KOMORA

SPECIÁL

PODNIKÁNÍ & BEZPEČNOST

NIS2 NASTUPUJE

NEJČASTĚJŠÍ CHYBY

BEZPEČNOST NENÍ SAMOZŘEJMOST

Foto: archiv Cybrela a Shutterstock.com

Nejčastější chyby při samoidentifikaci dle nové kyberlegislativy

Směrnice NIS2 a její zavedení do české legislativy se rychle blíží. Předpokládá se, že návrh nového zákona o kybernetické bezpečnosti bude platný již v polovině roku 2025. První klíčovou povinností podle nového zákona je se samoidentifikovat, tedy zjistit, jestli bude vaše společnost regulovaným subjektem.

Již v tomto bodě však mnoho podnikatelů tápe, a proto se podíváme na nejčastější chyby a jak se jich ideálně vyvarovat.

Chyba č. 1: Nevím, že mám nějakou sebeidentifikaci vůbec udělat

Přestože Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) dělá v této oblasti osvětu na velmi vysoké úrovni, stále najdeme společnosti, ke kterým se plánovaná novinka v jejich povinnostech nedostala. Množství všech regulací pro společnosti je obrovské, ale jak tvrdí známý právní princip: neznalost zákona neomlouvá.

Směrnice NIS2 rozšířila počet regulovaných subjektů z cca 360 na odhadovaných 12–15 000 v Česku a 10 000 subjektů na Slovensku. Předpokládaný nárůst je tedy dramatický a šance, že na vás nový zákon dopadne, je tak docela vysoká.

Proč je samoidentifikace vlastně tak klíčová povinnost? Pokud byste byli regulovaným subjektem a neohlásili se na NÚKIB, dopustíte se přestupku. A protože NÚKIB se na toto jednání dívá tak, že se chcete vyhnout svým povinnostem, může za něj uložit ty nejvyšší pokuty dvě stě padesát milionů korun nebo až 2 % čistého celosvětového ročního obratu podniku, a to podle toho, která částka je vyšší).

Chyba č. 2: Nepochopení regulovaných služeb

Návrh nové legislativy bude dopadat na společnosti, které poskytují službu z regulovaného odvětví a naplňují další kritéria. Regulované služby jsou významné pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost a jsou z 15 různých odvětví.

Jedná se o tato odvětví:

- veřejná správa a výkon veřejné moci;
- energetika;
- výrobní průmysl;
- potravinářský průmysl;

- chemický průmysl;
- vodní hospodářství;
- odpadové hospodářství;
- doprava;
- digitální infrastruktura a služby;
- finanční trh;
- zdravotnictví;
- věda, výzkum a vzdělávání;
- poštovní a kurýrní služby;
- obranný průmysl;
- vesmírný průmysl.

Zní to poměrně jednoduše, a pokud tedy nedělám nic v těchto odvětvích, nemusím novou kybernetickou legislativu vůbec řešit? Chyba. Pořád se na vás může vztahovat jedna z výjimek uvedených v zákoně.

Další a mnohem častější chybou, kterou společnosti dělají, je, že zaměňují svou hlavní činnost s odvětvími regulované služby. Nový zákon se však nezajímá jen o činnosti, které jsou vaším klíčovým byznysem, ale o vše, co děláte.

Můžeme si to uvést na příkladu, kdy společnost vyrábí třeba hračky pro domácí mazlíčky. Firma si ověřila, že výrobní průmysl se na tuto výrobu nevztahuje, a tak udělala závěr, že se na ni regulace nebude vztahovat. To by pak ale nebyl dobrý příklad, kdyby to byl konec příběhu. Jenže tato společnost má dceřinou společnost, která šije oblečky pro psy, a mateřská společnost ji spravuje celé jejich IT, přičemž jí tyto služby následně i fakturuje. Toto ji už klasifikuje do odvětví digitální infrastruktury a služeb, konkrétně by mohla poskytovat regulovanou službu poskytování řízené služby (MSP) či poskytování řízené bezpečnostní služby (MSSP). Nezáleží na tom, že poskytování IT služeb není její hlavní činností.

Společnosti musí identifikovat všechny regulované služby, které poskytují, ať se jedná o jejich hlavní činnost, nebo nikoliv. Zamyslete se nad všemi svými aktivitami, přestože vám na první pohled vůbec nepřipadají důležité. A nezapomeňte, regulovaných služeb můžete poskytovat i více a nahlásit musíte všechny.

Chyba č. 3: Špatné určení velikosti podniku

Kromě činnosti v regulovaných odvětvích je dalším typickým kritériem velikost podniku. Pokud byste vykonávali činnost v rámci regulovaného odvětví, ale nenaplnili potřebnou podmínku požadované velikosti, nový kybernetický zákon na vás dopadat nebude.

Ani v tomto případě však nezapomínejme na výjimky a další kritéria bez ohledu na velikost. Velikost subjektu se počítá podle doporučení Komise 2003/361/ES, které definuje mikropodniky, malé, střední a velké podniky. Posouzení podniku vychází buď ze zaměstnaneckého, nebo z finančního ukazatele.

Malé společnosti mají maximálně 49 zaměstnanců, střední 50 až 249 a velké 250 a více. Problém nastává v tom, že do počtu zaměstnanců se musí zohlednit i takzvané „relevantní vazby mezi majetkově spřízněnými organizacemi“. Co to znamená? Například to, když jste dceřinkou velké společnosti nebo součástí holdingu. V těchto případech se totiž jedná o zmíněnou majetkovou spřízněnost a do celkového počtu zaměstnanců se započítávají i zaměstnanci dceřiných, sesterských či mateřských společností. A to buď v plné míře, nebo poměrně podle míry majetkové spřízněnosti. Společnost s 10 zaměstnanci se tak díky své mateřské společnosti může stát i velkým podnikem, protože

Kateřina Hůtová

v souhrnu bude mít více než 250 zaměstnanců. Do návrhu kybernetického zákona byla v květnu letošního roku vložena nová výjimka pro tyto majetkově propojené společnosti. Ta říká, že za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od technických aktiv, jež používá posuzovaná osoba při poskytování regulované služby. Dle důvodové zprávy by se mělo typicky jednat o situace investování do startupů. Jak to s touto výjimkou však dopadne, si ale budeme muset počkat do konce legislativního procesu.

Chyba č. 4: Zmatek v režimech regulovaných služeb

Když se sebeidentifikujete a jako regulovaný subjekt ohlásíte svou regulovanou službu na NÚKIB, máte první krok za sebou. NÚKIB vás zaregistruje a dále vám začínají další povinnosti dle režimu, ve kterém regulovanou službu poskytujete. Pokud máte jen jednu regulovanou službu, budete se řídit bezpečnostními opatřeními a splňovat povinnosti dle režimu, který tato regulovaná služba určuje. Může se jednat o vyšší režim (více povinností), nebo nižší režim.

