Kybernetické bezpečnostní incidenty: Jak jim předcházet chytře a efektivně

Počty kybernetických útoků rostou. Po celém světě a ve všech sektorech.

Stále závaznější a dražší jsou i dopady těchto útoků. Náklady na opravu, odstranění chyb systémů či aplikací, placení odškodného klientům nebo pokuty od dozorových úřadů. Náklady na opravu, odstranění chyb systémů či aplikací, placení odškodného klientům nebo pokuty od dozorových úřadů. Trend je zcela zjevný bez ohledu na to, jestli se jedná o globální obchodní společnosti, domácí výrobní podniky, úřady, samosprávu, školy či nemocnice.

S rostoucím počtem a závažností kybernetických bezpečnostních incidentů rostou i nároky na ochranu informací. Zabezpečení informačních systémů, nastavení procesů pro ochranu dat, předcházení kybernetickým incidentům a událostem. A rychlé řešení těch incidentů, kterým se organizace přeci jenom nevyhne.

Počet organizací, které budou muset informační bezpečnost řešit komplexně, jako systém, výrazně vzroste po přijetí nové EU směrnice o kybernetické bezpečnosti, tzv. NIS2. To se bude týkat rovněž nastavení pravidel a postupů pro předcházení a řízení kybernetických bezpečnostních incidentů.

Abychom na nic nezapomněli

Kvalitní a chytré řešení útoků na data (bez ohledu na jejich citlivost) vyžaduje komplexní a široký přístup. Izolované nasazení jednoho technického nástroje nebo zavedení jednotlivého organizačního či procesního opatření samo o sobě nestačí. Naopak, řešení, které nebude komplexní a úplné, může vést i k falešnému pocitu bezpečí, ačkoliv skutečnost bude jedná. Efektivní, důsledné a chytré řízení kybernetických incidentů zkrátka vyžaduje komplexní pohled a zapojení různých útvarů uvnitř dané organizace.

A právě tento komplexní přístup detailně popisuje nová publikace *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. V nakladatelství Wolters Kluwer ČR, a.s., ji vydává autorský tým pod vedením Františka Nonnemanna, dlouholetého experta na ochranu osobních údajů a compliance. Dalšími autory jsou Vlastimil Červený, zkušený manažer v oblasti informační a kybernetické bezpečnost a řízení IT rizik, a Dominik Vítek, advokát v advokátní kanceláři PIERSTONE, který se ve své praxi se zaměřuje se zejména na IT právo, právo ochrany soukromí a osobních údajů a regulaci kybernetické bezpečnosti.

3D přístup

Jak už název napovídá, publikace *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*, se zaměřuje na tři hlavní složky procesu pro předcházení a řešení kybernetických útoků.

Které to jsou?

1) IT. Ať už jde o fungování IT útvaru, informační a komunikační nástroje využívané k běžnému provozu, nebo technická opatření k ochraně informací a detekci neobvyklých událostí, publikace radí, jak IT nástroje a útvary vhodně zapojit do řízení a předcházení kybernetických incidentů.

2) Compliance. Předcházení a řešení kybernetických incidentů není jednorázovým opatřením. V praxi je nezbytné nastavená opatření a kontroly vnímat jako jednotný systém, resp. cyklus, který musí být přizpůsobený podmínkám každé organizace, jejím zákonným povinnostem i provozním potřebám, a také pravidelně hodnocen a upravován. Samostatnou součástí je pak

proces pro řízení jednotlivých kybernetických incidentů, který je v publikaci rovněž detailně popsán.

3) Právo. Útoky na interní informace, jejich únik, ztráta, nedostupnost i narušení integrity mají řadu právních souvislostí. Začít můžeme od pravidel kybernetické bezpečnosti, která se v České republice s novou směrnicí NIS2 brzy rozšíří na tisíce společností, nebo pravidla pro zpracování osobních údajů, která již dnes dopadají prakticky na každý úřad, obec i obchodní či výrobní podnik. Právních souvislostí, které monografie analyzuje, je však daleko více, od některých sektorových úprav (telekomunikace, platební služby), přes autorské právo či monitoring zaměstnanců až po připravovanou právní úpravu hromadných žalob.

Praktický návod pro řešení kybernetických incidentů

Kniha *Kybernetický bezpečnostní incident 3D: IT, právo a compliance* je psána jako praktický návod. Popisuje vhodná opatření k řízení kybernetických incidentů z technického, právního i procesního pohledu. Opatření a postupy nejenže popisuje, ale i radí, jak je nastavit v nezbytném a přiměřeném rozsahu, jak využít další zdroje informací a zavedené procesy v každé organizaci a co všechno je vhodné či možné dále zohlednit.

Jinak řečeno, poradí, jak kybernetické incidenty řídit chytře, efektivně a přiměřeně.

Kdy se to může hodit

Situací, ve kterých se návod na chytré předcházení a řešení incidentů může hodit, je celá řada. Ať už organizace řeší zavedení nového systému pro řízení kybernetických incidentů, chce si ověřit stav a funkčnost historicky zavedených opatření, nebo se připravuje na novou legislativu či certifikaci, ve všech těchto situacích a případech jí publikace *Kybernetický bezpečnostní incident 3D: IT, právo a compliance* pomůže.

S čím vám tato nová kniha v praxi pomůže?

1) Mapování opatření k ochraně informací a řízení incidentů a posouzení, jestli vám některé zásadní opatření nechybí
2) Hodnocení bezpečnostní opatření v širších souvislostí správy a vývoje ICT, finančního plánování a procesního řízení
3) Nastavení proces pro řízení kybernetických incidentů takovým způsobem, aby se informace o incidentech včas dostali k odpovědným pracovníků, aby je řešili efektivně a využili je pro vylepšení svých postupů do budoucna
4) Posouzení, jakým způsobem v podmínkách konkrétní organizace nastavit přiměřený a odpovídající compliance systém, spravovat informační aktiva a řídit rizika
5) Kontrola, jestli plníte všechny právní povinnosti, které na vaši organizaci při předcházení a řízení kybernetických incidentů dopadají
6) Zmapování další právní souvislosti, které jste dosud neřešili, a zorientovat se v připravovaných předpisech, které budou mít na řízení kybernetických incidentů bezprostřední vliv
7) Rozhodnutí, zda a kterou normu pro řízení kybernetických incidentů je ve vašem případě vhodné implementovat

A kdy se hackeři zaměří na vás?

Po útočníka může být zajímavá úplně každá organizace. Kvůli svému know-how, databázi klientů, konkurenčnímu boji, kvůli snaze získat výkupné nebo při politicky motivovaném útoku a snaze omezit výkon veřejných služeb a činnost státu.

Otázka tedy nezní, zda bude vaše organizace cílem kybernetického útoku, ale kdy se tak stane a do jaké míry bude útok úspěšný. V publikaci *Kybernetický bezpečnostní incident 3D: IT, právo a compliance* naleznete praktický návod, jak se na tuto situaci připravit a útok vyřešit s co nejmenšími náklady a dopadem na vaši organizaci, klienty, dodavatele i zaměstnance.