HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA 23. – 25. AUGUSTA 2024

Odborná spolupráca

NBÚ

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Dnešná prevádzka zajtra nepostačí

TÉMA

Zoberme to od kritickej infraštruktúry cez priemyselné linky až po smart budovy. Bezpečnosť prevádzkových technológií je kľúčová pre každodenný život.

Sme priemyselná krajina vo svete, ktorý je v kybernetickej vojne. Ďalší rast bez zvyšovania kybernetickej odolnosti nie je možný. FOTO: DREAMSTIME

Pozrime sa na štruktúru hrubého domáceho produktu Slovenska či na to, kam chodíte do práce. Priemyselný park alebo kancelária v smart budove? Využívate služby zdravotníctva, dodávateľov energií, dopravu alebo chodíte do nákupného centra?

Všetky tieto oblasti sú už prešpikované technológiami. A umelá inteligencia, cloud a 5G prinášajú ďalšie výzvy pre bezpečnosť prevádzkových technológií. Alebo ako sa v brandži hovorí, pre OT (Operational Technology) bezpečnosť.

A kým povedomie o IT kyberbezpečnosti vo firmách či v štátnych organizáciách sa zvyšuje, „OT bezpečnosť si bude musieť túto bitku ešte len vybojovať“, hovorí Michal Srnec zo spoločnosti Aliter Technologies.

Dôležitá úloha

„Významnou oblasťou a aj výzvou pre bezpečnosť prevádzkových technológií je ich modernizácia,“ hodnotí trend Maroš Trnka, vedúci odboru informačných technológií vo Vodohospodárskej výstavbe.

V energetike sú napríklad v prevádzke riadiace systémy, ktoré už majú aj vyše dvadsať rokov. V tom čase mali vyrábané komponenty či samotné riadiace systémy dizajn často zameraný skôr na dlhú životnosť ako na bezpečnosť.

Bezpečnosť týchto systémov sa síce zvyšuje aplikáciou opatrení, ale Slovensko čaká rázny krok. Nové riadiace systémy v energetike už musia mať také parametre, aby spĺňali najprísnejšie požiadavky OT zabezpečenia.

Militarizácia technológií

Žijeme dobu, keď sa už samotné technológie, respektíve ich zneužitie stávajú zbraňou. Ako vidíme na východ od našich hraníc, ofenzíva sa začína útokom na kritickú infraštruktúru.

S novelizáciou zákona o kyberbezpečnosti, s rastúcimi útokmi a geopolitickou situáciou sa budú podniky čoraz viac zaoberať aj oblasťou OT bezpečnosti. „Nevyhnutne nás čaká praktické aplikovanie zmien, nástrojov zabezpečenia, segmentácie a stratégií bezpečnosti,“ predikuje Maroš Trnka.

A hneď upozorňuje na chronický neduh, čiže nedostatok kvalifikovaných odborníkov v OT bezpečnosti. Zároveň sa tým opäť otvorí otázka kvalitných dodávateľov.

Tradičný problém

Pre prevádzkovú bezpečnosť je totiž príznačná závislosť od dodávateľov špecializovaného hardvéru a softvéru. Riziko tretej strany znamená, že dodávatelia poskytujú, podporujú a často aj vyvíjajú špecifické technológie. Lokálna sieťová infraštruktúra je síce v rukách firmy, ale „kľúče od miešačky“ má dodávateľ.

Aj podľa skúseností kyberbezpečnostného odborníka Romana Čupku sa stáva, že prevádzkovateľ informačných systémov a kritickej infraštruktúry nemá dosah na bezpečnosť dizajnu komponentov. A musí sa spoliehať len na ich výrobcov.

Paradoxne, výrobcovia nepodliehajú takým prísnym legislatívnym rámcom ako prevádzkovatelia, a preto je dôležité, aby sa „kruh uzatvoril“. Zákon o kybernetickej odolnosti na úrovni EÚ by mal v budúcom roku definovať rámce zabezpečenia nielen pre výrobcov IT, ale aj pre výrobcov OT technológií. Tie majú zaistiť ich bezpečnostný životný cyklus prostredníctvom štandardov a opatrení.

> „VÝZNAMNOU OBLASŤOU A AJ VÝZVOU PRE BEZPEČNOSŤ PREVÁDZKOVÝCH TECHNOLÓGIÍ JE ICH MODERNIZÁCIA.
>
> **Maroš Trnka,**
> vedúci odboru IT
> Vodohospodárska výstavba

Posuňme sa ďalej

Prevádzkové technológie alebo IoT technológie si mnohí spájajú automaticky s priemyslom alebo výrobou a distribúciou energií. „Okrem spomenutých oblastí však nájdeme tieto technológie aj v zdanlivo netradičných prostrediach,“ upozorňuje obchodný špecialista KFB Control Tomáš Baksa.

Či už vojdeme do bizniscentra, nákupnej galérie, banky alebo na letisko, všade okolo nás sú inštalované desiatky a stovky malých pomocníkov. Menia náš život na pohodlnejší, príjemnejší a efektívnejší.