Společnosti zde chybují v případě, kdy se chtějí připravit na novou legislativu a poskytují více regulovaných služeb, přičemž jedna regulovaná služba je určena v nižším a druhá regulovaná služba ve vyšším režimu. Společnosti se pak chtějí připravovat na oba režimy zároveň nebo si zvolí pro ně výhodnější – nižší režim. Protože společnosti mohou mít pouze jeden režim, uplatňuje se zde pravidlo „vyšší bere“. Pokud máte i jen jednu z mnoha regulovaných služeb ve vyšším režimu, je pro vaši společnost rozhodující režim vyšších povinností.

Chyba č. 5: Jsem dodavatel regulovaného subjektu = jsem regulovaný subjekt?

Návrh nového zákona o kybernetické bezpečnosti se zmiňuje i o dodavatelích regulovaných subjektů.

Kateřina Kubíková

Ti budou muset splňovat určité povinnosti. Půjde hlavně o pravidla, která na ně dopadnou prostřednictvím jejich zákazníků (regulovaných subjektů). To, že dodáváte své služby regulovanému subjektu, vás samo o sobě mezi regulované subjekty nekvalifikuje.

Dodavatel musí sám poskytovat nějakou regulovanou službu, aby se stal regulovaným subjektem, a zároveň naplnit všechna ostatní kritéria, která daná regulovaná služba bude požadovat. Proto i dodavatel jako každá jiná společnost se musí sám samoidentifikovat a určit, jestli je regulovaným subjektem. Pokud nebude, budou se na něj vztahovat jen povinnosti jako na dodavatele regulovaných subjektů a nebudete se muset ohlašovat na NÚKIB.

Už víte, jestli spadáte pod novou legislativu? Ověřte si v bezplatné aplikaci URČI SE (viz QR kód), zda pod novou regulaci pravděpodobně spadnete, či nikoliv. Dozvíte se i to, co budete muset případně plnit a jaké by měly být vaše další kroky. ■

KATEŘINA HŮTOVÁ A KATEŘINA KUBÍKOVÁ, Cybrela

Pomocník pro samoidentifikaci

https://urci.se/

Firmy by neměly vyčkávat na to, co jim přikáže zákon

Tisíců tuzemských firem se v příštím roce dotkne zákon, který určí, jak se budou muset chránit před kybernetickými útoky. Pro firmy, které se svému zabezpečení doposud příliš nevěnovaly, může být zavedení nutných opatření velmi nákladné. Podle předpokladů přitom bude zákon představovat spíše minimální míru zabezpečení a firmy by měly být v kybernetické ochraně ve vlastním zájmu důslednější. Měly by se kybernetické ochraně věnovat dlouhodobě, jednorázová investice nestačí.

Zejména státní správa, zdravotnický segment a středně velké firmy v českém vlastnictví často vyčkávají na konkrétní legislativní pojetí zákona o kybernetické bezpečnosti a vůbec ne na to, zdali se jich povinnost bude týkat. I tyto subjekty by se každopádně měly před hackerskými útoky chránit, a to již nyní. Bez správného zabezpečení jim při úspěšném kybernetickém útoku hrozí až milionové finanční ztráty, případně i reputační problémy. Zákonná povinnost bude vycházet z evropské směrnice NIS2, kterou se Česko společně s ostatními unijními státy zavázalo přijmout nejpozději do 17. října letošního roku v rámci připravovaného zákona o kybernetické bezpečnosti. Již nyní je ovšem jasné, že zákon stihne nabýt účinnosti nejdříve až v lednu 2025.

Důležitá je aktivní ochrana

Přijetí zákona se protáhne i z toho důvodu, že začátkem dubna vrátila Legislativní rada vlády návrh zákona Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB) s připomínkami k přepracování. Očekává se, že u návrhu zákona se upraví řada detailů, nicméně hlavní povinnosti pro firmy zůstanou beze změny, a měly by s nimi proto již teď předběžně počítat. Zákon se dle předkladatele má dotknout šesti tisíc firem, nejnovější analýzy ukazují na minimálně dvojnásobný počet. Pro firmy bude nová povinnost znamenat nejprve vytvoření dokumentů, které budou stanovovat postupy a chování organizace v souladu s novým zákonem o kybernetické bezpečnosti. Očekávají se výdaje řádově ve stovkách tisíc korun. Druhým krokem bude zavedení technických bezpečnostních opatření. Pokud firma nemá dosud žádná technická opatření, náklady se mohou pohybovat v rozmezí vyšších stovek tisíc až jednotek milionů korun. K tomu se přičte následná podpora těchto technologií v dalších letech jejich provozu. Firmy by měly mít na paměti udržování aktivní ochrany a potřebného financování dlouhodobě. Stává se, že sice mají v pořádku nastavené procesy i dokumentaci, jenže samotná praxe za tím zaostává, čímž se firma zbytečně dostává do rizika.

Nastavit a prověřit

Až budou mít firmy svou ochranu nastavenou, měly by svou odolnost vůči útokům prověřit – externími testy zranitelnosti, nebo tzv. penetračními testy. Zároveň by si firmy měly v kritických systémech udělat audit toho, jaké mají dodavatele, jak ti jsou zabezpečeni a jaká u dodavatelů existují rizika.

Kybernetické útoky jsou stále komplexnější a zákeřnější, pro firmy je tak zásadní sledovat aktuální trendy, aby se před nimi mohly chránit a mohly správně proškolit své zaměstnance. Jednou z relativních novinek je vylákání citlivých údajů už ne za pomoci širokého a relativně nahodilého posílání spamů, ale díky zacílení na konkrétního zaměstnance. Metoda nazývaná spear phishing spočívá ve vytipování lidí, jejichž údaje jsou nejcennější, kterým útočníci pošlou zprávu přesně na míru, aby zvýšili pravděpodobnost úspěchu a vylákali z nich, co potřebují. ■

TOMÁŠ KUBÍČEK

NIS2: TÝKÁ SE NOVÉ NAŘÍZENÍ I VAŠÍ SPOLEČNOSTI?

Nová legislativa se v česku dotkne více než 9000 společností.
Řídit kybernetická rizika a chránit svá aktiva by měl každý.

