HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA 25. – 27. FEBRUÁRA 2022

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Keď je infraštruktúra pod útokom

TÉMA

Ešte v minulej dekáde to bol výborný triler, dnes je to realita kúsok za hranicami. Ochromenie infraštruktúry je bolestivým nástrojom kybernetickej vojny aj zdrojom rastúcich príjmov vydieračských gangov.

Napriek tomu, že sme priemyselná krajina, OT bezpečnosť sa u nás nikde nedá vyštudovať a venuje sa jej iba malá pozornosť. SNÍMKA: DREAMSTIME

Prevádzkové technológie tvoria nervovú sústavu priemyslu a kritickej infraštruktúry. V ostatnej dekáde komunikujú s manažérskymi systémami a zberajú dáta z vonkajšieho prostredia. Operational Technologies – OT sú tak čoraz viac vystavené nástrahám online sveta.

OT bezpečákov sú stovky, vyznajú sa v jadrových reaktoroch, vo vodných turbínach, v montážnych linkách aj celých priemyselných komplexoch. Na pracovnom trhu sú vzácni a majú desiatky rokov praxe. Pravdou však je, že ich prudko prepadla digitalizácia a internet vecí. Dokonca rýchlejšie, ako boli schopní absorbovať v množstve povinností.

Jedným klikom

V ostatných rokoch sa prevádzkové technológie dostávajú z izolácie. Stojí za tým postupná digitalizácia aj snaha o zefektívnenie ich manažovania. Mnohé priemyselné riadiace systémy sú pritom zároveň zastarané a niektoré neboli aktualizované aj celé roky.

A tak aj pani účtovníčka v rafinérii, ktoré klikne na phishingový mail, môže „dať dole“ celú sieť čerpacích staníc na kontinente. Nie hneď. Útočníci si počkajú. Čas na odhalenie malvéru v infraštrukúre môže byť rádovo desiatky až stovky dní.

Všetko naraz

Aktuálne je najväčšou hrozbou pre OT svet ransomvér, ktorý pácha škody na dennom poriadku. Ale, ako upozorňuje bezpečnostný konzultant a architekt Martin Fábry, v tých uvedomelejších organizáciách sú hrozby zároveň najlepším drajverom implementácie preventívnych opatrení.

Neuvedomelé organizácie, ktorých je podľa Fábryho skúseností majorita, sa môžu chystať na počítanie finančných a reputačných škôd, lebo skôr či neskôr ich ransomvér dostane. Ďalším extrémom sú firmy, ktoré sú po útoku a naďalej ignorujú opatrenia a hrozby z toho vyplývajúce. Ransomvérové gangy tieto spoločnosti milujú a rady sa k nim vracajú. K pesimistickým predpovediam prispieva aj rastúca geopolitická tenzia medzi Východom a Západom.

Následky uvidíme

Certifikovaný etický hacker Ľubomír Kopáček definuje minulý rok ako „kybernetickú apokalypsu“. Jeden príklad za všetky – živelný home office. Nepripravené firmy poslali domov nepripravených zamestnancov a ani OT operátori sietí, žiaľ, neboli výnimkou. Alebo dodávateľský reťazec – môžete mať najlepšie zabezpečené siete a systémy, stačí jediný dodávateľ s výnimkou a celý koncept bezpečnosti sa vám zrúti. Špeciálnu pozornosť si preto zaslúži manažment tretích strán, kde je často nepostačujúca kyberhygiena pri prevádzke a údržbe alebo v projektovom riadení.

Najslabšie stránky

Profesionáli sa vzácne zhodujú, že najväčším problémom kybernetickej bezpečnosti, či hovoríme o prevádzkových alebo informačných technológiách, je a bude človek. Útok na technické zariadenia bez predchádzajúcej interakcie s človekom je strata času a komplikácia. Najefektívnejšie je útočiť na cieľový systém zneužitím zamestnanca s notorickým nedostatkom povedomia, znalostí a skúseností. Osobitnou kapitolou je chýbajúci a účinný OT monitoring kybernetických hrozieb, nedostatočná segmentácia siete, strata kontroly nad prenositeľnými médiami a nedostatok kvalifikovaného personálu na prevádzku týchto technológii.

