e-PRŮVODCE KYBERBEZPEČNOSTÍ

CHYTRÝ MĚSÍČNÍK PRO BEZPEČNOST VAŠÍ FIRMY | **UKÁZKOVÉ ČÍSLO**

Zákon o kyberbezpečnosti schválen: Nová pravidla krok za krokem

Nový zákon o kybernetické bezpečnosti je schválený a už ho nemůže nic zastavit. Účinný bude s největší pravděpodobností od 1. října 2025. Firmy a organizace tak čekají desítky povinností, ale nepanikařte: poradíme vám 5 základních kroků, jak začít.

Jaké povinnosti nová regulace přináší?

Připravovaná legislativa o kyberbezpečnosti přináší komplexní soubor povinností, které mají zajistit vyšší úroveň ochrany organizací před kybernetickými hrozbami. Mezi klíčové povinnosti v novém zákoně NZKB patří:

- registrace regulovaných služeb, § 6: organizace musí registrovat své regulované služby do 60 dnů od splnění identifikačních kritérií, respektive účinnosti NZKB;
- hlášení kontaktních a dalších údajů, § 11: povinnost hlásit kontaktní údaje a jejich změny – nové údaje do 30 dnů, změny do 14 dnů;
- stanovení rozsahu řízení kybernetické bezpečnosti, § 12: organizace musí určit rozsah, ve kterém řeší kybernetickou bezpečnost; pokud jej neurčí, automaticky se předpokládá, že se požadavky regulace vztahují na celou organizaci;
- zavádění bezpečnostních opatření, § 13: organizace musí implementovat bezpečnostní opatření v souladu s předepsaným režimem vyšších či nižších povinností do jednoho roku od oznámení o zařazení do evidence;
- hlášení kybernetických bezpečnostních incidentů, § 15: povinnost hlásit incidenty podle jejich závažnosti a režimu příslušným orgánům veřejné moci;
- reaktivní protiopatření, § 20: organizace musí okamžitě reagovat na varování či reaktivní opatření stanovená Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB).

Jak začít a úspěšně provést adaptační projekt?

Úspěšná adaptace na požadavky nové legislativy vyžaduje pragmatický, systematický a promyšlený přístup. Na základě našich dosavadních zkušeností se zaváděním požadavků kybernetické bezpečnosti do praxe doporučujeme v adaptačním projektu postupovat v následujících krocích:

1. Expoziční analýza
2. Zmapování aktuálního stavu a slabin
3. Stanovení priorit a plánu adaptace
4. Implementace opatření
5. Kontinuální zlepšování

Expoziční analýza aneb Neskákej do neznámé vody

Expoziční analýza představuje první krok k určení, zda a v jakém rozsahu se nová legislativa o kybernetické bezpečnosti na vaši organizaci vztahuje. Daný proces zahrnuje systematické posouzení vašich obchodních a provozních procesů podle kritérií stanovených regulací. Analýza je klíčová pro pochopení, které povinnosti se vás týkají a jaký režim opatření – vyšší, nebo nižší – na vaši organizaci dopadá.

Projděte si kritéria podle směrnice NIS2, jež zahrnují věcná a velikostní hlediska (např. počet zaměstnanců, hodnota aktiv či kumulovaný obrat za uplynulé období), a posuďte význam vašich služeb pro společnost. Na základě analýzy můžete rozhodnout, zda na vás dopadá vyšší, nebo nižší režim povinností. Vyšší režim znamená jejich širší rozsah a odpovídá přibližně povinnostem, které mají povinné osoby podle stávajícího zákona o kybernetické bezpečnosti a jeho prováděcí vyhlášky. Oproti tomu nižší režim se zaměřuje pouze na základní opatření počítačové hygieny a bezpečnosti. V tomto kroku vám může částečně pomoci „kalkulačka" dostupná na portal.nukib.gov.cz.

Vedle směrnice NIS2 doporučujeme zároveň posoudit, zda na vás nedopadá i další relevantní regulace v oblasti digitální provozní odolnosti a informační a kybernetické bezpečnosti:

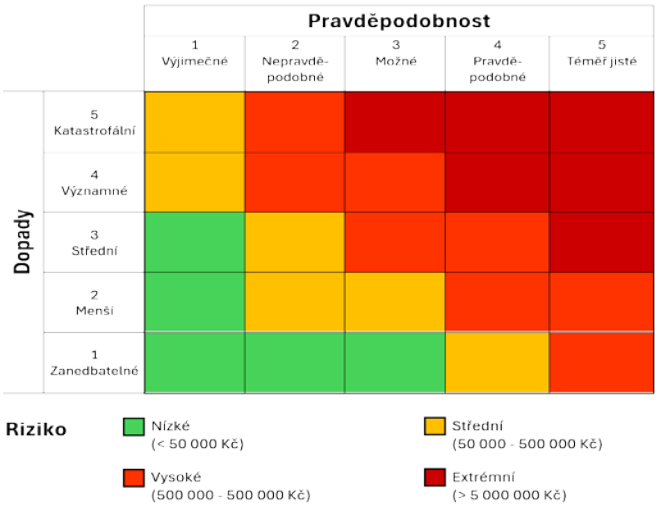
- nařízení DORA neboli Digital Operational Resilience Act pro finanční instituce a jejich ICT dodavatele;
- směrnice CER alias Critical Entities Resilience pro subjekty kritické infrastruktury;
- nařízení CRA čili Cyber Resilience Act a nařízení AIA neboli Artificial Intelligence Act pro organizace uvádějící na trh chytré produkty či služby s digitálními prvky nebo spojené s umělou inteligencí.

Zmapování aktuálního stavu a slabin aneb Kde nám protéká střecha

Další krok při adaptaci na novou legislativu tvoří důkladné zmapování aktuálního stavu organizace v oblasti kybernetické bezpečnosti. Zmíněný proces zahrnuje nejen pochopení současného nastavení, ale také identifikaci slabin a rizik, jež je nutné řešit, aby organizace splnila požadavky nové legislativy. Popsaný krok zahrnuje následující položky:

- přehled aktiv organizace: identifikujte všechna důležitá aktiva organizace, která mají význam z hlediska kybernetické bezpečnosti; patří mezi ně fyzická aktiva (servery, počítače, síťová zařízení a jiné technologické celky), digitální aktiva (data, informační systémy, softwarové aplikace) i lidské zdroje (klíčoví pracovníci a jejich role);
- analýza rizik: analyzujte svá rizika a určete, jaké kyberbezpečností hrozby nejvíce ohrožují vaši organizaci; zvažte pravděpodobnost jejich výskytu i jejich dopad;
- dokumentace stávajících opatření: zhodnoťte a zdokumentujte stávající bezpečnostní opatření a procesy; zaměřte se na technická opatření (fyzická a síťová bezpečnost, správa identit) i organizační opatření (bezpečnostní politiky, školení zaměstnanců);
- GAP analýza: porovnejte stávající stav bezpečnostních opatření, procesů a evidencí s požadavky nové legislativy; identifikujte mezery neboli „gaps", které je nutné zaplnit.

Společným výsledkem popsaných aktivit by se měl stát dostatečně podrobný přehled o aktuálním stavu kybernetické bezpečnosti, identifikovaných slabinách a rizicích organizace a o konkrétních oblastech, jež vyžadují zlepšení. Uvedené informace poslouží jako základ pro plánování a implementaci adaptačních opatření.



Přehled v organizaci
- Jaké vykonávám agendy a poskytuji služby?
- Co pro výkon těchto agend potřebuji?
- Z toho vyplývá rozsah, ve kterém KB řeším.

Aktuální stav KB
- Mám již zavedena některá opatření?
- Zdokumentuji aktuální stav zavedených a chybějících opatření.

Určení priorit
- Jaké mám finanční a personální kapacity?
- Co je má prioritní služba?
- Provedu analýzy, stanovím plán se zohledněním kapacity a priorit.

Zavádění opatření
- Určím osobu odpovědnou za KB.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Vytvořím bezpečnostní politiku, kterou lze v praxi reálně používat.
- Pokračuji dle plánu.

Stanovení priorit a plánu adaptace aneb Dvakrát měř, jednou řež

Stanovení priorit znamená klíčový krok adaptačního projektu, který vychází z důkladného zmapování stávajícího stavu organizace, provedení GAP analýzy a analýzy rizik. Na základě popsaných zjištění je dále třeba zohlednit finanční a personální kapacity organizace, identifikovat nejkritičtější služby, procesy a oblasti, jež vyžadují okamžitou pozornost, a stanovit proveditelný plán pro zavádění opatření. I NÚKIB ve svých výstupech uvádí, že právě realistický plán je pro dlouhodobý rozvoj souladu organizace s kyberbezpečnostní regulací důležitý.