- Počet kyberútoků se meziročně téměř zdvojnásobil.
- Aktéři používají jako prvotní přístup především phishing a sociální inženýrství.
- Roste počet útoků na firmy přes jejich dodavatelské řetězce.
- Kybernetické útoky jsou díky AI sofistikovanější a ničivější.
- Cílem je nainstalovat škodlivý ransomware, nebo ochromit firmu zahlcením internetové služby (DDoS).
- Nejčastějšími cíli hackerů jsou firmy významné pro chod státu a ekonomiky.

?

- Spadá vaše společnost mezi regulovaná odvětví nebo spolupracuje s firmami, na které se vztahuje?
- Jak se vhodně připravit na zavedení NIS2, abyste plnili nové povinnosti?
- Jak zajistit kybernetickou bezpečnost firmy a jejich aktiv, abyste byli odolní vůči kybernetickým hrozbám?
- Jak řídit kybernetická rizika dlouhodobě a efektivně?

Zdroj: NÚKIB, ENISA Threat Landscape 2023

CO VÁM UMÍME V OBLASTI NIS2 NABÍDNOUT?

01
Zajistíme, aby byla vaše společnost adekvátně připravena na nové regulatorní povinnosti.

02
Provedeme vaši firmu celým procesem zavádění změn tak, abyste dosáhli a udrželi pod kontrolou soulad s regulací prakticky a efektivně (děláte to primárně pro ochranu vlastní firmy, ne kvůli regulaci).

03
Posoudíme účinnost implementovaných bezpečnostních opatření a ověříme soulad s aktuální legislativou a nejlepší oborovou praxí u vaší společnosti nebo třetích stran, se kterými spolupracujete.

04
Poskytneme vám kapacitu našich zkušených odborníků, kteří jsou oprávněni zajišťovat role manažera, architekta, nebo auditora kybernetické bezpečnosti.

05
Pomůžeme vám vyznat se ve světě bezpečnostních technologií a vyvážit zvýšení vaší kyberodolnosti s náklady.

06
Nabízíme různé možnosti spolupráce dle individuálních představ a potřeb (co-sourcing, outsourcing, interim, odborné konzultace).

07
Pomůžeme vám nastavit technické a organizačně-procesní prostředí tak, aby byla vaše firma dostatečně odolná vůči kybernetickým rizikům a hrozbám dnes i zítra.

08
Díky globální síti můžeme čerpat ze znalostí a odvětvových zkušeností expertů celého světa.

POSOUZENÍ

- GAP analýza technické a procesní bezpečnosti
- Posouzení stávající situace, hodnocení a návrh řešení, které bude splňovat legislativu i specifické potřeby firmy
- Analýza možností financování vč. využití dotací

DOSAŽENÍ SOULADU

- Návrh a implementace procesních a technických změn
- Asistence při výběru a nasazení bezpečnostních technologií
- Zavedení systému pro správu a řízení rizik a událostí

OVĚŘOVÁNÍ SOULADU

- Ověření souladu s platnou legislativou
- Ověřování třetích stran (dodavatelů, partnerů)
- Cílené konzultace a jiné formy spolupráce s týmy interního auditu a IT klienta
- Penetrační testování

BĚŽNÝ PROVOZ

- Školení
- Aktualizace systému informační a kybernetické bezpečnosti
- Implementace systémového SW řešení pro správu a řízení rizik a událostí (BDO RiskFlow)
- IT Security monitoring

SLUŽBY BDO DIGITAL

Technologické poradenství
- Řízení IT projektů
- Systémová integrace
- Vývoj a modernizace IT systémů

Kybernetická odolnost
- Zvyšování kybernetické odolnosti
- Penetrační testování a testování zranitelnosti
- Incident response

Digitalizace
- Strategie a řízení inovací
- Digitální transformace
- Automatizace a robotizace procesů
- Datová věda, BI
- Využití AI

Compliance a regulace
- Zákon o kybernetické bezpečnosti dle NIS2, DORA
- SW pro správu a řízení rizik a událostí s prvky AI
- ISO27001 a ISMS: nastavení procesů a příprava na certifikaci
- IT audity

www.bdo.cz

INNOVATION | SOLUTIONS | COMPLIANCE

Návrh nového zákona o kybernetické bezpečnosti v části Hospodářské komory vzbuzuje velké vášně

Kybernetická bezpečnost v krabici

Kybernetickou bezpečnost stejně tak jako GDPR za vás nevyřeší nikdo tím, že vám prodá krabici. Řešit a zvyšovat její úroveň můžete a musíte sami, třeba s pomocí. Každý, kdo vám bude tvrdit, že nákupem jeho řešení vše vyřešíte, chce jen vaše peníze.

Nový kybernetický zákon se bude tentokrát týkat velkého množství organizací, zejména pak malých a středních podniků, které budou muset nově investovat nemalé částky do infrastruktury a zaměstnanců. Situace je o to horší, že nezaměstnanost v ČR je na velmi nízké úrovni, a navíc odborníků je všeobecně velký nedostatek, což tlačí ceny specialistů nahoru. Situaci ještě komplikuje fakt, že organizace musejí povinně provádět prověřování svých významných dodavatelů, což jsou dodavatelé, na nichž jsou přímo závislé, nebo by výpadky jejich dodávek přímo ohrozily fungování společnosti. Na tyto dodavatele pak budou muset přenést i část svých povinností. Povinných organizací tedy pravděpodobně bude více, než odhadují aktuální statistiky, které mluví o 5 000 až 6 000 společnostech. Odhady se různí, ale více než 12 tisíc společností nebude překvapením.

Nové povinnosti

Pro specialistu KB není problém s pochopením povinností. Vlastně to není ani problém pro manažera. Stačí si udělat seznam jednotlivých paragrafů a odškrtávat splněné povinnosti. Pojďme se na ně tedy podívat.

Systém řízení bezpečnosti informací

Definovat cíle KB, sledovat je a hodnotit. Vytvořit základní směrnice a postupy pro nakládání s daty (klasifikace, formy zabezpečení, řízení rizik a incidentů, zálohování, provádění auditů/kontrol, monitorování KB, plány pro změny, postupy pro bezpečný vývoj).

Povinnosti vrcholového vedení

Zajistit a podporovat KB a zajistit zdroje, seznámit se s KB, vzdělávat sebe a zaměstnance v oblasti KB, podílet se na analýzách, auditech, řízení rizik, podporovat cíle, zajistit mlčenlivosti, zajistit testování a prokazatelně řídit KB. Zajistit ustanovení rolí (manažera, architekta a auditora kybernetické bezpečnosti, jmenovat garanty aktiva a jmenovat výbor KB).

