Z BLOGU IUSTORIA

Kyberútok nebo únik dat ve firmě: co udělat v prvních 72 hodinách

> *Zašifrované servery, výzva k výkupnému, uniklá databáze zákazníků. Co ohlásit ÚOOÚ do 72 hodin, kdy hlásit NÚKIB do 24 hodin, co pojišťovně a partnerům a proč neplatit.*

TÝM IUSTORIA

5. 11. 2026 · 12 min čtení

V pondělí ráno nejdou otevřít soubory na sdíleném disku a na obrazovkách svítí zpráva, že data jsou zašifrovaná a kam poslat výkupné. Nebo zavolá zákazník, že jeho údaje z vaší databáze někdo nabízí na internetu. První telefonát vede ke správci IT a je to správně. V kanceláři ale vídáme, že na právní stránku se vzpomene až po týdnu, kdy servery zase běží. Ohlašovací lhůty v tu dobu už uplynuly a stopy, které by firmu obhájily u úřadu, u pojišťovny nebo u soudu, zmizely s reinstalací.

Během prvních tří dnů se ale nerozhoduje jen o technice. Rozhoduje se i o tom, co a komu ohlásit, koho informovat, jak zajistit důkazy a zda platit. Projdeme lhůty podle obecného nařízení o ochraně osobních údajů (GDPR) a podle nového zákona o kybernetické bezpečnosti, co čekat od pojišťovny a obchodních partnerů a kdo odpovídá za rozhodnutí o výkupném.

První hodiny: zastavit útok a nesmazat stopy

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) doporučuje po zjištění ransomwaru zařízení odpojit od sítě a vypnout je jen tehdy, když to jinak nejde, protože vypnutím se ztratí stopy v operační paměti. Zálohovací server se odpojuje jako první, aby útok nezasáhl i zálohy. Dál doporučuje pořídit bitové kopie zasažených systémů, shromáždit záznamy o provozu (logy) a vzorky škodlivého kódu a komunikovat mimo napadenou síť, třeba telefonem. Útočník totiž může firemní poštu dál číst.

Z právního pohledu přidáváme dvě věci. Zaprvé si od první minuty veďte deník incidentu: kdy a kdo útok zjistil, co se stalo, kdo co rozhodl a proč. Okamžik zjištění spouští lhůty a správce osobních údajů musí každé porušení zabezpečení zdokumentovat, i když ho nakonec neohlásí (čl. 33 odst. 5 GDPR). Zadruhé nic nepřeinstalovávejte, dokud nemáte kopie. Stopy útoku potřebuje policie, pojišťovna i Úřad pro ochranu osobních údajů (ÚOOÚ). Hlavně je ale budete potřebovat vy, až budete dokazovat, že firma byla zabezpečená přiměřeně.

Únik osobních údajů: ÚOOÚ do 72 hodin

Porušením zabezpečení osobních údajů je kromě jejich úniku i jejich náhodné nebo protiprávní zničení, ztráta nebo změna (čl. 4 bod 12 GDPR). Ransomware, který zašifruje databázi zákazníků nebo mzdovou agendu, je tedy porušením zabezpečení i tehdy, když útočník nic neodnesl. ÚOOÚ i Evropský sbor pro ochranu osobních údajů to řadí mezi porušení dostupnosti.

Ne každé takové porušení se ale musí hlásit. Evropský sbor uvádí jako příklad malou firmu, která měla data uložená šifrovaně, obnovila je z funkční zálohy během několika hodin, provoz se nezastavil a analýza záznamů s jistotou ukázala, že útočník nic nezkopíroval; riziko pro lidi tam bylo nepravděpodobné a stačilo incident zdokumentovat. U firmy, která obnovovala data pět pracovních dnů z papírových podkladů, už ohlášení považuje za nutné. A kde si správce není jistý, jak daleko se útočník dostal, má podle Evropského sboru počítat s horší variantou.

Správce ohlásí porušení ÚOOÚ bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Neohlašuje jen tehdy, je-li nepravděpodobné, že by porušení vedlo k riziku pro práva a svobody lidí. Ohlásí-li později, musí uvést důvody zpoždění (čl. 33 odst. 1). Podle Evropského sboru pro ochranu

osobních údajů se správce o porušení „dozvěděl“, jakmile má přiměřenou jistotu, že k incidentu došlo a osobní údaje byly zasaženy. Lhůta se počítá v hodinách a víkend ji nezastaví.