Nie všetky títo IoT pomocníci však boli navrhnutí vzhľadom na kyberbezpečnosť. Sú často pripojení cez rôzne aplikácie naprieč organizáciou a je pomerne ťažké ich segmentovať. Preto predstavujú atraktívne ciele pre útočníkov a hrozby pre organizácie.

Lebo elekroošiaľ

Konzultant pre kyberbezpečnosť kritickej infraštruktúry Martin Fábry upozorňuje v tejto súvislosti na kybernetickú bezpečnosť nabíjacích staníc. Je to nová téma hodná zamyslenia vzhľadom na fakt, že elektromobilita na Slovensku prudko stúpa a za posledný rok pribudla približne tretina nabíjacích staníc.

Aktuálne je viac ako dvetisíc verejných nabíjacích bodov pre elektromobily takmer v deväťsto lokalitách. Tieto „nabíjačky“ sú vybavené inteligentnými technológiami, čo otvára dvere potenciálnym kyberhrozbám. Kyberútoky tu môžu mať vážne následky, od ohrozenia bezpečnosti dopravy, narušenia siete až po vydieranie prevádzkovateľov.

A smart ošiaľ

Samotné označenie „smart budovy“ znamená, že sú vybavené pokročilými technológiami na riadenie a optimalizáciu. Patrí sem osvetlenie, vykurovanie, ventilácia, výťahy, bezpečnosť a ďalšie kritické funkcie.

„Na Slovensku aktuálne panuje situácia, že bezpečnosť smart budov sa skoro vôbec nerieši. Manažér bezpečnosti často ani netuší, že niečo také v budove má a mal by to riešiť,“ hodnotí stav Martin Fábry.

Ochrana systémov správy budovy je často na nízkej úrovni. A pritom kybernetická bezpečnosť smart budov je kľúčovým aspektom, ktorý nesmieme podceňovať. Na Slovensku je to ešte málo známa téma, ale v zahraničí je vnímaná veľmi intenzívne.

Už sa to deje

Systém riadenia budovy môže byť zneužitý napríklad na ťažbu kryptomien. Tomáš Baksa uvádza prípad, keď prevádzkovateľ zaznamenal nezvyčajne vysoké zaťaženie súčastí systému riadenia budovy. „Po aplikácii bezpečnostnej sondy v sieti bolo odhalené, že to spôsobuje neoprávnene inštalovaný softvér na ťažbu kryptomien, ktorý bol spravovaný z externej lokality,“ hovorí o úspešnej koncovke.

Ďalším príkladom bezpečnostného incidentu je výpadok chladiacich systémov v dátovom centre uprostred leta. V priebehu niekoľkých hodín spôsobil prehriatie serverov, čo viedlo k urgentnej požiadavke na ich odstavenie.

UPÚTAVKA NA ANKETU

Anketová otázka pre kyberbezpečnostných profesionálov:

Prečo sú naše domácnosti rajom útočníkov?

Odpovede na 10 až 60 sekúnd.

Špeciálnu prílohu podporujú

AC/DC, pivo a OT hrozby

VAROVANIE

Kyberútoky v priemysle môžu spôsobiť aj absurdné situácie, no následky sú vážne.

Príbehy kybernetických útokov na priemyselnú bezpečnosť môžu mať desiatky nečakaných podôb. FOTO: DREAMSTIME

Žiaden milovník piva by iste nepohrdol možnosťou degustácie v obľúbenom pivovare. Predstavte si však situáciu, keď popri vychutnávaní obľúbeného nápoja nezostane orosený len pohár, ale mokré budú aj vaše nohy. Kybernetické útoky v priemyselnom prostredí majú rôzne formy, a niekedy môžu na prvý pohľad pôsobiť naozaj komicky. V konečnom dôsledku však spôsobujú obrovské škody.

Nielen AI je kreatívna

Ak by ste sa AI spýtali na bizarné kyberbezpečnostné incidenty v OT prostredí, možno by ste aj vy dostali príbeh o tom, ako útočníci prenikli do systému riadenia výroby v nemeckom pivovare a manipuláciou spôsobili, že sudy s pivom začali pretekať.

Správa o tom, ako sa degustačná miestnosť plná návštevníkov zaplavila pivom, by zaiste obletela celý svet. AI si však vymýšľa – a žiaden podobný kybernetický útok sa v skutočnosti nestal. Tento, hoci vymyslený príbeh však poukazuje na vážne nedostatky zabezpečenia priemyselných technologických zariadení, ktoré sú reálne. A vďaka digitalizácii aj čoraz častejšie.

Potvrdzujú to aj dáta – v uplynulom roku zažilo kybernetický útok takmer 70 percent priemyselných organizácií. Nie je preto prekvapivé, že globálne výdavky podnikov na kybernetickú bezpečnosť v oblasti OT by sa podľa odhadov mali do roku 2028 zvýšiť o 70 percent a dosiahnuť 21,6 miliardy dolárov.

