HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
13. – 15. DECEMBRA 2024

Odborná spolupráca
NBÚ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Zákon je schválený. Ako sme na tom?

TÉMA

Čakali na to tisícky firiem a inštitúcií. Od januára 2025 bude účinný nový zákon o kybernetickej bezpečnosti.

Podľa nového kyberzákona pribudne od januára viacej ako deväťtisíc subjektov, ktoré sa stanú povinnými osobami. FOTO: DREAMSTIME

Prvé, čo vás zarazí, je masívny dosah kyberzákona na široké podnikateľské spektrum.

Počet povinných subjektov stúpne niekoľkonásobne a všetci potrebujú profesionálov kyberbezpečnosti. Pribudnú povinnosti. Pokuty narastú až na desať miliónov eur alebo dve percentá ročného obratu.

Mantra roka

Smernica NIS2 je už viac ako rok dôvodom na články, školenia, prezentácie a občas aj bezdôvodnú paniku v kyberbezpečnosti. Koniec teoretických odporúčaní, parlament schválil novelizáciu zákona, od začiatku roka sa očakávajú vykonávacie vyhlášky.

Podľa slov kyberbezpečnostného profesionála Mariána Illovského zo skupiny Cyllium vidieť vo firmách aj inštitúciách zvýšený záujem o to, „čo to vlastne tá NIS2 je, či je pre nich povinná a čo musia urobiť“.

Prečo je regulácia

Advokát Miroslav Chlipala prirovnáva kybernetickú bezpečnosť k prevencii a ochrane pred prírodnými živlami. V tomto prípade ide o prevenciu a ochranu pred „živlami“ v kybernetickom priestore.

Regulácia je kľúčová na ochranu infraštruktúry a sektorov dôležitých pre náš každodenný život pred rastúcimi kybernetickými hrozbami. Tým, že sa stanovia harmonizované a vynútiteľné pravidlá, v konečnom dôsledku sa zabezpečuje stabilná ochrana nás všetkých.

Ťahúni trhu

Ak hovoríme o podnikoch, ktoré sa dobre pripravujú na nový kyberzákon, príkladom ide riadenie služieb IKT. V tomto sektore si už zákazníci presadili nastavenie určitého bezpečnostného štandardu cez dodávateľské zmluvy, ak sa na nich vzťahoval kyberzákon.

V zdravotníctve potvrdzuje posun k lepšiemu Dominik Procházka, riaditeľ odboru kybernetickej bezpečnosti v skupine Agel: „Najmä štatutári majú zvýšený záujem počúvať a diskutovať.“

Tiché rozjímanie

Marián Illovský po desiatke rokov skúseností vidí posun na slovenskom trhu minimálne v uvedomení. „A postupne príde aj pocit zodpovednosti. Najvýraznejší katalyzátor je incident, ale ozaj nechcem priať nikomu nič zlé.“ Zároveň tu však v súvislosti s novým kyberzákonom poukazuje na rezistenciu sektorov, ktoré neboli doteraz povinnými, napríklad segment výroby alebo výroba, spracovanie a distribúcia potravín.

Princíp rezistencie proti kyberbezpečnostným opatreniam platí, aj pokiaľ ide o pracovné pozície. „Ide tu skôr o individuálny postoj, keď konkrétna osoba potrebuje prijať zmenu a uvedomiť si zodpovednosť,“ vysvetľuje Dominik Procházka.

Kto nám chýba

Na Slovensku pribudne podľa kyberzákona viac ako deväťtisíc povinných subjektov, nehovoriac o tých existujúcich. Preto je cieľom získať kvalifikovaný personál na obsadenie aspoň v povinných zákonných rolách ako manažér a audítor kybernetickej bezpečnosti.

Keďže počet auditovaných subjektov sa zvýši až na dvojnásobok, nastane rovnaký problém ako pred rokmi. Aktuálne máme približne 50 aktívnych audítorov kybernetickej bezpečnosti. Potreba trhu bude dvojaž trojnásobný počet aktívnych audítorov. „Musíme zintenzívniť hľadanie, upskilling aj certifikáciu odborníkov,“ varuje Tomáš Hettych z Kompetenčného a certifikačného centra kybernetickej bezpečnosti.

Malá pomôcka

Aj keď kyberzákon dáva vybraným subjektom možnosť samohodnotenia kyberbezpečnosti, je tu háčik. Samohodnotenie si subjekty urobia každé dva roky, ale po piatich rokoch si musia dať urobiť audit kyberbezpečnosti.

Podľa novelizácie pribudne takmer päťtisíc takých subjektov, ktoré budú mať možnosť samohodnotenia. Kvalifikovaný návod bude poskytovať webová stránka Národného bezpečnostného úradu, ale pre malé obce, mestá či subjekty s outsourcingom IT môže byť aj táto úloha náročná.

A sme opäť na začiatku.

Plán máme

Personálna téma je boľavá všade a novelizácia zákona ide ešte ďalej. Okrem certifikovaného audítora a manažéra kyberbezpečnosti pribudne ďalších desať rolí v tejto oblasti. Bezpečáci a audítori kybernetickej bezpečnosti sa preto obzerajú, kde by našli kolegov. Tomáš Hettych je sám príkladom kariérnej zmeny, a preto často a rád prezentuje prístup, že ideálne je „upskillovať“ IT špecialistov.

