KOMORA
SPECIÁL

PODNIKÁNÍ & BEZPEČNOST

LEGISLATIVA:
SMĚRNICE NIS2

PROBLÉM:
ČELÍME NOVÝM KYBERHROZBÁM

PŘÍKLAD:
SOUKROMÝ DETEKTIV A FIRMY

Nový zákon o kybernetické bezpečnosti

Firmy čekají zásadní změny

Počet a rozsah kybernetických hrozeb podle NÚKIB průběžně roste a stávají se stále sofistikovanějšími. Jedním z evropských nástrojů boje proti kyberkriminalitě je směrnice NIS2 a na ni bude navazovat národní právní úprava, která se dotkne minimálně 6 000 českých firem včetně jejich dodavatelských řetězců. Přestože přesná pravidla ještě nejsou známá, je nejvyšší čas začít se připravovat. Protože dost toho lze udělat již dnes.

Nový zákon je nový nejen povinnostmi, které přinese, ale zejména svým důrazem na bezpečnost třetích stran. Proto bude zajisté nejspornějším bodem celé právní úpravy právě to, koho nakonec zákon vyhodnotí jako rizikového a vyřadí jej z poskytování služeb regulovaným subjektům. Na toto téma můžeme čekat ještě obsáhlé diskuze.

Zákon dosáhne až za hranice

S ohledem na bezpečnost České republiky bude riziko u poskytovatelů služeb vyhodnocováno i podle země dodavatele. Ta musí splňovat podmínku

demokraticky zvolené vlády, existenci právního státu a nesmí považovat ČR za nepřátelský stát. Dodavatelé dále musí respektovat hospodářskou soutěž a nesmí čelit mezinárodním sankcím.
Předlohou pro vznikající zákon se stala směrnice o kybernetické bezpečnosti NIS2. Česká republika, stejně jako ostatní členské státy EU, se zavázala v prosinci 2022 k naplnění cílů směrnice. Jakou formou jich dosáhne, je přitom už na tuzemských legislativcích, nejde tedy o žádné dogma. Zásadní je nicméně termín splnění, zákon by měl být účinný dle závazků nejpozději od 17. října příštího roku.
Prvotní návrh zpracoval a publikoval Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) v lednu tohoto roku, následně běžela lhůta pro připomínky ze strany veřejnosti. Nakonec úřad zaznamenal 1 144 unikátních podnětů. Plně akceptoval 15 % z nich a dalších 22 % přijal s upravenou formulací. Téměř polovinu připomínek zamítl. Ve zbytku šlo spíše o dotazy ke vznikajícímu zákonu, na které by úřad měl odpovědět.

JAKÉ NEJDŮLEŽITĚJŠÍ ZMĚNY OČEKÁVÁME OD NOVÉHO ZÁKONA?

- Nová regulace by se měla v určitém rozsahu týkat nejen velkých, ale i středně velkých společností a také firem, které regulovaným společnostem poskytují svá technologická řešení a služby. Z hlediska dodavatelského řetězce mohou změny významně ovlivnit například telekomunikační operátory a jiné ICT společnosti, jež ve svých datových centrech využívají řešení dodavatelů jako např. Huawei, který NÚKIB označuje jako rizikový.
- Novinkou by měla být povinnost oznamovat incidenty, jako je tomu u ochrany osobních údajů.
- Neméně významnou změnou bude i trestně-právní odpovědnost vedení společnosti. Management bude muset být vyškolen a bude nést odpovědnost za případné incidenty a jejich následky.

Náklady firem budou statisícové, pokuty by byly o několik řádů vyšší

Dosavadní zákon se zaměřoval převážně na velké společnosti, které byly součástí kritické infrastruktury, tedy takové společnosti, jež mají důležitý význam pro fungování státu, jako je doprava, zdravotnictví, státní správa, energetika… Nový zákon půjde dál, a dopadne zejména na velké a střední firmy. Pro ty z nich, které svou digitální ochranu dosud příliš neřešily, půjde o zásadní změnu, u níž by neměly podcenit čas nutný k přípravě. Investovat do souladu s legislativou budou muset statisíce korun v závislosti na stavu připravenosti, velikosti společnosti a její činnosti.
Nicméně pozor – budou-li chtít dotčené firmy prokázat, že zákonu vyhovují, budou muset v mnoha případech přenést nároky i na své dodavatele. Podobně jako to nastavují nová pravidla pro nefinanční reporting.
Kromě technických aspektů zvyšování digitální ochrany budou muset firmy proškolit své zaměstnance, spolehlivě určit, kdo za co při reakci na kybernetický útok odpovídá, a hlásit případné incidenty příslušnému úřadu, stejně tak jako informovat své zákazníky o incidentech a o možných hrozbách.
Za přestupek vůči zákonu hrozí sankce ve výši až 250 milionů korun či do dvou procent čistého celosvětového ročního obratu. Zároveň NÚKIB bude moci ukládat i pořádkové pokuty až do výše 100 tisíc korun, což může i opakovaně až do souhrnné výše 10 milionů korun. A za hrubé nedodržování zákona hrozí sankce, jejímž výsledkem může být i zastavení činnosti společnosti až na půl roku. ■

JAKÁ JE SOUČASNÁ SITUACE VE FIRMÁCH?

Z dosavadních zkušeností, které jsme získali při realizaci IT auditů dle stávající legislativy nebo ISO 27000, nebo auditů interního charakteru, se nejčastěji setkáváme s tím, že společnostem chybí dokumentace a pravidla, jak se chovat: uživatelé používají např. vlastní zařízení, která si přinesou do zaměstnání. Ta nejsou ošetřena proti kybernetickým hrozbám. Uživatelé nejsou seznámeni s pravidly. Ta buď nejsou nastavena vůbec, nebo nevědí, kde se s nimi mohou seznámit. Případně je dokumentace jen formálního charakteru, ale postrádá důležité praktické informace. Typickým příkladem je používání USB disků, které bývají často zdrojem problémů a branou, kterou se do firemní IT infrastruktury šíří viry. Ty pak způsobují problémy jako zašifrování firemní dat, jejich znepřístupnění, dlouhé a nákladné obnovování.

JAK BY SE MĚLA FIRMA NA PLÁNOVANÉ ZMĚNY PŘIPRAVIT A KDE ZAČÍT?

- Ověřit si, zda se nový zákon o kybernetické bezpečnosti na společnost vztahuje, nebo nikoli. Vymezení není zcela jednoduché.
- Provést analýzu rizik, která ověří, jak jsou ošetřena klíčová aktiva společnosti, aby nedošlo k jejich zneužití, narušení, nebo znepřístupnění.
- Zaměřit se na řešení těch oblastí, kde jsou rizika největší – s cílem je minimalizovat a přijmout opatření technického a organizačního rázu, aby byla rizika přijatelná
- Učinit organizační opatření a zpracovat potřebnou dokumentaci od vrcholových dokumentů přes směrnice až po příručky provozního charakteru. Každý by měl být s relevantní dokumentací seznámen a také dostatečně proškolen.
- Učinit technická opatření, průběžně sledovat hrozby a na ty relevantní včas reagovat. NÚKIB a jiné zdroje informují o zranitelnostech a rizicích.
- Bezpečná firma by měla být proaktivní – sledovat situaci, konat a komunikovat.

LIBOR ŠRÁM, expert na kybernetickou bezpečnost BDO

Bezpečí není samozřejmost

Česká republika patří podle Global Peace Index z roku 2023 mezi 12 nejbezpečnějších zemí světa, současně je v ČR vyhlášen a platí první stupeň ohrožení terorismem – obecné ohrožení terorismem. Nicméně po covidovém období se nám podle policejních statistik zvyšuje trend kriminality. Rostou majetkové delikty, například registrovaná kriminalita vzrostla meziročně v roce 2022o 18,8 % a nárůst trestné činnosti v on-line prostoru během posledních deseti let je dokonce vyšší než 745 %. Přestupek a jeho hranice výše škody pro trestní stíhání se zvýšily z 5 000 Kč na 10 000 Kč (2020) a v přípravě je novela Trestního zákoníku, kdy se počítá s mírnějšími tresty za opakované drobné krádeže, což je jeden ze základních pilířů, na kterých novela stojí a kterým chce vláda snížit vězeňskou populaci.

Současná zhoršující se ekonomická situace, energetická krize, válka na Ukrajině, palestinsko-izraelský konflikt, zhoršující se bezpečnostní situace na Balkáně kolem Kosova, vojenské puče a střety v Africe, Ázerbájdžán a obsazení Náhorního Karabachu, provokace a rozepře mezi Čínou a Tchaj-wanem, migrace, dezinformátoři, zvyšující se radikalismus, sociální sítě, to vše má vliv na bezpečnost a na jednotlivé hrozby, kterým čelíme. A to jak v soukromém životě, tak v pracovním prostředí.

Zvyšuje se agresivita některých obyvatel, dochází ke zvýšeným fyzickým útokům, vyhrožování, a to jak fyzicky, tak především na sociálních sítích, zaznamenáváme i útoky aktivních střelců a další formy násilné kriminality.

Základem je firemní bezpečnostní politika

Každá zodpovědná společnost, firma by měly mít zpracovanou politiku a strategii bezpečnosti.

ASIS INTERNATIONAL

Největší mezinárodní sdružení bezpečnostních profesionálů s více než 34 000 členy po celém světě a delší než padesátiletou tradicí. Jeho základní vizí je rozvoj celosvětové bezpečnosti. Posláním sdružení je podpora vzdělávání, setkávání profesionálů a zvyšování prestiže bezpečnostního oboru.

V rámci BCM (Business continuity management) se připravovat na jednotlivé hrozby, například kyberbezpečnost, klimatické změny, bezpečnostní incidenty, živelní pohromy, teroristické útoky a útoky na měkké cíle, přerušení dodávek energií a vody, selhání dodavatelského řetězce, poškození dobrého jména, nákazy, epidemie, pandemie, poškození životního prostředí, úrazy, válečné konflikty, veřejné nepokoje, havárie, násilnosti a v neposlední řadě trestní odpovědnost organizace.

Velmi zjednodušeně řečeno, je dobré mít připravené reálné plány bezpečnostních postupů, plány obnovy a analýzu rizik: co chci chránit, proti komu a čemu to chci chránit. Společnosti by měly k bezpečnosti přistupovat aktivně a řešit všechny její úrovně.

Fyzická bezpečnost

Pořád je nejrozšířenějším typem ochrany ta fyzická, ne vždy lze totiž lidskou sílu nahradit. Očekávám, že v souvislosti s novelizací Zákoníku práce a změnám u dohod o pracovní činnosti o provedení práce to pravděpodobně v roce 2024 zvedne částku za hodinu fyzické ostrahy v rozmezí 20 až 40 %. Dovolím si tvrdit, že na tohle nebude většina společností připravena. V rámci fyzické ostrahy je nejvíce viditelná absence zákona o bezpečnostních

službách (Zákon o bezpečnostní činnosti), který politici ladí 25 let. Zákon musí být vyvážený a měl by správně nastavit nejen povinnosti, ale i základní ochranu zaměstnanců bezpečnostních služeb, měl by reagovat na moderní technologické trendy. Je nutno podotknout, že fyzická ostraha jsou lidé, kteří jsou první na místě mimořádných událostí v objektech, první, kdo může řídit evakuaci do příjezdu záchranných složek státu, první, kdo může poskytnout první pomoc zraněným osobám při nehodě v objektech a areálech, ale také jsou první na ráně, což ukazují statistiky napadení zaměstnanců ostrahy při výkonu služby.

Technická a technologická bezpečnost

To je obor, který se rozvíjí obrovským tempem. Prvky jako poplachový tísňový a zabezpečovací systém (PTZS), bezpečnostní brány v obchodech (EAS), kamerový systém (CCTV), přístupové systémy a další technické či technologické produkty, včetně chytrého softwaru, využívání neuronových sítí, umělá inteligence (AI) – všechny tyto technologie nemusí být zaměřeny jen na bezpečnost, ale dají se jimi řešit všechny smart prostředky, jako jsou heat mapy nakupujících (to je chytrá pomůcka pro zobrazení nasbíraných dat), ovládat a řídit chlazení, topení, klimatizaci, již dnes existují čisticí stroje s integrovanou kamerou nebo robotický pes, který provádí obchůzky perimetru objektu, RFID technologie pro sledování zboží, detekce podezřelého chování, Sound Event Detector, který upozorní na nežádoucí akustické události, jakými jsou výkřik, výstřel a podobně. Velmi usnadňují kontrolu nad prostorem.

Kybernetická bezpečnost

Ta představuje dnes asi nejvýznamnější a nejrychleji se rozšiřující obor. Kvůli kyberútokům dochází k finančním ztrátám v řádu miliard. Mezi nejčastější hrozby patří krádeže nebo ztráty osobních údajů, poškození dobrého jména organizace, porušení práv duševního vlastnictví včetně krádeže dat, přerušení služeb, regulatorní riziko a pokuty, včetně vysokých nákladů na vyšetřování a odstranění následků. Od roku 2024 vejde v platnost nová směrnice EU o kybernetické bezpečnosti NIS2. Ta je novou směrnicí, jejímž cílem je zavést standardní hlášení incidentů, řízení rizik v oblasti bezpečnosti. NIS2 uvádí okruhy a druhy opatření, které budou muset povinné osoby zavést. Jsou mezi nimi například provádění analýzy kybernetických rizik, přijetí politiky pro zajištění kybernetické bezpečnosti, řízení kybernetických incidentů, zajištění bezpečnosti dodavatelského řetězce, pravidla pro provoz a vývoj informačních systémů atd.