Implementace opatření aneb Řízni pořádně!

Implementace opatření vychází z prioritizovaného plánu a je „akčním" krokem k dosažení souladu s požadavky legislativy a ke zvýšení celkové kybernetické bezpečnosti organizace. Mezi klíčové kroky implementace patří:

- zavedení technických a organizačních opatření: zajistěte fyzickou a technickou bezpečnost (ochrana sítí, řízení přístupu, šifrování dat);
- určení odpovědnosti: jmenujte osobu odpovědnou za kybernetickou bezpečnost (CISO nebo jiný klíčový pracovník); rozdělte odpovědnosti mezi jednotlivé členy týmu podle jejich kompetencí;
- příprava dokumentace: vypracujte potřebné politiky, postupy a další podklady, které poslouží jako základní rámec pro řízení kybernetické bezpečnosti; patří sem například bezpečnostní politika, plány řízení incidentů nebo metodiky řízení rizik či dodavatelského řetězce;
- řízení dodavatelů: řízení dodavatelského řetězce tvoří klíčovou součást kybernetické bezpečnosti organizace a zahrnuje nastavení minimálních smluvních standardů, jasné rozdělení odpovědností a zavedení bezpečnostních záruk pro dodavatele; doporučuje se využívat precertifikace a ověřování dodavatelů, aby se zajistilo, že splňují požadované standardy; součástí řízení by mělo být i pravidelné hodnocení bezpečnostních rizik spojených s dodavateli a případná revize smluv;
- vzdělávání a školení: proškolte všechny zaměstnance, včetně vrcholového managementu, aby rozuměli své roli v oblasti kybernetické bezpečnosti; zajistěte pravidelnou osvětu o základních principech kybernetické hygieny a ochraně proti nejčastějším hrozbám;

- testování a audit: pravidelně testujte účinnost zavedených opatření pomocí auditů, penetračních testů a simulací kybernetických útoků; provádějte průběžné hodnocení, abyste zajistili, že opatření odpovídají aktuálním hrozbám;

Při zavádění opatření postupujte podle stanoveného plánu a priorit a nenechte se rozptylovat nahodilými událostmi ani přemírou pozornosti, které se nyní oblasti kybernetické bezpečnosti pochopitelně dostává. Složitější či nákladnější kroky realizujte postupně, podle plánu, aby nedošlo k přetížení organizačních kapacit.

Kontinuální zlepšování aneb Neusnout na vavřínech

Jednorázovou implementací zavádění opatření nekončí. Kybernetická bezpečnost představuje dynamickou oblast, která vyžaduje průběžnou aktualizaci a přizpůsobování se novým hrozbám i požadavkům.

Doporučení na závěr

- Neotálejte s přípravou, ale přistupujte k ní rozumně. Při implementaci opatření se řiďte zásadou přiměřenosti – náklady na bezpečnostní opatření by neměly převyšovat náklady spojené s mitigací nebo eliminací rizik.
- Kyberbezpečnost organizace vyžaduje nepochybně významné investice úsilí a času. Nejde však o neřešitelný problém – většinu základních kroků zvládnete sami, aniž byste potřebovali zásadní externí pomoc. Současně platí, že není nutné řešit vše najednou. Postupné zavádění opatření přitom zajistí efektivitu i udržitelnost celého procesu. Pečlivé plánování a správné stanovení priorit vám umožní efektivně implementovat požadavky nové legislativy a zajistit tak ochranu vašich dat, systémů a procesů.
- Nezapomínejte však, že kybernetická bezpečnost neznamená jen splnění legislativních požadavků. Hlavním přínosem je ochrana samotné organizace, její stability, důvěryhodnosti a kontinuity podnikání. Investice do kyberbezpečnosti se tak stává významným benefitem, který posiluje nejen odolnost vůči hrozbám, ale také konkurenční výhodu na trhu.

Mgr. Ing. Petra Věžníková, JUDr. Ing. Jindřich Kalíšek, Ph.D.
experti v oblasti kybernetické bezpečnosti

LEGISLATIVNÍ NÁLOŽ V KYBERBEZPEČNOSTI: NOVÝ ZÁKON, NOVÉ HROZBY, VAŠE ODPOVĚDNOST

Nový zákon o kyberbezpečnosti startuje od 1. 10. 2025 – dožeňte kybernetickou bezpečnost vaší firmy

Termín: 16. 10. 2025

Místo konání: Praha, Hotel Olympik

Od 1. října 2025 vstupuje v účinnost nový zákon o kybernetické bezpečnosti. Zasáhne firemní procesy, IT systémy, smluvní vztahy i každodenní práci zaměstnanců. Přináší nové povinnosti pro vedení, IT i dodavatele – a vysoké sankce za jejich nesplnění.

- Víte, která bezpečnostní opatření musíte zavést?
- Jste připraveni doložit řízení kyberrizik při kontrole?
- Máte plán, jak proškolit zaměstnance a řídit incidenty?
- Víte, co (ne)sdílet s umělou inteligencí?

Cílem konference je připravit firmy na účinnost nového zákona o kybernetické bezpečnosti. Účastníkům nabídne praktický přehled povinností, které musí splnit vedení, IT týmy i zaměstnanci, a ukáže, jak zákon proměňuje firemní procesy i odpovědnost. Konference propojí legislativní rámec s reálnými dopady a nabídne konkrétní návody, jak zvládnout přechod na nový režim bezpečnosti.

TÉMATA KONFERENCE:

- Nový zákon o kybernetické bezpečnosti 2025 a jeho dopady
- 1. linie: IT manažeři, manažeři kyberbezpečnosti = kyberzákon v praxi
- 2. linie: Vedoucí zaměstnanci, management = hlavní odpovědnost
- 3. linie: Váš zaměstnanec = nejslabší článek firmy
- **BONUS:** AI jako hrozba pro kybernetickou bezpečnost

Přijďte na odbornou konferenci, která vám pomůže zorientovat se v nové legislativě a přenést požadavky zákona do praxe.

Na konferenci se můžete přihlásit ZDE.

PORADNA

Jsme 3 firmy, kdy každá firma má svoje vlastní IČO, ale všechny tři mají společné DIČ a určitou provázanost (první firma-malá vyrábí dřevěná okna a dveře, druhá-malá prodává a třetí je majitel budov a strojů a na střeše má FVE s výkonem 168 kW bez baterií-licencovaná). Poslední firma je mikrofirma s 10 zaměstnanci a podle obratu spadla do kybernetického zákona. Musí se nahlásit na NÚKIB pouze tato firma, nebo všechny 3 firmy díky provázanosti?

V první řadě je nutné blízce sledovat dění okolo návrhů prováděcích předpisů a ověřit, zda skutečně v jejich finální podobě budete regulovaným subjektem podle nového ZKB.

Aktuální podoba návrhu vyhlášky o regulovaných službách (tj. z května 2025 před zapracováním připomínek) pracuje u služby Výroba elektřiny (2.1) s podmínkou instalovaného elektrického výkonu výrobny elektřiny z obnovitelných zdrojů nad 1 MW.

Tato podmínka vychází z energetického zákona, který výrobu elektřiny ve výrobnách elektřiny z obnovitelných zdrojů energie s výkonem nad 1 MW považuje za činnost uskutečňovanou ve veřejném zájmu, což představuje hranici, od které již výrobna může významným způsobem přispívat k výrobě a dodávkám elektřiny spotřebitelům – a tedy, může mít dopad na distribuční (resp. elektrizační) soustavu.

NÚKIB – po konzultaci s ERÚ – v tomto ohledu argumentuje, že vyloučení menších výrobců je v souladu s požadavky směrnice NIS 2, která míří na největší producenty elektřiny, u nichž je výroba elektrické energie hlavní podnikatelskou činností. Zároveň také pracuje s předpokladem, že rizika spojená s malými zdroji jsou obvykle řešena již ve fázi připojování k distribuční soustavě.

V případě, že by se třetí firma dle finální verze vyhlášky poskytovatelem regulované služby i přesto stala, pak by se ohlašovací (ad.) povinnosti týkaly primárně této entity.

Samotná provázanost firem hraje roli zejména v prvotním určení regulované služby – tzn. slouží k prevenci účelného vyčleňování regulovaných služeb z organizací prostřednictvím zahrnutí podílů tzv. partnerských a propojených podniků při určení velikosti podniku.

