Ste si istí, že nepomáhate útočníkom?

ANKETA

Až neuveriteľné prehrešky robia firmy v kyberpriestore, keď píšu o sebe. Takže – aké informácie by sa nemali zverejňovať nikdy a čo vám hrozí?

Tomáš Hettych,
člen predstavenstva, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Firmy často zverejňujú informácie o svojich zamestnancoch bez ich súhlasu alebo bez interných pravidiel. Najčastejšie fotografie, e-mailové adresy a mobilné čísla. Platí to aj pre skupinové fotky z teambuildingov a firemných pracovných stretnutí. Máloktorá firma to má formálne ošetrené.

Marek Zeman,
vedecký pracovník, Fakulta informatiky a informačných technológií STU Bratislava

Organizácie píšu veľmi otvorene o svojich interných nastaveniach a procesoch s cieľom čo najviac sa priblížiť klientom. Nerozmýšľajú nad tým, že všetky informácie čítajú aj útočníci. Zverejňovať by sa mali údaje k tovarom a službám. Komunikáciu klientov je potrebné smerovať do kontrolovaných kanálov, ktoré sú určené pre klientov a služby. Akúkoľvek inú komunikáciu je potrebné riešiť separátne a s porozumením.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti, Aliter Technologies

Je to jeden z najlepších príkladov, kde je zladenie informačnej bezpečnosti a biznisu a priori nemožné. Biznis by, samozrejme, najradšej marketoval a zdieľal všetko, aby si budoval miesto na sociálnych sieťach, weboch a v médiách. No a naopak, informačná bezpečnosť by najradšej nezdieľala žiadne informácie, aby dala potenciálnym útočníkom čo najmenej šancí. Tento rozkol je nutné z pohľadu informačnej bezpečnosti prijať a nastaviť v organizácii pravidlá, čo je možné zdieľať a čo nie. Vhodné je zdieľať len generické informácie, aktuálne novinky a eventy až ex post. Nezdieľať to, čo sa dá ľahko zneužiť: konkrétne názvy a verzie softvéru, systémov, cloudových služieb, kontakty na technických pracovníkov, podrobné prípadové štúdie, e-maily vedenia.

Ján Golais,
poradca bezpečnosti, Slovak Telekom

Spoločnosti často nevedomky zverejňujú rizikové technické informácie – typ operačného systému, používané platformy, sieťové schémy či mená a funkcie administrátorov, všetko v duchu „na webe sa riadne odprezentujeme“. Tieto informácie môžu výrazne zjednodušiť prácu útočníkom pri plánovaní kybernetických útokov. Zverejňovanie takýchto detailov je v rozpore s princípmi kybernetickej hygieny a odporúčaniami NBÚ SR. Spoločnostiam môžu byť za zanedbanie bezpečnostných opatrení uložené finančné sankcie. Nezverejňovať technické detaily ani interné informácie je základom prevencie a ochrany voči rastúcim hrozbám v kyberpriestore.

Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

Analýza otvorených zdrojov, čiže OSINT, je vynikajúci nástroj, ktorý používajú kyberzločinecké skupiny na dizajnovanie útokov. Nekoncepčná komunikácia, ktorá si mýli transparentnosť a exhibicionizmus, je vynikajúcim informačným zdrojom, či už ide bežné vyhľadávače, alebo automatizované nástroje. A do tohto sa počíta všetko – webové stránky, profily na sociálnych sieťach, verejné diskusie, vizibilita v médiách, povinné zverejňovanie v štátnych registroch, výročné správy aj fotky kamarátov.

Tomáš Valenta,
riaditeľ, Check Point Software Technologies

Odporúčam v kontaktných informáciách používať všeobecné e-mailové adresy namiesto konkrétnych osobných a predchádzať tak phishingu a sociálnemu inžinierstvu. Dobré je vyhnúť sa detailným informáciám o infraštruktúre a interných systémoch. Znižujeme tak riziko cielených útokov na konkrétne verzie softvéru alebo platformu. Rovnako neodporúčam zdieľať citlivé obchodné informácie a plány. Jednak kvôli kyberútokom, ale tiež kvôli konkurencii.

