HOSPODÁŘSKÉ NOVINY

SPECIÁLNÍ PŘÍLOHA

KYBERNETICKÁ BEZPEČNOST

Dejte nám peníze
Když je firma napadena a útočníci chtějí vyjednávat o výkupném, jde nejen o data, ale i o čas. Expert radí, jak jednat s hackery.

Technologický dluh
Jak nastavit bezpečnost firemních dat dlouhodobě tak, aby společnost nebyl schopen hacknout třeba dvanáctiletý kluk z Indie?

Kyberútoky

Zašifrovali jsme vám firemní data, dejte nám peníze. Expert na kyberbezpečnost vysvětluje, jak vyjednávat s hackery

Adam Mašek
adam.masek@economia.cz

Vyjednávat s kyberútočníky, nebo ne? *V případě kyberútoků na firmy je rozhodující rozsah škod a co vše je ještě podnik schopen zachránit, říká Václav Svátek, majitel a generální ředitel společnosti ČMIS.* **Foto: HN – Libor Fojtík**

Sportisimo, Rohlik.cz či Košík.cz jsou jen některé z firem, které se v posledních měsících musely potýkat s následky kybernetických útoků hackerů. Ve všech případech šlo o určitý druh ransomwaru, což je typ škodlivého softwaru, který uzamkne nebo zašifruje firemní data. Útočníci pak pro jejich odblokování požadují výkupné, typicky vyplácené v kryptoměnách. Často může jít o vysoké desítky až stovky milionů korun, záleží na velikosti napadené společnosti.

V tu chvíli management firem řeší zásadní dilema: platit, či neplatit? A dá se o ceně vyjednávat? „Otřepaná fráze zní, že s teroristy se nevyjednává. V případě kyberútoků na firmy to ale neplatí zcela. Rozhodující je, jaký je rozsah škod a co vše je ještě podnik schopen zachránit," říká Václav Svátek, majitel a generální ředitel společnosti ČMIS. Ta se kromě cloudových služeb specializuje i na něco, co sám Svátek popisuje jako Ransomware „pohotovost".

Co si pod pojmem Ransomware pohotovost představit?
Já už jsem dávno rezignoval na to vysvětlovat firmám, že by měly mít alespoň nějaká základní pravidla pro kybernetickou bezpečnost. Že by bylo dobré, že až k útoku dojde, aby alespoň trochu věděly, co mají dělat, a měly v rukách nějaké karty. Tato osvěta se moc s účinkem nesetkala, takže jsem si řekl, že bude možná lepší nabízet službu jakési pohotovosti pro tyto nemocné zanedbané firmy, které se stanou cílem útoku. Je to jako s lidmi, kteří o sebe dlouhodobě nepečují, pijí hodně alkoholu, kouří a nezdravě jedí. V jednu chvíli potřebují, aby se o ně někdo postaral. A to podobné děláme my, akorát s firmami a v oblasti kybernetické bezpečnosti.

To tedy v praxi znamená co?
Volají nám firmy, které jsou už napadené a nevědí si moc rady. A nutno říct, že to neví většina podniků, pokud pominu ty největší korporáty ze sektorů kritické infrastruktury, jako jsou největší banky nebo energetické společnosti. Když napadená firma zavolá, je nutné situaci ihned řešit, co nejrychleji diagnostikovat příčinu, co nejvíce eliminovat škody a zabránit dalším únikům dat. Vždy je klíčový čas. Většina IT oddělení přitom nemá příliš tušení co dělat. A pokud to alespoň trochu vědí, může jim kompletní diagnostika trvat kvůli nedostatku pracovních kapacit i tři dny. Když my na případ nasadíme 10–15 specialistů, zvládneme to klidně v řádech hodin.

Co se děje poté, kdy se situace po útoku trochu stabilizuje? Jaký je typicky další postup?
Postup je většinou takový, že útočníci napadené firmě pošlou například e-mailem informace, jak se s nimi má spojit. Komunikace probíhá třeba přes chatovací aplikaci Signal anebo na jiných platformách, jež používají trošku pokročilejší šifrování. Zde musím jen vzpomenout na jednu poměrně bizarní situaci, kdy se jedna napadená firma nedokázala kvůli technickým potížím s hackery spojit a ti tak do společnosti sami zavolali a ptali se, kde je problém a proč se jim nikdo neozývá. Útočníci samozřejmě chtějí, aby s nimi podnik komunikoval, protože jedním z primárních cílů je dostat z firmy nějaké peníze.

Tím se dostáváme k zásadní otázce: má firma výkupné za odblokování dat platit, nebo ne?
Zde je naprosto zásadní, jak velký je rozsah škod. Pokud má firma zálohy a dokáže většinu dat a systémů obnovit v jiném prostředí – a případné nenávratné ztráty jsou pro ni akceptovatelné –, pak se doporučuje neplatit nic. Jsou tu ovšem případy, kdy napadená firma nemá v ruce absolutně žádné karty. Pak se situace kompletně mění.

Jak?
Vysvětlím na poměrně nedávném případu jedné velké firmy s miliardovými obraty. Byl jsem zrovna na dovolené v Japonsku, obdivoval jsem tamní chrámy a najednou mi zvoní telefon. Na druhé straně IT oddělení této firmy s tím, že jejich systémy jsou pod rozsáhlým kyberútokem. Firma přišla o veškerá produkční data a útočníci jí ukradli i kódy ke klíčovému informačnímu systému, který řídil přijímání objednávek, nákup i distribuci. Takový software se ve firmě vyvíjí klidně 10, 15 let. Vzhledem k tomu, že firma neměla prakticky žádné zálohy, byl její manévrovací prostor prakticky nulový. V takovém případě jsme jí doporučili vyjednávat a případně zaplatit, protože bez odblokování těchto klíčových kódů to může firmu klidně položit.

Dá se o ceně nějak vyjednávat?
V první řadě je potřeba si uvědomit své možnosti. Na druhé straně proti mě stojí profesionálové, kteří rozhodně nepodcenili rešerši, a pokud jde o velkou firmu, moc dobře díky veřejně dohledatelným zdrojům vědí, jak je na tom po finanční stránce. Čili pokud má podnik miliardové obraty, s jedním milionem korun se útočníci nespokojí. Obecně doporučuji nechat si dát první nabídku a tu se postupně snažit snižovat.

Jsou hackeři ochotni dát „slevu"?
Jsou. Většinou to funguje tak, že jako první nastřelí tu vyšší částku, aby pak případně mohli jít s cenou níž, pokud je první nabídka pro napadenou firmu neakceptovatelná. Proto je ale velice důležité, aby podnik neukazoval své karty – vůbec nesděloval, jak moc vážné jsou škody, co vše má zálohované nebo v jaké fázi je obnovování systémů. Důležité je také nespěchat a mezi každou odpovědí nechat klidně den, dva. Když odpovídám každých pět minut, je jasné, že mě tlačí čas. Čili nějakou dobu počkat a pak zkusit nahodit třeba čtvrtinu původní ceny. Je to trošku jako na tureckém tržišti.

~ Volají nám firmy, které jsou už napadené a nevědí si moc rady. A nutno říct, že to neví většina podniků.

Kde je nejslabší článek v zabezpečení firem?
Z našich dlouhodobých analýz vyplývá, že jednoznačně největší zranitelnost ve firmách je samotný IT administrátor. Když to přeženu, ten kdyby se zbláznil, tak tu firmu dokáže systematickou prací – aniž by si toho někdo všimnul – výrazně poškodit až klidně položit. Jsou to lidi, kteří mají důvěru, takřka neomezený přístup a také možnosti, jak obejít bezpečnostní systémy. Když se rozhodnou dělat neplechu, tak než si toho tamní security týmy všimnou, může to trvat i hodiny. Proto je nutné se těmto pracovníkům věnovat – zcela bez přehánění – i po psychologické stránce a zjišťovat, jak se cítí, jaký je jejich rodinný život a zdali třeba nemají problém s alkoholem či drogami.

Narazili jste někdy na případ, že se firemní IT administrátor, jak vy říkáte, „zbláznil" a způsobil záměrně nějakou škodu?
Jednou jsme se setkali s případem, kdy měl šéf IT oddělení jedné firmy pocit, že jej chce generální ředitel vyhodit. Proto si zřídil zadní vrátka do firemního systému a nainstaloval tam aplikaci pro vzdálený přístup zvaný AnyDesk, aby tam v případě potřeby zřejmě mohl nějak škodit, případně stáhnout nějaká citlivá data. Stalo se ale to, že útočníci tato zadní vrátka využili a zašifrovali celou firmu. Onen generální ředitel tomu nejdříve vůbec nechtěl věřit.

Poněkud tragikomické také bylo, že zmíněný šéf IT oddělení svou vinu popíral a tvrdil, že on to nebyl. Přitom byl jediným člověkem ve firmě, který podobná oprávnění a přístupy měl, takže důkazy hovořily jednoznačně proti němu a nakonec jej usvědčily.

Příloha: Kybernetická bezpečnost
• **Ředitel speciálních projektů** Aleš Mohout • **Editor** Ján Chovanec • **Grafika a zlom** Vizuální studio Economia • **Obchod a inzerce** Jakub Růžička (jakub.ruzicka@economia.cz)

Partneři přílohy: ANECT pwc AuditMaster.ai

▸ **Základy kyberbezpečnosti**

Radek Kubeš
radek.kubes@economia.cz

Co byste dnes měli vědět o kybernetické bezpečnosti

Není to tak dlouho, co bezpečnostní rizika představovala především technický problém, řešený oddělením IT. Dnes jde ovšem o strategickou záležitost nejvyššího vedení firem. I proto si možná kladete otázku: kde začít a jak poznat, zda jsme dostatečně chráněni?