Návrh zákona v tomto ohledu pracuje s metodologií stanovenou v doporučení Komise 2003/361/ES, který definuje partnerské a propojené podniky prostřednictvím podílů základního kapitálu nebo hlasovacích práv.

Zároveň však NÚKIB v návrhu zákona – a to odlišně od úpravy NIS 2 – poskytuje několik výjimek. Jedna z těchto se týká osob, které nesdílí technická aktiva. Konkrétně dle § 7 c) zákona: „za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od technických aktiv, která používá posuzovaná osoba při poskytování regulované služby."

Určitou míru povinností by ostatní podniky měly v případě, že by byly pro poslední firmu např. „významným dodavatelem" IT služeb. Nicméně i tato situace by zakládala zejména povinnostem na smluvní a bezpečnostní opatření mezi vašimi firmami, nikoliv vůči NÚKIB dle zákona. Z vašeho popisu však odvozuji, že se případně může jednat o situaci spíše opačnou.

Pro úplnost je však nutné dodat, že v případě, že by třetí firma poskytovala IT (nebo i bezpečnostní) služby vašim ostatním firmám, pak je potřeba ověřit, zda nenaplní definici některé z těchto regulovaných služeb: Poskytování služby cloud computingu (16.8), Poskytování služby datového centra (16.9), či Poskytování řízené (bezpečnostní) služby (tzv. „Managed (security) service provider", body 16.13 a 16.14).

Michael Bátrla
expert na kybernetickou bezpečnost

5 největších kyberhrozeb pro vaši firmu v roce 2025

Hackerské útoky na firmy jsou už na denním pořádku. Problém ale je, že jsou díky AI stále vynalézavější! Na co si dát pozor? Jak se bránit?

Vstupujeme do období, kdy jsou kybernetické útoky nejen stále častější, ale i sofistikovanější. Digitalizace, práce na dálku, propojení systémů a raketový rozvoj umělé inteligence posouvají laťku kyberbezpečnosti výše než kdy dřív, neboť díky AI jsou útočníci mnohem rychlejší, schopnější a dokážou útoky mnohem lépe cílit. Na to musejí reagovat české i světové firmy, které jsou tak nuceny vynakládat větší úsilí i prostředky.

V tomto článku se zaměřujeme na pět kyberhrozeb, jež umělá inteligence ovlivnila. Seznam nebezpečí tak rozhodně není úplný, nicméně v těchto případech spatřujeme významné změny, na které je třeba reagovat. Inspirujeme se reálnými doklady z praxe a upozorňujeme na nejčastější chyby i na možnosti obrany.

1. Dvojité vydírání: „Zaplaťte, nebo všechno zveřejníme!“

Ransomware prošel značným vývojem a běžnou součástí útoků je nejen zašifrování dat, ale i stažení a následně zveřejnění údajů na darknetu v případě, že oběť vydírání nezaplatí. Vznikají celé služby „Ransomware-as-a-Service“, kde si útok může objednat kdokoliv, případně si jen pronajmout nástroj, jehož dodavatel bere část „zisku“. Výjimečné nejsou ani „akční nabídky“, tj. při rychlém jednání sleva. AI může pomáhat s celou řadou oblastí, od automatizované identifikace zranitelností přes analýzu získaných dat po asistenci při vývoji sofistikovanějších řešení. Řada programátorů dnes AI využívá a platí to i pro vývojáře vyděračského softwaru.

Firmy, které při útoku odmítly platit výkupné a měly funkční zálohování, se v praxi mnohdy zotavily rychleji než ty, jež výkupné zaplatily. Mimoto platba nezaručuje obnovu dat ani to, že je útočníci nezveřejní.

Příklady z praxe:
Netřeba připomínat nemocnici v Benešově, která v roce 2020 utrpěla škodu přes 59 milionů korun, ani útok na slovenský katastr. Ten byl obzvláště nebezpečný, neboť velmi negativně ovlivnil trh s nemovitostmi na Slovensku a důvěru občanů v kybernetickou bezpečnost veřejných institucí. Nicméně možné zveřejnění údajů na darknetu si do médií najde cestu vždy či skoro vždy, takže je ohrožena i reputace mnohem méně významných institucí (viz články o útoku na Správu služeb hlavního města Prahy). Ztráta reputace bolí a vyděrači to dobře vědí.

Jaké chyby firmy nejčastěji dělají?
- Nevyužívají offline zálohy – doporučuje se část záloh provádět „ručně“ a nespoléhat jen na automatizované systémy.
- Zálohovací systém je dostupný zevnitř sítě, a útočník jej tak rovněž zašifruje.
- Neexistují pravidla pro odpojení automatického zálohování v případě útoku. Nezašifrovaná data v záloze se tak přepíšou zašifrovanými daty, protože zálohovací systém nikdo neodpojil.
- Nedostatečné či žádné vyhodnocování nestandardních aktivit v síti.
- Nedostatečná segmentace sítě – útočník po průniku do jedné části sítě snadno zasáhne další oddělení i zálohovací systémy. Cíleně jsou vyhledávány servery pro dohled nad sítí a dalšími systémy.
- Školení zaměstnanců je povrchní nebo jednorázové.

Doporučení:
- Uchovávejte minimálně jednu zálohu zcela odděleně od produkční sítě (tzv. air-gap). Skvělý je princip 3-2-1, tedy tři zálohy, dvě různá zařízení a jedna záloha v jiné lokalitě. Lze jej přitom samozřejmě ještě vylepšit.
- Pravidelně testujte obnovu dat, nejen samotné zálohování. Není nic horšího než zjistit, že jsou vaše zálohy nedostupné.
- Segmentujte síť – například oddělte produkční, zálohovací, kancelářskou a výrobní část.
- Investujte do behaviorálních detekčních systémů, které včas odhalí neobvyklé chování v síti.
- Pravidelně a kvalitně školte zaměstnance v rozpoznávání podvodných zpráv a příloh.
- Dohledovým systémům přidělujte minimální potřebná oprávnění pro přístup k dalším serverům. Jde o častý cíl útočníků.
- Nechte si od AI pomoci: Například detekci anomálií a reakci na incidenty zvládá dnes již dobře.

2. AI v akci: Deepfake a automatizované phishingové kampaně

AI přinesla zhoršení phishingu a odborníci očekávají ještě další posun k horší-

mu, a to v relativně blízké době. Útoky jsou uvěřitelnější a jejich příprava snazší. Umělá inteligence zvládá celou řadu úkolů, od vytvoření uvěřitelné kopie stránek banky po vyhotovení videa, na němž hovoří „známá osobnost". Modely sice obsahují četné mechanismy, které brání jejich zneužití k páchání kriminální činnosti; nicméně je-li možné model stáhnout a provozovat „on-premise" (v místě), útočníci tyto bezpečnostní funkce často vypínají. Umělá inteligence jim pomáhá generovat autenticky vypadající phishingové e-maily i SMS bez gramatických chyb, uvěřitelné jsou rovněž hlasové hovory. Samozřejmě to však neznamená, že by e-maily plné gramatických chyb a nesmyslů úplně vymizely. Část útočníků cílí právě na osoby, jež se nechají nalákat na amatérsky připravený podvrh, protože dle některých názorů existuje větší pravděpodobnost, že si taková oběť těsně před cílem vše nerozmyslí a peníze podvodníkům skutečně pošle. Netřeba dlouze psát o možnostech věrného napodobení hlasu či vzhledu třetích osob, s čímž si už dnes hrají i děti. Velký problém ovšem představují výrazně propracovanější personalizované útoky, neboť AI dokáže v relativně krátkém čase vyhledat a analyzovat veřejně dostupné informace o firmě i zaměstnancích a připravit podklady pro samotný útok.

Příklady z praxe:
Před útoky typu „falešný šéf" dnes varují i banky. Ani Česku se již nevyhýbají případy, kdy naléhání od falešného šéfa vyústí v odeslání vysokých částek kamsi do ciziny.

Na co si dát pozor?

- Automatizované útoky s využitím AI mohou probíhat ve velkém rozsahu a s minimálními náklady.
- AI personalizuje obsah e-mailů podle informací z firemních webů, sociálních sítí i předchozích úniků.
- Útočníci využívají i jiné komunikační kanály než e-mail: SMS (smishing), chatovací aplikace (WhatsApp, Telegram) i hlasové hovory (vishing).
- Deepfake videa nebo hlasové hovory dokážou oklamat i zkušené zaměstnance.
- Útočníci mohou analyzovat vaši veřejnou komunikaci, internetové stránky nebo příspěvky na sociálních sítích a vytvářet přesvědčivé podvody. E-mail od „šéfa na dovolené" v době, kdy je šéf opravdu u moře, tak nepředstavuje nic neobvyklého.
- Pokud volá někdo „z banky" a požaduje převod peněz s cílem je „zachránit", pravděpodobně není z banky. Pro banku není problém zablokovat jakoukoliv podezřelou transakci.