KĽÚČOVÉ ZMENY KYBERZÁKONA 2025

Rozšírenie pôsobnosti zákona **na nové sektory a subjekty**

Identifikácia regulovaného subjektu na základe jeho zaradenia do sektora

Aplikácia bezpečnostných opatrení na základe analýzy rizík

Úprava bezpečnosti **dodávateľského reťazca**

Úprava **hlásenia incidentov**

Koordinované **zverejňovanie zraniteľností**

Audit a samohodnotenie

Certifikácia bezpečnosti IKT produktov a služieb

Zdroj: Národné centrum kybernetickej bezpečnosti

Najlepší kandidáti sú IT profesionáli, administrátori, interní audítori, dátoví analytici, špecialisti ochrany osobných údajov či manažéri riadenia procesov. Ak už spĺňajú znalostné a kompetenčné predpoklady, môžu absolvovať certifikačné kurzy a posunúť sa ďalej.

Úlohy pokračujú

Zatiaľ čo v strednodobom horizonte je najefektívnejšie kontinuálne vzdelávania vo vzdelávacích inštitúciách, dlhodobo je tento problém riešiteľný iba formou vysokoškolského vzdelávania.

Informačná a kybernetická bezpečnosť sa však buduje niekoľko rokov. „Rovnako aj vzdelávanie a spôsob výchovy mladých nie je záležitosťou jedného roka,“ pripomína Pavol Sokol z Univerzity Pavla Jozefa Šafárika v Košiciach. „K študentom sa musia dostať aj iné poznatky a zručnosti, napríklad ako sa zachovať v konkrétnych situáciach, čo to znamená správať sa morálne a podobne.“

Nová misia

Dodávatelia kyberbezpečnostných služieb profesionálov hľadajú, „kde sa len dá“. Či sú to platené stáže, spolupráce s univerzitami alebo často uvádzaný prechod z IT do kyberbezpečnosti.

Tu je príznačný postreh riaditeľa spoločnosti Aliter Technologies Jána Grujbára: „Každá generácia prináša na trh práce špecifiká. Jedným z hlavných trendov, ktorý pozorujeme u mladých ľudí, je túžba po zmysluplnej práci. Mladí nechcú slepo vykonávať aktivity v duchu monkey see, monkey do. Naopak, hľadajú príležitosti, kde môžu prispieť k väčšiemu strategickému cieľu, ovplyvniť výsledky a zanechať stopu.“

Zákon a pokuty sú jedna vec, presvedčenie sa však nedá vynútiť. „Preto by som rád úprimne zdôraznil nevyhnutnosť vzdelávania pre budovanie kybernetickej odolnosti proti globálnym hrozbám,“ uzatvára Miroslav Chlipala.

ANKETA:

Koho a čoho sa vyvarovať v kyberbezpečnosti v roku 2025?

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 13. – 15. DECEMBRA 2024

Základný kybermanuál od januára 2025

PRAX

Novelizácia kyberzákona je významnou legislatívnou zmenou z viacerých dôvodov. Zodpovednosť štatutára za kyberbezpečnosť nie je totiž možné preniesť na manažéra kybernetickej bezpečnosti.

Riadenie kyberbezpečnosti ako proces

Zoznam sektorov podľa novelizácie zákona o kybernetickej bezpečnosti

Ak sa nachádzate v uvedenom sektore a spĺňate ďalšie veľkostné podmienky, ste povinnou osobou zo zákona.