Jakub Berthoty,
advokát, Dagital Legal

Ak ako podnikateľ zverejníte svoj kontaktný e-mail alebo telefónne číslo pre záujemcov o vaše služby, tak podľa paragrafu 116 ods. 15 zákona o elektronických komunikáciách vás môže ktokoľvek kontaktovať s cieľom priameho marketingu cez email alebo SMS. Od prijatia zákona v roku 2021 hovoríme o tom, že táto prax nie je súladná s GDPR. Odporúčame podnikateľom brániť sa pred marketingom používaním kontaktných formulárov a zapísaním svojho telefónneho čísla na Robinsonov zoznam.

Jaroslav Oster,
predseda správnej rady, Preventista.sk

Jedným z rizík promovania sú nesporne sociálne siete. Malé i veľké firmy nedostatočne zadefinovanou politikou vytvárajú priestor pre vznik kritických diskusií, ktoré často dostanú celé PR do úplne opačnej polohy, než bol zámer. Agilný zamestnanec, ktorý neuváženou reakciou na kritické komentáre rozpúta vlnu zákerných a reputačne neželaných komentárov. A stačili jasne definované pravidlá zavedené do praxe.

Dominik Procházka,
riaditeľ odboru bezpečnosti, AGEL

Neodpustiteľným bezpečnostným prehreškom je prílišne zdieľanie, či už na weboch spoločnosti, alebo sociálnych sieťach. Zo získaných informácií sa dajú tvoriť personalizované kampane, slovníky pre lámanie hesiel, prípadne útočník dokáže získať prehľad o cieľovej infraštruktúre a ďalšom zabezpečení.

Jana Puškáčová,
vedúca špecialistka IT bezpečnosti, Slovnaft

V digitálnej ére nie je zdieľanie informácií prejavom transparentnosti, ale zraniteľnosti. Pred zverejnením akýchkoľvek informácií na internete by si firmy mali premyslieť odpoveď na otázku „Mali by sme?“, a nie len „Môžeme?“. Internet si viac pamätá, než odpúšťa.

Martin Orem,
hacker, Binary House

Každá zverejnená informácia nad rámec legislatívy musí byť firmou starostlivo zvážená. Popisy pracovných ponúk, profily zamestnancov na kariérnych sociálnych sieťach či verejné repozitáre zdrojových kódov môžu naviesť útočníka na použité technológie, prístupové údaje a štruktúru firmy. Vedie to k sofistikovanejším útokom napríklad cieleným phishingom, k únikom dát alebo k porušeniu GDPR.

Benjamin Würfl,
obchodný manažér, Eviden Slovakia

Z mojej skúsenosti si myslím, že firmy by o sebe nemali zverejňovať mená a kontakty zamestnancov, ale ani informácie o interných procesoch alebo používanom softvéri. Takéto informácie uľahčujú nielen útok „headhunterom“, ale aj útočníkom, ktorí plánujú phishingový alebo iný kyberútok.

Július Selecký,
senior technický špecialista, ESET

Firmy, ale aj samotní zamestnanci občas zverejňujú citlivé informácie, ako napríklad technológie, ktoré používajú, alebo detaily z projektov. Niekedy uvádzajú pracovné pozície ľudí či dokonca bezpečnostné opatrenia. Útočníci sa potom len pohodlne usadia a tieto údaje využívajú na phishing alebo cielené útoky. Riziká zahŕňajú únik dát, poškodenie reputácie či právne následky. Pri odhaľovaní niektorých detailov platí, že menej je niekedy viac.

Katarína Kročková,
právnička, Kročka & Partners

Po účinnosti GDPR som nachádzala na webových stránkach spoločností bezpečnostnú dokumentáciu, ktorú ja osobne považujem za dôvernú. Boli to rôzne bezpečnostné smernice a posúdenia vplyvu na ochranu osobných údajov. Vnímam to ako návod pre útočníkov. Príliš veľa zverejnených osobných údajov môže útočníkom výrazne uľahčiť realizáciu útokov založených napríklad na sociálnom inžinierstve alebo iných formách.

Marián Illovský,
audit partner, Cyllium

Zameral by som sa na informácie, o ktorých možno ani neviem, že ich zverejňujem. Zapamätajte si tu názov Open Source Intelligence – analýza informácií z verejne dostupných zdrojov. Existuje veľa OSINT nástrojov, ktoré umožňujú skontrolovať, čo je viditeľné na internete a hlavne z internetu. Mám na mysli zle nastavené zariadenia pripojené do internetu, ktoré môžu byť otvorenou bránou pre útočníka.

