BE
RISK
PROTECTED.

PODACI O LIČNOSTI.
SAJBER RIZICI.
OSIGURANJE.

SADRŽAJ

Fotografije: Unsplash i Pixabay
Izdavač: **BeRiskProtected**

DA LI NOVE TEHNOLOGIJE ŽELE NOVE NAS?!

Kad bi pre svega pedesetak godina sin krenuo recimo u Ameriku, roditelji su mogli samo da ostanu kod kuće da plaču jer ne znaju da li će ga za života još videti, i da čekaju poštara sa pismom napisanim i po nekoliko nedelja pre nego što stigne. Danas možemo sa njima da razgovaramo i da se gledamo u realnom vremenu, a nije isključeno da ćemo uskoro preko ekrana moći da osetimo i miris njihove kose.
Doprinos tehnologije medicini je neverovatan: od toga da najbolji lekari sa druge strane planete mogu da asistiraju tokom operacije preko video poziva, do toga da uz pomoć veštačke inteligencije mogu da hodaju oni koji su o tome samo sanjali.
I svakodnevni život nam je znatno olakšan: kad krenemo na put ne moramo više da razvlačimo mape jer nas aplikacija vodi do odredišta, a pametni frižideri u stanu sami naručuju ono što je potrošeno...
S druge strane, priča o mentalnom zdravlju nikad nije bila aktuelnija, a jedna od novih bolesti zavisnosti jeste i zavisnost

od interneta i društvenih mreža. U svetu je sve više sanatorijuma za odvikavanje od ovoga, a neke studije pokazuju da je razvoj tehnologije učinio život užurbanijim, a da ljudska priroda nije uspela da uhvati korak sa novonametnutim tempom, i da upravo to izaziva sve veću anksioznost i povećanu potrošnju lekova za smirenje.

Iako u prvi mah sjajno zvuči to što stvari rade umesto nas, to povlači određene negativne promene po ljudski organizam. Sve manja potreba za kretanjem može dovesti do smanjenja funkcije mišića i promene građe, a sve manje angažovanje mozga – do slabljenja nekih njegovih funkcija. Neki će reći, istina, ali zato se razvijaju neke druge sposobnosti... Gde je tu ravnoteža, pokazaće iskustvo.

Ali, na toj "vagi" dobrih i manje dobrih strana razvoja tehnologije, rizici ozbiljno drže "jezičak". Na brojnim svetskim top listama najvećih rizika sadašnjosti i budućnosti, sajber rizici su već treću godinu uzastopno na prvoj poziciji. Privrednici najviše brinu o materijalnim, i reputacionim rizicima – što se opet svodi na materijalne.

Pojedinci se time manje bave. Često će reći "a šta ja imam s tim – nisam ni bogat ni slavan?!" ali to kradljivcima podataka nije najvažnije. Čak naprotiv! Krađa identiteta je ono što im je od nas najzanimljivije: onaj ko nam ukrade identitet, može u naše ime i da pljačka, i da otvara firme, i da obmanjuje druge ljude i čini razna krivična dela. Umesto njega, u zatvor možemo otići mi... i tek tada shvatiti da gubitak novca nije najstrašnije što može da nam se desi.

Zato bi trebalo da budemo svesni rizika, i da korišćenju novih tehnologija i gedžeta pristupamo sa oprezom. Naravno, ne da ih se odreknemo - jer danas nije lako, a uskoro neće biti ni moguće živeti kao pre pedesetak godina. Stvar je u tome da se dobro raspitamo, najpre šta sve u kući od sprava koje imamo, prikuplja naše podatke, a zatim da naučimo šta i na koji način da delimo, i da čuvamo.

Nove tehnologije očigledno donose novu epohu, a oni koji su dobro pripremljeni – imaju najviše šanse da opstanu.

« POVRATAK NA SADRŽAJ

ŠTA SU SVE PODACI O LIČNOSTI

Piše:
Dragan Milić
Milić Law Office

Jedan od najvažnijih zadataka u sklopu podizanja nivoa svesti o zaštiti podataka o ličnosti kod građana predstavlja razumevanje pojma "podatak o ličnosti" odnosno mogućnost identifikovanja određene informacije kao podatka o ličnosti. To je potrebno kako bi fizička lica mogla dalje da ostvaruju svoja prava, a rukovaoci i obrađivači da tretiraju takve podatke na adekvatan i zakonom propisan način.

Pored očiglednih podataka o ličnosti, poput imena i prezimena, matičnog broja, broja ličnog identifikacionog dokumenta, često se zanemaruju podaci koji na prvi pogled ne vode direktno do identiteta fizičkog lica, ali su svakako vezani za ličnost, pa samim tim i potpadaju pod kategoriju – podaci o ličnosti.

Zakon o zaštiti podataka o ličnosti (ZZPL) propisuje da je podatak o ličnosti *svaki podatak koji se odnosi na fizičko lice* čiji *je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta kao* što *je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta.*

Praktično, i mnogi drugi podaci koji posredno vode do identiteta ili čine identitet nekog fizičkog lica, takođe predstavljaju podatke o ličnosti.

IP adresa, istorija pretrage na pretraživačima, lokacija mobilnog telefona, ali i visina zarade, datum korišćenja godišnjeg odmora - sve su to podaci koji su vezani za nečiju ličnost i kao takvi imaju ZZPL-om obezbeđenu zaštitu.

Uz takve "indirektne" podatke treba pomenuti tzv. *meta podatke* - "podatke o podacima" koji mogu mnogo reći o licu na koje se odnose i u velikoj meri kompromitovati nečiji identitet i privatnost. Meta podatke ZZPL ne razdvaja posebno od standardnih kategorija podataka, ali zavisno od svrhe i načina obrade oni u praksi mogu imati specifičan tretman, posebno ako se koriste za neku vrstu automatske obrade u cilju profilisanja. Licu na koje se meta podaci odnose mora unapred biti predočeno da se takvi podaci obrađuju, sa popisom svih metapodataka, opisom svrhe, vremena čuvanja, kao i drugih važnih činjenica vezanih za obradu u skladu sa ZZPL-om.

U okviru podataka o ličnosti, ZZPL izdvaja i tzv. *posebne kategorije*, tj podatke koji su u pogledu rizika koji nosi njihova obrada, osetljiviji za pojedinca od običnih odnosno standardnih podataka o ličnosti.

U posebne kategorije potpadaju podaci o zdravlju, političkoj i verskoj pripadnosti, seksualnoj orijentaciji itd.

ZZPL obradu ovakvih podataka posebno reguliše i propisuje taksativno propisane uslove za njihovu obradu, kada se posebno mora voditi računa o njihovoj bezbednosti.

Šta je obrada podataka o ličnosti?

Obrada se često poistovećuje sa korišćenjem ili prikupljanjem podataka. Obrada, međutim, pokriva mnogo veći broj aktivnosti u vezi sa podacima poput beleženja, razvrstavanja, grupisanja, strukturisanja, pohranjivanja, upodobljavanja ili menjanja, otkrivanja, uvida, upotrebe, otkrivanja prenosom odnosno dostavljanjem, umnožavanja, širenja ili na drugi način činjenja dostupnim, upoređivanja, ograničavanja, brisanja ili uništavanja, sve to - bilo automatski ili neautomatizovano.

Pristanak kao osnov obrade podataka

Iako ZZPL propisuje šest različitih pravnih osnova na koje se možete osloniti prilikom obrade, pristanak predstavlja jedan od najčešće pominjanih u praksi. Često, kada se pravo na obradu ne može pronaći u ZZPL-u ili se može vezati za izvršenje neke ugovorne obaveze itd, pristanak predstavlja najlogičnije pravno sredstvo čijim ispunjenjem se može zakonito pristupiti obradi.

Među osnovnim karakteristikama pristanka su njegova dobrovoljnost, nedvosmislenost i informisanost.

Pristanak ne sme biti plod bilo kakve prinude, ili odnosa subordinacije. Ne sme biti ni skriven, kako fizički npr. u sklopu nekog dužeg teksta, ali ni ostavljen da bude predmet tumačenja da li se radi o pristanku ili ne. Pristanak takođe kao takav mora biti naslovljen, sa precizno opisanim podacima koji se obrađuju, svrhom, poukom o pravu na opoziv itd.

Lica na koja se podaci odnose moraju biti svesna i prava na opoziv i o tome moraju biti adekvatno unapred poučena. Povlačenje pristanka ima dejstvo samo ubuduće, a obrada sprovedena do trenutka povlačenja ostaje zakonita.

Dejstvo date saglasnosti je vezano isključivo za svrhu za koju je i data. Samim tim se podaci ne mogu obrađivati u druge svrhe, a za svaju drugi nameravani cilj obrade mora se pribaviti nov pristanak.

Pored prava na opoziv pristanka, licu na koje se podaci odnose stoji na raspolaganju niz drugih prava, među kojima su pravo na informisanost, pravo na pristup, na kopiju itd. Ukoliko želite da budete sigurni da li je neka obrada obustavljena po vašem zahtevu ili da li su podaci obrisani nakon ispunjenja svrhe u koju su prikupljeni odnosno nakon isteka vremena koje je označeno za njihovo čuvanje, to možete proveriti kroz ostvarivanje nekog drugog prava koje vam ZZPL garantuje.

« POVRATAK NA SADRŽAJ

OBAVEZE KOMPANIJA U POGLEDU ZAKONA O ZAŠTITI PODATAKA O LIČNOSTI

Piše:
Jelena Todorović
advokat
TSG Law Office

U eri savremenog digitalnog doba, dostupnosti informacija i brzine življenja, zaštita podataka o ličnosti postaje trend i goruća tema kojoj sve više kompanija opravdano posvećuje veliku pažnju. Rizici nepoštovanja zaštite podataka ne ogledaju se samo u kaznenom smislu, već i u reputacionom, a to u današnje vreme nema cenu.
U duhu evropskih integracija i koraka sa modernim pravnim svetom, Republika Srbija je svoj pravni okvir na ovu temu uredila donošenjem Zakona o zaštiti podataka o ličnosti 2018. godine (dalje: **ZZPL**). ZZPL je donet pod snažnim uticajem Opšte uredbe o zaštiti podataka o ličnosti Evropske Unije (dalje: **GDPR**) i u njemu se ogledaju skoro svi principi, vrednosti, načela i obaveze GDPR-a.

Primena Zakona o zaštiti podataka o ličnosti
Cilj ZZPL-a je zaštita osnovnih prava i sloboda fizičkih lica, a posebno njihovog prava na zaštitu podataka o ličnosti.

ZZPL se primenjuje na obradu podataka o ličnosti koju obavljaju rukovaoci i obrađivači koji imaju sedište, prebivalište ili boravište na teritoriji Republike Srbije, u okviru svojih aktivnosti. U određenim slučajevima primenjuje se i na rukovaoce i obrađivače koji nemaju sedište, prebivalište ili boravište na našoj teritoriji, ukoliko su radnje obrade vezane za:
1) ponudu robe ili usluga licu na koje se podaci odnose na teritoriji Republike Srbije,
2) praćenje aktivnosti lica na koje se podaci odnose, ako se aktivnosti obavljaju na teritoriji Republike Srbije.