Jak se bránit?

- Zavádějte víceúrovňové ověřování klíčových transakcí a změn (princip „čtyř očí").
- Pravidelně školte zaměstnance v rozpoznávání deepfake podvodů a neobvyklých požadavků.
- Zaveďte pravidlo „ověřuj vždy i jiným kanálem", zejména při nestandardních požadavcích na finance.
- Nastavte limity pro schvalování finančních transakcí nad určitou částku více lidmi. Další člověk nebude od útočníků „zpracovaný" a může věc včas zarazit.
- Sledujte nové technologie na detekci deepfake obsahu – některé nástroje jsou již běžně dostupné.
- Zvažte, zda je nutné zveřejňovat na sociálních sítích fotky z dovolené ještě v době, kdy jste na dovolené. Přátelům se lze pochlubit i po návratu.

Z praxe:
V Evropě se v roce 2025 rozšiřuje „voice phishing" – deepfake hovory napodobující šéfy, často kombinované s e-maily, které pravost hovoru „potvrdí". Velmi časté jsou podvodné telefonáty s podvrženým číslem volající instituce, kdy se podvodník vydává za zaměstnance ban-

ky nebo policistu. Útočníci mají často připravené velmi kvalitní „call scripty", obsahující strukturovaný průběh hovoru, možné odpovědi a další informace. Zapojení více osob – „bankéře", „policisty" a dalších – také tvoří součást scénáře.

3. Útoky na dodavatelský řetězec: Nejslabší článek rozhoduje

Propojení firem přes společné dodavatele a outsourcované služby dnes představuje realitu. Není například výjimkou, že IT společnost poskytuje služby více nemocnicím a ještě jim provozuje systémy ve svém cloudu. Útočníci to dobře vědí a mnohdy se jim vyplatí investovat do kompromitace takového dodatele nemalé úsilí, neboť se odměna násobí právě počtem klientů dané firmy. Roste i počet útoků přes kompromitované aktualizace softwaru – tzv. supply chain attacks.

Příklady z praxe:

Incident SolarWinds ukázal, že útok na jednoho významného poskytovatele softwaru může kompromitovat tisíce firem a institucí. Podobné scénáře se nevyhýbají ani Česku. Pokud je napaden například dodavatel IT služeb pro nemocnice, může výpadek v krajním případě ohrozit životy ve více zdravotnických zařízeních zároveň.

Riziková místa:

- Externisté a dodavatelé s širokými právy v místní síti.
- Nedostatečné smluvní zajištění bezpečnostních standardů.
- Chybějící monitoring aktivity třetích stran v rámci interních systémů.
- Vzdálený přístup nikoliv přes VPN.

Jak se bránit?

- Vyžadujte od všech dodavatelů jasné prokázání odpovídající úrovně kybernetické bezpečnosti. Pomáhají i standardy jako ISO 27001, nicméně dané certifikace nepřeceňujte. Pokud vám dodavatel předá šanon se slovy „tady máte tu bezpečnost", zbystřete.
- Monitorujte aktivitu partnerů a třetích stran, například pomocí SIEM nástrojů. Porovnávejte data se záznamy v administrátorském deníku a ptejte se, pokud nesedí.
- Omezte přístup třetích stran na principu nejnižších nutných práv.
- Přístup jen přes VPN znamená nutnost, ideálně s dvoufaktorovým ověřováním.
- Pravidelně auditujte dodavatelský řetězec a zařazujte kybernetickou bezpečnost do smluv.

Z praxe:

Dojde-li k napadení dodavatele, který poskytuje IT služby většímu počtu firem, a je-li třeba věc nahlásit například Úřadu pro ochranu osobních údajů, učiňte tak. S pravděpodobností hraničící s jistotou minimálně jeden z klientů napadeného dodavatele věc nahlásí a firmy, jež danou povinnost nesplní, budou mít následně co vysvětlovat.

4. Hrozby spojené s novými technologiemi: IoT, cloud, kvantové počítače

Kybernetická bezpečnost dnes nezahrnuje pouze servery a počítače:

- IoT zařízení jako chytré kamery, klimatizace, senzory či tiskárny mohou být špatně zabezpečená a tvořit i snadný vstupní bod do sítě.
- Případy neznámých komunikačních prvků byly zaznamenány dokonce v solárních panelech.
- I chytrou žárovku lze upravit a originální firmware nahradit vlastním s „funkcemi navíc".
- Rovněž cloudové služby mohou být napadeny – takových případů existuje celá řada.
- Kvantové počítače sice ještě nejsou masově dostupné, ale už nyní je potřeba sledovat vývoj postkvantové kryptografie. Firmy, které uchovávají data na desítky let (např. oblast práva, zdravotnictví), by měly být ve střehu.

Příklady z praxe:

- Téma „Harvest now, decrypt later" začíná bezpečnostní komunitou hodně rezonovat. To, že je obtížné nějakým šifrováním projít nyní, neznamená, že nebude možné data dešifrovat za pár let.
- Byla zaznamenána celá řada případů, kdy byl „modbus server" solární elektrárny volně přístupný z internetu. Zde reálně hrozí i rozsáh-

lé škody, pokud by bylo kupříkladu možné přepnout výstupní napětí či vypnout bezpečnostní ochrany.
- Hrozí rovněž úniky informací. Nenechávejte přednastavené klíče pro šifrování komunikace ani u zařízení pro dálkové odečty spotřeby a podobné technologie.
- Vzdáleně přístupné kamery byly využity i během konfliktu na Ukrajině.

Doporučení:
- Vyměňte výchozí hesla na všech IoT zařízeních a oddělte je od hlavní podnikové sítě, je-li to jen trochu možné.
- Pravidelně aktualizujte a záplatujte firmware i software.
- Sledujte a logujte přístup do cloudových služeb, nastavte princip nejnižších nutných práv.
- Průběžně sledujte trendy v oblasti postkvantové kryptografie a zapojujte se do diskuse s odborníky.
- Pravidelně provádějte bezpečnostní audity i mimo hlavní IT infrastrukturu, nevynechejte ani IoT zařízení v síti.

5. Vnitřní hrozby: Zaměstnanci, subdodavatelé atd.

Kybernetická bezpečnost je často vnímána jako obrana před útoky zvenčí, tj. před hackery, skupinami organizovaného zločinu nebo zahraničními státními aktéry. Značné riziko přitom může představovat „nepřítel uvnitř", ať už jde o stávající či bývalé zaměstnance, spolupracovníky, stážisty, nebo subdodavatele, kteří mají či měli přístup k systémům, datům nebo citlivým informacím.

Vnitřní hrozby nelze redukovat pouze na případy úmyslného poškození. Mnohdy se jedná o **neúmyslné selhání** – neopatrné nakládání s daty, obcházení pravidel, použití osobního cloudu pro pracovní účely nebo sdílení citlivých informací s externím nástrojem, který data ukládá. Lidský faktor je zkrátka jedním z nejslabších článků bezpečnostního řetězce.

Možné projevy vnitřních hrozeb:
- Chyby v nastavení oprávnění – například když mají všichni ve firmě přístup ke stejným sdíleným složkám nebo databázím bez ohledu na pracovní zařazení.
- Zbytečně rozsáhlé administrátorské přístupy – typickým příkladem je „admin pro všechny", ačkoliv uvedený přístup již naštěstí není vidět tak často.
- Nedostatečné odstraňování přístupů – bývalý zaměstnanec má ještě týdny po odchodu aktivní VPN nebo přístup do firemního e-mailu.
- Nevědomé vyzrazení informací – například nahrání zdrojového kódu do veřejného AI nástroje (kupř. čínského chatbota), který si kód uchová pro další trénování modelu.
- Úmyslné zneužití dat třeba bývalým zaměstnancem, který používá databázi klientů v další práci nebo zveřejní neveřejné dokumenty ze msty.

Příklady z praxe:
- Bývalý zaměstnanec hrozil vedení firmy, že se mohou po jeho odchodu „někde objevit nějaká data".
- Zaměstnanec požádal čínského chatbota, aby mu analyzoval zdrojový kód programu, který tvořil součást firemního know-how.
- Zaměstnanec mobilního operátora nabízel k prodeji osobní údaje klientů.

