataka o ličnosti. Takva obrada je zakonita samo ako je neophodna za obavljanje poslova nadležnih organa i ako je propisana zakonom, kojim se određuju najmanje ciljevi obrade, podaci o ličnosti koji se obrađuju i svrhe obrade. Ova okolnost proizvodi i niz drugih obaveza rukovalaca koji obrađuju podatke u posebne svrhe, u skladu sa ZZPL.

Video-identifikacija, te čuvanje video-zvučnih zapisa, predstavlja kvalitativno novu obradu podataka o ličnosti, koja, zbog upotrebe novih informacionih tehnologija, nosi nove rizike.

Neophodna izričita saglasnost stranke

Odlukom NBS uređuju se neophodni organizacioni, kadrovski i tehnički uslovi obrade, što jeste opšta obaveza rukovaoca po ZZPL i preduslov poštovanja načela „integriteta i poverljivosti“ podataka o ličnosti. Odluka propisuje da je obveznik „dužan da pre otpočinjanja postupka video-identifikacije pribavi izričitu saglasnost stranke na ceo postupak video-identifikacije, a naročito na snimanje slike i zvuka i čuvanje snimljenog materijala (video-zvučnog zapisa) u skladu sa zakonom“. Saglasnost mora biti snimljena, a zaposleni je dužan da stranku prethodno obavesti o obavezi pribavljanja saglasnosti i o tome da će se i davanje te saglasnosti video i zvučno snimati. Međutim, s obzirom na to da se video-identifikacija lica obavlja u posebne svrhe, potrebno je razmotriti pravnu prirodu ove saglasnosti. Pored činjenice da ZSPNFT ne poznaje saglasnost, već pristanak lica čiji se identitet utvrđuje, treba imati na umu da je u pitanju izvršavanje zakonske obaveze, te uslove zakonitosti obrade podataka u posebne svrhe, u skladu sa odredbama ZZPL.

U skladu sa Odlukom NBS, prilikom utvrđivanja identiteta stranke, zaposleni kroz razgovor sa strankom „procenjuje da li su odgovori stranke na postavljena pitanja ubedljivi, smisleni i dosledni“, što inicira pitanje primene člana 10. ZZPL, koji propisuje da je nadležni organ dužan da, u meri u kojoj je to moguće, podatke o ličnosti koji su zasnovani isključivo na činjeničnom stanju jasno izdvoji od podataka o ličnosti koji su zasnovani na ličnoj oceni.

> Uspostavljanje poslovnog odnosa koji uključuje video-identifikaciju dobijaće na značaju, ali izazovi su brojni i povlače rizike

Takođe, Odluka NBS propisuje obavezu obveznika koji već poseduje određene podatke o stranci, da njegov zaposleni upoređuje te podatke s podacima koje je pribavio u toku postupka video-identifikacije. U skladu sa Odlukom Poverenika o listi vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti procena uticaja na zaštitu podataka o ličnosti i tražiti mišljenje Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti, postoji obaveza rukovaoca da izradi ovaj dokument pre nego što započne sa obradom podataka o ličnosti ukrštanjem, povezivanjem ili proverom podudarnosti iz više izvora, što je ovde slučaj.

Odluka NBS propisuje da je obveznik u određenim slučajevima dužan da pribavi kopije službenih isprava, kao što je saobraćajna dozvola, rešenje o utvrđivanju poreza na imovinu, kao i računa za telefon ili komunalne usluge, što otvara pitanje normativnog uređenja ovakve obrade podataka, kao i mogućnosti obrade podataka o drugim licima, a što dalje inicira obaveze iz člana 24. ZZPL, koje se tiču transparentnosti obrade.

Nadalje, postavlja se pitanje bezbednosti softvera koji obveznici koriste za ove potrebe, kao i načina skladištenja podataka o ličnosti, zabeleženih u ovim video-zapisima, kako bi se očuvali integritet i poverljivost istih podataka.

Najzad, Odluka NBS poznaje i poveravanje poslova video-identifikacije trećem licu, koje na ovaj način postaje obrađivač podataka, što podrazumeva niz obaveza rukovaoca povodom izbora obrađivača, te uređivanja njihovog međusobnog odnosa.

Izvesno je da će obavljanje transakcija i uspostavljanje poslovnog odnosa, koje uključuje video-identifikaciju, sve više dobijati na značaju u budućnosti. Međutim, izazovi koje nosi ovakav vid obrade podataka o ličnosti bez sumnje su brojni i povlače rizike, koji se mogu ostvariti i dovesti do povrede podataka o ličnosti, ako se inicijalno ne sagledaju i ne preduzmu mere za upravljanje njima. Takođe, normativni aspekt ove delikatne obrade mora biti jasan i nedvosmislen, kako bi građani u punoj meri mogli da ostvare svoje pravo na zaštitu podataka o ličnosti.