Kybernetické hrozby jsou už několik let na vzestupu – ransomwarové útoky dokážou během pár hodin paralyzovat celé korporace, úniky osobních údajů znamenají nejen ztrátu důvěry a dobré pověsti, ale také milionové sankce a sofistikované APT (Advanced Persistent Threat) kampaně mohou i celé roky bez povšimnutí odčerpávat citlivé obchodní informace. Obrana proti těmto i mnoha dalším rizikům není snadná. Kybernetická bezpečnost představuje komplexní disciplínu vyžadující koordinaci technických opatření, procesů a lidských zdrojů.

Do hry navíc vstupuje stále přísnější legislativa, jako je aktuálně schvalovaný zákon o kybernetické bezpečnosti (vycházející z evropské regulace NIS2), která vyžaduje zavádění konkrétních opatření. Současně je ale důležité vědět, že mnoho velmi účinných bezpečnostních opatření nemusí být ani nákladné, ani složité zavést. Přesto jsou v mnoha firmách opomíjena. Jak tedy začít a na co se primárně zaměřit?

Strategické řízení kyberbezpečnosti

Zásadní chybou je delegování kybernetické bezpečnosti výhradně na oddělení IT. Bezpečnost informací představuje zásadní riziko pro celý podnik, a proto vyžaduje strategické řízení na úrovni nejvyššího vedení. Vytvoření efektivní bezpečnostní architektury začíná definicí jasné strategie, založené na obchodních cílech a rizikovém profilu společnosti.

Tato strategie musí odpovědět na základní otázky: jaká informační aktiva jsou pro podnik kritická, jaká úroveň rizika je akceptovatelná, jak budou rozděleny odpovědnosti za bezpečnost v rámci firmy a jaké regulatorní požadavky musí podnik splňovat. Na základě těchto informací lze definovat bezpečnostní politiku a související směrnice stanovující jasná pravidla a postupy pro zajištění kybernetické bezpečnosti a reakce na incidenty.

Prioritou je ochrana dat

Data a informace představují nejcennější aktivum firem. Paradoxně ale firmám často chybí přesný přehled o tom, kde se jejich kriticky významná data nacházejí a jak jsou chráněna. Proto první krok k jejich efektivní ochraně spočívá v mapování informačních aktiv a jejich klasifikaci podle důležitosti a citlivosti.

Speciální ochranu vyžadují především databáze zákazníků, smlouvy, finanční data, data z výzkumu i další citlivé informace. Základním opatřením je šifrování a zálohování těchto dat, stejně jako kontrola přístupu k nim. Nejlépe na základě principu nejnižších nutných oprávnění, který vyžaduje, aby měli zaměstnanci přístup pouze k informacím nezbytným pro výkon jejich práce. Řeší se to implementací systémů na řízení identit a přístupu, které automatizují přidělování a odebírání oprávnění na základě rolí v organizaci. V praxi ale zaměstnanci často získávají při přechodech mezi pozicemi stále další oprávnění a účty externích pracovníků nejsou zrušeny ani dlouho po ukončení projektů.

~ Do hry vstupuje přísnější legislativa, která vyžaduje zavádění konkrétních opatření.

Nezbytnou součástí ochrany dat a zajištění kontinuity provozu jsou rovněž plány jejich zálohování a obnovy. Bez pravidelného testování skutečné možnosti obnovy dat ze záloh ale často v krizových situacích dochází k technickým problémům a zjištěním, že jsou zálohy rovněž infikované škodlivým softwarem, zašifrované ransomwarem nebo zkrátka jen nepřístupné nebo neúplné.

Ani cloud není automaticky bezpečný

Nezbytná technická bezpečnostní opatření nemusí nutně znamenat nákup nových zařízení – často stačí jen efektivněji využívat ta stávající. Navíc zahrnují i opatření, jako jsou pravidelné aktualizace operačních systémů a aplikací. Ty představují nejjednodušší a nejúčinnější způsob, jak omezit bezpečnostní rizika. Známé zranitelnosti softwaru totiž slouží útočníkům jako vstupní brána do podnikových sítí, přestože pro většinu z nich jsou již k dispozici příslušné opravy. Účinnost dalších bezpečnostních technologií, jako jsou firewally a antivirové programy, pak závisí na správné konfiguraci a rovněž na pravidelných aktualizacích.

Technická a procesní opatření musí řešit také firmy využívající ke své činnosti především cloudové služby. Navzdory obecné (mylné) představě totiž data uložená v rámci cloudových služeb zpravidla nejsou automaticky chráněna před ztrátou nebo odcizením. Podle principu sdílené odpovědnosti zabezpečuje poskytovatel cloudu infrastrukturu služby, zatímco zákazník odpovídá za konfiguraci, přístupová práva a ochranu svých dat. Mnoho bezpečnostních incidentů ale vzniká právě nesprávnou konfigurací cloudových služeb, a nikoli technickými zranitelnostmi platformy.

Kritická role lidského faktoru

Účinnost sebedokonalejších technických a procesních opatření vždy závisí na lidech, kteří je používají nebo se jimi mají řídit. Současně ale zaměstnanci představují nejslabší článek a první linii obrany organizace proti kybernetickým hrozbám, zejména pokud jde o phishing a další útoky využívající techniky sociálního inženýrství.

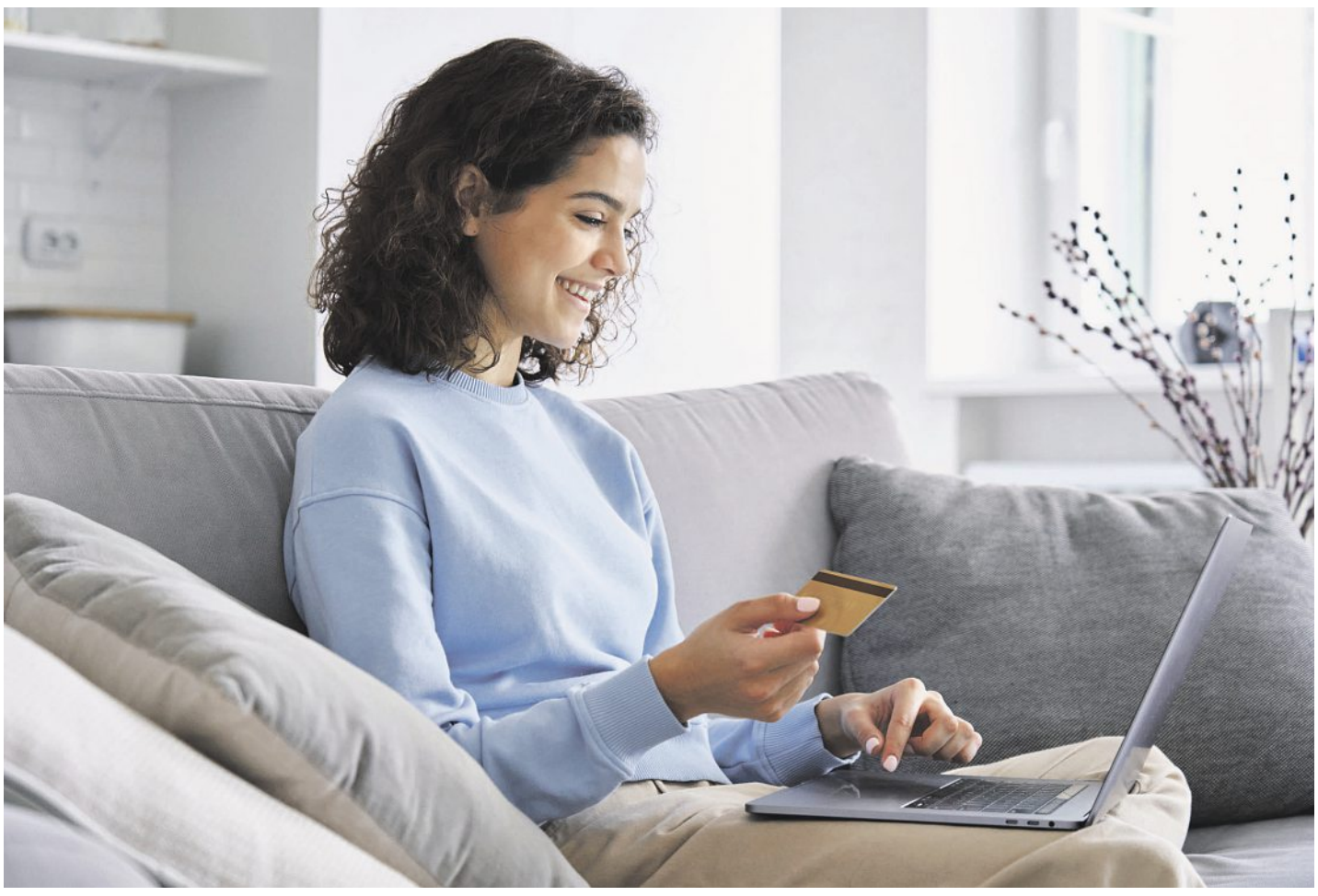
Ukazuje se přitom, že právě investice do vzdělávání a zvyšování povědomí o kybernetické bezpečnosti přinášejí měřitelné výsledky v podobě významného snížení množství bezpečnostních incidentů. Zapojení zaměstnanců zvyšují především konkrétní příklady kybernetických útoků, stejně jako simulované phishingové kampaně nebo gamifikované vzdělávací programy. Zcela klíčová je přitom pravidelnost vzdělávacích aktivit, aktualizace jejich obsahu podle současných hrozeb a povinnost jejich absolvování skutečně všemi zaměstnanci, u kterých existuje riziko kyberútoku – tedy včetně nejvyššího managementu. Důležité je rovněž vytvoření prostředí „kultury bezpečnosti“, kde zaměstnanci cítí podporu při nahlašování bezpečnostních incidentů bez obav z postihů.

