HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
25. – 27. APRÍLA 2025

Odborná spolupráca
NBÚ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Malinké krabičky, veľké problémy

TÉMA

Kamery, senzory, merače, smart zariadenia. Sú už všade. V energetike, doprave, zdravotníctve, v malých aj vo veľkých firmách. Zbierajú, analyzujú, posielajú a ukladajú dáta.

Pojem Internet of Things (IoT), teda internet vecí, sa používa už približne 25 rokov, od roku 2010 je štandardom v médiách, priemysle a technologických kruhoch. FOTO: DREAMSTIME

Prienik medzi IoT svetom a prevádzkovými technológiami sa označuje ako priemyselný internet vecí. Tento nový svet so sebou prináša veľa bezpečnostných výziev. Navyše, dlhý životný cyklus robustných prevádzkových technológií kontrastuje s rýchlym vývojom IoT zariadení.

Napred sa ísť musí

Firmy zvyčajne kupujú alebo vyvíjajú IoT zariadenia preto, aby priniesli nové služby, zvýšili efektivitu, zautomatizovali rutinné procesy a ideálne pritom ušetrili náklady.

„Problém nastáva vo chvíli, keď sa začne hromadiť čoraz väčší počet IoT zariadení – od senzorov cez kamery, aktuátory až po sofistikované zariadenia v logistike alebo vo výrobe. Boli navrhnuté s dôrazom na kompatibilitu a funkcie, nie na bezpečnosť," hovorí Rudolf Klein, produktový manažér Aliter Technologies.

Ale bežať netreba

Tu Rudolf Klein neľútostne pokračuje v opise prostredia. Zariadenia majú slabé alebo nemajú žiadne šifrovanie komunikácie, pretože snaha o ich „neviditeľnosť" v sieti by mohla narušiť ich kompatibilitu. Bežní používatelia chcú jednoduchú inštaláciu, moderné rozhrania a viditeľný pocit hodnoty za vynaložené náklady a tu „nudná bezpečnosť ustupuje požiadavkám".

Navyše aj výrobcovia často prestanú podporovať inovácie po pár rokoch a prestanú vydávať bezpečnostné aktualizácie. A ak sú dostupné, zariadenie je pripojené vzdialene a na aktualizácie spotrebuje drahé dáta.

Znamená to, že v sieti sa často nachádzajú zariadenia, ktoré sú buď na hrane bezpečnostnej politiky, alebo ju úplne obchádzajú. Pripojené sú však na tú istú sieť ako firemné počítače, servery, interné systémy a databázy vrátane citlivých informácií údajov.

Každá zraniteľnosť sa počíta

V priemyselných systémoch sa čoraz častejšie používajú IoT zariadenia ako súčasť prevádzkových technológií. Oboje sú často pripojené do siete, čo ich vystavuje kybernetickým hrozbám, alebo sú nositeľmi zraniteľností. Kompromitované IoT zariadenie môže byť vstupným bodom útoku na celý systém.

Bohuš Levčík, bezpečnostný špecialista so skúsenosťami v energetike viac ako dve dekády, uvádza príklad – ak smart elektromer alebo senzor vibrácií na turbíne nemajú zabezpečenú komunikáciu alebo sú zraniteľné, môžu byť zneužité ako vstupný bod do celej infraštruktúry prevádzkových technológií.

Tematika je čoraz širšia

„Pravdupovediac, téma IoT bezpečnosti ešte stále nie je vo firemnom prostredí vnímaná v celom svojom obsahovom spektre," hovorí Bohuš Levčík. Vo väčších firmách si odborníci uvedomujú riziká spojené s IoT, hlavne v kritických infraštruktúrach, ako je energetika či priemysel. V malých a stredných firmách je IoT bezpečnosť často podceňovaná. Opatrenia síce existujú, ale často nie sú systematické.

A aj tu zostáva hlavným problémom nedostatok odborníkov, ktorí by vedeli správne vyhodnotiť IoT hrozby v priemyselnom prostredí.

Varovania pribúdajú

Kyberbezpečnostný profesionál Michal Legerský rovnako poukazuje na posun za ostatné roky. „Veľa firiem sa v minulosti skôr zameriavalo na bezpečnosť IT prostredia a prevádzka a IoT boli skôr vnímané ako niečo, na čo sa neútočí, a preto ich nie je potrebné až tak chrániť. Súčasnosť nám, žiaľ, ukazuje že opak je pravdou."