Gotovo da ne postoji kompanija koja ne dolazi u posed i ne obrađuje podatke o ličnosti: ako ne dolazi u posed tih podataka u okviru svoje delatnosti, sasvim sigurno obrađuje lične podatke svojih zaposlenih u različite svrhe.

Mere zaštite
Kompanije su u obavezi da primenjuju odgovarajuće tehničke, organizacione i kadrovske mere kako bi se obezbedila obrada u skladu sa ZZPL-om. Te mere između ostalog obuhvataju pseudonimizaciju i kriptozaštitu podataka, kao i sposobnost obezbeđivanja trajne poverljivosti, integriteta, raspoloživosti i otpornosti sistema i usluga obrade. Ipak, tehničke, organizacione i kadrovske mere ZZPL nije jasno definisao, čime je kompanijama jasno stavljeno do znanja da ih je potrebno redovno preispitivati i ažurirati, imajući u vidu konstantan razvoj digitalizacije, informacionih sistema i tehnologija.
Primenom ovih mera, kompanije su dužne da konstantno obezbeđuju odgovarajuću zaštitu što uključuje i zaštitu od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja podataka o ličnosti.

Povreda podataka o ličnosti

ZZPL definiše povredu podataka o ličnosti kao povredu bezbednosti podataka koja dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima o ličnosti koji su preneseni, pohranjeni ili na drugi način obrađivani.

Posledice povrede podataka o ličnosti su brojne, i ocenjuju se prema potencijalnom riziku po prava i slobode fizičkih lica. U zavisnosti od vrste podataka, povrede mogu uzrokovati materijalnu ili nematerijalnu štetu, povredu ugleda ili krađu identiteta, a posebno ukoliko se radi o naročito osetljivim podacima o ličnosti kao što su npr. rasno ili etničko poreklo, obrada genetskih i biometrijskih podataka, zdravstveno stanje ili seksualna orijentacija fizičkog lica.

Ukoliko se radi o povredi podataka o ličnosti koja može da prouzrokuje rizik po prava i slobode fizičkih lica, kompanije su dužne da što pre obaveste Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti (dalje: Poverenik) ili ako je to moguće, u roku od 72 časa od saznanja za povredu, i da preduzmu sve odgovarajuće mere za umanjenje štetnih posledica.

Ukoliko se radi o visokom riziku po prava i slobode fizičkih lica, kompanije su dužne da bez nepotrebnog odlaganja o povredi obaveste i lice na koje se podaci odnose.

Lice koje je pretrpelo materijalnu ili nematerijalnu štetu zbog povrede podataka o ličnosti ili bilo koje druge povrede odredaba ZZPL-a, ima pravo na novčanu naknadu štete od kompanije koja joj je štetu prouzrokovala.

« POVRATAK NA SADRŽAJ

Pored navedenog, u slučaju povrede podataka o ličnosti ili povrede odredaba ZZPL-a, Poverenik može izreći odgovarajuću novčanu kaznu u zavisnosti od okolnosti svakog pojedinačnog slučaja.

Kazne koje se mogu izreći kompanijama u slučaju bilo koje povrede odredaba ZZPL-a kreću se u rasponu od 50.000,00 dinara do 2.000.000,00 dinara.

Lice za zaštitu podataka o ličnosti

Lice za zaštitu podataka o ličnosti, popularnije *Data Protection Officer* ili *DPO*, jeste stručno lice imenovano od strane kompanija, koje je u skladu sa odredbama ZZPL-a dužno da:

- informiše i daje mišljenje kompanijama, kao i zaposlenima o njihovim zakonskim obavezama u vezi sa zaštitom podataka o ličnosti;
- prati primenu odredbi ZZPL-a, drugih zakona i internih propisa kompanija što uključuje i podizanje svesti i držanje obuka zaposlenima o obradi podataka o ličnosti;
- daje mišljenje o proceni uticaja obrade na zaštitu podataka o ličnosti i prati postupanje po toj proceni;
- sarađuje sa Poverenikom i savetuje se sa njim u vezi sa pitanjima koja se odnose na obradu.

Lice za zaštitu podataka o ličnosti određuje se na osnovu njegovih stručnih kvalifikacija, a naročito znanja i iskustva u ovoj oblasti. Ovo lice ne mora biti zaposleno u kompaniji, već može biti i eksterno angažovano.

Iako nije uvek obaveza, primetno je da sve veći broj kompanija imenuje ovo lice, što je svakako poželjno i preporučljivo, budući da se na taj način ostavlja utisak profesionalnosti i odgovornog poslovanja.

Kompanije koje su u skladu sa ZZPL-om dužne da imenuju Lice za zaštitu podataka o ličnosti jesu one čije se aktivnosti sastoje u radnjama obrade koje po svojoj prirodi, obimu, odnosno svrhama, zahtevaju redovan i sistematski nadzor velikog broja lica na koje se podaci odnose i one koje obrađuju posebne, odnosno, naročito osetljive vrste podataka o ličnosti ili podatke o ličnosti u vezi sa krivičnim presudama i kažnjivim delima.

Lice za zaštitu podataka o ličnosti uključeno je u sve poslove koji se tiču obrade ličnih podataka i kompanija je dužna da mu obezbedi nezavisnost kao i neophodna sredstva za izvršavanje obaveza, pristup podacima o ličnosti, radnjama obrade i stručno usavršavanje. Za svoj rad, Lice za zaštitu podataka o ličnosti odgovara kompaniji koja mu ne može raskinuti ugovor o radu, niti ga na bilo koji drugi način sankcionisati zbog vršenja svojih obaveza koje su jasno propisane ZZPL-om.

« POVRATAK NA SADRŽAJ

GARANT TOOL 24 – PAMETNI ORMAN ZA USPEŠNE

Kompanija Rotometal alati d.o.o. Beograd, dugogodišnji partner Hoffmann Group iz Nemačke, predstavlja na tržištu Srbije PAMETNI ORMAN – GARANT TOOL24, jednostavno rešenje za nabavku, izdavanje i skladištenje alata i potrošnog materijala u vašoj proizvodnji, uz maksimalnu uštedu i kontrolu.

JEDAN ORMAN – 1.000 MOGUĆNOSTI

- Izdavanje alata bez magacionera
- On-line kontrola utroška potrošnog materijala u proizvodnji
- Smanjivanje nepotrebnih zaliha
- Automatsko naručivanje uz kontrolu zadatih minimalnih i maksimalnih količina
- Sve vrste izveštaja potrošnje po vašim zahtevima

Hoffmann Group je jedan od vodećih svetskih dobavljača alata i potrošnog materijala u industriji.

Stogodišnje iskustvo u radu sa najvećim svetskim firmama dovelo je do stvaranja savršenog sistema u praćenju i nabavci potrošnog materijala u vašoj proizvodnji. Implementacijom pametnog ormana GARANT Tool24, dobijate ne samo magacin za vaše proizvode već kompletan sistem uvida u trenutno stanje i potrošnju materijala i alata.

Smenski rad u 2-3 smene iziskuje isto toliko magacionera i njihova neusaglašenost sa službom nabavke često može dovesti do zastoja u proizvodnji, što pametni orman automatskim naručivanjem, kontrolom zaliha i kontrolisanim izdavanjem ne dozvoljava.

Analizom izveštaja koji sami birate i osmislite, znatno efikasnije možete kontrolisati svoju proizvodnju. Izveštaje koje dobijate u Excell tabeli možete prilagoditi projektu, mašini, radniku, sektoru, mestu troška, alatu ili prema vašim posebnim željama.

Naš software je kompatibilan sa većinom poznatih poslovnih programa i moguće ga je implementirati na više uređaja po vašoj želji – PC, tablet, pametni telefon...

Izdavanje alata iz pametnog ormana GARANT TOOL24 je vrlo jednostavno. Ovlašćena lica pomoću ličnog koda, otiska prsta ili karticom pristupaju ormanu i odabirom traženog alata (slika, šifra artikla, naziv...) zadužuju alat na svoje ime. Sistem automatski prati stanje zaliha i ako se zalihe svedu na minimalne količine, obaveštava odgovornu osobu e-mail-om o potrebnoj dopuni. Sistem tom prilikom sam definiše potrebne e-mail adrese za svakog dobavljača posebno.

Više informacija i prezentaciju pametnog ormana GARANT TOOL24, možete dobiti od naših kolega:

Aleksandar Ilić – 063/21 87 17
Boško Dolovački – 064/22 62 246
E-mail: info@rotometal-alati.rs

Hoffmann Group
ROTOMETAL ALATI

KAKVE ŠTETE SAJBER NAPADI MOGU DA SE NANESU KOMPANIJI, A KAKVE POJEDINCIMA?

Piše:
Petar Mijatović
advokat

Zakon o zaštiti podataka o ličnosti koji je u primeni više od četiri godine i koji je u normativnom delu pretežno usklađen sa Opštom uredbom EU o zaštiti podataka o ličnosti, iako (za sada) nije doneo očekivane rezultate, između ostalog, imao je uticaj na podizanje svesti kompanija ali i pojedinaca o potrebi postizanja znatnog većeg nivoa zaštite ličnih i poslovnih podataka, posebno u kontekstu sajber napada koji se dešavaju na svakodnevnom nivou, a koji targetiraju informacione sisteme, računarsku mrežu, kao i lični računar/pametni telefon.

Zahvaljujući phishing-u, nakon što kliknemo na link ili prilog, napadač dobija pristup našem uređaju/sistemu što može da iskoristi za prikupljanje poverljivih podataka, bilo unutar organizacije bilo samo onih koji se vezuju za nas. Nezakonito raspolaganje poverljivim informacijama i ličnim podacima može proizvesti za kompanije direktnu štetu, poput uništavanja informacionog sistema, raspolaganja finansijskim/sredstvima i podacima, ali i indirektnu štetu - kako onu koju pretrpe kršenjem obaveza prema poslovnim partnerima (kršenje klauzule poverljivosti, povreda bezbednosti ličnih podataka u kontekstu ugovora o obradi podataka o ličnosti), tako i onu prema fizičkim licima (povreda bezbednosti ličnih podataka). Sve ove ugovorne i zakonske povrede nastale kao posledica „samo“ jednog sajber napada mogu imati za posledicu ogromnu finansijsku štetu koju organizacija mora da snosi prema klijentima, fizičkim licima i nadležnim organima u kontekstu prekršaja načinjenih u tom procesu, ali i reputacionu štetu koja može dovesti do prekida poslovne saradnje, gubitka poverenja, i konačno, kolapsa celokupnog poslovanja.

U ovom kontekstu ne treba zaboraviti na pojedince - *sajber napadi dovode i do krađe identiteta, putem phishing-a, ali i neretko usled nesmotrenog ostavljanja podataka nepouzdanim izvorima (ime, prezime, broj računa, adresa, broj lične karte i dr.)*. Napadač ovo čini radi sticanja finansijske koristi.