Specifickou kategorii rizik představují interní hrozby, které vyžadují vyvážený přístup mezi důvěrou a kontrolou. Nespokojení zaměstnanci nebo neúmyslné chyby mohou vést k úniku citlivých informací nebo narušení provozu firmy. Proto se stále častěji zavádějí systémy pro monitoring uživatelského chování, které pomáhají identifikovat a případně i zastavit nestandardní aktivity, které mohou indikovat bezpečnostní incident.

Rychlá reakce znamená méně škod

Žádná obrana nemůže být z principu věci stoprocentní – už proto, že útočníci neustále objevují nové techniky průniku do sítě, odcizení cenných dat, finančních podvodů nebo narušení provozu. Je tedy spíše otázkou, kdy k nějakému incidentu dojde. O rozsahu škod a rychlosti návratu k běžnému provozu rozhoduje rychlost reakce na takový incident. Proto musí plán reakce definovat jasné role a odpovědnosti, komunikační kanály i postupy pro zastavení hrozeb a následnou obnovu. Bez předem připraveného (a natrénovaného) plánu reagují podniky často chaoticky a neefektivně.

I z tohoto velmi stručného přehledu základních technik a postupů je asi dobře vidět, jak komplexní disciplínu kybernetická bezpečnost představuje. Především pro menší firmy proto může být zajištění všech potřebných znalostí a technického vybavení velmi náročné – a přitom může být celé jejich podnikání závislé právě na datech a jejich ochraně před ztrátou či odcizením. Jistě i proto si v poslední době získává na popularitě „kyberbezpečnost formou služby“ – tedy outsourcing zajištění kybernetického zabezpečení včetně detekce a reakce na incidenty na poskytovatele služeb centra bezpečnostních operací (Security Operations Center, SOC). Kyberbezpečnost formou služby může být zajímavou alternativou nejen pro menší a středně velké firmy.



Ochrana dat na prvním místě. *Při online platbě je klíčová ochrana citlivých údajů, jako jsou osobní data zákazníků, finanční informace či smlouvy. Základ tvoří šifrování, zálohování a přísná kontrola přístupu.* **Foto: Shutterstock**

▸ Bezpečnost dat

I cloud má své limity. Kritická infrastruktura musí být připravena

Marcela Štefcová
marcela.stefcova@economia.cz

Cloud a cloud computing jsou dnes pro firmy i státní instituce standardem. V případě výpadku ale může být i standardní řešení problém. O to větší, čím důležitější data v něm běží. Pro provozovatele kritické infrastruktury i veřejné správy je klíčová nejen dostupnost a bezpečnost, ale i funkčnost záložního scénáře.

Cloudová řešení mají za sebou raketový vzestup. Díky nižším nákladům, škálovatelnosti i možnosti rychlého vývoje nových aplikací se stala běžnou součástí provozu od start-upů po státní instituce. Cloud přináší bezesporu obrovské výhody. Ale čím strategičtější služba, tím větší důraz musí být kladen na její dostupnost a bezpečnost a musí být eliminovány nevýhody cloudu.

„To, na čem opravdu záleží, třeba šifrovací klíče ke cloudovému úložišti, si uložím bezpečně u sebe on-premise *(software, který se instaluje a provozuje přímo na počítačích dané firmy nebo uživatele, celý software má tak firma „u sebe“ – pozn. red.)*, rozhodně je neukládám v tom samém cloudu," popisuje příklad Michaela Stonová, bezpečnostní ředitelka OKsystemu.

Hybridní model jako cesta

Zejména firmy spadající do kategorie kritické infrastruktury dnes kombinují cloudová řešení a on-premise, kde systémy běží na vlastních zařízeních uživatele. „On-premise provozujeme klíčové komponenty systému. V cloudu jsou převážně méně podstatné či podpůrné aplikace," uvádí David Olszyński, bezpečnostní architekt Air Bank. Podobnou strategii volí společnosti jako ČEZ, Státní zemědělský intervenční fond (SZIF) nebo Raiffeisenbank, která cloudové služby využívá tam, kde to dává smysl z hlediska efektivity, škálovatelnosti a dostupnosti. Výběr ověřených poskytovatelů je vždy podmíněn bezpečnostními a právními požadavky.

Důvod je jasný. Sázka na cloud neznamená rezignaci na kontrolu. Zákazníci by se měli aktivně ptát: Kde jsou moje data? Jak jsou zálohována? Mám přístup k celému obsahu i v případě výpadku? A co když poskytovatel zkrachuje nebo dramaticky změní podmínky? Ani v těchto případech nemůže být ohrožen chod firmy, natož strategických služeb. Pro ně by měl být vždy připraven plán B. Ať už v podobě redundance, offline režimu nebo záložního provozu na lokálním serveru.

Státní cloud: jen prověření poskytovatelé

Od roku 2024 smí veřejná správa využívat pro strategické systémy jen eGovernment cloud. Za jeho budování a provoz je zodpovědná Státní pokladna Centrum sdílených služeb (SPCSS) a ta je plně pod kontrolou státu. Systémy zde běží v nejvyšším bezpečnostním režimu, v úrovni 4, což znamená velký důraz na zajištění integrity a důvěrnosti dat státu, kontrolu přístupů a vysokou dostupnost. Poskytované služby jsou zapsány v Katalogu cloud computingu spravovaném Digitální a informační agenturou. Jsou zde také uvedení další přísně prověření poskytovatelé. „Státní cloud má ochránit kritická data a informace z nich vyplývající, protože data mají v našem světě největší hodnotu," zdůrazňuje Roman Vrba, generální ředitel SPCSS.

Rizika? Nejen technická

Cloud ale neznamená pouze technické nebo bezpečnostní výzvy. V dnešním globalizovaném světě ovládá podle Romana Vrby bezmála 98 procent světového trhu pět hráčů z USA a Číny, AWS, Microsoft, Google, Alibaba a Oracle, kteří investují do cloudu a umělé inteligence ročně násobky státních rozpočtů evropských zemí. Evropa bohužel zaspala. Outsourcují se služby, tím i kompetence. Ztrácí se tak know-how, schopnost inovovat i udržovat vlastní systémy. Naštěstí tomuto trendu nepodléhají všichni. „Jsme si vědomi, že kvalitní IT vzdělávání mladých lidí je pro budoucnost klíčové. I proto jsme založili OKlab, centrum inovací pro studenty již od středních škol. Důležité pro nás nejsou zkušenosti, ale hledáme tvořivost, nadšení a snahu něco dokázat. Naším cílem je pomoci vytvářet špičkové odborníky, kteří budou formovat naši digitální budoucnost," shrnuje Michaela Stonová.

▸ Sdílení dat

Stát nesmí být jen konzumentem cloudových služeb. Buduje si vlastní kompetenci

Marcela Štefcová
marcela.stefcova@economia.cz

Kyberbezpečnost je otázkou národní bezpečnosti. Kritické informační systémy musí být dostupné, chráněné a odolné vůči výpadkům i útokům. „Stát nesmí zůstat závislý jen na globálních technologických gigantech. Nejkritičtější informační systémy musí být plně pod kontrolou v privátním cloudu tohoto státu," upozorňuje Roman Vrba, generální ředitel státního podniku Státní pokladna Centrum sdílených služeb, s. p. (SPCSS), který je pověřen zajištěním státní části eGovernment Cloudu.

Co přesně je úkolem SPCSS a jaké služby poskytuje?

Naším hlavním úkolem je výstavba a provoz státní části eGovernment Cloudu, tedy infrastruktury určené pro provoz nejkritičtějších informačních systémů státu. Ty musí běžet v nejvyšším bezpečnostním režimu, v úrovni 4. To znamená nejen velký důraz na zajištění integrity a důvěrnosti dat státu, kontrolu přístupů a vysokou dostupnost, ale i to, že poskytovatelem je subjekt plně kontrolovaný státem. Služby, které poskytujeme, jsou vypsány v Katalogu cloud computingu. Jeho agendu má na starosti Digitální informační agentura.

Které systémy už u vás běží?

SPCSS byla jmenována poskytovatelem služeb cloud computingu pro státní správu na konci roku 2024. Ale připravovat jsme se začali mnohem dříve. Výsledkem je, že už více než rok funguje v našem prostředí systém ARES ministerstva financí. Jde o hybridní model. Veřejná, méně citlivá data jsou v public cloudu, ta citlivá jsou ve státním. Dále zajišťujeme infrastrukturu pro informační systém státní pokladny (IISSP), zmínil bych i část daňového systému ADIS, Celní portál. Také k nám míří například nový systém s pracovním názvem eVolby. Ten bude zajišťovat technické zpracování kandidátních listin a další agendu spojenou s volbami, ale nikoli elektronické hlasování. V budoucnu by mělo být ve státním cloudu provozováno zhruba 20 nejdůležitějších systémů. Ty ostatní, kterých je na jedenáct tisíc, budou pravděpodobně provozovány hybridně nebo v komerčním public cloudu.