Povratak na sadržaj

DANIEL ŠUŠNJAR, PREDSEDAVAJUĆI ODBORA ZA TELEKOMUNIKACIJE I DIGITALNU EKONOMIJU U SAVETU STRANIH INVESTITORA

Sajber bezbednost treba da bude deo poslovne kulture

Pitanje bezbednosti podataka posebno je važno u situaciji kada se u okviru lanca snadbevanja ili zbog organizacije poslovnih procesa određeni poslovni podaci čine dostupnim trećoj strani. Tada se već u procesu nabavke usluga postavljaju zahtevi u pogledu čuvanja podataka u skladu sa standardima u određenoj industriji

Kakvi su novi trendovi kad je reč o proceni velikih kompanija gde investirati – kolika je uloga stepena digitalizacije i sajber bezbednosti neke države, i na koji način strani investitori mogu da utiču na pozitivne promene u toj oblasti? O tome za naše čitaoce govori Daniel Šušnjar, predsedavajući Odbora za telekomunikacije i digitalnu ekonomiju u Savetu stranih investitora.

Da li strani investitori, pre nego što odluče šta će i koliko investirati u nekoj državi, procenjuju i stepen digitalizacije u toj državi, i kakav je opšti utisak o Srbiji u tom kontekstu?

Apsolutno. Baš kao što se procenjuju uslovi poslovanja u pogledu infrastrukture, autoputeva ili dostupnosti i kvalifikacije radne snage. Razmatra se stepen digitalizacije, počevši od nivoa razvijenosti telekomunikacionih usluga, digitalnih veština i nivoa digitalne „osvešćenosti" stanovništva, preko razvijenosti inovativnih platnih usluga i uopšte pratećeg digitalnog ekosistema, pa sve do fleksibilnosti regulatornog okvira i usluga elektronske uprave koje olakšavaju poslovanje.

Značaj pojedinih kategorija zavisi od toga da li je strani investitor u Srbiji izvozno orijentisan, ili su usluge i proizvodi prvenstveno namenjeni domaćem i regionalnom tržištu. U svakom slučaju, u Savetu stranih investitora prepoznali smo da pouzdana i pravno relevantna identifikacija u digitalnom okruženju predstavlja okosnicu daljeg procesa digitalizacije u Srbiji, zajedno sa inovativnim i digitalizovanim finansijskim uslugama. Smatramo da postoji veliki potencijal u međusektorskoj saradnji telekomunikacionih operatora, banaka i osiguranja, ali, isto tako, i u partnerstvu i činjenici da se privatni sektor oslanja na dostignuća i digitalna rešenja razvijena od strane države. Primećujemo da našu ambiciju dele i druga poslovna udruženja, pa je tako Privredna komora Srbije pokrenula Centar za digitalnu transformaciju sa preduzećima različite veličine i iz različitih sektora. Ovakve i slične inicijative su i više nego dobrodošle.

Istraživanja pokazuju da su i dalje u najvišoj meri digitalizovane kompanije čija je delatnost u osnovi tehnološka, dok tradicionalne industrije poput poljoprivrede, mašinske i metalske kasne u tom procesu. Logistika i turizam, na primer, takođe su pokazali sposobnost za brzo prilagođavanje digitalnoj ekonomiji.

Ipak pandemija virusa Covid19 širom sveta naterala je na brzu reorganizaciju i digitalnu transformaciju i one kompanije koje to nisu planirale. Došlo je do promene u načinu komunikacije sa korisnicima i slično, čime se ovaj proces dodatno ubrzao. Stoga smatramo da će one kompanije koje nisu iskoristile ovaj trenutak, imati problem u poslovanju i komunikaciji sa klijentima i nakon što pandemija prođe. Mi zaista verujemo da je digitalna transfor-

Povratak na sadržaj

macija opšta potreba i da to nije privilegija rezervisana samo za velike kompanije i sisteme.

Da li se prilikom odluke o investiranju ispituje i otpornost na sajber napade, i šta sve je tu uključeno?

Ispitivanje otpornosti na sajber napade podrazumeva nekoliko ključnih komponenti koje čine sajber bezbednost. U prvom redu, postavlja se pitanje postojanja adekvatnog regulatorno-pravnog okvira, kao i kapaciteta policije, tužilaštava i sudova da rade na suzbijanju i sankcionisanju visokotehnološkog kriminala. Sa druge strane, neophodno je da privatni sektor, zajedno sa civilnim društvom i akademskom zajednicom, uloži u stručnost i sticanje iskustva profesionalaca zaduženih za kontrolu i primenu tehničkih standarda u domenu korišćenja infrastrukture i pružanja digitalnih servisa, jer trenutno na tržištu rada postoji manjak kvalifikovanih stručnjaka iz oblasti informacione bezbednosti.