Svet sa digitalizuje

Tento očakávaný nárast výdavkov nasleduje po vlne narastajúcich útokov, ktoré cielia na zariadenia vystavené internetu v priemyselných odvetviach. Či už ide o zásobovanie pitnou vodou, energetiku, poľnohospodárstvo alebo výrobu, priemyselná automatizácia sa stala ich kľúčovou súčasťou. Kybernetická bezpečnosť preto už nie je voľbou, ale nevyhnutnosťou. No súčasný stav nepoteší – v porovnaní s IT systémami sú totiž OT systémy často podstatne menej chránené. A to z nich robí lákavý cieľ pre kybernetických zločincov.

Slovensko so svojou silnou priemyselnou základňou nie je žiadnou výnimkou a mnoho slovenských podnikov pravidelne zaznamenáva nejakú formu kybernetického útoku na svoje OT systémy. Hoci presné štatistiky nemáme, podľa analýzy spoločnosti Check Point Research cielili kybernetické útoky v prvom polroku 2024 na Slovensku najčastejšie na výrobný sektor. Týždenne ich bolo až 1 380.

Smiech cez slzy

Spomínaný príbeh o pive možno pôsobí humorne, no v realite môžu mať kybernetické incidenty katastrofálne následky. Spomeňme si na sabotáž iránskeho jadrového programu, keď vírus Stuxnet prevzal kontrolu nad riadením centrifúg v zariadeniach v neslávne známom jadrovom komplexe pri meste Natanz. Výsledkom bolo znefunkčnenie tisícky kritických a veľmi drahých strojov. Útočníci boli v tomto prípade údajne dokonca takí „vtipní“, že sa neuspokojili s ochromením jadrového programu krajiny, a k svojmu útoku pridali aj soundtrack. A čo sa hodí viac ako pieseň Thunderstruck od kapely AC/DC?

Áno, čítate dobre. Uprostred noci sa vraj na niekoľkých pracovných staniciach prehrávala pieseň, ktorú si, možno aj s pivom v ruke, len nedávno vychutnávali účastníci koncertu austrálskej legendy v Bratislave. Určite viac než pracovníci v napadnutom iránskom zariadení, ktorí sa tak museli pasovať nielen s technologickým chaosom, ale i nekontrolovateľným hlukom.

Koľko to celé stojí?

Finančné straty sabotáže iránskeho jadrového programu doteraz nie sú verejne známe, zrejme by boli aj ťažko vyčísliteľné. Náklady na vývoj tohto vírusového softvéru však údajne dosiahli až jednu miliardu dolárov.

O koľko však zvyčajne prídu obete pri iných útokoch? Ak sa pozrieme na najdrahšie incidenty za obdobie posledného roka, tie stáli napadnuté podniky desiatky až stovky miliónov dolárov. Kybernetický útok na OT systémy spoločnosti Johnson Controls bol vyčíslený na 27 miliónov dolárov, spoločnosť Clorox zas prišla v dôsledku útoku o 49 miliónov dolárov, strata až 450 miliónov dolárov je spojená s útokom na spoločnosť MKS Instruments.

Slovensko sa prebúdza

Aby sa zabránilo podobným astronomickým škodám, je nevyhnutné, aby si priemyselné podniky týchto rizík a dosahov boli vedomé a na ich eliminovanie či zmiernenie zaviedli príslušné bezpečnostné opatrenia. Podľa prieskumu spoločnosti Nozomi Networks z roku 2023 má len 40 percent slovenských priemyselných podnikov zavedené komplexné opatrenia na ochranu svojich OT systémov.

Aj keď v otázke kybernetickej bezpečnosti ide na Slovensku o posun k lepšiemu, myslíme si, že toto číslo je stále nízke. A útočníkom vysiela jasný signál: naše OT systémy majú veľký potenciál zraniteľnosti.

Bezpečná digitalizácia

Digitalizácia slovenských podnikov napreduje, no dôležité je, aby sa to dialo bezpečným spôsobom. Neopatrné pripojenie výrobných systémov a ich dostupnosť z internetu totiž môže viesť k novým rizikám, ktorých dôsledkom nie sú len spomínané finančné straty, ale aj narušenie výroby, poškodenie dobrého mena a narušenie kontinuity podnikania. Nové technológie, ako sú umelá inteligencia alebo 5G, ktoré predstavujú nové príležitosti, môžu taktiež znamenať nové vektory hrozieb pre OT infraštruktúru.

Preto je nevyhnutné, aby bezpečnosť išla ruka v ruke s technologickým pokrokom. Aby technologické inovácie boli prínosom, nie hrozbou.

Silvia Strežová,
void SOC, centrum kybernetickej bezpečnosti SOITRON

TREND

Len aby naše nadšenie nepredbehlo bezpečnosť

Zatiaľ čo smart budovy a elektromobilita prinášajú významné výhody v oblasti efektivity, komfortu a udržateľnosti, zároveň predstavujú nové ciele pre kybernetické hrozby.

