HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

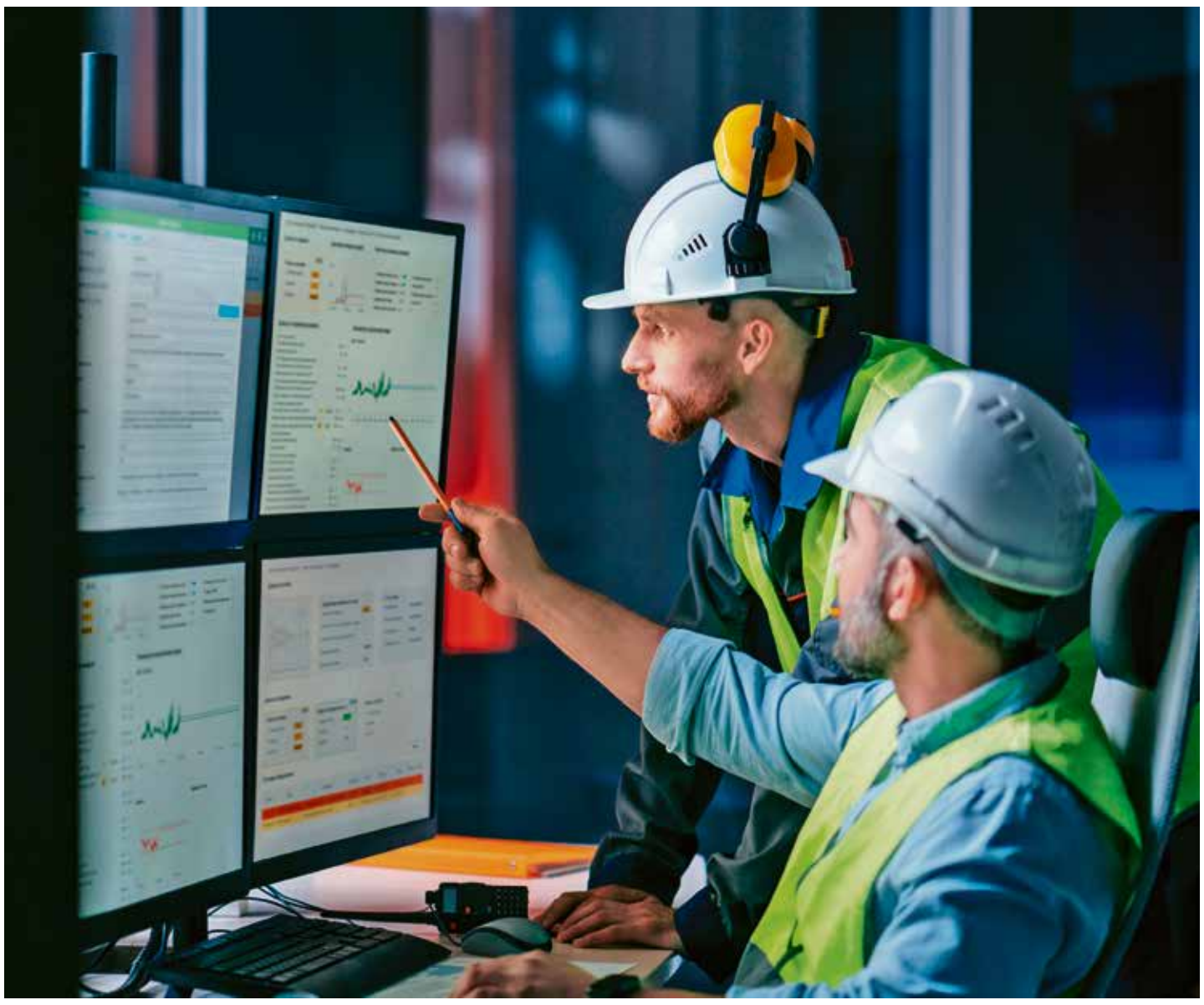
PIATOK – NEDEĽA
26. – 28. MÁJA 2023

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Zdvorilé mlčanie bezpečnosť nezvýši

TÉMA

Prevádzkové technológie predstavovali izolované ostrovčeky infraštruktúry. Priemyselná revolúcia 4.0 ich však digitalizovala a vytiahla „na svetlo“. Už ich vidia aj kyberzločinci a špionáž.



Bezpečnosť OT infraštruktúry sa stáva aj pre Slovensko jednou z priorít. FOTO: DREAMSTIME

Pri úspešnom kyberútoku na banku ide zvyčajne „len“ o peniaze. A, samozrejme, ešte o osobné údaje. V prípade kyberútoku na prevádzkové technológie môže ísť o život. Hovoríme o elektrárňach, vodárňach, tepelnom hospodárstve, ale aj o nemocniciach či laboratóriách.

Ak by kyberútok ochromil slovenský automobilový priemysel, straty by išli do astronomických súm. Stačí však aj predstava útoku na malú fabriku v „hladovej“ doline či rodinnú firmu piplanú dve desiatky rokov.

Dlhy z minulosti

Prevádzkové technológie kedysi neriešili kyberbezpečnosť, hovorí Marián Klačo, vedúci oddelenia bezpečnosti informácií Volkswagen Slovakia, a hneď to vysvetľuje. „Vo výrobe išlo predovšetkým o dostupnosť a nie o dôvernosť alebo integritu ich súčastí. Ale aj to je už prekonaný fenomén.“

Digitalizácia, potreba online monitoringu výrobných procesov, prediktívna údržba a príchod cloudových služieb spojili svety IT a OT bezpečnosti. Zároveň však hrozby, ktoré boli v minulosti doménou IT prostredia, sa usídlili aj v prevádzkových technológiách.

Už sa to nedá zastaviť

Útočníci sa dnes sústreďujú na spôsobenie fyzickej škody, ktorá je priamym dôsledkom poškodenia výrobného procesu. A majú stále veľa príležitostí.