Sa manjim zakašnjenjem, Srbija uglavnom sledi regulativu Evropske unije u domenu sajber bezbednosti, a slično je i sa okvirom zaštite podataka o ličnosti. U prethodnom periodu napravljeni su značajni pomaci. U tom pravcu Usvojen je Zakon o informacionoj bezbednosti, kojim je uspostavljen bazični pravni okvir u ovoj oblasti kroz koji su implementirane odredbe Konvencije iz Budimpešte Saveta Evrope o borbi protiv sajber kriminala. U pogledu organizaciono-operativnih mehanizama, pri Ministarstvu unutrašnjih poslova uspostavljena je Služba za borbu protiv visokotehnološkog kriminala (VTK), zatim Posebno odeljenje Višeg javnog tužilaštva za borbu protiv VTK, dok je na nivou sudstva ustanovljena posebna nadležnost za VTK pri Višem sudu u Beogradu, odnosno posebno odeljenje Apelacionog suda u Beogradu kao drugostepena instanca. Takođe, pri Regulatornoj agenciji za elektronske komunikacije i poštanske usluge (RATEL) osnovan je i Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (CERT).

Naravno da je potrebno i u narednom periodu nastaviti rad na ovom polju, pa se tako očekuje operacionalizacija usvojenog Zakona o kritičnoj infrastrukturi kroz utvrđivanje kriterijuma za određivanje kritične infrastrukture u različitim oblastima, kao i preciziranje načina zaštite ove infrastrukture iz perspektive informacione bezbednosti.

Koliko strani investitori polažu na sajber bezbednost bankarskog sektora, platnog prometa u državi, snagu IT sektora, kvaliteta kompanija koje se bave sajber bezbednošću...?

Sigurnost i stabilnost bankarskog sektora i, uopšte, platnog prometa veoma je važna pri ukupnoj oceni uslova poslovanja u jednoj zemlji. S obzirom na to da dolazim iz telekomunikacionog sektora u kome je informa-

Povratak na sadržaj

ciona bezbednost na visokom nivou, ono što mogu da primetim je da je ista situacija i u bankarskom sektoru, i da je i ovaj aspekt njihovog poslovanja pod punom kontrolom Narodne banke Srbije kao regulatora u ovoj oblasti. Što se tiče kvaliteta domaćih kompanija koje pružaju usluge iz ove oblasti, to nije jedan od ključnih kriterijuma, imajući u vidu da su pretnje na nivou informacione bezbednosti po svojoj prirodi međunarodnog karaktera. Shodno tome i rešenja koja se primenjuju za zaštitu nisu nužno vezana za države, i često su centralizovana kod kompanija koje su deo multinacionalnih grupacija.

Da li strane kompanije proveravaju sajber bezbednost stejkholdera, a posebno preduzeća sa kojima sarađuju – jer su i oni potencijalni kanal kroz koji mogu procuriti podaci iz same kompanije?

Pitanje bezbednosti podataka posebno je važno u situaciji kada se u okviru lanca snadbevanja ili zbog organizacije poslovnih procesa određeni poslovni podaci čine dostupnim trećoj strani. Tada se već u procesu nabavke usluga postavljaju zahtevi u pogledu čuvanja podataka u skladu sa standardima u određenoj industriji, na primer, postavlja se pitanje postojanja sertifikata kakav je ISO 27001/27701, zaključuju se prateći ugovori o poverljivosti i slično. Ovo posebno dolazi do značaja prilikom poveravanja podataka o ličnosti. Tada se preduzimaju posebne mere koje proizlaze iz našeg Zakona o zaštiti podataka o ličnosti, koje između ostalog podrazumevaju zaključenje sporazuma o obradi podataka, tzv. DPA sporazuma, čime se na precizan način definišu prava i obaveze obe strane.

Kada strane kompanije dolaze u Srbiju, da li traže za sebe osiguranje od sajber rizika ukoliko dođe do prekida poslovanja, i kako te polise obezbeđuju s obzirom na to da je ponuda na domaćem tržištu izuzetno slaba (samo jedna kompanija nudi te polise)?

Sa razvojem tehnologija i digitalnih poslovnih modela raste i potreba za sajber odgovornošću i to ne samo u smislu učestalosti rizika već i u smislu pratećih troškova.

Postoje dve vrste šteta kod IT osiguranja od sajber odgovornosti: direktne štete koje nastaju kao posledica sajber rizika i odražavaju se na poslovanje kompanije, dok drugu vrstu čine štete koje nastaju prema trećim licima. U prvom slučaju, cilj je da se klijentima olakšaju potencijalno veoma visoki troškovi u slučajevima povrede sopstvenih podataka. Kod osiguranja od rizika štete prema trećim licima, cilj je da se kompanije zaštite od rizika visokih odštetnih zahteva svojih klijenata čiji su podaci narušeni.

