HOSPODÁŘSKÉ NOVINY

SPECIÁLNÍ PŘÍLOHA

KYBERNETICKÁ BEZPEČNOST

Regulace, kam se podíváš

Nová kyberbezpečnostní pravidla EU se budou týkat vyšších tisíců českých firem. Problémy s jejich naplněním mohou mít hlavně malé podniky.

Kyberútoky jsou díky AI rychlejší

A protireakce musí být okamžitá, přitom systémy zastarávají mnohem rychleji, říká Ondřej Koutský z firmy BitServis.

▸ **Nové směrnice**

Adam Mašek
adam.masek@hn.cz

Rozsáhlý regulační proces z EU v Česku zasáhne tisíce nepřipravených firem

Firmy i státní instituce v Česku se musí v posledních letech stále ve větší míře vypořádávat s hrozbou kybernetických útoků. Jejich počet se významně zvýšil zejména během covidových let 2020 a 2021, kdy se masivně zrychlila digitalizace soukromého i veřejného sektoru. Tento trend ještě více posílilo vypuknutí války na Ukrajině na počátku roku 2022, kdy se následně Západ musel kolektivně obrnit proti zvýšené aktivitě proruských či přímo ruských hackerských skupin.

Zvýšený počet kyberútoků potvrzují i aktuální čísla Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Ten v říjnu zaznamenal 47 incidentů, což je nejvyšší měsíční hodnota za celou dobu evidence. Tři z nich byly klasifikovány jako významné, zbylých 44 bylo méně významných. Ve většině případů šlo o takzvané DDoS útoky, jejichž cílem je zahlcení vybraných serverů velkým množstvím požadavků, což vede k jejich vyřazení. Došlo též k evidenci devíti ransomwarových útoků – i to je rekordní počet za jeden měsíc. Ransomware je škodlivý program blokující počítačový systém nebo šifrující data v něm zapsaná. Útočníci pro odblokování většinou požadují výkupné.

Státy EU včetně Česka nárůst kyberútoků s postupující digitalizací odhadovaly. I proto na konci roku 2020 představily strategii s názvem EU Cyber Security Strategy for the Digital Decade (volně přeloženo jako Strategie EU v oblasti kybernetické bezpečnosti pro digitální dekádu). A v jejím rámci postupně schvalují nové regulace s cílem výrazně zvýšit úroveň kybernetické bezpečnosti na jednotném trhu.

„Tyto regulace představují pro evropské firmy a instituce významnou výzvu, ale zároveň i příležitost ke zvýšení své odolnosti vůči stále sofistikovanějším kyberhrozbám," říká Jan Pich, kyberbezpečnostní manažer oddělení technologického consultingu a IT ve společnosti EY Česká republika.

NIS2 a co dál?

Nejdiskutovanější v posledním roce je směrnice NIS2. Ta rozšiřuje a zpřísňuje požadavky na kyberbezpečnost v klíčových sektorech, jako je energetika, doprava, zdravotnictví či finanční služby. Pro firmy a státní instituce mimo jiné zavádí povinnost hlásit incidenty a současně je nutí k přijímání opatření, jež povedou k minimalizaci dopadů kyberútoků a také zvýšené prevenci.

To ale není zdaleka jediná regulace. Velmi podobnou směrnicí, která stejně jako NIS2 nabyla účinnosti loni v lednu, je i CER (Critical Entities Resilience). Ta se zaměřuje konkrétně na subjekty kritické infrastruktury – například v oblasti energetiky, dopravy či zdravotnictví – a také má za cíl je zrobustnit tak, aby případné útoky měly jen minimální dopad na chod celé společnosti. Tyto subjekty by měly být odolnější vůči hrozbám souvisejícím nejen s kybernetikou, ale i s přírodními riziky, teroristickými a hybridními útoky či různými druhy sabotáží.

NIS2 i CER jsou směrnicemi, což znamená, že členské státy mají povinnost transponovat požadavky z nich vyplývající do svých vlastních právních řádů. „Čas na transpozici obou směrnic byl do poloviny letošního října, přičemž tento termín nebyl dodržen. To ale není výjimečný stav, podobně je tomu ve velké části dalších států EU," říká Eliška Kühnerová, expertka na kyberbezpečnost v poradenské společnosti KPMG.

Zatímco NIS2 je v Česku transponována prostřednictvím zákona o kybernetické bezpečnosti, jehož finální podobu nyní projednávají poslanci, požadavky vyplývající z CER budou promítnuty do nového zákona o odolnosti subjektů kritické infrastruktury a jeho zněním se parlament bude teprve zabývat.