Kľúčové subjekty

Bankovníctvo

Dodávka a distribúcia pitnej vody

Doprava

Energetika

Infraštruktúra finančných trhov

Odpadová voda

Riadenie služieb IT

Vesmír

Dôležité subjekty

Digitálna infraštruktúra

Elektronické komunikácie

Pošta

Priemysel

Voda a atmosféra

Odpadové hospodárstvo

Poštové a kuriérske služby

Priemyselná výroba

Výroba a distribúcia chemických látok

Výroba dopravných prostriedkov

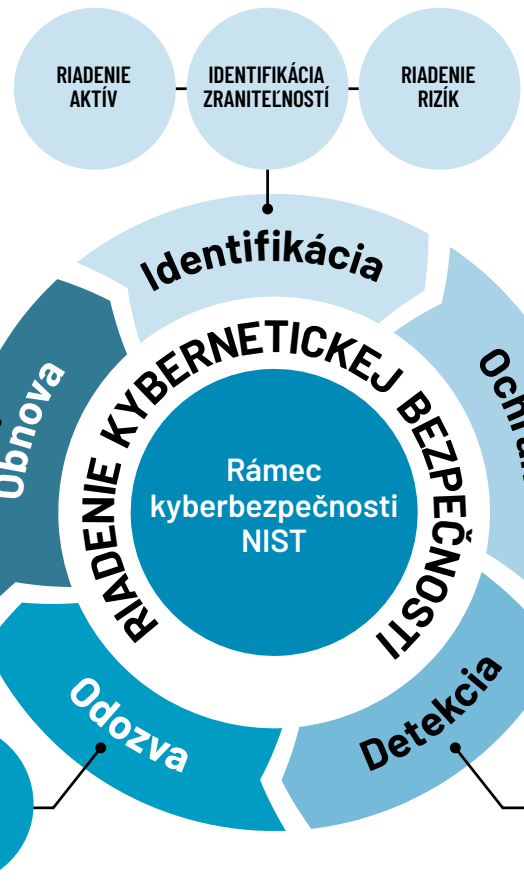
Výroba elektrických strojov a zariadení

Výroba motorových vozidiel

Výroba počítačových elektronických a optických výrobkov

Výroba, distribúcia a spracovanie potravín

Výskum



ZHRNUTIE

Novela zákona o kyberbezpečnosti nie je revolúcia, ale evolúcia

Slovensko už pri transpozícii Smernice NIS išlo s požiadavkami nad rámec smernice.

Väčšina všeobecne záväzných právnych predpisov vrátane sektorových opatrení je inšpirovaná uznanými technickými normami, príkladom je tak často zmieňovaná EN ISO/IEC 27002:2022

Pri praktickej implementácii opatrení nie je potrebné bezpodmienečne sa riadiť detailom právnych predpisov. Existuje množstvo použiteľných technických noriem. Podstatný je účinok primeraného opatrenia.

Novelizáciu zákona treba vnímať v kontexte bezpečnostných opatrení. Novelou sa zdôrazňujú špecifiká odvetví a zároveň sa zlepšia procesy riadenia hrozieb a rizík.

Odpočítavanie do januára sa začína. FOTO: DREAMSTIME

Zavádza sa koordinované zverejňovanie zraniteľností a celkovo sa miera kooperácie a komunikácie týkajúca sa hrozieb a rizík zvyšuje.

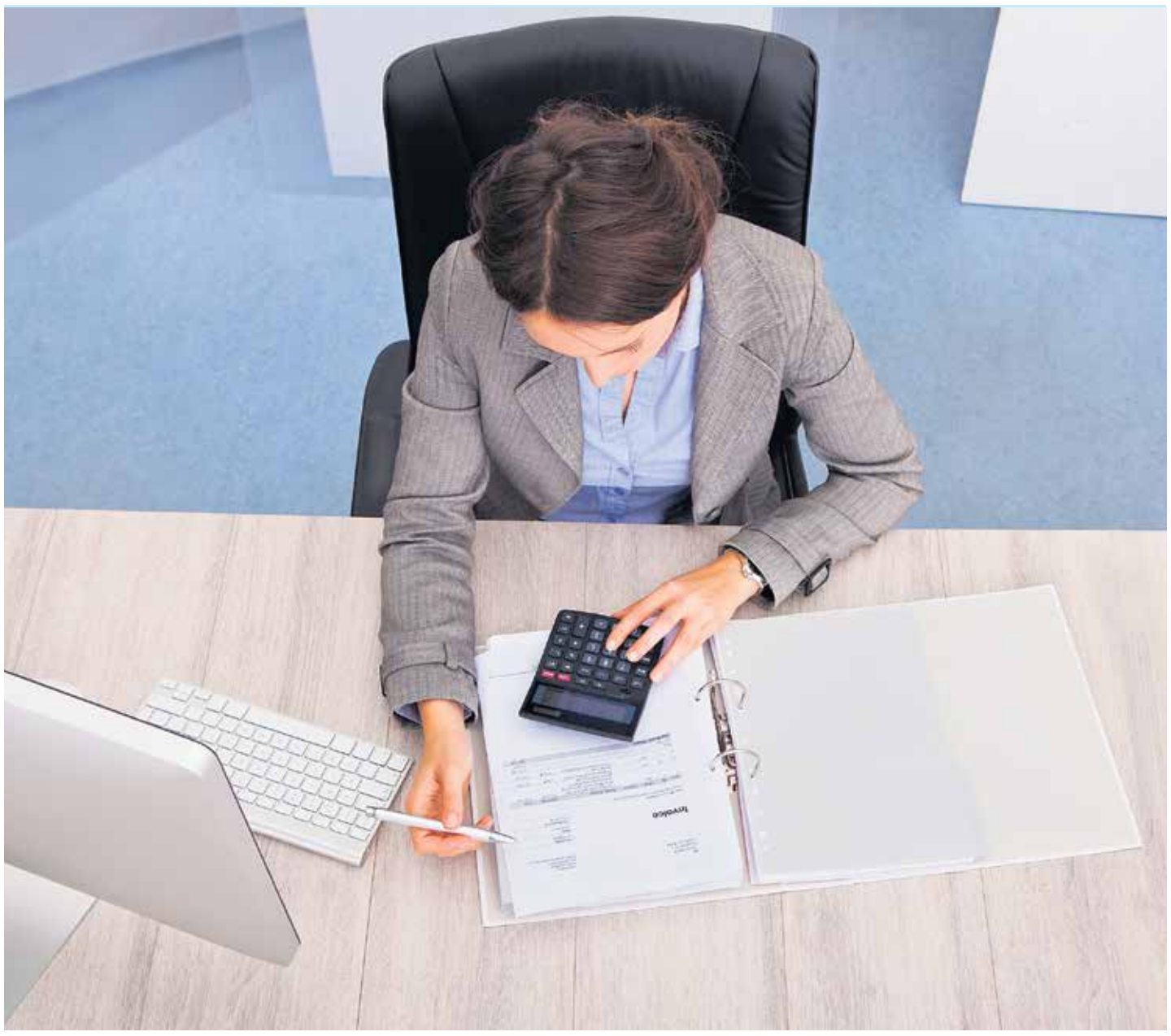
Rozšírením pôsobnosti zákona na dodávateľské reťazce sa zvýši celková úroveň odolnosti proti hrozbám. A v neposlednom rade – zavádzajú sa dlhoočakávané mechanizmy bezpečnostnej certifikácie výrobkov, procesov a služieb.