Foreign Investors Council

Čini se da je ova vrsta osiguranja u razvoju i da će u budućnosti imati veći značaj nego što je to trenutno slučaj.

Da li se od domaćih ponuđača očekuje da imaju polisu osiguranja od sajber rizika, kao uslov da bi se prijavili na tender?

Po našim saznanjima, to još nije praksa na srpskom tržištu.

Savet stranih investitora pokrenuo je krajem prošle godine inicijativu za digitalizaciju finansijskih usluga u Srbiji, i s tim u vezi Vladi Srbije predložio niz mera koje bi trebalo primeniti u funkciji ubrzanja dalje digitalizacije usluga u finansijskom sektoru. Koje predložene mere biste istakli kao najznačajnije/najurgentnije, i dokle se stiglo sa njihovom realizacijom?

Nakon nekoliko veoma uspešnih regulatornih promena tokom 2018/19. godine čime su uvedeni novi digitalni finansijski proizvodi i usluge, a imajući u vidu da je digitalizacija danas apsolutni prioritet, posebno kao posledica pandemije COVID-19 i socijalnog distanciranja, Savet je u saradnji sa svojim članovima pripremio inicijativu radi pune digitalizacije finansijskih usluga. Inicijativa sadrži 23 različita predloga, od kojih neki imaju značaj visokog prioriteta, primera radi digitalizacija menice, digitalna razmena podataka između finansijskih institucija i državnih organa, identifikacija klijenata na daljinu i dr. Sa zadovoljstvom možemo da istaknemo izvanrednu saradnju sa svim državnim organima radi realizacije inicijative, razumevanje i spremnost za implementaciju predloga. Neki od prioritetnih predloga Saveta su već u planu realizacije od strane Vlade RS i Narodne banke Srbije poput digitalne menice, prihvatanje dokaza o elektronskim transakcijama od strane javnih institucia i drugo, te ih možemo očekivati u primeni u bliskoj budućnosti. Verujemo i da je velikom broju građana u interesu da što veći broj usluga može da obavlja “iz fotelje”, pa nas posebno raduje sve veća mogućnost identifikacije klijenata na daljinu, o čemu će verujemo uskoro biti više reči u javnosti.

Da li postoji namera da se ubrza i proces unapređenja sajber bezbednosti – ako postoji, kakve mere se mogu kao predlog očekivati od Saveta stranih investitora?

Povratak na sadržaj

Sajber bezbednost više ne može da se posmatra odvojeno od bezbednosti u realnom svetu. Šteta koja nastane kao rezultat sajber napada vrlo je realna i izaziva stvarne posledice i u fizičkom svetu. Ipak, zbog specifičnosti vezanih za tehnologiju, vrste, počinioce i žrtve ovakvih napada, pitanje sajber bezbednosti zahteva posebnu brigu svih koji se bave internetom.

Svedoci smo da ono što može da se upotrebi u korist društva, kao recimo tehnologija, može nažalost da se upotrebi i na njegovu štetu.

Kada pomenemo sajber bezbednost, obično pomislimo na neke krupnije stvari, kao što su skupi specijalizovani softveri. Često postoji nerazumevanje da povećanje budžeta za sajber bezbednost, ma koliko on bio velik, ne može da dovede do potpune sigurnosti kompanije od sajber napada, niti donosi brze rezultate.

Zato je bitno u vremenu pandemije, kada određene industrije beleže značajne gubitke, krenuti od rešenja koja ne zahtevaju velika ulaganja.

Kao što stručnjaci za bezbednost često ističu, ljudski faktor je jedan od najvećih sigurnosnih problema sa kojim se kompanije suočavaju. Stoga moramo da radimo na unapređenju sajber bezbednosti kroz edukaciju i podizanje svesti ljudi o pretnjama u sajber prostoru i merama prevencije, pogotovo prilikom rada od kuće, van kontrolisanog okruženja. Definisanje kompanijske politike u vezi sa radom od kuće u brojnim segmentima, kao što je politika upotrebe sopstvenih, privatnih, uređaja mobilnih telefona i laptopova, u odnosu na službene uređaje koji poseduju licencirani softver i antivirusne programe.

Svaka kompanija bi trebalo da razvija strategiju za zaštitu i oporavak podataka i sistema usled sajber napada. Prva 24 sata su ključna u sprečavanju gubitaka i zaštiti podataka i igraju ključnu ulogu u percepciji javnosti o brendu i njegovoj pouzdanosti. Zato je neophodno da kompanije uspostave timove za krizni menadžment i izrade planove za upravljanje kontinuitetom poslovanja i IT infrastrukturom u slučaju bezbednosnih incidenata, komunikacije, plan oporavka i reagovanje usled incidenata.

Sajber bezbednost u kompanijama ne treba da bude zadatak koji će se povremeno obavljati. Ona mora da bude utkana u poslovnu kulturu, a kompanije moraju da imaju strogo definisane politike.