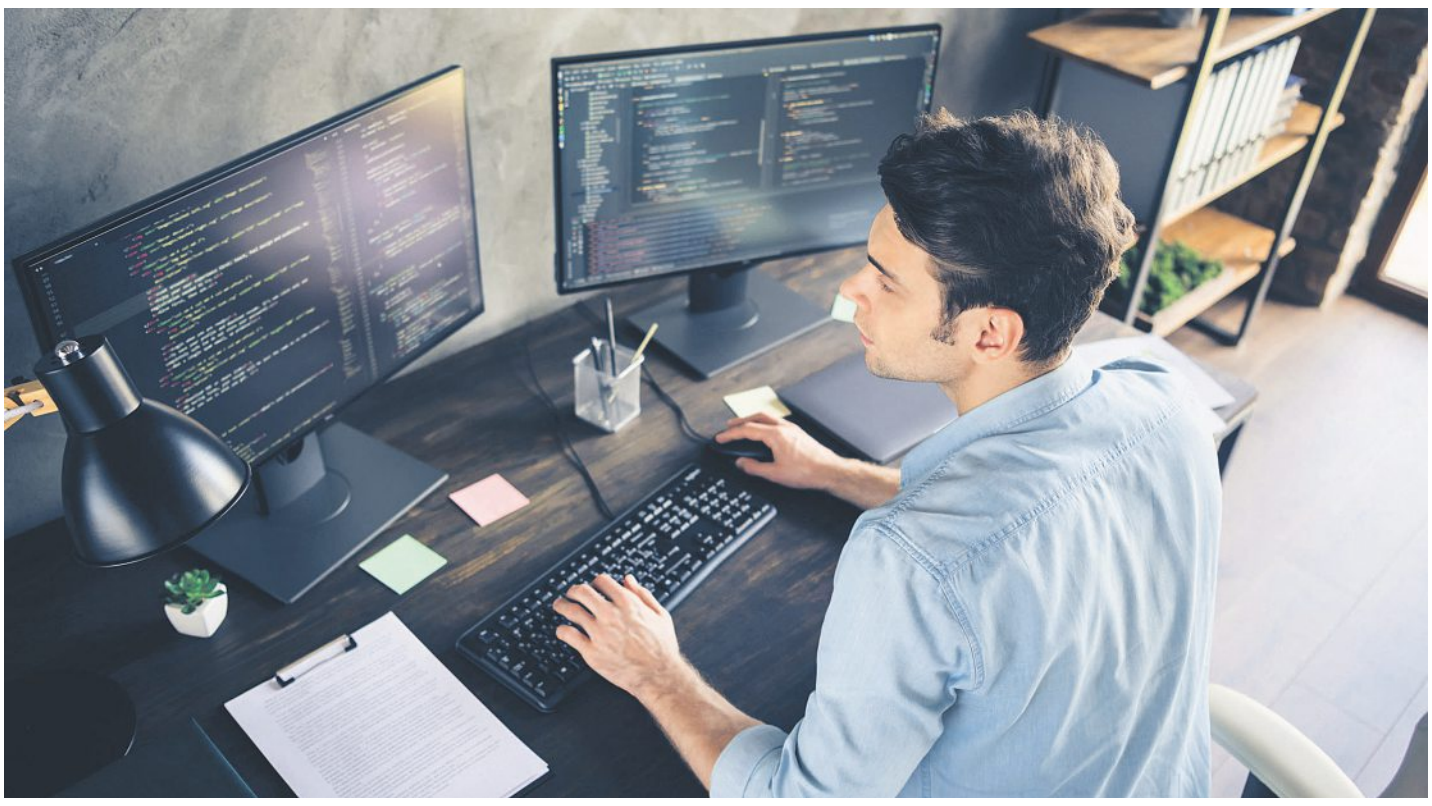
Kromě směrnic i nařízení

EU však postupně zavádí i další právní normy, takzvaná nařízení. Ta mají obecnou působnost a na rozdíl od směrnic nevyžadují přímou implementaci do legislativy členských států. Jsou tedy přímo použitelné v celém svém rozsahu.

Takovým nařízením je například DORA (Digital Operational Resilience Act). Zaměřuje se na kybernetickou odolnost speciálně pro firmy ve finančním sektoru. Banky, pojišťovny anebo investiční společnosti budou muset zavést robustní systémy pro řízení incidentů, pravidelně provádět stresové testy a zajistit kontinuitu svých služeb. Obdobně jako u NIS2 budou požadavky dopadat přeneseně i na dodavatele ICT a IT služeb těchto finančních subjektů. Nařízení je účinné od půlky ledna příštího roku a v Česku je součástí zákona o digitalizaci finančního trhu. Dohledovým orgánem nad dodržováním pravidel bude Česká národní banka.

Poslední z velkých regulací, které budou mít v nejbližších letech výrazný dopad na fungování evropských firem včetně těch českých, je nařízení s názvem Cyber Resilience Act (CRA). To se týká širokého spektra podniků a stanovuje požadavky na kybernetickou odolnost produktů a služeb, které tyto společnosti vyrábějí. Cílem je zajistit, aby byly navrženy a vyvíjeny s ohledem na bezpečnost koncových uživatelů. To bude mít dopad nejen na výrobce, ale i na dodavatele a distributory.

V praxi to znamená, že například výrobce chytrých mobilních telefonů bude muset před jejich uvedením na trh v EU zajistit jejich vyšší kybernetické zabezpečení. Výrobci pak za nižší zranitelnost výrobku zůstanou odpovědní po celý životní cyklus produktu. „Toto nařízení je zaměřeno zejména na ochranu koncového spotřebitele," říká Kühnerová.



Odborníci jsou problém. *Ne každá firma si bude moci dovolit mít vlastní oddělení, byť jen s pár lidmi věnujícími se kyberbezpečnosti. Zbytek, hlavně z řad malých a středních firem, bude muset minimálně část svých služeb outsourcovat.* **Foto: Shutterstock**

~ Zásadní změna nastane u menších firem, které s regulací kyberbezpečnosti nemají zkušenosti.

Brzdí firmy regulace, anebo pomáhá?

Z výše uvedeného výčtu je jasné, že půjde o masivní regulační proces, který pouze v Česku dopadne na vyšší jednotky tisíc firem. Ty největší a nejdůležitější z nich pak může zavádění opatření stát i stovky milionů korun. Paradoxně ale právě tyto podniky budou mít se zaváděním nejméně problémů. Zaprvé díky svým rozpočtům a pak také proto, že už některým standardům z dřívějška vyhovují.

Nejzásadnější změna tak nastane u menších firem, které s regulací v kyberbezpečnosti nemají žádné anebo jen minimální zkušenosti. „Je to jako rozjet těžký vlak – zrychlit z 60 na 100 km/h je snazší než z nuly," přirovnává Pich z EY.

„Pro banku nebo velký moderní podnik budou nové regulace komplikací spíše provozního charakteru. Pro firmu, která kyberbezpečnost neřešila, to může být dohánění i 10 nebo 20 let technologického dluhu. A to navíc bez strategické vize a směru, kde začít a kudy se na této cestě vydat," souhlasí Petr Špiřík, partner pro kybernetickou bezpečnost v poradenské společnosti PwC.

Společným problémem pro obě skupiny je pak dlouhodobý nedostatek odborníků v této oblasti na trhu. Zde opět platí, že zdaleka ne každá firma si bude moci dovolit mít vlastní oddělení, byť jen s pár lidmi věnujícími se kyberbezpečnosti. I v tomto ohledu budou mít větší výhody korporáty a velké firmy, které budou schopné ostatní přeplatit. Zbytek, hlavně z řad malých a středních firem, bude muset minimálně část svých služeb outsourcovat specializovaným společnostem.

Podniky budou muset také mnohem více investovat do vzdělávání svých zaměstnanců, kteří stále zůstávají nejzranitelnějším bodem v obraně proti kyberútokům. Oslovení experti i přes tyto náročnosti vidí kroky EU v oblasti regulace kyberbezpečnosti spíše jako pozitivní. Jednoduše proto, že kdyby nové právní normy nepřicházely, řada firem by toto odvětví ve svých provozech podceňovala. „Z našich průzkumů vidíme, že více než 90 procent zvýšené pozornosti a reálných investic do kybernetické bezpečnosti je u firem taženo právě regulatorikou," říká Špiřík.