Zvýšený počet kyberútokov na IoT zariadenia súvisí s ich širokým využitím a nárastom implementácie. Dôvodom je hlavne optimalizácia a zefektívnenie údržby strojných zariadení, čo predlžuje prevádzkyschopnosť a životnosť výrobných jednotiek a znižuje náklady. Tu Michal Legerský odvážne hovorí aj o tom, že medializácia incidentov a zdieľanie skúseností výrazne napomáha zvyšovaniu povedomia a je potrebné v tom pokračovať.

Ekosystém bujnie

Medializácia útokov aj tlak legislatívnych zmien spôsobujú, že vedenie osvietených firiem si uvedomuje, že kybernetické riziká nie sú len IT otázkou. „Majú priamy dosah na kontinuitu biznisu, reputáciu aj finančné výsledky," upozorňuje manažérka a konzultantka kyberbezpečnosti Viktória Blažíčková.

IoT zariadenia tu nie sú už len ako technické doplnky. Riziko narastá s ich rozšírením, pričom ich slabé zabezpečenie môže ohroziť nielen samotnú firmu, ale aj celý dodávateľský reťazec.

Viktória Blažíčková preto vysoko hodnotí, že kyberbezpečnosť sa dostáva čoraz vyššie na zoznam priorít top manažmentu. Za kľúčové však považuje, aby sa stala súčasťou strategického rozhodovania, nielen odpoveďou na incidenty.

Výnimky už nebudú

Tak ako sa prísne uplatňujú bezpečnostné opatrenia v prevádzkových technológiách, musia byť implementované aj na IoT zariadenia. Vedúci oddelenia bezpečnosti informácií Volkswagen Slovakia Marián Klačo tu prepája tieto dva svety.

Prevádzkové technológie majú oveľa dlhší životný cyklus ako IT technológie, sú často zastarané a pridružujú sa k tomu chýbajúce bezpečnostné znalosti. „Preto s implementáciou IoT bezpečnostných opatrení ide ruka v ruke aj potreba zvyšovania znalostí v tímoch spravujúcich prevádzkové technológie."

Ešte sme neskončili

Neriadenú kombináciu informačných a prevádzkových technológií môže ešte zhoršiť rastúce využívanie umelej inteligencie. Prepojenie týchto troch faktorov dramaticky zvyšuje kyberbezpečnostné riziká. „Útok na IT infraštruktúru sa môže rýchlo rozšíriť do prostredia prevádzkových technológií, čo môže viesť k zastaveniu výroby alebo poškodeniu zariadení," opisuje scenár kyberbezpečnostný expert Ivan Kopáčik.

Systémy, ktoré využívajú AI, môžu byť zneužité na automatizované útoky alebo manipuláciu rozhodovania. Nezabezpečené AI modely môžu byť ovplyvnené falošnými vstupmi, čo môže viesť k nesprávnym reakciám v riadiacich procesoch.

V globálnom priemysle pozorujeme duálny trend – technologický aj personálny. „Implementácia postkvantovej kryptografie a bezpečnostných systémov na báze AI ide ruka v ruke s budovaním špecializovaných tímov kybernetických expertov," dodáva Matej Michalko, predseda dozornej rady Asociácie kritickej infraštruktúry Slovenskej republiky.

Treba ísť ďalej

O bezpečnostných požiadavkách je nutné školiť tímy, ktoré technológie implementujú, aj tímy, ktoré sa o ne starajú. Toto široké spektrum zahŕňa integrátorov, dodávateľov, pracovníkov oddelenia plánovania aj údržieb.

Už pri zavádzaní prevádzkových technológií alebo ich obmene je potrebné pamätať aj na ich zabezpečenie. Napríklad v rámci nasadzovania urobiť takzvaný hardening, čiže niečo ako posilnenie infraštruktúry a myslieť na antivírusovú ochranu, kde to je vhodné. Tu Marián Klačo opäť pripomína mantru pre výber prevádzkových technológií Security by design.

čítajte **Správu o etickom hackingu 2024**

profesionáli našli **priemerne 6 zraniteľností** v každom testovanom projekte

VAROVANIE

96 percent kybernetických útokov v roku 2024 zneužilo zraniteľnosti, ktoré boli známe už predtým a mali aktualizácie k dispozícii

simulované útoky na zdravotnícke zariadenia ukázali **71 percent kompromitovaných zariadení** kvôli zraniteľnostiam starším viac než dva roky

Zdroj: Check Point Cyber Security Report 2025

Špeciálnu prílohu podporujú

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

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 25. – 27. APRÍLA 2025

Máte šťastie, ak to zistia „tí dobrí“

REPORT

V priebehu rokov spoločnosť Citadelo realizovala už tisíce bezpečnostných posúdení a penetračných testov po celom svete.