Jak se díváte na rostoucí závislost na amerických nebo čínských technologiích?

Bohužel Evropa zaspala. USA a Čína investují do cloudu a umělé inteligence ročně násobky státních rozpočtů evropských zemí. Superglobalizace v této oblasti už proběhla. Dnes ovládá bezmála 98 procent světového trhu pět hráčů. Na jejich dohnání bychom potřebovali minimálně deset let. A my si musíme přiznat, že nemáme ani finanční, ani lidské zdroje. Bez úzké spolupráce s velkými dodavateli to tedy nepůjde. Zároveň ale musíme počítat s geopolitickými riziky, proto musíme mít vlastní infrastrukturu a kompetence. Nejen kvůli bezpečnosti, ale také abychom nebyli jen pasivními uživateli, kteří netuší, jak technologie fungují.

Jak je zajištěna dostupnost státního cloudu v případě krizí?

Máme nastavené scénáře, zálohy a pravidelně trénujeme různé typy incidentů včetně fyzického výpadku, kyberútoku nebo selhání hardwaru. Naše služby běží v režimu 24/7 s dostupností SLA 99,99 procenta. Každý zásah má přesně definované kompetence, aby nebylo nutné v krizové chvíli „čekat na povolení".

Jaké máte plány do budoucna?

Kromě migrací dalších systémů se chystáme rozšiřovat naše datová centra, včetně specializovaných zařízení pro využití umělé inteligence. Také budeme budovat rovnováhu mezi různými typy bezpečnosti – kybernetickou, fyzickou, informační i personální. Cílem je mít ve státním cloudu všechny systémy udržované a běžící v bezpečném a flexibilním prostředí. A zároveň mít tým lidí, kteří ho umí provozovat, rozvíjet a řešit mimořádné události bez paniky. To je ta největší přidaná hodnota – stabilita, kontinuita a kompetence.

▸ Zabezpečení

Zuzana Keményová
zuzana.kemenyova@economia.cz

Firmy často fungují na technologický dluh. Hackne je dvanáctiletý kluk z Indie

Nemůžete čekat, že budete chráněni před kyberútoky, když používáte Windows XP, říká Petr Špiřík, partner v poradenské společnosti PwC a odborník na kybernetickou bezpečnost. Základem obrany je mít ve firmě aktuální software i hardware. V Česku také sílí trend, že si firmy kybernetické zabezpečení kupují od specialistů na klíč jako službu. Žádný expert ale podle Špiříka nezaručí, že pod jeho správou je firma stoprocentně v bezpečí. „Pokud to tvrdí, tak lže," říká Špiřík.

Jaké typy kyberútoků jsou dnes nejčastější?
Nejčastěji firmy řeší útoky ransomwaru, trvá to už posledních pět let, možná i více. Je to výnosný byznys a má už několik různých variant.

Ransomware zašifruje data a útočníci chtějí po firmě za navrácení dat výkupné. Platit, nebo neplatit?
Zašifrování dat a výkupné byl první model útoků, od té doby už ransomware prošel generačními obměnami. Další verzí je, že útočníci ukradnou data, pak je zašifrují, chtějí výkupné a hrozí, že pokud je nedostanou, tak data zveřejní. Variací je také, že prodají přístup do vaší firmy dalším útočníkům. Obecně je však důležité neplatit, protože tím povzbuzujeme byznys model útočníků. Navíc nemáme jistotu, že útočníci i po zaplacení data stejně někomu neprodají. V některých zemích může být jednatel, který rozhodl o zaplacení výkupného útočníkům, dokonce stíhán pro napomáhání organizovanému zločinu.

Jaká jiná východiska kromě placení jsou?
Nejčastěji se stává, že je poškozena jen část organizace nebo firmy, třeba jen třicet nebo šedesát procent. Je proto možné nepoškozenou část firmy izolovat, zabezpečit a postupně získat zpět napadenou část dat, například obnovováním ze záloh.

Jsou české firmy připravené na nový zákon o kyberbezpečnosti NIS2, nebo je změna zastihne nepřipravené?
I větší a technologicky vyspělejší firmy, které už dnes podléhají regulaci, zůstávají často zranitelné. Nejvíce ohrožené jsou však středně velké, až větší firmy – jsou atraktivním cílem, protože mají peníze, fungují digitálně a mají co ztratit. Zároveň si ale často ještě nevybudovaly vlastní bezpečnostní tým. Až dosud převažoval postoj: „Na komplexní kyberzabezpečení nemáme rozpočet, tak raději neuděláme nic, nebo jen to nejnutnější." Spoléhaly na to, že útok je třeba mine. Nyní tyto firmy vyčkávají, jak přesně bude nový zákon vypadat, aby se nepouštěly do kroků navíc. O prodlení tedy nejde – spíš o strategické vyčkávání.

Určuje nový zákon o kyberbezpečnosti, že se bude vztahovat na firmy podle počtu zaměstnanců?
Ano, kromě kritéria ročního obratu nad deset milionů eur a vybraných odvětví je tam také kritérium počtu zaměstnanců nad padesát. Ale nemyslím si, že by NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) hned začal obcházet a pokutovat malé firmy. To určitě není cílem. Alespoň ne v prvních dvou letech platnosti zákona.

Jaké tedy mají být první kroky firmy, která dosud nedělala pro kyberbezpečnost nic a nyní chce začít?
Spousta těchto firem funguje na takzvaný technologický dluh. Používají třeba Windows XP nebo 2003, pracují s 25 let starou technikou a poslední člověk, který věděl, jak funguje, odešel před deseti lety do důchodu. V této situaci má smysl začít s úklidem a dostat ten podnik technologicky do roku 2025. Když bude mít moderní operační systém, moderní aplikace a bude používat běžná zabezpečení jako dvoufaktorovou autentizaci, spousta věcí se tím sama vyřeší. Je to mnohem lepší než žít na systému, který už výrobce dvanáct let nepodporuje a umí jej hacknout dvanáctiletý kluk z Indie.

Musí si na to firmy někoho najímat, nebo to zvládnou většinou svépomocí?
Jako střední beru podnik od dvou set do dvou tisíc zaměstnanců. Většinou jejich IT nebo security oddělení buď vůbec neexistuje, nebo je poddimenzované. Ti ajťáci většinou dělají, co mohou, ale nelze očekávat, že v jednom nebo dvou lidech zvládnete všechno, od tiskárny po detekci hackerského útoku. Taková firma může zainvestovat a posílit své IT a security oddělení, a dramaticky tak zvýšit své náklady na zaměstnance a technologie.

Druhá možnost je, že jednorázově zaplatí externí firmě, třeba systémovému integrátorovi nebo konzultační společnosti, a pojme to spíše projektově. Řekne: My se chceme letos posunout o významný krok tímto směrem, udělejte to. A až našetříme další peníze, provedeme další krok. Třetí možnost – a to je trend posledních pár let – je security outsourcing, tedy forma poskytování bezpečnosti jako služby. Dodavatel kyberbezpečnosti provozuje security za danou firmu a ona se tak může soustředit na svůj hlavní byznys. Tato varianta je v Česku stále oblíbenější, je to trend, který přišel z Velké Británie a USA.

Nabízejí tyto externí firmy záruky, že pod jejich správou k úspěšnému útoku určitě nedojde?
Možná to bude ostré tvrzení, ale pokud nějaká firma říká, že pod jejich správou vás nikdo nehackne, tak lže. Není možné tohle zaručit. Kyberbezpečnostní firma může pouze garantovat, že udělá maximum podle posledního vývoje v oboru. Může také zaručit – a my to rovněž zaručujeme –, že pokud vás někdo hackne, do dvou hodin s vámi ten útok začnou řešit. Budete mít k dispozici tým, který se specializuje na řešení bezpečnostních incidentů a souboj s hackery. V dnešní době přitom už díky technologickému pokroku máme k dispozici technologie, které umožňují efektivní obranu. To nebylo dřív samozřejmostí. Míra zabezpečení je tak dnes více než technologickými možnostmi limitována rozhodnutím vedení. Jednu dobu také bylo mezi firmami a pojišťovnami populární nabízet pojištění proti kyberútokům, ale mnoho pojišťoven od toho ustupuje, protože útoků je opravdu hodně a finančně na tom krvácely.

Které zabezpečovací principy by každá firma měla mít, aby byla alespoň základním způsobem chráněná?
Znovu zdůrazním, že software, hardware a služby musí být současné a aktuální, nikoli zastaralé. Ze security oblastí je to dále zálohování dat, které je proti ransomwarovým útokům efektivní obranou. Nemělo by se samozřejmě zálohovat na systémy, které jsou připojené ke stejné síti, již zálohují. Je to logické, protože cílem útočníků je ty zálohovací servery najít a napadnout zálohy. Když se jim to podaří, ještě posilují svou pozici při požadování výkupného. Pokud má firma kvalitní zálohy, které dejme tomu jednou měsíčně odveze do odděleného data centra nebo do trezoru, je v daleko lepší pozici, protože jí hrozí maximálně ztráta dat za poslední měsíc, a nemusí se tedy tak moc s útočníky bavit. Dále je to vícefaktorová autentizace. Všichni ji známe z mobilního bankovnictví. Přístup do důležitého systému pouze pomocí jména a hesla je špatně, v dnešní době už by tohle vůbec nemělo být. Nějaké potvrzení, ať už minimálně pomocí SMS nebo přes aplikaci, je velmi žádoucí. Bezpečnost přihlášení to zvyšuje několikanásobně.