Bezpečnostní role

Zajistit výše jmenované role s vhodnou kvalifikací, stanovit povinnosti, odpovědnosti, zajistit jim další vzdělávání, zajistit dostatečné zdroje pro jejich fungování a zajistit jejich nezávislost.

Řízení bezpečnostní politiky a bezpečnostní dokumentace

Tato kapitola je doplňkem či rozšířením k systému řízení bezpečnosti informací – jde o doplnění a o pravidelné aktualizace, nastavení procesu a postupů pro jednotlivé kapitoly a činnosti v rámci KB.

Řízení aktiv

Tato kapitola je jedním ze základních prvků a zároveň nejpalčivějším problémem. Je třeba vytvořit seznam všech aktiv (tedy všeho, co se podílí nebo má vliv na fungování společnosti a může ovlivnit její fungování) a nastavit pro ně pravidla.

Řízení rizik

Identifikovat Hrozby a Zranitelnosti a zjistit, které působí na daná aktiva. Nastavit proces snížení finálních rizik, vypracovat plány na snižování identifikovaných rizik a zajistit aktualizaci a řízení rizik na všech úrovních.

Řízení dodavatelů

Významnou novinkou je výběr takových dodavatelů, kteří budou mít dostatečně nastavenou KB, a to tak, aby neohrozili své a tím i vaše podnikání/aktivity/poskytované služby. Což obsahuje prověření dodavatele před samotným započetím spolupráce, nastavením vhodného smluvního vztahu nebo pravidelnými kontrolami / audity takových dodavatelů.

Bezpečnost lidských zdrojů

Tato kapitola je spíše rozšířením již běžně vykonávaných činností. Tedy zajistit plány školení KB pro zaměstnance, vedení, administrátory (osoby s privilegovanými rolemi a účty), osoby zastávající bezpečnostní role. Ale také zajistit vhodné prověření zaměstnanců před náborem. ■

PETR GONDEK, VOJTĚCH NOL (gdpr-support.cz)

Monitoring a prevence kybernetických hrozeb

Ochrana firemních systémů a webových aplikací

Firmy v Evropské unii čelí stále většímu tlaku na posílení kybernetické bezpečnosti, což je dáno zejména novou směrnicí NIS2, kterou zavedla EU. Směrnice klade důraz na ochranu kritické infrastruktury a zajištění nepřerušeného provozu i při vážných kybernetických hrozbách. Tyto hrozby dnes ohrožují nejen technické systémy, ale i kontinuitu podnikání a pověst firem. Úspěšná obrana proti kybernetickým útokům je klíčová pro ochranu firemních operací a dlouhodobou stabilitu.

Foto: Daria Yevsieieva

Implementace směrnice NIS2 vyžaduje zavedení moderních technologií, monitoringu a preventivních opatření. Firmy musí reagovat proaktivně, aby byly schopné předcházet útokům a chránit své systémy. Důraz se klade na rychlou detekci hrozeb a okamžitou reakci, což umožňuje minimalizovat rizika a zajišťuje kontinuitu provozu.

DNS servery jako kritická infrastruktura

Jednou z nejdůležitějších částí firemní IT infrastruktury jsou DNS servery. Mnoho společností si DNS servery spravuje interně, aby měly kontrolu nad svou sítí. Nicméně tato infrastruktura je často zranitelná, ať už z důvodu své zastaralosti, nebo náchylnosti k výpadkům a útokům.

Mezi nejčastější hrozby, které mohou DNS servery ohrozit, patří DDoS útoky (Distributed Denial of Service). Tyto se zaměřují na přetížení serverů tím, že na ně posílají obrovské množství požadavků, což vede k jejich výpadku. Útoky mohou mít devastující dopad na provoz firem, protože vedou k výpadkům webových stránek, nefunkčnosti e-mailových služeb a k paralyzování interních systémů, jako jsou CRM nebo skladové a výrobní systémy.

Pokud dojde k výpadku DNS serverů, firma se může dostat do stavu úplné paralýzy. Webové stránky, které slouží zákazníkům pro prohlížení produktů nebo stahování technické dokumentace, přestanou fungovat. Dále dojde k narušení e-mailových služeb, což může znamenat ztrátu důležitých obchodních příležitostí. V neposlední řadě bude ohrožen i provoz interních systémů, což by mohlo zastavit celou výrobu nebo jiné klíčové procesy.

Monitoring jako pomocník při plnění požadavků NIS2

V kontextu směrnice NIS2 hraje monitoring IT systémů zásadní roli při zajištění kybernetické bezpečnosti. Monitoring umožňuje firmám nepřetržitě sledovat jejich infrastrukturu, identifikovat anomálie a detekovat potenciální hrozby v reálném čase. To umožňuje nejen rychle reagovat na incidenty, ale také splnit oznamovací povinnost, kterou směrnice NIS2 ukládá. Tato povinnost zahrnuje hlášení kybernetických incidentů, které mohou mít vliv na provoz společnosti, což je klíčový aspekt zajištění kontinuity firemních činností.

WEDOS Global Protection (WGP) je účinný nástroj pro ochranu firemních webových stránek, DNS serverů a dalších částí infrastruktury. Chrání servery před DDoS útoky a udržuje webové stránky dostupné. Díky inteligentní filtraci škodlivého provozu snižuje počet požadavků na server, šetří jeho kapacitu a snižuje náklady. Použitá technologie rozkládá zátěž mezi DNS servery po celém světě, což zajišťuje vysokou dostupnost, stabilitu a rychlost webových služeb a zároveň zvyšuje důvěru zákazníků. Součástí služby je právě i výše zmiňovaný monitoring.

Ochrana webových stránek – klíčový prvek bezpečnosti

Webové stránky často představují veřejnou tvář firmy a jsou důležitým komunikačním kanálem se zákazníky a partnery. Přesto jsou mnohdy přehlíženým prvkem v rámci celkové kybernetické bezpečnosti. Kybernetické útoky zaměřené na webové stránky, jako jsou DDoS útoky nebo neoprávněné zásahy do obsahu, mohou nejen snížit jejich dostupnost, ale také výrazně poškodit firemní reputaci. Ochrana webových platforem, jakou poskytuje WEDOS Global Protection, je proto nezbytným doplňkem k ochraně interních firemních systémů. Zatímco firmy investují do zabezpečení svých výrobních procesů a interních IT infrastruktur, nesmí podcenit rizika spojená s veřejně dostupnými webovými stránkami. Ochrana těchto stránek zajistí jejich nepřetržitý provoz a ochrání firmu před finančními ztrátami nebo poškozením dobrého jména. Řešení WGP bylo navrženo tak, aby jeho implementace byla co nejjednodušší, bez nutnosti investovat do nového hardwaru či složitých technických změn.