Každým rokom sa nasadzuje množstvo IoT zariadení, ktorým chýbajú bezpečnostné prvky alebo ich nikdy ani nemali. To prinesie viac a viac útokov typu DDoS.

Skúsený OT bezpečák David Dvořák zo spoločnosti auditori.it identifikuje priemyselné prostredia ako veľmi zraniteľné proti útokom z dodávateľských reťazcov, napríklad cez ekonomické či komunikačné softvéry.

Manažér informačnej bezpečnosti zo Stredoslovenskej distribučnej Tibor Paulen už vidí dôsledky aj na Slovensku: „Manažéri v priemyselných odvetviach si začali na konkrétnych situáciách uvedomovať, že automatizácia a digitalizácia ich technologických procesov neprináša len výhody, ale aj riziká.“

Prekvapenie roka

Ak pošlete otázku k bezpečnosti prevádzkových technológií slovenským profesionálom v priemysle, polovica z nich sa „zašije“ alebo ospravedlní. Alebo neexistujú. To, že chýbajú profesionáli v kyberbezpečnosti so špecializáciou na OT bezpečnosť, je zúfalo naliehavý fakt.

Tohto roku sa však konalo prekvapenie – respondenti uvádzajú, že OT bezpečnosť sa dostáva čoraz viac do hľadáčika v regulácii a čoraz viac šéfov spoločností s priemyselným prostredím považuje kyberbezpečnosť za dôležitú. Ako však vzápätí dodáva David Dvořák, ešte stále to ani zďaleka neprekročilo kritickú masu.

Limitované nadšenie

Názory kolegov potvrdzuje aj Roman Čupka, hlavný konzultant Progress Software. „Pozorujem investície do základných pilierov zabezpečenia OT prostredia.“ Dochádza k segmentácii a monitoringu priemyselných sietí a snahu vidieť aj v zabezpečení koncových zariadení.

Sú to však len parciálne kroky a nereflektujú celkové potreby zabezpečenia tohto prostredia. Špecifickým príkladom sú nemocnice, teplárne či vodárne, ktoré by si zaslúžili väčšiu pozornosť. Mnohé organizácie trpia technickým dlhom, a ak nevedia využiť investície z plánu obnovy či eurofondy, je to až smutné. Základné nedostatky však ešte stále vidí Roman Čupka v kyberbezpečnostnom povedomí. „Ak nebudeme upozorňovať OT špecialistov a inžinierov na prijatie možných rizík spojených s touto problematikou, nepomôže ani legislatívny tlak.“

Všetci o nej hovoria

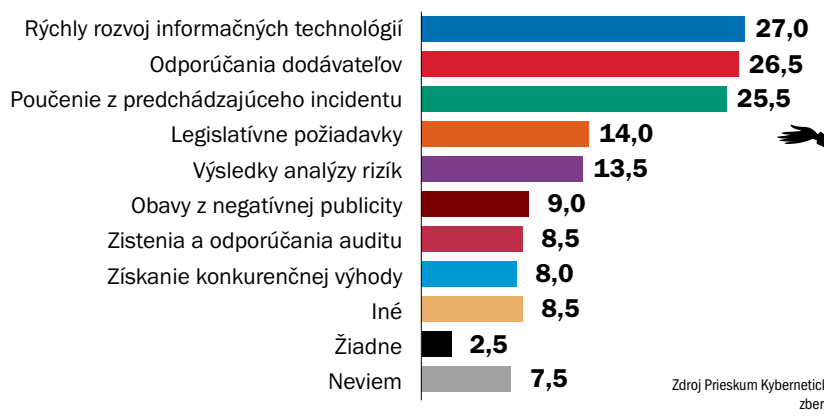
Toľko akcentovanou legislatívou je nová smernica o bezpečnosti sietí a informačných systémov NIS2. Ako upozorňuje riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT Rastislav Janota, rozšíri sa počet regulovaných subjektov aj v oblasti výrobných podnikov z rôznych sektorov.

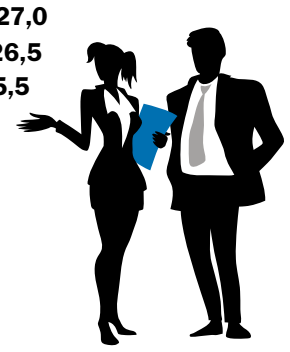
Odhadom tak pribudnú budúci rok na Slovensku stovky až tisícky nových povinných osôb, na ktoré sa budú vzťahovať existujúce aj nové povinnosti v zmysle zákona o kyberbezpečnosti.

Ide napríklad o výskum, výrobu zdravotníckych pomôcok a liekov, ale aj o výrobu, spracovanie a distribúciu potravín, výrobu počítačov, elektrických zariadení vozidiel či iných dopravných zariadení. Niektorí z nich už teraz argumentujú nedostatkom finančných prostriedkov a kvalifikovanej pracovnej sily.

> Počet regulovaných subjektov sa rozšíri aj v oblasti výrobných podnikov z rôznych sektorov.
>
> **Rastislav Janota,** riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Malé a stredné firmy na Slovensku:
Aké sú faktory, ktoré majú vo vašej organizácii najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti? (možnosť viacero odpovedí, v percentách)





Zdroj Prieskum Kybernetická bezpečnosť 2023 v SME podnikoch, zber dát: Agetnúra AKO, 24. 4. - 2. 5. 2023

Niečo do vlastných radov

Potrebných kyberbezpečnostných a OT bezpečnostných profesionálov tu nenájdeme ani do času, kým bude novelizovaný zákon o kyberbezpečnosti. Výrobné podniky sa budú musieť posunúť v nastavení. IT a OT profesionáli musia viac spolupracovať a komunikovať na všetkých úrovniach.