Jak se bránit?
- Pravidelně kontrolujte a revidujte přístupová práva všech uživatelů i partnerů.
- Zaveďte systém okamžitého odebrání přístupu při odchodu zaměstnanců nebo ukončení spolupráce.
- Sledujte a vyhodnocujte podezřelou aktivitu v sítích a systémech. Zejména neumožňujte hromadné exporty klientů a dokumentů; přístup k datům by měl být logován.
- Zaměstnance kvalitně proškolujte. Měli by umět rozpoznat také elektronicky podepsané PDF, do kterého někdo se zlým úmyslem přidal další revizi, a tím i obsah, aniž by elektronický podpis PDF zneplatnil.
- Zavažte zaměstnance smlouvou o mlčenlivosti; měla by však být vyvážená a dostatečně konkrétní. Nezapomeňte na výjimky, které se do takových smluv obvykle uvádějí. V případě špatně napsané NDA riskujete, že soud zmoderuje výši smluvní pokuty, nebo NDA přímo zneplatní.
- Bojujte s šedým využíváním umělé inteligence tím, že dáte zaměstnancům k dispozici AI, kterou má firma pod kontrolou.
- Budujte firemní kulturu, kde bezpečnost představuje společnou odpovědnost.

Pravidelně auditujte dodavatelský řetězec a zařazujte kybernetickou bezpečnost do smluv.

Závěr: Prevence, vzdělávání a kybernetická hygiena jako klíč k přežití

Obrana proti aktuálním kybernetickým hrozbám spočívá v kombinaci moderních technologií, neustálého vzdělávání zaměstnanců, pravidelného testování odolnosti a důsledného řízení rizik. Právě firmy, které investují do prevence a rychlé reakce na incidenty, získávají v digitálním světě zásadní konkurenční výhodu – chrání své know-how, finance i důvěru klientů.

Pamatujte, že kybernetická bezpečnost není stav, nýbrž proces. Demingův cyklus (známý také jako PDCA cyklus, Plan-Do-Check-Act) má smysl, nic lepšího dosud nikdo nevymyslel. Zároveň ovšem nezapomeňte, že zbytečné extrémy škodí. V kybernetické bezpečnosti se často snažíme právě o nalezení rovnováhy, kde ochranné mechanismy odpovídají reálným rizikům a hodnotě aktiv. Také o tom je tento časopis – méně někdy znamená více a zlatá střední cesta je optimální.

Jaromír Kuba
soudní znalec v oboru kybernetika

Nový kyberzákon pod lupou

Budete spadat do režimu vyšších, či nižších povinností? Jaké bezpečnostní opatření z toho pro vás vyplývají? Podrobně rozebíráme nový zákon i doprovodné vyhlášky.

Minimálně pro šest tisíc firem v Česku se již brzy změní kybernetická bezpečnostní pravidla hry. Nový zákon o kybernetické bezpečnosti se blíží ke konci svého dlouhého legislativního procesu. Díky změně na plovoucí datum účinnosti se ho dočkáme již tři měsíce po publikování ve Sbírce zákonů. Podle posledních odhadů Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) by k tomu mohlo dojít už letos v říjnu.

Návrh nového zákona o kybernetické bezpečnosti dosáhl po četných změnách a posunech termínů 11. června 2025 významného milníku – schválení Senátem. Nyní následuje podpis prezidenta a publikace ve Sbírce zákonů. Podle současných odhadů by měly být popsané kroky dokončeny do léta.

Zákon by tak vstoupil v účinnost letos na podzim, téměř rok po vypršení transpoziční lhůty požadované Evropskou unií. EU nyní vyvíjí tlak na zbývajících přibližně dvacet členských států, které základ nového zákona – evropskou směrnici NIS2 – dosud do svých právních řádů nezačlenily, přičemž hrozí i pokutami. Může jít o jeden z faktorů, proč by mohl zbytek procesu u nás proběhnout bez větších zdržení.

Proč je třeba nový zákon? Nestačila pouze novela, když už ČR zákon o kybernetické bezpečnosti má?

Odpověď na uvedené otázky poskytuje právě evropská směrnice NIS2, celým názvem směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, která začala platit začátkem roku 2023. Ve srovnání s předchozí verzí totiž přináší řadu významných změn a mezi ty hlavní patří: zásadní rozšíření množství regulovaných odvětví a služeb v členských státech, minimální úrovně bezpečnostních opatření a v neposlední řadě i sjednocení výše finančních sankcí, blížících se částkám známým z GDPR.

Mimo to směrnice zavádí i řadu méně známých opatření na úrovni EU, kupříkladu pro společné posuzování rizik v dodavatelském řetězci, usnadnění mezinárodní spolupráce nebo lhůty pro oznamování a nástroje koordinace řešení kybernetických incidentů s přeshraničními dopady.

Kromě směrnice NIS2 přihlédl NÚKIB při tvorbě nového zákona také ke zkušenostem z implementace zákona předchozího, a proto je česká úprava v některých ohledech rozsáhlejší, konkrétnější i přísnější.

Koho se zákon dotkne? Jak to zjistím?

Směrnice i zákon pracují se dvěma kategoriemi tzv. regulovaných subjektů. Směrnice používá pojmy základní subjekty *(essential)* a důležité subjekty *(important)*, přičemž v překladu může být poněkud matoucí, že „základní" mají ve skutečnosti vyšší míru důležitosti a přísnější požadavky. Proto NÚKIB v českém zákoně používá jasnější označení subjekty v *režimu vyšších povinností* (pro základní) a subjekty v *režimu nižších povinností* (pro důležité).

Odpověď na otázku, zda a do jaké kategorie bude organizace spadat, poskytuje vyhláška o regulovaných službách, která tvoří součást balíčku nového zákona.

Klíčový koncept nového zákona představuje tzv. samoidentifikace. Je tedy na subjektech, aby samy – případně po konzultaci s NÚKIB v případě nejasností – vyhodnotily, zda naplňují kritéria regulované služby, a oznámily danou skutečnost Úřadu. Pokud tak neučiní, vystavují se možným postihům.

Do vyššího režimu spadají podniky s více než 250 zaměstnanci nebo s obratem nad 50 mil. eur.

Prvním krokem je určení služby podle příslušného seznamu. Vyhláška definuje služby ve 22 odvětvích, od finančního sektoru (kde mj. figuruje nové nařízení DORA jako lex specialis) a energetiky přes digitální infrastrukturu a služby až po obranný či vesmírný průmysl.

Pokud organizace některou z těchto služeb provozuje, následuje určení dle velikosti organizace. Použitá metoda vychází z Doporučení Komise 2003/361/ES ze dne 6. května 2003, o definici mikropodniků a malých a středních podniků, jež kategorizuje organizace podle počtu zaměstnanců a ročního obratu.

Do vyššího režimu spadají podniky s více než 250 zaměstnanci nebo s obratem nad 50 mil. eur (příp. s rozvahou

Přímo k zákonu náležejí vyhlášky o:

- regulovaných službách;
- bezpečnostních opatřeních – vyšší režim;
- bezpečnostních opatřeních – nižší režim;
- Portálu Úřadu a požadavcích na vybrané úkony.

K doprovodnému zákonu náležejí vyhlášky o:

- bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu;
- bezpečnostních úrovních informačních systémů veřejné správy.

Vyhlášky též vstoupily v polovině května 2025 do svého legislativního procesu, konkrétně do meziresortního připomínkového řízení.

nad 43 mil. eur). Do nižšího režimu patří organizace s více než 50 zaměstnanci nebo s obratem nad 10 mil. eur. Každá organizace má přitom pouze jedno určení režimu: Jestliže provozuje více služeb, odvozuje se výsledný režim od nejvýše určené služby.

Metodika zahrnuje do celkového součtu i partnerské a propojené podniky. Směrnice i zákon jdou popsaným přístupem proti účelovému vyčleňování organizací okolo služeb pro snížení či absenci naplnění podmínek. Aktuální česká úprava však obsahuje jedno zmírnění: Za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od těch používaných posuzovanou osobou při poskytování regulované služby.

Vyhláška upravuje konkrétní kritéria pro specifické služby, která je nutné zohlednit, například:

- Poskytovatel služby cloud computingu střední velikosti bude pravděpodobně zařazen do nižšího režimu. Pokud by však byl poskytovatelem služeb cloud computingu pro orgány veřejné správy, bude spadat do režimu vyššího.
- Podnik zabývající se průmyslovou výrobou, zpracováním či velkoobchodní distribucí potravin bude nejspíše zařazen do režimu nižších povinností – bez ohledu na to, zda se jedná o podnik velký, nebo střední.

