

KOMORA

SPECIÁL



HK ČR
LEGISLATIVA A KVALITA

SONDA
KYBERBEZPEČNOST

POZVÁNKA
SNÍDANĚ S EXPERTY

Soukromé bezpečnostní služby – legislativa a kvalita

Soukromá bezpečnostní činnost má dlouhodobě své stabilní a nezastupitelné místo v ochraně majetku a osob, ale i v systému vnitřní bezpečnosti. Ve stále větší míře doplňuje činnost orgánů státu a územních samosprávných celků při zajišťování vnitřního pořádku. Podstatně se však liší od jiných forem koncesovaného podnikání. Je to především možnost zasahování do právních poměrů třetích osob – při ostraze osob a majetku, při činnosti soukromých detektivů i při instalaci technologií.

Bohužel, postavení soukromých bezpečnostních služeb dosavadní právní úprava neodpovídá. ČR je jednou z posledních zemí Evropy, kde není soukromá bezpečnost (ostraha, technické služby, detektivové, poradci) upravena zvláštním zákonem. O to větší by pak v praxi měl být kladen důraz na kvalitu.

Právní úprava soukromých bezpečnostních služeb

V současné bezpečnostní situaci se nám jeví, že je v oblasti soukromé bezpečnosti nutné vytvořit moderní, jasně strukturovaný a efektivní zákonný rámec, jenž by odpovídal bezpečnostním výzvám současnosti, přispěl ke zvýšení standardů poskytovaných služeb a zároveň zajišťoval dohled a kontrolu nad touto činností. Návrh zákona přirozeně vyvolává širokou odbornou diskuzi, neboť zasahuje do činnosti tisíců subjektů působících v tomto dynamickém a citlivém segmentu. Odborná veřejnost i seriózní podnikatelé se shodují, že chtějí právní rámec oboru řešit, chtějí zlepšit pověst a vztah k veřejnosti a chtějí odstranit současný stav obcházení koncesovaných živností jinými živnostenskými oprávněními – tzv. šedou zónu. Chtějí oddělit profesionální a eticky „naladěné“ firmy od těch druhých. Zákon měly ve svém programu prakticky všechny vlády v porevoluční době. Nikdy se však nedočkal celého legislativního procesu.

Právě nyní, v kontextu probíhajících odborných debat a přípravných legislativních kroků nové vlády, je nesmírně důležité otevřít znovu tuto problematiku. Hospodářská komora České republiky, která sdružuje významnou část podnikatelské sféry působící v oblasti soukromé bezpečnosti, je schopna nabídnout kvalifikovaný pohled z praxe a věcnou argumentaci k jednotlivým navrhovaným ustanovením připravovaného návrhu zákona o soukromých bezpečnostních službách.

Kvalita zakázek bezpečnostních technologií

V odborné i laické veřejnosti stále rostou diskuse o kvalitě techniky, služeb i komplexních dodávek bezpečnostní techniky a technologií. Týká se to jak různých

podomních rábdoby řemeslníků, tak velkých zakázek a bohužel výjimkou nejsou ani veřejné zakázky. Asociace technických bezpečnostních služeb Grémium Alarm (AGA), autorizované Živnostenské společenstvo HK ČR, má ve svém poslání propagaci kvality a garanci odbornosti a profesní etiky. V rámci své působnosti AGA dbá mimo jiné na to, aby její členové vykonávali podnikatelskou činnost odborně a v souladu s obecně závaznými právními předpisy. A také radí, jak volit správnou techniku a technologii pro očekávanou funkci. V neposlední řadě je důležité i správné zadání zakázky a výběr dodavatele nejen podle nejnižší ceny.

Členské firmy AGA s ověřenou právní a odbornou způsobilostí a schopností zpracovat zakázku od kvalitní nabídky přes projekt a montáž až 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>. Ověřování kvality firmy se provádí v souladu se schválenou metodikou Hospodářské komory ČR.

Evropský pohled

V celoevropském měřítku je kvalita instalací bezpečnostních zařízení a technologií řešena technickou normou ČSN EN 16 763: Služby pro požárněbezpečnostní zařízení a zabezpečovací systémy. Ta je v platnosti již několik let, ale v naší republice není doposud naplňována. Norma 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. V ČR není splnění požadavků na služby v tomto citlivém oboru praktikováno a ani investory požadováno. V řadě evropských zemí je tato norma naplňována a odbornou způsobilost prověřuje a certifikát vydává profesní sdružení příslušného oboru. V těchto zemích je tento certifikát samozřejmě i vyžadován a jeho neexistence znevýhodňuje naše firmy při zájmu o zdejší zakázky.

Česká praxe

Asociace technických bezpečnostních služeb Grémium Alarm, která je pro obor technických bezpečnostních služeb autorizovaným živnostenským společenstvem Hospodářské komory ČR, toto osvědčování kvality a registraci firem zahájila. Podle ČSN EN 16763 a dle metodiky HK ČR odborná komise posoudí právní, a především odbornou způsobilost firmy. Firma, která uspěje, obdrží certifikát a je zaregistrována podle ČSN EN 16 763. Zároveň je zařazena na seznam firem s prokazatelně kvalitní profesionální dodávkou požárněbezpečnostního zařízení nebo bezpečnostních technologií, který je uveřejněn mimo jiné na www.gremiumalarm.cz.

Evropské technické normy

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 např. advokátní kanceláře. Poskytuje přehled o mechanickém zabezpečení, poplachových zabezpečovacích a tísňových systémech, kamerách a jejich kombinaci vhodnou 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> nebo <https://mv.gov.cz/>.

Metodika pro veřejné zakázky

Důležitým krokem pro dosažení požadavků, které od bezpečnostních systémů očekáváme, 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 pultu centralizované ochrany. Týká se dodávek komponentů systému (technologické prvky, hardware, software včetně licencí), služeb (např. služby systémové integrace, průběžný servis) nebo díla (např. 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 jen 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>. Odvolávka je také na webových stránkách Ministerstva pro místní rozvoj: <https://mmr.gov.cz> a Ministerstva vnitra ČR na odkazu: <https://prevencekriminality.cz>. ■

Václav Nepraš,
člen prezidia Asociace Grémium Alarm,
člen představenstva HK ČR,
předseda Bezpečnostní sekce HK ČR

Nový zákon o kybernetické bezpečnosti: Co čeká některé firmy

Kybernetická bezpečnost se stává povinností, ne volbou

Hrozby působící z kybernetického prostoru jsou problémem i pro malé a střední podniky. Právě proto přichází nová evropská směrnice NIS2, směrnice (EU) 2022/2555 o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v EU.



Tato směrnice navazuje na původní směrnici NIS z roku 2016, přičemž:

- výrazně rozšiřuje okruh subjektů, které musí dodržovat kyberbezpečnostní pravidla;
- zpřísňuje požadavky na řízení rizik a na bezpečnostní opatření;
- zavádí přímou odpovědnost managementu;
- zajišťuje harmonizaci v rámci EU, především sjednocuje sankce a dohled.

Požadavky směrnice NIS2 jsou natolik rozsáhlé a koncepčně odlišné, že vznikl zcela nový zákon č. 264/2025 Sb. o kybernetické bezpečnosti včetně prováděcích předpisů, především vyhlášky pro regulaci v režimu vyšších a nižších povinností (tzv. dvourychlostní regulace), a to s účinností k 1. 11. 2025.

Cílem nové legislativy je zvýšit odolnost firem i státu vůči rostoucím hrozbám v online prostředí. Dopadne mj. na tisíce firem, které se kybernetické bezpečnosti doposud nevěnovaly.

Koho se nový zákon týká

Nový zákon rozšiřuje povinnost dodržovat kybernetickou bezpečnost i na střední a menší podniky, které působí v důležitých odvětvích – například výroba, energetika, doprava, zdravotnictví, IT služby, finance nebo správa dat. Nezáleží jen na velikosti firmy, ale i na tom, jaké služby poskytuje a komu. Pokud například spolupracujete s větší organizací spadající pod novou legislativu, je pravděpodobné, že požadavky dopadnou i na vás. Ověřte si, zda spadáte do působnosti nového zákona (<https://portal.nukib.gov.cz/kalkulacka>).

Co bude potřeba udělat

Již nejde o pouhou formalitu. Firmy, na které se zákon vztahuje, budou muset především:

- Zajistit kybernetickou bezpečnost svých systémů a sítí.
- Mít zajištěny požadované bezpečnostní role.
- Nastavit procesy pro hlášení a řešení kybernetických bezpečnostních incidentů.
- Školit zaměstnance, a to alespoň v rozsahu požadavků prováděcích předpisů.

Poskytovatel regulované služby musí hlásit Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB) kontaktní údaje a doplňující údaje, stanovit rozsah řízení kybernetické bezpečnosti, plnit uložená bezpečnostní opatření, hlásit kybernetické bezpečnostní incidenty a také je zvládat, plnit informační povinnost vůči uživatelům regulované služby, poskytnout NÚKIB při zajišťování podkladů pro vydání protiopatření nezbytnou součinnost a provádět reaktivní protiopatření.

Proč se vyplatí být připraven

Nedodržení zákona může znamenat vysoké pokuty (až milionové částky), ale hlavní riziko spočívá jinde: v přerušení provozu, ztrátě dat nebo důvěry zákazníků. Firmy, které kybernetickou bezpečnost pojmu strategicky, mohou získat výhodu na trhu – stanou se důvěryhodnějšími partnery s potenciálem uspět ve výběrových řízeních.