Smart budovy

Inteligentné budovy sú smart aj preto, lebo sú vybavené pokročilými technologickými systémami na riadenie a optimalizáciu osvetlenia, vykurovania, výťahov, ventilácie, bezpečnosti a ďalších kritických funkcií. Kybernetická bezpečnosť smart budov je preto kľúčovým aspektom, ktorý nesmieme podceňovať.

Jednou z hlavných hrozieb je neoprávnený prístup k systému správy budovy. Hackeri môžu manipulovať s výťahmi, osvetlením či dokonca s vykurovacím systémom a klimatizáciou. Môže to viesť k narušeniu prevádzky, vysokým energetickým nákladom alebo dokonca k fyzickým škodám.

Bezpečnostné systémy, ako sú kamery a prístupové dochádzkové systémy, môžu byť znefunkčnené, čo zvyšuje riziko fyzického preniknutia do budovy. Ďalším rizikom je odstavenie napájanie v dátovom centra, čo môže mať ďalekosiahle následky na prevádzku.

Kyberbezpečnosti smart budov by sa mala venovať pozornosť, pretože z pohľadu ochrany je to zanedbaná infraštruktúra, ktorá nemá zavedené silné bezpečnostné opatrenia. Sem esenciálne patrí segmentácia sietí, pravidelné aktualizácie softvéru, šifrovanie komunikácie a dôkladný monitoring systému.

Rovnako dôležitá je aj vzdelanosť a školenie zamestnancov v kybernetickej bezpečnosti, aby sa minimalizovalo riziko ľudskej chyby.

Iba kombináciou technologických a organizačných opatrení môžu smart budovy plne využívať svoj potenciál bez toho, aby sa stali obeťou kybernetických útokov.

Nabíjacie stanice

S rastúcou popularitou elektrických vozidiel sa stáva kybernetická bezpečnosť ich nabíjacích staníc kľúčovou témou. Inteligentné technológie umožňujú monitorovanie a riadenie nabíjacieho procesu na diaľku, čo však otvára dvere pre potenciálne kybernetické hrozby.

Hackeri dokážu manipulovať s nabíjacím procesom, zneužívať osobné údaje, alebo dokonca narušiť elektrickú sieť, ak sú nabíjačky integrované do smart grid systémov.

Okrem toho môžu byť „nabíjačky“ použité ako nástroj na vydieranie prevádzkovateľov prostredníctvom ransomvéru, ktorý by zablokoval prístup k nabíjacím bodom.

Pre zabezpečenie kybernetickej bezpečnosti nabíjacích staníc je nevyhnutné implementovať silné bezpečnostné protokoly, ako je šifrovanie dát, pravidelné aktualizácie softvéru a autentifikácia používateľov.

Je dôležité, aby boli nabíjačky oddelené od iných kritických infraštruktúr a pravidelne monitorované pre identifikáciu a prevenciu potenciálnych útokov. Len tak môžeme zaručiť bezpečné a spoľahlivé využívanie nabíjačiek v rýchlo sa rozvíjajúcom trhu elektromobility.

Martin Fábry,
konzultant pre kyberbezpečnosť kritickej infraštruktúry Accura

S novými technológiami pribúdajú nové vektory kyberútokov. FOTO: DREAMSTIME

RIEŠENIA

Konvergencia, segmentácia, nulová dôvera. A nad tým dáždnik AI

Digitalizácia skladá do seba informačné a prevádzkové technológie ako puzzle. Odvrátená tvár tejto skladačky sú nové výzvy v bezpečnosti.

Povedzme si pravdu

Či už ide o priemysel, zdravotníctvo alebo energetiku, tradičné prevádzkové systémy neboli navrhnuté s ohľadom na kybernetické hrozby. S postupujúcou digitalizáciou sú však informačné a prevádzkové technológie čoraz užšie prepojené.

V súčasnosti sa preto čoraz viac dbá na zjednocovanie bezpečnostných politík a technológií, ktoré pokrývajú obe tieto prostredia.

Inšpirácia na dosah

Riešenia a postupy v oblasti kybernetickej bezpečnosti majú významný prínos aj v bezpečnosti prevádzkových technológií (operational technology). Alebo ako sa skrátene hovorí, v OT bezpečnosti.

Stále však platí, že OT systémy sú v priemyselných a kritických infraštruktúrach vystavené špecifickým hrozbám a tie si vyžadujú špecializované prístupy na ochranu.

Nikomu a ničomu neverte

Zero Trust prístup sa stáva neodmysliteľnou súčasťou aj v oblasti OT bezpečnosti. Tento prístup vyžaduje neustále overovanie identity a oprávnení každého zariadenia a používateľa, bez ohľadu na to, či sa nachádzajú vnútri alebo mimo siete.

Zero Trust architektúra tak predstavuje nevyhnutný nástroj na ochranu priemyselných riadiacich systémov pred modernými hrozbami. K trendom sa radí aj integrácia systémov na správu identity, integrácia Zero Trust Network Access a prístupy bez nutnosti používania hesiel.