Nečekejte, až IT dokončí analýzu. Neznáte-li ještě rozsah, ohlaste, co víte, a zbytek doplňte postupně; nařízení to výslovně dovoluje (čl. 33 odst. 4 GDPR). Neúplné ohlášení podané včas je lepší než úplné s omluvou za zpoždění.
Ohlášení musí obsahovat popis porušení s kategoriemi a přibližným počtem dotčených lidí a záznamů, kontakt na pověřence pro ochranu osobních údajů nebo jinou kontaktní osobu, pravděpodobné důsledky a přijatá opatření (čl. 33 odst. 3). ÚOOÚ k tomu má elektronický formulář. Vyplněný formulář lze poslat datovou schránkou (ID qkbaa2n), poštou nebo e-mailem na posta@uoou.gov.cz. E-mail ale musí nést uznávaný elektronický podpis; jinak ho úřad za řádné ohlášení považuje jen tehdy, když ho potvrdíte ručně podepsaným formulářem poštou nebo osobně. Nejjistější je datová schránka.

Odpovědnost nese správce, tedy ten, kdo o zpracování rozhoduje. Stal-li se útok u dodavatele, třeba u poskytovatele cloudu nebo mzdového softwaru, musí vám ho jako zpracovatel ohlásit bez zbytečného odkladu (čl. 33 odst. 2) a pomoci vám se splněním povinností (čl. 28 odst. 3 písm. f). ÚOOÚ ale ohlašujete vy. Za porušení těchto povinností hrozí pokuta až 10 milionů eur nebo 2 % celosvětového ročního obratu, podle toho, co je vyšší (čl. 83 odst. 4).

Evropská komise v listopadu 2025 v takzvaném digitálním omnibusu navrhla lhůtu prodloužit na 96 hodin a ohlašovat jen případy s vysokým rizikem. K 5. 11. 2026 návrh přijat nebyl a platí 72 hodin.

Kdy napsat lidem, jejichž údaje unikly

Je-li pravděpodobné, že porušení bude mít za následek vysoké riziko pro práva a svobody lidí, musí je správce bez zbytečného odkladu informovat i přímo (čl. 34 odst. 1 GDPR). Typicky jde o uniklá hesla, rodná čísla, čísla účtů, zdravotní údaje nebo cokoli, co se dá zneužít k podvodu. Oznámení se píše jasně a jednoduše, s kontaktem, pravděpodobnými důsledky a přijatými opatřeními (čl. 34 odst. 2). Doporučujeme přidat i to, co mají lidé udělat: změnit hesla, nevěřit e-mailům a telefonátům, které se odvolávají na vaši firmu, a sledovat pohyby na účtu. Podvodníci uniklé údaje rádi použijí k přesvědčivě vypadajícím zprávám.

Oznamovat lidem nemusíte, jestliže byly údaje šifrované a pro útočníka nesrozumitelné, jestliže jste přijali opatření, po kterých se vysoké riziko už pravděpodobně neprojeví, nebo jestliže by oznámení vyžadovalo nepřiměřené úsilí. V posledním případě ale musíte vydat veřejné oznámení (čl. 34 odst. 3). ÚOOÚ může oznámení nařídit (čl. 34 odst. 4).

Kdo v důsledku porušení nařízení utrpěl hmotnou nebo nehmotnou újmu, má právo na její náhradu (čl. 82 odst. 1). Soudní dvůr EU v rozsudku ze dne 14. 12. 2023, Natsionalna agentsia za prihodite, věc C-340/21, posuzoval útok na bulharskou daňovou správu, po kterém se na internetu objevily údaje více než šesti milionů lidí. Řekl, že samotný únik po útoku třetích osob neznamená, že opatření správce nebyla vhodná. Ve sporu o náhradu újmy ale správce nese důkazní břemeno, že vhodná byla, a odpovědnosti se nezprostí jen tím, že únik způsobil útočník. Už

sama obava ze zneužití údajů přitom může být nehmotnou újmou, je-li za daných okolností opodstatněná (výrok, body 1, 3, 5 a 6; bod 85). Pro firmu z toho plyne, že se obhájí hlavně dokumentací: bezpečnostní pravidla, záznamy o školeních, aktualizacích a zálohách a deník incidentu.