„Už aj samotné zadelenie manažéra kyberbezpečnosti do štruktúry vedenia spoločnosti hovorí o prioritách vedenia, ktoré treba rešpektovať,“ delí sa o skúsenosti Jana Puškáčová, manažérka útvaru Informačná bezpečnosť MOL IT & Digital GBS Slovensko. Bez podpory a angažovanosti top manažmentu, vlastníkov aktív a procesov, ako aj prevádzkovateľov systémov vychádzajú aj tie najlepšie odporúčania nazmar.

Úlohou bezpečnostného manažéra je a bude zvládanie bezpečnostných rizík. V kontexte pridanej hodnoty pre biznis však musí túto pridanú hodnotu zrozumiteľne komunikovať.

Povedzme si pravdu

Životný cyklus IT technológií sú dva-tri roky, v prípade prevádzkových technológií dve až tri desiatky rokov. V minulosti fungovali tieto prostredia viac-menej oddelene a občas si ťažko rozumejú.

Technológie a ľudské zdroje s vyšším počtom odpracovaných rokov často nie sú schopné a ochotné absorbovať najmodernejšie bezpečnostné riešenia a postupy. Implementácia je aj o potrebe dôverného poznania prostredia, v dôsledku čoho bezpečnostné projekty pre prevádzkové technológie môžu trvať dlhšie a vyžadovať si prípravu prostredia ovplyvňujúceho samotné technológie.

Záverom a prakticky

Ak by mal Marián Klačo vytvoriť pre kolegov zoznam technologických opatrení, okrem spomínanej segmentácie OT sietí by tam malo byť vypínanie nepotrebných aplikácií či služieb, odstránenie prednastavených hesiel, riadenie zraniteľností a patchovanie. Netreba však zabúdať, že základným opatrením zostáva riadenie aktív.

Okrem špecializovaných nástrojov pripomína kyberbezpečnostný profesionál Jozef Bálint z Alison Slovakia zabezpečenie súladu s priemyselnými štandardmi. V základom bezpečnostnom režime by podniky mali dbať na pravidelnú automatizovanú inventúru zariadení a ich zraniteľností, o nepretržitý monitoring sietí, detekciu hrozieb a anomálií v reálnom čase.

Aktuálnou výzvou je zabezpečenie viditeľnosti do vzájomne prepojených IT a OT sietí, automatizácia manuálnych procesov, správa zraniteľností, forenzná analýza a schopnosť reakcie na incident vrátane včasného varovania. Lebo ľahšie to už nebude.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · auditori.it · CHECK POINT · ESET · Progress · SOITRON · SK CERT Národné centrum kybernetickej bezpečnosti

Ako ochránime svet IoT zariadení?

Aký bezpečný je IoT svet?

- Riziká kybernetickej bezpečnosti pre priemyselné organizácie v roku 2022 naďalej rástli.
- Mesačne pribudne priemerne 115 zraniteľností
- Útoky sa zvýšili najmä na sektory priemyselnej infraštruktúry, akcelerovali aj v elektrických a vo výrobných vertikálach a v námornej doprave.
- Objem útokov pochádzala najmä od oportunistických útočníkov, ktorí cielili na kritickú infraštruktúru. APT skupiny sa špecificky fokusujú na infraštruktúru riadiacich systémov a prevádzkových technológií. Techniky, taktiky a procedúry, ktoré používajú, sú sofistikovanejšie.
- Rastú ransomvérové útoky na báze Ransomware-as-a-Service a útoky z dodávateľských reťazcov.
- Boli identifikované nové kmene industriálneho malvéru ako INDUSTROYER2 a modulárny malvér PIPEDREAM, ktorý predstavuje novú evolúciu útokov na infraštruktúru riadiacich systémov. Modulárnosť mu umožňuje zneužívať zraniteľnosti viacerých výrobcov s deštruktívnymi efektmi.
- Geopolitický konflikt na Ukrajine sa odzrkadlil v kyberpriestore aj v infraštruktúre riadiacich systémov, kde sme boli svedkami wiper útokov proti ukrajinskej kritickej infraštruktúre.
- V druhom polroku 2022 klesol celkový počet zraniteľností, čo je dôkazom, že výrobcovia vnímajú potrebu zabezpečiť kybernetic-ko-fyzické systémy, alokujú čas, ľudí a peniaze na plátanie softvéru a firmvéru.
- Počet zraniteľností rástol v oblasti prevádzkových technológií, tvorili 74 percent datasetu.

Trend 2023

- Presadzuje sa pojem Rozšírený internet vecí (Extended Internet of Things, XIoT). Zahŕňa všetky kybernetické fyzické zariadenia pripojené na internet v rôznych kontextoch, ako sú priemyselné zariadenia, čiže riadiace systémy aj prevádzkové technológie, pripojené zdravotnícke zariadenia, aj systémy riadenia budov a podnikový internet vecí.
- Rastie podiel XIoT cloudu v prevádzkových technológiách. Prináša to nové výzvy, pretože biznis čoraz viac tlačí priemysel do prediktívnej údržby, digitálnych dvojčiat a k lepšej analytike a efektivite výrobných procesov.
- **Eskalujú útoky na námornú a lodnú dopravu, LNG terminály a satelitné vesmírne systémy.**

Počet zraniteľností podľa typu zariadenia

(v percentách)

	1H 2021	2H 2021	1H 2022	2H 2022
IoT zariadenia	33	68	113	28
zdravotnícke IoT zariadenia	51		23	17
prevádzkové technológie	371	455	455	485
IT zariadenia	101	143	123	125
viacnásobné	95	93	33	22

Zdroj: Claroty Team82, State of XIoT Security: 2H 2022

Ako na Slovensku?

Pozitívne trendy badať u niektorých prevádzkovateľov základných služieb a kritickej infraštruktúry na Slovensku, kde sa segmentovala sieť, nasadili nové firewally alebo monitoring hrozieb v OT prostredí. Stále sme však na míle ďaleko od solídnej bezpečnosti v OT. Cloudové úložiská predstavujú pre prostredie prevádzkových technológií nové vektory útokov a výzvy, ktoré bude nutné zdolávať aj v slovenských podmienkach.