Jak začít

Nemusíte hned pořizovat drahé technologie. Zmapujte si služby, které poskytujete, a vyhodnoťte pro ně dopad v případě narušení důvěrnosti, integrity, dostupnosti. Určete kritické služby a proveďte pro ně dopadovou analýzu (BIA). Z dopadové analýzy odvoďte kritické procesy a aktiva. Zavádějte bezpečnostní opatření a určujte priority podle výsledků. Využijte nabídku školení nebo konzultací, které poskytuje NÚKIB či HK ČR. Nový zákon o kybernetické bezpečnosti může znít složitě, ale jeho podstata je prostá: Chránit to nejcennější, co máte – data, zákazníky a důvěru. Firmy, které začnou s přípravou včas, budou mít kybernetickou bezpečnost pevně pod kontrolou. ■

Jiří Sedláček

Nové možnosti pro české firmy

CyberSecurity Innovation Hub vstupuje do druhé fáze

Úspěšný pilotní projekt EDIH ukázal obrovský zájem českých firem o kyberbezpečnost. Nyní přichází jeho pokračování s rozšířenými možnostmi – včetně podpory pro větší podniky a zaměření na bezpečnost umělé inteligence.

Pilotní projekt EDIH CyberSecurity Innovation Hub se v současnosti úspěšně blíží ke svému závěru. Zájem českých firem a veřejných organizací splnil veškerá očekávání. Proto přichází navazující EDIH projekt, který plynule staví na osvědčených základech a otevírá nové možnosti.

Co přinesl pilotní projekt

Za dobu fungování pilotního EDIH projektu jsme získali cenné poznatky a prokázali obrovskou poptávku po kyberbezpečnostních službách. Důkazem je více než 150 uzavřených smluv s firemními i veřejnoprávními klienty z celé České republiky. Mezi našimi klienty najdete společnosti z průmyslové výroby, leteckého průmyslu i služeb, stejně jako instituce veřejného sektoru – od Úřadu vlády ČR nebo Policie ČR až po nemocnice a soudy. Vyškolili jsme přes 2 500 osob ve více než 260 turnusech školení a oslovili okolo 5 300 účastníků osvětových aktivit. Téměř všechny organizace těží z odborné podpory. Ukázkovým příkladem je Fakultní nemocnice Brno, kde jsme po letech od ransomwarového útoku realizovali komplexní kybercvičení, které výrazně zlepšilo připravenost personálu na skutečné hrozby.

Organizacím nabízíme přes 40 expertních služeb, které na trhu nemají obdoby – například společný vzdělávací program všech tří univerzit (MU, VUT, ČVUT) nebo přenos nejnovějších výsledků výzkumu z AI do kurzů pro malé a střední podniky. Tyto aktivity financují programy Digitální Evropa a Národní plán obnovy.

Čtyři klíčové změny v navazujícím EDIH projektu

1. Bezpečnost umělé inteligence jako priorit

Pilotní EDIH projekt se zaměřoval na kyberbezpečnostní aspekty digitalizace. Navazující EDIH projekt přidává kyberbezpečnost AI jako hlavní téma.

2. Podpora pro větší podniky

Pilotní projekt byl kvůli podmínkám financování omezen na firmy do 499 zaměstnanců. Navazující projekt zvyšuje limit na 3 000 zaměstnanců.

3. Mezinárodní spolupráce včetně sdílení infrastruktury

V pilotním projektu byla zahraniční spolupráce omezena na výměnu zkušeností. Navazující projekt umožňuje sdílet i infrastrukturu, a to napříč Evropou.



4. Rozšíření spektra služeb

Model navazujícího projektu umožní poskytovat ještě širší spektrum služeb a zajistí dlouhodobou udržitelnost projektu.

Co to znamená pro vaši firmu

Pokud je vaše společnost součástí českého průmyslu, digitalizujete procesy nebo zavádíte nástroje AI, CyberSecurity Innovation Hub II vám nabízí odbornou podporu, kterou na trhu jinde ne získáte.

Projekt předkládá čtyři kategorie služeb v jednom místě:

- Testování před investováním – kyberbezpečnostní hodnocení, penetrační testy, využití CyberRange.cz pro praktické kybercvičení.
- Vzdělávání a digitální dovednosti – školení pro manažery i IT specialisty, od základních po pokročilé úrovně.
- Inovační ekosystém a networking – napojení na AI Factories, AI-on-Demand platformu a další evropské iniciativy.
- Přístup k investicím a financování – zprostředkování přístupu k veřejným i k soukromým zdrojům financování.

Služby začínají vstupní konzultací, při níž společně identifikujeme vaše potřeby. Díky širokému konsorciu máte přístup k expertize špičkových univerzit a odborných organizací v jasně strukturovaném modelu. Díky tomu je výsledkem skutečné posílení vaší bezpečnosti a odolnosti. ■

Martin Horák

Více informací najdete na webových stránkách
cshub.cz



Foto: archiv Axenta

SOC – dříve neznámý pojem se dnes stává standardem

S příchodem nového Zákona o kybernetické bezpečnosti nastává zásadní posun pro větší počet organizací – čekají je nové povinnosti, jejichž součástí budou nevyhnutelně také technická opatření.

Kybernetická bezpečnost stojí na třech pilířích

Důvěrnosti, dostupnosti a integrity. V AXENTA se zákazníci budujeme vztah založený na vzájemné důvěře, s jistotou, že se mohou opřít o partnera s dlouholetou expertizou a zkušenostmi v oboru.

Poměrně dlouho bylo obtížné přesvědčit veřejnost, že kybernetická bezpečnost nepatří přímo do kategorie IT, tedy informačních technologií, ale je samostatným oborem, přičemž IT pouze zajišťuje její provoz. Dnes už je to obecně známý fakt.

Co se skrývá za zkratkou SOC?

Security Operations Centre (dále jen SOC) je specializovaným centrem kybernetické bezpečnosti, které umožňuje zákazníkům eliminaci rizik spojených s kybernetickými hrozbami. Důležité je vnímat SOC jako souhrn tří základních prvků – technologií, lidí a správně nastavených procesů. Zjednodušeně si jej můžeme představit jako stroj s ozubenými koly: funguje správně jen tehdy, když do sebe jednotlivá kola a jejich zuby zapadají. Pokud se jedno zasekne nebo poškodí, celý stroj se zastaví.

Antivirus? Dnes už nestačí, potřebujete víc

Kybernetické incidenty jsou dnes bohužel běžnou součástí našeho života. Útočníci si dávno nevybírají jen vel-

ké firmy, napadají i ty „menší“. Pokud se tedy vyhýbáte realitě a stále žijete v pocitu bezpečí s oblíbenou frází: „Mně se to stát nemůže, vždyť mám antivirus na všech zařízeních“, děláte velkou chybu.

Role antiviru je bezpochyby důležitá – představuje první obranný štít a dokáže se vypořádat s jednoduššími hrozbami. Moderní a sofistikované útoky, jako je ransomware, pokročilý malware nebo útoky s využitím vzdáleného přístupu, však tradiční antivirové programy často překonají. V těchto případech je už jejich účinnost nedostatečná a iluzorní. Cílem útočníků je získat přístup do systémů, zcizit či poškodit data nebo přerušit výrobu. To jsou situace, které si zcela jistě nikdo nepřeje řešit.

Moderní technologie rozhodují o síle SOC

Zákazníci očekávají, že jejich systémy budou stále odolné, dostupné, plně funkční a vždy chráněné – a právě technologie to umožňují. Klíčovou roli při zachování vysokého standardu bezpečnosti hraje

plánování. Technické návrhy AXENTA týmu zohledňují nejen plnění požadavků legislativy, ale jejich neoddělitelnou součástí je také integrace vlastní či externí infrastruktury zákazníka do jednoho funkčního celku. Dalšími faktory jsou samozřejmě individuální požadavky zákazníka ohledně implementace technologií pro ochranu jeho systémů a také finance – náklady na provoz i náklady na lidské zdroje. A nad tím vším stojí špičkové technologie, které tvoří základní esenci celého systému.

Mám technologii, tedy jsem chráněn? Není to tak jednoduché...

Technologie bez procesů neznamena bezpečnost. Je nutné mít jasně nastavené odpovědnosti, úkoly a kontrolní mechanismy. Pouze dobře definované procesy zabrání chaosu a zajistí efektivní reakce na incidenty.

Bez správných expertů zůstává i nejlepší technologie neúplnou

Lidé jsou klíčem funkčního SOC. Tým odborníků se musí neustále vzdělávat, sdílet zkušenosti a tím zvyšovat kvalitu celého řešení.

Vzdělávání – klíčová investice do bezpečnosti

Nedostatek kvalifikovaných expertů je celosvětovým problémem. V AXENTA jsme se rozhodli jednat a zapojili do výuky kybernetické bezpečnosti střední školy. Tím jsme umožnili studentům získat praxi v našem SOC. Tento model se osvědčil: dnešní kolegové jsou mimo jiné absolventy tohoto programu.

Čas hraje proti nám – automatizace je nutností

Nedostatek lidí a rostoucí počet incidentů vedou k automatizaci. Díky ní lze zrychlit detekci hrozeb, analýzu incidentů i reporting. Automatizace zvyšuje efektivitu, snižuje chybovost a umožňuje analytikům soustředit se na komplexní úlohy. Nástroje jako SIEM, SOAR a AI umožňují pokročilou analýzu hrozeb. Automatizovaný reporting přináší přehled a lepší rozhodování.

V AXENTA dlouhodobě vyvíjíme vlastní projekty automatizace SOC procesů.

Chci SOC, který funguje. Na co se při výběru zaměřit?

Volba poskytovatele služeb bezpečnostního dohledu patří mezi klíčová rozhodnutí v oblasti řízení kybernetických rizik. Organizace, které se rozhodují pro outsourcing nebo posílení interních kapacit, často narážejí na otázku, jak správně definovat své potřeby a jak nastavit kritéria výběru poskytovatele, aby výsledkem byl funkční a dlouhodobě udržitelný model spolupráce. Před oslovením potenciálních poskytovatelů je ze strany zákazníka nezbytné provést důkladnou přípravu, která zahrnuje definici kritických systémů a služeb, stanovení požadavků na dobu reakce, přehled stávajících bezpečnostních a provozních procesů, posouzení možností integrace a určení rozpočtu. Dále je nutné porovnávat režimy poskytování dohledu – standardní pracovní doba (8x5), nepřetržitý dohled (24x7) či hybridní modely – a jejich dopad na rizika a provozní náklady. Zvláštní pozornost je věnována rozdílu mezi on-site modelem (tzv. body shopping, kdy dodavatel poskytuje lidské kapacity přímo v prostředí zákazníka) a off-site variantou využívající Managed Security Service Provider (MSSP). Oba přístupy mají své výhody i nevýhody: on-site model nabízí hlubší znalost prostředí a lepší integraci do interních procesů, zatímco MSSP řešení přináší škálovatelnost, sdílené know-how a nepřetržité služby bez nutnosti vysokých interních investic.