Nenechávejte kybernetickou bezpečnost ani NIS2 na poslední chvíli

Začněte chránit svou firmu už dnes a zajistěte si bezproblémový provoz. Rádi se s vámi spojíme na obchod@wedos.cz, nebo pro více informací navštivte https://www.wedos.cz/nis2. ■

MARKÉTA PRŮŠOVÁ, specialista obchodní komunikace a B2B spolupráce

Příchod evropské směrnice NIS2 znamená rozšíření působnosti kybernetického zákona

Boj s kybernetickou zranitelností

Co je směrnice NIS2? Obnovená směrnice NIS (směrnice o bezpečnosti sítí a informačních systémů), která vstoupí v platnost po transpozici do českého zákona o kybernetické bezpečnosti v roce 2024. Během této doby mají firmy z veřejného i soukromého sektoru čas se na splnění svých povinností připravit. NIS2 je vlastně mladší sestrou NIS. Je však zkušenější, poučená z chyb minulosti, ale hlavně přísnější a nekompromisnější. Proč bychom se o ni měli zajímat?

Prvním důvodem budou povinnosti vyplývající z právních předpisů, kontrola jejich dodržování ze strany státu a dále pak sankce za jejich nedodržování. Druhým důvodem je celkový stav kybernetické bezpečnosti. Rychlý nárůst počtu kybernetických útoků se netýká jen velkých společností, ale vzhledem k nižší úrovni zabezpečení i malých a středních podniků. Podle dostupných statistik (Sophos) se počet útoků ransomwaru meziročně zvýšil až o 62 %. Celkově byly napadeny dvě organizace ze tří. Nezanedbatelné byly i náklady na řešení útoků. Průměrná výše celkových nákladů byla vyčíslena na 1,9 milionu eur.
Útokům je však možné účinně čelit zavedením bezpečnostních opatření, která definuje a zejména zpřísňuje NIS2. Zavedením preventivních opatření mohou organizace lépe předcházet bezpečnostním incidentům a zvýšit tak svou odolnost. Stoprocentní bezpečnost neexistuje, ale preventivní opatření jsou vždy méně nákladná a bolestivá než řešení dopadů kybernetického incidentu.

Regulační změny

Vzhledem k situaci v zemích EU se v NIS2 také výrazně rozšiřují odvětví a pododvětví, která budou povinna řešit kybernetickou bezpečnost, a tím i počet povinných subjektů. Jedná se o následující nová odvětví, která přibudou ke stávajícím:

- zdravotnictví – výroba a výzkum léčivých přípravků;
- dálkové vytápění a chlazení;
- poskytovatelé ICT služeb;
- správa ICT služeb;
- prostor;
- nakládání s odpady;
- odpadní vody;
- kurýrní služby;
- potravinářský průmysl – výroba, distribuce;
- výroba (automobilový průmysl, strojírenství, lékařské přístroje, PC a elektronika);
- výzkum;
- sociální sítě.

Rozsah bezpečnostních opatření se řídí regulovaným režimem, do kterého společnost spadá. Bezpečnostní opatření jsou povinná pro všechna regulovaná odvětví. Jediný rozdíl bude v přísnosti a rozsahu bezpečnostních opatření.
Budou existovat dva regulované režimy:

- Klíčové subjekty (tzv. Základní) – přísnější opatření
- Důležité subjekty (tzv. Important) – méně přísná opatření

První podmínkou pro určení povinného subjektu je poskytování alespoň jedné služby ze seznamu regulovaných služeb. Celý proces je založen na principu vlastní identifikace.
Druhou podmínkou je velikost podniku. Regulo-

vány budou střední a velké společnosti (podle současných definic velikosti společnosti). U některých služeb bude organizace regulována bez ohledu na velikost. Z tohoto důvodu je třeba sledovat legislativní změny. Další skutečností, kterou je třeba mít na paměti, je skládání velikosti společností například v případě holdingových společností, kdy se z malé společnosti může rychle stát střední až velká společnost.

Jaké povinnosti například vyplynou z regulace?

Povinnosti, které vyplynou ze směrnice, jsou pro některé společnosti již známými pojmy. Pro nově regulované subjekty to však nemusí platit. V následujících bodech proto uvádíme výčet těch nejdůležitějších.

- Analýza rizik a bezpečnostní politika informačních systémů
- Řešení incidentů (prevence, detekce a reakce na incidenty)
- Řízení kontinuity provozu a krizové řízení
- Bezpečnost dodavatelského řetězce, včetně bezpečnostních aspektů týkajících se vztahů mezi jednotlivými subjekty a jejich dodavateli nebo poskytovateli služeb, jako jsou poskytovatelé služeb ukládání a zpracování dat nebo řízených bezpečnostních služeb
- Zajištění nákupu, vývoje a údržby sítě a informačních systémů, včetně zveřejňování informací o zranitelnostech a o jejich řešeních
- Zásady a postupy (testování a audit) pro hodnocení účinnosti opatření pro řízení rizik v oblasti kybernetické bezpečnosti
- Používání kryptografie a šifrování
- A mnoho dalšího…

Všechny další potřebné informace o vývoji kolem NIS2 a novely zákona poskytuje obnovený portál NUKIB https://portal.nukib.gov.cz/.

Pokud si jako společnost nejste jisti svým současným stavem kybernetické bezpečnosti, je dobré nejprve vytvořit analýzu GAP nebo snímku svého současného stavu. Tento pohled poskytne firmě odrazový můstek například pro identifikaci největších problémů nebo plánování financí. Pokud jsem již doma v kybernetické bezpečnosti, mohu začít uvažovat o různých technologiích.

O jakých technologiích mohou společnosti uvažovat?

V oblasti kybernetické bezpečnosti existuje celá řada technologií a pro každou část infrastruktury se hodí jiná technologie.

EDR neboli Endpoint Detection and Response se od běžných antivirových řešení odlišuje zejména schopností logovat dění v rámci sledovaného zařízení a schopností vyhodnotit podezřelé aktivity. Bezpečnostní specialista tak získává nástroj, který mu umožňuje včas odhalit činnost útočníka a zasáhnout proti němu prostřednictvím reakce na jeho chování. EDR tedy představuje nástroj pro detekci bezpečnostních hrozeb a reakci na incidenty.