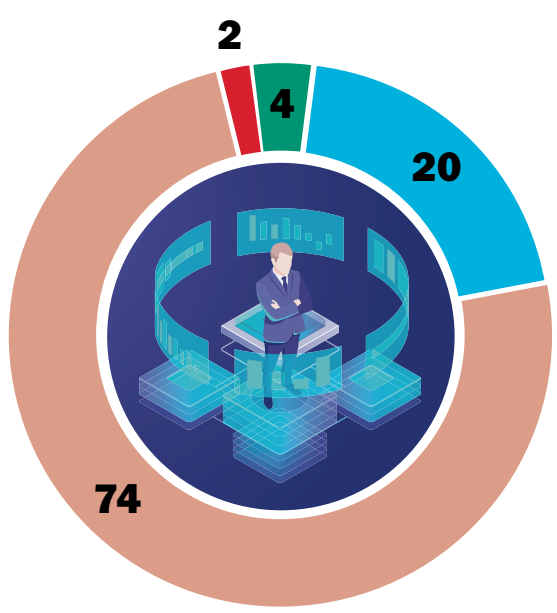
Martin Fábry,
konzultant pre kyberbezpečnosť kritickej infraštruktúry

Útočné stratégie

Spolu s rozrastajúcim sa využitím riešení v rámci Industry4.0 bude rásť aj počet kyberútokov na IoT zariadenia. Rovnako ako je geograficky rozmanitá komunikácia zamestnancov veľkých firiem, tak aj vo svete priemyslu sa komunikuje naprieč lokalitami. Takúto komunikáciu v nemalej miere zabezpečujú práve IoT zariadenia. Limitácie IoT zariadení, akými sú výkon procesora či veľkosť pamäte RAM, nevytvárajú veľký priestor pre ich dôkladné zabezpečenie, a aj preto sú často terčmi kybernetických útokov. Zapojenie IoT komponentov do reálneho výrobného procesu môže mať potom katastrofický dosah. Kritickým faktorom sú IoT zariadenia často zneužívané ako „sprostredkovatelia“ pre ďalšie kyberútoky.

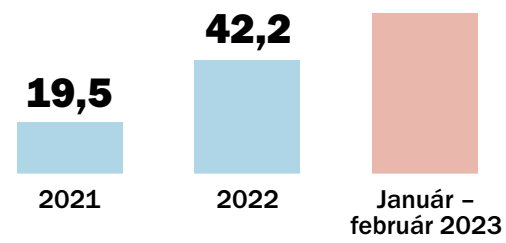
Michal Srnec,
CISO Aliter Technologies

Podiel zraniteľnosti podľa zariadenia (2H 2022 v percentách)



Zdroj: Claroty Team82, State of XIoT Security: 2H 2022

Priemerný počet útokov na organizáciu zameraných na IoT zariadenia týždenne



Najčastejšie útoky sú evidované na európske IoT zariadenia. Na jednu organizáciu týždenne smeruje priemerne až 70 útokov.

Zdroj: Threat Report spoločnosti Check Point Software Technologies

Aktuálne publikované XIoT zraniteľnosti

kritická	vysoká	stredná	nízka
82	242	112	7

Prečo treba investovať do OT

INVESTÍCIE

V oblasti kybernetickej bezpečnosti sa na účinné zabezpečenie organizácií často využíva koncept korunných klenotov.

Je nevyhnutné, aby Slovensko začalo hneď investovať do industriálnej bezpečnosti. SNÍMKA: XXXX

Korunné klenoty sú tie najkritickejšie a najcennejšie aktíva v organizácii. Hoci tento koncept sa často spája s informačnými technológiami, môžeme ho aplikovať aj na oblasť výroby. Tam to môžu byť kľúčové aktíva, systémy alebo procesy, ktoré sú nevyhnutné na prevádzku organizácie, jej konkurencieschopnosť a duševné vlastníctvo.

No a z hľadiska kybernetickej bezpečnosti na úrovni štátu je práve výrobný sektor korunným klenotom Slovenskej republiky, keďže ten predstavuje signifikantnú časť našej ekonomiky.

Škody rastú

Bezpečnostná správa spoločnosti Fortinet ukazuje, že 78 percent organizácií zaoberajúcich sa prevádzkou technológií (OT) zažilo aspoň tri útoky v priebehu posledných 12 mesiacov. Tie spôsobili škody na produktivite, príjmoch, dôvere v značku, na duševnom vlastníctve a fyzickej bezpečnosti. V roku 2021 bolo hlásených 64 incidentov v priemysle a priemyselných procesoch, pričom 22 z nich boli kyberútoky so skutočnými fyzickými následkami, čo predstavuje až 144-percentný medziročný nárast. A keďže je Slovensko krajina s rozsiahlym priemyselným a výrobným sektorom, musíme do bezpečnosti priemyselných technológií investovať hneď z niekoľkých dôvodov.

Ochrana kritickej infraštruktúry

Priemyselný a výrobný sektor často riadi kritickú infraštruktúru, ako sú elektrárne, čistiarne vôd, dopravné siete a výrobné zariadenia. Ochrana týchto aktív je kľúčová na zabezpečenie stabilnej prevádzky kritických služieb a celkovej ekonomiky.

Zníženie možných porúch

Kybernetické útoky na priemyselné systémy môžu mať vážne dôsledky vrátane prerušenia prevádzky, straty výroby a porušenia dodávateľského reťazca. Investovanie do OT bezpečnosti umožňuje krajine preventívne znižovať riziká spojené s kybernetickými incidentmi. Implementácia robustných bezpečnostných opatrení a postupov pomáha minimalizovať pravdepodobnosť a dosah porúch.

Ochrana ekonomickej konkurencieschopnosti

Priemyselný a výrobný sektor zohráva kľúčovú úlohu v ekonomickej konkurencieschopnosti krajiny. Kybernetické útoky zamerané na tieto sektory môžu mať ďalekosiahle dôsledky vrátane ekonomických strát, zníženej produktivity a poškodenia reputácie krajiny.