Ich zistenia reprezentujú pohľad kyberútočníka, ktorý skúma slabiny na prienik do systémov.

V roku 2024 „hackli“ tímy Citadelo takmer päťsto projektov a našli vyše 2 800 zraniteľností. Takmer polovica projektov obsahovala aspoň jednu zraniteľnosť vysokej alebo kritickej závažnosti.

Súhrnné údaje z testovacích postupov prezentujú v Správe o etickom hackingu, pričom nevyužívajú žiadne informácie z externých zdrojov. Vzniká tak originálny reprezentatívny materiál, ktorý podáva správu o stave kybernetickej bezpečnosti v rôznych segmentoch a oblastiach.

Aké zraniteľnosti obsahovali projekty?

6 zraniteľností priemerne v každom projekte

Kategorizácia zraniteľností

Kritické: okamžité a potenciálne katastrofálne technické riziká

Vysoké: veľmi vážne technické riziko, vyžadujúce si rýchle riešenie

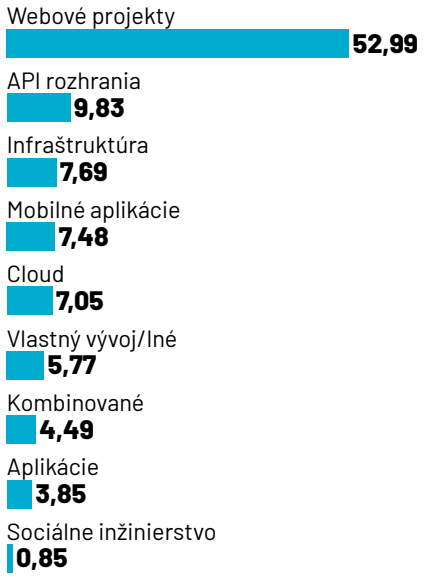
Stredné: značné technické riziko, mali by sa riešiť bezodkladne

Nízke: nízky technický dosah alebo veľmi nízka pravdepodobnosť, ale nemali by ostať bez povšimnutia

Upozornenie: odchýlky od osvedčených postupov, ktoré by sa mali odstrániť, aby bola zabezpečená optimálna bezpečnosť

Testované projekty podľa typu

(v percentách)



Testované segmenty

(v percentách)

Webové projekty

V digitálnej dobe sa webové stránky a webové projekty vyskytujú najčastejšie a vykazujú najvyšší počet zraniteľností v porovnaní s inými typmi projektov. V tomto segmente bol identifikovaný najvyšší počet kritických zraniteľností – strednej a vysokej závažnosti, v porovnaní s akýmkoľvek iným typom projektu.

Mobilné aplikácie a aplikácie

Rastúca popularita mobilných aplikácií prináša aj výrazný nárast zraniteľností v tomto segmente.

Infraštruktúra

V tomto segmente našli etickí hackeri druhý najvyšší počet kritických zraniteľností. Je to pravdepodobne spôsobené tým, že mnohé z testovaných projektov zahŕňali aj internú infraštruktúru, čiže nepripojenú k internetu, pri ktorej boli klienti menej opatrní ako pri externej infraštruktúre.

Zdroj: Ethical Hacking Report 2024, Citadelo

Cloud

Podobne ako v prípade internej infraštruktúry, aj klienti využívajúci cloud často trpia falošným pocitom bezpečia, čo vedie k vyššiemu počtu kritických zraniteľností.

Sociálne inžinierstvo

Záujem o testovanie sociálneho inžinierstva, najmä phishingu, vishingu, OSINT kampaní a útokov Redteamu poklesol. Vzhľadom na to, že sociálne inžinierstvo zostáva najbežnejším typom kybernetického útoku, varujú výskumníci pred odklonom od tohto testovania.

Varovanie:

Interné štatistiky Citadelo naznačujú, že už pri prvých testoch dochádza v dôsledku sociálneho inžinierstva v organizáciách k narušeniu bezpečnosti až v štyridsiatich percentách prípadov. Pravidelné školenie zamestnancov a opakované testovanie dokážu pomôcť udržať výsledky takýchto testov v jednociferných hodnotách.