Ivan Makatura, generálny riaditeľ, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Povinnosti a rozpočet súvisia

SKÚSENOSTI

Investície do kybernetickej bezpečnosti rastú pod tlakom legislatívy, technologických trendov aj geopolitického napätia. Aktuálne sa pozeráme na investície a povinnosti aj optikou nového zákona.



Investície do bezpečnosti by mali reflektovať výsledky analýzy rizík a zákonných povinností. FOTO: DREAMSTIME

Podľa najnovšej správy Európskej agentúry pre kybernetickú bezpečnosť ENISA sa rozpočty na kyberbezpečnostné opatrenia vo firmách v Únii medziročne zvyšujú.

Prieskum v organizáciách rôznej veľkosti ukázal, že informačná bezpečnosť predstavuje v súčasnosti priemerne deväť percent objemu investícií do IT.

V porovnaní s rokom 2022 je to významný nárast o 1,9 percentuálneho bodu. Ide o druhý za sebou nasledujúci rok rastu investícií do kybernetickej bezpečnosti po pandémii.

Aj starí, aj noví

Agentúra ENISA hodnotila aj vplyv smernice NIS 2 na investície do kyberbezpečnosti v organizáciách, pričom do prieskumu zahrnula doterajšie aj budúce povinné subjekty.

Ak porovnáme nové sektory zahrnuté pod NIS 2 s existujúcimi subjektmi podľa predchádzajúcej smernice, objem investícií je porovnateľný. Výdavky sú zamerané najmä na rozvoj a udržiavanie základných kapacít.

Očakávaný nárast

Väčšina organizácií v Únii očakáva jednorazové alebo trvalé zvýšenie rozpočtov na kybernetickú bezpečnosť, aby zabezpečila súlad so smernicou NIS 2.

Nie je prekvapením, že významný počet subjektov nebude môcť rátať s potrebným zvýšením rozpočtu. V segmente malých a stredných podnikov deklarovala až tretina respondentov (34 percent), že im bude chýbať rozpočet na potrebné opatrenia.

Takmer 90 percent európskych organizácií hlási, že bude potrebovať viac zamestnancov na zabezpečenie súladu so smernicou NIS 2, najmä v oblasti architektúry a inžinierstva kybernetickej bezpečnosti a prevádzky.

Fakty nepustia

Aj keď v prípade Slovenska novelizácia kyberzákona neprináša revolučné novinky, opäť zdôrazňuje staré známe pravdy – kybernetická bezpečnosť nie je jednorazový projekt, ale nepretržitý proces. Ak si organizácie nenájdu čas na prípravu a opatrenia teraz, môžu čeliť oveľa vyšším nákladom v budúcnosti.

Pre mnohé firmy to bude len ďalšie „opakovanie známeho“, no tentoraz so sprísnenými pravidlami a s väčšími dôsledkami za ich nedodržiavanie.

Druhú skupinu tvoria organizácie, ktoré vstupujú do regulovaného prostredia v januári budúceho roku a čaká ich debata o technológiách a rozpočtoch.

> AK SI ORGANIZÁCIE NENÁJDU ČAS NA PRÍPRAVU A OPATRENIA TERAZ, MÔŽU ČELIŤ OVEĽA VYŠŠÍM NÁKLADOM V BUDÚCNOSTI.
>
> **Jozef Bálint,** bezpečnostný špecialista ALISON Slovakia

Pre začiatočníkov

Ak stále nemáte zavedené potrebné procesy, začnite gap analýzou alebo analýzou rizík, ktoré odhalia, kde sú vaše slabiny. Tieto kroky sú základom na pochopenie aktuálneho stavu a naplánovanie ďalšieho postupu.

Pre menšie firmy

Ak nemáte interné kapacity, zvážte externé riešenia, ako napríklad služby Security Operations Center (SOC). SOC poskytuje 24/7 dohľad nad bezpečnosťou, rýchle riešenie incidentov a minimalizáciu škôd, a to všetko bez potreby budovania vlastného tímu.