Ochrana národnej bezpečnosti

Priemyselný a výrobný sektor často zohráva strategickú úlohu pre národnú bezpečnosť. Napríklad výroba pre obranný priemysel, kritická infraštruktúra a citlivé odvetvia vyžadujú spoľahlivú ochranu pred kybernetickými útokmi.

Zmeny pred nami

Bezpečnosť výrobných podnikov má kritický význam nielen z hľadiska súčasnej legislatívy. Nová verzia európskej smernice NIS, transponovaná do slovenskej legislatívy prostredníctvom zákona o kybernetickej bezpečnosti, prináša prísne požiadavky na bezpečnosť a zvýšenie ochrany. Na Slovensku bude práve výrobný priemysel jednou z oblastí s najvyšším nárastom počtu subjektov.

> Investícia do OT bezpečnosti nie je nákladová položka, ale konkurenčná výhoda.
>
> **Stanislav Smolár,** manažér oddelenia bezpečnosti, Soitron

Okrem toho sa NIS2 viac zaoberá bezpečnosťou dodávateľských reťazcov, zjednodušuje povinnosti podávania správ a zavádza prísnejšie dohľadové opatrenia aj požiadavky na vynucovanie. Dodržiavanie NIS2 je pre výrobný priemysel nevyhnutné, pretože pomáha chrániť kritickú infraštruktúru pred kybernetickými útokmi.

Pohľad inou optikou

Investícia do OT bezpečnosti nie je nákladová položka, ale konkurenčná výhoda. Investovanie do OT bezpečnosti nám dáva možnosť vytvárať odolnejšie a flexibilnejšie systémy, ktoré sú menej náchylné na výpadky – úmyselné aj neúmyselné alebo kybernetické útoky.

Firmy s takýmto prístupom získavajú nielen väčší pokoj na duši, ale aj výhodu oproti konkurencii, pretože ich biznis bude fungovať a generovať tržby aj vtedy, keď výrobné linky konkurencie už budú nehybne stáť.

V praxi boli takéto situácie najviditeľnejšie počas rozsiahlejších útokov ransomvéru NotPetya, keď boli mnohé spoločnosti, nielen zo sveta industriálnych technológií, doslova prinútené takto zmeniť svoj pohľad a v súčasnosti sú lídrami investícií do bezpečnosti.

Varovanie aj sľubný začiatok

Slovensko, ako krajina závislá od výrobného sektora, stojí pred výzvou, a táto výzva neplatí len pre veľké priemyselné podniky. Aj malé a stredné podniky často podceňujú svoju atraktivitu pre útočníkov s presvedčením, že nie sú dostatočne zaujímavým cieľom.

Avšak malé a stredné podniky sú rovnako na radare kyberzločincov, pretože citlivé údaje majú hodnotu bez ohľadu na veľkosť spoločnosti. Navyše, často zaostávajú v moderných technológiách a ľudských zdrojoch kyberbezpečnosti, čo z nich robí relatívne ľahký terč pre útočníkov.

Podľa našich odhadov nebude problém zabezpečiť financovanie týchto investícii, keďže na to bude alokované dostatočné množstvo eurofondových financií.

Problémom však bude kritický nedostatok kvalifikovaných odborníkov, ktorí sa venujú tejto problematike. Práve preto by sme nemali čakať, kým nová legislatíva nadobudne platnosť, ale mali by sme už teraz postupne riešiť slabé miesta a nedostatky.

PORADŇA

Finančná podpora

Aká je možnosť financovania alebo spolufinancovania kyberbezpečnostných projektov z európskych fondov pre firmy a inštitúcie?

Aktuálne otvorila Európska komisia ďalšie výzvy na financovanie kyberbezpečnostných projektov.

Európske granty na kyberbezpečnostné projekty sú určené pre firmy, štátnu správu aj samosprávu, školy, univerzity, vedecké pracoviská a organizácie tretieho sektora. Tieto právne subjekty sa o financovanie uchádzajú samostatne alebo v konzorciách, pričom výška grantu je zväčša 50 percent, pre malé a stredné podniky až 75 percent rozpočtu.

V aktuálnej výzve budú podporené projekty na budovanie tréningových centier, stredísk bezpečnostných operácií (SOC), projekty s inovatívnymi riešeniami, podpora vzdelávania či implementácie smernice NIS2.

Keďže Digitálna Európa patrí medzi priamo riadené programy EÚ, výzvy sa vyznačujú rýchlym rozhodovaním, komunikáciou s Bruselom, jednoduchou administráciou a aj implementáciou. Úspešné projekty nepodliehajú kvótam a národným obmedzeniam, takže predstavujú rovnakú príležitosť pre všetkých.

Žiadatelia sa prihlasujú priamo podľa znenia výzvy a podávajú žiadosti online. Projektový formulár obsahuje ciele projektu, opis aktivít, harmonogram a finančný plán, pričom štúdie uskutočniteľnosti nie sú potrebné.

Webinár Ako správne napísať projekt a získať európske financovanie bude Kompetenčné a certifikačné centrum kybernetickej bezpečnosti organizovať počas júna.

Aktuálne výzvy na kyberbezpečnostné projekty sú otvorené od 25. mája do 6. júla 2023.

Valentína Michálková, riaditeľka odboru programov EÚ KCCKB

Otázky posielajte na adresu: **kyberporadna@mafraslovakia.sk**

TRENDY

Tridsať miliárd terčov na útok? Treba sa pripravovať už teraz

Bratislava – Podľa odhadov spoločnosti Statista bude do roku 2030 vo svete takmer 30 miliárd IoT zariadení. Kamery, snímače, vysávače aj interaktívne hračky zlepšujú život, ale prinášajú so sebou nové riziká a hrozby.