Proaktivnost je ključni faktor, jer se ne sme čekati da se problem desi – tada je šteta već učinjena. Umesto toga, potrebno je učiniti sve da do nje ne dođe.

Lela Saković

Povratak na sadržaj

ŠTA POSLODAVCI U SRBIJI MOGU DA RADE SA PODACIMA ZAPOSLENIH

Smeju da nadziru, ali uz opravdanje

Svako uvođenje tehnologije koja automatski obrađuje podatke o ličnosti neophodno je da bude praćeno obaveštavanjem zaposlenih. Praćenje poslovne korespodencije dozvoljeno je uz valjan razlog

Za najviše 90 evra mesečno poslodavac može da otkrije skoro sve tajne zaposlenog. Špijunski softver ugrađen u službeni telefon snima razgovore preko mobinog telefona, ali i one obavljene nedaleko od njega. Prepiska je "otvorena knjiga", baš kao i fotografije. On može i više, pa ako zatreba, sam aktivira kameru da ovekoveči momente iz života i rada podređenog. Ovaj i slični "svevideći paketi" neke firme nude javno na sajtovima, pa čak i kroz biltene, uprkos tome što se u Srbiji od avgusta 2019. godine primenjuje Zakon o zaštiti podataka o ličnosti. A on kaže da za nadziranje zaposlenih mora da postoji opravdanje - u suprotnom, preti kazna do dva miliona dinara.

Većina zaposlenih, pa i poslodavaca često i ne zna u kojim situacijama otkrivaju, odnosno barataju tuđim ličnim podacima. Tu spadaju i spisak zaposlenih, datumi njihovog rođenja, brojevi tekućeg računa, ali i snimci kamere.

"Najčešće ne postoje uređeni mehanizmi zaštite relevantnih poslovnih podataka, pa nadziranje postaje invanzivno u strahu da će zaposleni zloupotrebiti te podatke", objašnava Mladen Raonić, čija firma Absolut support pomaže kompanijama da


Marijana Stojanović

se prilagode novoj regulativi. "Na primer, komercijalista tokom radnog vremena, pa čak i posle njega, deli svoje lične podatke sa poslodavcem, a suštinski za sve obrade ne postoji legitimni interes ili nema drugog osnova za obradu. Na posao dolazi službenim vozilom sa GPS sistemom. Prijavljuje se na sistem za kontrolu radnog vremena, kancelarija je pod video nadzorom i termo kamerom. I dok obilazi teren, njegovo vozilo se prati".

> Zaposleni, međutim, moraju da budu svesni da mnoge njihove aktivnosti nadređeni prate sa punim pravom

Postavlja se pitanje da li je zaista neophodno profilisanje recimo komercijaliste u ovom obimu, ako se imaju u vidu njegova zaduženja poverena ugovorom. Pravu meru trebalo bi da odredi osoba zadužena za zaštitu podataka o ličnosti.

"Ta funkcija i dalje ide ispod radara i nije prepoznata, i često se formalno dodeljuje zaposlenima koji i ne znaju šta je njihov zadatak", dodaje Raonić. "Špijunski softveri prate aktivnost ekrana, brzinu otkucaja na tastaturi, nadgledaju preko web kamere ili prate zvuk preko mikrofona. Poslodavci su često slobodni da ih instaliraju, ali to se ne može smatrati legitimnim nadzorom zaposlenih. Kazne mogu biti i do dva miliona dinara".

Ograničeno čuvanje podataka

Zakon o zaštiti podataka o ličnosti je preuzeo načela obrade iz evropske direktive – GDPR, a jedno od njih je i ono koje ograničava čuvanje.

Povratak na sadržaj

"Prema ovom načelu podaci se mogu čuvati u obliku koji omogućava identifikaciju lica samo u roku koji je neophodan za ostvarivanje svrhe obrade", ističe advokat Tijana Žunić Marić. "Drugim rečima, ako ne postoji svrha obrade, ne postoji osnov da se podaci čuvaju - oni se moraju brisati. Iz ovog načela dalje proističe da svaki rukovalac podacima o ličnosti mora da utvrdi pravila po kojima će utvrditi rokove za čuvanje svake vrste podataka koju obrađuje, a zatim i procedure za brisanje nakon proteka tog vremena. U praksi se to najčešće vrši posebnim Pravilnikom o čuvanju i brisanju podataka o ličnosti".

Taj dokument bi trebalo, između ostalog, da sadrži vrstu ličnih podataka, svrhu obrade, zakonski osnov za obradu, kategoriju lica na koja se podaci odnose, način vođenja evidencije internih zbirki, fizičke i tehnološke mere zaštite podataka... Ko obrađuje podatke suprotno bilo kom od ovih načela, rizikuje kaznu u rasponu do 50.000 do dva miliona dinara.