Pro úspěšný výběr služby SOC je nezbytné definovat takzvaná KO kritéria, která umožní rychle vyloučit nevhodné poskytovatele: dostupnost, SLA, certifikace, zkušenosti týmu, technická kompatibilita a důvěryhodnost. Důležité je také nastavit jasná očekávání v oblastech, jako jsou reporting, reakční postupy při incidentech, možnosti testování služeb či zapojení zákazníka do rozhodování. Kvalitní příprava a jasná očekávání vám zajistí správnou volbu partnera. ■

Petra Lichvárová

AXENTA CyberSOC

Nepřetržitě monitoruje, analyzuje a zmírňuje kybernetické hrozby v reálném čase, 24/7 – zajistí, že vaše systémy zůstanou odolné, dostupné, funkční a vždy chráněné.

- Hladce a bezbolestně integrujete vlastní nebo externě dodávanou infrastrukturu.
- Využíváte odborných znalostí bezpečnostních specialistů s více než patnáctiletou praxí v oboru.
- Zajistíte si soulad s legislativou i vlastními požadavky v oblasti kybernetické bezpečnosti.
- Získáte jistotu ve stabilní a spolehlivé službě s vysokou dostupností (High Availability) v České republice a na Slovensku.
- Vaše důležitá data budou chráněna s důrazem na důvěrnost, integritu a dostupnost (Confidentiality, Integrity, and Availability).
- Využíváte inovativní řešení a nejmodernější technologie bezpečnostního monitoringu s nejvyšší úrovní ochrany.
- Získáte kvalitní, na míru šité řešení, které je efektivní a přizpůsobí se vašim specifickým požadavkům.
- V zákaznickém dashboardu Cyber Copter přehledně zobrazíte výstupy technologií, které vás chrání.

Success Story

Každá vteřina se počítá – odbornost zachraňuje

Jak vypadá konkrétní kyberbezpečnostní incident si můžeme ukázat na zásahu našeho týmu Digital Forensics and Incident Response (DFIR) u společnosti, která podcenila bezpečnostní opatření a v důsledku toho se stala obětí kybernetického útoku.



Ukážeme, jak je klíčové mít zkušený tým, který i v chaotické situaci reaguje rychle a systematicky.

DFIR tým je specializovaný tým zaměřený na digitální forenzní analýzu a reakci na kybernetické incidenty. Jeho úkolem je identifikovat, analyzovat a obnovit kompromitované systémy, včetně zajištění důkazů pro další šetření.

Co se vlastně stalo?

Náš DFIR tým zasahoval u firmy, která nás kontaktovala, protože se stala obětí kybernetického útoku. Jednalo se o ransomware útok. Zašifrovány byly produkční servery i dvě zálohy – lokální a uložené u dodavatele. Situace se zkomplikovala tím, že jsme byli povoláni téměř 24 hodin po útoku, přičemž dodavatel servery již restartoval a přemazal, čímž jsme přišli o možnost extrahovat šifrovací klíč z paměti RAM a zajistit tak obnovení dat.

Jak probíhal zásah na místě?

Po úvodní analýze jsme identifikovali ransomware LockBit 3. O. Prověřili jsme dostupné decryptory i možnost reverzního inženýrství, ale žádné řešení nebylo použitelné. Bylo nutné získat dešifrovací nástroj od útočníků. Ten jsme nejprve bezpečně otestovali a následně provedli dešifrování produkčních serverů, záloh i infrastruktury, čímž jsme obnovili klíčová data.

Podarilo se dostat situaci pod kontrolu?

Ano. Díky rychlé reakci, spolupráci s dodavatelem systému a odbornému postupu jsme do týdne obnovili provoz firmy. Rychlost týmu včetně jeho připravenosti

umožnily minimalizovat ztráty. Díky tomu mohl zákazník pokračovat v běžné činnosti.

Dalo se útoku předejít?

Ano, pokud by byla již dříve zavedena adekvátní bezpečnostní opatření. Po každém incidentu je klíčové zjistit příčiny, nasadit monitoring a odstranit zranitelnosti. V tomto případě se však zákazník rozhodl útok neanalyzovat a vybudovat zcela novou síť s novými technologiemi a dodavateli.

Jak může správný zásah expertů ochránit organizaci?

DFIR tým dokáže urychlit obnovení provozu, minimalizovat škody a často i snížit finanční, reputační a další obdobné negativní dopady. Zároveň provádí analýzu incidentu a pomáhá uzavřít bezpečnostní mezery, aby se podobná situace neopakovala. Díky rychlosti, odbornosti a systematickému přístupu chráníme provoz organizací a zmírňujeme dopady útoků.

Proaktivní přístup dnes znamená méně škod zítra

Je třeba si uvědomit, že trend kybernetických útoků směřuje k větší četnosti i sofistikovanosti. S rozvojem AI a dalších technologií se útočníci stále více zaměřují na deepfake a manipulaci obsahu, AI-generované phishing útoky a zranitelnosti v nových technologiích. Podcenění či absence bezpečnostních opatření často způsobí, že prostředí organizace je zranitelné. Příčinou často bývají jiné priority vedení převážně provozního charakteru, včetně nedostatku zdrojů, odborníků či zkušeností. Útočníci využívají každé slabiny. Kybernetické incidenty jsou stále častější a sofistikovanější, od tichých infiltračních aktivit až po rychlé kampaně. Mohou zasáhnout každou organizaci a otřást nejen rozpočty, ale i důvěrou partnerů a zákazníků. Když dojde k incidentu, správně zvolené preventivní kroky a postupy umožňují eliminovat či minimalizovat škody a rychle obnovit provoz každé organizace. A právě v okamžiku krize je neocenitelná přítomnost zkušeného a odborně vybaveného týmu, který dokáže reagovat rychle, řízeně a efektivně. ■

Petra Lichvářová

Dárkové poukazy

Divadelní zážitek
pro vaše blízké



**HUDEBNÍ
DIVADLO
KARLÍN**

www.hdk.cz



Prima

BLESK

Mateřidouška

kdyžde

RPM

DERMACOL

PRAGUE BOATS

sodastream

LIBERSKÉ
LAHODKY

VÁJBAR

PRA
PRA
GA
PRA
G

Nové hrozby v kyberprostoru:
člověk, kvantové počítače a umělá inteligence

S užitím ICT se svět mění rychleji, než stíháme reagovat

Kybernetická bezpečnost už dávno neznamena jen instalaci antiviru a používání silných hesel. Technologie se vyvíjejí nebývalým tempem – a stejným tempem se přizpůsobují i metody útočníků. Zatímco organizace investují do zabezpečení sítí, serverů a cloudových služeb, často si neuvědomují, že nejslabším článkem zůstává člověk.

**KYBERBEZPEČNOST
DNES NENÍ JEN ÚKOLEM
NĚJAKÉHO ODDĚLENÍ
ČI BEZPEČNOSTNÍ ROLE,
ALE SOUČÁSTÍ FIREMNÍ
KULTURY.**



Rychlý technologický pokrok však přináší i nové výzvy. S rozvojem kvantových počítačů a stále „chytřejší“ umělé inteligence se objevují zcela nové typy hrozeb, na které současné bezpečnostní přístupy nemusí stačit. Jaké riziko tedy tyto trendy představují – a jak se na ně můžeme včas připravit?

Lidský faktor: nejslabším článkem zůstává člověk

Kyberútoky se stále častěji zaměřují na to, co žádný software ani hardware neochrání – na lidskou chybu. Útočníci vědí, že nejrychlejší cestou do firemní sítě není složitý hack, ale obyčejný e-mail. Pomocí takzvaného spear-phishing útoku dokážou vytvořit důvěryhodnou zprávu, která vypadá, jako by přišla od kolegy, nadřízeného, nebo obchodního partnera. Stačí jeden klik na odkaz a útočník získá přístup k vašim datům i účtům.

Podle statistik bezpečnostních autorit je více než 80 % incidentů v ČR způsobeno lidskou chybou – nejčastěji kliknutím na podvržený odkaz, sdílením hesla nebo špatným nastavením přístupových práv v cloud službách. Často používaná hesla typu *Firma2023!* či *Heslo12345* už dnes opravdu neobstojí. Útočníci využívají databáze uniklých přístupových údajů, včetně automatizovaných nástrojů, s jejichž pomocí vyzkouší během sekund tisíce kombinací...

Co s tím? Klíčové kroky k posílení kybernetické bezpečnosti organizace

- Určete odpovědnou osobu za oblast kybernetické bezpečnosti.
- Zaved'te interní bezpečnostní pravidla a doplňte je vhodnými technologiemi.
- Používejte vícefaktorové ověřování (MFA) u všech klíčových přístupů.

- Pravidelně školte zaměstnance, ideálně formou praktických simulací (např. phishing útoků).
- Udržujte bezpečnostní povědomí na stabilní a dostatečné úrovni napříč celou organizací.
- Testujte pravidelně odolnost vůči phishing útokům a vyhodnocujte výsledky.
- Budujte interní bezpečnostní kulturu – motivujte zaměstnance, aby hlásili podezřelé zprávy a nebáli se přiznat chybu, pokud k ní dojde.

Kyberbezpečnost dnes není jen úkolem nějakého oddělení či bezpečnostní role, ale součástí firemní kultury.