Sve ove nabrojane posledice bi trebalo da predstavljaju, kako za kompanije, tako i za pojedince, alarm i podsetnik da bi, pored zaštite informacionih sistema, uvođenje redovne edukacije u vezi sa sajber rizicima (i to neretko na najosnovnijem nivou - ne otvarati linkove i ne skidati datoteke poslate sa nepoznatih eksternih mejlova) u najvećem procentu slučajeva sprečilo kompromitaciju informacionih sistema/podataka i posledično, nastanak svih gore pobrojanih šteta.

« POVRATAK NA SADRŽAJ

ŠTEDNJA PO VIĐENJU

MOŽEŠ DA KORISTIŠ NOVAC U SVAKOM TRENUTKU I DA POLETIŠ U SUSRET SVIM SVOJIM ŽELJAMA!

Dodatna pogodnost bonus kamata

4%*

uz štednju u dinarima

Mobi Banka

*više informacija i reprezentativne primere pogledajte na sajtu Banke: www.mobibanka.rs

ŠTA HAKERI NAPADAJU I ZAŠTO

Piše:
Mikica Ivošević
Founder&CTO
Seif.ai

Hakeri “napadaju” računarske sisteme, a razlozi mogu biti dijametralno suprotni – od krađe i preprodaje osetljivih podataka do tzv. “penetracionog testiranja”, to jest pronalaženja ranjivosti u sistemima, kako bi se te ranjivosti uklonile.
Prvi se obično nazivaju “black hat”, odnosno sajber kriminalci, i oni su u suprotnosti sa “white hat”, ili etičkim hakerima. Ova distinkcija je veoma važno da se razume: reč “haker” obično ima negativnu konotaciju, iako su etički hakeri ti koji konstantno rade na unapređivanju sajber bezbednosti svih ljudi na internetu.
Jednom rečju, sajber kriminalci napadaju kompanije, dok etički hakeri doprinose njihovoj odbrani.
Motivi sajber kriminalaca su gotovo uvek isti: kroz ugrožavanje sajber bezbednosti kompanija i drugih organizacija, oni stiču novac. Među najpopularnije metode spada iznuda putem blokiranja poslovanja i krađa osetljivih podataka (kako klijentskih, tako i podataka o zaposlenima) i preprodaja na brojnim crnim berzama interneta.
Ukradeno intelektualno vlasništvo dostiže visoku cenu na tržištu, naročito kada ponuda dolazi od konkurencije. Industrijska špijunaža je u tom smislu potpuno prešla u domen sajber kriminala.

Kako sajber kriminalci zarađuju na kompanijama?

Kako bi se bolje razumeo kontekst, potrebno je objasniti obim sajber kriminala danas.

Sajber kriminal je ustrojen kao industrija sa godišnjim obrtom od preko osam triliona dolara godišnje. Ova cifra daleko prevazilazi BDP mnogih razvijenih ekonomija, kao što su Velika Britanija, Japan, ili Nemačka.

Postoje čitava tržišta posvećena prodaji ukradenih podataka. Međutim, to je samo jedan od vidova monetizacije. Drugi podjednako popularan način je iznuda pomoću malicioznih softvera poznatih kao ransomver (ransomware). On funkcioniše po jednostavnom principu: maliciozni softver se različitim metodama infiltrira u sisteme, koje zaključava nakon aktivacije. Bez pristupa računarima, ili pristupa podacima koji su ključni za funkcionisanje, kompanija ostaje paralisana. Da bi se oslobodile, kompanije moraju da plate otkupninu, nakon koje sajber kriminalci oslobađaju “taoce” – blokirane računare i podatke.
Ukoliko odbiju, podaci mogu vrlo lako biti obrisani, oštećeni ili pušteni u javnost, što sa sobom nosi niz novih problema. Važno je napomenuti da, čak i ukoliko plate otkupninu, ne postoji prava garancija da napadači nisu kopirali podatke i da se spremaju da ih preprodaju.

Sajberkriminalci pružaju usluge, ili iznajmljuju svoje malicioznе softvere svojim manje tehnički obučenim, ali jednako ambicioznim kolegama, ili "investiraju" u kupovinu ukradenih podataka kako bi hakovali druge, veće mete.

Zašto napadaju pojedince?

Pojedinci najčešće stradaju u masovnim *phishing* kampanjama – posebnim prevarama preko elektronske pošte u kojima se sajber kriminalci lažno predstavljaju, kako bi naveli primaoce da "skinu" maliciozni prilog ili kliknu na link na kom će ostaviti svoje poverljive podatke (kredencijale, finansijske podatke i sl.). Ove prevare često izgledaju kao rutinske poruke od banke, pošte, ili – kao što je izraženo bio slučaj za vreme COVID pandemije – medicinskih ustanova.

Iako sajber kriminalci retko napadaju ciljano jednu osobu, postoje i takvi slučajevi. Recimo, nedavno je objavljeno da su korisnici Apple mobilnih uređaja bili špijunirani kroz svoje mobilne telefone zahvaljući prethodno nepoznatom propustu u iOS operativnom sistemu. Nedavno je otkriveno i da su preko ovog propusta prisluškivane diplomate i zvaničnici vlada na Bliskom Istoku.

S druge strane, instalacija malicioznih softvera na velikom broju pojedinačnih uređaja se može iskoristiti za kreiranje tzv. *botnet*-a. Ako bi napadač "umrežio" veliki broj zaraženih računara, mogao bi da pokrene *ransomware* napad na sve njih istovremeno i traži neku priuštivu otkupninu, na koju bi žrtva lako pristala. Pored otkupnine, mogao bi istovremeno da izvuče osetljive informacije, kredencijale za društvene mreže i – što je najvažnije – bankovne podatke kao što su brojevi kartica i CVV brojevi.

Napadači koriste *botnet* mreže za izazivanje preopterećenja saobraćaja na određenim sajtovima, što je poznato kao DDoS napad. Posledica ovakvog napada je prestanak rada sajta, što za komercijalne sajtove predstavlja ogroman problem – finansijski i reputacioni. Kompanije su često spremne da plate napadačima kako bi izbegle bilo kakav zastoj u poslovanju.

Na kraju, upravljanje velikim brojem računara može se iskoristiti za tzv. *black hat marketing*. Koncept je sledeći: sajber kriminalci koriste tuđe računare pod svojom kontrolom da posećuju sajtove i klikću na reklame, veštački stvarajući saobraćaj. Google Adsense, koji reguliše monetizaciju sajtova na osnovu posete, zatim novčano nagrađuje sajber kriminalce.

Što će kome podaci pojedinca?

Na pitanje šta će kriminalcima podaci pojedinaca, ako ovi ne žele da ih otkupe ili nemaju para za otkup - osim ako je ucena sa snimcima "nedozvoljenih radnji" u pitanju, prvi odgovor se nameće sam: radi krađe identiteta. Recimo, u svrhu otvaranja naloga u menjačnici za kriptovalute, koja nema izuzetno stroge *Know Your Customer (KYC)* procedure, zadužene za temeljnu proveru identiteta klijenta.

Sa tuđim identitetom moguće je i pozajmljivanje novca, transfer sredstava, iznajmljivanje životnog ili poslovnog prostora, ili preuzimanje penzije, socijalne ili druge vrste pomoći od države.

« POVRATAK NA SADRŽAJ

Na kraju, mogu jednostavno da iskoriste nečiji identitet tokom krivičnog dela kako bi zavarali trag pred policijskim organima.
S druge strane, ukoliko napadač ostvari pristup nalozima na društvenim mrežama svoje žrtve, može kontaktirati prijatelje te osobe i tražiti novčanu pomoć ili slično.

Kad je reč o snimcima "nedozvoljenih radnji", jedna takva prevara je pre nekoliko godina zabeležena i na našim prostorima. Ovakve iznude su uglavnom zasnovane na lažnim snimcima koji se šalju na hiljade nasumičnih adresa i treba ih ignorisati.

Dok su kompanije dužne da svoje sajber incidente prijave nadležnim organima koji, zauzvrat zaista rade na tome da utvrde ko su odgovorni, pojedinci obično sami pokušavaju da saniraju štetu i retko kada uspevaju da isteraju pravdu za sebe.

Kakve sve zastoje u funkcionisanju života mogu da izazovu hakeri?
Možda najsvežiji primer sajber napada koji je imao direktan uticaj na funkcionisanje života u fizičkom svetu bila je blokada Nagoya Port, najveće japanske luke, odgovorne za oko 10% ukupnog uvoza i izvoza u zemlji. Napad se desio u julu ove godine i zaustavio kompletnu delatnost luke, što je dalje izazvalo velike logističke pometnje širom sveta. Na sreću, japanski stručnjaci su nakon manje od jednog dana uspeli da vrate luku u pogon.

Kod nas je i dalje slučaj bez presedana napad na novosadsku Informatiku iz marta 2020. Ishod u našem slučaju nije bio kao kod japanskih kolega – nakon što su gradski čelnici odbili da plate otkup od 20 bitkoina (što je tada iznosilo 18.500.000 dinara), napadači su pokrenuli brisanje podataka. Pun opseg štete je ostao nepoznat, međutim, sudeći po oporavku koji je trajao više nedelja, možemo pretpostaviti da je bio pozamašan.
Opet, nisu svi slučajevi tako crni. Čak i među sajber kriminalcima postoji kodeks ponašanja koji zabranjuje napade na određene mete. Na primer, nakon što se *ransomware* proširio od svoje prvobitne mete i zahvatio datoteke jedne dečije bolnice u Americi, grupa odgovorna za napad, Lockbit, odmah je preduzela korake da oslobodi zarobljene bolničke datoteke, kako životi dece ne bi bili ugroženi.

ZNAČAJ SIGURNOSNIH SISTEMA U INDUSTRIJI

Piše:
Marko Gulan
Cybersecurity Consultant SEE
Schneider Electric

Za industriju, menadžment i finansije ključni su u uspostavljanju sigurnih sistema!

U industriji, sajber bezbednost postaje najkritičniji aspekt za uspeh poslovanja. Savremena industrija sve više zavisi od tehnologije i digitalnih sistema koji su podložni sajber napadima. Zbog toga je nužno da menadžment i odeljenja finansija shvate i pravilno upravljaju sajber bezbednošću kao ključnim prioritetom.
Sajber bezbednost nije samo pitanje tehnologije, ona je evoluirala i postala multidisciplinarna grana koja sve više zahteva razumevanje rizika.

Upravljačke strukture moraju razumeti specifične sajber rizike sa kojima se industrijski sektor susreće. To uključuje prepoznavanje potencijalnih pretnji, ranjivosti, moguće finansijske posledice, ali i važnost kontinuirane procene rizika i redovnih ažuriranja sajber bezbednosne strategije namenjene industrijskim kontrolnim sistemima.

Stoga je ključno osigurati neophodne resurse za implementaciju sigurnosnih mera, kao i sredstva za obuku i edukaciju zaposlenih o sajber bezbednosti. Na kraju, i nikako manje važno, neophodno je stvaranje kulture bezbednosti koja uključuje podizanje svesti o sajber bezbednosti među zaposlenima, uspostavljanje jasnih bezbednosnh politika i procedura i podršku integraciji sajber bezbednosti u poslovne procese.