Nový zákon o kybernetické bezpečnosti: týká se vás?

Od 1. 11. 2025 je účinný zákon č. 264/2025 Sb., o kybernetické bezpečnosti, který do českého práva přenáší evropskou směrnici NIS 2. Dopadá na poskytovatele regulovaných služeb v 15 odvětvích, od energetiky, výroby a potravinářství přes dopravu, vodní a odpadové hospodářství a zdravotnictví po digitální služby (§ 4 odst. 1). Zpravidla jde o střední a velké podniky; malý podnik jen tehdy, je-li pro stát zvlášť významný, a některé služby registruje úřad bez ohledu na velikost (§ 5). Konkrétní služby stanoví vyhláška č. 408/2025 Sb., o regulovaných službách. Na výzvu úřadu nečekejte: službu musí NÚKIB ohlásit poskytovatel sám, a to nejpozději do 60 dnů ode dne, kdy podmínky splnil (§ 6 odst. 1). Velikost podniku se přitom počítá i se společnostmi ve skupině, takže zákon může dopadnout i na malou dceřinou firmu velkého koncernu; nezapočítávají se jen společnosti ze skupiny, jejichž technická aktiva jsou zcela oddělena od těch, které firma používá k poskytování regulované služby (§ 7 písm. c). Firma, která nedávno vyrostla, přibrala novou činnost nebo vstoupila do skupiny, by si to měla ověřit hned.

Poskytovatel v režimu vyšších povinností hlásí incidenty NÚKIB, poskytovatel v režimu nižších povinností Národnímu CERT, a to jen ty s významným dopadem na službu (§ 15 odst. 1 až 3). Lhůty jsou kratší než u GDPR: prvotní hlášení nejpozději do 24 hodin po zjištění incidentu (§ 16 odst. 1). Do 72 hodin pak následuje oznámení s prvotním posouzením a do 30 dnů od něj závěrečná zpráva. To platí v režimu nižších povinností pro každý hlášený incident s významným dopadem na službu, v režimu vyšších povinností tehdy, když NÚKIB sdělí, že incident má významný dopad na kybernetický prostor státu (§ 16 odst. 2 a 3). Hlásí se přes Portál NÚKIB (§ 16 odst. 4). S hlášením musí poskytovatel začít nejpozději do roka od doručení rozhodnutí o registraci (§ 15 odst. 4). Za jeho opomenutí hrozí pokuta až 250 milionů Kč nebo 2 % celosvětového obratu v režimu vyšších povinností a až 175 milionů Kč nebo 1,4 % v režimu nižších, podle toho, co je vyšší (§ 59 odst. 4).

Hlášení NÚKIB a ohlášení ÚOOÚ jsou dvě samostatné povinnosti a jedno nenahrazuje druhé. Úřady si jen vyměňují informace, aby za porušení téže povinnosti netrestaly dvakrát (§ 64 odst. 5). A firma, na kterou zákon nedopadá, může incident NÚKIB ohlásit dobrovolně (§ 15 odst. 5); zákon počítá s tím, že se úřad nebo Národní CERT i k takovému hlášení vyjádří a pomůže metodicky (§ 17 odst. 5).

Policie, pojišťovna a obchodní partneři

Útok bývá trestným činem neoprávněného přístupu k počítačovému systému a zásahu do něj (§ 230 trestního zákoníku), výzva k výkupnému k tomu vydíráním (§ 175). Kontaktovat policii doporučuje i NÚKIB. Trestní oznámení navíc dokládá, že firma byla obětí, a pojišťovna i partneři se na něj budou ptát.

Kryje-li škodu pojištění, oznamte událost pojišťovně bez zbytečného odkladu, podejte pravdivé vysvětlení, předložte doklady a postupujte způsobem ujednaným ve smlouvě (§ 2796 odst. 1 občanského zákoníku). Poslední část se snadno přehlédne. Než objednáte forenzní firmu nebo začnete s útočníkem cokoli řešit, přečtěte si pojistné podmínky; co v nich stojí o postupu po události, zavazuje i vás. Jak dlouho smí pojišťovna šetřit a kdy můžete chtít zálohu, popisuje průvodce Šetření a záloha.