Dalším požadavkem je sběr a uchování informací z informační a komunikační infrastruktury. Ke sběru, přenosu, uchovávání těchto událostí a jejich archivaci slouží tzv. Log Management. Nástroje pro Log Management ukládají záznamy – logy ve formě strukturovaných událostí. Tím vzniká auditní stopa pro uložení a archivaci. Strukturovaný formát a možnost provádět nad takovými daty vyhledávání umožňují bezpečnostnímu analytikovi využít nástroj k pokročilé analýze potenciálního bezpečnostního incidentu. Kvalita výstupů takových analýz je závislá na kvalitě sesbíraných událostí. Tedy jedním z důležitých parametrů při výběru bezpečnostního řešení Log Managementu je úroveň kvality logování jednotlivých zdrojů logů.

Log Management umožňuje uchovávat jakékoli logové záznamy, tedy nejen z bezpečnostních technologií, ale také logy z aplikací, serverů, databází nebo koncových stanic.

Počítačová síť, servery, aplikace a jiná zařízení mohou generovat tisíce logů za vteřinu. Je proto nemožné detekovat nad těmito daty potenciální bezpečnostní události pouze pomocí manuálního procházení událostí.

Jak detekovat hrozby nad obrovským množstvím dat?

A jak detekovat pokročilé typy útoků vyžadující korelaci událostí z více zdrojů nebo bezpečnostních technologií? To je další požadavek NIS2, a to Detekce a řešení bezpečnostních událostí a incidentů.

K tomuto účelu lze využít technologie SIEM (Security Information and Event Management) a procesu bezpečnostního vyhodnocení. Ty slouží k vyhodnocování událostí v reálném čase s využitím předpřipravených korelačních pravidel. Pravidla na základě známých vzorců potenciálně nebezpečného chování detekují bezpečnostní události. Stále je však potřeba mít na paměti, že stejně jako u ostatních bezpečnostních technologií je potřeba se o obsah SIEMu starat a vytvořená pravidla ladit (výjimky a false positive) a plnit jej nejen logy, ale také kontextovými informacemi o monitorovaném prostředí a změnách, které v něm nastávají. V jiném případě se přínos technologie SIEM výrazně snižuje.

Zabezpečení komunikačních sítí je další požadavek

Proto Bezpečnostní analýza síťového provozu je dalším důležitým pilířem při snaze o zabezpečení sítě, který přidává pohled na detekci podezřelých aktivit v síti. K tomuto jsou využívány NBA (Network Behavior Analysis) nástroje, které slouží k monitoringu počítačových sítí. Základem těchto nástrojů je zaznamenávání komunikace v rámci síťové infrastruktury a její bezpečnostní analýza. Dalším vývojovým stupněm těchto nástrojů jsou tzv. NDR (Network Detection and Response) řešení, která rozšiřují funkcionalitu NBA nástrojů pro bezpečnostní monitoring sítí o možnosti automatické reakce na detekované bezpečnostní události. Typickým příkladem reakce je automatické zablokování komunikace na IP adresu, která je na seznamu nebezpečných adres, a to na základě vzájemného propojení s firewallem. Další typickým příkladem je zablokování odesílání dat při podezření na jejich únik.

Neméně důležitým faktorem je z pohledu NIS2 řešení zranitelnosti

Bez vhodného nástroje, který by detekoval zranitelnosti, nelze tuto oblast kvalitně řešit. IT je odkázáno na pravidelné studování informací o aktualizacích jednotlivých nástrojů a k jejich „slepému“ provádění. Právě z tohoto důvodu vznikly Vulnerability Management (VM) nástroje, které umožňují provádět audit prostředí, dekovat zranitelnosti, a co je nejdůležitější, pomáhají s prioritizací aktualizací na základě kritičnosti dané zranitelnosti. Vulnerability Management není jen nástroj. Jedná se o proces zahrnující detekci, analýzu, vyhodnocení a návrh správného postupu na jejich odstranění. ■

LUKÁŠ PŘIBYL, Axenta

Věděli jste, že samotný antivirus nestačí?

Ochrana koncových zařízení je základním kamenem informační bezpečnosti každé organizace. Většina firem se spoléhá na antivirus, aby chránil jejich počítače a další zařízení. To však může být vážná chyba. Dnes už totiž antivirus není schopen efektivně čelit stále sofistikovanějším moderním hrozbám.

Antivirové programy byly dlouho považovány za dostatečnou ochranu, ale útočníci neustále hledají nové způsoby, jak je obejít. Moderní hrozby, jako jsou například ransomware, pokročilé malwary nebo útoky s využitím vzdáleného přístupu, často úspěšně překonají tradiční antivirové programy.

Proč antivirus stále potřebujeme?

Odinstalace antiviru by byla špatným rozhodnutím. Neposkytuje sice plnou ochranu, ale stále plní důležitou funkci. Chrání zařízení před jednodušími hrozbami, jako jsou základní viry a malware, které útočníci stále často používají. Antivirus je sice jen základní ochrannou vrstvou, ale bez něj bychom byli vystaveni i těm nejjednodušším a nejběžnějším hrozbám.

Před čím nás antivirus neochrání?

Moderní hrozby, které antiviry nedokáží zastavit, mohou mít katastrofální důsledky. Mezi ně patří:

- Pokročilý malware: Dnes již viry nejsou hlavní hrozbou. Útočníci používají moderní a sofistikované malwary, které dokáží obejít antivirovou ochranu.
- Ransomware: Tento typ útoku může zašifrovat data a vyžadovat výkupné za jejich obnovení.
- Útoky pomocí vzdáleného přístupu: Útočník získá přístup k vašim systémům a může způsobit rozsáhlé škody.
- Krádeže dat a citlivých informací: Bez pokročilé ochrany je riziko úniku důležitých firemních nebo osobních dat velmi vysoké.

Jaké je řešení? Nasazení systému EDR

Jedním z pokročilých řešení, které organizace mohou implementovat, je EDR (Endpoint Detection and Response). Tento systém je schopen nejen detekovat hrozby, ale také reagovat na útoky v reálném čase. Jedním z doporučovaných systémů je Heimdal EDR, který nabízí ochranu proti běžným virům i pokročilým malwarům a dalším nebezpečím.

Heimdal EDR kromě detekce a reakce na hrozby také uzavírá bezpečnostní mezery v systémech, které útočníci často využívají ke kompromitaci zařízení. Díky tomu je EDR mnohem účinnější než klasický antivirus.

Náklady a složitost implementace

Nasazení EDR systému Heimdal sice není zdarma, ale cena je srovnatelná s náklady na pokročilé antivirové systémy. Co se týče složitosti implementace, není důvod se obávat. Nasazení systému zvládne pokročilý IT správce během pár hodin. Navíc je k dispozici podpora od prodejce, která pomůže s počátečním nastavením. Heimdal EDR využívá umělou inteligenci a strojové učení, takže jeho provoz je vysoce automatizovaný, což znamená, že vás nebude nutit k posílení IT týmu.