Personální bezpečnost

Obor, který díky online prostředí získává na významu a důležitosti. Ověření uchazečů o zaměstnání, background check, se pomalu, ale jistě zabydluje i v českých firmách a na úřadech. Zvykáme si na to, že si náš nový zaměstnavatel ověří, jestli jsme v životopise nelhali, nepředložili mu zfalšovaná vysvědčení a certifikáty, nebo zda vlastně vůbec existujeme a nevystupujeme pod falešnou identitou. I to se totiž stává. České firmy mají stále nouzi o vývojáře, při náboru se jich tak ani tolik nevyptávají a jsou rádi, když se jim podaří získat někoho, kdo vypadá jako schopný a zkušený ajťák. Toho se někteří lidé snaží zneužít, výrazně jim v tom pomáhají moderní nástroje využívající umělou inteligenci, jako je třeba Midjourney a Dall-E. Existuje však i mnoho jiných nástrojů, jako například Verif Tools s podtitulem Fake Document Generator. Za přibližně devět dolarů si zde lze snadno objednat falešnou fotografii českého dokladu, občanka může třeba ležet na stole. V současné době jsou nabízena řešení pro kontrolu identity a dokladů, zda vaši kandidáti nejsou zrovna v pátrání Interpolu nebo české policie. Rovněž si také můžete ověřit, že nefigurují na žádném z globálních sankčních seznamů. Zaměstnání takového kandidáta by mohlo být v rozporu s právními nebo regulatorními požadavky. Dále mezi kontroly patří základní kredibilita, ověřování předchozích zaměstnání, vzdělání, certifikace, beztrestnost, a to vše v souladu s ochranou osobních údajů a požadavky GDPR. ■

MEZI NEJČASTĚJŠÍ KYBERNETICKÉ HROZBY PATŘÍ KRÁDEŽE NEBO ZTRÁTY OSOBNÍCH ÚDAJŮ, POŠKOZENÍ DOBRÉHO JMÉNA ORGANIZACE, PORUŠENÍ PRÁV DUŠEVNÍHO VLASTNICTVÍ VČETNĚ KRÁDEŽE DAT, PŘERUŠENÍ SLUŽEB, REGULATORNÍ RIZIKO A POKUTY, VČETNĚ VYSOKÝCH NÁKLADŮ NA VYŠETŘOVÁNÍ A ODSTRANĚNÍ NÁSLEDKŮ.

JAROMÍR PRŮŠA, expert na bezpečnost,
předseda Asis International pro Českou a Slovenskou republiku

Zaměstnanci firem čelí stále se zvyšujícímu počtu kybernetických útoků

V dnešním digitálním světě jsou kybernetické útoky čím dál větší hrozbou pro firmy v České republice. Útoky jsou častější a sofistikovanější než kdy dříve. Úspěšný útok může společnosti způsobit vážné škody na firemních datech, celkové pověsti a velké finanční ztráty.

Přestože se zvyšuje povědomí o kybernetických hrozbách a přestože přichází evropská směrnice NIS2, společnosti se stále potýkají s nedostatečnou připraveností svých zaměstnanců na tato možná rizika. V tomto článku se zaměříme na to, proč lidský faktor představuje největší hrozbu pro kybernetickou bezpečnost českých firem a jak lze tuto zranitelnost minimalizovat.

Lidský faktor jako největší hrozba

Jsou to právě zaměstnanci, kteří jsou nejčastěji první linií obrany proti kybernetickému útoku. Proto jejich schopnost rozpoznat a reagovat na podezřelé aktivity znamená často klíčový rozdíl mezi neúspěšným útokem a úspěšným útokem. Bohužel stále zůstává lidský faktor jednou z nejzranitelnějších částí každé organizace.

Statistiky

Dle zprávy Acronis Cyberthreats Report počet napadení způsobený phishingem se zvýšil o 60 % a uniklé nebo odcizené citlivé údaje firmy, pomocí kterých útočníci snadno provádějí kybernetické a ransomwarové útoky, způsobily více než polovinu všech hlášených útoků v roce 2022. Tudíž za více než 50 % úspěšných útoků může právě lidský faktor.

Nedostatečná kybernetická gramotnost a edukace zaměstnanců

Stále velké množství firem neklade dostatečný důraz na kybernetické vzdělávání a dlouhodobou osvětu svých zaměstnanců. Právě nedostatečná osvěta může znamenat, že zaměstnanci nejsou dostatečně obeznámeni s nejnovějšími hrozbami a aktuálními metodami obran proti cíleným útokům. To může vést k nesprávnému chování, jako je například klikání na podezřelé odkazy, zadávání citlivých informací a otevírání infikovaných příloh v e-mailových zprávách.

Phishingové útoky

Útočníci často využívají právě techniky phishingu, aby získali přístup k citlivým informacím. To zahrnuje vytváření falešných e-mailových zpráv,

ODVĚTVÍ NEJVÍCE ZASAŽENÁ PHISHING ÚTOKY:

1. Stavebnictví
2. Retail
3. Reality
4. Profesionální služby
5. Finance

které se zdají být legitimní a jsou zasílány na zaměstnance, s cílem získat citlivé údaje firmy nebo proniknout do infrastruktury. Pokud zaměstnanci nejsou dostatečně obeznámeni s těmito technikami, mohou se snadno stát oběťmi.

Nedodržování bezpečnostních politik

Dalším problémem je nedodržování bezpečnostních politik a postupů ve firmách. Zaměstnanci mohou ignorovat předpisy týkající se hesel, sdílet citlivé informace nebo používat osobní zařízení pro pracovní účely, což zvyšuje riziko úniku dat a kybernetických útoků.

Potřeba testování a pravidelného tréninku

Aby se společnosti mohly účinně bránit kybernetickým útokům, je nezbytné zaměstnance testovat a na základě toho dále vzdělávat. Je to dlouhodobý proces edukace. Testování probíhá jako reálná simulace skutečných phisingových útoků, kdy se připraví podvrhnuté falešné e-maily obsahující odkazy na falešné webové stránky nebo žádosti o zadání citlivých informací, jakou jsou třeba hesla. Na základě útoku se sleduje, jak zaměstnanci reagují, to znamená, zdali kliknou na podvržené odkazy, stáhnou přílohy, zadají citlivé informace firmy. Po skončení útoku organizace ví, jak jsou na tom jejich zaměstnanci z pohledu kybernetické gramotnosti. Toto je klíčová fáze, která slouží pro nastavení vzdělávacího programu zaměstnanců, jak rozpoznávat tyto útoky a jak na ně správně reagovat.

Politiky, vzdělávání, kontroly

Lidský faktor je největší hrozbou v kybernetické bezpečnosti českých firem. Aby firmy mohly účinně snižovat toto riziko, je nezbytné, aby kladly větší důraz na kybernetické vzdělávání svých zaměstnanců, uplatňovaly přísné bezpečnostní politiky a prováděly pravidelné kontroly a simulace kybernetických útoků. Jedině tak mohou firmy minimalizovat riziko kybernetických hrozeb spojených s lidským faktorem a lépe se bránit v dnešním digitálním prostředí. ■

LUKÁŠ PIRKL, obchodní ředitel společnosti Zymestic Solutions (firma se specializuje na kybernetickou bezpečnost)

korus

DYKENO
by KORUS

SPOJUJEME BEZPEČNOST S EFEKTIVITOU

Pracujeme na tom, aby každý pohyb při práci byl nejen bezpečný, ale i provázený maximálním pocitem pohodlí. Zjednodušujeme výrobní procesy díky kompletnímu zajištění ochranných racovních pomůcek i průmyslového materiálu pro práci, ochranu a provoz. Jsme po vašem boku, od zákaznického servisu, přes klientské služby až po marketingovou podporu.

WORK&SAFETY

Spojení pohodlného nošení a bezpečnosti zároveň. To je DYKENO Work & Safety. Produkty, které chrání při práci a splňují nejen legislativní požadavky (BOZP), ale také se dobře nosí. Kvalita, design, funkce a zachování ergonomie do každého prostředí, ať pracujete venku nebo ve vnitřním provozu.

Kompletní ochranné a pracovní oděvy, rukavice, ochrana zraku, sluchu i dýchání pro bezpečnost a ochranu zdraví při práci.

TECH

DYKENO Tech přináší inovaci do vaší výroby. Technické produkty vytvořené na základě zkušeností a testování přímo v technologických provozech, osvědčené v praxi a podpořené letitými zkušenostmi. Vyvíjíme produkty k usnadnění výroby do každého průmyslového odvětví i do běžného provozu.

Lepicí pásky, průmyslové čištění, brusivo i nástroje a nářadí do zakázkové i sériové výroby napříčo bory.

PREMIUM

DYKENO Premiun je zárukou TOP kvality a designu. Oblečení, ve kterém se budete cítit skvěle, ať už ve volném čase nebo v práci. Základem DYKENO Premium je funkční oblečení a produkty, které mají mnohostranné a praktické využití.

Volnočasové oblečení a doplňky, které spojují pohodlí, funkčnost, atraktivní vzhled a styl.

www.korus.eu / ww.dykeno.cz

Pro bezpečná data v průběhu digitalizace

Digitalizace, která dnes probíhá ve většině firem, přináší řadu výhod, ale též nebezpečí, především kybernetických útoků. O názorech na tuto situaci i o tom, co může firmám pomoci, jsme si povídali s Michalem Andraškem, obchodním ředitelem společnosti Asseco Solutions, která je producentem ERP systémů Helios.

Jak vnímá oblast kyberbezpečnosti vaše společnost i vy osobně?
Hlavním rizikem jsou kybernetické útoky, kterým čelí digitální infrastruktura. Hackeři a organizované skupiny se zaměřují na potenciálně zranitelná místa a ke zvýšení úspěšnosti těchto útoků přispívá skutečnost, že mnohým zaměstnancům chybí potřebná opatrnost.

Které chyby nejčastěji ohrožují kybernetickou bezpečnost firem?
Kyberbezpečnost je mnohdy výrazně poddimenzovaná. Souvisí to s tím, jak se rozšiřují digitální služby, které jsou těmito zařízeními poskytovány, ale i s vybavením, které firmy používají. Problémem však stále zůstává chování samotných zaměstnanců firem, protože podle statistik je minimálně 90 procent útoků provedeno zevnitř organizace. Vždycky jde o nejslabší článek řetězce. Spousta IT oddělení vystaví kolem firmy pomyslný perimetr ochrany, ale přece jenom uživatel-zaměstnanec je zpravidla tím nejsnáze ovlivnitelným článkem, kde dochází k chybě. V naprosté většině se přitom jedná o nezaviněné či neúmyslné jednání zaměstnance. Často se lze setkat například s lepítky s heslem pro odemykání počítačů na monitorech, otevíráním odkazů v e-mailech z neznámých adres a následné zatajování skutečnosti, že došlo k rizikovému chování a podobně. Zabránit se tomu dá jedině edukací lidí a vysvětlováním toho, co může nastat. Trendem je dnes také mnohem větší využívání možnosti home office. V tomto případě záleží na tom, zda zaměstnanci používají firemní počítač, nebo ne. Většina společností používá pro práci z domova VPN připojení, které bývá zabezpečeno. Málokdy se však již dohlíží na koncové zařízení uživatele.

Které služby by podle vás měl kvalitní producent ERP firmám v oblasti kyberbezpečnosti nabízet?
Může jít například o školení zaměstnanců, simulaci phishingových kampaní a odhalování bezpečnostních rizik v systémech. Všechny tyto služby by měly být doplněny přehlednými reporty a analýzami, které pomohou firmám lépe porozumět jejich kyberbezpečnostnímu stavu a přijmout opatření ke zlepšení.

„Naše budoucí vize ERP systémů reflektuje aktuální trendy. Namísto jednoho velkého systému vidíme ekosystém menších specializovaných aplikací v cloudu propojených s umělou inteligencí," říká Michal Andraško.

Kromě automatizace uvnitř samotného ERP systému se na trhu objevuje stále více specializovaných aplikací, které se do systémů integrují.

Pro své útoky kyberzločinci využívají i RDP (Remote Desktop Protocol) určený pro bezpečný vzdálený přístup k firemním aplikacím. Nabízíte svým zákazníkům nějaký produkt pro zabezpečení vzdáleného přístupu?
Ano. Jeho název je ERPORT a jedná se o cloudové prostředí speciálně navržené pro systémy Helios. Umožňuje však provozovat nejen je, ale i další aplikace s maximálním důrazem na bezpečnost. Zajišťuje šifrování komunikace, omezuje přístup jen na konkrétní IP adresy, podporuje VPN a umožňuje multifaktorovou autentifikaci uživatelů, což výrazně zvyšuje bezpečnost. Vše je provozováno v České republice, což poskytuje jistotu ohledně ochrany dat.

Významným tématem pro většinu společností jsou dnes digitalizace, automatizace, vzdálený přístup. Posunul se v návaznosti na to i vývoj ERP systémů?
Kromě automatizace uvnitř samotného ERP systému se na trhu objevuje stále více specializovaných aplikací, které se do systémů integrují. Mnoho z nich je postaveno v cloudu, a pokud chcete tyto aplikace efektivně integrovat, stává se přechod do cloudu pro podnikový informační systém logickou evoluční cestou.