Richard Kiškováč,
generálny riaditeľ, Elkan

Úroveň hrozieb sa odvíja od zaujímavosti cieľa. Pokiaľ je organizácia strategicky zaujímavá, alebo pre takýto subjekt pracuje, je na mieste adekvátna obozretnosť. Verejné informácie slúžia útočníkom najmä pri prieskume cieľa a plánovaní útoku. Vyhľadávajú sa informácie o používaných technológiách, ako sú referencie na projekty, o zamestnancoch pre cielený phising, alebo o fyzických lokalitách či subdodávateľoch, ak ide o útok cez dodávateľa. Čím viac informácií je dostupných, tým lepšia je príprava a úspešnosť útoku.

Tomáš Zaťko,
CEO, etický hacker Citadelo

Vždy sa poraďte so svojím bezpečnostným tímom. Diskutabilné sú kontaktné údaje, roly a bežiace projekty, fotky a screenshoty, detaily interných procesov a pravidiel. S takýmito údajmi sú útoky formou manipulácie veľmi presvedčivé.

Marek Madžo,
technický riaditeľ centra kybernetickej bezpečnosti void SOC, Soitron

Okrem zmlúv a organizačnej štruktúry by mali organizácie zvážiť pracovné pozície a náplň, ktorú inzerujú. Tu sa dá zistiť, aké technológie sú používané, napríklad ako avizuje pozícia Network administrator Fortigate FW. Dá sa predpokladať stav kyberbezpečnosti, keď „hľadáme špecialistu na kybernetickú bezpečnosť pre zavedenie technických a procesných opatrení“, a niektorí pri pozícii Sysadmin – migrácia Win 2012 prezradia aj stav infraštruktúry.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť, Západoslovenská energetika

Aj tu platí, že diabol sa skrýva v detailoch. Vždy zvažujte mieru detailu poskytnutých informácií – bezpečnosť je o balanse medzi pridanou hodnotou a mierou rizika. A popravde? Bezpečnostný mini-selftest si robím zakaždým, aj keď odpovedám do tejto ankety.

Roman Varga,
manažér kybernetickej bezpečnosti, Dôvera zdravotná poisťovňa

V sektore zdravotníctva môže únik údajov spôsobiť priame ohrozenie životov pacientov. Hackeri môžu získať prístup k zdravotným záznamom, liečbe či plánovaným zákrokom, čo vedie k narušeniu starostlivosti, nesprávnej liečbe alebo oneskoreniu operácií. Preto je kľúčové chrániť IT infraštruktúru, šifrovať dáta a nezverejňovať citlivé detaily.

Štefan Pilár,
advokát, AK Signum

Firmy bez ohľadu na veľkosť zverejňujú aj citlivé údaje ako údaje zamestnancov, detaily interných procesov, IT infraštruktúry či jej ochrany. Následky môžu byť v podobe kyberútokov, úniku dát, pokút od regulátorov alebo zneužitia identity. Rozsah zdieľaných informácií je nutné vždy vážiť v kontexte potenciálnych rizík. Prílišná transparentnosť v kybernetickej bezpečnosti totiž môže byť drahá.

Ivan Makatura,
predseda, Asociácia kybernetickej bezpečnosti

V kyberbezpečnosti platí: čo nemusí byť verejné – to by nemalo byť verejné. Poskytnúť informácie o detailoch vlastnej infraštruktúry je to isté ako odovzdať „mapu“ vášho domu zlodejovi. Zverejnenie podrobností bezpečnostných opatrení znižuje ich účinnosť, pretože útočník ich veselo obíde. Ak to spojíte s ostentatívnym vychvaľovaním sa vlastnou odolnosťou, máte „zamiesené“ na problém

* **Robinsonov zoznam** je databáza telefónnych čísel, kde sa môžu zaregistrovať osoby, ktoré si neželajú byť kontaktované na účely priameho marketingu. Zriadil ho Úrad pre reguláciu elektronických komunikácií a poštových služieb a cieľom je ochrana pred nevyžiadanými volaniami a ponukami tovarov a služieb. Registrácia platí pre fyzické aj právnické osoby a je bezplatná.

www.nevyziadanevolania.sk