Úřad by měl také disponovat zákonnou pravomocí zařadit organizaci mezi regulované subjekty nebo ji přesunout z nižšího do vyššího režimu i bez splnění velikostních kritérií. Takové rozhodnutí by mělo zohlednit význam organizace pro společnost, ekonomiku, dané odvětví či potenciální přeshraniční dopady.

Zároveň existuje zvláštní nepočetná kategorie strategicky významných služeb, na kterou budou dopadat zejména požadavky na řízení bezpečnosti dodavatelského řetězce. Ačkoliv šlo v minulosti o mediálně atraktivní téma, naprosté většiny organizací se tato specifická opatření netýkají.

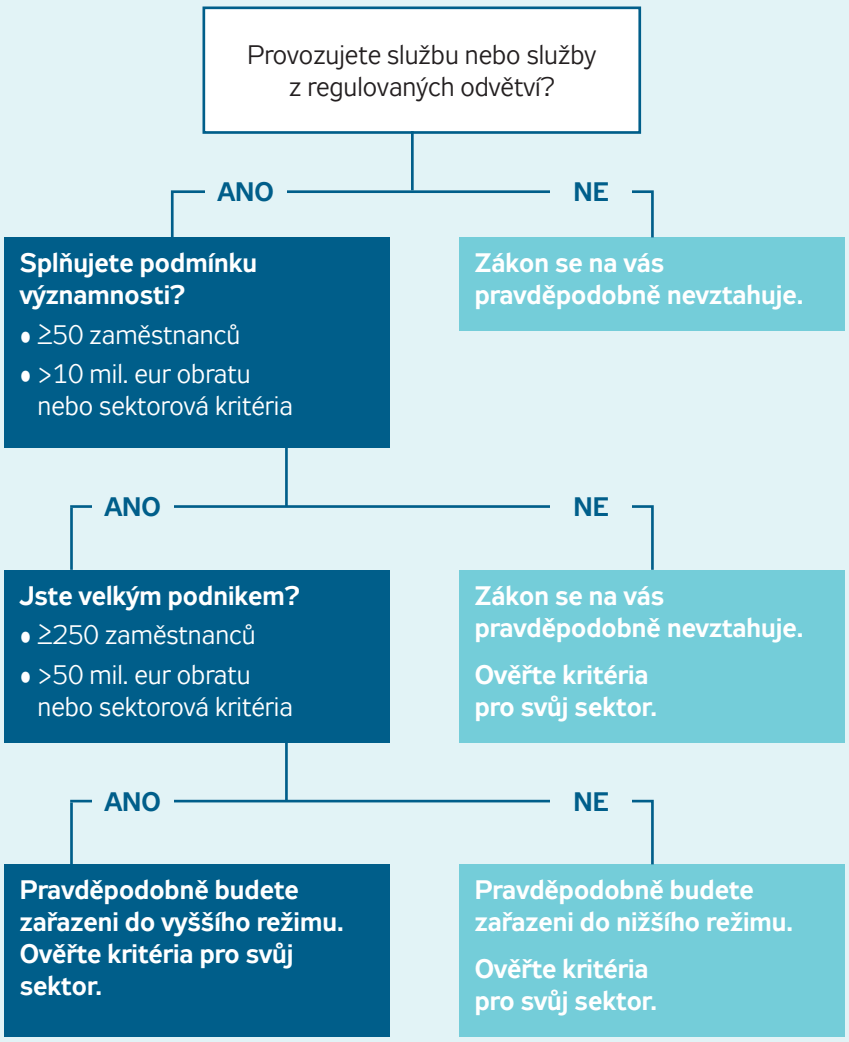
Jaké povinnosti zákon organizacím přináší?

Vůbec první povinností je výše zmíněná *samoidentifikace* regulovaných subjektů a jejich ohlášení NÚKIB, a to ve lhůtě 60 dnů od naplnění podmínek pro registraci. Pro většinu subjektů poběží daná lhůta od data účinnosti zákona.

Ohlášení se provede prostřednictvím standardizovaného elektronického formuláře na Portále NÚKIB, jenž bude fungovat jako hlavní komunikační kanál mezi regulovanými subjekty a Úřadem – a to nejen pro registraci, ale i pro další úkony, jako je hlášení kontaktních údajů či kybernetických incidentů. NÚKIB bude Portál využívat rovněž k průběžnému informování o hrozbách a zranitelnostech.

Další společnou povinnost představuje určení všech primárních aktiv. Z nich se vyberou aktiva související s poskytováním regulované služby a následně

Rychlý test: Spadáte pod zákon?



ně se k nim určí podpůrná aktiva. Uvedený přehled poslouží jako základ pro analýzu rizik a stanovení bezpečnostních opatření k zajištění nezbytné míry kybernetické bezpečnosti regulované služby.

Jak se liší povinnosti a opatření v nižším a vyšším režimu?

Návrh zákona rozděluje bezpečnostní opatření na organizační a technická. Právě v této oblasti se nejvýrazněji liší míra povinností mezi vyšším a nižším režimem. Vyšší režim vyžaduje celkem 25 opatření, zatímco nižší pouze 13. Rozdíl tkví také v tom, která opatření jsou povinná vždy a která se určují na základě analýzy rizik a zajištění nezbytné míry bezpečnosti služby.

U nižšího režimu patří mezi povinné součásti především zavedení procesů systému řízení bezpečnosti informací (ISMS), řízení rizik a bezpečnostní dokumentace. Vyšší režim navíc definuje konkrétní opatření: například požadavky na vrcholné vedení, bezpečnost lidských zdrojů, řízení kontinuity a řešení kybernetických bezpečnostních incidentů. Stanovuje také přísnější systém výběru a dokumentace opatření – zavedených, plánovaných i nezavedených – včetně jejich odůvodnění. V neposlední řadě se liší ohlašovací povinnost u kybernetických bezpečnostních incidentů nebo předpokládané množství či úroveň detailu dohledu NÚKIB.

Zákon s vyhláškami je v rozsahu opatření poměrně přesný a preskriptivní, zejména co se týče implementace specifických technologií a nástrojů. Podle aktuální úrovně kybernetické bezpečnosti a velikosti organizace mohou implementační projekty trvat několik měsíců a vyžadovat značné finanční investice.

Je však důležité si uvědomit, že se nový zákon netýká pouze technologických řešení. Nelze jednoduše nakoupit „zázračné“ nástroje, které by soulad se zákonem zajistily. Jde především o systematické zavedení a důsledné uplatňování řízení bezpečnosti, se všemi souvisejícími dopady.

Zároveň je nutné zdůraznit závažnost sankcí za přestupky proti zákonu. Finanční postihy za některé z nich mohou nově dosahovat až 250 mil. Kč nebo 2% čistého celosvětového ročního obratu pro poskytovatele služby ve vyšším režimu či strategicky významné služby. Pro nižší režim je strop postihu nižší, avšak stále značný: až 175 mil. Kč nebo 1,4% celosvětového obratu. U vyššího režimu se také nově zavádí osobní postih formou dočasného zákazu výkonu funkce člena statutárního orgánu.

Závěrem

Nový zákon o kybernetické bezpečnosti v Česku se blíží a možná se ho dočkáme již letos na podzim. Přináší značné rozšíření regulovaných subjektů a povinnost samoidentifikace i zpřísnění bezpečnostních opatření. Zvyšuje také možné sankce až na 250 mil. Kč nebo 2% obratu, případně osobní postihy pro členy statutárních orgánů některých poskytovatelů regulovaných služeb. Je tedy rozhodně potřeba se na příchod nového zákona adekvátně připravit.

Michael Bátrla
Expert v oblasti kybernetické bezpečnosti

STÁHNĚTE SI VZOR

VZOR SMĚRNICE O KYBERNETICKÉ BEZPEČNOSTI

Kybernetické bezpečnostní minimum pro zaměstnance a spolupracovníky společnosti

1. Úvodní ustanovení

1.1. Účel a cíl směrnice

Tato směrnice stanovuje základní pravidla kybernetické bezpečnosti pro všechny zaměstnance *[název a identifikace organizace]* (organizace). Cílem směrnice je minimalizovat rizika spojená s používáním informačních technologií, ochránit citlivé informace organizace a předejít kybernetickým incidentům.

Zajištění kybernetické bezpečnosti je odpovědností každého zaměstnance. Dodržováním této směrnice přispívají zaměstnanci k bezpečnému provozu informačních systémů, ochraně dat a prevenci proti kybernetickým útokům.