Základným princípom pre ochranu však stále zostáva aj tu segmentáciu sietí. Umožňuje izolovať citlivé OT systémy od ostatných častí siete, čím sa minimalizuje riziko šírenia útoku.

Riziko s vysokou prioritou

S rastúcou hrozbou ransomvéru v kritickej infraštruktúre rastie aj dôraz na ochranu OT systémov. Zahŕňa to nielen detekciu a prevenciu útokov, ale aj rýchlu reakciu a zotavenie po útokoch.

Už aj bezpečnostní architekti na Slovensku si začínajú uvedomovať potrebu rýchlej reakcie a záložných systémov, ktoré môžu pomôcť zmierniť dosahy potenciálnych útokov.

Aj tu hrá AI prím

S prechodom na priemysel 4.0 sa čoraz viac údajov spracováva na mieste, kde sú generované, namiesto ich odosielania do centralizovaných cloudových systémov. Technológia Edge AI umožňuje využívať umelú inteligenciu na takzvanej edge úrovni, čiže priamo v zariadeniach. Umožňuje to rýchlejšie a efektívnejšie rozhodovanie v reálnom čase, čo je kľúčové pre tieto systémy.

Veľké jazykové modely sa čoraz viac využívajú aj na prediktívnu údržbu. Dokážu predpovedať zlyhanie zariadení a optimalizovať plánovanie, čím sa zvyšuje efektivita.

Stále všetko sledujte

Systémy využívajúce umelú inteligenciu a strojové učenie sa uplatňujú pri monitorovaní normálneho chodu a identifikácii odchýlok, ktoré by mohli signalizovať kybernetický útok.

Vzhľadom na špecifické vlastnosti OT systémov sa behaviorálna analýza a detekcia anomálií stávajú čoraz dôležitejšími.

Na druhej strane, AI môže byť zneužitá na vytváranie sofistikovanejších útokov a obchádzanie bezpečnostných opatrení.

Už to nezastavíme

Umelá inteligencia sa využíva aj na posilnenie bezpečnosti OT systémov, napríklad na automatizovanú analýzu kybernetických hrozieb, detekciu narušení a zabezpečenie rýchlej reakcie na incidenty. AI dokáže identifikovať komplexné vzory, ktoré by tradičné metódy mohli prehliadnuť.

Tieto trendy ukazujú, ako sa OT bezpečnosť a umelá inteligencia prelínajú a prispôsobujú výzvam, ktoré prináša digitálna transformácia priemyselných odvetví.

Pre komplexnú OT bezpečnosť je preto kľúčové kombinovať moderné technológie s dôkladným monitorovaním, so školením zamestnancov a silnými bezpečnostnými politikami.

Tomáš Vobruba,
vedúci bezpečnostný inžinier Check Point Software Technologies Slovakia

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 23. – 25. AUGUSTA 2024

Hrozby trvajú, obrana je vyspelejšia

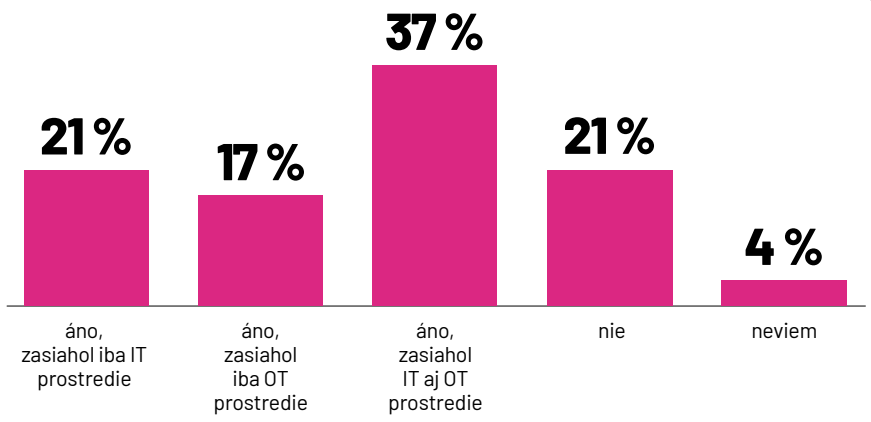
REPORT
Výročnú správu pod názvom Globálny stav priemyselnej kybernetickej bezpečnosti pravidelne publikuje spoločnosť Claroty.

Tento koncern sa zaoberá kybernetickou bezpečnosťou s dôrazom na ochranu priemyselných riadiacich systémov, prevádzkových technológií a kritickej infraštruktúry a ich riešenia sú často považované za štandard v tejto oblasti.

Prieskumná agentúra Pollfish oslovila na všetkých kontinentoch viacej ako tisíc odborníkov na IT a OT bezpečnosť a zmapovala ich názory a skúsenosti za rok 2023. Účastníkmi prieskumu boli bezpečnostní profesionáli z automobilového, chemického, potravinárskeho, ropného, plynárenského, papierenského, farmaceutického a biotechnologického priemyslu, z dopravy, vodného a odpadového hospodárstva, z oblasti spotrebných produktov, ťažby a materiálov, IT hardvéru, lesníctva a energetických služieb.