Sanacija napada višestruko je skuplja od investicije u sigurnost!

Finansijske posledice sajber napada u industrijskom sektoru značajne su i dugoročno štetne. Iako konkretni podaci o napadima često nisu javno dostupni, jer organizacije ne žele da dele detalje o napadima iz razloga tajnosti, reputacije ili pravnih pitanja, ipak postoje okvirni pokazatelji štete.
Neka od istraživanja nam govore o izuzetno visokim troškovima sajber napada.

Prosečan trošak, na globalu, iznosi do 13,2 miliona dolara po kompaniji, a troškovi uključuju direktne finansijske gubitke, troškove oporavka, gubitka produktivnosti, i troškove naknadnog uspostavljanja sigurnosnih rešenja.

Saradnja sa Schneider Electricom ključ je uspostavljanja sigurnosti i otpornosti u industriji!

Kompanije treba da se povežu sa Schneider Electric-om - tržišnim liderom za industrijsku sajber bezbednost - kako bi implementirale rešenja specifična za njihove potrebe. Ova saradnja omogućava pristup najnovijim informacijama, najkvalitetnijim kadrovima, trendovima i najboljim praksama kako bi se povećala otpornost organizacije na sajber pretnje.

« POVRATAK NA SADRŽAJ

NAJZASTUPLJENIJE TEHNIKE SOCIJALNOG INŽENJERINGA

Piše:
Radoje Gvozdenović
Viši savetnik
Sektor za informacione tehnologije,
Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti

Prema podacima Proofpoint **98%** svih sajber napada koristi tehnike **socijalnog inženjeringa** (eng. social engineering). Među najvećim u 2023, dva su koristila upravo socijalni inženjering.

Prema izveštaju IBM za 2023, globalna procečna cena povrede podataka prozrokovana korišćenjem socijalnog inženjeringa kao početnog vektora sajber napada – iznosi prosečno **4,45 mil. američkih dolara!**

Da bi shvatili moć socijalnog inženjeringa, zamenićemo ga na kratko, ne bez razloga, manje popularanim pojmom „društveni inženjering“. **Društveni inženjering** prisutan je u našim životima od najranijeg detinjstva. Situacija u kojoj su roditelji uspevali da nas navedu da popijemo „onaj“ gusti slatkasti sirup, “školski” je primer društvenog inženjeringa.

U 21. veku doživeo je svoj procvat. Koristeći informaciono-komunikacione tehnologije i najnovija naučna saznanja iz oblasti psihologije, sociologije i neurofiziologije, stavio se u službu moćnih korporacija i političkih elita, manipulativno injektirajući u podsvest odabranih ciljnih grupa vrednosne stavove, potrebe, navike ili akcije. Iako između pojmova „društvenog“ i „socijalnog inženjeringa“ ne postoje semantičke, pa ni suštinske razlike, pojam „**socijalni**“ etablirao se u oblast sajber bezbednosti izmeštajući iz fokusa širi kontekst svog malignog uticaja i pogubne posledice “**hakovanja mozga**”.

Socijalni inženjering je skalabilan i kreativan skup manipulativnih tehnika čiji je cilj da na osnovu poznavanja obrazaca u ponašanju ljudi iste navedu da nevoljno i bez svesti o stvarnoj prirodi i posledicama svog činjenja, omoguće realizaciju sajber napada i ostvarivanje lukrativnih ili destruktivnih ciljeva napadača. Sa **psihološkog stanovišta** cilj mu je da potakne ishitrene ili nesvesne reakcije žrtve bazirane na predrasudama, konformizmu i nekritički usvojenim socijalnim, kulturološkim, etničkim i drugim stereotipima. Ciljajući

na strah (od smrti, autoriteta, odgovornosti, finansijskog gubitka itd.), a zatim i na druge "okidače" poput pohlepe, sujete, znatiželje, empatije i sl, napadač se poput iluzioniste igra percepcijom žrtve, navodeći je da bez fizičke prisile učini ono što od nje želi.

Verizon u svom izveštaju za 2023. navodi **tri najzastupljenije** tehnike socijalnog inženjeringa:

Fišing (Phishing): Podrazumeva slanje imejlova sa sumnjivim prilogom ili zlonamernim linkom, kojim se od korisnika traži ažuriranje lozinke radi ovladavanja njegovim korisničkim nalogom ili provocira pokretanje ransomware i drugih malvera. U zahtevnijim scenarijima napadač se lažno predstavlja putem e-pošte, SMS-a, telefonskih poziva ili poruka na društvenim mrežama, nastojeći da navede žrtvu da mu pruži "hitnu" finansijsku pomoć, oda lične podatke, lozinke, brojeve kreditnih kartica i druge poverljive informacije. Direktno ili redirekcijom uz zaobilaženje MFA, pokušaće da navede žrtvu na lažnu veb stranicu sa istom URL strukturom i izgledom poput prave, gde će prigrabiti njene akreditive i kompromitovanjem korisničkih naloga doći do poslovnih tajni i drugih vrednih informacija.

*Koristeći modifikovanu verziju **ChatGPT** napadači automatizuju fišing napade i na više jezika kreiraju personalizovanu, stilski i gramatički uverljivu e-poštu.*

***Obmana pričom** (Pretexting):* Tehnika koja podrazumeva kreativnost i komunikacijske veštine napadača, koji preuzimajući lažni identitet u cilju vršenja prevare u direktnoj komunikaciji nastoji da eksploatiše sugestibilnost žrtve i u tako izgrađenom odnosu poverenja istu navede da mu oda osetljive informacije u cilju krađe identiteta ili izvršenja druge inkriminisane radnje.

Direktorska prevara (BEC): Koristeći pretexting i informacije proistekle iz prethodno vođene poslovne komuni-

kacije preko e-pošte ili telefona, napadač nastupa u ulozi dobavljača, poslovnog partnera ili čak zaposlenog iz organizacije žrtve, navodeći je da mu na vešto lažiran račun preusmeri uplate novca ili informacije koje može da monetizuje.

ChatGTP i **Deepfake** sadržaji učinili su navedene tehnike još opasnijim, implicirajući potrebu za još temeljnijim obukama zaposlenih, davanjem praktičnih smernica i prezentacijama simulacija sajber napada.

No, i pored toga, ne zaboravimo da su kvalitetno opšte obrazovanje i prosvećenost "prva linija odbrane" od svakojakih vrsta manipulacije, pa tako i od socijalnog inženjeringa.

Kada su u pitanju prodori u bezbednost podataka, ljudski faktor ima ulogu u **74%** slučajeva!

Ulazni vektor napada skoro uvek je imejl.

Zato, uvek budite skeptični, "klikćite pametno", i ne otvarajte e-poštu kada ste umorni!

« POVRATAK NA SADRŽAJ

KOJE NAS SVE „SPRAVE“ PRATE

Piše:
Vojislav Pavlović
IT Security Expert
A1 Srbija

Piše:
Siniša Manojlović
UAT Expert
A1 Srbija

Sa vremenom koje provodimo na internetu raste i broj opasnosti. Lični podaci sve su vredniji na „crnom tržištu“ (tzv. Dark web), pa se postavlja logično pitanje: odakle vrebaju opasnosti?

Društvene mreže

Razmislite o sadržaju koji delite. Iako je slika mukom stečene diplome, avionske karte ili putne isprave sigurno interesantna vašim bliskim prijateljima, zanimljiva je i potencijalnim hakerima koji koristeći se OSINT-om (*Open source Inteligence*) lako dolaze do podataka o vama koji se mogu iskoristiti za razne vrste napada poput *phishing*-a, *spear phishing*-a i krađe identiteta.

Uz to, pratite bezbednosne vesti i obaveštenja o ranjivostima vaših naloga na društvenim mrežama: to vam može pomoći da budete svesni potencijalnih pretnji i preduzmete odgovarajuće mere.

Otvorene internet mreže

Otvorene mreže na aerodromima, kafićima, *public wi-fi hot-spot* kao i hotelski *wi-fi* su nešto što treba zaobići. Nikada ne znate da li haker vreba u pozadini. Ako baš morate da ih koristite, ne unosite nikakve kredencijale za vaše naloge, i ne obavljajte onlajn plaćanje. Savet je da uvek koristite sopstvene paketne podatke, ili da kupite lokalnu karticu za jednokratnu upotrebu: nije skupa, ali para vredi.

Dobri stari *phišing*

Mada je i dalje najčešći napad *phishing*-om preko mejla, sada su razvijene i nove vrste poput *vishing*-a (to je *phishing* preko telefonskog poziva), *smishing*-a (*phishing* preko SMS poruke) i jedan od novijih je i *quishing* (*phishing* preko QR koda) **.**

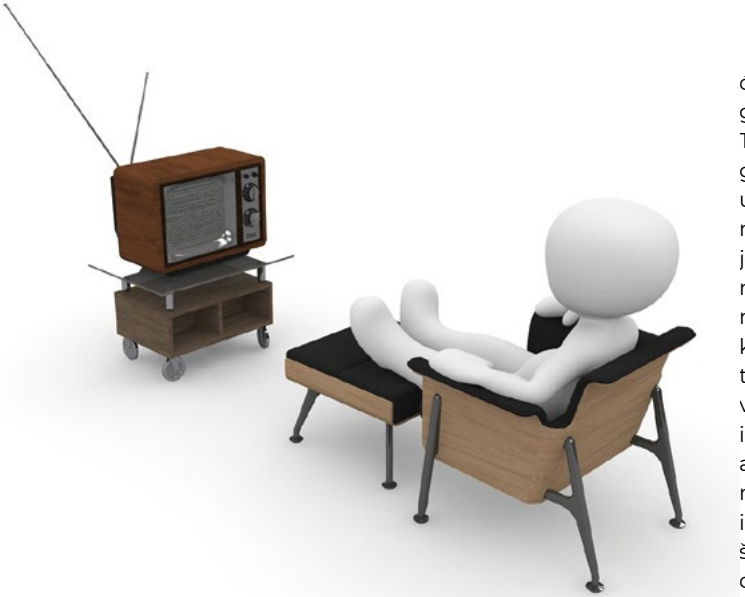
Kako se zaštiti? Koristiti 2FA autentifikaciju, neku vrstu autentifikatora, a organizacije moraju imati striktne politike o šiframa (redovno menjanje i zabrana da se ista šifra ponavlja, ili koristi na više naloga).

Phišing je u oku posmatrača. Ako deluje sumnjivo, poziva na hitnost, zahtev stiže u vreme koje nije uobičajeno, u mejlu se nalazi grupa ljudi koje ne znate - najbolje je obrisati sporni mejl, a ako je reč o poslovnom mejlu, potrebno ga je prijaviti IT odeljenju za sajber bezbednost.