Dá se na kyberútok nějak připravit?
Ano, dá a velmi to pak zjednodušuje situaci. Firma by například měla vědět, kdo je v případě útoku zodpovědný danou situaci řešit. A nemusí to být nutně security pracovník – ten často neexistuje, ale třeba člen boardu nebo IT manažer. Musí být jasné, kdo bude v minutách a hodinách po útoku koordinovat průchod tou situací a co k tomu potřebuje. Často to s klienty simulujeme. Na čtyři hodiny si sedneme na jedno místo a představíme si, že právě ve firmě přestaly fungovat všechny počítače. Útok se zhoršuje, hackeři říkají, že půjdou do médií, že v nich zveřejní špinavá tajemství o vaší firmě. Vzácná situace je, že firma řekne, že na obranu mají určený postup a že ho před půl rokem testovali. Většinou jde spíše o brainstorming, kdy se vedení rozhoduje, co kdo bude dělat. Ale už tento nácvik velmi pomůže utřídit si myšlenky, a když skutečně k útoku dojde, už trochu vědí, jak postupovat.

Zažil jsem třeba situaci, kdy CFO firmy řekl: Tak bychom to obnovili ze záloh, ne? Šéf IT ale upozornil, že před dvěma lety dané systémy zálohovat přestali, protože se krátil rozpočet. Výsledkem simulace bylo, že o půl roku později ta firma zálohování obnovila. CFO pochopil, že kdyby opravdu přišel útok ransomwarem, tak z jeho rozhodnutí by firma nebyla schopna se bránit.

Kyberexpert. *Partner v PwC, vede Cybersecurity & Privacy v ČR a Managed Cybersecurity Services pro EMEA region. Zaměřuje se na oblasti bezpečnostních center a reakcí na incidenty. Věří v technologický pokrok a vzdělávání mladých lidí, že je možné nad útočníky zvítězit.* **Foto: HN – Václav Vašků**

Text vznikl ve spolupráci se společností **PwC**.

▸ Zabezpečení firem

Nejděsivější je vidět bezmocnost nepřipravených firem během kybernetického útoku

Ivana Gračková
ivana.grackova@economia.cz

Kybernetické útoky dnes ohrožují nejen státní instituce a banky, ale prakticky každou firmu, která pracuje s daty. O tom, jak se firmy mohou bránit, jak funguje Security Operation centrum a co se děje v zákulisí boje s kybernetickými hrozbami, jsme hovořili s Michalem Trtilem, Head of Security and Network Operations Center ve společnosti ANECT. Firma patří už více než tři desetiletí k významným českým dodavatelům IT služeb, specializuje se na kybernetickou bezpečnost, enterprise architekturu a řízené služby. Do portfolia ANECT patří i vlastní inovační hub, z něhož vzešly nástroje jako Clashing nebo XtendISE.

Co si má běžný čtenář představit pod zkratkou SOC?
SOC, tedy Security Operations Center, je zjednodušeně místo, kam se soustředí obrana před útočníky. Jeho úkolem je předcházet kybernetickým hrozbám, detekovat bezpečnostní události a incidenty a následně na ně reagovat. Pracujeme se spoustou dat, která k nám proudí z různých systémů, a snažíme se v nich včas odhalit anomálie, které mohou znamenat bezpečnostní problém. V ideálním případě dříve, než způsobí nějakou škodu.

Máte zkušenost, že firmy o SOC často nemají úplně reálnou představu?
Ano, to se děje velmi často. Existuje představa, že jakmile firma zřídí nebo si objedná SOC, má tím kybernetickou bezpečnost vyřešenou. Jenže SOC je jen jedna část mnohem širšího rámce. Je to preventivní, detekční a reaktivní vrstva, která pomáhá zvládat události a incidenty, ale nezastoupí další důležité prvky, například správné nastavení bezpečnostní architektury, vzdělávání zaměstnanců nebo pravidelné testování odolnosti.

Komu se tedy SOC opravdu vyplatí a kdo jej naopak nepotřebuje?
Jednoduše řečeno SOC je pro každého, kdo má co ztratit. Každá organizace by si měla položit otázku, jaká má aktiva, která chce chránit, a jaká jsou s nimi spojená rizika. Má know-how? Pracuje s osobními daty? Poskytuje kritické služby? Pokud ano, SOC může být smysluplnou investicí.

Velké firmy, typicky banky, mají interní SOC. Společnosti střední velikosti dost často spoléhají na externí SOC zejména z ekonomických důvodů. Malé firmy využívají základní úrovně našich služeb nebo se na nás obrací formou konzultací. Nejmenší zákazník, se kterým v SOC pracujeme, má do 100 zaměstnanců.

Pokud se firma rozhodne SOC využívat, kdy je pro ni výhodnější budovat si ho sama a kdy je lepší objednat si ho jako službu?
Zásadní roli hrají finance, ale i čas a dostupnost kvalifikovaných lidí. Pokud chce firma provozovat vlastní SOC v režimu 24/7, potřebuje minimálně sedm lidí. Musí počítat se směnami, zákonnými přestávkami, zaškolením, fluktuací a hlavně s časem, než se vše podaří vybudovat. Proto doporučujeme většině organizací využít outsourcing. Je důležité ho ale nastavit tak, aby firma nezůstala závislá na jediném dodavateli. Podmínky musí být nastaveny transparentně a tak, aby byl dodavatel v případě potřeby nahraditelný.

Bezpečnostní incident. *Častou motivací pro pořízení SOC je to, že firma sama čelila kybernetickému útoku, říká Michal Trtil ze společnosti ANECT.* **Foto: Tomáš Škoda**

Co všechno dělá typický analytik v SOC?
Pracuje s různými technologiemi pro monitorování a analýzu bezpečnostních událostí. Na základě detekcí z těchto technologií reaguje na jednotlivé události. Analytik vyhodnocuje logy z různých zařízení, dívá se na jejich kontext, případně nálezy eskaluje na vyšší úroveň. Pokud jde o incident, aktivuje se proces incident response. Dále máme specialisty na nastavování pravidel v jednotlivých technologiích, specialisty na vyhledávání hrozeb, na správu zranitelností, vzdělávání a další oblasti. Je to pestré.

A jak vypadá běžný den v SOC?
Jelikož služba SOC běží 24/7, každé ráno začíná předáním směny. Následně analytik sleduje události a vyhodnocuje, jestli se jedná o běžný provoz, nebo potenciální hrozbu. Pokud má podezření, analyzuje data do hloubky. Připojuje se do dalších systémů, hledá souvislosti. Někdy se nic neděje, jindy řeší události celý den. Sbíráme data z koncových stanic, serverů, firewallů, síťových prvků, cloudových prostředí a podobně. Navíc SOC řeší nejen bezpečnostní monitoring, ale poskytuje i další služby. Každý den je proto jiný.

Jak často dochází ke skutečnému zásahu?
To záleží na velikosti a typu zákazníka. Někde máme desítky alertů denně, jinde stovky. Bezpečnostní incidenty jsou méně časté, typicky jednotky za rok.

Vzpomenete si na konkrétní případ, kdy SOC zásadně pomohl?
Ano, zažili jsme například situaci, kdy jsme zachytili phishingovou kampaň. Šlo o maily s přílohou, která obsahovala škodlivý kód. Jeden uživatel soubor stáhl. Rychle jsme reagovali, analyzovali jsme kód, izolovali stanici, zablokovali adresy, nasadili opatření. Důležité je, že jsme útok zachytili včas a zabránili dalšímu šíření.

Existují chyby v zabezpečení firem, které se stále opakují? Které jsou nejčastější?
Bohužel jsou to pořád ty stejné. Neměněná hesla opakující se pro různé systémy, sdílené účty, chybějící aktualizace, otevřené porty. Často se něco nastaví dočasně a zapomene se to vrátit zpátky. Firmy neprovádějí aktualizace systémů, ačkoliv výrobce vydal opravy. Nebo když dojde k incidentu, vyřeší se jen akutní problém, ale už neproběhne poučení. Fáze „lessons learned“ chybí.

Která situace vás osobně zatím nejvíce zaskočila, nebo dokonce vyděsila?
Kupodivu nešlo o skutečný problém. Bylo to tabletop cvičení u jednoho velkého zákazníka. Simulovali jsme incident, u stolu seděl celý top management. A bylo naprosto zřejmé, že ti lidé vůbec nevědí, co mají dělat. Neměli nastavené žádné postupy, žádné role. Ta bezmocnost byla děsivá. Pokud přijde reálný útok, a firma není připravená, může to mít vážné následky.

Jak se mění způsoby, jakými útočníci operují?
Dnes existují služby typu ransomware-as-a-service, takže útočníci ani nemusí umět programovat. Koupí si nástroj a útočí. Zvyšuje se využívání AI k přípravě phishingu, ale i ke generování kódu. Ovšem klasické metody jako DDoS nebo zneužití zranitelností jsou stále účinné. Útočníci hledají nejslabší místo.

Jak se tomu dá bránit?
Je potřeba mít strategii, investovat do bezpečnosti kontinuálně. Nečekat, až se něco stane. Správně nastavit architekturu, školit zaměstnance, testovat. A ideálně mít SOC, který to celé monitoruje a dokáže reagovat. SOC není jen technologie, je to komplexní služba, která může firmě zachránit reputaci i finance.