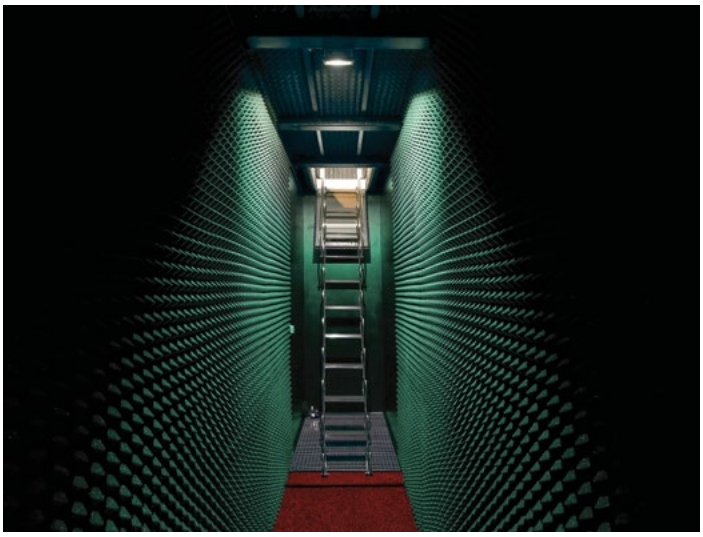
Jaká je vaše vize do budoucna? Co by měly ERP systémy splňovat?
Naše budoucí vize ERP systémů reflektuje aktuální trendy. Namísto jednoho velkého systému vidíme ekosystém menších specializovaných aplikací v cloudu propojených s umělou inteligencí. Každý klient si sestaví mix aplikací na míru svým potřebám. Uživatelské rozhraní bude intuitivní, přestože systém bude zajišťovat složité procesy. Systém se automaticky přizpůsobí uživateli a jeho akcím na základě analýzy dat a umělé inteligence. To zahrnuje dynamické vytváření formulářů, funkcí a řešení pro konkrétní situace. Naše systémy budou uživatele aktivně usměrňovat k efektivnímu řešení jejich potřeb a problémů. ■

REA KŘÍŽOVÁ, Brand Manager Helios iNuvio ve společnosti Asseco Solutions

Bezpečnost soukromých i firemních objektů

Když je bezpečí neviditelné

Bezpečnost je slovo v dnešní době skloňované mnohokrát denně ať už v souvislosti s konfliktem na Ukrajině, či kvůli nedávným útokům Hamásu v Izraeli. Možná si říkáme, že to je pořád kus od nás, ale je to skutečně kus? Není to už jen velmi malý kousek, který by nás měl přimět k zamyšlení, jestli jsme skutečně schopni zajistit své rodině či firmě bezpečí?



Úniková chodba podzemního krytu

Pod zemí můžete mít i luxusní jednací místnost

Foto: archiv Tebrix a Shutterstock.com

Útoky na školách jsou ve světě bohužel téměř dennodenní záležitostí. Podobné riziko hrozí v nemocnicích či v jiných veřejných budovách. Je až zarážející, že se zatím žádná česká škola nerozhodla realizovat zásadní bezpečnostní opatření. Bezpečnost firmy si představíme spíše jako zabezpečení proti kybernetickým hrozbám, případně máme na mysli ostrahu objektu. Ale v mnoha zemích nejsou výjimkou ani ozbrojené útoky v soukromých společnostech. A došlo k nim i u nás. Jak se takovým hrozbám bránit?

Bezpečí je vlastností prostoru

Především je nutné si riziko uvědomit, stanovit si únikovou cestu a připravit si bezpečný úkryt. Pod pojmem bezpečný úkryt se dá schovat mnohé, ale v zásadě rozlišujeme dva druhy; bezpečnou místnost, tedy prostor, který nás ochrání v horizontu pár hodin, a podzemní kryt, který nám nabídne úkryt i na mnoho týdnů či měsíců podle vybavení a velikosti.

Vybudování bezpečné místnosti je samo o sobě vlastně jednoduché; stačí si zvolit místnost, která má dostatečně pevné zdi, má přístup vzduchu a vody, dokáže přijímat rádiové vlny a lze do ní snadno uniknout. Zásadní podmínkou pro bezpečnou místnost jsou bezpečnostní dveře, ideálně dveře odolávající balistickému útoku. Nejedná se tedy o bezpečnostní dveře, které máme u bytu či domu a které pomohou zabránit nechtěnému vstupu zlodějů. Dveře od bezpečné místnosti jsou pancéřované, s vybetonovaným meziprostorem, vážící i několik tun. Takové dveře se mohou vsadit pouze do zdí k tomu připravených, což mohou být i původní zdi domu či bytu, ale vyztužené tak, aby pancéřované dveře dokázaly udržet. Do místnosti by měla být zavedena voda a nesmí chybět ani nezávislý zdroj světla, minimálně baterka. Pokud jsme v takto chráněném prostoru a pokud si dokážeme rádiovým spojením zavolat pomoc, pak bychom se měli cítit bezpečně.

Jistota je kryt

Podzemní kryt je už složitější projekt, neboť se předpokládá jeho užívání v řádu týdnů či měsíců. Kryty jsou schopné odolat i tlakové vlně v případě výbuchu, záleží na požadavcích uživatelů, ale vždy se musí jednat o kryty vyrobené dle normy ČSN 73 9001. Nejprve je tedy nutné si zvolit vhodné místo pro podzemní kryt. Mělo by být zvenku neviditelné, ale přesto propojené s hlavním domem. Samozřejmostí je i druhý východ z krytu pro případ závalu. Voda i vzduch v krytu jsou filtrovány podle stupně ohrožení. Teplo zajišťuje rekuperační jednotka. Aby se uživatel vyvaroval psychických problémů s pobytem pod zemí, jsou světla v krytu navržena tak, aby odpovídala dennímu cyklu i intenzitě denního světla; tedy plná v poledne, ale tlumená večer a po ránu. Vybavení krytu odpovídá jeho účelu, přičemž velmi záleží na rozměrech krytu. Standardní rodina se dvěma dětmi může přemýšlet o krytu o velikosti 50 až 60 m^2, náročnější uživatelé volí kryt 150–200 m^2. Každý kryt je vybaven kuchyňkou, koupelnou s WC a obytnou částí, která je zároveň ložnicí, pokud se jedná o malý kryt. Důležitou součástí krytu jsou zásoby, a to nejen potravin s dlouhou trvanlivostí, ale také drogistického zboží, lékárny, osobních věcí, ale také ochranných prostředků. Elektřina je do krytu dodávána buďto ze sítě, nebo z FVE či z dieselového agregátu. Rádiová stanice je součástí vybavení, neboť to může být jediné funkční spojení se světem.

Kryt lze využít i bez nebezpečí

Podzemní kryty jsou pro mnoho uživatelů také výhodnou investicí, protože nejen, že dodají oprávněný pocit bezpečí, ale jsou dalším obytným prostorem, který v případě prodeje nemovitost zásadně zhodnotí. A k čemu může kryt sloužit, když neslouží jako kryt? Ideální místo třeba pro střelnici ve spojovací chodbě, nebo jako pánský klub. Pokud si myslíte, že chcete zvýšit pocit bezpečí pro vás, vaši rodinu či kolegy, najděte si odborníky, kteří vám pomohou ať už s bezpečnou místností, která může být i v bytě, nebo s podzemním krytem. V dnešní neklidné době to je více než dobrá investice. ■

MICHAL TERENDY, majitel společnosti Tebrix

Zabezpečení majetku v Česku bude čelit novým kyberhrozbám

Míra zabezpečení staveb je v ČR stále na podprůměrné úrovni oproti západním státům. Poněkud vágní legislativa dostatečně nenavazuje na příslušné normy a zásadně nejde ruku v ruce s pojišťovnami. Není tak vytvářen soustředěný pozitivní tlak na trh ohledně zabezpečování majetku obecně.

Jinak je tomu ve velkých městech, centrech, kde se realizuje podstatná část obchodu a průmyslu, zde převládají moderní sofistikované technologie zabezpečení – elektronické přístupové systémy. Jinak je to v okrajových regionech, maloměstech a na venkově, kde tvoří mechanické klíčové systémy většinu instalací. Naproti tomu nová výstavba a rekonstrukce zažívají určitý boom ve způsobu uvažování investorů či vlastníků, kdy se od začátku snaží o zpracování určitého bezpečnostního projektu stavby a o související pokrytí většiny rizik. Ale i toto aktuální uvažování ukazuje svá negativa – jednak se neřídíme doporučením profesionálů, stále spekulujeme – jaká míra zabezpečení „by nám tak mohla stačit" a navrch všeho chceme maximálně ušetřit. To se projevuje jak v rezidenční, tak komerční výstavbě. Upřednostnění úspor či ekonomičnosti řešení je samozřejmě na úkor účinnosti a celkového pojetí zabezpečení daného objektu. Ve výsledku se bezpečnostní záměr až nezdravě často omezí např. na systém generálního klíče (SGHK) v závislosti na PBŘ stavby. Což však zcela zásadně ovlivňuje hrozby a rizika spjaté s budoucím provozem objektu.

Fenomény doby

Vidím vliv dvou fenoménů. Za prvé – jako společnost jsme si navykli požadovat luxus a komfort v mnoha stránkách našeho života. Tedy to, co je trendy, jakékoliv moderní usnadnění chceme mít v rámci konzumního způsobu žití a za honbou určité společenské prestiže. Toto uvažování máme takřka bez ohledu na mnohem důležitější faktory, jako je naše skutečná potřeba a účinné pokrytí rizik – nikoliv mít pouze na pohled pěkný produkt, který reaguje třeba na otisk prstu. To si samozřejmě uvědomují výrobci nových technologií, globální hráči, kteří v rámci postupující digitalizace zvyšují ekonomickou dostupnost takových řešení, jelikož systém je dlouhodobě nastavený na výkon a maximalizaci zisku. Díky tomu roste tlak na spotřebitele, aby si pořizovali nové elektronické systémy a usnadnili si tak ovládání vstupu do svého obydlí nebo firmy apod.

Za druhé – jsou to samotné elektronické přístupové produkty, jejich kvalita a možnosti použití. S postupem vývoje v posledních dvou letech čelíme stále rostoucí nabídce těchto produktů zejména přes velké internetové e-shopy. Jejich výhodou je neuvěřitelně nízká pořizovací hodnota a poměrně široká nabídka možností obsluhy a ovládání. Jejich zcela zásadní nevýhodou je, že ve většině případů neznáme výrobce ani zemi původu, respektive známe pouze dovozce či distributora v ČR. Typicky firma výhodně nakoupí kontejner takových produktů, doveze je a nabídne je třeba na Mall.cz. Takto zakoupený produkt nám však nikdo, natož

odborně, nenamontuje ani nesdělí, zdali je pro náš záměr vhodný, či ne. V případě servisu neexistuje firma, kterou bychom zavolali, a u reklamací je to stejné. Tato situace se historicky opakuje, pouze s jinými produkty. V roce 2010–2013 byl obrovským problémem masový dovoz levných bezpečnostních dveří z východu, bez certifikace a průlomové odolnosti. Byly levné včetně snadné instalace a spotřebitelé je ve velkém pořizovali. Následovaly série vloupání a majetkové trestné činnosti. V těchto případech nebylo plnění ze strany pojišťoven, neboť nikdo nebyl schopen doložit platné certifikáty či cokoliv, co prokazuje splnění alespoň určité míry zabezpečení dle platných norem. U elektronických produktů a přístupových systémů (různá kování, kliky, motorické zámky, mechatronické vložky a jakákoliv další zařízení) je situace horší v tom, že veškeré takové systémy jsou ovládané pomocí mobilní či webové (cloudové) aplikace. Nejčastěji mobilem, právě pro nepřeberné možnosti správy produktu v reálném čase a odkudkoliv, máte-li data na mobilním telefonu. To, co je však největší devízou takových řešení, a to, co chce každý – aby měl možnost kompletní správy kdykoliv, odkudkoliv – je zároveň rapidně rostoucí a nekontrolovatelnou kybernetickou hrozbou!

Jinými slovy: pořídíte si levný produkt zabezpečení v rámci SMART HOME nebo zkrátka jen chcete mít moderní otvírání či odemykání bytu na čip, kód nebo otisk prstu. K takovému produktu si stáhnete volnou platformu – nabízenou aplikaci, ve které založíte účet, vygenerujete si přístupové heslo, zadáte svůj e-mail či telefonní číslo, popřípadě jiné osobní, tedy citlivé údaje, čímž vznikne také vaše databáze. Dále již vytváříte či mažete uživatele, kterým udělujete přístup do vašeho bytu několika způsoby – typicky rodiče svým dětem, příbuzným, resp. společnosti svým zaměstnancům.

Co dnes nikdo neřeší

Otázkou je, kde se nachází cílové úložiště takto vytvořené databáze a veškerých údajů. Není výjimkou, že takové aplikace mívají cílové servery a úložiště v čínských, ruských či jiných konfliktních oblastech, kde absolutně nezkontrolujeme, kdo k našim údajům má přístup.