***Malware* napadi**

Izašla je najnovija sezona tvoje omiljene serije? *Beteshda* je konačno objavila da lanisira dugo očekivani nastavak *Elder*

Scroll-a i na internetu već nude da se sve to pogleda ili skine besplatno.
U IT bezbednosti važi isto pravilo kao i u životu: nema besplatnog ručka! Često ćete prilikom instalacije softvera iz nepoznatih izvora dobiti i „dodatne programe“ koji vam mogu naneti više štete nego koristi pa vaš uređaj ili uređaji mogu biti deo *botnet* mreže za dalje širenje virusa ili sajber napada, ili biti korišćeni za rudarenje kripta. Takođe može doći do curenja vaših privatnih i poslovnih podataka ili do krađe identiteta.



USB uređaji
Takođe su jedan od načina da ugrozite svoje podatke. Ako već koristite USB u svakodnevnom radu, uradite kriptovanje uređaja i lozinku ne delite ni sa kim.

Veštačka inteligencija
AI je nova pojava u svetu sajber bezbednosti: uz pomoć AI može se lako doći do vaših podataka, a u te svrhe se neretko koriste i mobilni telefoni. Ne javljajte se na pozive koji vam nisu poznati - pogotovu iz inostranstva, i brišite SMS poruke od nepoznatih pošiljalaca. Zlonamerne osobe mogu snimiti vaš glas i pomoću AI doći do vaših podataka.

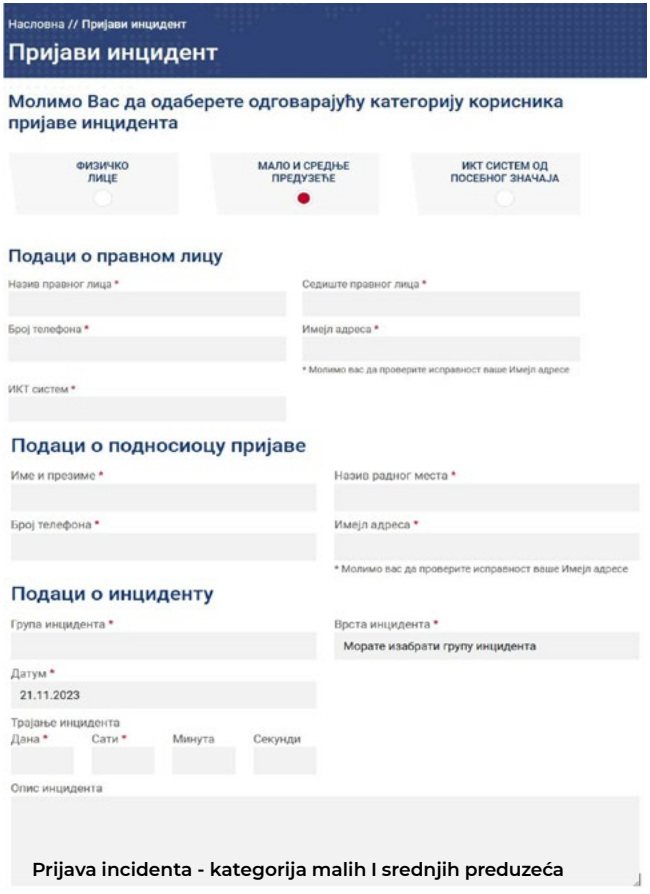
Uređaji na mreži (IoT)
Svi uređaji povezani na mrežu mogu biti hakovani. Dobar deo nas sada koristi IoT (Internet of things) da kontroliše klimu, prećiščivač vazduha, svetla, grejanje i kućne uređaje. To hakerima daje mogućnost da zloupotrebe uređaje kao deo *botnet* mreža, za DDOS napade ili jednostavno za špijuniranje korisnika. Mada su im najčešće mete nadzorne kamere, računari, mobilni telefoni, meta može biti i vaš televizor koji najčešće ima sopstveni pretraživač, a ažuriranja su često neredovna. Mnogi televizori imaju i *Web cam built in* što omogućava hakerima da vas prisluškuju i snimaju što im dalje može poslužiti za razne aktivnosti poput ucena, krađe podatka i hakovanja drugih uređaja kako bi ispunili neki viši cilj.
Ukoliko je vaš TV zaštićen šifrom, neka to bude komplikovanija i što duža šifra. Ako ima fizičku vezu sa ruterom, vodite računa i o šifri rutera, ne ostavljajte je zapisanu na vidnom mestu i menjajte je. Preporuka je da TV ažurirate redovno, kao i da sve aplikacije koje skidate budu sa proverenih izvora.
Najslabija karika u svakom sistemu je na kraju ipak čovek, zato razmislite šta već danas možete da učinite kako biste zaštiti svoje lične podatke na internetu. Kao što je sasvim normalno i sastavni deo vašeg dana da raspremite krevet, skuvate kafu ili odete u šetnju, navikavajte se i na redovne promene vaših lozinki, ažuriranja vaših uređaja i na to da ličnim podacima nije mesto na internetu. Do sledećeg klika...

« POVRATAK NA SADRŽAJ

KAKO I KOME PRIJAVITI SAJBER NAPAD

Piše:
Marko Krstić
rukovodilac
Nacionalni CERT

Ukoliko kompanija/preduzeće doživi sajber napad ili krađu podataka korišćenjem tehnika socijalnog inženjeringa, incident može prijaviti Nacionalnom CERT-u preko internet stranice cert.rs ili slanjem mejla na adresu **info@cert.rs**. Prijavu preko sajta je moguće obaviti u svakom trenutku klikom na dugme *Prijavi incident*. U okviru forme za prijavu potrebno je uneti i opisati incident koji se dogodio. Nacionalni CERT je za ovu svrhu napisao uputstvo za prijavu incidenata koje možete pronaći na linku:
https://www.cert.rs/prijava.html.



Prijava incidenta - kategorija malih I srednjih preduzeća

Nakon dobijene prijave incidenta zaposleni u Nacionalnom CERT-u je analiziraju i na osnovu analize i dostupnih informacija o incidentima pružaju savete i preporuke. Takođe ne treba zaboraviti da shodno članu 15. Zakona o informacionoj bezbednosti Nacionalni CERT prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, te

informacije o tehnikama napada korišćenim u incidentu koji ste vi prijavili mogu sprečiti napad u nekoj drugoj kompaniji/preduzeću.

Ovo je posebno značajno za napade koji se baziraju na tehnikama socijalnog inženjeringa, jer oni mogu biti i samo prva faza napada.

Ukoliko se na osnovu prijave incidenta može zaključiti da je došlo do izvršenja krivičnih dela koja se gone po službenoj dužnosti, Nacionalni CERT će o tome obavestiti tužilaštvo za visokotehnološki kriminal. Ova dela su definisana Krivičnim zakonikom i u njih spadaju:

1. oštećenje računarskih podataka i programa,
2. računarska sabotaža,
3. pravljenje i unošenje računarskih virusa,
4. računarska prevara,
5. neovlašćen pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka
6. sprečavanje i ograničavanje pristupa javnoj računarskoj mreži
7. pravljenje, nabavljanje i davanje drugom sredstva za izvršenje krivičnih dela protiv bezbednosti računarskih podataka.

Za svako od ovih dela u Krivičnom zakoniku definisani su uslovi u smislu radnje, objekta radnje, posledica, namere koje moraju biti ispunjeni kako bi se smatralo krivičnim delom i došlo do
sankcionisanja. Konačnu odluku da li je prosleđeni incident krivično delo i dalje korake u postupanju određuje tužilaštvo za visokotehnološki kriminal.

U slučaju krađe podataka veoma je važno koji su podaci ukradeni.

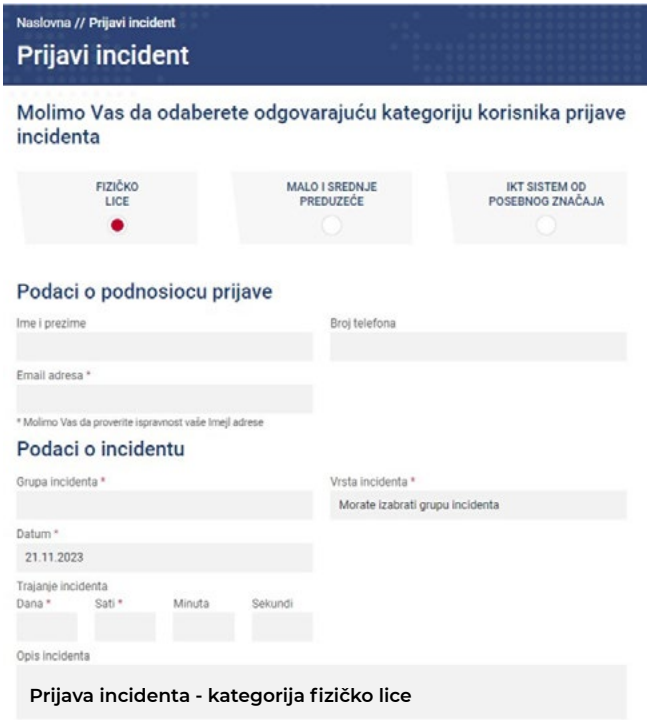
Ukoliko je došlo do krađe podataka o ličnosti kojima preduzeće/kompanija rukuje, prema Zakonu o zaštiti podataka o ličnosti postoji obaveza prijave incidenta Povereniku za informacije od javnog značaja i zaštitu podataka o ličnosti.

S druge strane ukoliko kompanija upravlja tajnim podacima, postupanje u slučaju kada je ugrožena ova vrsta podataka regulisano je propisima kojima se uređuje oblast zaštite tajnih podataka.

Kakva je procedura za građane/fizička lica?

Procedura prijave incidenta Nacionalnom CERT-u od strane fizičkih lica se suštinski ne razlikuje od procedure prijave od strane kompanija/preduzeća. Jedina razlika je što je kod prijave od strane preduzeća neophodno popuniti i kontakt podatke koji se tiču same kompanije. Cilj razvrstavanja prijava na one koje se tiču fizičkih lica, malih i srednjih preduzeća i IKT sistema od posebnog značaja Nacionalnom CERT-u je dalja analiza pretnji za svaku od ovih kategorija.

Sa stanovništva Nacionalnog CERT-a takođe ne postoji razlika ni u smislu procesa obaveštavanja tužilaštva za visokotehnološki kriminal. U istim situacijama se ova institucija obaveštava od strane Nacionalnog CERT-a kada postoji sumnja na krivično delo.



Link za uputstvo

« POVRATAK NA SADRŽAJ

SAJBER-PREVARANTI: KAD VEĆ LAŽU CEO SVET, ZAŠTO MISLITE DA VAS NEĆE SLAGATI?

Piše:
Vojislav Rodić
CEO
I Net

Navikli smo se da kupujemo preko interneta - svaka prodavnica je u ekranu našeg, sve pametnijeg, uređaja. Beskonačno listanje ogromne ponude samo pojačava naše potrošačke instikte. Završni „klik“ kojim zaključujemo ugovor o kupovini predstavlja kulminaciju našeg potrošačkog samopotvrđivanja. Kad porudžbina stigne, naše nestrpljenje je na vrhuncu, i baš pred isporuku dobijamo poruku: potrebno je da doplatimo zanemarljiv iznos na ime carine/poreza/dostave.

Od koga je stigla poruka?