Co firmy ke zřízení SOC nejčastěji motivuje?
Často motivací je, když firma zažila bezpečnostní incident. Méně časté jsou firmy, které chápou rizika dřív, než se naplní. Někdy přichází impulz od IT manažera, který má zkušenosti z předchozího působení. Dalším typem motivace jsou legislativní regulace a různé oborové standardy.

Jak důležité je pro SOC znát byznys zákazníka? Mění se přístup k detekci a reakci podle toho, jestli jde o nemocnici, výrobní podnik, nebo finanční instituci?
Jakákoliv technologie či služba je tu primárně od toho, aby pomáhala dosahovat byznysové cíle. SOC nevyjímaje. V první řadě musíme znát kritická aktiva zákazníků, která se na jejich byznysu podílí.

Následně určujeme a vyhodnocujeme relevantní hrozby a na základě toho nastavujeme detekce. Reakce se do určité míry mění na základě interních procesů dané společnosti nebo instituce.

Jak se v SOC pracuje s umělou inteligencí nebo strojovým učením? Jsou to buzzwordy, nebo skutečně pomáhají?
S trochou nadsázky by se dalo říct, že: „Co nemá umělou inteligenci, to se dnes neprodává.“ Každopádně AI v rámci technologií, které se v SOC využívají, dokáže pomoci při zpracování velkého počtu dat, zvyšuje efektivitu reakcí na bezpečnostní události a podobně. Neznamená to však, že by zcela dokázala nahradit bezpečnostní analytiky. Zároveň je třeba si uvědomit, k čemu ji využíváme a jaká data jí poskytujeme. Obecně je totiž téma zneužití nebo zveřejnění citlivých informací v kontextu chatbotů a AI hodně aktuální.

V jakých situacích vám dává smysl spolupracovat i s jinými SOC nebo bezpečnostními týmy napříč firmami?
Bezpečnostních technologií a výrobců je v současnosti tolik, že tvrzení, že znáte perfektně úplně vše, je nesmyslné. Takže spolupráce s dalšími společnostmi je namístě. Důležité je, aby byla jasně definovaná a hlavně přínosná pro zákazníka. Zároveň je velmi důležité sdílení informací o hrozbách, útocích apod. v rámci komunity SOC/CSIRT týmů, jako je například organizace TF-CSIRT, jejíž jsme součástí.

Bude podle vás SOC za deset let zásadně jiný? A co by mělo zůstat stejné?
Předpokládám, že za deset let bude SOC mnohem více automatizovaný, od reaktivního přístupu se přesune k předcházení útokům: Bude mnohem méně závislý na lidských zdrojích, avšak zodpovědnost a poslední slovo by vždy mělo zůstat na nás, lidech.

Pokud byste měl jednou větou poradit firmám, jak přistoupit ke kybernetické bezpečnosti, co byste řekl?
Poznejte své prostředí, aktiva a byznysové potřeby, zorientujte se, v jakém vnějším prostředí se pohybujete, a na základě toho postupujte v oblasti kybernetické bezpečnosti.

Text vznikl ve spolupráci se společností **ANECT**.

Gordic

HN064840

Jak na řízení bezpečnosti podle NIS2 a nZoKB? Jednoduše

Evropská směrnice NIS2 a související nový zákon o kybernetické bezpečnosti (nZoKB) znamenají pro firmy řadu nových výzev. V České republice se dotknou řádově tisíců organizací. NIS2 však přináší nejen nové bezpečnostní požadavky, ale vyžaduje zcela nový přístup – klade důraz na proaktivní a komplexní řízení kybernetické bezpečnosti v rámci členských států Evropské unie. Co konkrétně to pro firmy znamená, nám řekl Vojtěch Hvězda, specialista na kybernetickou bezpečnost ve společnosti Gordic.

Nová legislativa se dotkne vyšších tisíců českých organizací, přičemž změna se netýká jen IT firem nebo kritické infrastruktury jako doposud. Nově budou muset svou kybernetickou bezpečnost řídit například i nemocnice, vodohospodářské a energetické podniky, poskytovatelé digitální infrastruktury, správci odpadů nebo dopravci, a střední a velké podniky s více než 50 zaměstnanci či obratem nad 10 milionů eur. Legislativa nově požaduje, aby tyto organizace nejen zabezpečily své informační systémy, ale aby svá rozhodnutí v oblasti bezpečnosti zakládaly na systematické analýze rizik.

Co taková analýza rizik obnáší a proč je klíčová?
Analýza rizik je efektivním nástrojem pro účelovou implementaci technických a organizačních bezpečnostních opatření. Bez možnosti navázat investice do bezpečnostních opatření na reálné výstupy z analýzy rizik střílí vedení společností slepými náboji.

Analýza rizik spočívá v identifikaci aktiv, zhodnocení hrozeb a zranitelností a určení rizik. Teprve po takové analýze lze navrhnout a zavést přiměřená bezpečnostní opatření proti zjištěným reálným rizikům. Problém je, že většina firem s něčím takovým nemá zkušenost a neexistuje jednotná metodika, jak uvedené procesy v té které organizaci realizovat. Proto jsme s ohledem na nZoKB, nVoKB, ISO27001, nařízení DORA a další vyvinuli aplikaci Gordic CSA (Cyber Security Audit), která proces analýzy rizik výrazně zjednodušuje a vede uživatele krok za krokem v souladu jak s osvědčenými postupy v oblasti řízení rizik, tak aktuální legislativou.

Jak konkrétně CSA pomáhá s naplněním legislativních požadavků?
CSA je softwarová aplikace dostupná formou služby, která pokrývá celý proces řízení kybernetické bezpečnosti a analýzy rizik v organizaci. Výrazně zjednodušuje nejen zpracování zmíněné analýzy rizik, ale i průběžné plnění dalších povinností vyplývajících z nZoKB, a to vše v jednotném, uživatelsky přívětivém prostředí. Mezi hlavní funkcionality aplikace CSA patří:

- **Evidence aktiv**, v jejímž rámci identifikuje a přehledně eviduje klíčové regulované služby a s nimi související potřebné informace, a technická a organizační podpůrná aktiva nutná pro poskytování regulované služby.
- **Identifikace rizik a jejich hodnocení**, v rámci které poskytuje seznam aktuálních hrozeb a zranitelností, které lze přiřazovat k daným aktivům. To pomáhá manažerům kybernetické bezpečnosti ve zjednodušení celého procesu hodnocení rizik, jenž je z velké části automatizovaný.
- **Návrh bezpečnostních opatření**, která aplikace poskytuje na základě zjištěných rizik, a to nejen adekvátní technická, ale i organizační opatření.
- **Prohlášení o aplikovatelnosti, tzv. self-audit**, v rámci kterého aplikace zaznamenává veškerou činnost, jež může ovlivňovat bezpečnost organizace. Organizace tak má kdykoliv k dispozici přehledný výstup, který lze použít při kontrole ze strany regulačních orgánů nebo jako podklad pro interní reporting.
- **Aktualizace v reálném čase**, která zajišťuje, že aplikace CSA neposkytuje jednorázovou analýzu rizik, ale komplexní proces řízení aktiv a hodnocení rizik pro průběžnou a kontinuální práci. Mimo jiné nahrazuje i tradiční a zastaralou manuální práci s tabulkovými a textovými editory typu excelovské tabulky.

Aplikace CSA je dostupná jako služba. Jaké výhody to má pro podniky a uživatele?
Používání softwarových produktů formou služby zaručuje jejich jednoduché nasazení, minimální požadavky na infrastrukturu a jasně předvídatelné náklady. Organizace nemusí investovat do licencí, serverů ani školení zaměstnanců a samotní uživatelé dostanou intuitivní rozhraní pro komplexní náhled na kybernetickou bezpečnost firmy včetně metodické podpory našich expertů.

Nová legislativa klade důraz i na detekci a řízení incidentů. Jak s tímto firmám pomáháte?
Pro detekci a řízení bezpečnostních incidentů máme nástroj v podobě otevřené platformy pro centrální správu bezpečnostních událostí. Ten umožňuje jednoduše spojit stávající bezpečnostní řešení, jako SIEM, XDR a SOAR, do jednoho funkčního celku a s využitím AI technologie nabídnout efektivní a spolehlivé vyhodnocení a korelaci bezpečnostních událostí napříč celou podnikovou infrastrukturou v jednom přehledném rozhraní.

Aplikace Cyber Security Audit pro analýzu rizik a řízení kybernetické bezpečnosti od českého tvůrce a dodavatele informačních systémů Gordic.

Vojtěch Hvězda, specialista na kybernetickou bezpečnost ve společnosti Gordic

Zdroj: Gordic

Legislativa pamatuje i na vzdělávání zaměstnanců. Jak k němu přistupujete?
Lidský faktor je z pohledu zajištění bezpečnosti firmy dnes tím nejrizikovějším. A právě proto legislativa klade důraz na povinnost školit nejen zaměstnance, ale i obchodní partnery nebo dodavatele. To přirozeně vytváří tlak na efektivitu celého vzdělávacího procesu. V rámci našeho portfolia proto nabízíme službu GDPO pro komplexní vzdělávání nejen v oblasti kybernetické bezpečnosti. Aplikace GDPO je jednoduchý nástroj pro online školení, testování a certifikaci, který pokrývá vše potřebné v jednom intuitivním prostředí.