Zde se dostáváme k novému typu hrozby, kdy na jedné straně tato zařízení neuvěřitelně zrychlují administraci a celý proces přístupu oprávněným osobám do objektu, stejně jako okamžitou možnost uživatele ze systému vymazat v případě potřeby. Na straně druhé jde řeč o nakládání s citlivými daty, hesly a přístupovými informacemi, kde se jedná o ochranu firemních či uživatelských dat, o nakládání s těmito daty a zcela zásadně – o řízení přístupu k těmto informacím a možnost jejich čtení, kopírování, replikace.

PRÁVĚ NAPADNUTÍ A ZÍSKÁNÍ PŘÍSTUPOVÝCH ÚDAJŮ KONKRÉTNÍCH OSOB Z DATABÁZE SYSTÉMU, KTERÝ POUŽÍVAJÍ JEDNOTLIVCI NEBO CELÉ ORGANIZACE, JE ZCELA ZÁSADNÍ KYBERNETICKOU HROZBOU!

Zde zmiňuji přelomovou směrnici NIS2, kterou bude muset uvést do života odhadem více než 30 tisíc komerčních subjektů do října roku 2024. A která pojednává o souboru opatření, kontrolních mechanismů a povinností právě z hlediska zodpovědného přístupu firem ke zvyšující se kybernetické kriminalitě.

Směrnice se zabývá firmou a jejími daty, ochranou těchto dat, serverovými a cloudovými úložišti a zabezpečením důležitých technologií či aktiv v rámci objektu firmy. Tedy bavíme se o kyberochraně firmy, jejího know-how, ekonomického, účetního, skladového hospodářství a odběratelsko-dodavatelského řetězce.

Co je však dosti upozaděné, je, že vlastní způsob elektronického přístupu osob do prostor firmy, což jsou nejen zaměstnanci, ale například ostraha, externí úklidová/facility agentura, návštěvy a další, je téměř nezmíněn, respektive neřešen.

Důležitá je spolupráce s odborníky

A právě napadnutí a získání přístupových údajů konkrétních osob z databáze takového systému, který používají jednotlivci nebo celé organizace – je zcela zásadní kybernetickou hrozbou! V případě, kdy nekontrolujeme, kde naše data máme. První případy takových útoků jsou již známy z USA. Pachatel vyčetl přístupové údaje a do objektu dané firmy se tak dostal – jako její fiktivní zaměstnanec a jednalo se o průmyslovou špionáž v malé vývojářské firmě, která měla do domku s kancelářemi na vstupu instalovanou chytrou elektronickou kliku z tamního e-shopu, kterou pořídili jako výhodnou koupi se samoinstalací produktu a volně stažitelnou aplikací k obsluze. Z těchto důvodů je nesmírně důležité nepodléhat skvělé ceně a řešit pořízení veškerých elektronických přístupů, smart produktů pro obydlí, zkrátka čehokoliv, pouze s odborníky a profesionály z oboru!

Ti spotřebitelům doporučí zároveň i nezbytné komponenty důležité pro správný chod, funkci a míru zabezpečení. Nezřídka se stává, že zákazník si pořídí i sám namontuje chytrou kliku na vstup do bytu a pak se diví vykradení, jelikož v tomto případě chyběla výměna stávajícího zadlabacího zámku za samozamykací typ. Tak zůstával jeho byt nezabezpečen a dveře byly jištěny pouze střelkou zámku, kterou sice spínala chytrá klika po zadání hesla či otisku, ale tyto dveře se daly velmi jednoduše otevřít vyhmatáním a zatlačením střelky, namísto aby byly zamčené.

Je tedy velmi důležité nepodcenit výběr dodavatele takového produktu, informovat se o veškerých aspektech. Zajímat se, zdali dodavatel nabízí volnou platformu nebo má k ovládání vyvinutou vlastní aplikaci s deklarovaným úložištěm dat (ideálně v ČR) nebo zda nabízí provoz na serveru přímo u zákazníka (pak by vše spadalo zcela do režimu směrnice NIS2, pro firmy, kterých se to týká, anebo by firmy byly schopny doložit tuzemské úložiště a ochranu dat).

Zajímat se o možnosti upgradu nabízeného řešení, dostupnost servisu a záruky. To vše je velmi důležité!

Tradiční tuzemští a evropští výrobci a distributoři nabízí prověřené řešení a transparentní nakládání s databázemi uživatelů elektronických přístupových systémů stejně jako deklaraci úložiště, pokud se nachází v zahraničí. ■

TOMÁŠ POSPÍŠIL, MBA,
cechmistr Cechu mechanických zámkových systémů ČR

archiv Doverville

Neřešme bezpečnost až po průšvihu

Jak vnímáme bezpečnost? Proč se firmy soustředí spíš na bezpečnost majetku než bezpečnost lidí? Jak napravit fakt, že nám chybí schopnost hodnotit rizika i znalost bezpečnostní abecedy? To je téma pro Veroniku Fáberovou, majitelku společnosti Doverville, která se specializuje na ochranu měkkých cílů.

Když vznikal tento rozhovor, intenzivně se rozhořela válka mezi Izraelem a Palestinou. Svět bedlivě sleduje vývoj situace. Každého z nás napadne, jaký vliv to bude mít na bezpečnost ve střední Evropě a u nás…

Všechny velké bezpečnostní incidenty, které se ve světě stanou mají samozřejmě dopad i na naši republiku, ale to neznamená, že to běžný občan ihned pocítí či postřehne. Bezpečnostní hrozby či incidenty jsou velmi proměnlivá veličina. Je jedno, jestli jde o ojedinělý brutální teroristický útok nebo konflikt, který vede k válce. Bezpečnostní odborníci tyto hrozby soustavně vyhodnocují a připravují plány na nová bezpečnostní a krizová opatření. Ať už se jedná o veřejné instituce nebo korporátní byznysovou sféru, je potřeba situaci ve světě sledovat a neříkat si, že ale nám nic nehrozí. Efekt zjevení se takzvaných černých labutí prostě existuje a zpravidla s sebou přináší devastující účinky.

Česko je ale jednou z nejvíce bezpečných zemích na světě. Proč se věnujete právě bezpečnosti veřejných prostor?

Už jste někdy slyšela o státu, který o sobě prohlašuje, že není bezpečný? U nás je relativně dost bezpečno. Problém dneška vidím někde jinde – naučili jsme se brát naši bezpečnost jak něco zcela samozřejmého, a hlavně jako starost někoho jiného. Před covidem jsme si dělali průzkum, jak návštěvníci různých veřejných akcí a prostor vnímají svou bezpečnost – se zajímavým výsledkem. Většina lidí v momentě, kdy si nechá utrhnout vstupenku nebo překročí práh veřejné instituce, automaticky spoléhá na to, že je v bezpečí. Absurditou je, že pořadatelé akcí většinou nemají o bezpečnosti ani základní znalosti a veřejné instituce se soustředí spíš na to, aby jim veřejnost něco neukradla, než aby u nich byla ve skutečném bezpečí. Moc dobře to nevidím ani u budoucích staveb, architekti o pochopení koncepce bezpečnosti nemají zájem a developery pak jednoznačně zajímá pouze nejnižší cena bezpečnostních instalací. To je naše dnešní realita. Bohužel i mezi bezpečnostními agenturami je velmi malá znalost bezpečnostního řemesla. Já ještě patřím ke generaci, co si ve škole čistila plynové masky a měla jakýsi základní branný výcvik – i když si z toho dneska děláme legraci. Jenže dnes základní bezpečnostní znalosti mezi lidmi prostě chybí. A v tom se lišíme od řady vyspělých zemí, jako jsou například Švýcarsko, UK nebo Spojené arabské emiráty, kde je mezi lidmi bezpečnostní povědomí mnohem větší než u nás. Dokonce třeba existují i nové přístupy v architektuře, kde se k modelování bezpečného prostředí používá metoda CPTED (Prevence kriminality prostřednictvím designu a návrhu prostředí).

To myslíte vážně?
Naprosto. Potřebu bezpečnosti považujeme za samozřejmost, i když víme, že na ní stojí celá pyramida lidské motivace. Taková je nyní situace. Například k událostem 11. září došlo také i z toho důvodu, že nikdo před tím neřešil, že je potřeba preventivně ošetřit bezpečnost samotných pilotů při letu, to přece byla samozřejmost. Bezpečnost je hlavně o prevenci, kterou všichni podceňujeme – ve všem, například pokud jde o naše zdraví, podceňování dopadu kybernetických rizik třeba na naše děti, nedostatečné pojištění našich domovů a další preventivní oblasti. Myslíme si, že jsme neporazitelní. Víte, kterou větu od klientů slýchám nejčastěji?

Kterou?
My to tak děláme už patnáct let a až doteď se nám to nikdy nestalo… U nás se vše řeší až po nějakém průšvihu. Je hodně smutné, že před tím se musí lidé ušlapat a zranit v davu při panice, musí dojít ke střelbě v nemocnici či restauraci, musíme zažít několik brutálních útoků nožem či mačetou v našich školách, vražd úředníc při výkonu jejich práce, fyzická zranění po brutálních napadeních zdravotnických pracovníků, napadení IT systémů institucí. To hovořím opravdu o událostech v naší republice. Náprava pak stojí hodně času a peněz. Upřímně oceňuji práci Policie ČR.

I v médiích se množí podobná oznámení o vzrůstající agresi ve společnosti. Jaké je řešení?
Dobře nastavený bezpečnostní systém není žádná nukleární věda, je to o znalosti prostředí a potřeb lidí, kteří to prostředí využívají, a pak hlavně o zdravém selském rozumu. Dnes máme k dispozici spoustu úžasných bezpečnostních technologií i AI, které nám pomáhají řešit různé bezpečnostní výzvy, ale vždy nejdříve musí proběhnout řádná analýza a pak se dají navrhnout vhodná i ekonomicky efektivní řešení problémů, a to nejen nápravná, ale i preventivní.

Teď mluvíte skoro jako auditor…
Ano, mám za sebou i praxi v nastavování a auditování procesních systémů. Vycházím ze znalosti různých druhů prostředí a pracovních i výrobních procesů. Jako bezpečnostní konzultant řeším řadu specifických a citlivých problémů, bohužel většinou až po té, co došlo k nějakému průšvihu. Největší podceňovatelé bezpečnostní prevence kupodivu pochází z oblasti korporátního byznysu. Jejich svaté přesvědčení, že všechny své aktivity mají proceduralně podchyceny a auditovány různými autoritami, často vedou k velkému zaspání na vavřínech.

Jaké služby tedy klientům nabízíte?
Ráda pro to používám termín Likvidátor potíží. Rozklíčujeme příčiny bezpečnostního problému. Navrhneme řešení, které zahrnuje nejen implementaci nových bezpečnostních postupů a technických prvků, ale především návrhy na úpravy některých jejich vnitřních procesů. Umíme pomoci v personální oblasti – ať už se jedná o výběr bezpečnostně prověřeného personálu na klíčová místa, nastavení systému průběžného prověřování spolehlivosti klíčových manažerů, nebo nastavení bezpečných HR procesů. Důležitá je i oblast PR, firemní kultury, a hlavně i krizové komunikace, se kterou umíme také pomoci. Na základě bezpečnostního procesního auditu jsme schopni odhalit skrytá rizika v různých provozních a procesních částech výroby či aktivit. Připravit podklady pro vypsání různých bezpečnostních tendrů i posouzení oblasti BOZP a požární ochrany. Připravit návrh bezpečnostního rozpočtu, aktualizovat a zjednodušit bezpečnostní dokumentaci. Realizujeme poutavé výcviky jak pro manažerský tým, tak i pro určené skupiny zaměstnanců.

Vaše metody výcviku mě překvapily. Příjemně…
Děkuji. Skutečně používáme trošku netradiční, o to však účinnější metody. Razíme postup učení se hrou a používáme i metody zážitkové pedagogiky. Pro demonstrace situací používáme náš vlastní profesionální herecký a kaskadérský tým. Simulujeme různé důležité dílčí situace a učíme, jak deeskalovat vzrůstající nebezpečí a jak postupovat v již nebezpečných situacích. Pro celé týmy organizujeme nácviky týmového řešení různých krizí. Umíme zorganizovat i praktický nácvik evakuace, invakuace, ale i námětová součinnostní cvičení s Policií ČR i s dalšími složkami IZS.

To musí být nesmírně finančně náročné aktivity…
Ale vůbec ne. Jsme zvyklí pracovat s nikterak horentními rozpočty. A především naše výcviky přinášejí okamžitý praktický efekt. Účastníci chválí, že si mohou vyzkoušet, jak mají reagovat v různých nebezpečných situacích. Manažeři oceňují, že se jim při našich simulacích podaří odhalit díry v jejich systému a mají šanci je včas a bezbolestně vyřešit. ■

IVA PROUZOVÁ

VERONIKA FÁBEROVÁ

Více než 30 let se věnuje bezpečnostní problematice a vzdělávání dospělých v různých bezpečnostních disciplínách. Zaměřuje se hlavně na bezpečnost veřejných prostor, prevenci kriminality, násilí a terorismu v nemocnicích, poliklinikách, školách, kulturních zařízeních, úřadech, hotelech, dopravních terminálech, při velkých eventech a podobně.

Jak na kvalitu zakázek bezpečnostních technologií?