Pre väčšie organizácie

Veľkých podnikov podľa medzinárodnej metodiky máme na Slovensku iba niekoľko, takže tu patrí súkromná sféra medzi lídrov v hodnotení kyberbezpečnostných opatrení. S prihliadnutím na počet zamestnancov sú diskutabilné veľké zdravotnícke zariadenia vo verejnej správe.

Pre všetky veľké organizácie v budúcom roku je dôležité, že okrem technológií sa budú sústreďovať na školenia zamestnancov, aktualizáciu plánov reakcie na incidenty a pravidelné penetračné testy.

Pre všetkých

Kybernetická bezpečnosť je dnes neoddeliteľnou súčasťou fungovania každej organizácie. Aj keď sa o nej hovorí už roky, smernica NIS2 či novela zákona opäť pripomínajú povinnosť prijať adekvátne opatrenia.

V skratke? Základom je mať silné heslá, šifrovať citlivé dáta, pravidelne zálohovať a neustále monitorovať systémy.

PORADŇA

Aké opatrenia potrebujete?

Nová legislatíva kladie väčší dôraz na systematické riadenie kybernetických rizík.

Organizácie musia zaviesť bezpečnostné opatrenia, ktoré zohľadňujú aktuálny stav technológií a sú primerané rizikám ohrozujúcim ich informačné systémy.

Tieto opatrenia zahŕňajú napríklad správu zraniteľností a kybernetických hrozieb, šifrovanie, ochranu pred škodlivým softvérom či riadenie kybernetických bezpečnostných incidentov.

Zvláštny dôraz sa kladie na hlásenie kybernetických incidentov, ktoré musí byť vykonané promptne – už do 24 hodín od ich zistenia.

Kyberzákon zároveň vyžaduje, aby organizácie pravidelne testovali a hodnotili efektívnosť svojich bezpečnostných opatrení, čím sa zabezpečuje ich aktuálnosť voči novým hrozbám.

Nepretržitá aktualizácia ochranných systémov a kontrola dodržiavania bezpečnostných štandardov sú základnými piliermi prevencie pred kybernetickými útokmi.

Dodržiavanie zákona pomáha organizáciám nielen napĺňať zákonné požiadavky, ale aj výrazne znižovať pravdepodobnosť úspešného kybernetického útoku.

Implementácia takýchto opatrení však môže byť pre mnohé organizácie výzvou, a práve tu vstupujú do hry pokročilé riešenia, ako je ESET PROTECT MDR.

Tento službovo-produktový balík je navrhnutý tak, aby organizáciám pomohol splniť veľkú časť povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti.

Kyberbezpečnostnú detekciu a reakciu podporuje AI. FOTO: DREAMSTIME

Vďaka špičkovej technológii riadenej detekcie a reakcie (MDR), podporovanej umelou inteligenciou, umožňuje organizáciám zavádzať a udržiavať opatrenia, ako je správa zraniteľností, identifikácia bezpečnostných incidentov v reálnom čase či ochrana pred škodlivým softvérom.

Neustála dostupnosť tejto služby 24 hodín denne, 7 dní v týždni znamená, že bezpečnosť organizácií je monitorovaná bez prerušenia, čo výrazne posilňuje ich schopnosť reagovať na hrozby okamžite.

ESET PROTECT MDR predstavuje ochranu spravovanú odborníkmi zo spoločnosti ESET, čo umožní špičkové zabezpečenie aj pre firmy bez vlastných špecialistov na IT bezpečnosť.

Július Selecký, senior technický špecialista ESET, odborný asistent Fakulta managementu UK

KOMENTÁR

Takto si tu žijeme. Bezpečnosť je jedna, prístupy rôzne

Je rozdiel v prístupe ku kybernetickej bezpečnosti v súkromnom a vo verejnom sektore? Je to debata na desiatky hodín, ale rozdiely sa dajú opísať.

Vzhľadom na komplexnosť a prepojenosť IT technológií s narastajúcimi hrozbami v kyberpriestore dnes už veríme, že nemusíme obhajovať postoj, keď sa kybernetická bezpečnosť radí medzi základné potreby fungovania spoločnosti tak vo verejnom, ako aj v súkromnom sektore.

Ako dodávateľ kyberbezpečnostných riešení a služieb máme skúsenosti s klientmi z oboch prostredí, a hoci počet klientov nepredstavuje celý trh, opakujúce sa vzorce v oboch sférach nám poskytujú celkom ucelený obraz o ich prístupe ku kybernetickej bezpečnosti.

Verejné tajomstvo

Verejný sektor si jednoznačne uvedomuje potrebu riešiť kybernetickú bezpečnosť. Jedným z hlavných hnacích motorov tohto procesu je legislatívny tlak, ktorý núti organizácie prijímať bezpečnostné opatrenia.

Hoci inštitúcie chápu význam kybernetickej bezpečnosti, respektíve ochranu údajov či samotných dát a systémov aj ako súčasť dobrej praxe, mnohé sa zameriavajú len na splnenie minimálnych legislatívnych požiadaviek, a to z rôznych dôvodov. Výrazný problém predstavuje technologický dlh – zastarané IT infraštruktúry, ktoré komplikujú zavádzanie moderných bezpečnostných riešení.