Co byste doporučil organizacím, které teprve stojí před výzvami nové legislativy v oblasti kyberbezpečnosti?
Jak říká zakladatel společnosti Gordic Jaromír Řezáč, kybernetická bezpečnost je nejen legislativní povinnost, ale existenční nutnost. Začněte tedy včas a nebojte se požádat o pomoc. Nepodceňujte analýzu rizik, ta je základem pro úspěšné zajištění kybernetické bezpečnosti vaší organizace. Pokud hledáte nákladově efektivní řešení, které vás spolehlivě provede celým procesem a pomůže vám nejen splnit legislativní požadavky, ale i zvýšit a zefektivnit reálnou bezpečnost vaší organizace, obraťte se na nás. Produkt Gordic CSA je určen právě pro vás.

www.gordiccybersec.cz

▸ **Firemní zabezpečení**

Radek Kubeš
radek.kubes@economia.cz

Jak řešit bezpečnostní rizika podnikové mobility?

S rostoucí mírou využívání mobilních zařízení a souvisejících systémů či aplikací ve firmách nutně rostou i s tím spojená rizika. V současné době už prakticky nelze oddělit používání mobilních zařízení pro soukromé a pracovní účely, což ovšem znamená, že se v našich každodenně používaných zařízeních běžně vyskytují citlivá podniková data. Ať už jde o e-maily, dokumenty, nebo třeba různé přístupové údaje k podnikovým aplikacím a systémům, citlivý obsah chytrých telefonů či tabletů si žádá odpovídající zabezpečení. Uvědomuje si to i stále více firem, což odpovídá setrvalému růstu investic do podnikových řešení pro zabezpečení mobilních zařízení. Například analytici Mordor intelligence uvádějí, že trh těchto řešení poroste z letošních 1,35 miliardy dolarů na 2,35 v roce 2030.

Mobilní zařízení zkrátka představují pro podniky nejen velké příležitosti pro zvýšení efektivity díky dostupnosti systémů a dat skutečně odkudkoli, ale také zásadní výzvu z hlediska kybernetické bezpečnosti. Podle zprávy Zimperium's 2025 Global Mobile Threat Report používá polovina mobilních zařízení zastaralé verze svého operačního systému a čtvrtinu z nich ani aktualizovat nelze. Používání zařízení s operačními systémy s neošetřenými bezpečnostními mezerami je přitom doslova pozvánkou pro kyberútočníky, kteří se dnes již soustřeďují na mobilní zařízení více než na klasické počítače.

Útoky stále častěji využívají AI

K hlavním formám útoků na mobilní zařízení patří bezpochyby smishing, tedy obdoba phishingových útoků prostřednictvím e-mailů, která využívá jak SMS, tak i další formy zpráv posílaných mezi mobilními telefony (například WhatsApp, Telegram, Signal). Cílem smishingu je především získat přístupové údaje k podnikovým systémům prostřednictvím podvržených přihlašovacích stránek, vylákat z uživatelů jiné citlivé informace nebo je navést k instalaci škodlivých aplikací (malwaru). Velmi často jde také o finanční podvody, kdy se prostřednictvím zpráv jménem nadřízených manažerů snaží útočníci své oběti přesvědčit, aby provedly finanční transakce v jejich prospěch.

Podobně jako v případě e-mailového phishingu se i na mobilních zařízeních stále častěji objevují vysoce cílené, sofistikované útoky, které využívají techniky sociálního inženýrství a hlubokou znalost prostředí konkrétní firmy (takzvaný spear smishing). S nezbytným průzkumem informací z veřejně dostupných zdrojů pomáhá dnes útočníkům i technologie umělé inteligence (AI), kterou kyberzločinci zneužívají také k vytváření stále důvěryhodnějších smishingových zpráv.

Další kategorii mobilních hrozeb představuje již zmíněný malware, nejčastěji v podobě škodlivého softwaru, schopného zachytávat citlivé informace, jako jsou přihlašovací údaje, a odeslat je útočníkům. Tento stalkerware ale umí z mobilů vytěžovat i jiná data, včetně komunikace, kontaktů či dokumentů, stejně jako může pořizovat snímky obrazovek.

~ Žádný přístup není považován za implicitně bezpečný. I v případě, kdy útočník projde první vrstvou zabezpečení, musí opakovaně prokazovat oprávnění a incident může být včas zastaven.

Pro kompromitaci dat ale není nezbytné mobilní zařízení infikovat malwarem. Při používání veřejných wi-fi sítí představují závažnou hrozbu útoky typu Man-in-the-Middle (MitM), kdy útočník vstoupí do komunikace uživatele s cílovým serverem, aby zachytával nebo modifikoval přenášená data. Prostředkem MitM útoků bývají přístupové body k wi-fi sítím, které vypadají jako legitimní služby na letištích, v kavárnách nebo třeba v nákupních centrech. Po připojení k takové síti bez využití podnikové VPN může útočník zachytávat nešifrovaný síťový provoz.

Když chybí kontrola

Studie analytiků se shodují v tom, že více než 80 procent podniků dnes nějakým způsobem aplikuje strategii BYOD (bring your own device), a tedy umožňuje svým zaměstnancům využívat k pracovním účelům i jejich vlastní zařízení. Pro firmy to znamená možnost zásadních úspor a často též zvýšení spokojenosti a loajality zaměstnanců, nicméně to přináší také značná rizika.

Mezi hlavní problémy patří především riziko kompromitace citlivých dat v případě ztráty nebo odcizení zařízení, velmi omezená kontrola nad zařízením a tím, kdo ho ve skutečnosti používá, a samozřejmě také menší možnosti aplikování bezpečnostních politik na taková zařízení. Jakýkoli způsob správy mobilních zařízení používaných v rámci programu BYOD komplikuje rovněž vysoká variabilita operačních systémů takových zařízení.

Technická řešení pro mobilní bezpečnost

Základem efektivní mobilní bezpečnosti je nasazení systémů pro správu mobilních zařízení (mobile device management, MDM) nebo alespoň správu mobilních aplikací (mobile application management, MAM). Oba tyto systémy umožňují firmám zavést centralizovanou správu a alespoň základní zabezpečení mobilních zařízení. Pokročilejší jsou řešení MDM, která umožňují i vzdálenou úpravu nastavení mobilních zařízení, včetně aplikování bezpečnostních politik (například vynucení šifrování a používání silných přístupových hesel), kontrolu instalovaných aplikací a v případě ztráty zařízení jeho vzdálené vymazání a uzamknutí. Kromě toho poskytuje MDM také přehled o celkovém stavu a způsobech používání mobilních zařízení v rámci podniku.

Technické řešení pro oddělení soukromého a pracovního obsahu spočívá v takzvané kontejnerizaci, kdy dojde ke vzájemné izolaci firemních a soukromých aplikací a dat do samostatných prostředí. Používání podnikových aplikací a dat následně vyžaduje dodatečnou autentizaci, typicky prostřednictvím hesla nebo biometrie. Pro zajištění ještě vyšší úrovně ochrany citlivých dat je také možné zablokovat různé funkce mobilních zařízení, jako je třeba možnost používat jejich fotoaparát, kopírovat textový obsah, pořizovat snímky obrazovky a samozřejmě také instalovat neschválené aplikace.

Rizika vzdáleného přístupu

Jestliže mluvíme o podnikové mobilitě, nelze opomenout ani způsob, jakým se zaměstnanci ze svých mobilních zařízení přihlašují k firemním systémům a aplikacím. Významný podíl úspěšných kybernetických útoků totiž začíná právě zneužitím uživatelských oprávnění, získaných typicky prostřednictvím phishingu. Proto zabezpečení podnikových mobilních řešení závisí především na správném řízení přístupových oprávnění.

Minimálním opatřením na posílení klasického přihlašování prostřednictvím uživatelského jména a hesla je zavedení vícefaktorového ověřování (multi-factor authentication, MFA). Je ale paradoxní, že mnoho firem MFA nezavádí kvůli určitému „nepohodlí", nebo jej aktivují všem zaměstnancům kromě managementu. Ve skutečnosti ale právě toto opatření dokáže zastavit většinu útoků hned v jejich zárodku.

Další posílení MFA představuje takzvaný podmíněný přístup, kdy dochází k vyhodnocování dalších faktorů (použité zařízení, lokace nebo čas přihlášení) a dynamické úpravě pravidel pro ověření oprávněného uživatele. Ještě silnějším konceptem je princip nulové důvěry (zero-trust), kdy se ověřování provádí průběžně, a nikoli jen při úvodním přihlášení. Žádný přístup není považován za implicitně bezpečný a vše se ověřuje. I v případě, kdy útočník projde první vrstvou zabezpečení, musí opakovaně prokazovat oprávnění a incident může být včas zastaven.

Aktuálně nejvyšší úroveň zabezpečení mobilního přístupu poskytují privátní sítě 5G. Ty poskytují vlastní izolovanou síť ve vyhrazeném pásmu, ve které může podnik sám spravovat připojená zařízení. Koncept privátní sítě 5G může nahradit i podnikovou VPN pro vzdálené připojení výrazně bezpečnější a pro uživatele komfortnější technologií.

Podobně jako ve všech ostatních oblastech kybernetické bezpečnosti ale platí, že ani mobilní bezpečnost není konečný stav. Jde o průběžný proces kontroly a posilování bezpečnostních opatření v reakci na nové poznatky a hrozby.