Potřeba dohledu nad bezpečností

Bezpečnostní dohled nad IT provozem je vždy doporučený, ale nasazení systému Heimdal EDR nebude tím, co rozhodne, zda budete dohled potřebovat či nikoliv. Vysoká míra jeho automatizace minimalizuje potřebu ručních zásahů. Přesto se vždy doporučuje, aby organizace zajistila průběžný dohled nad svými systémy, zejména pokud jde o větší podniky s citlivými daty.

Možnost vyzkoušení systému

Pokud si nejste jisti, zda je Heimdal EDR pro vás to pravé řešení, máte možnost systém vyzkoušet v rámci zkušebního provozu. Můžete se ozvat a dohodnout si podmínky testování, abyste měli jistotu, že bude systém ve vašem prostředí fungovat bez problémů a poskytne vám požadovanou úroveň ochrany a komfortu.

Bude Heimdal EDR dostačující i v budoucnu?

Předpovídat budoucnost bezpečnostních hrozeb je obtížné, ale Heimdal EDR je navržen tak, aby se neustále vyvíjel a přizpůsoboval novým hrozbám. Díky integraci s Threat Intelligence a schopnostem prevence proti neznámým útokům je EDR schopno reagovat nejen na současné hrozby, ale také se připravit na ty, které mohou přijít v budoucnosti.

Rozšíření ochrany pomocí XDR

Heimdal kromě EDR nabízí také rozšířenou ochranu, kterou lze nad EDR systém vrstvit, čímž vzniká tzv. **XDR (Extended Detection and Response)**. XDR nabízí další vrstvy zabezpečení, například:

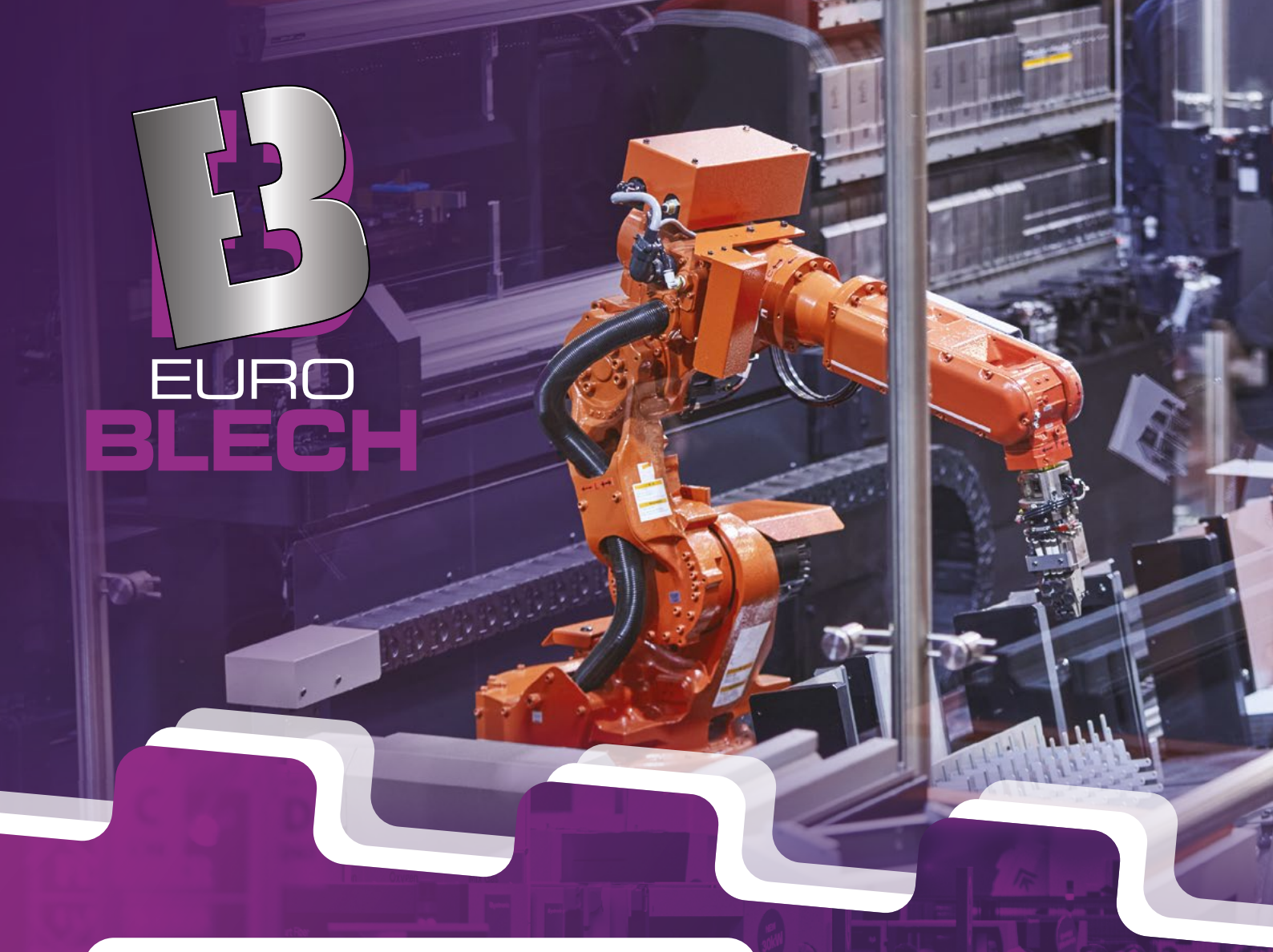
- Ochranu proti šifrování úložišť (lokálních i cloudových)
- Řízení privilegovaných účtů
- Ochranu proti podvodům typu CEO fraud a phishingovým útokům
- Spamové filtry
- Ochranu perimetru sítě

Tato flexibilita vám umožňuje systém vylepšovat podle potřeby a chránit organizaci před širším spektrem hrozeb.

Pokročilá ochrana je krok správným směrem

Zatímco antivirus stále plní svou roli základní ochrany proti jednodušším hrozbám, je zřejmé, že pro moderní a sofistikované útoky již nestačí. Nasazení systému EDR, jako je Heimdal, přináší vyšší úroveň ochrany díky schopnosti detekovat a reagovat na pokročilé hrozby. Navíc umožňuje organizacím chránit svá zařízení nejen dnes, ale i do budoucna, s možností rozšíření na systém XDR. Investice do takovéto pokročilé ochrany je krokem správným směrem, který může zachránit nejen data, ale i reputaci a budoucnost celé organizace. ■

JOSEF JAVORA, TISP



EURO BLECH

22.– 25. října 2024 | Hannover, Německo

THE POWER OF PRODUCTIVITY

Navštivte přední světovou výstavu zpracování plechu!