Ransomvérové útoky v OT prostredí sú na vzostupe a predstavujú vysoké náklady

Mala vaša organizácia skúsenosti s ransomvérovým útokom za posledný rok? (*2023)



Vplyv ransomvérových útokov sa v roku 2023 z IT prostredia presunul aj do OT prostredia. Nárast ransovérových útokov ovplyvňujúcich súčasne IT aj OT prostredie o 10 percent za dva roky je obzvlášť významný.

69 percent

zasiahnutých organizácií zaplatilo výkupné.

Ako ovplyvnili útoky prevádzku?

EXTRÉMNE	STREDNE	MINIMÁLNE	ŽIADNY DOSAH	ŽIADNY INCIDENT	NEVIE SA
12% odstavená prevádzka na viac ako týždeň.	**42%** napadnuté webové sídla alebo funkcionality a prevádzka odstavená niekoľko dní.	**21%** zaslahnutý web alebo biznis funkcionality.	**12%** prevádzka nebola prerušená.	**10%** organizácií.	**3%** organizácií.

Stúpa dopyt po poistení kybernetického rizika

80 % organizácií sa rozhodlo pre poistenie kybernetického rizika

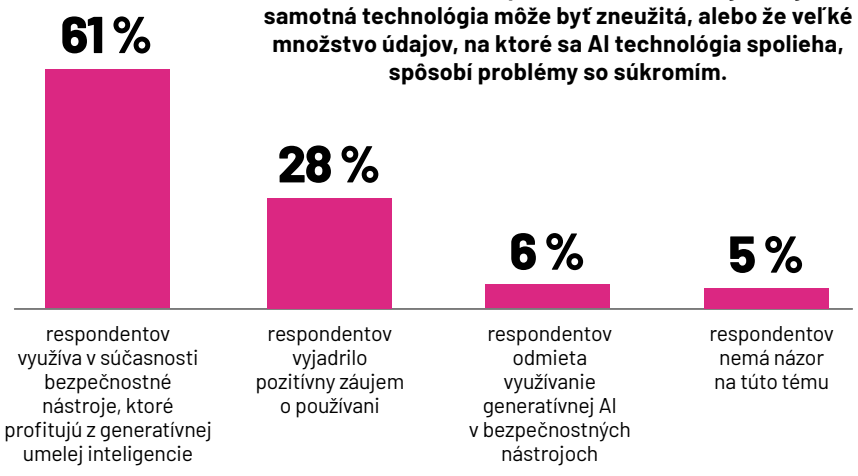
49 % poistených organizácií zvolilo pre prípad útoku poistné krytie vo výške pol milióna dolárov a viac.

Rastúce riziko ransomvérového útoku a súčasne rastúce finančné straty nútia organizácie proaktívne riešiť odolnosť a myslieť na riešenie následkov incidentov.

Využívanie generatívnej umelej inteligencie rastie

Využívanie generatívnej umelej inteligencie v priemyselnej bezpečnosti rastie, vzbudzuje však značné obavy o celkovú bezpečnosť.

Polovica progresívnych respondentov sa obáva, že útočníci budú manipulovať a klamať AI systémy, že samotná technológia môže byť zneužitá, alebo že veľké množstvo údajov, na ktoré sa AI technológia spolieha, spôsobí problémy so súkromím.



67 percent

organizácií, ktoré zažili ransomvérové útok, utrpeli finančnú stratu vo výške minimálne **100 000 USD**.

Väčšina finančných následkov ransomvérových útokov sa pohybovala v od 100 000 do 499 000 USD. Najvyšší počet respondentov v tejto kategórii je zo Severnej Ameriky, až 23 percent.

Progres odstraňuje nedostatky v procesoch a technológiách

Najvýznamnejšie výzvy v OT bezpečnosti

- posúdenie rizika
- riadenie aktív, zmien a/alebo životného cyklu
- manažovanie zraniteľností.

- Takmer polovica (43 %) respondentov uviedlo, že ich kľúčovou bezpečnostnou iniciatívou v roku 2024 je posúdenie rizika.

- Viac ako tri štvrtiny organizácií identifikuje zraniteľnosti „stredne" alebo „veľmi" proaktívnym spôsobom, čo je výrazný nárast v ostatných dvoch rokoch

- Viac ako tri štvrtiny respondentov v súčasnosti pristupuje k segmentácii siete „umierneným" alebo „vyspelým" spôsobom. Segmentácia siete je esenciálnym opatrením, aby sa obmedzil laterálny pohyb útočníka po sieti, ako aj prienik z IT do OT prostredia.

Míľniky OT bezpečnosti

Stuxnet (2010)
Malvér špeciálne navrhnutý na sabotáž iránskych jadrových zariadení. Šíril sa infikovanými USB kľúčmi zavlečenými do zariadení.