Výstražné svetlo

Dlhé roky bola synonymom bezpečnosti energetika, avšak aj to už je podľa Ľubomíra Kopáčka do značnej miery minulosťou. Prispeli k tomu prestupy medzi IT a OT sieťami, rôzne „inteligentné“ technológie, neschopnosť detekcie incidentov, nulová vizibilita aj nedostatok odborníkov.

> Neuvedomelé organizácie sa môžu chystať na počítanie finančných a reputačných škôd, lebo skôr či neskôr ich ransomvér dostane.
>
> **Martin Fábry,** bezpečnostný konzultant a architekt

Mimoriadnu pozornosť si na Slovensku aj vo svete zaslúžia zdravotníctvo, výroba a distribúcia vody a tepla, doprava, inteligentné mestá a výroba.

Július Peterec z Mondi SCP mu sekunduje technickými faktami: „Prioritou je zavedenie monitoringu prevádzky v OT sieťach. Po integrácii s IT monitoringom by tento centrálny systém mal poskytnúť nepretržitú viditeľnosť do siete.“ Ako infraštruktúrny odborník však kladie dôraz aj na pravidelné vzdelávanie OT špecialistov v prevádzkach a ich povedomie v kyberbezpečnosti.

Známe bolesti

Peter Škorvánek, vedúci sekcie infraštruktúry a špecialista na IT bezpečnosť v spoločnosti KIA Slovakia, ide k podstate problému: „Povedomie odborníkov z prostredia prevádzkových technológií o IT bezpečnosti je veľmi nízke a nerozumejú jej potrebe.“

Všetci oslovení špecialisti sa zhodujú v tom, že kultúrne rozdiely medzi IT a OT ľudmi sú stále citeľné, čo v mnohých prípadoch limituje ochotu spolupracovať. Martin Fábry na to používa metaforu: „V lepších rodinách riešia obranu do hĺbky IT a OT spolu, a to preventívnou formou, zatiaľ čo v horších rodinách sa bavia až po útoku a navzájom sa obviňujú, čia to bola chyba.“

Učebnice nestíhajú

Neustále zmeny v kybernetickom prostredí ovplyvňujú zameranie školení, témy tréningov či konferencií aj spôsob a formu vzdelávania. Špecializovaná platforma Qubit Academy preto organizuje výročné prestížne podujatie aj intenzívne workshopy pre malé skupiny. „V oboch prípadoch sa kladie dôraz na efektívne riešenie problematiky a aktívnu diskusiu,“ prízvukuje Katarína Gamboš.

GLOBÁLNY STAV PRIEMYSELNEJ KYBERBEZPEČNOSTI 2021

IT a OT profesionáli v kritickej infraštruktúre

80 PERCENT
prišlo do kontaktu s ransomvérom

47 PERCENT
reportovalo priamy dosah na priemyselné riadiace systémy

60 PERCENT
zaplatilo výkupné

z toho viac ako polovica zaplatila výkupné vyše
500 000 USD

Dôvody
- digitalizácia prevádzkových technológií
- vzdialená práca
- nedostatok kvalifikovaného kyberbezpečnostného personálu

Zdroj: prieskum spoločnosti Claroty 2021 Odolnosť uprostred disrupcie

Špecifiká OT segmentu, ktorými sú technologické procesy a nevyhnutná dostupnosť, vplývajú aj na pravidelné vzdelávanie ľudí. Musí byť nielen kontinuálne, špecificky zacielené, ale aj zamerané na efektívne a promptné reakcie pri bezpečnostných incidentoch.

Okrem toho, žiadny profesionál na bezpečnosť nevznikne iba absorbovaním teoretických vedomostí. OT bezpečáci by mali čo najviac trénovať na simulátoroch a zažiť „bojové hry“ na reálnych OT zariadeniach, čo je luxusná a drahá záležitosť.

Musíme to riešiť

Potrebný počet odborníkov na OT bezpečnosť nie je a nebude, určite nie v dohľadnom čase. „Nie je to slovenský fenomén, my sme sa iba zobudili päť rokov po zvyšku sveta,“ hovorí Ľubomír Kopáček. Pomôže nám iba kombinácia systematického a zmysluplného vzdelávania, certifikácií, výmena skúseností a vedomostí v bezpečnostných komunitách a najmä prax, veľmi veľa praxe.