Celé zle

Aj keď odvšadiaľ znejú varovania, že IoT zariadenia sú pre kyberzločincov atraktívnym terčom, ich zabezpečenie je často v žalostnom stave. Zastarané operačné systémy, nezaplátané zraniteľnosti, nepravidelné aktualizácie či používanie prednastavených hesiel z nich robia ľahký cieľ.

A ani výrobcovia často nemajú príliš veľkú motiváciu investovať do zabezpečenia softvéru či hardvéru, najmä v prípade lacnejších produktov. Preto tu má stále dôležitú úlohu legislatíva a dôraz na dodržiavanie predpisov.

Zlomyseľné hračky

Jedným z motívov útokov na IoT zariadenia sú krádeže dát a špehovanie. Osobné údaje a prístupové oprávnenia sa výhodne predávajú na darknete, hacknuté kamery sa používajú na špionážne účely alebo vydieranie.

Útočníci vedia zneužiť zariadenie rôznymi spôsobmi, meniť jeho funkcie, spôsobiť na ňom škody, použiť ho na šírenie malvéru alebo ako nečakaný vektor útoku na podnikovú sieť. Výkonnejšie IoT zariadenia kyberzločinci zapájajú do botnetov, kde sú ich desiatky tisícov či milióny „zotročené“ a používané na nelegálne činnosti.

Kritické body

Keďže industriálne siete čoraz viac stavajú na priemyselné IoT zariadenia (Industrial Internet of Things_– IIoT), o to drastickejší dosah majú útoky, ktoré využívajú zraniteľnosti zariadení v prevádzkových technológiách.

Napríklad priemyselné mobilné smerovače a brány patria medzi najrozšírenejšie súčasti. Ponúkajú rozsiahle možnosti pripojenia a dajú sa bez problémov integrovať do existujúcich prostredí a riešení s minimálnymi úpravami. Avšak často trpia rovnakými neduhmi ako spomínané spotrebiteľské IoT zariadenia.

Aj takto sa útočí

Jedným z vektorov útoku na priemyselné siete, obľúbeným medzi ransomvérovými gangmi, je prienik na stránky cloud manažmentu IIOT zariadení za počiatočný prístupový bod. Tieto zariadenia sú ohrozené v dôsledku vstavanej VPN konektivity, čo následne umožní šírenie útokov v sieti, až napríklad do riadiacich centier a serverov SCADA (Supervisory Control and Data Acquisition).

V ostatnom čase je varovaním jedenásť veľmi vážnych zraniteľností v platformách pre cloudovú správu troch výrobcov priemyselných celulárnych smerovačov. Umožňovali vzdialené spustenie kódu, aj keď platforma nie je aktívne nakonfigurovaná na správu cloudu.

Zraniteľnosti sú také závažné, že aj keď ovplyvňujú iba zariadenia Sierra Wireless AirLink, Teltonika Networks RUT a In-Hand Networks InRouter, môžu mať vplyv na tisíce priemyselných IoT zariadení a sietí v rôznych sektoroch.

Detekcia? Už je neskoro

Dostať sa k zraniteľným zariadeniam môže byť ľahšie, ako sa zdá. Napríklad cez vyhľadávač Shodan sa dajú nájsť nezabezpečené IoT zariadenia, takže milióny domácností je možné špehovať ich vlastnými kamerami. Že je vaše zariadenie infikované a súčasťou botnetu, zistíte okrem iného aj poklesom jeho výkonu.

Hrozby a útoky je potrebné eliminovať ešte predtým, ako spôsobia škody, a preto je prevencia nenahraditeľná.

Jedným zo spôsobov je ochrana s Nano Agent technológiou. Umožňuje priamo v rámci lokálnej siete detegovať a v reálnom čase zastaviť sofistikované útoky a hrozby, vrátane zero-day zraniteľností, čiže tých, na ktoré ešte neexistujú záplaty.

Nano agent

Výrobcovia bezpečnostných technológií sa často stretávajú s tým, že koncoví používatelia nemajú skúsenosti a nevedia alebo nemôžu integrovať pokročilé prvky ochrany do svojich sietí.

V tomto prípade sa integruje vlastný bezpečnostný nano agent už priamo do výrobného cyklu. Ochranný prvok sa stáva súčasťou IoT/IIoT zariadenia už vo výrobe a pre koncového používateľa je úplne transparentný, podobne ako napríklad antivírusový softvér na pracovnej stanici. Predpokladá sa, že to bude motivátor pre všetkých výrobcov, aby takto začali integrovať bezpečnostné mechanizmy.

Ak sa teda zatiaľ spoliehame na štandardné mechanizmy a prístupy k ochrane IoT zariadení, už to nestačí. Princíp „security by design“ treba intenzívne presadzovať už v procese ich výroby.

Tomáš Vobruba, Check Point Software Technologies

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 26. – 28. MÁJA 2023

Povedzme si pravdu. Máme problém

ANKETA

Pýtame sa profesionálov: Ktorý sektor alebo ktorá profesia by potrebovali intenzívne precitnutie v kyberbezpečnosti? Úprimne a krátko poslali odpovede, podporené rokmi skúseností, faktmi a štatistikou.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC Soitron

Slovensko je v európskom Indexe digitálnej ekonomiky a spoločnosti 2022 na 23. mieste z 27. Ak chceme byť vyššie, čaká nás rozsiahla digitálna transformácia verejných služieb, zlepšovanie digitálnych zručností populácie aj rýchlejšia digitalizácia malých a stredných podnikov. A práve v nich sú dnes rezervy vo vnímaní aj v prijímaní bezpečnostných opatrení, čo bude mať s intenzívnou digitalizáciou nepríjemné dôsledky.

Rastislav Janota,
riaditeľ Národné centrum kybernetickej bezpečnosti SK-CERT

V Správe o kybernetickej bezpečnosti za rok 2022 Národný bezpečnostný úrad vyhodnotil ako absolútne najhorší sektor teplárenstvo. Lepšia, dokonca o dosť, je verejná správa a potom o trochu lepšia je doprava. Tieto údaje korešpondujú aj s mojím pozorovaním pri dennej práci s incidentmi. Ale nedá mi a rád by som povedal, že najlepší sektor je plynárenstvo, nasledovaný bankovníctvom a elektronickými komunikáciami.