Kybernetická bezpečnosť je často vrstvená nad existujúce IT systémy, čo znamená, že pokiaľ nie sú základné systémy aktualizované a zabezpečené, pokročilé technológie strácajú význam alebo ich efektivita a celkový význam veľmi prudko klesá.

Ďalšia méta

Opakovane pripomínam, že často je primárnym dôvodom riešenia kybernetickej bezpečnosti vo verejnom sektore legislatíva. Tá vytvára tlak na splnenie aspoň minimálnych požiadaviek.

Napriek tomu, že legislatíva je dôležitá, ide len o jednu časť širšieho rámca GRC – Governance, Risk Management, Compliance.

Kybernetická bezpečnosť by však mala byť o proaktívnom riadení rizík a systematickom riešení, nie iba o reakcii na právne predpisy. Tu však primárne zohrávajú rolu pridelené finančné prostriedky.

Pestrofarebná škála

Prístup v súkromnom sektore je rozmanitejší. Niektoré firmy, ba dokonca celé sektory, investujú do špičkových technológií a budujú profesionálne tímy, ktoré sa bezpečnosti venujú na veľmi vysokej úrovni – typickým predstaviteľom je napríklad finančný sektor.

Na druhej strane existujú odvetvia, kde sa tejto oblasti venuje len minimálna pozornosť.

Flexibilita súkromného sektora umožňuje rozmanité riešenia bezpečnostných problémov. Hlavnou motiváciou pre firmy je tu však hospodársky výsledok. Kybernetickú bezpečnosť vnímajú ako nástroj na ochranu svojho podnikania a aktív.

Hoci legislatíva hrá dôležitú úlohu, pre firmy, ktoré už bezpečnosť riešia, je prioritou nielen splnenie si litery zákona, ale hlavne ochrana svojho podnikania. Nové legislatívne požiadavky však môžu byť pre firmy, ktoré sa doteraz tejto téme vyhýbali, dôležitým impulzom na zmenu prístupu.

Rôzne cesty, jeden cieľ

Diskusia o tom, či by mala byť hlavným motorom legislatíva alebo trhové mechanizmy, je oprávnená, avšak v kontexte rastúcich kybernetických hrozieb je podstatné, že sa táto téma rieši na oboch frontoch.

Nech už je motiváciou zákon alebo ochrana podnikania, kroky na posilnenie kybernetickej bezpečnosti prispievajú k celkovej odolnosti spoločnosti proti digitálnym hrozbám.

Autorský tím Aliter Technologies

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 13. – 15. DECEMBRA 2024

Koho a čoho sa vyvarovať v roku 2025?

ANKETA

365 nových kalendárnych dní pred nami a kybernetický útok každých 38 sekúnd. Každý zamestnanec má minimálne jedno zariadenie s pripojením do internetu. Čoraz viac povinností. Takže vyberte si aspoň jednu radu, ako to všetko prežiť.

Jaroslav Ďurovka,
riaditeľ,
Národné centrum kybernetickej bezpečnosti

Vyvarujte sa nečinnosti. No a prevádzkovatelia základných služieb by nemali zabúdať na povinné hlásenia kybernetických bezpečnostných incidentov a iných udalostí podľa novelizovaného zákona o kybernetickej bezpečnosti.

Jaroslav Oster,
predseda Správnej rady,
Preventista.sk

Vyhýbajte sa zbytočnej panike a chiméram o instantných, rýchlych a efektívnych riešeniach. Jednoducho – aj v roku 2025 bude dostupné krabicové mlieko a kybernetická bezpečnosť stále ostane procesom, ktorému bude nutné sa venovať.

Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Ak sa pýtate, koho sa vyvarovať, tak diletantov, ktorí sa tvária, že všetkému rozumejú a všetko vedia, ale ako prví sadnú na lep útočníkovi. A vyvarovať sa čoho? Nerozvážnych reakcií, ak niečo nefunguje a zdá sa to ako problém.

Stanislav Smolár,
manažér oddelenia bezpečnosti,
Soitron

Stráňte sa každého, kto vám tvrdí, že pozná „zaručenú" tému ďalšieho roka. Či to bude AI (2024), Zero Trust (2023) alebo postkvantové šifrovanie (2025?), nepôjde o zásadnú zmenu v smerovaní kyberbezpečnosti, ale skôr o ďalší cyklus inovácií, ktoré postupne prejdú do používania.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti,
Aliter Technologies

Phishingové a ransomvérové útoky, slabé heslá či deepfake technológie? Ani tieto hrozby určite nezmiznú v roku 2025. Každý rok však prináša svoje špecifiká a predpovedať hlavnú hrozbu je ťažké, najmä vzhľadom na fenomén čiernych labutí, ktoré majú často najväčší dosah. Preto je kľúčové snažiť sa byť krok pred útočníkmi, dodržiavať bezpečnostné štandardy, osvedčené postupy a nezaspať na vavrínoch – aj keď sa zdá, že je všetko pod kontrolou.