Ako dobrý príklad uvádza Július Peterec susedné Česko. Kvalitný systém vzdelávania s priamym prepojením na súkromný sektor tam umožnil vznik množstvu startupov, ktoré dosiahli v kyberbezpečnosti svetové renomé.

Ruka v ruke s tým však musí ísť celé nastavenie školstva a materiálové vybavenie, aby už od začiatku dokázalo pritiahnuť deti k technickým predmetom. Ale to je už iný ťažký a dlhý príbeh.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

auditori.it · ESET · Progress | Flowmon · Qubit · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 25. – 27. FEBRUÁRA 2022

Tieto argumenty sa dajú iba zažiť

ANKETA

Profesionáli dostali náročnú úlohu. Presvedčiť talentovaného človeka, aby sa stal ich kolegom či kolegyňou. Aká je najpríťažlivejšia profesionálna a osobná motivácia pracovať v kybernetickej bezpečnosti?

Diana Legdanová,
vedúca úseku bezpečnosti Východoslovenská energetika Holding

Je to najvzrušujúcejšia a najsexi oblasť tejto dekády v biznis zmysle slova. Lebo je záhadná, nepredvídateľná, dynamická a expanzívna, sofistikovaná a zároveň komplexná, ochraňujúca aj investigatívna. Je prierezová a významná na globálnej úrovni. Na druhej strane sa priamo dotýka a je veľmi blízko každého človeka. Tieto atribúty robia kybernetickú bezpečnosť pre mňa atraktívnou z dlhodobého hľadiska.

Ľubomír Kopáček,
konateľ iseco

Možno to mladým ľuďom len nevieme dostatočne atraktívne „predať“. Ak má niekto chuť učiť sa neustále niečo nové, pracovať s najnovšími technológiami, cestovať a ešte aj nadštandardne zarábať, tak mu poradím jediné – venuj sa kybernetickej bezpečnosti.

Ivan Makatura,
generálny riaditeľ Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Nájsť talentovaného a technicky zdatného človeka je ako hľadať ihlu v kope sena. Naše vysoké školy medzeru nezaplnia ani za ďalších desať rokov. Ak by som však mal šťastie pri hľadaní a mal by som presvedčiť nerozhodného, môj argument býva: poctivá práca na strane spravodlivosti s možnosťou dlhej kariéry, odborného uznania a nebudem tajiť, že aj slušných príjmov. Dopyt práce je vyšší ako ponuka.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií Volkswagen Slovakia

Hlavnou motiváciou, prečo pracovať v kybernetickej bezpečnosti, je možnosť neustáleho osobného aj odborného rastu. Penetrácia IT/OT technológiami v rôznych odvetviach je čoraz komplexnejšia. Bezpečnostné opatrenia a technológie by mali na tieto trendy reagovať. Nové technológie, napríklad cloudové služby, prinášajú nové výzvy, ako aj nové hrozby. Čiže „kybersekuriťák“ sa nemusí obávať žiadneho stereotypu.

Rastislav Janota,
riaditeľ, Národné centrum kybernetickej bezpečnosti SK-CERT

Pre mojich kolegov a mňa má práca v kybernetickej bezpečnosti rozmer národnej bezpečnosti, ochrany záujmov Slovenskej republiky, firiem aj občanov. Zvyšovanie odolnosti rôznych slovenských subjektov je preto najdôležitejším cieľom všetkého, čo robíme. A pre tieto ciele sa snažíme neustále hľadať nových kolegov s rovnakou motiváciou – pomáhať v oblasti kybernetickej bezpečnosti.

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

Ak by som niekoho presviedčal, aby pracoval pre našu organizáciu, s platovým argumentom by som asi neobstál. Neprekonateľnou motiváciou je však prístup k veľkej škále a rôznorodosti bezpečnostných incidentov. Naše kompetencie v kybernetickej bezpečnosti umožňujú prístup k palete rôznorodých technológií aj k vytváraniu budúcnosti ochrany osobných údajov.

Ján Grujbár,
generálny riaditeľ a predseda Predstavenstva Aliter Technologies

Pre niekoho je motiváciou možnosť podieľať sa na odhaľovaní a zneškodňovaní kybernetických zločinov, pre iných je to vzrušujúca investigatívna práca a pre niekoho potreba byť neustále o krok vpred. V našej firme sme pochopili, že KB je kreatívny interdisciplinárny odbor, v ktorom je dôležité zamestnancom ponúknuť priestor a prostriedky na neustály odborný rozvoj, vďaka čomu môžu patriť medzi špičku.