Vincent Karovič,
prodekan pre IT, Fakulta managementu Univerzity Komenského v Bratislave

Školstvo a ešte raz školstvo. Učitelia síce majú predstavy o hrozbách pri odosielaní citlivých údajov cez súkromnú mailovú adresu alebo cez četové aplikácie, ale aj tak to robia. Často nemajú iné komunikačné možnosti so zákonnými zástupcami žiakov. Zamestnávatelia zväčša neposkytujú služobné telefóny ani zabezpečené emailové schránky. Aplikácia EduPage je síce rozšírená, no menej využívaná ako četové aplikácie alebo nezabezpečené emailové účty. Táto oblasť nie je zo strany zriaďovateľa často doriešená.

Roman Čupka,
hlavný konzultant Progress Software a CEO Synapsa Networks

Platí základné pravidlo, že človek je najslabším článkom v kyberbezpečnosti. Na druhej strane môže byť ten istý človek aj tým najsilnejším článkom. Preto by mal každý používať návyky z fyzického sveta a myslieť bezpečne aj v digitálnom priestore. Pokiaľ každá organizácia a aj jednotlivec prevezmú túto zodpovednosť, je veľká šanca na zvýšenie odolnosti proti akýmkoľvek kyberhrozbám.

Martin Oczvirk,
riaditeľ odboru informačnej bezpečnosti a certifikácie Úrad na ochranu osobných údajov

Každý sektor by mal venovať dostatočnú pozornosť ochrane svojich dát. Do úvahy musí brať hlavne špecifiká svojho odvetia. Osobne si myslím, že štátny sektor má prístup k najväčšiemu rozsahu osobných údajov a citlivých dát, a preto vzdelávanie od úradníka až po vrcholových pracovníkov štátu je nevyhnutné a musí byť povinné.

Ján Andraško,
SOC Manažér Binary Confidence

V kyberbezpečnosti nejde o sektory alebo profesie. Ide o to, aby vzdelávanie nebolo určené len „sekuriťákom“, ale všetkým zamestnancom, ktorí vo firme využívajú IT prostriedky. Inak sa aj naďalej bude stávať, že finančný riaditeľ naletí na phishing a účtovníčka zaplatí podvrhnutú faktúru.

Jaroslav Oster,
predseda Správnej rady Preventista.sk

Nárast incidentov často prerastajúcich hranicu trestného práva, výsledky interných aj externých auditov jasne poukazujú na skutočnosť, ktorá môže generovať obvyklé klišé „každý sektor“. Kategorizácia – kto koľko, je však oveľa náročnejšia. Ak by som mal vyzdvihnúť dva kľúčové, tak určite zdravotníctvo z dôvodu vysokej citlivosti a rizikovosti a školstvo ako okamžitú investíciu do budovania ľudských kapacít kyberbezpečnosti.

Andrej Žucha,
generálny riaditeľ ALISON Slovakia

Zvýšenú pozornosť si zaslúžia priemyselný a akademický výskum a vývoj. Sú pre organizácie cenné zdroje a kyberútoky, ktoré cielia na krádež duševného vlastníctva, môžu spôsobiť veľké straty. Výskumníci a vývojári by mali byť vyškolení v kyberbezpečnosti, aby ochránili inovácie, dáta a know-how pred neoprávneným prístupom a zneužitím. Výskumné inštitúcie a vývojové oddelenia by mali posilňovať kyberbezpečnosť a zaviesť prísne opatrenia na ochranu výsledkov výskumu.

Tomáš Zaťko,
CEO, etický hacker Citadelo

Ako prvé mi ihneď napadlo zdravotníctvo. Ale tam to je zároveň najmenej reálne. Ako druhé – výroba. Chemická, potravinárska a akákoľvek iná. A tam to reálne je. Zdravotníctvo ešte stále ostalo v komunizme – s úplným centrálnym plánovaním a bez možnosti využívať spätnú väzbu trhu. Prežíva a nemá kultúru investovať do niečoho zdanlivo vedľajšieho, ako je kyberbezpečnosť. Platí to hlavne pre štátne nemocnice, súkromné to už seriózne riešia.

Tomáš Hettych,
viceprezident, ISACA

Zo sektorov je najviac zanedbaná tepelná energetika, verejná správa a zdravotníctvo. Pričom nejde len o nedostatok peňazí na vzdelávanie alebo implementáciu opatrení. Problémom je dlhodobá ignorácia problematiky kyberbezpečnosti a podceňovanie rizík. A z pracovných pozícií alebo rolí by vzdelávanie najviac potreboval stredný a vyšší manažment. Teda tí, ktorí rozhodujú, vlastnia a riadia procesy a riziká v organizáciách.

Pavol Sokol,
vedúci CSIRT-UPJS Univerzita Pavla Jozefa Šafárika v Košiciach

Keďže pôsobím v oblasti vzdelávania, upriamil by som pozornosť na profesiu učiteľa. Jedným z hlavných problémov, ktorým čelíme v oblasti informačnej a kybernetickej bezpečnosti, je nedostatok kvalifikovaného personálu na rôznych pozíciách. Na zvýšenie tohto počtu nie je potrebné len kvalitné materiálne zabezpečenie, ale aj odborne zdatní učitelia, ktorí budú viesť svojich žiakov v tejto oblasti.

Tomáš Valenta,
riaditeľ Check Point Software Technologies na Slovensku

Celkovo o vzdelávaní hovoríme veľa, ale stále je to málo. Je otázne, či to postačuje a čo sa reálne robí. Lebo zásadný pokrok zatiaľ nevidím. Ale je to úloha nás všetkých. Ak by som mal vybrať jeden alebo dva sektory, zameral by som sa na opatrenia v zdravotníctve, kde môže ísť mnohokrát o život, a potom na vzdelávanie mladých ľudí v školách, kde o život určite ide.