To na jednu stranu může přispívat ke konkurenceschopnosti firem EU vůči ostatním trhům. Na druhou stranu to vznáší otázku, zdali v unii soukromý sektor nečelí přílišné přeregulovanosti. „Vnímám to jako palčivý problém. Protože tyto masivní investice znemožní firmám použít peníze na další investice do primárního byznysu a rozvoje. Přeregulovanost navíc vede i k určité mentální únavě. Příliš často v podnicích slyším rezignovaným hlasem pronést, že manažeři a majitelé chtějí dělat věci správně, ale předpisů už je tolik, že mají pocit, že jen plní nové regulace," upozorňuje Špiřík.

Příloha: Kybernetická bezpečnost
• **Ředitel speciálních projektů** Aleš Mohout • **Editor** Ján Chovanec • **Grafika a zlom** Vizuální studio Economia • **Obchod a inzerce** Daniel Hort (daniel.hort@economia.cz)
partnerské logo: FORTINET

Safee

HN064135

Kyberútoky jsou realita a firmy nejsou připravené

V dnešní době se útočníci vzhledem k automatizovaným řešením a množství dostupných informací již nezaměřují jen na velké firmy a korporace jako v minulosti, ale ve střehu musí být i střední a malé organizace.

Nezáleží na oboru podnikání nebo velikosti firmy, kyberútoky míří na společnosti každý den. „I přesto ale není ochrana proti nim ve firmách stále dostatečná," říká Petr Kacálek, zakladatel společnosti Safee, poskytující služby v oblasti kyberbezpečnosti. „Nejenže není dostatečná, ale řada firem to vůbec neřeší. Když při kyberútoku ztratí veškerá data, stojí často na prahu vlastní existence. Teprve tehdy nás žádají o pomoc," doplňuje druhý ze zakladatelů Lukáš Skála.

Jaké hrozby aktuálně u firem řešíte?

P. K.: Největší hrozbou jsou asi ransomware útoky, kdy vám útočníci zašifrují data a tím ochromí celé vaše podnikání. Dále to mohou být špatně zabezpečené cloudové služby, webové aplikace, IoT řešení nebo DDoS útoky, které zahltí servery tak, že se stanou nedostupnými pro uživatele.

L. S.: Samostatnou kapitolou jsou zaměstnanci, sociálním inženýrstvím a phishingem na ně útočníci míří pomocí personalizovaných podvodných e-mailů. Jejich hlavním cílem je získat přístupové údaje. Dále to jsou také hrozby zevnitř organizace, ať už úmyslné, nebo neúmyslné, pocházející od zaměstnanců či jiných lidí s přístupem k systémům firmy.

Jak takový ransomware útok vypadá?

P. K.: Útočník často získá přístup do systému pomocí podvodného e-mailu a následně zašifruje data oběti. Někdy je to sám hacker, jindy pouze ransomware nebo oba naráz. Poté požaduje výkupné. S přibývajícími útoky v poslední době se ale stává, že cíl nemusí být nutně výkupné, útočníkovi stačí paralyzování nebo kompromitace firmy.

Jak by měla firma při útoku nejlépe postupovat?

P. K.: Nepanikařit. Při výzvě o zaplacení výkupného neplatit. Firma musí co nejrychleji ohrožené systémy vypnout a rychle kontaktovat odbornou pomoc, která pomůže s izolací nákazy. Když do firmy dorazí náš tým kybernetické pohotovosti, panuje většinou chaos. Zásah obvykle začínáme s identifikací typu ransomwaru.

Zakladatelé společnosti Safee Lukáš Skála a Petr Kacálek. Zdroj: HN – Honza Mudra

Data lze někdy dešifrovat bez zaplacení, ale to je spíše výjimka. Pokud jsou k dispozici aktuální zálohy, použijí se k obnovení dat po odstranění ransomwaru. Po vyřešení incidentu je nezbytné provést audit bezpečnosti. Identifikovat slabiny a provést kroky k jejich odstranění, například nasazením lepší ochrany proti phishingu nebo posílením zabezpečení sítě a serverů. Pokud se poškozená firma rozhodne zaplatit, měla by myslet na to, kde peníze končí. Stává se také, že oběť zaplatí, ale nic nedostane.

Nejlepším řešením je samozřejmě kybernetickým hrozbám předcházet. Co tedy doporučujete?

L. S.: Kybernetickou bezpečnost je dobré řešit komplexně. Začněme u zaměstnanců, každá firma, malá i velká, by měla řešit jejich školení, aby byli schopni včas rozpoznat rizika a reagovat na ně. V Safee pro firmy v rámci školení realizujeme rovnou i phishingové kampaně, tzn. simulujeme reálné útoky na jejich e-maily, takže během školení pracujeme s reálnými výsledky dané firmy. Nyní navíc může skoro každá firma využít 100procentní příspěvek na tuto aktivitu v rámci programu NPO – DIGI pro firmu, to je skvělé. Další řešení je poplatné velikosti firmy, od základů, jako je vícefaktorová autentizace pro přihlašování, přes ochranu koncových zařízení, firewall, bezpečné zálohy dat, penetrační testy webových aplikací až pro připojení na bezpečnostní dohledové centrum. U větších firem se samozřejmě začíná auditem kybernetické bezpečnosti, u těch menších doporučujeme alespoň základní analýzu aktuálního stavu.

■ Debata HN

Poradit se, zálohovat, hlásit incidenty. Experti radí, jak se připravit na NIS2

Anežka Hesová
anezka.hesova@economia.cz

Evropská unie vyrazila do boje proti kybernetickým útokům a chystá se uvést do praxe sérii nařízení zaměřených na digitální bezpečnost firem, úřadů a institucí. Česko se aktuálně připravuje především na implementaci směrnice NIS2, která má novelizovat aktuálně platný zákon o kybernetické bezpečnosti. Už teď je zřejmé, že její plánované schválení do konce letošního roku se nestihne, pravděpodobnější termín přijetí je polovina roku 2025. To ale neznamená, že by se organizace neměly na novou regulaci připravovat už teď.

O tom, co budou nová pravidla obnášet a koho se budou týkat, přišli do studia Hospodářských novin debatovat odborníci na legislativu a kyberbezpečnost. „Zákon se velmi dotýká například telefonních operátorů, kteří mají být více regulovaní. V návrhu se objevují sporné body týkající se toho, zda budou mít povoleno nebo zakázáno přijímat zboží od konkrétních výrobců," vysvětlil průtahy v projednávání zákona Radim Trávníček, espoluzakladatel společnosti BeSecured zaměřené na informační a kybernetickou bezpečnost.

Děláme si to přísnější, než je potřeba?