OSINT (Open Source Intelligence): když útočník „nehackuje“, ale jen hledá

Moderní útočníci často nepotřebují prolomit žádné zabezpečení – stačí jim to, co lidé o sobě a o své firmě veřejně v kybernetickém prostoru sdílejí. Z otevřených zdrojů – jako jsou sociální sítě, komunikační platformy, webové stránky, tiskové zprávy nebo veřejné rejstříky – lze během několika minut poskládat detailní obraz o organizační a vlastnické struktuře firmy, její platební bilanci, o kontaktních údajích, e-mailových adresách, firemní kultuře i zvyklostech zaměstnanců. Tyto informace jsou pak velice efektivně využity k cíleným phishing útokům nebo například k přípravě podvodů typu CEO fraud, kdy útočník přesvědčivě napodobí styl komunikace vedení.

Jak se bránit?

Omezte množství zveřejňovaných informací o vnitřním fungování firmy.

- Pravidelně provádějte OSINT audity – zjistíte, co lze o vás a vaší firmě veřejně dohledat.
- Učte zaměstnance, že i neškodné vypadající příspěvky (např. fotka z kanceláře nebo podpis v e-mailu) mohou útočníkovi poskytnout velmi cenné indicie.

OSINT není sám o sobě nebezpečným – nebezpečné je, když ho někdo použije proti vám.

Postkvantová éra: Když matematika přestane chránit

Zatímco dnes používáme šifrování, které by běžný počítač prolomil až za tisíce let, kvantové počítače (QC) mohou tuto situaci změnit. Využívají principy kvantové fyziky a matematiky, díky nimž dokážou řešit složité výpočty výrazně rychleji než klasické stroje. To znamená, že současné kryptografické algoritmy, jako jsou RSA nebo ECC, mohou být v horizontu několika let prolomeny. Zpočátku navíc pravděpodobně nebude veřejně známo, kdo tyto schopnosti ovládá – což mu poskytne výraznou taktickou výhodu. Historie nabízí podobný příklad – prolomení německé šifry Enigma během druhé světové války bylo pečlivě utajeno. Tak byla zachována právě výrazná taktická výhoda.

Zní to jako science fiction, ale výzkum v oblasti kvantových počítačů postupuje mlhovými kroky. USA, Čína i EU investují miliardy do vývoje kvantových technologií. Jakmile se podaří vyvinout stabilní kvantový procesor s dostatečným počtem qubitů, všechny staré šifry budou ohroženy – od e-mailů až po datové přenosy mezi bankami.

Co s tím?

- Firmy by měly sledovat vývoj takzvané postkvantové kryptografie (PQC) – nových algoritmů odolných vůči kvantovým útokům.
 - Začít mapovat, jaká data uchovávají a šifrují (pokud vůbec...) – zejména ta, která musí zůstat důvěrná i za deset let.
 - Spolupracovat s IT dodavateli, kteří už nyní počítají s přechodem na post-quantum security.
- Kvantová revoluce sice ještě nenastala, ale je blíž, než si myslíme. A kdo se začne připravovat včas, ušetří si v budoucnu velké starosti. Útokům s využitím QC se na svých web stránkách věnuje i naše národní autorita v oblasti kybernetické a informační bezpečnosti – NÚKIB.

Umělá inteligence (AI): Nástroj i hrozba, tedy dobrý sluha, ale zlý pán

AI přináší obrovský potenciál – automatizuje rutinní práci, analyzuje hrozby a zajišťuje ochranu sítí. Zároveň však vytváří zcela nové typy útoků a její nadměrné používání může mít nepříznivé dopady na psychiku uživatelů. Zejména u dětí může nadměrné užívání ICT, včetně AI, negativně ovlivnit jejich vývoj. Útočníci dnes využívají AI k psaní dokonalých, gramaticky správných phishing e-mailů, k tvorbě realistických deepfake videí nebo generování hlasů manažerů, kteří „volají z dovolené a potřebují rychle převést peníze“ z účtu na účet.

AI navíc dokáže napodobovat lidské chování – například komunikaci na sociálních sítích nebo styl psaní konkrétního člověka. To zvyšuje úspěšnost útoků s využitím sociálního inženýrství, protože oběť nemá šanci odhalit, že nekomunikuje s člověkem, ale s AI.

Jak se bránit?

- Používat ověřené komunikační kanály (například oficiální firemní aplikace místo „volných“ messengerů).
- Zavést interní procesy pro ověřování finančních transakcí – žádný převod se nesmí realizovat na základě e-mailu nebo telefonátu bez ověření a potvrzení.
- Sledovat, jaké nástroje AI používají zaměstnanci, co s nimi mohou sdílet a sdílejí, a zajistit jejich bezpečné nastavení.

AI je mocným nástrojem. V rukou zodpovědných lidí dokáže chránit, v rukou útočníků ohrožovat. Klíčem je vědět, jak ji využívat bezpečně.

Kybernetická bezpečnost jako konkurenční výhoda

Kybernetické hrozby se vyvíjejí stejně rychle jako technologie, které používáme. Bezpečnostní strategie proto musí být živým procesem, nikoli jednorázovým projektem. Lidský faktor, PQC i AI mají společného jmenovatele: potřebu vzdělávání, prevence a včasné reakce. Firmy, které pochopí, že kybernetická bezpečnost není jen nákladem, ale investicí do důvěry a stability, budou připraveny i na budoucí výzvy. ■

Jiří Sedláček

Kybernetická bezpečnost jako nová manažerská odpovědnost

Jak ochránit podnik před útoky a ztrátou důvěry

Digitální prostředí se stalo neoddělitelnou součástí podnikání. Stejně jako daňové povinnosti, pracovní smlouvy nebo ochrana majetku. S rostoucím počtem útoků po celé Evropě se kybernetická bezpečnost mění ze „zbytného IT tématu“ na zákonnou odpovědnost vedení firem. A to bez ohledu na velikost společnosti.

Jak na funkční kyberbezpečnost?

Základem není jen správná technologie, ale pochopení rizik, nastavení odpovědností a vytvoření firemní kultury podporující bezpečné chování.

Audit a analýza rizik

Detailní zmapování zabezpečení z pohledu technologií, procesů, dokumentace i lidského faktoru. Výsledkem je identifikace slabých míst a konkrétní návrhy opatření.

Implementace do praxe

Doporučení nestačí. Klíčové nastavení procesů a postupů, přijetí interních předpisů, jasné vymezení odpovědností, úprava vztahů s dodavateli a kontrolní mechanismy.

Školení managementu a zaměstnanců

Lidé jsou nejčastějším cílem útoků i v první linii obrany. Vzdělávání je proto nedílnou součástí bezpečnostní strategie. Zahnuje jak onboarding nového pracovníka, tak pravidelný trénink aktualizovaný podle měnících se hrozeb.



Foto: archiv VIA JURIS a AttentiD, Canva.com

Kybernetické riziko? Otázka není, jestli k němu dojde, ale kdy

Ransomware, výpadky dodavatelského řetězce, únik dat, nebo „obyčejná“ lidská chyba. Kybernetická bezpečnost dnes nechrání pouze citlivé informace, ale přímo kontinuitu podnikání, finanční stabilitu a reputaci společnosti. Moderní útoky jsou sofistikované, často cílené na menší a střední podniky, právě kvůli nízké úrovni zabezpečení.

Přijmout bezpečnostní opatření dnes neznamená jen pořídit antivir, firewall nebo uspořádat jednorázové školení. Efektivní ochrana spočívá v propojení technologií, procesů, návyků lidí a aktuálních právních povinností. To vše ale získá skutečný smysl až ve chvíli, kdy se vše podaří správně uvést do každodenní praxe.

Legislativní realita: Přímá odpovědnost vedení

K 1. listopadu 2025 nabytí účinnosti nový zákon o kybernetické bezpečnosti (ZoKB), který implementuje evropskou směrnici NIS2. Rozšířil se tak okruh regulovaných firem – nově i na sektory jako stavebnictví, potravinářství, poštovní a kurýrní služby nebo zpracovatelský průmysl.

Za dodržování bezpečnostních opatření nese přímou odpovědnost vedení firmy, nikoliv jen IT správce nebo dodavatel. V praxi to znamená nutnost schvalovat opatření, dohlížet na jejich plnění a nést následky při pochybení včetně možného zákazu výkonu funkce statutára. Ve hře tak není jen ochrana firemních dat a reputace, ale i právní důsledky včetně možných osobních postihů.

Co podniky nejčastěji podceňují?

Mnoho firem má obecné povědomí o rizicích, ale chybí jim systém. Mají pocit, že „nejdou dost velké, aby někoho zajímaly“ nebo že „kybernetická bezpečnost je záležitostí IT oddělení“. Jenže právě absence procesního a právního zakončení bývá největší slabinou. A často i nejdražší chybou.

Typický scénář? Společnost si nechá vypracovat technický audit. Výsledky jsou jasné, doporučení rozumná, ale jejich implementace skončí v šuplíku. Lidově řečeno: „neudělá se to B“. Neexistují interní postupy a předpisy. Zaměstnanci nejsou proškoleni. Povinnosti nejsou jasné definovány. Bezpečnostní opatření nejsou součástí onboardingu, nikdo nekontroluje jejich dodržování. Nebo jiný příklad z praxe: Firma uzavře smlouvu s IT dodavatelem, ale chybí bezpečnostní doložky. Při incidentu pak nelze prokázat odpovědnost, škodu nese firma sama. Běžné je také, že zaměstnanec klikne na podvodný e-mail, stáhne přílohu a firma musí na několik dní stopnout provoz. Bez krizového plánu a právně ošetřených pravidel přichází zmatek, reputační ztráta a někdy i právní dohry.

To všechno může být z právního hlediska považováno za porušení péče řádného hospodáře. Obzvláště pokud firma do bezpečnosti investovala, ale opatření nepřivedla do praxe.

Kde začít? Využijte dostupné zdroje

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) v současné době vydává velké množství doporučení a materiálů pro subjekty, které od 1. 11. 2025 spadají pod ZoKB. Vydal ale také například podpůrný materiál pro subjekty, na které se ZoKB nevztahuje, a to v podobě minimálního bezpečnostního standardu. Jedním z dalších materiálů NÚKIB, kterým je vhodné věnovat pozornost, je dokument obsahující požadavky na smlouvy s dodavateli. Ten na necelých 20 stranách podrobněji vysvětluje, jaké požadavky, resp. ustanovení mohou být z hlediska kybernetické bezpečnosti vhodné k začlenění do obchodních smluv.