Od Pošte Srbije ili od nekog od poznatih globalnih kurirskih službi (DHL, FedEx, UPS, itd). Kako znate da je poruka zaista stigla od njih? Za vas je „dokaz“ o ispravnosti primljene poruke pre svega poznati logo kompanije, koji ste viđali na internetu, dostavnim vozilima, uniformama poštara/kurira itd. A i u zaglavlju poruke piše da zaista dolazi od pošiljaoca. Da li ćete mišem da postavite pokazivač na adresu pošiljaoca, pa onda pritisnete desni taster i pročitate šta tamo piše i sa kog domena izgleda da dolazi poruka? Isto možete da uradite i na telefonu prstom. Zar vas samo ta uplata deli od vaše porudžbine? Nikakav problem, kliknete da link u poslatoj poruci i dolazite na sajt dostavljača gde vas opet čeka poznati logo.

Ako popunite sva polja pošiljalac preuzima sve potrebne podatke – broj kartice, rok važenja, datum isteka, kontrolni broj. Šta će dalje da uradi sa podacima sa vaše kartice? Možda će podeliti saradnicima, da u što kraćem roku izvrše što veći broj plaćanja, ili će da izvrši samo jednu veću transakciju, ili će da doda podatke vaše kartice podacima brojnih drugih kartica u komplet za prodaju na „tamnom internetu“.

Čitajte slovo po slovo

Ako ste pažljivo pročitali tekst poruke, mogli ste da primetite više jezičkih nepravilnosti, ili samo neuobičajenih jezičkih konstrukcija. Nemojte da vas zavara ćirilica: oni koji spremaju „digitalne mamce“ znaju koje je pismo vašeg jezika. U stvari to im je i previd, većina korisnika na srpskom jeziku ne koristi ćirilicu, ali su navikli da su poruke od državnih institucija i javnih preduzeća najčešće na ćirilici. Ali: zašto je oznaka za PDV prikazana kao VAT (Value Added Tax)? Da li je bilo koja od uobičajenih dodatnih poveznica na „veb stranici“ aktivna tj. da li se klikom na tu poveznicu ide na odgovarajuću stranicu? Naravno da nećete da sprovodite ovakvu mini „istragu“ zbog plaćanja 52,48 dinara. Kada bi bilo samo to, ali u ovom slučaju svoju brzopletost (a o tome se radi) ne plaćate sa traženih 52,48 dinara nego potpunim pristupom vašem bankovnom računu neovlašćenim licima.

Zato je neophodan, najčešće i sasvim dovoljan, zdravorazumski oprez u svim operacijama u kojima nekome (kome?) saopštavate vaše lične podatke, posebno one finansijske prirode.

Moramo da imamo na umu i to da nemaju svi koji danas koriste internet u Srbiji dovoljno iskustva sa tipičnim on-lajn zloupotrebama. Prema podacima RZS u Republici Srbiji se za 2,3% povećao broj korisnika interneta u poslednja tri meseca

u odnosu na 2021. godinu, za 5,1% u odnosu na 2020. godinu. Najveći broj novih korisnika nema osnovna informatička znanja, ali im to ne smeta da efikasno koriste sve veći broj novih servisa. Brza kriva „učenja“ novih veština ih i zbog toga čini čestim žrtvama više puta ponovljenih klasičnih scenarija.

Perfidne metode za poslovne korisnike

Ako mislite da su iskusni, najčešće poslovni, korisnici manje ugroženi, imajte na umu da ni oni nisu pošteđeni sajber napada. Metode koje se za njih koriste kreću se od trivijalnih do izuzetno perfidnih. Popularno je slanje poruka sa „dokumentima“ kao što su narudžbina ili podaci za plaćanje (a u stvari virusima) do vrlo složenih operacija (Man In The Middle) u kojima se mesecima tiho prati vaša korespondencija sa partnerima, da bi se u nekom trenutku neko drugi „ubacio“ u prepisku i jednoj strani dao pogrešna uputstva za fakturisanje a drugoj za plaćanje. Sve ovo će biti dodatno pogoršano razvojem tehnologije veoma naprednih falsifikata (deep fake). Pri tom se ne radi samo o prepisci, već i drugim tipovima komunikacije, za koje sada mislimo da su pouzdani (zvučna i video).

Mnogo smo slabi prema našim “pametnim asistentima” - telefonima, ali to ne želimo ni sebi da priznamo.

Teško je poverovati, ali sajber pecaroši nas „upecaju“ zato što sve češće želimo da nas obasja zavodljivi sjaj nerealnih obećanja.

Imajući na umu tehnološke mogućnosti koje im stoje na raspolaganju, to su sada ribokradice koje koriste istovremeno dinamit i struju za istovremeno omamljivanje ogromnog broja svojih žrtava. Otrežnjenje je bolno i često sa dugotrajnim posledicama, ali mnogima ni to nije dovoljno da povrate svesno prisustvo u sopstvenom životu. Ne prestajte da sanjarite, ali pažljivo odaberite sa kim ćete to da radite.

« POVRATAK NA SADRŽAJ

SAJBER OSIGURANJE: „ZDRAVSTVENO OSIGURANJE“ NAŠE KOMPANIJE

Piše:
Bojan Jovanović
direktor sektora za
korporativne klijente
Marsh McLennan Srbija

Sajber osiguranje se praktično može smatrati „zdravstvenim osiguranjem kompanija“, jer je ono odgovor na situacije u kojima kompaniju napada „bolest“, odnosno doživi određene hakerske napade. U Srbiji je rast ove vrste osiguranja na godišnjem nivou vrlo simboličan - oko 1,5%, i što je dodatno poražavajuće, na vrlo malu osnovicu poredeći sa zaključenim polisama i premijama plaćenim u prethodnim godinama. U poređenju sa zapadom, pokazujemo znatno nižu svest o sajber riziku, pa su samim tim i ulaganja u prevenciju i zaštitu, kako informatičku tako i osiguravajuću, na nivou na kome je na zapadu svest bila početkom ovog veka.

Kako je sve počelo?

Sajber osiguranje datira iz kasnih 90-tih godina prošlog veka, praktično kada su tehnologija i internet evoluirali. U početku je bilo koncipirano kao osiguranje od profesionalne odgovornosti, sa fokusom na rizike koji su povezani sa medijima i softverom, da bi u kasnijim 2000-im godinama počelo da pokriva i gubitak podataka, bezbednost mreže i kompjuterske viruse i u tom periodu je već stasavala ideja da je pored pokrića sajber osiguranjem trećih lica potrebno pružiti i pokriće prvog lica, odnosno imovinu same kompanije u smislu datoteka, prekida rada, sajber iznude i sličnih rizika.

Kako hakeri napadaju?

Danas najveći rizik predstavljaju sistemski rizici, odnosno oni koji pogađaju jako veliki broj osiguranika, kao što su *Petya – Not petya*, *Wannacry* i *Log4j*, samim tim i veliki broj polisa (npr. napadom Log4j je pogođeno oko 10.000 polisa jednog svetskog osiguravača) te dovode do disrupcije u lancima snabdevanja. Tu su i *ransomware* rizici poput onog koji je pogodio naftnu kompaniju Colonial.

Iz našeg iskustva koje je na globalnom nivou veliko, došli smo do zaključka da u principu dva uzroka mogu dovesti do realizacije sajber rizika, a to su zlonamerni napad usmeren ciljano na vašu kompaniju ili slučajni događaj koji se svodi na nenamerno slanje osetljivih podataka trećem licu. Kada do ovih slučajeva dođe, poslovanje kompanije je ugroženo sa tri aspekta. Najpre postoji problem sa poverljivošću, kako naših podataka tako i informacija koje držimo o trećim licima, koji su osetljivi, a nad kojima više nemamo kontrolu. Tu je i problem integriteta podataka kojima raspolažemo i koje napadač može promeniti, te se nalazimo u sitauciji da je upitno da li su podaci koje ćemo koristiti u obavljanju svog posla tačni. I konačno postoji i problematika naše dostupnosti i mogućnosti da funkcionišemo kao do tada. Sve ovo dovodi do posledica koje se ogledaju u gubitku prihoda, dodatnim troškovima za kompaniju da se od napada odbrani, i odgovornosti prema trećim licima, odnosno onom što nazivamo „nefizičkim sajberom“.

Šta polisa „radi“?

Kada dođe do sajber incidenata, polisa osiguranja bi po pravilu morala da pokrije celokupnu lepezu rizika. Ova zaštita počinje od asistencije u toku samog sajber napada i saveta kako delovati i postaviti se kada je napad prepoznat i dok je u toku. Imajući u vidu da će kada do sajber napada dođe posledice najverovatnije biti kompleksne, polisa osiguranja pokriva najpre angažovanje IT stručnjaka na samoj rektifikaciji i obnovi podataka i datoteka koje su oštećene ili uzurpirane. Pored navedenog rizika, koji smatramo osnovnim, polisom se dalje pokriva prekid rada, odnosno gubitak profita koji smo pretrpeli usled nemogućnosti da redovno obavljamo svoju delatnost, a polisom se može pokriti i sajber iznuda do koje dolazi kada napadač „zaključa“ naše datoteke i traži određeni iznos novca, najčešće u formi kriptovaluta, kako bi nam dostavio kod kojim bismo otključali i opet uspostavili pristup našim podacima. Konačno, polise osiguranja bi morale da pruže pokriće i za regulatorne kazne i penale koje regulatorno telo može odrediti kompaniji, kao i eventualne tužbe trećih lica zbog izloženosti i gubitka njihovih podataka.

A šta „ne radi“?

Bitno je napomenuti da polise sajber osiguranja po pravilu ne pokrivaju tzv. „fizički sajber“, odnosno štete na imovini koje nastanu usled npr. požara izazvanog u nekom proizvodnom pogonu napadnute kompanije, kao i prekid rada do koga dolazi usled ovakvih i sličnih uzroka, kao i tužbe trećih lica koje bi bile opet posledica neke povrede ili oštećenja imovine čiji je uzrok „fizički sajber“.

Većina ljudi očekuje da bi sajber osiguranje trebalo da pokrije i krađu novca sa računa i prilikom određenih transakcija: bitno je skrenuti pažnju da i ova vrsta rizika nije pokrivena sajber osiguranjem, već vrstom osiguranja koje se naziva „crime“ osiguranje.

Sajber rizik je u svetu trenutno prepoznat kao jedan od najvećih rizika po poslovanje kompanija. Sajber higijena nam je na raspolaganju u vidu raznih vrsta sajber zaštite, a kao dodatna brana i kao „zdravstveno osiguranje naše kompanije“ na raspolaganju nam je sajber osiguranje koje je tu da svoje poslovanje vratimo u normalne tokove najbrže moguće i bez gubitaka koji ga mogu ugroziti na duže staze.