V odborné i laické veřejnosti je stálá, snad i rostoucí polemika o kvalitě techniky, služeb i komplexních dodávek bezpečnostní techniky a technologií. Objevují se informace o neodborném, neseriózním a často přímo podvodném jednání některých podomních prodejců či montážníků při nabídkách zabezpečení bytů, domů i jiných objektů ve styku B2C (poskytovatel služby – spotřebitel) – většinou bezpečnostní zámky, dveře, zabezpečovací signalizace, kamery. Často se to týká i velkých zakázek s rozsáhlými systémy nejvyšší generace (B2B) a bohužel výjimkou nejsou ani veřejné zakázky (B2G) pro města či státní správu.

Asociace technických bezpečnostních služeb Grémium Alarm, která je pro obor technických bezpečnostních služeb autorizovaným živnostenským společenstvem Hospodářské komory ČR, má ve svém poslání propagaci kvality a garanci odbornosti a profesní etiky. V rámci své působnosti AGA mimo jiné dbá na to, aby její členové vykonávali podnikatelskou činnost odborně a v souladu s obecně závaznými právními předpisy. Členské firmy s ověřenou právní a odbornou způsobilostí a schopností zpracovat zakázku od kvalitní nabídky přes projekt a montáž po uvedení do provozu a zajištění kvalitního servisu dostávají Osvědčení o kvalitě a jsou zařazeny na seznam, který je publikován a uveřejněn mimo jiné na https://www.gremiumalarm.cz/clenstvi/firmy-s-osvedcenim-kvality/. Ověřování kvality firmy se provádí v souladu se schválenou metodikou Hospodářské komory ČR.

ING. VÁCLAV NEPRAŠ,

prezident Asociace Grémium Alarm, člen představenstva HK ČR a předseda Bezpečnostní sekce HK ČR

V oboru komerční bezpečnosti pracuje od roku 1991. Asociace technických bezpečnostních služeb Grémium Alarm sdružuje více než sto podnikatelských subjektů oboru. V Hospodářské komoře ČR má v gesci soukromé bezpečnostní služby. Je členem Poradního sboru MV ČR pro situační prevenci kriminality.

archiv Asociace Grémium Alarm

Pro kvalitu zabezpečení je velmi důležitá správná volba techniky

Nabídka na trhu je velká a pro laika nepřehledná. Vhodným doporučením jsou evropské technické normy. Asociace Grémium Alarm iniciovala a ve spolupráci s Ministerstvem vnitra ČR zpracovala dokument Stanovení úrovně zabezpečení objektů a provozoven proti vloupání podle evropských technických norem. Dokument, který vydala Česká agentura pro standardizaci, přehledně uvádí doporučené úrovně zabezpečení pro různé objekty: od bytu, domu až po například advokátní kanceláře. Poskytuje přehled o mechanickém zabezpe-

čení, poplachových zabezpečovacích a tísňových systémech, kamerách a jejich kombinaci vhodné pro ochranu majetku a osob. Společná pravidla pro aplikaci mechanických zábran a poplachových systémů umožňují optimalizovat zabezpečení majetku pro konkrétní rizika. K nahlédnutí na https://www.gremiumalarm.cz/o-asociaci/ke-stazeni/, nebo www.mvcr.cz.

Důležitým krokem je správné zadání zakázky

Asociace technických bezpečnostních služeb Grémium Alarm v úzké spolupráci s Odborem práva veřejných zakázek Ministerstva pro místní rozvoj ČR proto zpracovala Metodický pokyn pro zadávání veřejných zakázek na dodávku bezpečnostních technologií. Tento dokument obsahuje doporučující pokyny k zadávání veřejných zakázek, zahrnující širokou oblast technických služeb a zařízení sloužících k ochraně osob a majetku: poplachové zabezpečovací a tísňové systémy, dříve označované jako elektronické zabezpečovací systémy, elektrická požární signalizace, kamerové sledovací systémy, elektronická kontrola vstupů, mechanické zábranné systémy, služby dohledových center s pulty centralizované ochrany. Týká se dodávek komponentů systému (technologické prvky, hardware, software včetně licencí), služeb (například služby systémové integrace, průběžný servis apod.) nebo díla (například komplexní dodávka bezpečnostního systému). Hlavním cílem zpracování metodiky bylo ukázat a doporučit postup, jak lze zadat zakázku a také vybrat dodavatele podle kvalitativních kritérií, a ne pouze podle ceny. Metodiku lze dobře využít i při zadávání běžných komerčních zakázek, mimo režim veřejných zakázek. Metodický pokyn je uveden v plném znění včetně příloh na webových stránkách asociace na odkazu: https://www.gremiumalarm.cz/o-asociaci/ke-stazeni/. Odvolávka je také na webových stránkách Ministerstva pro místní rozvoj: www.mmr.cz a Ministerstva vnitra ČR na odkazu: https://prevencekriminality.cz/metodicky-pokyn-pro-zadavani-verejnych-zakazek-na-dodavku-bezpecnostnich-technologii/.

Certifikace a registrace

V celoevropském měřítku je kvalita instalací bezpečnostních zařízení a technologií řešena technickou normou ČSN EN 16763: Služby pro požárněbezpečnostní zařízení a zabezpečovací systémy. Ta je v platnosti již několik let a vychází ze Směrnice Evropského parlamentu a Rady 2006/123/ES a našeho zákona č. 222/2009 Sb. Není však v naší republice doposud naplňována. Norma v odstavci 3.2 stanovuje, že poskytovatel služby musí mít registraci podle příslušných národních požadavků a stanovuje minimální požadavky na poskytovatele uvedených služeb a na odbornou způsobilost, znalosti a dovednosti v tomto oboru. Tento obor je u nás zastřešen především koncesí Poskytování technických služeb k ochraně majetku a osob. Některé podnikatelské subjekty požadavky této evropské normy splňují, ale není na celorepublikové úrovni stanoven způsob a systém jejich ověření, certifikace a stanovené registrace. Také není splnění požadavků na služby v tomto citlivém oboru v ČR praktikováno a ani investory požadováno. V řadě evropských zemí je tato norma naplňována tak, že odbornou způsobilost prověřuje a certifikát vydává profesní sdružení příslušného oboru. V těchto zemích je samozřejmě i vyžadován a neexistence tohoto certifikátu handicapuje naše firmy při zájmu o zdejší zakázky. Asociace Grémium Alarm toto Osvědčování kvality a registraci firem zahájila. Podle Pravidel pro osvědčování kvality a registraci firem odborně způsobilých dodávat služby v souladu s ČSN EN 16763 a dle metodiky HK ČR odborná komise posoudí právní, a především odbornou způsobilost firmy. Která firma uspěje, obdrží certifikát a je zaregistrována podle ČSN EN 16763. Zároveň je zařazena na seznam firem s prokazatelně kvalitní profesionální dodávkou požárně bezpečnostního zařízení, nebo bezpečnostních technologií. Tento seznam je uveřejněn mimo jiné na www.gremiumalarm.cz. ■

VÁCLAV NEPRAŠ

Nový kybernetický zákon je za rohem

A dopadne téměř na každého

Informační (kybernetická) bezpečnost je velkým tématem, které nás bude provázet mnoho následujících roků, až se stane běžnou součástí našeho života na stejné úrovni, jako jsme zvyklí zamykat domy a nepouštět k sobě neznámé osoby.

Jaké jsou základy kybernetické bezpečnosti? Jak nastavit kybernetickou bezpečnost ve vaší společnosti, aby byla pro byznysová, a jak ji budovat, aby to byl váš štít, který zmírní následky incidentů, které se dějí každý den?
Základním předpokladem je, že kybernetická bezpečnost by měla být v zájmu společností i jednotlivce, ať už budou spadat pod legislativní rámec kybernetické bezpečnosti, či ne. Pokud ale chceme jít cestou nejmenšího odporu, prvotním krokem s ohledem na návrhy nové legislativy je určení, jestli budete spadat pod návrh nové legislativy, či nikoliv. A pozor – máte povinnost se určit sami, což je změna proti nynějšímu zákonu, kdy vás určil NÚKIB.

DŮLEŽITÉ BODY

- Podívejte se na návrh vyhlášky o regulovaných službách – zde jsou vypsané činnosti, obory, které pod tuto novou legislativu budou spadat.
- Věnujte pozornost velikosti podniku. Legislativa primárně (jsou zde výjimky) dopadá na střední a velké společnosti, ale pozor – do výpočtu se započítávají i mateřské, dceřiné a další společnosti skupiny.
- Pokud jste držitel licence, mohou se vás týkat další případné povinnosti.

Není to jen o službách

Podívejte se pozorně na celý seznam regulovaných služeb, protože směrnice se netýká jen těch, které tvoří hlavní předmět vašeho podnikání, ale jakýchkoliv jiných činností, které ve společnosti činíte. A není zde vždy pravidlo, že službu musíte poskytovat třetí straně. Typickým příkladem je fotovoltaika – i když ji využíváte pouze pro vlastní potřeby, pokud máte licenci vztahující se k fotovoltaice a máte nad 50 zaměstnanců, spadáte pod návrh nové legislativy v kategorii energetika, i když v ní primárně nepodnikáte.
Doporučujeme také vyzkoušet webovou aplikaci urci.se, kde si můžete vyzkoušet, zda pod legislativu spadáte. Při využití pamatujte, že aplikace je spíše informativní, není nahrazením právní rady a výsledek není závazný, takže pokud vám vyjde ve výsledku, že nespadáte, ptejte se, zda jste opravdu prozkoušeli všechny služby, které děláte. Co fotovoltaika, co odpadové hospodářství?
A pokud opravdu pod směrnici nespadáte, nejste například významní dodavatelé pro své zákazníky? Nebudou po vás oni stejně chtít prokázání alespoň základů kybernetické bezpečnosti? Prohlášení o aplikovatelnosti, základní risk analýza či disaster recovery plány se vám zkrátka hodí, i když primárně nemusíte naplňovat legislativu.

archiv Cybrela a Shutterstock.com

Kateřina Hůtová, manažerka informační bezpečnosti a zakladatelka konzultační společnosti Cybrela

Co je druhý krok?

Udělejte si Gap analýzu – čili analýzu toho, jaké opatření již dneska máte ve společnosti zavedeno. Věřte mi, nezačínáte od úplné nuly. Je tu např. GDPR, vytváříte účty a přidělujete oprávnění, máte firewall a podobně. To, co již máte, musíte komparovat s tím, jaké nové povinnosti se k vám budou vztahovat nebo jaký cílený stav si zvolíte.
Na základě Gap analýzy je pak krok třetí, udělejte si road mapu toho, co kdy musíte splnit, jaké na to budete potřebovat finance. Čím dřív se začne, tím pomalejší a klidnější tempo můžete nasadit a nemusíte vše dohánět na poslední chvíli.

CYBRELA

Konzultační společnost, která se zaměřuje na poskytování poradenství v oblasti informační a kybernetické bezpečnosti.

Hlavním pilířem je risk management

Ke kybernetické bezpečnosti přistupujte tak, abyste eliminovali rizika, která by pro vás mohla mít fatální dopad za použití přiměřených prostředků. Risk management, to je selský rozum na papíře. Nebojte se ho, napište si, jaké základní procesy, služby, informace potřebujete a ve své společnosti máte, a na ně si upřímně navažte znatelnosti a hrozby. Risk analýza vám pak dá ucelený pohled na to, co se vám může stát, a společně s výsledky Gap analýzy máte jasný maják, který ukazuje cestu, kudy se vydat.
A poslední rada, zvažte si, jestli se vám vyplatí některé úkoly outsourcovat konzultantům na kybernetickou bezpečnost nebo investovat do vzdělávání vlastních zaměstnanců. Nikdo nebude vaší společnosti rozumět tak jako vaši zaměstnanci. Nejlepší cesta je postupně zaučovat zaměstnance a kooperovat je v konzultanty, kteří vám pomohou či vás vedou v začátcích. Žádný konzultant vám nezabezpečí společnost sám, bez vás to zkrátka nikdy nebude efektivní. ■

KATEŘINA HŮTOVÁ

NÁVRH NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

NÁVRH VYHLÁŠKY O REGULOVANÝCH SLUŽBÁCH

Nové povinnosti v oblasti kybernetické bezpečnosti

S mnoha změnami přichází evropská směrnice NIS2. Jejím prostřednictvím Unie reaguje na růst digitalizace a zavádí nová opatření na ochranu důležité infrastruktury členských států. Počet organizací v ČR, které jsou podle aktuálního zákona o kybernetické bezpečnosti povinny se jím řídit, výrazně vzroste. A to z několika stovek na vyšší jednotky tisíců.

Hlavním cílem je dosáhnout toho, aby organizace zaváděly bezpečnostní opatření k posílení své kybernetické bezpečnosti a tím zvyšovaly bezpečnost důležité infrastruktury a celé společnosti. Nově do této skupiny povinných subjektů budou spadat všechny organizace, které poskytují alespoň jednu službu uvedenou v přílohách směrnice NIS2 a zároveň jsou středním nebo velkým podnikem (zaměstnávají 50 a více lidí, nebo dosahují ročního obratu, nebo bilanční sumy roční rozvahy alespoň 10 milionů eur).

Kdy se začít chystat?

Jistě co nejdříve, čas se organizacím krátí. Česká republika by sice měla mít zaveden nový rámec povinností v národní legislativě (formou novelizace zákona o kybernetické bezpečnosti a některých dalších relevantních předpisů) do října 2024, ale NÚKIB doporučuje co nejdříve zahájit přípravné práce na přizpůsobení svého vnitřního prostředí novým požadavkům. Než se organizace pustí do zavádění bezpečnostních opatření a nových, s tím spojených procesů, je třeba provést analýzu rizik a bezpečnostní audit. To pomůže k jednoznačné identifikaci rizikových oblastí, kritických míst, na které bude jednodušší aplikovat bezpečnostní opatření.