Všechny citované materiály jsou dostupné na webových stránkách NÚKIBu a v rámci implementace jakýchkoli kyberbezpečnostních opatření je vřele doporučujeme vaší pozornosti. A to i v případě, že se na vás ZoKB nevztahuje.

Již nyní lze předpokládat, že právě tyto minimální standardy a doporučení budou v budoucnu považovány za best practice v oblasti kyberbezpečnosti. Jejich dodržováním se tedy v krajním případě může z hlediska odpovědnosti za vznik a důsledky bezpečnostního incidentu vyvinut nejen firma, ale i její vedení.

Dlouhodobá stabilita se nebuduje zavedením technologií, ale přístupem

Pro firmy, které chtějí být nejen chráněné, ale i dlouhodobě v bezpečnosti udržitelné, už nestačí soustředit se pouze na technické nastavení. Aby bezpečnostní opatření skutečně fungovala a měla oporu v právním rámci, je nezbytné propojit technologické, procesní a legislativní aspekty v jeden celek.

V praxi to znamená nejen zajištění přehlednosti a právní jistoty, ale i odstranění zbytečných duplicí mezi doda-

vatelem, snížení nákladů, a především přizpůsobení celého systému konkrétnímu provozu firmy. Teprve tehdy má kybernetická bezpečnost reálný dopad na kontinuitu podnikání.

Podle advokátky Alexandry Máry Paurové, zakladatelky advokátní kanceláře VIA IURIS, není cílem vytvořit složitou dokumentaci, která skončí v šuplíku: „*Skutečná bezpečnost vzniká teprve tehdy, když firma opatření pochopí, přijme za svá a začne je reálně používat. Jinak řečeno, až když se stanou součástí její kultury a fungování.*“

Na to navazuje i zkušenost specialisty na kyberbezpečnost Štěpána Horáka, zakladatele firmy AttentID, který v oblasti kybernetické bezpečnosti dlouhodobě spolupracuje s firmami napříč obory: „*Bezpečnost není jen technická disciplína. Je to vědomé rozhodnutí, jak jako firma přistupujete k rizikům. A to musí začít u všech lidí ve firmě, u vedení i u zaměstnanců.*“

Kyberbezpečnost pro firmy: Když právo a IT najdou společnou řeč

Spolupráce advokátní kanceláře VIA IURIS a kyberneticko-bezpečnostní společnosti AttentID přinesla na trh unikátní službu pro malé a střední podniky, které chtějí mít vše pod jednou střechou: od zhodnocení výchozího stavu, analýzy rizik přes návrh technických opatření až po právní implementaci, školení a krizovou podporu. Společný projekt nese název Kyberbezpečnost pro firmy. Vznikl jako odpověď na rostoucí bezpečnostní rizika a nové legislativní povinnosti.

„*Z praxe víme, že firmy často investují do bezpečnostních technologií, ale selhávají při jejich právní a procesní implementaci. To je nejen neefektivní, ale může to představovat i právní riziko pro vedení společnosti,*“ upozorňuje advokátka Mgr. Alexandra Mára Paurová z kanceláře VIA IURIS, která se dlouhodobě věnuje ochraně podnikatelů a vedení firem, a to i v digitálním prostředí.

„*Nejde o jednorázové opatření nebo audit. Stavíme most mezi právem, technologiemi a bezpečnostní kulturou firmy. Pomáháme firmám nastavit interní pravidla, odpovědnosti, školení, ale i smlouvy s dodavateli tak, aby obstály v praxi i v případném právním sporu,*“ dodává Štěpán Horák, specialista na kybernetickou bezpečnost a zakladatel AttentID.

Kybernetická bezpečnost už dnes není otázkou výběru – stala se pevnou součástí odpovědného podnikání. Otázkou není, zda do ní investovat, ale jak to udělat správně. ■

Hana Grmelová



Mgr. Alexandra Mára Paurová

Štěpán Horák

Workshop: Kyberbezpečnost pro firmy

Chcete ochránit firmu a splnit legislativní požadavky?

Workshop vám poskytne:

- ucelený přehled právních povinností;
- konkrétní příklady nejčastějších hrozeb a postupů k jejich efektivní eliminaci;
- představení přínosů propojení technických a právních opatření v oblasti kybernetické bezpečnosti.

První termín: listopad 2025, Praha

kyberbezpecnostprofirmy.cz



AttentID
VIAIURIS

Kybernetickou bezpečnost za vás IT nevyřeší

Odpovědnost ponese vedení

V souvislosti s kybernetickou bezpečností často panuje představa, že „o bezpečnost se nám stará IT“. Nový zákon o kybernetické bezpečnosti (účinný od 1. listopadu 2025) tuto iluzi ale definitivně bourá. Zákon totiž jasně stanovuje, že konečnou a neprenositelnou odpovědnost za kyberbezpečnost nenesou administrátoři ani IT technici, ale přímo vedení společností – tedy majitelé, jednatele a top management. A proč? Protože kybernetická bezpečnost není o IT, ale o chodu společnosti.



Kateřina Hůtová, manažerka kybernetické bezpečnosti a spoluzakladatelka Cybrela

Nový zákon o kybernetické bezpečnosti je účinný od 1. listopadu 2025. Do konce roku 2025 musejí společnosti ověřit, jestli pod zákon spadají a ohlásit regulovanou službu.

Cybrela je česká konzultační společnost specializovaná na kyberneticko-informační bezpečnost, která poskytuje své služby v rámci Evropy.

www.cybrela.com

IT zvládne nástroje, vedení musí nést odpovědnost

IT oddělení nebo externí dodavatel vám dokáže zajistit technická opatření, jako jsou firewally, připomenout změnu hesla, monitorovat síť nebo zavést nové systémy. To všechno je potřebné, ale samo o sobě to nestačí. Kybernetická bezpečnost není jen o tom, jestli funguje software či počítač. Znamená schopnost podnikat, prodávat a udržet si zákazníky i v době, kdy čelíte útoku nebo jiné bezpečnostní hrozbě. Je to o jasném rozhodnutí, jak dlouho si můžete dovolit mít systémy mimo provoz – hodiny, nebo dny – a jak velkou ztrátu ještě ustojíte, než začne být ohrožen chod celé firmy. „Rozhodující není, kolik technologií nasadíte, ale zda je kybernetická bezpečnost pevnou součástí vašeho fungování. Jestli je začleněna do firemní strategie, do řízení rizik a do každodenních procesů. Právě proto nový zákon o kybernetické bezpečnosti přesouvá odpovědnost na vrcholové vedení, protože to je jediná úroveň, odkud lze zajistit, aby bezpečnost nebyla jen technickou položkou, ale součástí řízení celé firmy,“ vysvětluje Kateřina Hůtová, manažerka kybernetické bezpečnosti ve společnosti Cybrela.

Nová role managementu

Nová role vrcholového vedení je v tomto ohledu jasně vymezena. Zákon počítá s tím, že vedení nebude pouze podepisovat bezpečnostní dokumenty a schvalovat rozpočet, ale že bude rozumět základním principům kybernetické bezpečnosti. Ne proto, aby se z jednatele stal administrátor, ale aby dokázal činit informovaná rozhodnutí.

Součástí nových pravidel je proto také povinnost, aby se členové vrcholového vedení pravidelně školili v oblasti kybernetické bezpečnosti. Smyslem těchto školení není zvládnout technické detaily, ale porozumět hrozbám a jejich byznysovým dopadům. Jen tak může vedení efektivně alokovat zdroje, reagovat v krizových situacích a zajistit, aby kybernetická bezpečnost byznys podporovala – a nikoli brzdila.

Proč se to týká byznysu

Kybernetické hrozby už dávno nejsou jen o „spadlém serveru“, „nám se to nemůže stát“ nebo „kdo by na nás útočil“. Nebavíme se tu o cílených útocích, ale o tom, co

se stane „mimoděk“, protože jsou v systémech a procesech „díry“. Výrobní podnik může stát dny kvůli útoku na řídicí systémy. E-shop přijde o klíčovou část tržeb, když mu před Vánoci přestane fungovat platební brána. Technologická firma může v jediném okamžiku ztratit svou konkurenční výhodu, pokud unikne její know-how. Takové situace mají přímý dopad na hodnotu společnosti – od výpadku tržeb přes pokuty regulátorů až po reputační ztráty, které se napravují roky. Důležité je také zmínit, že kyberbezpečnostní incident nebo únik dat mohou mít přímý dopad na tržní hodnotu společnosti, zejména v případě jejího budoucího prodeje či akvizice. Odpovědnost vedení proto není formalita, která se přidala do zákona jen tak, ale přímá ochrana hodnoty společnosti. Investoři, partneři i zákazníci dnes sledují, jak je firma připravena na krizové situace, a kybernetická bezpečnost je jedním z prvních testů.

Změna firemní kultury

Pro management to znamená změnu přístupu. Pro někoho větší, pro někoho menší. Kybernetická bezpečnost se ale musí v určité míře stát součástí firemní kultury, podobně jako etický kodex, compliance pravidla, zásady bezpečnosti práce nebo péče o kvalitu.

„Samozřejmě, chvíli si vystačíte s jednorázovým projektem a dokumentací, ale aby to dlouhodobě fungovalo, je potřeba zapojení seshora: pravidelný dohled, průběžný reporting přímo na board, jasné reakční plány a viditelný zájem vedení.“ doplňuje Kateřina Hůtová, manažerka kybernetické bezpečnosti ve společnosti Cybrela.