Tlak na zmírnění požadavků na prověřování dodavatelského řetězce přichází také ze strany Hospodářské komory. Někteří kritici se obávají takzvaného gold-platingu, tedy toho, že si evropskou směrnici v rámci její implementace do českého právního prostředí zbytečně zpřísňujeme a snižujeme tím konkurenceschopnost tuzemských firem.

Experti ale oponují, že už je běžnou praxí, že se prověřuje, zda některé produkty typicky z Číny neohrožují bezpečnost. „Například ve Spojených státech jsou tyto mechanismy naprosto běžné. V porovnání s právní úpravou v zahraničí jsou naše navrhované požadavky spíše mírné," dodal k připravované novele zákona Jiří Císek, řídící partner advokátní kanceláře Cisek.

Bezpečnostní opatření v oblasti informačních technologií navíc bude po firmách požadovat nejen legislativa, ale i vývoj trhu a mezinárodní standardy. „Firma, která v současné době neřeší svou kyberbezpečnost, vlastně nemá zájem udržet se na trhu a přežít," shrnul to Vladimír Kaděra, senior specialista kybernetické bezpečnosti ve společnosti ATS-Telcom Praha.

Spíš než zákon pud sebezáchovy

Oproti současné právní úpravě se NIS 2 bude vztahovat k většímu množství organizací. „Myslím, že se regulace bude přímo týkat zhruba deseti tisíc českých společností," odhadl Trávníček. Kritériem přitom není jen velikost firmy, ale také odvětví, ve kterém působí. Podle účastníků debaty podniky často vůbec nevědí, zda se jich nová pravidla budou týkat. „Firmy by si měly udělat sebeidentifikaci, ideálně k tomu pozvat nějakého konzultanta," doporučil Císek s tím, že v kritériích zařazení jednotlivých firem do příslušných kategorií jsou i skryté nuance. „Může jít například o fotovoltaiku. Firma si vyhodnotí, že regulovaným subjektem není, jenže má na svém výrobním závodě solární panely, pro které si musela vyřídit licenci energetického regulačního úřadu. A rázem se může stát regulovaným subjektem v oblasti energetiky, i když to není její hlavní byznys," uvedl jako příklad.

Orientačně si tuto sebeidentifikaci mohou firmy ověřit na webu Národního ústavu pro kybernetickou bezpečnost, kde je k tomu vytvořena online kalkulačka. Zda se na firmu budou, nebo nebudou vztahovat nová pravidla, ale není v debatě o zabezpečení rozhodující. „Firmy, které v určitém rozsahu provozují IT, by se měly zabývat kybernetickou bezpečností bez ohledu na to, zda podle zákona jsou, nebo nejsou regulovanou organizací. Měly by to dělat z pudu sebezáchovy," připomněl Kaděra.

Nemusí přitom jít o drakonická nebo předražená opatření, spíše se jedná o revizi základních mechanismů, které by měly být nastavené adekvátně k případným rizikům. „U řízení rizik to prakticky začíná," popsal doporučený postup Trávníček. „Firma musí vědět, s jakými daty pracuje, jaké má technologie, kde jsou jaké hrozby."

Podle toho si pak firma sestaví plán a nastaví systém zálohování. „Potom je potřeba ty škodlivé situace vyhledávat. Hlásit incidenty, vzdělávat lidi, aby události nahlašovali," zdůraznil Trávníček. „Když daná společnost usoudí, že základní pravidla dodržuje a bezpečnost má dobře nastavenou, tak by si to měla zdokumentovat, aby se při výměně lidí neztratilo know-how," doplnil další doporučení Kaděra. Důležitá je podle obou expertů také podpora vedení. Kyberbezpečnost by ve velkých společnostech neměl mít na starosti řadový IT pracovník, ale manažer, který dokáže vnést do celé organizace bezpečnostní kulturu.

Podle odborných odhadů je většina firem v Česku na relativně dobré kyberbezpečnostní úrovni. „Často jsou v zabezpečení i dál, než to požaduje chystaný zákon. Jenom to třeba nemají zdokumentované," poznamenal Císek. Podle jeho zkušeností takovým firmám prospěje počáteční konzultace s odborníkem, který jim poradí, jak si stanovit rozsah řízení, a může je také odradit od nákupu zbytečně drahých a nepotřebných řešení.

Účastníci debaty se shodli na tom, že obavy z chystané novely zákona nejsou namístě. Bezpečnostní kritéria definovaná tímto zákonem mohou být naopak užitečným standardem pro hodnocení konkrétních opatření a motivací pro firmy i veřejné instituce, aby se ochraně svých dat a informačních systémů věnovaly i z jiných než legislativních důvodů.

Radim Trávníček
spoluzakladatel, BeSecured

Jiří Císek
řídící partner, AK Cisek

Vladimír Kaděra
specialista kyberbezpečnosti, ATS-Telcom Praha

Foto: Lukáš Bíba

V zahraničí je prověřování bezpečnosti dodavatelských řetězců běžné.
Jiří Císek, AK Cisek

Odhaduji, že regulace se bude přímo týkat v Česku zhruba deseti tisíc společností.
Radim Trávníček, BeSecured

Kybernetickou bezpečností by se firmy měly zabývat bez ohledu na připravovaný zákon.
Vladimír Kaděra, ATS-Telcom

Fortinet

HN064140

Kybernetická rizika se stávají obchodními riziky a ohrožují podnikání

Kybernetická rizika jsou zároveň podnikatelská rizika. Cokoliv, co ohrožuje informační technologie, ohrožuje firmu. Stali jsme se extrémně závislí na našich digitálních aktivech a v důsledku toho si vedoucí pracovníci firem musí uvědomit rozsáhlost změn. Jak do toho zapadá pozice manažerů pro informační bezpečnost?

Zřejmě nejzásadnější úlohou manažerů pro informační bezpečnost (CISO) je řadit kybernetická rizika podle skutečného dopadu. „To vyžaduje stejnou míru porozumění byznysu a technologiím, ale i smysl pro to, jak se při útoku chovají objekty, které nikdy nebyly navrženy jako bezpečné. Není to snadný úkol, a to nejen z technologických důvodů. Součástí tohoto hodnocení je nutnost pochopení priorit uvnitř hodnotového řetězce organizace a jejich odpovídajícího zabezpečení," vysvětluje Ondřej Šťáhlavský, regionální ředitel společnosti Fortinet pro střední a východní Evropu.