Dominik Procházka,
riaditeľ odboru bezpečnosti AGEL SK

Oblasť je výzvou pre každého, kto sa chce posúvať. Je tam neustále vzdelávanie, analýza dát či zvládnutie zložitých technických riešení, pomocou ktorých je možné zabrániť množstvu pokusov o prienik do systému. V hierarchii spoločnosti sa dá vypracovať na pozíciu, ktorá je najbližšie k vedeniu spoločnosti a môže svojím rozhodnutím ovplyvňovať celý chod. Pre mňa osobne je chrániť nemocnice poslaním.

Vladimír Jančok,
vedúci oddelenia informačná bezpečnosť VÚB

To, že práca v oblasti kybernetickej bezpečnosti ponúka široké kariérne možnosti a obrovský potenciál pre profesionálny rast, už mnohí z nás vedia. Zrejme sme už počuli aj o možnostiach špecializácie, kde každá nová technológia so sebou prináša aj bezpečnostný aspekt. No najväčšou motiváciou je možnosť pracovať s množstvom veľmi šikovných a inteligentných ľudí, či už v rámci firmy, alebo medzinárodnej komunity.

Denisa Lavková,
obchodná manažérka Qubit Security

Deti veria v rozprávky, kde dobro vyhráva nad zlom. Ja verím v tímovú prácu v realite, kde sa snažíme o výsledky, ktoré sú benefitom pre väčšinu. Takže pocit z dobre vykonanej práce, ktorá navyše prispieva k bezpečnejšej realite a budúcnosti, je na nezaplatenie. A, samozrejme, ide o jeden z najlepšie platených džobov v súčasnosti.

Július Selecký,
senior technický špecialista ESET

Byť súčasťou spoločnosti, ktorá zabezpečuje kybernetickú bezpečnosť, znamená prispieť schopnosťami a zručnosťami k oblasti s veľkou pridanou hodnotou. Väčšina uchádzačov dnes hľadá v práci vyšší zmysel, integritu a prínos pre spoločnosť, a preto vnímajú kyberbezpečnosť atraktívne a perspektívne. Rozvoj vlastnej kariéry spájajú s víziou budúcnosti a s rastovým potenciálom, ktorý táto oblasť ponúka.

Matej Síleš,
manažér IT bezpečnosti UPC BROADBAND SLOVAKIA

Pre mňa osobne je najpríťažlivejšiu osobnou motiváciou práce v kybernetickej bezpečnosti stále pretrvávajúca jedinečnosť práce spočívajúca najmä v nedostatku odborníkov. Ako najväčšiu profesionálnu motiváciu by som mohol určiť každodenné vzdelávanie, a to v rôznych manažérskych a odborných zručnostiach. Zároveň mám možnosť sa dotknúť rôznych tém v živote organizácie, čo je veľakrát vzrušujúce.

Andrej Žucha,
generálny riaditeľ ALISON Slovakia

Je to práca ako akákoľvek iná, ak ju robíte dobre a radi. Je však výnimočne perspektívna a nikdy, ani na minútu, vás nenechá spať na vavrínoch. Vyvoláva adrenalínovú závislosť.

Ivan Kopáčik,
bezpečnostný expert Gordias

Vzdelávať sa v kybernetickej bezpečnosti je náročné, preto by som zdôraznil mentoring. Dlhodobý profesionálny vzťah so skúseným odborníkom, kde nový zamestnanec odborne rastie a všestranne rozvíja svoj talent. A prečo práve kyberbezpečnosť? Pretože je takmer bez limitov kariérneho rastu, uplatnenia i finančného ohodnotenia a umožňuje využiť prakticky všetky zručnosti.

Michal Ďorda,
audítor kybernetickej bezpečnosti Auditori.it

Skúseného „bezpečáka“ presvedčí a motivuje záujem top manažmentu, ktorý mu podá pomocnú ruku a zároveň preukáže dôveru. Pre mladé pušky je motiváciou možnosť zásadne ovplyvňovať alebo až meniť procesy a technológie v existujúcich organizáciách. Ak pridáme ešte rýchly kariérny postup a možnosť učiť sa na praktických skúsenostiach, nemôže existovať zaujímavejšia a tak výborne platená pracovná pozícia.