Oceliareň v Nemecku (2014)
Útočníci získali prístup do podnikovej siete pomocou spearphishingových e-mailov na zamestnancov. Presunuli sa na OT systémy a spôsobili fyzické škody na zariadení

BlackEnergy 3 (2015)
Malvér sabotoval priemyselné riadiace systémy a spôsobil masívny výpadok elektrickej energie na Ukrajine.

WannaCry (2017)
Ransomvér sa šíril v celom svete a postihol aj priemyselné systémy. Dôsledky útoku sa nachádzajú dodnes.

Triton (2017)
Komplexný malvér zameraný na systémy na riadenie bezpečnosti. Bol objavený v petrochemickom závode v Saudskej Arábii

Zavlažovací systém v Izraeli (2020)
Hacktivisti sa snažili zmeniť nastavenia zavlažovania a poškodiť plodiny.

Vodáreň v Oldsmare (2021)
Útočník získal vzdialený prístup do systému zariadenia a pokúsil sa zvýšiť hladinu chemických látok vo vode.

JBS Foods (2021)
Globálny ransomvérový útok narušil výrobu v Severnej Amerike a Austrálii, čo ovplyvnilo dodávky mäsa a ceny na trhu.

Industroyer2 (2022)
Malvér zameraný na vysokonapäťové stanice na Ukrajine. Útok bol včas zastavený

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 23. – 25. AUGUSTA 2024

Domácnosti sú rajom pre útočníkov

ANKETA

Mobily, počítače a smart zariadenia sú už súčasťou domácností. A pribúda spolu so zariadeniami aj povedomie? Preto sa pýtame profesionálov: Aká je najväčšia bezpečnostná diera v domácnostiach?

Ivan Makatura,
generálny riaditeľ, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Nejestvuje nič také ako „najväčšia" a už vôbec nie „jediná" bezpečnostná diera. Ide vždy o kombináciu zraniteľností, ktorá vedie ku konkrétnym hrozbám. Zjednodušene povedané: domácnosti sú z hľadiska bezpečnosti deravé ako ementál. Presnejšiu odpoveď na túto otázku poskytuje prieskum, ktorý vykonávame každý rok.

Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

Stručne povedané – domácnosti zničí slepá dôvera v technológie. Ak hovoríme o smart zariadeniach, tak vzhľadom na ich pripojenie do internetu je ich slabinou nedostatočné zabezpečenie. Môže viesť k narušeniu súkromia a zneužitiu domácej infraštruktúry útočníkom.

Tomáš Valenta,
riaditeľ, Check Point Software Technologies na Slovensku

Za obrovské riziko považujem nechránené mobilné zariadenia a správanie ich majiteľov. Či už dospelých, alebo aj detí. Zamestnancov už vzdelávame, musíme však aj naše deti a celú rodinu.

Jaroslav Oster,
predseda správnej rady, Preventista.sk

Smart zariadenia boli a v nemalej miere sú stále vyvíjané a vyrábané so zámerom minimalizácie ceny, čo prirodzene znižuje alebo vylučuje smerovanie na ich bezpečnosť. A najväčšia bezpečnostná diera v realite? Zastarané smart zariadenia a používatelia nevenujú pozornosť aktualizácii ich systémov.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC, Soitron

„Ocko, aké máme heslo na wifinu? Pýta sa kamoš z online hry." „Nechápem, že si ho už tri roky nevieš zapamätať, aj keď ho máme rovnaké ako na Netflix, Gmail a napísal som ti ho minule aj do poznámok v telefóne. Po kom si?!"

Henrich Šnajder,
manažér IT bezpečnosti, Orange Slovensko

Podceňovanie aktualizácií softvéru a firmvéru, nedostatočná segmentácia sietí a používanie zastaralých zariadení zvyšuje zraniteľnosť voči kyberútokom. Rizikom sú slabé alebo predvolené heslá a vystavenie zariadení priamo do internetu.

Richard Kišková,
generálny riaditeľ, Elkan

Najväčšia bezpečnostná diera v domácnostiach spočíva v stále veľmi nízkom bezpečnostnom povedomí jej obyvateľov. Pre to je príznačné aj ich správanie v online svete a minimálna ochrana. Často používajú starý, neaktualizovaný alebo nelegálny softvér, slabé heslá do systémov, aplikácií alebo do bezdrôtových sietí. Pravdou však je, že sa o tom reálne ani nemajú kde dozvedieť. Efektívne kampane v tomto smere v podstate neexistujú.

Jaroslav Ďurovka,
riaditeľ, Národné centrum kybernetickej bezpečnosti

Rizikom je, ak používate staré mobily a počítače, na ktoré nie sú aplikované bezpečnostné aktualizácie. Na zariadeniach by mali fungovať podporované operačné systémy alebo firmvér a mali by byť zapnuté automatické aktualizácie. Ohrozuje vás aj zlá konfigurácia routera, ktorým sa sieť pripája do internetu, a nechránená alebo zle nakonfigurovaná WiFi. Je dobré, ak sa váš poskytovateľ internetu stará aj o bezpečnosť routera – samozrejme, ak to robí dobre.