Druhým úkolem je podívat se mimo organizaci a zjistit, jak ji mohou ovlivnit vnější síly. „Nové zákony a předpisy jsou nezbytné – chrání lidi, duševní vlastnictví a schopnost vynalézat a inovovat. Z tohoto pohledu jsou požadavky na compliance dobré. Jejich nároky se ale denně zvyšují," říká Ondřej Šťáhlavský.

Právě tato dualita, dobrá a složitá, je výzvou pro mnohá IT oddělení. Musí být schopni začlenit právní aspekty do toho, co dříve bylo čistě technologickým bojištěm. Více než kdy jindy je tak dnes klíčové, aby se management riziky kybernetické bezpečnosti zabýval. V minulosti byla odolnost spíše technickým konceptem, dnes je to požadavek zákonný. Vše by mělo být podloženo čtyřmi typy přístupů:

• **Prioritní obnova:** Jakkoli je obtížné pořadí kybernetických rizik stanovit, jedná se o skutečně jedinečný způsob, jak propojit manažery pro informační bezpečnost a tým s byznysem firmy.

Nové zákony o IT jsou nezbytné. Mají chránit lidi, duševní vlastnictví a schopnost vynalézat a inovovat, říká Ondřej Šťáhlavský. Zdroj: Fortinet

• **Obranné strategie:** Méně je v tomto případě více. Po letech neřízeného rozrůstání bezpečnostní infrastruktury si kybernetičtí specialisté uvědomili, že velká změť produktů a dodavatelů není příliš efektivní. Příští éra bezpečnosti se bude odehrávat prostřednictvím konvergence, nikoli dalším přidáváním.

• **Možnosti nabídky:** Součástí práce manažera pro informační bezpečnost je nabízet scénáře jako řadu zdokumentovaných kroků: investice, harmonogram, přínosy a rizika. Může navrhnout i posloupnost jednotlivých kroků. Výběr postupu je ale úkolem vedení organizace.

• **Výkonné vedení:** Manažer pro informační bezpečnost se musí zodpovídat přímo generálnímu řediteli. V sázce je totiž přežití celé společnosti.

„Kybernetická bezpečnost není pouze o vyhýbání se ledovcům. Množství technologií, dodavatelů, procesů a rozsah digitálních transformací volají po zjednodušení. Příliš často se tento chaos mění ve velké incidenty, které fungují jako budíček. Pak se nejedná o jeden milion, který jsme neutratili, ale o 100 milionů, o které jsme právě přišli," uzavírá Ondřej Šťáhlavský.

Neznalost kyberbezpečnosti u zaměstnanců meziročně vzrostla

Nový výzkum společnosti Fortinet, světového lídra v oblasti kybernetické bezpečnosti, ukazuje souvislost mezi zvýšenou informovaností o kybernetických hrozbách v rámci společnosti a snížením jejich rizik. Klíčovou roli přitom mají kyberneticky zdatní zaměstnanci.

„Hackeři využívají nové technologie, jako je umělá inteligence, ke zvýšení sofistikovanosti svých útoků. Je tedy stále důležitější, aby zaměstnanci sloužili jako robustní první linie obrany. Nový výzkum zdůrazňuje důležitost kybernetické ochrany a zavádění bezpečnostního povědomí a školení v rámci celé organizace. Například v našem regionu je 96 procent manažerů přesvědčeno, že by zvýšení povědomí o bezpečnosti pomohlo snížit počet kybernetických útoků," říká Ondřej Šťáhlavský, regionální ředitel společnosti Fortinet pro střední a východní Evropu.

Manažeři se domnívají, že hrozby budou pro jejich zaměstnance obtížněji rozpoznatelné, jelikož útočníci využívají umělou inteligenci (AI) ke zvýšení objemu a rychlosti svých útoků. „Konkrétně v našem regionu je dobře vidět, jak naplno do oblasti kyberbezpečnosti umělá inteligence proniká. 92 procent společností využívá, implementuje nebo zkoumá řešení využívající umělou inteligenci, aby zabránily kyberútokům. A 61 procent manažerů zase očekává, že se naopak zaměstnanci stanou obětí útoků, při nichž kyberzločinci používají umělou inteligenci," říká Šťáhlavský.

„Navzdory všem těmto obavám ale 37 procent organizací neřídí ani nesleduje, jak zaměstnanci používají aplikace, které umělou inteligenci využívají," doplňuje Šťáhlavský. Dobrou zprávou však je, že většina respondentů (80 procent) také tvrdí, že celopodnikové znalosti o útocích využívajících AI přiměly jejich organizace k větší podpoře zavádění bezpečnostních školení.

Zaměstnanci mohou být v první linii ochrany společnosti, ale vedoucí pracovníci se stále více obávají, že pracovníci nemají dostatečné povědomí o bezpečnosti. Téměř 70 procent dotázaných se domnívá, že jejich zaměstnancům chybí kritické znalosti v oblasti kybernetické bezpečnosti, přičemž v roce 2023 to bylo 56 procent.

Koncoví uživatelé dle výzkumu zůstávají atraktivním cílem. Více než 80 procent organizací čelilo v loňském roce útokům, jako je malware, phishing a útoky na hesla, které byly přímo zaměřeny na jednotlivce. S vývojem útoků bude povědomí o bezpečnosti a školení stále důležitější. Téměř všichni (96 procent) dotázaní tvrdí, že jejich vedoucí tým podporuje školení zaměstnanců v oblasti bezpečnostního povědomí. Téměř všichni respondenti (98 procent) uvádějí, že prevence phishingu je součástí jejich školicích programů a plánů. Mezi další hlavní priority školení patří bezpečnost dat (48 procent) a ochrana soukromí (41 procent).

Povědomí o kyberbezpečnosti Vedoucí pracovníci se stále více obávají, že jejich podřízení nemají dostatečné povědomí o bezpečnosti v IT. Zdroj: Fortinet

Vzdělávání zaměstnanců v oblasti kyberbezpečnosti je klíčové, Fortinet chce zaškolit milion lidí.

Prostředí kybernetické bezpečnosti se stává stále složitějším, poptávka po kvalifikovaných zaměstnancích stále roste a odhaduje se, že k řešení nedostatku pracovních sil v tomto odvětví je celosvětově zapotřebí 4,8 milionu odborníků. Přístup společnosti Fortinet k tomuto problému odhaluje Ondřej Šťáhlavský, její regionální ředitel pro střední a východní Evropu.

Jak se do řešení tohoto problému Fortinet zapojil?