Rizika vlastních zařízení ve firmě. *Více než 80 procent firem dnes umožňuje zaměstnancům používat k práci vlastní zařízení. Strategie BYOD sice snižuje náklady a zvyšuje spokojenost zaměstnanců, zároveň ale výrazně zvyšuje riziko ztráty dat a snižuje kontrolu nad zabezpečením.* **Foto: Shutterstock**

▸ NIS2

Anežka Hesová
anezka.hesova@economia.cz

Spíš než pokuty hrozí firmám napadení a ztráta důvěryhodnosti

Jak bude firma fungovat v situaci ohrožení? Jak má zabezpečené své informační systémy a spolehlivý dodavatelský řetězec? Řadu podobných otázek budou muset mít zhruba za rok a půl zodpovězené a důkladně zdokumentované všechny organizace působící v ekonomicky, společensky a bezpečnostně významných odvětvích, jako je energetika, zdravotnictví či doprava, ale také jejich velcí dodavatelé. Udává jim to nově schválená novela zákona o kyberbezpečnosti, která implementuje do české legislativy evropskou směrnici NIS2. Od definitivního vyhlášení ji už dělí jen podpis prezidenta.

„Předpisová základna tohoto zákona je opravdu rozsáhlá, zahrnuje více než 35 politik a směrnic, které firmy musí sepsat," upozorňuje Vlad Cohen, který k usnadnění tohoto procesu spoluzaložil a řídí platformu AuditMaster. Ta využívá umělou inteligenci k tomu, aby sladila požadavky zákona s konkrétní podnikovou dokumentací a urychlila adaptaci dané firmy na nové bezpečnostní nároky.

Nová legislativa zpřísňující požadavky na kybernetickou bezpečnost se bude týkat tisíců firem, z nichž mnohé to ještě ani netuší. Jak zjistí, zda mezi ně patří, nebo ne?
Už teď si mohou provést sebeurčení na portálu Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) nebo se obrátit na odborníky, případně na své právníky, kteří posoudí, zda se na ně připravovaná legislativa vztahuje a v jakém režimu. Může se stát, že se firma do této kategorie zařadí na základě své vedlejší činnosti nebo kvůli tomu, že má výkonnou fotovoltaiku. Dá se očekávat, že některé firmy přehodnotí rozsah svého podnikání uvedený v obchodním rejstříku, aby se zařadily do režimu s nižší mírou regulatorních povinností.

Ujel podle vás vlak firmám, které s přípravou na nová pravidla kyberbezpečnosti ještě nezačaly?
To je velmi individuální. Záleží na tom, zda bude firma spadat do vyššího, nebo nižšího režimu, a také na její velikosti, komplexitě a současném stavu zabezpečení. Pokud to firma dosud neřešila vůbec a bude spadat do vyššího režimu, tak ji čeká intenzivní práce na celý rok. Zákon v červnu prošel Senátem a nyní čeká na podpis prezidenta. Očekávám, že nová sbírka zákonů vyjde na začátku srpna a poté mají firmy šedesátidenní lhůtu na to, aby se přihlásily k tomu, že se na ně zákon vztahuje. Další rok pak mají na přípravu požadovaných kyberbezpečnostních opatření.

Znamená to, že za rok od zahájení této lhůty už musí všechny požadavky NIS2 splňovat?
Zákon stanovuje, že poskytovatelé regulovaných služeb musí do jednoho roku přinejmenším se zaváděním bezpečnostních opatření začít. Požadavky zákona o kybernetické bezpečnosti směřují k neustálému zlepšování informační bezpečnosti, je to proces, který nikdy nekončí.

Nad rámec požadavků EU *Implementace unijních předpisů do české legislativy bývá přísnější než původní evropské zadání. Novela zákona o kyberbezpečnosti není výjimkou. „Proto vyvíjíme nástroj, který se detailně orientuje právě v české právní úpravě této směrnice," říká Vlad Cohen o softwaru AuditMaster.* **Foto: HN – Václav Vašků**

Jak na tom obecně české firmy jsou z hlediska kybernetického zabezpečení?
Ze zkušeností s firmami, se kterými spolupracujeme, mohu říci, že střední a větší podniky bývají po technické stránce dobře vybavené a mají kybernetickou ochranu systematicky řešenou. Nicméně z pohledu systému řízení bezpečnosti se zde často vyskytují zásadní nedostatky, zejména v oblastech řízení aktiv, řízení rizik, kontinuity činností a řízení dodavatelů. Pro naplnění požadavků zákona o kybernetické bezpečnosti je však klíčové prokázat auditovatelným způsobem, že bezpečnost je řízena systematicky a kontinuálně. To zahrnuje existenci bezpečnostních politik, směrnic, procesní dokumentace, řízení rizik a dalších organizačních opatření. Většina firem tyto prvky buď vůbec nemá, nebo má jen velmi základní nastavení. Největší část práce je tedy čeká právě v oblasti organizačních opatření.

Je vůbec na trhu dostatek odborníků, kteří by na požadovanou úroveň dostali najednou tisíce firem?
Samozřejmě ne. V ideálním světě by to teď šest tisíc subjektů začalo poctivě řešit a kapacity by k tomu nebyly. Realita je ale jiná, to jsme viděli už při implementaci zákona o ochraně osobních údajů. Řekl bych, že jsou v Česku čtyři skupiny firem. Jedna už se svědomitě připravuje na to, aby požadavky splňovala. Druhá se do toho pustí poté, co zákon oficiálně vejde v platnost. Třetí to začne řešit až v době, kdy se objeví kontroly a pokuty. A čtvrtá skupina začne řešit implementaci až ve chvíli, kdy se dostane do problémů.

Co hrozí firmám, které nebudou požadavky nového zákona splňovat?
Kontroly má provádět NÚKIB a avizované pokuty mohou dosáhnout 10 milionů eur nebo dvou procent z celosvětového obratu. Osobně si ale myslím, že takové sankce padat nebudou, ani za GDPR nikdo tak vysokou pokutu nedostal. Přesto jsem přesvědčen, že dostát požadovaným nárokům se vyplatí. Zákon ukládá chránit se proti kybernetickým útokům, takže to, co firmám reálně hrozí, není ani tak pokuta, jako napadení nebo ztráta kredibility.

Investice do větší odolnosti firmu posune o několik úrovní výš a řízení rizik je skutečně alfou a omegou bezpečného fungování jakékoli společnosti, pokud chce být důvěryhodná pro své zahraniční partnery a pro účast ve výběrových řízeních. Jde totiž nejen o ochranu před kybernetickými útoky, ale také o plán kontinuity činností, který zajišťuje chod firmy v případě jakékoli neočekávané události. Zákon o kybernetické bezpečnosti zvýší povědomí veřejnosti, a podnikatelé tak budou muset dbát na ochranu dat i v zájmu důvěry svých zákazníků.

Jak může s přípravou na NIS2 pomoci umělá inteligence?
Volně dostupné služby jako ChatGPT pochopitelně velmi omezeně. Ale my jsme ve spolupráci s odborníky z firmy Whirr Crew vyvinuli nástroj AuditMaster, který za pomoci umělé inteligence dokáže posoudit soulad firemních dokumentů s aktuální legislativou. Tento software zautomatizuje potřebné analýzy, což podnikům výrazně sníží náklady na procesy, které by jinak musely provádět zdlouhavě a neefektivně. Na českém trhu nevím o žádném jiném nástroji, který by tohle nabízel.

A v zahraničí?
Tady je potřeba si uvědomit, že NIS2 je sice evropská směrnice, ale její zakomponování do legislativy jednotlivých států má svá specifika. A v případě Česka je opravdu unikátní, české pojetí toho zákona je dost komplexní, takže firma potřebuje mít nástroj, který se specializuje právě na českou právní úpravu.

Co všechno takový nástroj umí?
V první řadě pomůže s rozdílovou analýzou, tedy s porovnáním, jak stávající dokumentace odpovídá požadavkům zákona. Poté navrhne plán nápravných opatření. Firmy, které zatím žádnou dokumentaci nemají, provede postupem přípravy krok za krokem a poskytne jim předpřipravené šablony. Pomůže ale i s následnou dlouhodobou správou systému. Ta obnáší řízení aktiv a rizik, analýzu dopadů na podnikání, správu dodavatelů a případně také hlášení bezpečnostních incidentů.

Nahradí takový software odbornou asistenci specialistů na kyberbezpečnost?
To rozhodně ne. Odborný konzultant – ať už interní, nebo externí – je v tomto procesu nenahraditelný. Rozdíl je ale v tom, že když takový expert bude dělat například rozdílovou analýzu standardním způsobem, tedy porovnávat každý ze stovek požadavků s příslušným dokumentem firmy, bude to podstatně delší a dražší proces, než kdyby k tomu využil chytrý software, jako je AuditMaster.

Jaký další vývoj očekáváte v oblasti kyberbezpečnosti a jak se na něj připravit?
Z geopolitického pohledu bohužel všechno nasvědčuje tomu, že kybernetických útoků bude dál přibývat, už teď je meziroční nárůst téměř dvacetiprocentní. Zvyšování požadavků na ochranu je proto velmi logické. Z legislativního pohledu můžeme určitě počítat s dalším zpřísňováním v rámci NIS3 a obecně s pokračujícím tlakem na zabezpečení i těch firem, které do aktuálně platné legislativy zatím nespadají. Donutí je k tomu mimo jiné tendry a zahraniční partneři, kteří budou příslušné standardy stále více vyžadovat.

Text vznikl ve spolupráci se společností **Whirr Crew**.