Zákon jako bezpečnostní standard

Požadavky zákona o kybernetické bezpečnosti, který vychází z evropské směrnice NIS2, mnohé společnosti vnímají jako další byrokratickou zátěž. Ve skutečnosti se jedná o příležitost. Kybernetická bezpečnost nemusí a nemá být brzdou byznysu. Pokud je nastavena pro byznysově a řízena rozumně, podporuje kontinuitu provozu, zvyšuje důvěru investorů a zákazníků a v řadě případů otevírá i nové tržní příležitosti. Zkušenosti ukazují, že firmy, které mají bezpečnostní kulturu pod kontrolou, zvládají krize rychleji, levněji a s menšími ztrátami. A to je výsledek, který už rozhodně není jen „IT záležitostí“. ■

Hana Skoupá

Cybrela

Efektivní proškolení zaměstnanců na kybernetickou bezpečnost

Jak nevyhodit peníze

Ještě v poměrně nedávné minulosti se kybernetický útok bral jako hypotetické riziko. Dnes je to realita, která každý den ohrožuje firmy všech velikostí. Podle Cybersecurity Ventures až 60 % malých podniků ukončí činnost do šesti měsíců po napadení hackery. Ztráta dat, peněz i důvěry zákazníků bývá pro mnohé fatální.

Firewall, zálohy, šifrování, monitoring – to vše dnes patří k základní výbavě většiny firem. A přesto útoky pokračují – kvůli lidem. Když zaměstnanec podlehne podvodnému e-mailu, vyrazí přihlašovací údaje, nebo dokonce sám pošle peníze útočníkům, nepomůže ani nejlepší technologie.

Lidé jsou nejslabší článek

Podle studie Ponemon Institutu z roku 2016 způsobili lidé 48 % všech bezpečnostních incidentů. Je ale těžké dělat statistiky v tak rozbouraných vodách. Řada firem drobnější incidenty vůbec nehlásí. Novější výzkum Mimecast z roku 2025 posouvá čísla ještě výš: až 95 % všech úniků je způsobeno lidským faktorem. Jen osm procent zaměstnanců přitom stojí za osmdesáti procenty chyb!

Jak se dostat k těm osmi procentům? V srpnu letošního roku se terčem podvodníků stalo Muzeum Mladoboleslavska. Zaměstnankyně ekonomického oddělení uvěřila telefonátu údajného policisty a následně i falešnému „bankéři“. Oba ji přesvědčili, že hrozí útok hackerů a peníze instituce je nutné okamžitě převést na „bezpečný účet“. Během několika minut z účtu zmizelo více než jedenáct milionů korun – klasický příklad tzv. vishingu, tedy sociálního inženýrství po telefonu.

Školení ve VR

Paní ekonomka přitom podle médií nedávno prošla kyberbezpečnostním školením. S jistotou můžeme potvrdit, že se nejednalo o kyberbezpečnostní školení ve virtuální realitě (VR), které například reprezentuje řešení Company (Un)Hacked. Studie společnosti PwC ukazuje, že účastníci VR školení se učí čtyřikrát rychleji než při klasických metodách a zároveň si o 275 % lépe pamatují získané informace. Důvod je prostý – virtuální realita zapojuje emoce, soustředění i svalovou paměť. Člověk se stává součástí děje, nikoli jen pasivním posluchačem. A i když samozřejmě neexistuje stoprocentní ochrana před lidskou chybou, platí jednoduchá rovnice: čtyřikrát efektivnější trénink znamená čtyřikrát menší riziko.

Školení Company (Un)Hacked lze implementovat jak do malých firem, tak do korporací. Může probíhat formou workshopu s lektorem, nebo zcela samostatně – bez ohledu na čas či místo. Každý zaměstnanec si jednoduše nasadí headset a aplikace ho provede celým tréninkem od začátku až do konce. HR nebo IT oddělení, které školení spravuje, má přitom k dispozici přehledné výsledky: kdo už začal, kdo ještě ne a jaké má procento úspěšnosti při řešení jednotlivých úloh. Díky tomu se dá přesně měřit, jak se zlepšuje úroveň kybernetické odolnosti celé organizace.

„Bylo to první školení, do kterého mě nikdo nemusel nutit. Postupně jsem, během několika měsíců, prošel všemi scénáři a vždy jsem měl chuť se do něj vracet,“ říká jeden z účastníků tréninku Company (Un)Hacked. Taková reakce není výjimkou. Právě silný zážitek z prostředí virtuální reality způsobuje, že se lidé do tréninku skutečně ponoří a zapamatují si víc než jen seznam zákazů a doporučení. Ve virtuální realitě prostě nemůžete opisovat, vyřizovat e-maily ani si u toho vařit oběd.

Bezpečnostní technologie jsou základ

Přestože je školení řadových zaměstnanců klíčové (zejména těch náchylnějších osmi procent, kteří pravidelně klikají na testovací phishingové e-maily), nesmíme zapomínat ani na pevné technologické základy bezpečnosti. Ty v portfoliu ZEBRA SYSTEMS zajišťuje značka Acronis, která se stará o zálohování a obnovu dat, dále GFI Software, poskytující pokročilou e-mailovou a síťovou ochranu, a N-able, určená pro vzdálenou správu a monitoring firemní infrastruktury. Teprve kombinace správných technologií a efektivně poučených zaměstnanců přináší organizacím maximální možnou ochranu před kyberútoky a minimalizuje pravděpodobnost narušení obchodní kontinuity. ■

Marek Prorok,
specialista školení ve virtuální realitě



Foto: ZEBRA SYSTEMS

Kybernetická rizika rostou

Nepodceňujte je a investujte do bezpečnosti

V posledních měsících a letech se v médiích objevilo hned několik vážných kybernetických incidentů – útoky na nemocnice, napadení českých univerzit nebo výpadky systémů v logistických a výrobních firmách. Tyto události ukazují, že digitální prostředí se stává stále rizikovějším a útoky stále sofistikovanějšími.

O RENOMIA

RENOMIA se řadí mezi významné mezinárodní společnosti v oboru pojištění a risk managementu. V roce 1993 ji založila Jiřina Nepalová se svými syny Jiřím a Pavlem. Cílem společnosti je poskytovat klientům kvalitní péči s detailní znalostí jejich oboru a hájit jejich zájmy na pojišťovacím trhu. RENOMIA je rodinná firma s mezinárodním zázemím, která zajišťuje servis pro své klienty po celém světě. Od roku 2019 je minoritním akcionářem RENOMIA americká společnost Gallagher, světová trojka v oboru pojištění a risk managementu. Globální servis Gallagher mohou využívat i klienti RENOMIA. Více o RENOMIA GROUP najdete na www.renomia.cz.

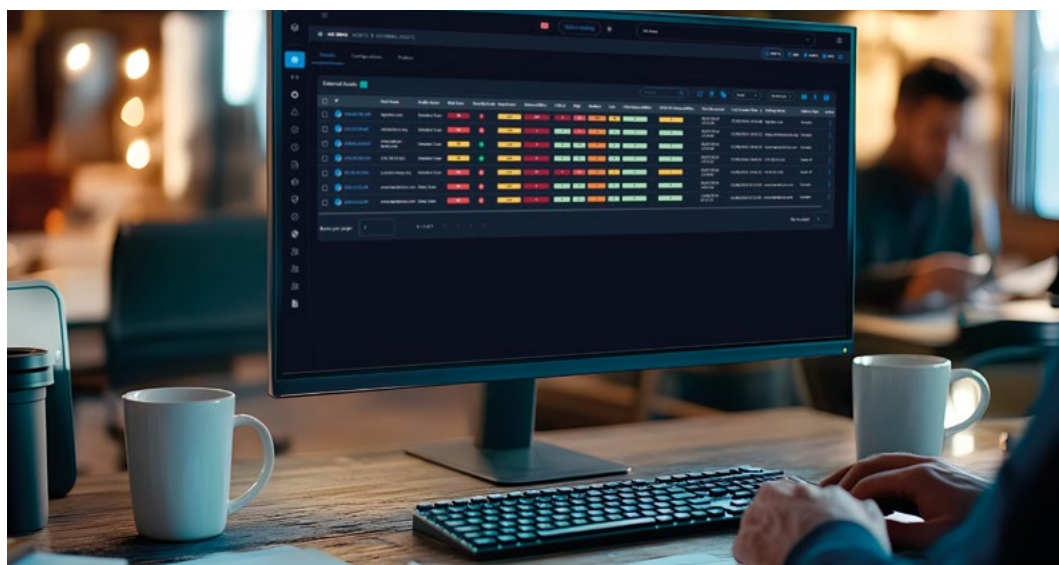


Foto: Věra Křeňáková, RENOMIA

K yberzločinci dnes necílí jen na velké korporace. Naopak, stále častěji napadají malé a střední podniky, které bývají méně chráněné, a přitom zpracovávají hodnotná data. Útoky probíhají prostřednictvím phishingových e-mailů, kompromitovaných přístupů, vyděračského softwaru (ransomware) nebo manipulace s platebními pokyny.

Jak se riziko vyvíjí – statistiky hovoří jasně

Podle Evropské agentury pro kybernetickou bezpečnost (ENISA) došlo v roce 2024 k meziročnímu nárůstu kybernetických incidentů o více než 30 %. Každá druhá firma v EU zaznamenala alespoň jeden útok, a u malých podniků je tento podíl dokonce vyšší než u velkých korporací.

Zároveň se mění i charakter útoků – přibývá tzv. supply chain útoků (útoky na dodavatelské řetězce) a incidentů spojených s cloudovými službami. Mezi další typy útoků, kterých přibývá patří: spear-phishing, Business Email

Compromise nebo útoky využívající umělou inteligenci. Tyto nové formy útoků se často kombinují. Například ransomware bývá výsledkem úspěšného spear-phishingu, který otevřel dveře k interní síti. Nebezpečí spočívá i v tom, že mnoho útoků se odehrává dlouho předtím, než si jich firma všimne – útočníci si v síti „vytvářejí pozice“ a čekají na vhodný okamžik k útoku. Pozitivní zprávou je, že úroveň kybernetické bezpečnosti v českých firmách se postupně zlepšuje. Přispívá k tomu nejen vyšší povědomí o rizicích a větší důraz na řízení kybernetických rizik, ale i nové legislativní požadavky, například směrnice NIS2 a s tím spojený nový zákon o kybernetické bezpečnosti, která nutí podniky zavádět systematictější opatření a pravidelné audity.