• Fortinet řeší nedostatek kvalifikovaných lidí napříč společností tak, že nabízí oceněné vzdělávací a certifikační osnovy, které mají jednotlivce vybavit potřebnými dovednostmi a znalostmi k efektivnějšímu zmírnění kybernetických rizik. Zavázali jsme se, že do konce roku 2026 vyškolíme v oblasti kybernetické bezpečnosti na celém světě jeden milion lidí. Zatím jich našimi školeními prošlo více než půl milionu, takže jsme na dobré cestě tento závazek splnit.

Jak je to s běžnými zaměstnanci firem a institucí?

• Zatímco bezpečnostní a IT týmy jsou klíčové pro ochranu organizací před kybernetickými hrozbami, důležitou roli v prevenci narušení hrají také zaměstnanci podniku. Ti mohou sloužit jako silná první linie obrany proti kyberútokům. Naštěstí pracovníci jsou zvyšování povědomí o kybernetické bezpečnosti a školením na toto téma otevření.

▸ Rozhovor

Ján Chovanec
jan.chovanec@economia.cz

Vidím jako velký problém, že chybí definitivní podoba zákona o kyberbezpečnosti

Několik tisíc českých firem čeká v následujících měsících příprava na pravidla ochrany před elektronickými útoky. Tato nová evropská regulace vzniká na základě unijní směrnice označované jako NIS2. Lidé z kyberbezpečnostní branže proto pozorně sledují, jak zákonodárci směrnici začlení do vznikajícího zákona o kybernetické bezpečnosti. O jeho konkrétní podobě se právě v těchto týdnech svádí boj v Poslanecké sněmovně.

IT firma Bit Servis, sídlící v pražské Libuši, pomáhá svým zákazníkům budovat odolnou digitální infrastrukturu. Poskytuje analýzy bezpečnosti těchto systémů a pomáhá firmám například i s přípravou na požadavky nového zákona.

Ondřej Koutský, odborník na kyberbezpečnost, jednatel a spolumajitel Bit Servisu, připravovaná jednotná pravidla ochrany vítá. Podle něj je zásadní změnou, že nový zákon učiní jednatele a topmanažery firem zodpovědnými za bezpečnost elektronických systémů. „Pokud své nové povinnosti nebudou plnit, nejednají s péčí řádného hospodáře a může se stát, že třeba výkupné v případě ransomwaru budou platit ze své kapsy. To je výrazný posun proti stávající situaci, kdy kyberbezpečnost není zákonem stanovená," říká Koutský.

Máme dnes přesný obrázek toho, co se v kyberprostoru děje? Statistika Národního úřadu pro informační a kybernetickou bezpečnost (NÚKIB) hlásí desítky „incidentů" měsíčně, ale úřad sám přiznává, že to jsou jen ty větší a nahlášené případy. Jaký je váš pohled na situaci?
Existují veřejně dostupné webové stránky a samozřejmě i jiné zdroje, které útoky online monitorují. Je tam vidět, že to rozhodně není dvacet případů za měsíc, spíše dvě stě za den. Všichni naši partneři říkají, že útoků přibývá a jsou sofistikovanější. U našich klientů řešíme nějakou formu útoku prakticky každý den. Je ovšem nutné zmínit, že NÚKIB eviduje pouze ty incidenty, které mu byly nahlášeny podle stávajícího zákona, tedy zdaleka ne vše.

Data jsou dnes skutečně jednou z nejdůležitějších komodit. Ochromit konkurenci elektronickou cestou nedá mnoho práce a lze tak způsobit opravdu velké škody. A to pomíjím útoky kvůli výpalnému. V souvislosti s napjatou geopolitickou situací také narostly útoky na orgány státní správy a místních samospráv.

Odborníci poukazují i na fakt, že dnes jsou někteří útočníci placeni nepřátelskými státy s velkými rozpočty…
Z praxe je vidět, že téměř jakýkoli systém lze nabourat. Jde jen o to, kolik má útočník času a peněz. A to, že někteří z nich mají hodně peněz a dalších zdrojů, je realita. Proto je třeba postavit bezpečnostní systém tak, aby aktiva co nejvíce chránil. Klíčové je také dokázat zmírnit dopady případného úspěšného narušení.

Jak by měla firma nebo instituce o kyberbezpečnostních opatřeních rámcově uvažovat? Co klientům na úvod radíte?
Na začátku si musíte definovat aktiva, jejich důležitost, a provést analýzu rizik. A pak kolik do ochrany hodlají investovat a proč. Investice může být velká a chránit toho víc, nebo si lze říci, která aktiva maximální ochranu nepotřebují a která si můžete dovolit na nějakou dobu ztratit. My nabízíme klientovi na úvod analýzu označovanou jako GAP, aby bylo jasné, jak na tom s kyberbezpečností je, ať již vůči návrhu nového zákona nebo jiné normě. Od výsledků se pak může odrazit při dalším postupu.

Některé systémy, například výrobní nebo zdravotnické, je nejlepší úplně odříznout od okolního světa. Pak ale zase nemůžete počítat s rychlou dostupností z internetu. Musíte také zajistit, že k vašemu zařízení fyzicky nikoho nepustíte. Je to o vybalancování adekvátní ochrany a takových opatření, aby se v systému ještě dalo efektivně pracovat.

V oboru kyberbezpečnosti sehrává hlavní roli překotný rozvoj technologií, zejména nástup umělé inteligence (AI). Jak se AI už nyní projevuje?
Dnes je AI zabudovaná do mnoha bezpečnostních nástrojů. My ji také využíváme při návrzích různých technických řešení a pro následnou implementaci. Role umělé inteligence je asi nejdůležitější ve vyhodnocování provozu v síti a v řízení superrychlé reakce na nastalé hrozby. Ale používá ji v obrovské míře i nepřátelská strana. Je to cítit například na rostoucích počtech útoků.

AI všechno zrychlila. Reakce jsou dnes mnohem rychlejší a protireakce musí být srovnatelně rychlá. A systémy zastarávají mnohem rychleji. Jak hardware, tak software.

Velkým tématem je zmíněná směrnice NIS2 a její přetavení do českého prostředí, konkrétně do nového zákona o kybernetické bezpečnosti. Potřebujeme přísnější pravidla, jaká prosazuje Evropská unie?
Ano, jsou jednoznačně třeba. Jedním z důvodů je geopolitická situace a fakt, že počet útoků stoupá a jsou stále sofistikovanější. Důležitým prvkem NIS2 je vzájemná spolupráce mezi evropskými státy, jež dosud nebyla tak propracovaná. Směrnice řeší to, aby úroveň kyberbezpečnosti byla napříč unií stejná a samozřejmě vyšší, než je nyní.