« POVRATAK NA SADRŽAJ

POLISA SAJBER OSIGURANJA KAO FINANSIJSKA ZAŠTITA

„Predviđa se da će tržište sajber bezbednosti dostići 300 milijardi dolara do 2026. godine. Zbog pandemije, skoro 60 odsto korisnika interneta prijavilo je povećan rizik od povrede podataka. Štete koje su prouzrokovali sajber napadi u 2023. procenjene su na osam triliona USD, odnosno 667 milijardi dolara mesečno - pokazuju statistike sajber bezbednosti. Svakih 39 sekundi jedan sajber napad se dešava širom sveta. Globalno, jedan napad *ransomvare*-a dešava se na svakih 14 sekundi".
Ovako je ilustrovala brojkama razmere opasnosti od sajber napada

Zdravka Predojević, iz Direkcije za tehniku osiguranja, kompanije **Generali Osiguranje Srbija**.

Koji su to osnovni rizici koji su pokriveni polisom sajber osiguranja u Generali osiguranju?
Svakodnevno poslovanje obuhvata širok spektar onlajn aktivnosti koje sa sobom donose rizike od sajber napada. U želji da klijentima omogućimo sigurno i bezbedno poslovanje, nudimo sajber osiguranje koje pruža sveobuhvatnu zaštitu u slučaju prevara ili gubitka podataka. Uz našeg partnera, ComTrade, osiguranicima smo na usluzi 24 sata, kako bismo što pre reagovali u slučaju prijave sajber incidenta.
Evo šta **Generali** nudi u svojoj paleti sajber osiguranja.
• Odgovor na sajber incident:
- usluga eksperta koji zaustavlja i sprečava dalje širenje sajber incidenta,
- obnova softvera i podataka,
- troškovi obaveštavanja o kršenju zaštite podataka i obaveštavanja,
- troškovi zaštite ugleda u slučaju kršenja zaštite podataka,
- povraćaj oduzetih novčanih sredstava elektronskim putem;
• Odgovornost prema trećim licima:
- za kršenja poverljivosti i privatnosti,
- za mrežnu bezbednost,
- za neispunjavanje ugovornih obaveza osiguranika;
• Prekid rada kod osiguranika;
• Sajber ucena.
Ukoliko je posledica ucene sajber incident, nadoknadiće se štete koje su osiguraniku nastale zbog angažovanja eksperta (npr. angažovanje eksperta za komunikaciju sa ucenjivačima), kao i ostali troškovi, nastali zbog razrešenja sajber ucene. Takođe, nadoknadiće se šteta i po ostalim pokrićima, koje je osiguranik ugovorio.

Cena otkupa koju osiguranik plati za razrešenje ili prekid sajber ucene NIJE pokrivena osiguranjem.

Pomenuli ste da je osiguran i prekid rada usled sajber napada. Šta je tačno pokriveno osiguranjem?
Generali polisom sajber osiguranja pokriven je i prekid rada osiguranika, odnosno pokrivena je smanjena neto dobit, ili uvećani troškovi poslovanja koji su posledica sajber incidenta.

Šta sve utiče na visinu premije, i koji su maksimalni iznosi pokrića?
Obračun premije se radi na osnovu tarifa, shodno oceni rizika, delatnosti osiguranika, broju i vrsti ugovorenih pokrića. Sama ocena rizika predstavlja ocenu izloženosti osiguranika sajber napadu, gde se posmatra istorija poslovanja klijenta i mere bezbednosti koje osiguranik poseduje, a koje treba da

smanje ili spreče sajber napad. Limiti pokrića zavise od konkretne potrebe klijenta i zato ne postoji univerzalna ponuda, već se ona kreira za svakog pojedinačnog klijenta.

Šta polisa, osim pomenutog otkupa, NE pokriva, i kakvu preventivu osiguranik mora sam da preduzme?
Kao i kod druge vrste osiguranja, i kod sajber osiguranja su isključene sve štete koje su posledica namere, prevare ili neke druge zlonamerne radnje osiguranika, kao i njegove nemarnosti prema poštovanju definisanih procedura. Osiguranik je dužan da sve svoje poslovne aktivnosti vezane za sajber bezbednost i prevenciju sajber napada, obavlja savesno, sa pažnjom dobrog privrednika i u interesu poslovnog društva.

Očekivani nivo bezbednosti koji osiguranik treba da poseduje zavise od njegove delatnosti, pa tako delatnost osiguranika igra veliku ulogu u oceni nivoa bezbednosti prilikom procene rizika.

Našim osiguranicima kao dodatni benefit pružamo preventivu, koristeći alat za *risk report*, koji klijentu može da ukaže na potencijalne slabosti. Takođe, nudimo vrhunski tim stručnjaka.

Koliko su domaći privrednici svesni ovih rizika, i koliko su spremni da obezbede sebi ovakvu polisu?
Na našem tržištu još nije dovoljna razvijena svest o potrebi za sajber osiguranjem. Kada je u pitanju sajber osiguranje, naš tim stručnjaka prvo sa klijentima obavlja razgovor, da bi čuo sve brige o sajber bezbednosti i stekao uvid u to koliko je biznis izložen opasnostima u digitalnom svetu. Kada se dobije potpuna slika, preduzimamo korake da sprečimo najgore. U slučaju sajber napada, MI smo tu da svakodnevne operacije klijenta pokrenemo što je brže moguće, na minimum svedemo eventualne finansijske gubitke i učinimo sve za klijenta, da njegova kompaniju bude otpornija na sajber rizike u budućnosti.

S obzirom na to da štete mogu biti ogromne, kako obezbeđujete pokriće za velike štete – koje reosiguravajuće kuće stoje iza vas?
U slučaju sajber napada mi smo uz klijente, fokusirani na to da se svakodnevne operacije pokrenu što je brže moguće, i da minimiziramo sve finansijske uticaje.
U slučaju velike štete prijavljene od osiguranika, Com Trade, naš eksterni partner, reaguje odmah, kako bi zaustavio i sprečio dalje širenje sajber incidenta.
Koristimo naše kompanijske prednosti i garantujemo stoprocentnu zaštitu delivši rizik sa Generali Reosiguranjem odnosno Generali Grupom, kroz reosiguranje.

« POVRATAK NA SADRŽAJ

ŠTA NAS ČEKA U BUDUĆNOSTI?

Hakovanje automobila

Moderna vozila su danas opremljena automatizovanim softverima i koriste *Bluetooth* i *WiFi* tehnologiju za komunikaciju što ih čini ranjivim na hakerske napade. U budućnosti nas očekuje preuzimanje kontrole nad vozilom i rast korišćenja mikrofona za prisluškivanje.

Veštačka inteligencija (AI) kao potencijalna opasnost

Veštačka inteligencija sa kombinacijom mašinskog učenja donela je ogromne promene u sajber bezbednosti. AI je bila najvažnija u izgradnji automatizovanih bezbednosnih sistema, obradi prirodnog jezika, detekciji lica i automatskom otkrivanju i predviđanju pretnji. Ipak, AI se može koristiti i za razvoj pametnog *malver-a* i napada kako bi se zaobišli najnoviji bezbednosni protokoli u kontroli podataka.

Mobilni uređaji i četbotovi kao nove mete

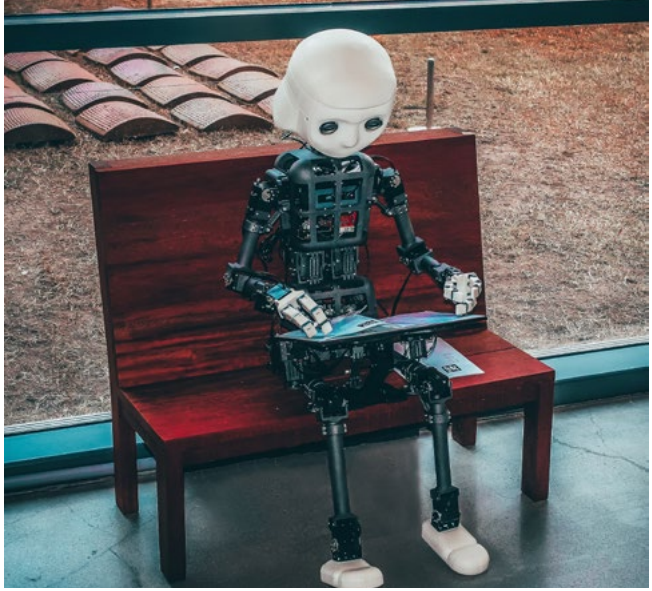
Naše aplikacije za mobilno bankarstvo, fotografije, finansijske transakcije, e-poruke i SMS poruke biće sve više meta hakera, a virusi se mogu lako „provući“ u telefon.
Četbotovi će biti meta tako što ih neko može iskoristiti za lažno predstavljanje, prikupljanje i krađu podataka.

„Oblak“ i njegove ranjivosti

Kod sve više organizacija koje su sada osnovane u „oblaku“ (*Cloude*), bezbednosne mere moraju biti kontinuirano nadgledane i ažurirane kako bi se podaci zaštitili od curenja. Iako su aplikacije u oblaku poput Google ili Microsoft-a dobro obezbeđene, krajnji korisnik je najslabija tačka posebno za fišing napade ili ubacivanje zlonamernog softvera.

Krađa podataka kao glavna meta

Podaci će i dalje biti najveća briga za organizacije širom sveta. Svaka manja mana ili greška u sistemskom pretraživaču ili softveru može biti „rupa“ kroz koju hakeri mogu da ubace zlonamerni virus.



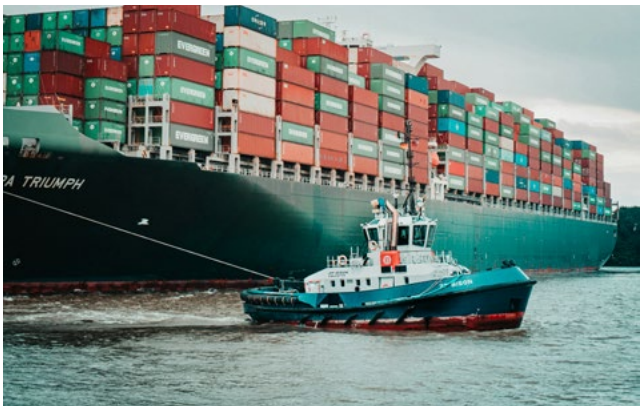
IoT sa 5G mrežom: nova era tehnologije i rizika

Sa pojavom i rastom 5G mreže povećavaće se i povezanost sa IoT. Međutim, 5G arhitektura je relativno nova i zahteva mnogo istraživanja kako bi se pronašle slabe tačke. Egzistiranje na 5G mreži može doneti mnoštvo mrežnih napada kojih možda nismo ni svesni.

Ciljani napadi

Ciljani *ransomvare* biće zastupljen naročito u industrijama razvijenih zemalja koje se u velikoj meri oslanjaju na specifičan softver za vođenje svojih svakodnevnih aktivnosti. Neki od primera su napadi na Nacionalne zdravstvene službe u Engleskoj i Škotskoj koji su oštetili više od 70.000 medicinskih uređaja.

Ciljano će, prema predviđanjima, biti napadani i lanci snabdevanja i kritična infrastruktura.