JAK KONKRÉTNĚ POMŮŽE S NIS2 PRODUKT CSA?

- Zhodnotí současný stav organizace. Umožní efektivně definovat aktiva včetně jejich ohodnocení. Identifikuje riziková místa a následně navrženými bezpečnostními opatřeními je sníží.
- Poskytne strukturovaný přístup k plánování a prioritizaci opatření na základě výsledků analýzy rizik.
- Umožní monitoring zaváděných opatření a jejich sledování v čase.

SLUŽBY Z PŘÍLOHY SMĚRNICE NIS2

- Energetika
- Vesmír
- Doprava
- Poštovní služby
- Bankovnictví
- Odpadní hospodářství
- Infrastruktura finančních trhů
- Chemický průmysl
- Zdravotnictví
- Potravinářství
- Pitná a odpadní voda
- Výroba
- Digitální infrastruktura
- Výzkum
- Poskytovatelé ICT služeb
- Poskytovatelé digitálních služeb
- Veřejná správa

Kde hledat pomoc?

Pro řadu organizací bývají nové povinnosti vyplývající z evropské legislativy náročné nejen finančně, ale také administrativně a procesně. A to i z důvodu složitého výkladu legislativních předpisů. Proto doporučujeme obrátit se na odborníky, kteří dokážou najít nejméně nákladné a efektivní řešení v souladu s evropskými požadavky. Takové sdružuje i společnost Gordic a její síť technologických partnerů.

Konec excelovským tabulkám

Aplikace CSA (Cyber Security Audit) umožňuje pomocí analýzy rizik jednoduše definovat a ohodnotit všechna identifikovaná aktiva, na základě toho určit rizika, automatizovaným způsobem je vyhodnotit a navrhnout relevantní řešení pro jejich snížení. *„Je potřeba nebrat NIS2 jako strašáka, ale jako příležitost, díky které organizace zvýší úroveň své bezpečnosti. A protože míra digitalizace v posledních letech obrovsky vzrostla, je nezbytné k ní zajistit i odpovídající bezpečnost. Nejen s analýzou rizik pomůže naše aplikace CSA. Neváhejte se na nás v oblasti zavedení směrnice NIS2 obrátit. Kybernetická bezpečnost není jen legislativní povinnost, ale existenční nutnost,“* říká Michal Řezáč, ředitel sekce bezpečnosti a informačních technologií Gordic. ■

VOJTĚCH HVĚZDA, Gordic

GORDIC

Ryze česká společnost GORDIC, spol. s r. o., již od roku 1993 vytváří prostor a nástroje pro srozumitelnou komunikaci lidí a organizací. Vizí předního českého tvůrce a dodavatele informačních systémů je propojená společnost, ve které bezpečné technologie usnadňují život. Produktové portfolio a služby společnosti Gordic zahrnují informační systémy určené pro veřejnou správu, včetně uznávané platformy GINIS, kterou využívá více než 6 000 organizací veřejné správy; dále otevřené modulární informační systémy pro soukromý sektor, včetně DMS, řešení fyzické i kybernetické bezpečnosti a integrační platformy pro ovládání IoT technologií a efektivní sběr dat. Gordic je iniciátorem a provozovatelem platformy KYBEZ, která je založena na dobrovolné spolupráci akademických, státních i komerčních a mediálních institucí z oblasti IT a telekomunikací a jejímž cílem je osvěta v oblasti kybernetické bezpečnosti a obrany.

Více informací na:

www.gordiccybersec.cz

Bezpečnostní dohled jako služba

Jaké jsou výhody a nevýhody?

Studie společnosti Arctic Wolf ukázala, že v USA nemá až 44 % organizací ve svých řadách žádného experta na kyberbezpečnost. Zbytek sice někoho takového zaměstnává, ale často není kyberbezpečnost jeho primární náplní práce a jen 23 % organizací má více než jednoho člověka, kteří se alespoň částečně kyberbezpečností zabývají.

To má k ideálnímu stavu daleko. *„Sdílené kompetence jsou problém. Když nemá expert za úkol pracovat aktivně jen na zajištění bezpečnosti, znamená to často, že umí fungovat jen reaktivně a že organizace například nevyčlenila prostředky na jeho vzdělávání,“* říká Daniel Hejda, expert na bezpečnostní audity ze společnosti Cyber Rangers. Bezpečnostní dohled by tedy měly organizace všeho druhu brát vážně.

Řada firem a organizací ho ale neřeší, přestože právě dohled vám umožní předcházet závažným následkům útoků. Bezpečnostní dohledové centrum lze přitom snadno pořídit jako službu, kterou u nás najdete pod hlavičkou O2 Security Expert Center, zkráceně O2 SEC.

Chce to specializovaný dohled

Bezpečnostní dohledové centrum (Security Operations Center, zkráceně SOC) má za úkol řešit preventivní ochranu před útoky a pomůže odhalit případné prolomení bezpečnosti v jeho samotném počátku. *„Řada firem používá základní ochranné prvky, jako třeba firewall, antivirová a antispamová řešení. Jenže když je útočník překoná, už vlastně dál nikdo ve firmě nevidí, co se děje. S bezpečnostním dohledem se ale tato neprůhledná zamlžená zóna zviditelní,“* popisuje účel dohledového centra Jiří Sedlák, který v O2 vede tým externí bezpečnosti. Dobře nastavený bezpečnostní dohled tedy pomůže odhalit i útočníka, který se skrývá a nechce být odhalen.

Bezpečnostní dohled lze zajistit dvěma hlavními způsoby. Společnost si může buď postavit svůj vlastní interní tým, který na bezpečnost dohlédne, nebo je možné si pořídit bezpečnostní dohled jako službu. Jaké jsou mezi těmito dvěma cestami rozdíly?

Výhody interního SOC: Kontrola nad daty a rychlejší odezva

Pokud firma disponuje odpovídajícími finančními a personálními zdroji, expertní znalostní bází a současně preferuje zachovat kompetence bezpečnostního dohledu ve vlastní režii, potom by měla sáhnout po interním řešení.

Interní řešení může být také lépe šité přímo na

míru některým potřebám organizace a současně být pružnější a rychlejší z hlediska řešení případných reakcí na vyšetřování a mitigaci následků bezpečnostních událostí. *„Když máte interní tým, který pro firmu dýchá, dovede být v mnoha věcech důslednější než externí dodavatel,“* zmiňuje Hejda jednu z výhod jinak finančně i manažersky náročnějšího řešení.

Kromě vyšších počátečních investic i dražšího provozu přináší interní řešení další výzvy a nevýhody. *„Často se v tomto případě setkáváme s tím, že není snadné do takového týmu sehnat kvalitní zaměstnance,“* popisuje hlavní nevýhodu Daniel Hejda. *„Lidé ze SOC týmu by měli být kamarádi, kteří spolu v pohodě zajdou na pivo a přitom umí v kritických situacích fungovat s chladnou hlavou,“* říká expert.

A tím, že seženete vhodné kandidáty do týmu, starosti nekončí. Tyto zaměstnance je potřeba neustále vzdělávat a firmy také musí odolat pokušení využít tyto zaměstnance k jiným účelům. *„Bezpečnostní dohled vyžaduje plnou pozornost,“* upozorňuje Hejda.

Externí dohledové centrum: nižší investice a lepší škálovatelnost

Z výše uvedeného je patrné, že pro řadu firem může být jednodušší pořídit si bezpečnostní dohled jako službu. Tato volba vyžaduje nižší počáteční investici a menší částky na provoz – například zde odpadají starosti o hardware i software, který je k dohledu potřeba. Externí SOC také může přinést lepší škálovatelnost a flexibilitu při růstu firmy a pružnější reakci na trendy v oblasti kyberbezpečnosti.

Nicméně výhody externího dohledu přicházejí za cenu sdílení kontroly nad daty. *„Externí dohled vaši organizaci doslova svlékne do naha. Vidí úplně vše, co se uvnitř děje. Musíte tedy najít partnera, kterému budete důvěřovat, ale zároveň potřebujete na své straně někoho, kdo bude s takovým partnerem kvalitně komunikovat, ať už ohledně rozvoje služby, nebo v případě bezpečnostních incidentů,“* vysvětluje Hejda. U externího dohledu také nemusí být pro firmu snadné najít partnera, kterému bude skutečně důvěřovat.

Nemáte vlastní specialisty pro splnění nároků NIS2?

Externí bezpečnostní dohledové centrum může pomoci i firmám, na které dopadnou nové povinnosti v souvislosti s evropskou regulací NIS2, respektive zákonem o kybernetické bezpečnosti, který NIS2 přenáší do české legislativy. Nový zákon zásadně rozšiřuje okruh povinných osob, tedy organizací, které musí významně posílit svoji kybernetickou bezpečnost. A nejen to, ze zákona bude rovněž povinné hlásit kybernetické incidenty a učinit celou řadu dalších opatření. Už proto se hodí mít na své straně tým zkušených expertů na kyberbezpečnost, kteří se splněním nových povinností pomohou.

VÝHODY A NEVÝHODY EXTERNÍHO SOC

Výhody	Nevýhody
Možnost úspor nákladů díky využití sdílených zdrojů a odborníků.	Potenciální riziko ohledně kontroly a ochrany dat.
Lepší škálovatelnost díky snadnějšímu přizpůsobení se změnám ve firmě nebo na trhu.	Možné problémy s komunikací a koordinací s externím poskytovatelem.
Nezávislé a objektivní hodnocení bezpečnostního postavení firmy.	Možná pomalejší reakce na incidenty v porovnání s interním týmem.
Možnost těžit ze sdílených zkušeností a informací o hrozbách mezi různými klienty a oborovými vertikálami.	Riziko spojené se závislostí na externím dodavateli.

INTERNÍ VERSUS EXTERNÍ DOHLEDOVÉ CENTRUM

INTERNÍ DOHLEDOVÉ CENTRUM	EXTERNÍ DOHLEDOVÉ CENTRUM
Větší počáteční investice i náklady na provoz	Menší počáteční investice i náklady na provoz
Detailní znalost vlastního firemního prostředí	Nezávislé a objektivní hodnocení stavu kyberbezpečnosti
Vysoké náklady na specializované zaměstnance, kterých je navíc na pracovním trhu nedostatek	Úspora mzdových nákladů
Potenciálně méně efektivní adaptace na nové hrozby a trendy, protože nečerpá z externího know-how	Hlubší know-how vycházející ze zkušenosti napříč mnoha klienty

Jedno správné řešení neexistuje

V otázce kyberbezpečnosti neexistuje jednoznačná odpověď, zda je lepší volit interní, nebo externí dohledové centrum. Každá z těchto možností přináší své výhody i nevýhody a správná volba bude záviset na konkrétních potřebách, kapacitách dané organizace a financích. Je nutné si připomenout, že jakýkoliv SOC, ať už interní, nebo externí, běžící na různých technologiích, nikdy neznamená stoprocentní ochranu. Je to pouze jedna z klíčových vrstev, která by v rámci kyberbezpečnosti měla být aplikována.

„I my v O2 jsme dodavatelem bezpečnostního dohledového centra. Většinou poskytujeme bezpečnostní dohled jako službu, ale máme i zákazníky, pro které jsme budovali jejich interní bezpečnostní dohledová centra přímo na míru,“ říká Jiří Sedlák s tím, že výhoda dohledu jako služby netkví jen v menších starostech se sháněním personálu. Tým externí bezpečnosti O2 má totiž v oblasti kyberbezpečnosti široký rozhled, a to umožňuje nasazovat u zákazníků přesně ty nástroje, které potřebují, a zároveň sdílet zkušenosti z útoků napříč celým portfoliem zákazníků. ■

BARBORA NOVÁKOVÁ, marketingový specialista pro B2B

O2 CyberNews

archiv WEDOS

Kybernetický štít nejen proti hacktivistům

Kybernetická bezpečnost se v současné době stává středem pozornosti mnoha podniků, a to zejména kvůli narůstajícím hrozbám ze strany proruských hacktivistických skupin, jež se snaží upoutat pozornost kybernetickými útoky na webové stránky států a významných společností.

Své cíle si vybírají podle toho, která vláda podpoří Ukrajinu, ať už hmotně, anebo třeba odvážným prohlášením. Naposledy jsme to jako občané České republiky poznali v září, když byly opakovaně nedostupné weby řady českých bank.

Co se stalo?

Jedna z nejaktivnějších hacktivistických skupin využila DDoS útoků, které mají za cíl narušit plynulý chod webových stránek – udělat je co nejdéle nedostupné. Následně se pochlubili svými úspěchy na sociálních sítích a těšili se z pozornosti médií. Tito hacktivisté nejsou motivováni finančním ziskem; jejich hlavní motivací je demonstrace jejich dovedností a vytvoření chaosu. Navíc ruská média často využívají úspěchy těchto skupin jako propagandu, což jim dává větší publicitu a význam. Bohužel domény a značky postižených společností jsou pak spojovány se slabou kybernetickou ochranou, což vede k obavám klientů.

Jaký to mělo dopad?