Někdo může namítnout, že ani nemůžete mluvit jinak, protože nová pravidla budou pro vaši firmu byznysem. Tisíce organizací se na nová pravidla musí připravit a budou potřebovat pomoc…
Moje odpověď zní, že zároveň jsme to my, kdo pak řeší následky kyberútoků u našich zákazníků. Podle informací, které prezentuje NÚKIB, je průměrná škoda způsobená jedním úspěšným kybernetickým útokem 90 milionů korun. Pokud toto společnosti považují za přijatelné riziko, tak O. K.

Nové povinnosti byly už několikrát v médiích zmiňovány: bezpečnostní audity, dedikovaní manažeři, proškolování zaměstnanců a řada technických požadavků. Co z toho je to nejpodstatnější?
Hlavní nová věc, kterou to přinese, je větší odpovědnost za kybernetickou bezpečnost na straně vedoucích pracovníků – jednatelů a členů představenstev. Pokud své nové povinnosti nebudou plnit, nejednají s péčí řádného hospodáře a může se stát, že třeba výkupné v případě ransomwaru budou platit ze své kapsy. To je výrazný posun proti stávající situaci u organizací, které dosud zákonu o kybernetické bezpečnosti nepodléhaly a kterých má být dle NÚKIB okolo 6000. Já jsem zaznamenal i odhad, který hovoří o čísle přes 10 tisíc. Nově má být kyberbezpečnost klíčovou součástí řízení společností a institucí.

Kdo řeší nová opatření? *Ti zodpovědnější si už vyhodnotili, zda se jich nová regulace dotkne, a uvědomují si, že není mnoho času. Kdo chce ušetřit, musí situaci řešit včas, říká Ondřej Koutský.* **Foto: Lukáš Bíba**

Jak jsou české firmy z hlediska zabezpečení připravené už nyní? NÚKIB například říká, že úroveň připravenosti zase není tak špatná…
Má to několik rovin. Zaprvé, kyberbezpečnostní opatření jako taková. Tam si myslím, že vybavení firem špatné není a stále se zlepšuje, přestože opravdu špičkové úrovně dosahuje jen malý počet subjektů. Pak je tu organizační rovina, tedy směrnice, interní postupy, školení zaměstnanců, audity a podobně. V této části podniky a instituce ještě nejsou na potřebné úrovni, protože tyto požadavky většina z nich zatím ani plnit nemusela. A také bude třeba obsadit nebo externě zajistit pracovníky na nové bezpečnostní pozice. Tam to bude složité.

Vzhledem ke zmíněným změnám, s čím se na vás tedy zákazníci nejvíce obracejí?
Zákon pravděpodobně vstoupí v platnost v polovině příštího roku, to je realistický termín uváděný i ze strany NÚKIB. Pak firmy mají dva měsíce na to, aby se takzvaně samoidentifikovaly, tedy zjistily, zda pod nové povinnosti spadají a v jakém rozsahu. Když od NÚKIB obdrží registraci, mají pak 12 měsíců na splnění povinností. Už teď by se na vše měly připravovat, protože naše zkušenosti ukazují, že účinné projekty na zvýšení kybernetické bezpečnosti trvají více než rok.

Je komplikace, že definitivní podoba zákona stále ještě není na světě?
Vidím to bohužel jako velký problém. Navíc se obsah nového zákona o kybernetické bezpečnosti stále mění. A to ještě nejsou v legislativním procesu prováděcí vyhlášky, které definují vlastní rozsah bezpečnostních opatření.

~ Průměrná škoda způsobená jedním úspěšným kybernetickým útokem je 90 milionů korun. Pokud to společnost považuje za přijatelné, tak O. K.

A vaši klienti už přípravy řeší?
Ti zodpovědnější si už vyhodnotili, zda se jich nová regulace dotkne, a uvědomují si, že není mnoho času. Kdo chce ušetřit a například nakupovat technologie na základě výběrových řízení, snaží se to řešit včas. Ví, že kdyby to řešil před koncem oné zákonné lhůty, nesežene ani hardware, ani lidi. Ti, kdo se tím už nyní intenzivně zabývají, chtějí mít prostor na to najít dobré řešení, vysoutěžit si dodavatele a taky mít prostor vymýšlet konkrétní postupy, jak požadavky zákona splnit. Na to jsou třeba celkem složité analýzy, které nelze udělat ze dne na den. Pokud rizika vyhodnotíte nedostatečně, nesplníte podmínky zákona. Když opatření přeženete, zaplatíte zbytečně moc peněz.

Jsou podle vás znevýhodněné menší firmy, které třeba nemají zahraniční vlastníky a dostatečně silné zázemí?
Obecně si myslím, že podniky střední velikosti jsou v nejtěžší situaci. Z regulace nula vstupují do regulace určité úrovně. Nemají všechna patřičná compliance oddělení, nejsou ani zvyklé řešit takto velké projekty. Je stále spousta organizací a firem, které zatím jen zjišťují informace, ale konkrétní akce zatím nedělají.

Moderní přístup ke kybernetické bezpečnosti:
Integrace EDR a proaktivní DNS ochrany v podání Exclusive Networks Czechia

Společnost Exclusive Networks Czechia je globální distributor s přidanou hodnotou pro kybernetickou bezpečnost a networking. Staví na kvalitních službách distribuce, podpory řešení, školení i implementací. Spolupracuje s předními výrobci jako Infoblox, Fortinet, CrowdStrike, Extreme Networks i dalšími. Zákazníkům poskytuje inovativní produkty a pomáhá při bezpečném přechodu do digitálního světa.

V současném dynamickém prostředí kybernetických hrozeb čelí organizace stále sofistikovanějším a cíleným útokům. Statistiky ukazují, že průměrná doba prolomení zabezpečení z pohledu útočníků je pouhých 62 minut, zatímco identifikace těchto narušení ze stran zákazníků může trvat více než 200 dnů, a to především z důvodu používání tradičních antivirových nástrojů. Tento znepokojivý trend jasně ilustruje rostoucí potřebu modernizace bezpečnostních řešení. Díky zvyšující se rychlosti útočníků a jejich sofistikovaným technikám je nutné kvalitně zabezpečit koncové stanice a firmy postupně přecházejí na moderní typy antivirů, tzv. Endpoint Detection & Response (EDR).

V nedávné době bylo u jedné organizace velmi zkušeným partnerem Security Avengers, který nabízí svým zákazníkům primárně poradenství v oblasti bezpečnosti, nahrazeno původní antivirové řešení implementací EDR od společnosti CrowdStrike. Již pět minut po nasazení řešení CrowdStrike na jednu z koncových stanic, kde byly do té doby používány konkurenční technologie, nástroj CrowdStrike zahlásil velmi závažné napadení malwarem. Nebýt tohoto EDR nástroje, nebylo by možné zjistit téměř nic o právě probíhajícím útoku.