Obchodní partneři vás zajímají ze dvou stran. Nedodáte-li kvůli útoku včas, odpovídáte za škodu a zprostí vás jen mimořádná nepředvídatelná a nepřekonatelná překážka (§ 2913 odst. 2 občanského zákoníku). Na to, že soud za takovou překážku uzná kyberútok, bychom dnes nesázeli: útoky jsou běžné a obrana proti nim se od firmy čeká. Projděte proto smlouvy, co v nich stojí o vyšší moci, o oznamování incidentů a o lhůtách. Jak má vypadat dobrá doložka o vyšší moci, popisujeme v článku Pět smluvních klauzulí, které nikdo nečte. Vlastní oznamovací lhůty mívají smlouvy o zpracování osobních údajů a smlouvy, které poskytovatel regulované služby uzavírá se svými dodavateli; do těch zákon o kybernetické bezpečnosti bezpečnostní požadavky přímo vyžaduje (§ 13 odst. 5). Partnerům, jejichž data nebo systémy mohly být zasaženy, napište včas a věcně, co se stalo a co mají udělat. Odhady viníka a úvahy o tom, co se mohlo udělat lépe, do takového dopisu nepatří.

Výkupné: rozhodnutí, za které odpovídá vedení

NÚKIB doporučuje výkupné neplatit za žádných okolností. Platba útočníka motivuje k dalším útokům, nic nezaručuje, že data odemkne nebo smaže, odemčení neodstraní škodlivý kód a zaplacení může z právního hlediska porušit péči řádného hospodáře. Poslední důvod se týká osobně jednatele nebo člena představenstva. Musí funkci vykonávat s nezbytnou loajalitou i s potřebnými znalostmi a pečlivostí (§ 159 odst. 1 občanského zákoníku) a ve sporu sám dokazuje, že tak jednal (§ 52 odst. 2 zákona o obchodních korporacích). Chrání ho pravidlo podnikatelského úsudku: obstojí, kdo mohl v dobré víře rozumně předpokládat, že jedná informovaně a v obhajitelném zájmu společnosti (§ 51 odst. 1).

Zvažuje-li vedení platbu, třeba proto, že bez dat firma nepřežije, potřebuje rozhodnutí podklady: posouzení, zda a jak rychle jde obnovit provoz ze záloh, vyčíslení škod, stanovisko pojišťovny a zápis o tom, proč rozhodlo tak, jak rozhodlo. Víc o odpovědnosti jednatele najdete v průvodci Za co jednatel odpovídá.

Dvě věci platí vždy. Peníze nesmějí jít osobám a skupinám na sankčním seznamu EU; pro kybernetické útoky má Unie vlastní sankční režim (čl. 3 odst. 2 nařízení Rady (EU) 2019/796) a porušení mezinárodní sankce ve větším rozsahu je trestný čin (§ 410 trestního zákoníku). Útočník se ovšem nepředstaví. Než vedení zaplatí, ať forenzní firma nejdřív určí, o jakou skupinu jde, zjištění se porovná se sankčními seznamy a výsledek patří do zápisu o rozhodnutí. A zaplacení nic nemění na ohlašovacích povinnostech: k porušení zabezpečení už došlo a slib útočníka, že data smazal, nikdo neověří.

Sepište si dnes na jednu stránku, kdo při útoku rozhoduje, telefonní čísla vedení, správce IT, pojišťovny a advokáta a postup ohlášení ÚOOÚ. Uložte ji mimo firemní systémy, třeba vytištěnou.
Ověřte, zda vaše služba není ve vyhlášce č. 408/2025 Sb. Kdo splňuje podmínky zákona o kybernetické bezpečnosti, musí se NÚKIB ohlásit sám do 60 dnů.

Ve smlouvách s dodavateli IT a cloudu si zkontrolujte, do kolika hodin vám musí incident ohlásit a jaké podklady vám pošlou. Bez nich ohlášení ÚOOÚ nesestavíte.