Ivana Lysinová,
konzultantka, Cyllium

Ako častý problém vnímam to, že domácnosti si nezmenia predvolené nastavené heslo na routeri. Je bránou k internej sieti domácnosti a narušiteľ tak dostáva „kľúče" k všetkým zariadeniam, ktoré sú do siete pripojené. V prípade moderných smart domácností tak môže získať prístup aj k otváraniu brán a dverí do domu.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti, Aliter Technologies

Nápadne lacné zariadenia pofidérnych výrobcov s diskutabilnou mierou zabezpečenia predstavujú samy osebe bezpečnostné diery. Najväčšou slabinou je však zvyklosť pripájať rôznorodé zariadenia bez rozmyslu do siete. Som presvedčený, že ak by poznali základne riziká, ktorým sa vystavujú, boli by obozretnejší. Pripojili by ste si domácu pestúnku do siete, ak by ste vedeli, že kamerový záznam nejde priamo na vaše zariadenia, ale aj cez servery výrobcu?

Július Selecký,
senior technický špecialista, ESET

Jedným z najväčších bezpečnostných „prúserov" v domácnostiach je používanie nedostatočne zabezpečených IoT zariadení. Sú to rôzne zariadenia ako kamery, termostaty, inteligentné zámky a hlasoví asistenti. Sú navrhnuté pre pohodlie a často im chýbajú spoľahlivé bezpečnostné funkcie, čo ich robí zraniteľnými hackermi a neoprávneným prístupom.

Dominik Procházka,
riaditeľ odboru bezpečnosti, AGEL SK

Hrozbou je kombinácia faktorov – predvolené nastavenia, absencia aktualizácií, skenovanie sietí útočníkmi a riziko zneužitia získaných dát. Spolu s pripojením domáceho zariadenia na firemnú sieť cez VPN to môže viesť k útokom aj na firemné prostredie.

Katarína Kročková,
odborníčka na ochranu osobných údajov, Kročka & Partners

Najväčšou bezpečnostnou hrozbou je nedostatočné povedomie o ochrane súkromia. IoT zariadenia môžu totiž zhromažďovať obrovské množstvo osobných údajov vrátane hlasových správ, informácií z domácnosti, dokonca zdravotné údaje. Všetky tieto dáta môžu byť zdieľané s tretími stranami bez vedomosti používateľa. Odporúčam preto v týchto zariadeniach neustále kontrolovať nastavenia súkromia.

Ivan Kopáčik,
bezpečnostný expert, Gordias

Dnes takmer každá domácnosť disponuje pripojením na internet a WiFi sieťou spájajúcou aj IOT prvky. S tým sú spojené bezpečnostné nastavenia, pravidelné aktualizácie softvéru a podobne. Pri zanedbaní opatrení dochádza k situácii, ako keby sme nezamykali dvere, iba ich privreli. Skôr či neskôr to niekto zneužije.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov, Tatra banka

Za bezpečnostnú dieru považujem nízke povedomie o informačnej bezpečnosti a bagatelizovanie dosahov nefundovaného správania v online svete. Bagatelizovanie trvá len dovtedy, kým sa člen domácnosti nestane obeťou. Rodina potom buď odmieta člena, alebo sa správa múdro, hľadajúc pomoc v odbornej komunite. Potrebujeme neustále vysvetľovať, prečo sa musíme vzdelávať.

Roman Čupka,
hlavný konzultant, Progress a CSO Istrosec

Problémom je klasický „element medzi stoličkou a klávesnicou". Jeho závislý vzťah k sociálnym médiám, ktoré poskytujú jednoducho stráviteľný obsah, spomienkové optimizmy a prehnaná dôverčivosť prehlbujú bezpečnostnú dieru. Tá vytvára efekt snehovej gule formou nevyužívania a odlivu inovačného kapitálu. Následkom sú dlhodobé negatívne dosahy na ekonomickú a kybernetickú odolnosť domácností.

Roman Varga,
manažér kyberbezpečnosti, Dôvera, zdravotná poisťovňa

Tak ako si ceníme súkromie, tak aj bezpečnosť nášho smart sveta by mala byť prioritou. Smart zariadenia v domácnostiach prinášajú pohodlie, ale aj riziká. Hrozbou sú nežiaduce prístupy, útoky na súkromie a kyberútoky. Je dôležité zabezpečiť silné heslá, pravidelné aktualizácie softvéru a využívať bezpečnostné funkcie poskytované výrobcami.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť, Západoslovenská energetika

Neaktualizovaný softvér či antivírus, inštalácie dostatočne nepreverených smart vychytávok, sťahovanie rôznych „užitočných" aplikácií, ktoré sú z kyberpohľadu často čiernymi dierami, používateľské (ne)zručnosti členov domácnosti a monoheslové praktiky. Dosť dôvodov na to, aby niečo zlyhalo, keď sa to najviac nehodí.