Richard Kiškováč,
generálny riaditeľ Elkan

Na základe skúseností vidím dlhodobý nedostatok kompetencií v oblasti riešenia bezpečnostných incidentov. Rýchlo a správne zareagovať na kybernetický útok vyžaduje špecifické, komplexné znalosti, ako aj zohratý tím. Iba dôkladná analýza postupu útočníkov je základom pre správne vyriešenie incidentu a prijatie potrebných opatrení, aby sa podobný incident neopakoval. V tejto oblasti, žiaľ, stále zaostávame.

Jakub Berthoty,
advokát Dagital Legal

Sektor justície pracuje s veľmi citlivými dátami občanov, najmä orgány činné v trestnom konaní a súdy. Ich kyberbezpečnosť a súlad s predpismi na ochranu osobných údajov by mali byť prioritou. Úniky zo spisov do médií sú nemysliteľná vec, ktorú akosi tolerujeme.

Ivan Kopáčik,
bezpečnostný expert Gordias

Intenzívnejšie vzdelávanie, ešte pred prijímaním opatrení, by potrebovali primárne zákazníci ako takí. Kybernetická bezpečnosť sa stala zaujímavou obchodnou komoditou. Bez znalostí „čo to je“, „prečo to potrebujem“, „v čom mi to pomôže“ a podobne zákazník síce vynaloží finančné prostriedky, ale môže zakúpiť pre seba zbytočnú službu alebo produkt. Naletí. A keď to zistí, jeho nechuť riešiť kyberbezpečnosť to len prehĺbi.

Michal Ďorda,
audítor kybernetickej bezpečnosti, Auditori.it

Na pravidelnej báze vidíme, že vybrané subjekty štátnej a verejnej správy nevedia dostatočne ochrániť a zabezpečiť spracúvanie osobných údajov, zdravotných informácií a iných citlivých informácií o občanoch. Nevedia ani poskytovať dôveryhodné a dostupné elektronické služby občanom tejto krajiny. Nečudujme sa potom, ak nám šikovní a múdri odchádzajú žiť do zahraničia a využívať tam služby. Napríklad do Estónska.

Ivan Makatura,
generálny riaditeľ Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Vykonali sme prieskum v malých a stredných podnikoch o kybernetickej bezpečnosti a neveriacky krútime hlavou. Suverénne najviac „stratení“ v problematike sú štatutári organizácií. Akoby ich kybernetická bezpečnosť doslova obťažovala. V podstate to isté, žiaľ, vyplýva aj z výsledkov auditu vo veľkých organizáciách. To je prekvapivé zistenie, pretože digitálne zručnosti by mali byť elitnou vlastnosťou.

Pavel Nechala,
advokát, Nechala and partners

Budíček potrebujeme všetci, ale z hľadiska závažnosti dosahov sú to zdravotnícke zariadenia. Nesystémové riadenie a investičné dlhy vytvárajú zvýšené riziko práve v zdravotníctve. A to, že útoky prídu a budú rozsiahle, nám preukazujú iné európske štáty s lepšie pripravenými nemocnicami.

Martin Fábry,
konzultant pre kyberbezpečnosť kritickej infraštruktúry, Accura

Ransomvérový útok Black Basta na energetický konglomerát Hitachi Energy (ABB) ukázal, že útok cez dodávateľský reťazec na OT dodávateľa v priemysle a energetike môže mať dramatické globálne dôsledky, ak sa ransomvér začne šíriť k zákazníkom. Tento scenár sa tu nenaplnil, keďže mnoho spoločností servisné VPN spojenia s týmto dodávateľom okamžite deaktivovalo. Bezpečnosť prevádzkových technológií je celosvetovo zanedbaná oblasť. V blízkej budúcnosti však môžeme čeliť novátorským útokom s rozsiahlymi dosahmi.

Ján Grujbár,
generálny riaditeľ Aliter Technologies

Všetky.

Zuzana Motúzová,
advokátka Motúzová & Lacko advokátska kancelária

Jednoznačne štátny sektor a zdravotníctvo. Slovensko dnes čelí bezprecedentným kybernetickým a informačným hrozbám v dôsledku vojny na Ukrajine. Naši úradníci a štátni zamestnanci potrebujú byť dôsledne pripravení.

Miroslav Ilavský,
zodpovedná osoba na ochranu osobných údajov Centrum vedecko-technických informácií SR

Slováci si, žiaľ, nevedia chrániť svoje súkromie ani sa správať bezpečne v kyberpriestore. Je to dlhodobo zanedbaná oblasť. Riešením je systémové vzdelávanie. Začať treba u detí na školách a pokračovať na všetkých úrovniach vzdelávania, ako aj u zamestnancov štátnych a verejných inštitúcií a firiem. Riešiť to treba celoplošne a systematicky. Akékoľvek skratky v tomto prípade fungujú iba čiastočne.

Miroslav Chlipala,
partner Advokátska kancelária Bukovinský & Chlipala

Z hľadiska zodpovednosti a právnych následkov je úlohou štatutárov a vedúcich zamestnancov byť lídrami, motivátormi a budovateľmi kultúry kybernetickej odolnosti. Exponenciálny rast hrozieb a incidentov jednoznačne ukazuje, že kyberbezpečnosť nestačí iba delegovať. Každý štatutár musí pochopiť nezastupiteľnú úlohu v budovaní a udržiavaní kybernetickej odolnosti vo svojom „orchestri“!

„Je možné konštatovať, že stav kybernetickej bezpečnosti sa výrazne líši v závislosti od sektora. Hlavným zdrojom dát pre zhodnotenie pohľadu na jednotlivé sektory netvoria len výsledky auditných správ, ale aj zhodnotenie aktivít jednotlivých ústredných orgánov.“

Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2022