- >90 000 m² výstavní plochy
- Přibl. 1 500 vystavovatelů
- Prohlídky s průvodcem
- Fórum přednášejících
- Ocenění v oboru

EuroBLECH 2024 pokrývá celý technologický řetězec zpracování plechu:

Plechy, trubky, profily (železné a neželezné) • Plechové výrobky, komponenty, sestavy • Manipulace • Separace, řezání • Formování • Ohýbání plechu • Zpracování trubek / profilů • Zpracování hybridních struktur z plechu/plastů • Strojní prvky • Spojování, svařování, upevňování • Aditivní výroba • Povrchová úprava plechu • A mnoho dalšího

VÍCE INFORMACÍ VIZ

www.euroblech.com

Built by RX In the business of building businesses

NIS2: Posílení kybernetické bezpečnosti se firmy nevyhnou

NIS2 (Network and Information Systems) je nová směrnice EU v oblasti IT bezpečnosti, která míří především na ochranu kritické infrastruktury. Jejím hlavním účelem je zvýšit odolnost evropské ekonomiky proti stále sofistikovanějším kybernetickým útokům. Týká se nejen samotných podniků, ale také členů jejich dodavatelského řetězce, kteří mohou mít horší zabezpečení a tím ohrozit své obchodní partnery.

Foto: Archiv UNIKOM

Koho se směrnice týká? Předně organizací, které fungují v tzv. kritických odvětvích, jako jsou například energetické sítě, zdravotnictví, doprava, vodovodní a kanalizační sítě atd. a jejich dodavatelské řetězce. Další skupinou jsou tzv. důležitá odvětví, kam patří kupříkladu chemická výroba, potravinářství či průmyslová výroba včetně automotive, elektroniky či zdravotnických nástrojů a jejich subdodavatelé. Obecně se dotkne všech podniků ve vyjmenovaných odvětvích s více než 50 zaměstnanci či s obratem přesahujícím 50 milionů eur, v rámci celé EU tedy nejméně 160 000 subjektů.

Co NIS2 pro tyto podniky a organizace bude znamenat:

1. **Rozšířený záběr:** NIS2 rozšiřuje rozsah o více sektorů a typů entit, včetně veřejných správ a středně velkých podniků, což zahrnuje například také poskytovatele IT služeb. Ti také budou muset nově plnit přísnější bezpečnostní požadavky.
2. **Zpřísněné bezpečnostní požadavky**: Organizace musí přijmout pokročilejší bezpečnostní opatření, včetně aktivní kybernetické ochrany, nástrojů na detekci a odezvu na incidenty (EDR).
3. **Povinné hlášení incidentů**: Nová směrnice zavádí povinnost hlásit kybernetické incidenty do 24 hodin a podat závěrečnou zprávu do 1 měsíce. Neplnění této povinnosti může vést k sankcím.
4. **Vyšší odpovědnost a pokuty**: Nerespektování směrnice může vést k administrativním pokutám, k pozastavení licencí nebo k jiným sankcím.
5. **Důraz na bezpečnost dodavatelského řetězce**: Podniky, které jsou součástí technologického řetězce, musí zajistit bezpečnost svých vlastních systémů i systémů svých dodavatelských řetězců.
6. **Inovace a automatizace**: Směrnice podporuje využívání pokročilých technologií, jako jsou umělá inteligence (AI) a strojové učení (ML), které mohou pomoci při detekci a prevenci kyberútoků.
7. **Důraz na ochranu před ransomwarem**: Ransomware je identifikován jako klíčová hrozba, kterou je nutné řešit pomocí aktivních a preventivních opatření, jako je zálohování a zabezpečení systémů.
8. **Standardizace napříč EU**: Směrnice také znamená unifikaci a harmonizaci evropských standardů kybernetické bezpečnosti.

Tyto požadavky kladou zvýšené nároky na technologie IT bezpečnosti, které by organizace měly využívat ke splnění směrnice. Nechceme zahltit kompletním výčtem všech doporučených nástrojů, ale zcela jistě bude potřeba monitoring zdrojů (hardwarových, softwarových, změn), dále pak zajištění kontinuity provozu kritických IT systémů např. s pomocí technologií Disaster Recovery a nástroje pro analýzu a reporting bezpečnostních incidentů typu EDR či rozšířené detekce a reakce na incidenty (XDR).

Je nepochybné, že infrastruktura kybernetické bezpečnosti podniků a organizací bude muset být posílena. To může pro mnohé středně velké firmy znamenat značný zásah do jejich personálních stavů a finančních rozpočtů. Proto se doporučuje vedle budování vlastního zabezpečení také zvážit alternativu služeb MSP poskytovatelů, kteří umožňují splnit požadavky NIS2 bez nutnosti vysokých počátečních investic do IT. ■

ŠTĚPÁN BÍNEK, manažer prodeje cloudových řešení Acronis v ZEBRA SYSTEMS

ACRONIS EDR VE SPOLEČNOSTI UNIKOM

Akciová společnost UNIKOM Kutná Hora je podnikem působícím v oblasti Středočeského kraje. Společnost zaměstnává 250 pracovníků a je jedním z největších zaměstnavatelů na Kutnohorsku. Jako jedna z větších firem spadá UNIKOM mezi společnosti, které budou muset splňovat nároky směrnice NIS2, a to jak kvůli obratu, tak z pozice velkoobchodního dodavatele.

Společnost proto zprovoznila v rámci používané platformy Acronis Cyber Cloud balíček Acronis Advanced Security + EDR, který zahrnuje URL filtr, antivirus, anti-malware, anti-spyware, patch management a hodnocení zranitelností. Cloudové řešení pro ochranu koncových bodů poskytne nejen vyšší úroveň zabezpečení firemní infrastruktury, ale také reporty jako např. výstupy antivirových kontrol a další podklady vyžadované směrnicí NIS2.

KONFERENCE V AQUAPALACE HOTEL PRAGUE

11 konferenčních salonků a sál až pro 650 osob.

Výjimečné zážitky, které Vás spojí...

aquapalace HOTEL ★★★★ PRAGUE

aquapalacehotel.cz

ZDRAVOTNÍ POJIŠŤOVNA MINISTERSTVA VNITRA ČR 211

Bonusy 2024

až 34 000 Kč

pro zdraví vaší rodiny

více informací

Přidejte se k nám do 30. září 2024

www.211.cz