Útoky hacktivistů způsobily značné nepříjemnosti a ekonomické ztráty pro podniky, které se staly jejich oběťmi. Běžní lidé nevědí, jak funguje DDoS útok, a mají obavu o svá data a v případě finančních institucí i o peníze. Pokud útok trval déle a oni nemohli například zaplatit anebo se dostat do internetového bankovnictví, tak to není dobrou vizitkou a jen to posiluje obavu, zdali nepřišli o úspory.

Společnosti neví, jak tomuto druhu útoků čelit, a proto volí nevhodná krátkodobá řešení, jako je například odstřižení zahraniční konektivity. Což znamená, že pro zbytek světa mimo Česko přestanou na internetu existovat. Jejich klienti v zahraničí jsou kvůli tomu zcela odříznuti. Stejně tak ti, kteří používají například zabezpečené připojení přes VPN od třetích stran mimo ČR. Navíc útoku zcela nezabrání, protože ten jde i z napadených počítačů, mobilů, serverů a chytrých zařízení i z ČR.

Proč je WEDOS Global Protection odpovědí?

Zde přichází na řadu WEDOS Global Protection. Toto řešení je zvláště vhodné vůči útokům hacktivistických skupin díky své BGP AnyCast DNS s reverzními proxy. S více než 2 000 servery ve více než 30 lokalitách po celém světě je tento systém navržen tak, aby rozptýlil a minimalizoval útoky, které by jinak mohly způsobit vážné problémy. Na druhu kybernetického útoku přitom nezáleží, protože WEDOS Global Potection analyzuje každý požadavek individuálně a vyhodnocuje, jestli je v pořádku, nebezpečný anebo podezřelý. Podezřelé požadavky pak umí podrobit dodatečným testům anebo vrátit plnohodnotný statický otisk stránky, což přesně zde by bylo řešením.

Výhodou je čistý provoz

Centralizovaná řešení často nedokážou čelit útokům takového rozsahu, protože nemají kapacitu ani geografickou rozloženost k efektivnímu rozptýlení těchto hrozeb. WEDOS Global Protection se svým decentralizovaným designem a masivní infrastrukturou je postaven tak, aby útoky absorboval v dané lokalitě, analyzoval a případně vyčistil. Čistý provoz pak pošle z lokality k vám. Místo jednoho místa, na které se sesypou útoky z celého světa, máte přes 30 lokalit po celém světě, přes 2 000 serverů a přes 3 000 Gbps konektivity. Do konce roku 2023 je v plánu navýšení počtu lokalit na 40 a v roce 2024 na 250. Pro nás není problém přidávat další lokality, škálovat infrastrukturu a navyšovat konektivitu na rozdíl od tradičních řešení.

Zástupci společnosti WEDOS přednášející na konferenci v Lucemburku o kybernetické ochraně

V DNEŠNÍ DOBĚ JE NEZBYTNÉ MÍT ŘEŠENÍ, KTERÉ DOKÁŽE ČELIT HROZBÁM ZE STRANY HACKTIVISTŮ A DALŠÍCH KYBERNETICKÝCH ÚTOČNÍKŮ A U KTERÉHO NEMUSÍTE MYSLET NA TO, ŽE ZA PÁR LET UŽ NEBUDE STAČIT.

WEDOS GLOBAL PROTECTION

Nečekejte, až útočníci zaútočí

V dnešní době je nezbytné mít řešení, které dokáže čelit hrozbám ze strany hacktivistů a dalších kybernetických útočníků a u kterého nemusíte myslet na to, že za pár let už nebude stačit. WEDOS Global Protection poskytuje a bude poskytovat právě takovou ochranu.

Také proto chráníme ministerstva států, která byla pod útoky. Chráníme weby politických stran i politiků, e-shopy nadnárodních společností a webové prezentace (ne)oblíbených organizací. V posledních dnech se zdá, že i některé české – a nejen finanční – instituce pochopily, že potřebují řešení pro budoucnost, jakým je WEDOS Global Protection. Napsali nám a už domlouváme první společné projekty.

Nečekejte, až útočníci zaútočí. Váš web může WEDOS Global Protection chránit do 5 minut. Nemusíte kupovat žádný hardware ani nic instalovat. Stačí nasměrovat vaši doménu na naši ochranu. ■

Josef Grill, manažer obchodu WEDOS

Instalace serveru ve švýcarském datacentru (součást sítě WEDOS Global)

Připravte se na revoluci v monitorování a zabezpečení

V digitální éře, kdy technologie hraje stále větší roli ve všech oblastech, se většina společností přizpůsobuje a využívá těchto inovativních řešení pro zlepšení svého podnikání. Příkladem firmy, která klientům dlouhodobě dokazuje, jak mohou technologie přispět k bezpečnosti a efektivitě podnikání, je technologická divize Innovis společnosti M2C a její dohledové centrum Space. Innovis je znám svou specializací na správu technologií, automatizaci a zpracování dat pomocí nejmodernějších technologií v IoT, umělé inteligence a pokročilé analytiky. Mezi jeho nejnovější inovace v oblasti zajištění objektu patří Falcon, mobilní platforma určená k monitorování a zabezpečení prostor, kde je fyzické zabezpečení buď nerealizovatelné, nebo finančně nevýhodné.

Dohledové centrum Space poskytuje služby zákazníkům skrze vyspělé technologické nástroje. Ty umožňují širokou škálu služeb – od ostrahy přes údržbu až po vyhodnocování různých dat dané budovy. Efektivizace nákladů a moderní obsluha budov přitahuje mnoho firem.

„Vzdálený dohled Space poskytuje své služby více než 1 300 zákazníkům ve 12 zemích Evropy, v nichž M2C působí. V České republice mezi ně patří například retailový řetězec Albert, dále autosalony Auto Palace nebo hotely a obchodní centra společnosti CPI,“ říká Lukáš Převrátil, ředitel vzdáleného dohledu Space, a dodává: *„Přináší klientům mnoho výhod. Nabízí optimalizaci strážní služby, analytické nástroje a příležitosti k vyhodnocování dat pro různé účely, včetně marketingu. Kromě toho technologie, které využívá, jsou konstruovány tak, aby byly v souladu s nařízením o GDPR.“*

Izolovaným systémům odzvonilo

Ačkoli nové technologie mohou vyžadovat počáteční investice, studie proveditelnosti a návratnosti často ukazují, že se vyplatí, zejména s ohledem na mzdové náklady, které neustále rostou. Společnosti tak hledají způsoby, jak efektivněji využít technologie a snížit náklady na lidské zdroje. V oblasti vzdáleného dohledu to znamená, že se stále více využívají algoritmy, strojové učení a analytické nástroje, které dokáží automaticky vyhodnotit obrovské množství dat v reálném čase.

Další směr, kterým se firmy ubírají, je podle Lukáše Převrátila propojování různých systémů. *„Dříve měly kamery, čidla a další zařízení své vlastní izolované systémy. Dnes je však trendem integrace všech těchto zařízení do jedné centralizované platformy, což umožňuje lepší sledování, analýzu a reakci na různé situace.“*

Bezpečnost se stává klíčovou oblastí

S růstem kybernetických hrozeb je důležité zajistit, aby byla data přenášena a ukládána bezpečně. Toto se stává prioritou pro mnoho společností, které nabízejí služby vzdáleného dohledu. Ten je aplikovatelný v různých sektorech, od soukromých nemovitostí až po obchodní centra, hotely a průmyslové areály. Během pandemie covidu-19 přešlo např. mnoho hotelů k zabezpečení objektů vzdáleným dohledem, aby snížilo náklady na ostrahu.

„Vzdálený dohled Space nabízí nejvyšší možnou úroveň ochrany se značnou úsporou nákladů, a to až 82,5 % ročně. Toto řešení chrání majetek, minimalizuje ztráty a snižuje kriminalitu prostřednictvím dálkového monitorování speciálně vyškoleným týmem expertů“ upřesňuje Lukáš Převrátil.

Mezi nejnovější inovace Innovis v oblasti zajištění objektu patří Falcon, mobilní platforma určená k monitorování a zabezpečení prostor, kde je fyzické zabezpečení buď nerealizovatelné, nebo finančně nevýhodné. Přináší unikátní kombinaci chytrých kamer detekujících osoby i vozidla, alarmů v reálném čase přenášených do dohledového centra Space a možnosti integrovat bezdrátové detektory pohybu.

Technologie snižují náklady

Jedním z příkladů použití Falconu je zabezpečení dvou čerpacích stanic společností MOL poblíž dálnice D3– Chotýčany. Tyto stanice byly dokončeny, ale zůstaly neobsazené kvůli probíhajícím okolním silničním pracím. Díky Falconu bylo možné zajistit účinnou ochranu těchto lokalit.

Využitím této technologie bylo možné snížit náklady na zabezpečení o více než 50 % ve srovnání s tradiční fyzickou ostrahou. Kromě špičkového dohledu a bezpečnosti Falcon nabízí vlastní konektivitu, ochranu proti sabotáži, reflektory a záložní napájení. Výsledkem je komplexní bezpečnostní řešení, které nejenže zvyšuje kvalitu dohledu, ale také přispívá ke snížení uhlíkové stopy a doby trvání projektu. ■

PETR SIMON

Soukromý detektiv ve firemních službách? A proč ne?!

Soukromý detektiv: Krizový manažer i preventista

Denně jsou přijímána více či méně důležitá rozhodnutí a vždy poté přicházejí i plody těchto voleb. Když se rozhodnutí povede pouze za přispění našeho dobrého instinktu, máme radost, že jsme dítětem štěstěny, anebo jsme si k našemu rozhodování zajistili relevantní informace.

Ne nadarmo se říká, že štěstí přeje připraveným. Zjednodušeně řečeno, před provedením úkonu byla provedena kvalitní příprava. Kvalitní příprava/prevence totiž zakládá podmínky pro přijetí správného rozhodnutí. Zanedbaná, nebo žádná příprava zakládá podmínky k přijímání špatných rozhodnutí, což může vést až k vzniku krize.

Jak do toho všeho zapadá soukromý detektiv jako krizový manažer nebo preventista? A proč je v nadpisu uvedena nejprve krize a až po ní prevence? Vždyť logicky by se nejprve měla realizovat prevence, a když i tak vše selže, pojďme řešit krizi. Vysvětlení je prosté. Většina klientů se bohužel obrací na soukromého detektiva s poptávkou o jeho služby až v okamžiku, kdy ke krizi dojde. Méně klientů si služby soukromého detektiva vyžádá již v rámci přípravy/prevence, aby riziku vzniku případné krize pokud možno předešli. Věří, že udělali dost, a předpokládají, že se jim něco takového nestane. Přitom praxe opakovaně ukazuje, že náklady na přípravu/prevenci, včetně nákladů na služby soukromého detektiva, jsou vždy mnohem nižší než náklady na řešení důsledků vzniklé krize, nemluvě o možné škodě.

Reference vždycky nestačí

Pojďme si dát konkrétní příklad. Statutární zástupce obchodní společnosti byl osloven potenciálním obchodním partnerem s výhodnou nabídkou na spolupráci v oblasti nákupu výrobků a služeb. Statutární zástupce potenciálního odběratele se při tom prezentoval jako seriózní a solventní obchodní partner s možnostmi nákupu velkých objemů produkce dodavatele. Poskytl skvělé reference. Oslovený statuární zástupce dodavatele se v očekávání zajímavých zisků rozhodl tuto výhodnou nabídku přijmout. Jednalo se o obchod v řádu milionů, se zajištěním odbytu velké části produkce dodavatele. Dodávky zboží se rozjely v požadovaných objemech a vše fungovalo bezchybně. Bohužel jen do doby, kdy začaly nabíhat splatnosti faktur. Pak nastal klasický vývoj situace, od různých druhů výmluv statutárního zástupce odběratele až k úplnému radiovému klidu, kdy se v telefonu ozývalo, že volaný účastník je momentálně nedostupný.

V tomto okamžiku statutárnímu zástupci dodavatele došlo, že má problém, a ne malý. Místo zisků počítal ztráty v řádu milionů. Jedním slovem krize. Jelikož se nemohl se statutárním zástupcem dlužníka zkontaktovat, a to jak telefonicky, tak osobně v místě jeho sídla a ani místa bydliště, napadlo jej využít služeb soukromého detektiva. Poptávka zněla: Najít odpovědného zástupce dlužníka a případně zjistit, v čem je problém.

Investovat do prevence se vyplatí

Soukromý detektiv v tomto případě jako krizový manažer svou misi splnil, avšak výsledek šetření jeho klienta nepotěšil. Ukázalo se totiž, že statutární zástupce odběratele/dlužníka je notorický neplatič, zatížený mnoha exekucemi, který využil důvěry statutárního zástupce dodavatele se záměrem zčásti si pomoct vyřešit své osobní dluhy a uspokojit tak nejvíc neodbytné věřitele, a ještě si při tom přijít k nemalým penězům. Využil k tomu obchodní společnost, která se na první pohled jevila jako bonitní.

Avšak jak víme, zdání může klamat. Pokud by se totiž klient/dodavatel obrátil na soukromého detektiva jako na preventistu, a ještě před uzavřením kontraktu si nechal statutárního zástupce potenciálního odběratele prověřit, nemusel soukromého detektiva využívat jako krizového manažera. Stačilo investovat v rámci prevence, což v porovnání s nakonec vzniklou milionovou škodou znamenalo zanedbatelnou částku a ke krizi nemuselo vůbec dojít.