Michal Rampášek,
advokát WISE3 advokátska kancelária

Je to zábava, a pritom profesionálna výzva venovať sa niečomu inému. Motivuje ma hľadať odpovede na nové otázky, ktoré spájajú právo a technológie. Kybernetická bezpečnosť nie je len práca, ale aj životný štýl. V značnej miere je to aj hodnotová práca, keďže prináša zamyslenie aj pre vlastné morálne a etické založenie.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC Soitron

Práca v oblasti kybernetickej bezpečnosti môže mať rovnaké poslanie ako v tradičných bezpečnostných zložkách – „pomáhať a chrániť“ –, čo samotné môže pôsobiť veľmi motivujúco. Keď k tomu pridáme, že ide o moderné, rýchlo rastúce, neustále sa meniace odvetvie s veľmi širokým záberom a celosvetovým nedostatkom odborníkov, nemala by byť o motiváciu núdza.

Ján Golais,
konateľ JUDICIUM

Pri kybernetickej bezpečnosti ide o dynamickú oblasť s neutíchajúcou možnosťou osobného rozvoja a rastu, so štipkou napätia, s prekvapivými odhaleniami, nekončiacimi výzvami, ďalekými cieľmi, okamžite sledovanými zmenami a rýchlou reakciou externého prostredia, ktorá vie prekvapiť o to viac, o čo viac sa snažíš, ale ten pocit, ten je na nezaplatenie.

Martin Spál,
riaditeľ kybernetickej a fyzickej bezpečnosti SIA Central Europe

Dôsledky bezpečnostných incidentov môžu byť veľmi veľké. Byť súčasťou tímu, ktorý chráni spoločnosť, ako aj jej zákazníkov, je dostatočnou motiváciou pre prácu v neustále sa meniacom prostredí kybernetickej bezpečnosti. Pri každodenných výzvach spojených s novými hrozbami nepoznáte pojem rutina. Rozmanitá špecifikácia zamerania dáva možnosť neobmedzeného vzdelávania a profesionálneho rozvoja.

Roman Čupka,
hlavný konzultant Flowmon a CEO Synapsa Networks

„Peniaze, peneži a peníze...“ A je úplne jedno, na ktorej strane barikády v odbore kybernetickej bezpečnosti stojíte. No vždy v prvej línii, či už ako kybernetický lekár, alebo kybernetický vojak. A vedľajší efekt je len veľmi príjemný bonus, človek sa určite nenudí, odbor je dynamický, rýchly a vyžaduje veľkú dávku adaptability, inteligencie a chuti vzdelávať sa.

Richard Kiškováč,
generálny riaditeľ IstroSec

Ako profesionálnu motiváciu by som vyzdvihol postupnú digitalizáciu väčšiny odvetví a veľký nedostatok odborníkov. Poskytuje to dlhodobé a takmer neobmedzené možnosti kariérneho rastu a adekvátneho ohodnotenia. Z osobného pohľadu je to najmä účasť v profesionálnej komunite a neustály vývoj a zmeny v oblasti kybernetickej bezpečnosti. Je to oblasť, ktorej význam bude v budúcnosti iba vzrastať.

Robert Mramúch,
manažér kybernetickej bezpečnosti MH Teplárenský holding

Transformácia – možnosť podieľať sa na budovaní unikátnych a jedinečných riešení s dosahom až po koncového odberateľa. Trend – implementácia súčasných technológií a top produktov v oblasti priemyslu a utilít. Profesionalita – smer a ciele sú udávané strategicky vzhľadom na výsledok, pridanú hodnotu a využívanie synergií.

Marián Trizuliak,
architekt kybernetickej bezpečnosti Západoslovenská distribučná

Slogan k výberovému konaniu by mohol vyzerať aj nasledovne: Zbožňuješ adrenalín a napätie, ale nechceš sa len prizerať? Vieš vziať veci do vlastných rúk a zmeniť sám seba? Máš pocit, že ťa doma sleduje aj kávovar so žehličkou? Zo zásady čítaš len papierové denníky, lebo „co je psáno, je dáno“?