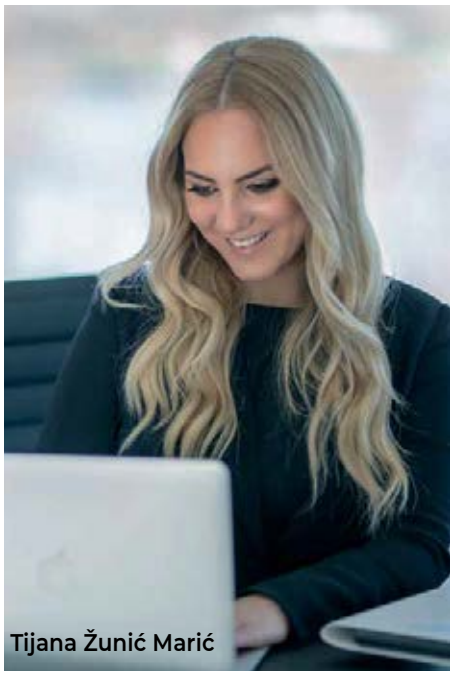

Mladen Raonić

Kompanijska pošta

Zaposleni, međutim, moraju da budu svesni da mnoge njihove aktivnosti nadređeni prate sa punim pravom. Preciznije rečeno, sa pravom koje im zakon pruža. E-mail korespodencija zaposlenog na službenom računaru i preko službene elektronske pošte ne smatra se privatnom.

"Poslodavac ima slobodu da takvu korespodenciju nadzire, ako postoji validan poslovni razlog ", ističe Raonić. "U tom slučaju trebalo bi da obavesti zaposlene kako bi se ispunilo načelo transparentnosti, shodno Zakonu o zaštiti podataka o ličnosti. Snimanje razgovora sa klijentima, bez adekvatnog poslovnog razloga i bez prethodnog obaveštenja, ne može biti validno niti legitimno. GPS u službenim vozilima je dozvoljen, ali pod uslovom da je kao sistem tehničke zaštite uveden

Povratak na sadržaj


Tijana Žunić Marić

kroz prethodnu procenu rizika i plan obezbeđenja. I da je nakon toga zaposleni obavešten o toj činjenici. Svako uvođenje tehnologije koja obavlja automatizovanu obradu podataka o ličnosti neophodno je da bude praćeno obaveštavanjem zaposlenih."

Kandidat bi već prilikom prijave za posao trebalo da zna koje podatke o ličnosti poslodavac koristi i u koje svrhe, koliko dugo ih čuva, da li ih daje na obradu nekom drugom. Ima pravo da bude obavešten o svakoj promeni, kao i da menja svoje podatke, pa i da ih briše. Ukoliko veruje da je poslodavac prekoračio ovlašćenja, može da prijavi povredu podataka povereniku, a ako je nastupila šteta, može da pokrene sudski postupak i - traži odštetu. Da do toga ne dođe, u mnogim kompanijama brinu i odeljenja za ljudske resurse.

"Da bismo nekoga zaposlili, prvi podaci nam stižu kroz radnu biografiju. Ona uglavnom sadrži datum rođenja, broj telefona, adresu", ističe Marijana Stojanović, HR menadžer u firmi Worldwide Clinical Trails. "Prilikom samog zapošljavanja očitavamo lične karte i uzimamo podatke potrebne za izradu ugovora o radu, dobijamo bankovni račun zbog isplate zarade, dobijamo podatke i od članova porodice zbog osiguranja. Bitno je da te podatke koristimo samo u svrhe zbog kojih je neophodno i da ih tretiramo sa pažnjom i opreznošću. HR profesionalci odavno su utrenirani kako da vode računa o ličnim podacima. Ukoliko su u tabelama, praksa je da su te tabele zaključane šifrom. Ukoliko su u softveru, onda treba da se tačno zna ko ima pristup. Tada svako ima svoju šifru i ona se periodično menja."

Šef zna i za "sudar"

U kompanijama u kojima nije bio problem prilagoditi se zahtevnijim pravilima zaštite ličnosti, zaposleni redovno prolaze obuke.

"Jednom godišnje svaki zaposleni mora da prođe trening da se podseti pravila", objašnjava Marijana Stojanović. "Uči se i kako da prepoznaju pokušaj izvlačenja nekih podataka, takozvano pecanje. Ako stigne mejl navodno od IT administratora, mora pažljivo da se vidi da li je adresa sa koje je poslat uopšte kompanijska. Ako u obraćanju u tom mejlu nije napisano naše ime, nego "dragi kolega", potrebno je da proverimo ko je zaista poslao mejl."