Nejde jen o ztrátu dat

Ztráta nebo poškození dat bývá prvním viditelným důsledkem kybernetického incidentu, ale zdaleka ne jediným. Firmy se často potýkají s:



Peter Gardlík,
Head of Cyber Risk Management,
RENOMIA

- výpadkem provozu, který může zastavit výrobu nebo dodávky na několik dní;
- únikem citlivých informací, což může vést k právním postihům a pokutám;
- poškozením reputace, zejména pokud se incident dostane na veřejnost;
- finanční ztrátou, například kvůli podvodným převodům nebo vynucenému výkupnému;
- narušením důvěry partnerů a zákazníků, které se obnovuje měsíce i roky.

Společnosti se často soustředí na jeden konkrétní prvek ochrany – například zálohování nebo spolupráci s externím IT partnerem – ale v dnešním prostředí to už nestačí. Mít zálohy je důležité, ale pokud nejsou oddělené, šifrované a pravidelně testované, mohou být k ničemu. Stejně tak IT partner nemusí zachytit všechny typy hrozeb, pokud chybí pravidelné testování zranitelností či školení zaměstnanců.

V RENOMIA kombinujeme technické know-how s konzultantským poradenstvím, abychom firmám pomohli nejen identifikovat slabá místa, ale také dlouhodobě budovat kulturu bezpečnosti a odolnosti. Naše řešení RENOMIA | Gallagher Cyber Defence Centre se zaměřuje na skenování externích zranitelností, testování odolnosti pomocí simulovaných phishingových kampaní a komplexní penetrační testování. Díky těmto nástrojům mohou organizace reagovat dříve než útočníci, a systematicky tak posilovat svou odolnost.

Pojištění kybernetických rizik jako součást prevence i krizového řešení

Součástí komplexního řízení kybernetických rizik je také pojištění. Firmám totiž může pomoci nejen zvládnout následky útoku, ale i reagovat na něj profesionálně – díky přístupu k IT expertům, právníkům i krizové komunikaci. Získat správnou nabídku pojištění kyberbezpečnosti nemusí být vždy jednoduché, ale pro firmy to zpravidla není nic neřešitelného. Konzultanti RENOMIA na základě znalosti rizikového profilu konkrétní firmy a znalosti trhu dovedou najít a sjednat nejvhodnější pojistné řešení. To znamená takové, které dobře pokryje všechna významná rizika a ostatní potřeby související s kyberbezpečností. Škody se mohou vyšplhat do milionů korun – a to nejen přímé, ale i reputační a právní. Proto se kybernetická

rizika stávají tématem, které se dotýká všech podniků bez ohledu na velikost.

Pojištění reaguje na široké spektrum hrozeb a potenciálních škod, které kybernetický útok může firmě způsobit. V první řadě jde o náklady na obnovu poškozených či ztracených dat. Dále lze z pojistného plnění hradit právní a PR služby při odškodňování zákazníků a ochraně dobrého jména. Pojištění kryje i pokuty spojené s únikem osobních údajů, výpadky provozu a ušlý zisk.

Velkou roli hraje také ochrana proti tzv. cybercrime – například situaci, kdy útočníci přímo odčerpají peníze z firemního účtu nebo zmanipulují účetní systém. Některé typy pojištění navíc pokrývají i incidenty způsobené lidskou chybou – třeba omylem zaslané citlivé informace nebo špatně nastavené přístupové oprávnění.

Pro menší podniky může být zajímavou výhodou i asistenční služba, která pomáhá reagovat okamžitě po incidentu – například zajištěním IT forenzního vyšetření, krizové komunikace nebo obnovením provozu.

Není výjimkou, že pojišťovna vyhodnotí organizaci jako příliš rizikovou a napoprve relevantní nabídku nepředloží. To ale neznamená konec. Firmy se mohou připravit a zvýšit svou pojistitelnost – například díky službě RENOMIA | Gallagher Cyber Assist, kterou na českém trhu nabízí RENOMIA.

Tato služba zahrnuje konzultace, simulace útoků i doporučení na posílení ochrany. Výsledkem je nejen větší šance získat pojištění, ale hlavně skutečné zvýšení odolnosti proti incidentům. Firmy tak získávají nejen pojistnou ochranu, ale i přidanou hodnotu v podobě lepšího povědomí o svém zabezpečení.

Investice, která se vyplatí

Pojištění kybernetických rizik se stává užitečným a čím dál potřebnějším nástrojem firemní bezpečnosti. Nejenže minimalizuje riziko finanční ztráty a pomáhá zvládnout krizi, ale zároveň motivuje organizace systematicky řídit svá rizika. V prostředí, kde kybernetické útoky rostou co do četnosti i sofistikovanosti, jde o investici, která se vyplatí. Firmy, které myslí na svou kybernetickou bezpečnost preventivně, získávají nejen klidnější spánek, ale i důvěru svých zákazníků a obchodních partnerů. ■

Peter Gardlík, Head of Cyber Risk Management, RENOMIA

JAK NA KYBERBEZPEČNOST

RENOMIA ve spolupráci s partnerskou společností Gallagher nabízí klientům kombinaci tří služeb, které komplexně minimalizují rizika a pomáhají řešit následky hrozeb spojených s kyberbezpečností. RENOMIA | Gallagher Cyber Defence Centre se zaměřuje na skenování externích zranitelností, testování odolnosti pomocí simulovaných phishingových kampaní a komplexní penetrační testování. Tím pomáhá firmám s prevencí kybernetických rizik. Služba RENOMIA | Gallagher Cyber Assist, kterou na českém trhu nabízí RENOMIA, pomáhá v komplikovanějších případech firmám s nastavením kybernetické bezpečnosti na úrovni, kterou požadují pojišťovny. A konečně služba RENOMIA Cyber Facility se zaměřuje přímo na rychlé a jednoduché sjednání výhodného pojištění kybernetických rizik.

Nemocnice Plzeňského kraje míří k vyšším standardům bezpečnosti

Jedním z nejskloňovanějších slov současnosti je „bezpečnost“. Řeší se v souvislosti s mezinárodními vztahy, klimatickými změnami, řeší se kyberbezpečnost, bezpečnost v dopravě i bezpečí obyčejných lidí v běžném životě. A stále víc se mluví o bezpečnosti také ve zdravotnictví. Nejen ve smyslu bezpečné péče, ale prakticky ve všech procesech.

Na cestu vyšších standardů bezpečnosti se vydaly i nemocnice Plzeňského kraje (NPK). Předpokládají postupné investice v řádech stovek milionů korun.

„Pravidelně se umísťujeme v popředí žebříčků spokojenosti a bezpečnosti pacientů. Koneckonců to se od nás čeká, že budeme léčit podle zavedených a bezpečných postupů. Bezpečnost se ale týká nejen léčby a nejen pacientů, ale také návštěvníků, zaměstnanců, budov, movitého majetku, dodávek energií a v neposlední řadě dat,“ popisuje předseda představenstev nemocnic Skupiny NPK Zdeněk Švanda s tím, že zejména rizika fyzického ohrožení a ohrožení dat se stále zvyšují.

Roste agresivita i počet kyberútoků

Přibývá agresivních pacientů i samotná míra agresivity, přibývá počítačových hackerů, kteří útočí na data i celé systémy, a ve společnosti přibývají i lidé, kteří si v důsledku frustrace, psychických potíží nebo z jiných důvodů vybírají veřejný prostor za cíl svého útoku.

Takovým prostorem mohou být i nemocnice. „A protože rizika rostou, začali jsme loni připravovat ucelený projekt zvyšování bezpečnosti nad rámec současné legislativy. Letos ho začínáme postupně naplňovat,“ upřesnil Švanda. Plány souvisí i s dalšími stavebními investicemi a jsou rozloženy minimálně do roku 2029.

Nestačí jen pořídit víc kamer, ochranu, lepší zámky do dveří nebo vyšší úroveň softwarové ochrany počítačů.

Je třeba systémy více automatizovat, využít AI, nastavit procesy, jak s bezpečnostními prvky pracovat nebo jak reagovat v případech rizik. A je třeba s těmito postupy seznámit personál. Nejdůležitějším článkem bezpečnosti totiž zůstanou sami lidé.

Ochrana začíná lokací

Jedním z prvních projektů zvyšování bezpečnosti osob i majetku bylo v prvním pololetí zavedení elektronického docházkového systému. Do jisté míry nepopulární

záležitost, protože se obecně považuje pouze za sledování dodržování pracovní doby zaměstnanců. Takzvané čipování má ale zásadní přínos i pro bezpečnost. Dokonce ve dvou rovinách.

„Ochrana zaměstnanců začíná tím, že víme, kde se nachází. Zda jsou vůbec v areálu nemocnice. Kdyby došlo k nějaké krizové situaci v některé z nemocnic, například k požáru, víme, kdo je uvnitř. A to platí i mezi nemocnicemi, když jede někdo pracovní do jiné,“ popisuje Zdeněk Švanda.

Druhá rovina užití čipů v bezpečnosti je spojená s tím, kam se jaký zaměstnanec dostane. Neboli rozšíří funkci klíčů. „Částečně už to funguje, ale budeme navyšovat počty dveří, které budou na čip a za které se dostanou jen oprávnění zaměstnanci. Ostatní buď vůbec, nebo jen jako doprovod. A opět se vrátíme k první rovině zabezpečení. Když nastane jakákoliv neočekávaná situace, víme, kdo a kolik lidí je v dané zóně v ohrožení,“ doplňuje šéf krajských nemocnic s tím, že podobné systémy se zavádí stále více a v různých odvětvích. Tím se nejen zdokonalují, ale také zlevňují.