Přehled

Otázka	Odpověď	Ustanovení
Je zašifrování dat ransomwarem porušením zabezpečení?	Ano, jde o ztrátu dostupnosti; hlásí se, ledaže je riziko pro lidi nepravděpodobné	čl. 4 bod 12, čl. 33 odst. 1 GDPR
Do kdy ohlásit ÚOOÚ	Bez zbytečného odkladu, pokud možno do 72 hodin od zjištění; později s odůvodněním	čl. 33 odst. 1 GDPR
Kdy informovat dotčené lidi	Při pravděpodobném vysokém riziku, bez zbytečného odkladu	čl. 34 GDPR
Pokuta za porušení ohlašovacích povinností	Až 10 milionů eur nebo 2 % celosvětového obratu	čl. 83 odst. 4 GDPR
Hlášení podle zákona o kybernetické bezpečnosti	Prvotní hlášení do 24 hodin; u incidentu s významným dopadem oznámení do 72 hodin a závěrečná zpráva do 30 dnů od oznámení	§ 16 zákona č. 264/2025 Sb.
Ohlášení regulované služby NÚKIB	Do 60 dnů od splnění podmínek	§ 6 odst. 1 zákona č. 264/2025 Sb.
Oznámení pojišťovně	Bez zbytečného odkladu a postupem podle smlouvy	§ 2796 odst. 1 občanského zákoníku
Výkupné	NÚKIB nedoporučuje; platba osobám na sankčním seznamu je zakázána	čl. 3 odst. 2 nařízení (EU) 2019/796

Řešíte útok nebo únik dat právě teď? Pomůžeme rozhodnout, co a komu ohlásit, připravíme ohlášení ÚOOÚ, oznámení dotčeným lidem i dopisy pojišťovně a partnerům a vedení dáme podklady pro rozhodnutí, která se budou později posuzovat. Ochranu dat a kybernetickou bezpečnost řešíme v rámci IT compliance. Napište nám.

Závěr

Právní lhůty po kyberútoku běží bez ohledu na to, kdy se rozjedou systémy: 72 hodin pro ÚOOÚ, u regulovaných služeb 24 hodin pro NÚKIB nebo Národní CERT a bez zbytečného odkladu pro pojišťovnu. Firma, která v prvních hodinách zajistí stopy, vede si deník a ohlásí včas i neúplné informace, má potom u úřadu, pojišťovny i soudu z čeho se bránit.

Firma, která předem ví, zda spadá pod zákon o kybernetické bezpečnosti a co jí ve smlouvách slibují dodavatelé, nebude o tom rozhodovat až během útoku.

Prameny

- Nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů, čl. 4 bod 12, čl. 28 odst. 3 písm. f), čl. 33, čl. 34, čl. 82 a čl. 83 odst. 4.
- Zákon č. 264/2025 Sb., o kybernetické bezpečnosti, § 4 až 8, § 13, § 15, § 16, § 17, § 59 a § 64 (znění účinné od 1. 11. 2025).
- Vyhláška č. 408/2025 Sb., o regulovaných službách.
- Zákon č. 89/2012 Sb., občanský zákoník, § 159, § 2796 a § 2913.
- Zákon č. 90/2012 Sb., o obchodních korporacích, § 51 a § 52.
- Zákon č. 40/2009 Sb., trestní zákoník, § 175, § 230 a § 410.
- Nařízení Rady (EU) 2019/796 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy, čl. 3.
- Rozsudek Soudního dvora EU ze dne 14. 12. 2023, Natsionalna agentsia za prihodite, věc C-340/21.
- Evropský sbor pro ochranu osobních údajů, Pokyny 9/2022 k oznamování porušení zabezpečení osobních údajů podle GDPR, verze 2.0, a Pokyny 01/2021 k příkladům oznamování porušení zabezpečení osobních údajů, verze 2.0, případy č. 01 a 02.
- NÚKIB, Ransomware: doporučení pro mitigaci, prevenci a reakci, verze 1.2 ze dne 22. 5. 2023, oddíl 4.
- Úřad pro ochranu osobních údajů, Porušení zabezpečení osobních údajů (uoou.gov.cz).

Tento článek má informativní charakter a nepředstavuje právní poradenství. Vychází z právního stavu ke dni publikace; zda a komu je třeba konkrétní incident ohlásit, závisí na tom, jaké údaje a služby zasáhl a zda firma spadá pod zákon o kybernetické bezpečnosti.

Kyberútok nebo únik dat ve firmě: co udělat v prvních 72 hodinách

Tým IUSTORIA · Publikováno 5. 11. 2026

https://www.iustoria.cz/blog/kyberutok-unik-dat-ve-firme/

Text je dílem chráněným autorským právem. Sdílení celého dokumentu bez úprav je vítáno; přebírání částí do jiných textů jen s uvedením zdroje. © IUSTORIA, advokátní kancelář, s.r.o.