> Snimanje razgovora sa klijentima, bez adekvatnog poslovnog razloga i bez prethodnog obaveštenja, ne može biti validno niti legitimno

Kompanije, s jedne strane, obaveštavaju svoje kolege zašto im uzimaju lične podatke i kako ih koriste. Traže im saglasnost svaki put kada se koriste u nekoj novoj situaciji. S druge strane, radnici često sami svoje privatne stvari, uglavnom iz neznanja, čine prilično javnim.

"Često zaposleni koriste službene računare i mobilne telefone u private svrhe", ističe Marijana Stojanović. "Instaliraju razne aplikacije, Facebook, Instagram, Tinder - koji sadrže lične informacije, a zaposleni zaboravljaju da su službeni računari i mobilni telefoni vlasništvo kompanije. U većini kompanija se redovno pohranjuju svi podaci na kompanijske servere i svi ti zapisi ostaju negde u bazama podataka u vlasništvu kompanija. Da ne pričam o privatnim fotografijama i dokumentima. Mora da postoji obostana informisanost, opreznost i svest o tome kako štitimo lične podatke.

A. Duždević

Mapa puta

Usklađivanje sa Zakonom o zaštiti podataka o ličnosti podrazumeva nekoliko procedura. Najpre se mapira proces prikupljanja podataka i radi GAP analiza trenutnog stanja. Sledi edukacija zaposlenih, srednjeg i višeg menadžmenta i kreće se u izradu evidencija, minimizacije podataka, procene uticaja za pojedinačne obrade za koje postoji indicija da mogu ugroziti privatnost zaposlenih, klijenata, posetilaca.

"Nakon toga se radi politika privatnosti, ugovaraju obaveze obrađivača kojima rukovalac poverava podatke o ličnosti i definišu procedure koje opisuju organizaciono - tehničke mere u cilju zaštite podataka", kaže Mladen Raonić. "Na kraju ostaje revizija kompletnog postupka, kontrola sprovođenja mera i uvođenje funkcije DPO – osobe zadužene za zaštitu podataka o ličnosti".

Povratak na sadržaj

Alterna
Partner for Achieving Goals

3 KORAKA DO EFIKASNIJIH OSTVARENJA **VAŠIH CILJEVA**

1. **Slušamo Vas**
   Zajedno definišemo unapređenja koja je potrebno postići. Zatim osmišljavamo pristup i strukturu obuke za Vaše timove i pojedince.

2. **Realizujemo program**
   U koordinaciji sa Vama, realizujemo program obuke u Vašoj kompaniji ili u prostorijama trening centra Alterna International.

3. **Pomažemo u implementaciji**
   Dajemo praktične metode kako da naučene veštine implementirate u procese rada i dostizanje željenih rezultata.

U SARADNJI SA KOMPANIJOM ALTERNA INTERNATIONAL **DOBIJATE:**

- Grupne i individualne trening i koučing programe koji su prilagođeni Vašim potrebama, strategiji i viziji.
- Praktično i primenljivo iskustvo koje je dokazano u praksi.
- Dugoročno poboljšanje stavova, veština i znanja koji donose vrhunski rezultat.

Alterna International je Master Partner kompanija
Brian Tracy Global, Focal Point Coaching i Structogram Training System

BRIAN TRACY GLOBAL
Professional Development | Executive Training
Achieving Personal and Business Goals Faster

STRUCTOGRAM®

FocalPoint
powered by Brian Tracy Global
Coaching & Training Excellence

Za sve dodatne informacije kontaktirajte nas na:
info@alternainternational.net | www.alternainternational.net
+381 11 4281 402 | + 381 62 278 187

Foto: Filmbeat

POZNATI NA UDARU SAJBER KRIMINALACA

I bogati plaču?

Dok jedni postaju bogati i poznati na legalan način, oni koji znaju kako da se obogate na njihov račun i sami imaju potrebu da se "pokažu" na društvenim mrežama, kačeći svoje fotografije sa desetinama roleksa na jednoj ruci, na luksuznim jahtama ili sa iguanom – svojim "kućnim ljubimcem"

Biti poznat – mnogima zvuči prilično izazovno i lagodno. Neki su zahvalni životu što ih je "zadesio" baš u vreme društvenih mreža, koje pružaju mogućnost za dodatno podizanje popularnosti.

Međutim, takav status donosi i dodatne rizike – što zbog novca kojim obično raspolažu, što zbog velikog broja pratilaca, i oni su često meta napada raznih internet kriminalnih grupa, ili sposobnih pojedinaca.

Krađu identiteta preko društvenih mreža doživeo je svojevremeno i sam Mark Cukerberg, vlasnik Fejsbuka – doduše, ne preko sopstvene mreže: hakovani su njegovi nalozi na Tviteru i na Pinterestu. I baš kao što rade teroristi, i ovi kriminalci su želeli da podignu svoju popularnost tako što će objaviti svoj "podvig": grupa "OurMine" priznala je da je počinilac ovog napada. Sa Cukerbergovog Tviter naloga sami su "tvitnuli" poruku: "Hej, Mark, imamo pristup tvom Tviteru, Instagramu i Pinterestu, samo testiramo tvoju sigurnost", a napisali su čak i njegovu lozinku do koje su došli... I kao šlag na torti – promenili su i ime njegovog Pinterest naloga u "Hacked by OurMine Team"!