Michal Rampášek,
advokát,
AK Peterka Partners

Nezostaňte ticho – pýtajte sa a otvorene diskutujte o rizikách na všetkých úrovniach firmy, zapojte vrcholové vedenie, ale aj svojich dodávateľov. Neignorujte nové regulácie, predovšetkým transpozíciu smernice NIS2 do zákona a jeho vyhlášok, ktoré budú mať zásadný vplyv najmä na subjekty v doteraz neregulovaných sektoroch. Prístup „počkáme a uvidíme" sa v kyberbezpečnosti nevypláca.

Jakub Berthoty,
advokát,
Dagital Legal

Bežná obchodná spoločnosť by sa v prvom rade mala zaoberať otázkou, či sa na ňu kyberzákon vzťahuje. To nemusí byť v každom prípade úplne jednoduché zodpovedať. Vyvaroval by som sa preto toho, aby sa táto úvodná analýza podcenila.

Martin Orem,
hacker,
Binary House

V roku 2025 sa treba vyvarovať predavačov, ktorí sľúbia a predajú desať deka instantnej bezpečnosti v podobe akejkoľvek služby, hadí olej ako neprekonateľný AI-driven produkt, a taktiež strašiakov v NIS2 poli. Ransomvér, sociálne inžinierstvo a cloudová bezpečnosť pravdepodobne zostanú horúcimi témami aj v nasledujúcom roku.

Tomáš Hettych,
viceprezident,
ISACA

Vyvarujte sa uspokojenia z dosiahnutého stavu. Stále je čo zlepšovať, tak nezaspite na vavrínoch po audite. Prichádzajú nové a sofistikovanejšie hrozby, je potrebné pripraviť sa a správne reagovať. Zabráňte priemernosti, žiadajte si najlepšie riešenia a expertov. Overujte si referencie, kontrolujte. A nezabudnite vzdelávať seba a svojich zamestnancov.

Jaroslav Ušiak,
prodekan pre vedu a výskum,
Fakulta politických vied a medzinárodných vzťahov UMB Banská Bystrica

Je potrebné vyvarovať sa dezinformácií a deepfake obsahu, keď sa rôzni štátni aj neštátni aktéri snažia s nami manipulovať a tým podkopávajú demokratické princípy. Pokročilé AI nástroje umožňujú manipulácie na novej úrovni. Preto je princíp „zero trust – never trust, always verify" kľúčový. Overujte si informácie, vyhnite sa nezabezpečeným zariadeniam, aktualizujte systémy a vzdelávajte sa v digitálnej gramotnosti.

Benjamin Würfl,
obchodný manažér,
Eviden Slovakia

V kontexte rastúceho množstva ransomvérových útokov by sme ani v budúcom roku nemali podceňovať edukáciu bežných používateľov, ktorí predstavujú najzraniteľnejšie miesto pri hackerských útokoch.

Marcela Macová,
lektorka,
DAPRO Consulting

Kyberbezpečnosť sa často prelína s ochranou osobných údajov a my budeme čeliť výzvam spojeným s technologickým rozvojom. Je potrebné sledovať zmeny a správne ich implementovať. V záujme efektívneho plnenia povinností a zvýšenia dôveryhodnosti je nevyhnutný správny výber zamestnancov či dodávateľov. Investujte do vzdelávania zamestnancov, overujte si referencie aj povesť dodávateľov. Vyvarujme sa toho, že nebudeme stáť za radami manažérov kybernetickej bezpečnosti či zodpovedných osôb.

Andrej Mišura,
partner,
Cyllium
Ocenený Asociáciou kybernetickej bezpečnosti ako Manažér kybernetickej bezpečnosti roka 2024

Zabudnite na skratky a rýchle riešenia. Kam vás posunul váš manažér kybernetickej bezpečnosti s mandátom dve hodiny do mesiaca alebo kamoško vášho dodávateľa IT? Nikam. Ušetrili ste, ale nikam ste sa nepohli. Hľadajte profesionálneho zodpovedného lekára, nie najlacnejšieho.

Tomáš Valenta,
riaditeľ,
Check Point Software Technologies Slovakia

V každom roku bude dôležité rozmýšľať nad svojím konaním v online priestore. Primárne by som odporúčal nedôverovať a nepodceňovať. Neklikať na neznáme odkazy a neotvárať prílohy z neznámych zdrojov. Vyvarovať sa tiež prílišného zdieľania citlivých údajov a ignorovania aktualizácií používaného softvéru.

Juraj Koník,
bezpečnostný manažér,
Allianz Slovakia

Kyberbezpečnosť je neustály boj. Aby sme sa ochránili a držali krok so zločincami, musíme byť neustále ostražití, vzdelávať sa a byť ochotní prijímať – prispôsobiť sa novým výzvam, i keď akceptácia zmeny je niekedy pre nás tá najväčšia výzva. Pre mňa sú tu top tri výzvy: umelá inteligencia ako dvojsečný meč, sociálne inžinierstvo na novej úrovni – deep fake videá a audionahrávky, cloud a jeho bezpečnosť.