Sajber ratovanje pod pokroviteljstvom države

Ovo ratovanje neće prestati ni u budućnosti kako zbog aktuelnih geopolitičkih tenzija, stvarnih ratova, ali i izbora u zemljama koje su velike sile poput SAD gde se izbori održavaju 2024. U budućnosti se mogu očekivati kršenja podataka visokog profila, kao i otkrivanje političkih i industrijskih tajni.

„Remote“ ranjivost

Radnici na daljinu mogu biti ranjiviji na sajber napade jer često imaju manje bezbedne mreže i uređaje.

Država kao finansijer napadača

Napadači koje sponzoriše država postali su sve sofisticiraniji, a organizacije moraju biti svesne da ih ovi hakeri mogu ciljati.

Razvoj regulative

Države će sve više razvijati regulativu koju će morati da implementiraju kompanije ne bi li se povećala i nacionalna i ekonomska bezbednost koje sajber napadi takođe mogu da ugroze. Najveće diskusije se trenutno vode u vezi sa regulacijom AI, ali je nesumnjivo da će regulacije definitivno biti kako na nivou EU tako i u SAD.

« POVRATAK NA SADRŽAJ

BROJKE

197,4 milijarde USD vredela je industrija sajber bezbednosti u 2021.

Izvor: Next Move Strategy Department

657 milijardi USD biće vredna industrija sajber bezbednosti 2030.

Izvor: Next Move Strategy Department

10 milijardi USD je najveća procenjena šteta od sajber napada na niz organizacija i kompanija nazvanog NotPetya/ExPetr koji se desio 2017. i krenuo iz Ukrajine, a zatim se proširio širom sveta.

7,08 triliona USD je bila vrednost globalnog indikatora nazvanog „Procenjeni troškovi sajber kriminala“ u 2022.

Izvor: Statista

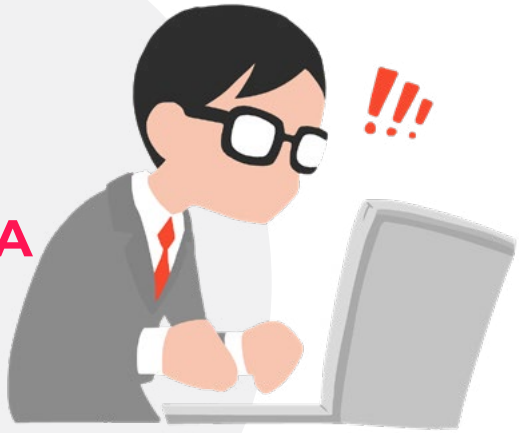
13,82 triliona USD biće vrednost globalnog indikatora nazvanog „Procenjeni troškovi sajber kriminala“ 2028.

Izvor: Statista

12% IT BUDŽETA

kompanije širom sveta u proseku troše na sajber bezbednost

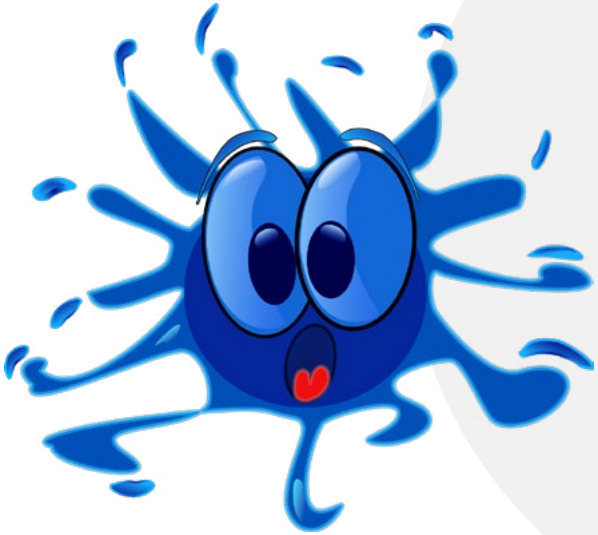
Izvor: Statista



98%

svih sajber napada koristi tehnike socijalnog inženjeringa.

Izvor: Proofpoint



4,45 miliona USD

prosečan godišnji trošak po kompaniji prouzrokovan korišćenjem socijalnog inženjeringa

Izvor: IBM

« POVRATAK NA SADRŽAJ

INTERNET-ZAVODNICI: LJUBAV ILI PLJAČKA?!

Kakve veze imaju kriza srednjih godina, i prevare preko interneta?
Prevare su postojale otkad je ljudskog roda, a društvene mreže su postale još jedan kanal kroz koji se prevarantima pružaju gotovo neograičene mogućnosti: do te mere, da danas postoje čitave firme koje koriste saznanja o ponašanju osoba u srednjim godinama, i koriste njihove uobičajene slabe tačke kako bi došli do materijalne koristi.
U te svrhe, prave se ozbiljni planovi, i čak koriste CRM softveri za vođenje "evidencije o klijentima" odnosno o potencijalnim žrtvama.

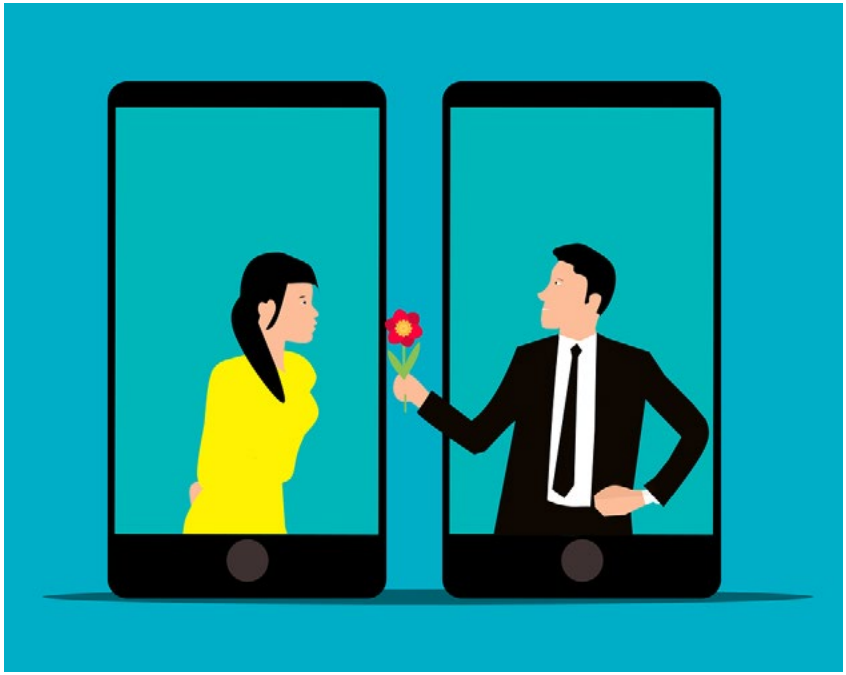
Statistike pokazuju da nešto više od 50 odsto žena u tzv. srednjim godinama oseća nedostatak samopouzdanja – zbog toga što se ne osećaju poželjnim kao ranije, zato što im slika u ogledalu više nije dopadljiva kao pre, zato što se bore sa osećajem da nisu u životu dovoljno postigle, zbog straha od budućnosti i svesti o sopstvenoj smrtnosti. I logično – željne su komplimenata i pažnje.
Slično je i sa muškarcima, ali su žene za nijansu lakša meta upravo zato što su empatičnije, imaju potrebu da pomažu i sažaljivije su: ako im servirate dovoljno tužnu priču, spremne su čak i da se žrtvuju kako bi pomogle ili utešile.
Tako se isprofilisao lik lekara ili IT inžinjera koji vodi poreklo iz zemlje susedne vašoj – tu su mu živeli roditelji pa ima veliku želju da se jednom vrati. Obično radi u ratom zahvaćenim područjima (dakle, human je), ili na naftnim platformama (što podrazumeva veliku zaradu). Udovac je, i ima ćerku koja je u internatu jer ne može sam o njoj da brine (potrebna mu je pomoć). Želja mu je da se vrati u zemlju svog porekla i da tamo pokrene biznis, a ko bi mu u tome bolje pomogao od vas...

Ume da pita, ume da sluša, a o sebi govori vrlo dozirano.

Dopisivanje je aktivno uglavnom dva puta dnevno po pola sata: navodno, pre početka radnog vremena, i za vreme pauze. U skladu sa vremenskom razlikom, navodi vas da svakodnevno planirate isto vreme za prepisku. Sve dok... ne proceni da je došlo vreme da "pokrene firmu" baš u vašoj zemlji. Pošto ne poznaje zakone vaše zemlje, a ni sa bankama ne stoji najbolje, logično je da se u to uključite, a zauzvrat je logično da budete suvlasnik. Jedino što će ubrzo nešto zaškripati sa njegovim papirima, ali će to rešiti tako što ćete mu vi upla-

titi na određeni račun vrlo malu sumu novca. I kao kod svakog "pecanja", mali iznos će vratiti, jednom a možda i dvaput, kako biste stekli poverenje. Zatim na red dolazi malo veći iznos, posle koga će nestati u vidu lastinog repa!

Ljubav ne zna za granice, pa ima slučajeva da su zaljubljene osobe prodavale sopstveni stan kako bi obezbedile polovinu za kupovinu novog, "zajedničkog" – bilo je potrebno "samo" da uplate novac na račun partnera-prevaranta kako bi on "regulisao papire". Ovome bi ozbiljno doprinelo i sažaljenje ka "jadnoj devojčici koja je ostala bez majke, i o kojoj treba neko da brine".



Iza ovakvih primera stoje ozbiljno strateški razrađene firme, gde su osobe koje traže žrtve dobro pripremljene da prepoznaju psihološki profil osobe koju pronalaze, njeno materijalno stanje na osnovu objava na društvenim mrežama, a često i njene želje i potrebe. O razgovorima se vodi detaljna evidencija, koja je olakšana upravo time što se vode u određeno vreme sa svakom žrtvom (može ih biti paralelno onoliko koliko je moguće tokom radnog vremena). Kao zemlja u kojoj prevarant-udvarač živi bira se ona koja bi odgovarala po vremenskoj razlici kako bi vreme javljanja bilo usklađeno i kako bi u plan komunikacije moglo da se upakuje bar petnaestak razgovora u toku dana.

Ovakvi "udvarači" obično imaju lepe fotografije na profilima na društvenim mrežama, ali ih na poslovnim mrežama nećete pronaći, baš kao ni na pretraživačima. Neće pristati na video poziv jer ćete u tom slučaju otkriti da to nije osoba sa fotografije: čak i ako obećaju, u poslednjem trenutku će nešto da iskrsne što će ih sprečiti. Ako počnete da sumnjate, spremni su da uključe i druge osobe u komunikaciju: ako vam, recimo, zatraže novac za lečenje, dostaviće vam i lekarske nalaze pa čak i "lekara" koji će posvedočiti. Razlozi za traženje novca mogu biti najrazličitiji, a ovo su bili samo neki od primera.

I ne zaboravite: čak i u ove teme sve više se uključuje veštačka inteligencija: to što ne zna dobro vaš jezik, deluje samo još autentičnije.

Naravoučenije:
Bolje je biti tužan i sam, nego tužan, sam i opljačkan!

« POVRATAK NA SADRŽAJ