1.2. Rozsah působnosti

Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky a další osoby, které využívají informační systémy organizace. Vztahuje se na veškerá zařízení, která jsou připojena k síti organizace, včetně mobilních zařízení, notebooků a pracovních stanic.

2. Bezpečnostní požadavky

2.1. Přístup k informačním systémům

- Zaměstnanec je povinen používat silné heslo pro přístup do systémů organizace.
- Heslo musí být minimálně *[počet znaků, doporučujeme nejméně 12]* znaků dlouhé a obsahovat velká i malá písmena, číslice a speciální znaky.
- Zaměstnanec nesmí sdílet své heslo s jinými osobami ani jej zapisovat na veřejně dostupná místa.
- Pokud to nastavení konkrétního systému organizace vyžaduje, zaměstnanec musí pravidelně měnit hesla, a to nejméně jednou za 90 dní.

2.2. Ochrana zařízení a dat

- Zaměstnanec musí zabezpečit pracovní stanici proti neoprávněnému přístupu (např. automatickým uzamykáním obrazovky po 5 minutách nečinnosti).
- Zaměstnanec nesmí instalovat neautorizovaný software nebo používat osobní zařízení k pracovním účelům bez schválení IT oddělením.
- Všechna zařízení musejí být pravidelně aktualizována. Zaměstnanec nesmí odkládat ani ručně vypínat pravidelné aktualizace operačního systému a softwaru.
- V případě ztráty nebo krádeže zařízení je zaměstnanec povinen neprodleně informovat IT oddělení.

2.3. Bezpečnost e-mailové komunikace

- Zaměstnanec nesmí otevírat přílohy nebo odkazy z podezřelých e-mailů.
- Zaměstnanec nesmí sdílet citlivé údaje prostřednictvím e-mailu, pokud to není nezbytné pro výkon jeho práce.
- Pokud zaměstnanec obdrží podezřelý e-mail, je povinen jej nahlásit IT oddělení.

2.4. Práce na dálku a připojení k síti

- Zaměstnanec smí pracovat na dálku pouze prostřednictvím zabezpečeného připojení (VPN).
- Zaměstnanec nesmí používat veřejné Wi-Fi sítě k přístupu do systémů organizace bez použití VPN.
- Mobilní zařízení využívaná k práci musejí být chráněna přístupovým kódem nebo biometrickou autentizací.

2.5. Bezpečné nakládání s daty

- Zaměstnanec je povinen uchovávat citlivá data pouze na schválených úložištích organizace (např. firemní cloud, síťové disky).
- Zaměstnanec nesmí ukládat pracovní soubory na osobní zařízení nebo externí úložiště bez souhlasu IT oddělení.
- Fyzické dokumenty s citlivými údaji musí být ukládány v uzamykatelných skříních a skartovány po skončení jejich platnosti.

3. Reakce na bezpečnostní incidenty
• Zaměstnanec je povinen neprodleně nahlásit jakýkoliv podezřelý incident související s kybernetickou bezpečností IT oddělení. • Mezi bezpečnostní incidenty patří zejména: — neoprávněný přístup k systémům nebo datům, zejména k osobním údajům, — podezřelá e-mailová komunikace, — únik citlivých informací, zejména osobních údajů, — narušení bezpečnosti zařízení. • Zaměstnanec nesmí zamlčovat bezpečnostní incidenty, neboť může dojít k vážným škodám pro organizaci.
4. Kontrola dodržování směrnice a sankce
• Dodržování této směrnice podléhá pravidelným kontrolám.
• Zaměstnanec je povinen absolvovat pravidelná školení v oblasti kybernetické bezpečnosti.
• Porušení této směrnice může vést k disciplinárním opatřením, včetně ukončení pracovního poměru v případě závažného porušení bezpečnostních pravidel.
5. Závěrečná ustanovení
• Tato směrnice nabývá účinnosti dnem jejího vydání.
• IT oddělení je odpovědné za její aktualizaci a školení zaměstnanců v oblasti kybernetické bezpečnosti.
• Každý zaměstnanec je povinen se s touto směrnicí seznámit a řídit se jejími ustanoveními.
Datum vydání: *[DOPLNIT]* Schválil: *[DOPLNIT]*

VZOR PROVÁDĚCÍ ZPRÁVY: VYDÁNÍ SMĚRNICE O KYBERNETICKÉ BEZPEČNOSTI

Vážení kolegové,

s rostoucím počtem kybernetických hrozeb a stále sofistikovanějšími útoky na organizace všech velikostí jsme se rozhodli zavést **Směrnici o kybernetické bezpečnosti**, která stanovuje základní pravidla a povinnosti pro všechny zaměstnance.

Cílem této směrnice je:

- zvýšit úroveň bezpečnosti v rámci organizace,
- ochránit citlivé informace a systémy před neoprávněným přístupem,
- snížit riziko kybernetických útoků a bezpečnostních incidentů,
- jasně definovat odpovědnosti a pravidla pro práci s IT systémy.

Tato směrnice je **závazná pro všechny zaměstnance**, externí spolupracovníky i dodavatele, kteří pracují s informačními systémy organizace. Obsahuje klíčová pravidla pro bezpečné používání hesel, ochranu zařízení, zabezpečenou e-mailovou komunikaci, práci na dálku a nakládání s citlivými daty.

Zároveň je zde stanovena povinnost **hlásit jakékoliv podezřelé aktivity**, které by mohly ohrozit kybernetickou bezpečnost organizace.

Prosíme všechny zaměstnance, aby se se směrnicí důkladně seznámili a řídili se jejími ustanoveními. Směrnice nabývá účinnosti dnem jejího vydání a její dodržování bude pravidelně kontrolováno.

V případě jakýchkoliv dotazů se obracejte na IT oddělení nebo osobu odpovědnou za kybernetickou bezpečnost.

Děkujeme za vaši spolupráci při ochraně naší organizace!

S pozdravem,

[Jméno odpovědné osoby]
[Funkce]
[Název organizace]

Zaměstnanec = nejslabší článek vaší firmy

Vaše největší riziko nejsou slabě zabezpečené systémy. Jsou to vaši zaměstnanci. A právě kvůli lidským (ne)úmyslným chybám mají bezpečnostní incidenty fatální dopady na celou firmu.

Kybernetická bezpečnost firem čelí stále sofistikovanějším hrozbám, ale paradoxně největší riziko často představují vlastní zaměstnanci. Podle zprávy Světového ekonomického fóra o globálních rizicích má lidský faktor podíl na 95 % kybernetických incidentů (viz weforum.org/publications/global-risks-report-2022). Verizon ve své zprávě za rok 2024 Data Breach Investigations Report (DBIR) uvádí, že 68 % narušení bezpečnosti zahrnuje neúmyslné chyby zaměstnanců (viz industryweek.com/technology-and-iiot/cybersecurity/article/55036701/employees-are-your-biggest-cybersecurity-threat). Ať už z nedbalosti, neznalosti, nebo s úmyslem poškodit – lidský faktor zůstává kritickou zranitelností. Přesto mnoho firem investuje primárně do technologií a podceňuje vzdělávání personálu. Tento rozpor představuje kritickou bezpečnostní mezeru.

Typologie vnitřních hrozeb

Zlomyslní zaměstnanci (malicious insiders)

- úmyslné poškození systémů nebo krádeže dat
- motivace: finanční zisk, pomsta, ideologie
- příklad: Edward Snowden, Chelsea Manningová

Kompromitovaní zaměstnanci (compromised insiders)

- nedobrovolná spolupráce s externími útočníky
- důvody: vydírání, infiltrace, social engineering

Nedbalí zaměstnanci (negligent insiders)

- neúmyslné bezpečnostní incidenty
- nejčastější kategorie, 60–70 % všech případů

Ověřte si, jak snadno mohou zaměstnanci naletět trikům podvodníků, a zhodnoťte jejich chování.

Rizikové pozice v organizaci

Pozice	Úroveň rizika	Hlavní rizikové faktory
IT administrátoři	vysoká	privilegovaný přístup, technické znalosti
HR specialisté	střední	přístup k osobním údajům
finanční oddělení	vysoká	přístup k finančním datům
vývojáři	střední	přístup ke zdrojovým kódům
management	vysoká	širší přístupová práva

Typy hrozeb ze strany zaměstnanců

Jak již zaznělo, zaměstnanci mohou představovat hrozbu záměrnou (např. úmyslné úniky dat) nebo neúmyslnou (např. chyby způsobené neznalostí). Hrozby tedy můžeme rozdělit do několika kategorií:

Nevědomé chyby: Nejčastější příčinou bezpečnostních incidentů jsou lidské chyby. Zaměstnanci mohou například kliknout na phishingový e-mail, sdílet citlivé informace na nezabezpečených kanálech nebo používat slabá hesla. Podle zprávy Verizon DBIR 2024 je až 68 % kybernetických útoků iniciováno sociálním inženýrstvím, které často zneužívá důvěřivost zaměstnanců.