Július Selecký,
senior technický špecialista,
ESET

V roku 2025 si treba dávať pozor najmä na útoky posilnené umelou inteligenciou. Odpoveďou môže byť využívanie pokročilých detekčných a reakčných systémov a využívanie patch managementu. Rok bude do značnej miery ovplyvnený novelou kyberzákona. Spoločnosti budú v oveľa väčšej miere vyhodnocovať riziká dodávateľského reťazca a prísnejšie ich hodnotiť. Školenia zamestnancov sa budú pre kvalitnejšie phishingové kampane ešte viac posilňovať.

Lucia Halásová,
špecialistka IT bezpečnosti,
Direct Parcel Distribution SK

Je dôležité nespoliehať sa na automatickú kyberhygienu ostatných. Neustále vzdelávaj všetkých okolo seba a buď im príkladom. Útoky cez dodávateľov budú častejšie, preto by mala byť analýza rizík dôležitou súčasťou každej organizácie. AI je dvojsečná zbraň, nauč sa ju využívať na obranu pred čoraz sofistikovanejšími útokmi a hrozbami. A nezabudni na citlivú mínu – správne chráň a zálohuj dáta!

Maroš Trnka,
vedúci odboru IT,
Vodohospodárska výstavba

Cez tretie strany vedie cesta k vám, a preto pokladám za dôležité vyhnúť sa dodávateľom, ktorí nedbajú na dostatočné bezpečnostné opatrenia. Starostlivo vyberajte partnerov, ktorí skutočne disponujú potrebnými vedomosťami a skúsenosťami. Vyhnite sa tomu, aby ste sa stali terčom. Proste si ozaj uvedomte, že už terčom ste.

Tomáš Loveček,
prodekan pre vedu a výskum,
Fakulta bezpečnostného inžinierstva, Žilinská univerzita

Snažte sa vyvarovať všetkých hrozieb a nech váš risk appetite je adekvátny vašim možnostiam. Nezabúdajte, že bezpečnostná dokumentácia nie je cieľ, ale cesta. Bezpečnostné opatrenia prijímajte pre seba, a nie pre audítora alebo regulátora. No ak sa vás bude niekto snažiť presvedčiť, že NIS2 má dosah aj na vašich domácich miláčikov, tak sa mu snažte oblúkom vyhnúť.

Roman Čupka,
hlavný konzultant,
Progress a CSO Istrosec

Chráňte sa pred podvodníkmi, a to na všetkých úrovniach! Budúci rok si musíme všetci držať klobúky a strážiť peňaženky. Oficiálne čísla trhu s kyberkriminalitou pomaly atakujú osem miliárd eur. Okrem toho nás čaká určite aj väčší tlak na odolnosť kritickej infraštruktúry. Preventívne opatrenia sú síce fajn, ale pokiaľ má akýkoľvek protivník dostatok prostriedkov a čas, jeho snaha dospeje vždy k úspešnému výsledku.

Ivan Makatura,
generálny riaditeľ,
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Chráňte sa pred samozvanými odborníkmi, takzvanými NIS2 fantómami. Kybernetická bezpečnosť je rýchlo sa rozvíjajúci odbor a podobne ako pred časom GDPR, aj kyberbezpečnosť priťahuje ľudí, ktorí vidia iba príležitosť zisku. Po novele zákona sa s takými roztrhne vrece. Overujte si kvalifikáciu a referencie dodávateľov.

Jozef Zoričák,
vedúci oddelenia informatiky,
Národný ústav pľúcnych chorôb Vyšné Hágy

Rýchle a unáhlené rozhodnutia pri ochrane spravovaného kyberpriestoru často znamenajú dlhú a tŕnistú cestu k cieľu. Začnime vždy dôslednou analýzou problému. Spolupracujme pri hľadaní najlepšieho riešenia. Nezanedbávajme a nepodceňujme bezpečnostné školenia štandardných používateľov. Priestor medzi klávesnicou a stoličkou je dlhodobo veľmi zraniteľný, často s pocitom nenahraditeľnosti.

Ivan Kopáčik,
bezpečnostný expert,
Gordias

Novela zákona o kybernetickej bezpečnosti spôsobila nástup pseudoodborníkov. Takých, čo potenciálnych klientov v prvom rade vystrašia hroziacimi sankciami. Aby im následne doslova a dopísmena fušerskými postupmi „implementovali požiadavky zákona". V praxi za takýmito „odborníkmi" ostanú zväčša iba papiere s nepoužiteľným, nezmyselným obsahom a kopa zistení v najbližšom audite kybernetickej bezpečnosti. Nedajte sa nachytať.

Aký názor má AI?

ChatGPT
V roku 2025 na Slovensku bude kľúčové vyvarovať sa laxného prístupu k ochrane dát. Pozor na phishing, falošné e-maily a weby, ktoré cielia na citlivé údaje. Zanedbanie aktualizácií softvéru otvára dvere kyberútokom. Tiež pozor na nezabezpečené cloudové služby a podozrivých dodávateľov IT riešení, ktorí môžu predstavovať skryté riziká.

Gemini
Za najväčšie výzvy považujem kombináciu phishingových útokov a zraniteľností softvéru. Ak sa k tomu pridá ešte nedostatočné zálohovanie, môže to mať pre firmu katastrofálne následky.