Na základě informací z EDR řešení bylo možné zjistit, že stanice byla kompromitovaná už více než rok. Tehdejší antivirové softwary hrozbu nedokázaly plně identifikovat a zamezit jí. Dále bylo nástrojem CrowdStrike zjištěno, že přítomný, velice komplexní a pokročilý malware na dané stanici dlouhodobě monitoroval stisknuté klávesy, pořizoval snímky obrazovky, kradl uložená hesla uživatele i přístupové údaje k různým wi-fi sítím. Obecně vykazoval chování infostealeru, tedy malwaru zaměřeného na odcizení citlivých dat.

Efektivní kybernetická obrana v dnešní době vyžaduje sofistikovanou kombinaci pokročilých technologií. Zatímco EDR řešení jako CrowdStrike poskytují hlubokou viditelnost na úrovni koncových stanic a dokáže odhalit i dlouhodobě probíhající velmi sofistikované útoky, DNS ochrana od společnosti Infoblox vytváří kriticky důležitou první obrannou linii na síťové úrovni. Tato kombinace je mimořádně účinná. Zatímco útočníci mohou relativně snadno měnit svůj malware, je pro ně výrazně obtížnější skrýt své komunikační vzorce na úrovni DNS.

DNS protokol jako základní stavební kámen internetu je s námi již přes 40 let a představuje kritický prvek v moderní kybernetické bezpečnosti. Bez této služby by současný internet prakticky neexistoval. E-maily, webové stránky i většina online služeb by zůstaly nedostupné. Tradiční přístupy zaměřené primárně na detekci malwaru již nestačí. Incident musí nejprve nastat, aby mohl být zastaven.

Společnost Infoblox přináší revoluci v podobě inovativního řešení založeného na proaktivní analýze DNS provozu. Jejich patentovaný systém využívá pokročilé algoritmy k analýze domén ještě před vytvořením malwaru, detekuje podezřelou infrastrukturu útočníků a dokáže blokovat až 60 procent útoků předtím, než k nim vůbec dojde. V případě probíhajícího útoku pak systém prokazuje mimořádnou účinnost, kdy dokáže zablokovat až 82 procent škodlivých dotazů během 24 hodin od jejich identifikace.

Pomocí pokročilé integrace těchto řešení získávají organizace komplexní přehled o bezpečnostních incidentech. EDR systémy poskytují detailní informace o aktivitách na koncových stanicích a detekci hrozeb, zatímco DNS monitoring doplňuje kriticky důležitý kontext o síťové komunikaci. Společná integrace umožňuje automatickou korelaci DNS událostí s dalšími bezpečnostními daty, což významně zkracuje čas potřebný k detekci a odstranění hrozeb.

Implementace tohoto kombinovaného řešení vytváří robustní vícevrstvou obranu. Infoblox zajišťuje nejen proaktivní DNS ochranu, ale díky svému komplexnímu přístupu ke správě DDI (DNS, DHCP, IPAM) poskytuje administrátorům také detailní přehled o stavu sítě. V kombinaci s EDR řešením od CrowdStrike tak vzniká ucelený bezpečnostní ekosystém, který umožňuje efektivní detekci a vyšetřování incidentů.

NIS2: Co přináší „nižší režim“ v návrhu nového zákona o kyberbezpečnosti?

Nový zákon o kybernetické bezpečnosti (nZKB) je v Poslanecké sněmovně a probíhá kolem něj poměrně živá mediální debata, která někdy nové zákonné povinnosti až démonizuje. Pojďme se podívat, jak konkrétně vypadají povinnosti pro většinu subjektů, které pod nový zákon „spadnou“.

Nárůst počtu regulovaných subjektů (RS) ze 450 na odhadem 6000 je velkou změnou. Vychází z pravidel evropské směrnice NIS2, kterou je ČR povinna převést do svého právního řádu – a dojde k tomu právě v rámci nZKB. Ačkoli počet regulovaných subjektů vychází ze směrnice EU, v implementaci pravidel je značná vůle.

NÚKIB napsal návrh nového zákona tak, aby situaci firmám a institucím co nejvíce usnadnil. **Povinnosti rozdělil dle významu RS do dvou režimů, vyššího a nižšího.**

Společné povinnosti pro oba režimy jsou následující:

- Ohlášení, že pod zákon spadáte;
- Ohlášení kontaktní osoby pro komunikaci s NÚKIB;
- Hlášení incidentů v případě úspěšného útoku – nižší režim hlásí pouze významné incidenty;
- Protiopatření: Plnění ad hoc pokynů NÚKIB v reakci na akutní hrozbu.

Pak je tu nejdůležitější povinnost, a to zavedení kyberbezpečnostních opatření.
Povinným minimem v nižším režimu je:

- Určení osoby odpovědné za kyberbezpečnost;
- Základní bezpečnostní dokumentace, zejména „Přehled bezpečnostních opatření“, tedy dokument o tom, co mám zavedeno, co zavádět nebudu a co zavedu a kdy;
- Nastavení základních bezpečnostních pravidel a jejich zohlednění ve smlouvách s dodavateli;
- Školení uživatelů a vrcholového managementu;
- Prosazování kyberbezpečnosti z úrovně managementu (jak deklarace, tak zcela praktická podpora – vedení by například nemělo mít bezpečnostní výjimky);
- Připravení plánu pro zvládání útoku a obnovu provozu;
- Používání softwaru s podporou výrobce a pravidelnými aktualizacemi.

Národní úřad pro kybernetickou a informační bezpečnost
NÚKIB

nZKB
NIS2

Vyšší režim je standardem, podle kterého by už mělo fungovat oněch 450 subjektů regulovaných stávajícím zákonem o kybernetické bezpečnosti.

Nižší režim, do něhož bude náležet většina (cca 5000) regulovaných subjektů, pak požaduje naprosté základy kybernetické bezpečnosti, které očekáváte od hotelu na dovolené.

*Povinnosti v nižším režimu se zavádějí dle **principu přiměřenosti** – náklady na zaváděné **opatření by neměly převyšovat náklady** na případnou nápravu kybernetického incidentu.*

*Plnění povinností se dá **rozložit v čase – instituce vyhodnotí a zdokumentuje** své možnosti zavádění opatření.*

Chcete vědět víc? Pojďte na **Portál NÚKIB**
→ www.portal.nukib.gov.cz