- **Phishingové útoky:** 20 % zaměstnanců klikne na podezřelý odkaz bez ověření zdroje. Příkladem jsou podvodné e-maily maskované jako interní komunikace o změnách směn nebo mzdových příspěvcích. S nástupem umělé inteligence je kvalita phishingových e-mailů na takové úrovni, že neškolený zaměstnanec nemá šanci útok poznat.
- **Nesprávné nakládání s daty:** Účetní v jedné firmě nahradila e-mailové přílohy veřejným cloudovým úložištěm bez šifrování, což vedlo k úniku finančních výkazů.
- **Rizika generativní AI:** Zaměstnanci společnosti Samsung sdíleli s ChatGPT citlivý zdrojový kód a zápisy z jednání, které se staly součástí tréninkových dat modelu. Jedná se o tzv. shadow AI, tedy využívání umělé inteligence

zaměstnanci bez regulace ze strany zaměstnavatele.

Záměrné úniky dat: Nespokojení zaměstnanci nebo ti, kteří firmu opouštějí, mohou úmyslně vynášet citlivá data. Příkladem je případ bývalého zaměstnance velké technologické firmy, který v roce 2023 odcizil zdrojový kód a prodal ho konkurenci, což způsobilo ztráty v řádu milionů dolarů.

- **Odcházející pracovníci:** Bývalý zaměstnanec Trend Micro zneužil přístupová práva k prodeji databáze klientů konkurenci.
- **Dlouhodobé špionáže:** V případě Boeingu pracoval zaměstnanec 27 let jako čínský špion, systematicky odcizující technologická data.

Nedostatečná bezpečnostní hygiena: Riziko úniku dat zvyšuje používání osobních zařízení pro práci (BYOD, Bring Your Own Device) bez řádného zabezpečení, ignorování aktualizací softwaru nebo ukládání firemních dat na nezabezpečená cloudová úložiště.

Vnitřní hrozby (insider threats): Zaměstnanci s přístupem k citlivým systémům mohou zneužít svá oprávnění. Například v roce 2022 zaměstnanec evropské banky zneužil administrátorský přístup k odcizení osobních údajů klientů, načež je prodal na dark webu.

Infiltrace externími aktéry: Proces, při kterém osoby nebo skupiny mimo organizaci pronikají do jejího prostředí s cílem získat neoprávněný přístup k informacím či systémům, často za účelem krádeže dat, špionáže nebo narušení provozu.

- **Falešné identity:** Organizované skupiny využívají umělou inteligencí generované doklady a LinkedIn profily k získání přístupu do firemních systémů.
- **Třetí strany:** Externí vývojář AWS zneužil chybu v konfiguraci firewallu Capital One, což vedlo k úniku dat 100 milionů klientů.

Přehled základních typů hrozeb

Typ hrozby	Podíl na incidentech	Dopad
neúmyslné chyby	74 %	finanční ztráty, pokuty GDPR
úmyslné jednání	35 %	krádež know-how, poškození reputace
rizika home office	30 %	průnik malwaru, únik dat

Strategie prevence a mitigace

Strategie prevence a minimalizace rizik se odvíjí od typu organizace, její činnosti apod. Jinými slovy nelze možná opatření implementovat šablonovitě. Je třeba nejprve identifikovat rizika, zvážit jejich míru a na základě toho realizovat vhodná opatření. Mezi některá z nich se řadí:

Systematické vzdělávání

- **Simulace phishingových útoků:** Testování reakcí a okamžitá nápravná školení. Firma CDC Data doporučuje pravidelné testování kombinované s analýzou zranitelnosti IT infrastruktury.
- **Témata školení:** Rozpoznávání sociálního inženýrství, bezpečné sdílení souborů, zásady používání veřejných wi-fi, ochrana osobních údajů nebo bezpečné využívání AI v organizaci.

Technická opatření

- **Vícefaktorová autentizace (MFA):** Snižuje riziko průniku i při odcizení hesla.
- **Správci hesel:** Nástroje jako Bitwarden, LastPass či 1Password generují a ukládají komplexní hesla.
- **Implementace DLP řešení:** Data Loss Prevention (např. Safetica) pro monitorování pohybu citlivých dat nebo zabránění potenciálnímu úniku dat. Implementace DLP přímo souvisí s praktickým zavedením pravidla „need to know", tedy poskytnout zaměstnanci pouze data nezbytná k jeho práci.
- **Role-Based Access Control (RBAC):** Přidělování práv na základě rolí s pravidelnými audity těchto přístupových práv.
- **Zavedení ZTA:** Bezpečnostní model Zero Trust Architecture nepředpokládá implicitní důvěru k žádnému z uživatelů, zařízení ani službě uvnitř či vně sítě a vyžaduje průběžné ověřování identity a oprávnění ke každému požadavku na přístup k firemním zdrojům.

Organizační opatření

- **Politika „clear desk":** Důsledné vynucování pravidel (např. zamykání obrazovek).

- **Nenásilná komunikace:** Zaměstnanci musejí mít důvěru k hlášení chyby bez strachu z postihu. Studie ukazují, že firmy s otevřenou kulturou řeší incidenty čtyřikrát rychleji. Firma, která zavedla anonymní hlášení bezpečnostních incidentů, snížila dobu detekce interních hrozeb o 30 %.
- **Role vedení:** Manažeři musejí jít příkladem (např. používání MFA, účast na školeních).
- **Screening zaměstnanců:** Při nástupu do zaměstnání provést ověření digitální identity, údajů uvedených v životopise, včetně informací z předchozího zaměstnání.
- **Exit interview:** Ukončení pracovního poměru s okamžitým odebráním přístupových práv a s monitoringem aktivit před odchodem zaměstnance – zejména zkontrolovat, zda nebyly zkopírovány citlivé informace. Z uvedeného důvodu je klíčová kvalita logů aplikací evidujících činnosti a chování uživatelů v systému.

Závěr

Zaměstnanci nejsou jen hrozbou, ale i klíčem ke kybernetické odolnosti. Kombinace technologií (MFA, VPN), pravidelných školení a kultury důvěry pomohou vytvořit silnou linii obrany. Nový zákon o kybernetické bezpečnosti vycházející z NIS2 a aktualizovaná ISO/IEC 27001 kladou důraz na prevenci interních hrozeb. Vedení firmy také musí zajistit soulad s AI Aktem při implementaci generativní AI, včetně explicitního zákazu sdílení firemních dat s veřejnými jazykovými modely.

Je třeba nejprve identifikovat rizika, zvážit jejich míru a na základě toho realizovat vhodná opatření.

Firmy, které kombinují technologická řešení s kontinuálním vzděláváním a jasnými bezpečnostními politikami, dokážou redukovat riziko interních hrozeb o 60–80 %. Klíč spočívá v pochopení, že kybernetická bezpečnost není jen otázkou IT oddělení, ale celkové organizační kultury. Bez investice do vzdělání bude vaše firma trpět častějšími incidenty. Nastavte procesy, školte reálnými scénáři (např. simulace útoků) a změňte „nejslabší článek" na „první linii obrany". Proveďte penetrační testy zaměřené na sociální inženýrství kombinované s auditem chování zaměstnanců. Data z praxe ukazují, že firmy s pravidelnými testy snižují úspěšnost phishingových útoků až o 60 % za jeden rok.

Luděk Nezmar
expert na zpracování a ochranu dat

e-PRŮVODCE KYBERBEZPEČNOSTÍ | Vydavatel: Nakladatelství FORUM s.r.o. | Adresa redakce: Střelničná 1861/8a, 182 00 Praha 8 | Šéfredaktorka: Bc. Kamila Rybářová | Zákaznický servis: Štěpánka Soukupová, office@forum-media.cz, tel.: +420 251 115 576 | Jazyková redakce: Mgr. Jana Vašinová | Fotografie: www.bigstockphoto.com | Zlom časopisu: Renata Brtnická | Roční předplatné 3 990 Kč. | Objednávka předplatného: office@forum-media.cz, informace o předplatném: +420 251 115 576 | Redakční uzávěrka: 10. 6. 2025 | E-PRŮVODCE KYBERBEZPEČNOSTÍ vychází každý měsíc, celobarevný, 18-20 stran.