Više desetina poznatih ličnosti bilo je ugroženo kada su hakeri napali Sony Pictures Entertainment, zbog satiričnog filma "Intervju" na račun severnokorejskog vođe Kim Džong Una. U novembru 2014. hakeri su ukrali lične podatke – adrese i telefone svih zaposlenih u ovoj kompaniji, ali i podatke iz brojnih ugovora i sadržaj elektronske pošte.

Pogođeni su bili i brojni glumci: primera radi, procurila je vest da je Set Rožers koji je glumio u tom filmu zaradio 8,4 miliona dolara, a Džejms Franko 6,5 miliona dolara.

Otkrivena su i imena koja poznate ličnosti koriste za zaštitu svoje privatnosti: Tom Henks se predstavlja kao Hari Loder ili Džoni Madrid, Džesika Alba se predstavlja kao Keš Mani, a Danijel Kreg kao Olven Vilijams.

U javnost su istovremeno izašli i brojevi socijalnog osiguranja više od 47.000 ljudi, među kojima i glumca Silvestra Stalonea i drugih javnih ličnosti.

Na svom Instagramu napad je doživela i glumica Selena Gomez, kada su na njenom nalogu sa oko 25 miliona pratilaca objavljene njene provokativne fotografije koje je svojevremeno napravio njen bivši dečko Džastin Biber.

Žrtve sajber incidenata bili su i Ema Votson, Leonardo Di Kaprio, Viktorija Bekam, Bijonse, Tejlor Svift...

I dok jedni postaju bogati i poznati na legalan način, oni koji znaju kako da se obogate na njihov račun i sami (bar neki od njih) imaju potrebu da se "pokažu" na društvenim mrežama, kačeći svoje fotografije sa desetinama roleksa na jednoj ruci, na luksuznim jahtama ili sa iguanom – svojim "kućnim ljubimcem". Neki od njih, poput pripadnika čuvene sajber kriminalne grupe EvilCorp postali su skoro pa internet zvezde zahvaljujući snimcima na kojima voze lambordžini ofarban kamuflažnim bojama.

Povratak na sadržaj

BE
RISK
PROTECTED.

Inicijativa za jačanje bezbednosti podataka

Inicijativu za jačanje bezbednosti podataka pod sloganom „Be Risk Protected“, pokrenuli su portali Sve o osiguranju i Sve o novcu kako bi – kroz aktivno promovisanje preventive i finansijske zaštite u široj poslovnoj javnosti - doprineli bezbednijem poslovanju u savremenom digitalnom okruženju.

Inicijativa za jačanje bezbednosti podataka okuplja institucije, kompanije, organizacije i nezavisne stručnjake koji svojim delovanjem mogu i žele da doprinesu ostalim preduzećima i široj zajednici da se lakše snađu u uslovima ubrzane digitalizacije i rizika koje digitalno poslovanje donosi.

Ako se bavite
- digitalizacijom
- IT servisima
- sajber bezbednošću
- finansijama (banke, osiguranja)
- oblastima Data Science, ML, Artificial Intelligence
- ili upravljanjem podacima

PRIKLJUČITE NAM SE.

Uključivanjem u Inicijativu za jačanje bezbednosti podataka, postaćete deo aktivne i napredne grupe poslovnih ljudi/preduzeća koja želi da doprinese bezbednijem društvu i poslovanju u doba digitalne transformacije.

Kroz razne aktivnosti – od izdavanja publikacija i digitalnih informatora, preko networking skupova i konferencija, do video i audio materijala – namera nam je da skrenemo pažnju poslovne javnosti na:
- *rizike po podatke* i poslovanje koje nosi digitalno doba
- načine *preventive*
- mogućnosti *nadoknade štete* ukoliko se ona dogodi.

Želimo da doprinesemo da poslovno okruženje u Srbiji bude prepoznato na svetskoj mapi rizika kao jedno od bezbednijih za ulaganje i poslovanje, kad je reč o čuvanju podataka.
A Vi?

www.beriskprotected.rs
office@beriskprotected.rs

GENERALI

OSIGURAJ I ODVEZI

Čeka vas preko 600 nagrada!

Od 10.02 do 11.05.

I nagrada
BMW 520D

II nagrada
GOLF TRENDLINE

III nagrada
MEGAN INTENS

Kontakt centar
011 222 0 555
0800 222 555

kontakt@generali.rs
generali.rs

Nagradna igra "Generali nagraduje".
Registracija traje od 29.3. do 11.5. 2021.