Výše uvedený příběh popisuje skutečnou událost a je exemplárním příkladem toho, že investice do prevence se opravdu vyplatí. Vzniklou škodu totiž nebylo na čem uspokojit. V této souvislosti je třeba připomenout i ustanovení Zákona o obchodních korporacích, Pravidla jednání voleného orgánu, § 51-§ 53, pojednávající o péči řádného hospodáře, říká v § 51: „*Pečlivě a s potřebnými znalostmi jedná ten, kdo mohl při podnikatelském rozhodování v dobré víře rozumně předpokládat, že jedná informovaně a v obhajitelném zájmu obchodní korporace; to neplatí, pokud takovéto rozhodování nebylo učiněno s nezbytnou loajalitou.*“ ■

VLADIMÍR LAKOMÝ, soukromý detektiv, člen prezidia Českého klubu bezpečnostních služeb a člen bezpečnostní sekce HK

NIS2: Čeká nás byrokratická fuška

Evergreenem posledních měsíců je v naší asociaci diskuze k možným dopadům nové kyberbezpečnostní směrnice NIS2, směrnice CER (o odolnosti kritických subjektů) a o tom, jak dopadnou na naše členy. Řada z nich jsou totiž malé podniky.

Lavina nových požadavků se netýká pouze nás, podnikatelů v ICT, ale řady dalších podniků, které se stanou regulovanými subjekty a budou se muset reálně starat o celou řadu konkrétních opatření a politik. Povinnosti jsou totiž doslova za rohem.

Příslušný zákon prošel nedávno meziresortním připomínkovým řízením. Národní úřad pro kybernetickou bezpečnost (NÚKIB) dostal stovky připomínek a zjevně bude muset návrh ještě významně přepracovat. Úřad naštěstí spolu s návrhem zákona

předložil i teze vyhlášek, takže přibližně víme, jaké budou konkrétní požadavky. Ty dopadnou na řadu odvětví – nesmíme si myslet, že jde jenom o IT, naopak, jde o všechno, kde se používá IT a co je významné pro fungování společnosti. Regulováno je asi šedesát služeb v osmnácti odvětvích.

Pokud jste se našli v boxu Koho se týká NIS2, stanete se pravděpodobně Poskytovatelem regulované služby. Řada středních podniků bude takzvaně v režimu nižších povinností, což je ale stále byrokratická fuška. U poskytovatelů služeb elektronických komunikací to navíc budou i malí a mikropodnikatelé.

Špatné a ještě horší zprávy

Pro manažery, kteří budou pověřeni zaváděním opatření podle nového Zákona o kybernetické bezpečnosti, bude mnohdy velmi složité rozpoznat, zda je požadavek pro jejich organizaci relevantní, což je špatná zpráva. Ještě horší zprávou je ale fakt, že odpovědnost za porušení jde podle NIS2 přímo na bedra statutára společnosti. Manažer

archiv VNICTP

KOHO SE TÝKÁ NIS2

- Energetika, například provozovatelé distribuční soustavy, ale i provozovatelé dobíjecích stanic
- Dálkové vytápění
- Skladování a těžba ropy
- Distributoři plynu
- Výrobci vodíku
- Letečtí dopravci a provozovatelé letišť
- Železniční dopravci
- Silniční orgány a ITS
- Banky a finanční trhy
- Zdravotnictví
- Dodavatelé a distributoři vody
- Odpadní vody
- Některé subjekty provádějící výzkum a vývoj
- Subjekty digitální infrastruktury, v podstatě jakékoliv ICT s jakkoliv garantovanou kvalitou služeb
- Veřejná správa
- Poštovní a zasilatelské služby
- Odpadové hospodářství
- Chemický průmysl
- Potravinářství
- Výrobní podniky s vlastní podskupinou
- Poskytovatelé online služeb

kybernetické bezpečnosti však může užít takzvané Prohlášení o aplikovatelnosti (v případě vyššího režimu regulace) nebo plán zavádění bezpečnostních opatření (nižší režim) a neaplikovatelné opatření vyloučit.

Snadné to ale nebude, stačí si ukázat konkrétní příklad, třeba přijímání bezpečnostních opatření pro všechny ICT systémy podniků. To cílí obecně na úkony spojené s ověřováním, kontrolou přenášených dat a blokováním nežádoucí komunikace, které v typické organizaci budou řešeny například

CO BUDOU MUSET DOTČENÉ FIRMY SPLNIT

- Vytvářet analýzu rizik a bezpečnostní politiku informačních systémů
- Dohlížet na řízení incidentů a vytváření eskalačních schémat
- Zajistit kontinuitu podnikání a krizového řízení
- Zajistit bezpečnost při pořizování, vývoji a údržbě sítí, včetně odhalování zranitelností
- Vytvářet bezpečnostní audity k posouzení účinnosti opatření
- Splnit povinnost používání kryptografie a šifrování
- Hlídat bezpečnost dodavatelského řetězce

na perimetrových firewallech, prostřednictvím DDoS praček nebo dalšími nástroji, které mají za úkol chránit interní prostředí organizace před vnějšími vlivy. Typicky jde o administraci, účetnictví, e-mailové služby, komunikaci se zákazníky, cloudové systémy, propojení datových zdrojů a čidel a podobně. Povinnost bude zabezpečit nejenom servery, ale i koncové stanice včetně způsobu jejich připojování do podnikové sítě včetně záznamu o připojování a přidělování rolí, s nutností vícefázového ověřování. Ochrana před škodlivým kódem bude muset být do velké míry automatizovaná. Taková opatření se dají zvládnout, pokud nebudou v praxi vyžadovány nepřiměřené požadavky a úřad akceptuje příslušné analýzy rizik. Což může, ale nemusí nastat.

Když k tomu přidáme i povinnost plnit úřadem plánovanou regulaci bezpečnosti dodavatelského řetězce, pak je čeho se obávat. Především pro malé a střední podniky s několika zaměstnanci to nebude nic jednoduchého. ■

JAKUB REJZEK, Výbor nezávislého ICT průmyslu

Využijte služeb expertů díky CyberSecurityHub[CZ]

Aby vaše kyberbezpečnost nezůstala v koutě

O tom, že je kyberbezpečnost pro vaši firmu důležitá, jste už zřejmě slyšeli. Přetavit povědomí ve smysluplnou akci je však často obtížné. Na tuto skutečnost reaguje CyberSecurityHub[CZ], který je v ČR jediným digitálním hubem (EDIH) zaměřeným na kyberbezpečnost. Díky němu můžete těžit z expertízy tří univerzit a řady dalších organizací, navíc zcela zdarma.

Služby, které CyberSecurityHub[CZ] nabízí, se dají shrnout do čtyř hlavních oblastí. Jedná se o testování produktů nebo služeb, vzdělávání a rozvoj dovedností, budování inovačního ekosystému a podporu pro rozvoj podnikání v oblasti kyberbezpečnosti, včetně poradenství při hledání investic. Tyto služby mají hned několik úrovní pokročilosti, a to se specializací na malé i střední podniky a veřejnou správu. Jejich smyslem je podpora digitální transformace a jejich poskytování je hrazeno z veřejných zdrojů. Klienti CyberSecurityHub[CZ] je tedy odebírají zcela zdarma.

Zaostřeno na malé a střední podniky

Malé podniky jsou páteří naší ekonomiky a digitální transformace je klíčem k jejich udržitelnému růstu. Podobně střední podniky musí neustále hledat cesty k příležitostem digitálních technologií. Jejich využívání s sebou však nese také rizika kyberhrozeb. Že jde o aktuální záležitost, a dokazují například pravidelná hlášení od Národního úřadu pro kybernetickou a informační bezpečnost. Zorientovat se v tom, co všechno oblast kyberbezpečnosti obnáší, však nemusí být snadné, protože se neustále proměňuje a zároveň zahrnuje řadu oblastí – od technologií přes procesy a právo až po vzdělávání zaměstnanců.

Hub jako expertní průvodce

Právě proto řada českých podniků vítá možnost mít expertního průvodce, jakým je CyberSecurityHub[CZ]. Jedinou skutečně zásadní podmínkou pro využívání jeho služeb je aktivní přístup ze strany podniku. V praxi začíná vše tím, že zájemce kontaktuje Hub a v návaznosti na to se na vstupních konzultacích setkají zástupci podniku s experty Hubu. Součástí vstupních konzultací je první služba, takzvané Kyberbezpečnostní posouzení. Jedná se o proces, kdy se identifikují možná rizika a vyhledávají se problematická místa v kyberbezpečnosti firmy. Poté experti Hubu navrhnou sadu doporučení a následné relevantní služby, které mohou podniku v jeho situaci pomoci. Nabídka služeb expertů CyberSecurityHub[CZ] je skutečně široká, řadí se do ní například: vzdělávání zaměstnanců, konzultace strategií a business modelů, pomoc při hledání digitálních příležitostí, výzkumná spolupráce či propojení s poskytovateli finančních prostředků a technologických řešení i dalšími digitálními huby zaměřenými například na oblast AI či průmyslových inovací.
Podnik následně odebírá doporučené služby až do ukončení spolupráce, které má podobu závěrečné reflexe a zpětné vazby. Hlavní výhodou pro české firmy je možnost využití odborných znalostí a zkušeností expertů z několika organizací, včetně tří špičkových univerzit, jimiž jsou brněnské Vysoké učení technické a Masarykova univerzita i pražské České vysoké učení technické. Díky CyberSecurityHub[CZ] se vše odehrává v nastavených mechanismech spolupráce a není nutné oslovovat každou organizaci zvlášť. ■

MARTIN HORÁK

EVROPSKÉ DIGITÁLNÍ HUBY (EDIH)

Iniciativa EU, jejímž cílem je vytvořit v členských státech systémy organizací – huby. Ty mají pomoci podnikům a organizacím veřejného sektoru reagovat na digitální výzvy. EDIH se zaměřují na různé oblasti, například na AI, průmyslové inovace či kyberbezpečnost. V těchto oblastech pak poskytují expertní služby pro zlepšování procesů, produktů i služeb.

O HUBU

Smyslem je posilovat odolnost státu, organizací i společnosti. Založily jej Masarykova univerzita, České vysoké učení technické v Praze a Vysoké učení technické v Brně v roce 2020. Od té doby posiluje pozici a konkurenceschopnost českého výzkumu, vzdělávání a spolupráce se soukromým i veřejným sektorem v oblasti kybernetické bezpečnosti. Nachází se uprostřed CyberCampus[CZ], který zároveň koordinuje. Více informací na www.cybersecurityhub.cz.

CyberCampus[cz]

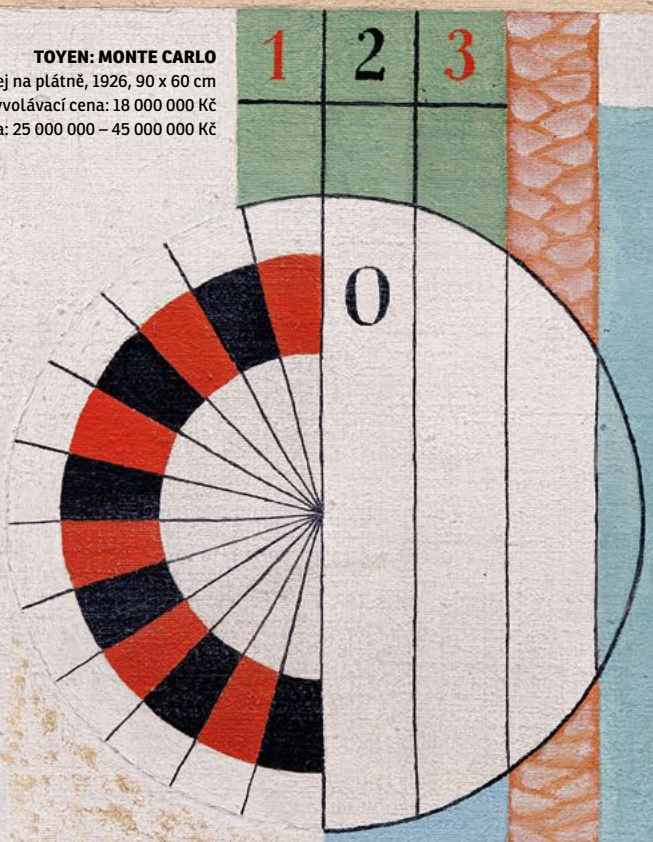
Prostor čelit výzvám budoucnosti

CyberCampus[cz] je symbolem sebevědomého přístupu České republiky k budování odolné digitální společnosti. Jde o geografické území v Brně, které koncentruje na jednom místě klíčové subjekty, kompetence, aktivity i infrastrukturu. Můžete být jeho součástí.

CYBERCAMPUS.CZ

KODL
GALERIE

KODL – TRADICE OD ROKU 1885



TOYEN: MONTE CARLO
olej na plátně, 1926, 90 x 60 cm
vyvolávací cena: 18 000 000 Kč
odhadní cena: 25 000 000 – 45 000 000 Kč

ZVEME VÁS NA LISTOPADOVOU PŘEDAUKČNÍ VÝSTAVU

Aukce se uskuteční 26. 11. na Žofíně
+ online na artslimit.com

TOYEN 26

Tel.: +420 251 512 728, +420 602 117 440
Národní 7, Praha 1 • galerie@galeriekodl.cz

www.galeriekodl.cz