Kamerový systém? Ano, ale s AI

To samé platí i pro zavádění třeba kamerových systémů. Objevují se stále častěji na ulicích, v průmyslu, obchodech i ve zdravotnických zařízeních. Už řadu let jsou instalované také v nemocnicích Plzeňského kraje. Jejich počty ale budou narůstat, a hlavně se bude rozšiřovat jejich funkční využití, a to nejen při detekování nebezpečného chování.

„Kamera je jen čidlo, které zaznamenává obraz v pohybu. Abychom z něho ale dostali nějakou informaci, musíme mít člověka, který neustále sleduje monitor a dokáže včas zaznamenat jakoukoli rizikovou situaci. Už to samo o sobě je náročné, a zvlášť pokud bude kamera přibývat. Chceme proto kromě kamer získat i ucelené softwarové řešení, které dokáže s využitím umělé inteligence vyhodnotit v reálném čase data z velkého



Nemocnice
Plzeňského
kraje

množství kamer nebo z i dalších čidel třeba elektronické požární ochrany a zachytit jakoukoli neobvyklou rizikovou situaci,“ vysvětluje vedoucí kyberbezpečnosti Skupiny NPK Tomáš Šenk.

Současná řešení dokáží velmi rychle rozeznat třeba nůž nebo jinou zbraň, podivné chování a pohyb, přičemž mozaiku chování si skládají ze všech kamer a záběrů, kde se konkrétní osoba objevuje. A pokud vyhodnotí chování jako rizikové, ihned na to upozorní pracovníka ostrahy. Následně dokáže systém stopovat rizikovou osobu pomocí detekce obličeje nebo i barvy oblečení. Podle barvy oblečení dokáže i vyhledat osobu.

„To se bavíme o bezpečnosti ve veřejných prostorech nemocnice, pokud by tam byl nějaký agresivní pacient, útočník, anebo kdyby se jen ztratilo dítě. Software pro nemocnice ale dokáže upozornit třeba i na to, kdyby nějaký pacient upadl na pokoji, třeba v noci cestou na toaletu a zůstal ležet. Hlídá tedy právě i bezpečnost pacientů během léčby,“ doplňuje Šenk.

Se školením zaměstnanců pomáhají odborníci

Nestačí ale jen čipy, kamery, čidla požáru a software. Neméně důležité je, aby zaměstnanci věděli, jak v rizikových situacích reagovat. *„S každým rozšířením bezpečnostních prvků budeme rozšiřovat i soubor organizačních zásad. Jedna věc je riziko detekovat a druhá věc je umět reagovat a nebezpečí eliminovat. V tomto směru jsme navázali spolupráci s několika odborníky,*“ uvedl Zdeněk Švanda.

Jedním z nich je i šéf bezpečnosti Fakultní nemocnice Ostrava Daniel Naivert, který patří v současnosti v oblasti bezpečnosti nemocnic k nejpovolanějším osobám v zemi. Fakultní nemocnice Ostrava totiž čelila v prosinci 2019 útoku šíleného střelce a od té doby patří v ČR k lídrům v zavádění bezpečnostních prvků a technologií včetně edukace zaměstnanců.

Právě prvotního proškolení zaměstnanců, jak reagovat na agresivní návštěvníky nebo přímo útočníka se zbraní, se Daniel Naivert ujal v nemocnicích Plzeňského kraje. *„Školení se konala od jara do podzimu postupně a opakovaně ve všech našich nemocnicích. Chtěli jsme, aby ho absolvovalo pokud možno co nejvíce zaměstnanců bez ohledu na to, v jaké pozici a kde pracují. Samozřejmě vyšší riziko je u pracovníků v přímém a častém kontaktu s veřejností, například v ambulantní části nemocnic. Ale k vyšší bezpečnosti může napomoci jakýkoli proškolený zaměstnanec,*“ řekl vedoucí provozně-technického oddělení krajských nemocnic Tomáš Petrmičl.

V jeho kompetenci je právě i revize provozně bezpečnostních postupů zahrnující, kdo bude veškerá bezpečnostní čidla sledovat, a hlavně co dělat, když dojde k jakémukoli narušení bezpečnosti. *„Důležitým prvkem je vytvoření centrálního pracoviště ochrany – jakéhosi bezpečnostního pultu pro všechny nemocnice, kam se budou sbíhat všechny informace ohledně narušení bezpečnosti, nestandardních stavů a jevů, informace o technických poruchách, o narušení dodávek energií a podobně. A samozřejmě zaměstnanci tohoto pracoviště budou mít jasný popis, co v jaké situaci dělat,*“ doplňuje vedoucí technik.



Zdeněk Švanda,
předseda představenstev nemocnic
Skupiny NPK

Data chrání nová záložní serverovna

Neméně důležitá je v nemocnicích také kyberbezpečnost a ochrana dat. I v tomto směru podniká Skupina NPK významné kroky. Jedním z nich je vybudování nového datového centra, které bylo zprovozněno v Klatovech v říjnu. Jeho kapacita přesahuje tisíc terabajtů. *„Dosud jsme v našich nemocnicích měli jedno datové centrum a menší kapacity v jednotlivých nemocnicích. Nově máme dvě moderní datová centra, která jsou na sobě nezávislá, jsou samozřejmě fyzicky oddělená, každé je jinde, ale přitom fungují jako záložní, to znamená každé z center shromažďuje a poskytuje v reálném čase veškerá data z nemocnic,*“ popisuje Tomáš Šenk s tím, že kdyby jedno datové centrum bylo z jakéhokoli důvodu nefunkční, nemocnice budou mít veškerá data stále k dispozici na záložních serverech.

Teoreticky se může stát, že jedno centrum zasáhne například požár, dlouhodobý lokální výpadek elektřiny, může dojít k fyzické závadě nebo mohou data i přes další softwarová zabezpečení napadnout hackeři. Záložní centrum tato rizika eliminuje a data jsou vždy dostupná. *„Dostupnost dat v režimu 24/7 je pro nemocnice klíčová, abychom nemuseli jakkoli omezovat péči a ochránili tím pacienty, i proto, že každý výpadek dat způsobuje ekonomické škody,*“ dodává manažer kyberbezpečnosti. ■

Jiří Kokoška

COTakhle snídani na téma...

Bezpečnost není samozřejmost

Bezpečnost jsme si po dlouhá desetiletí zvykli brát jako samozřejmost. Poslední roky nás ale upozorňují, že samozřejmostí není. A také že pojem bezpečnost toho zahrnuje mnohem víc než jen ochranu majetku nebo fyzickou bezpečnost lidí. Je to kombinace fyzických opatření, kybernetické odolnosti, organizačních procesů, legislativy a připravenosti.



Letošní snídane navazuje na loňskou, kdy jsme se zaměřili na to, co se v české realitě změnilo rok po bezprecedentním incidentu na Filozofické fakultě UK.

Tematické panely

- Bezpečnostní situace ve světě
- Nové trendy v metodikách ochrany měkkých cílů MV ČR (a doplňující pohled ze Slovenska)
- Personální bezpečnost (v návaznosti na NIS2, DORA, Zákon o kritické infrastruktuře)
- Pohled z praxe firem

Informace pro zájemce

Máte-li zájem o účast na snídani, kontaktujte Ivu Bendžalovou – iva.bendzalova@cot.cz.

Bezpečnost ovlivňuje životy jednotlivců, chod firem i stabilitu celé společnosti. Chceme-li hrozbám čelit efektivně, musíme bezpečnost vnímat jako komplexní a propojený systém, který se neustále vyvíjí – s novými hrozbami i novými technologiemi.

Proto na tento speciál navazuje v listopadu expertní diskuzní snídane, kterou komunikační agentura COT group ve spolupráci s ASIS International a Hospodářskou komorou ČR pořádá 18. listopadu od 9 hodin v sídle HK ČR v paláci Florentinum.

Ve čtyřech panelech se vystřídá hned dvanáct expertů, kteří budou společně diskutovat témata bezpečnosti z pohledu globálních rizik, metodiky ochrany měkkých cílů, kybernetické bezpečnosti i běžné firemní praxe. Svět kolem nás se rychle mění a bezpečnostní prostředí není výjimkou. Konflikty, hybridní hrozby, kybernetické útoky a geopolitická nejistota mají přímý dopad na Českou republiku. Jak ČR vnímá tyto hrozby, jak reaguje a jaké kroky by měly být prioritou v následujících letech?

Měkké cíle, tedy místa, kde se pohybují lidé a probíhají každodenní činnosti – školy, kulturní a administrativní prostory, firmy – jsou stále častěji cílem sofistikovaných útoků. Tento panel se bude věnovat novým trendům v jejich ochraně, využití moderních technologií, integraci kybernetické a fyzické bezpečnosti a posilování odolnosti lidí a procesů.



Foto: Petr Manuel Uřích

Firmy dnes čelí nejen ekonomickým výzvám, ale i bezpečnostním rizikům, která mohou ohrozit zaměstnance, majetek i chod celé organizace. Hybridní hrozby, kybernetické útoky a nečekané krizové situace vyžadují strategický přístup k bezpečnosti. V tomto panelu se zaměříme na moderní metodiky ochrany, prevenci incidentů a roli firemní kultury a leadershipu při ochraně lidí.

A konečně je tu realita. Kde a jak narážejí expertní rady na běžnou podnikovou praxi? O tom všem budeme diskutovat. V příštím vydání měsíčníku Komora pak přineseme výběr toho nejdůležitějšího a nejinspirativnějšího. ■

Petr Karban



Pomáháme firmám předvídat, minimalizovat
a řešit rizika v digitálním světě



RENOMIA | GALLAGHER CYBER DEFENCE CENTRE

Minimalizace kybernetických rizik skenováním externích zranitelností, testováním odolnosti pomocí simulovaných phishingových kampaní nebo komplexním penetračním testováním.



RENOMIA | GALLAGHER CYBER ASSIST

Zanalýzujeme vaše rizika a pomůžeme zvýšit vaši kybernetickou bezpečnost na úroveň, kterou požadují pojišťovny.



RENOMIA | CYBER FACILITY

Sjednáme pro vás rychle a jednoduše výhodné pojištění kybernetických rizik.