UKÁŽKOVÉ ČÍSLO

ODBORNÝ E-MAGAZÍN

PROFESIONÁL KYBERNETICKEJ BEZPEČNOSTI

Sprievodca pre bezpečnosť dát aj peňazí vašej firmy

KYBERÚTOKY NA SLOVENSKÝ KATASTER A ZDRAVOTNÚ POISŤOVŇU SÚ VÝSTRAHOU PRE ŠTÁT

Nový zákon o kyberbezpečnosti pritvrdil

NBÚ varuje pred čínskou AI

Keď odíde zamestnanec, odídu aj dáta?

Tlačiareň ako extra slabé miesto vašej kyber-ochrany

Získajte vzor, ako napísať správu o kybernetickom incidente

NEWSLETTER pre vašich zamestnancov

PROFESIONÁL KYBERNETICKEJ BEZPEČNOSTI

UKÁŽKOVÉ ČÍSLO

VYDAVATEĽ:
Nakladatelství Forum, s.r.o.,
organizačná zložka
www.forum-media.sk

ADRESA REDAKCIE:
Tallerova 4, 811 02 Bratislava

ZÁKAZNÍCKE ODDELENIE:
office@forum-media.sk
tel.: 02 / 20 62 00 10
fax: 02/ 20 62 00 19

ŠÉFREDAKTORKA:
Mgr. Klára Gajdošová

FOTOGRAFIE:
BigStockPhoto, Freepik
Pixabay, archív autorov

GRAFICKÁ ÚPRAVA A ZLOM E-MAGAZÍNU:
Renáta Brtnická

ROČNÉ PREDPLATNÉ:
189 eur (bez DPH)

OBJEDNÁVKA PREDPLATNÉHO:
office@forum-media.sk
Tel.: +420 251 115 576
Mobil: +420 603 248 054

INFORMÁCIE O PREDPLATNOM:
tel.: 02 / 20 62 00 10

ROČNÍK: I.

PERIODICITA: MESAČNÁ

E-magazín vychádza ako mesačník.

OBSAH

Národný bezpečnostný úrad upozorňuje na AI model DeepSeek

Redakcia

Čínsky jazykový model zbiera od používateľov dáta v zásadne väčšom rozsahu než konkurenčné AI modely. Na čo si musíte dať pozor?

Národný bezpečnostný úrad (NBÚ) vydal varovanie pred čínskym jazykovým modelom DeepSeek, ktorý podľa úradu zbiera nadštandardné množstvo detailných používateľských údajov, pričom tieto dáta sú ukladané na serveroch v Číne.

GDPR tam neexistuje, dáta môžu byť zneužité

Model DeepSeek nie je „len ďalší chatbot" – podľa NBÚ zhromažďuje údaje, ktoré môžu zahŕňať zadané pokyny (prompty), heslá, vkladané obrázky, presný čas stlačení jednotlivých klávesov či audio súbory. Výnimkou nie sú ani systémový jazyk, dokumenty či IP adresa zariadenia, z ktorého používateľ DeepSeek využíva.

Na rozdiel od modelov trénovaných a prevádzkovaných v EÚ, ktoré spĺňajú požiadavky GDPR, DeepSeek podlieha čínskej jurisdikcii – a tam ochrana osobných údajov prakticky neexistuje.

„Na základe porovnania pravidiel ochrany súkromia DeepSeek a OpenAI zbiera čínsky model viac dát než americký OpenAI. Rozdiel je aj v tom, kde sa tieto dáta ukladajú. V EÚ, kde OpenAI deklaruje súlad s GDPR, máme robustný systém na ich ochranu pred zneužitím. Takýto koncept v Číne chýba. Naopak, súkromné údaje sú tam aktívne využívané pre potreby komunistickej strany (štátu)," vysvetľuje NBÚ.

Úrad zároveň upozorňuje, že v podmienkach používania DeepSeek sa nachádza klauzula, ktorá umožňuje využívať údaje „v prospech verejnosti" alebo na „dodržiavanie zákonných nariadení".

Získané údaje tak podľa NBÚ môžu byť použité na vytváranie osobnostných profilov, identifikáciu zamestnania používateľa či dokonca na cielené kybernetické útoky.

Cenzuruje informácie citlivé pre režim

Aj výsledky vyhľadávania prostredníctvom modelu DeepSeek môžu byť skreslené alebo neúplné. Jazykové modely sa síce učia z obrovského množstva dát, no to, aké konkrétne informácie sa do tréningu dostanú, závisí od ich tvorcov. Po natrénovaní sa modely ešte dolaďujú tak, aby ignorovali určité citlivé alebo zakázané témy. V prípade západných AI systémov ide napríklad o obsah týkajúci sa sexuálneho zneužívania, návodov na výrobu výbušnín, obchodovania s drogami a iných eticky sporných oblastí.

„Model DeepSeek aktívne cenzuruje informácie, ktoré sú citlivé pre čínsky režim. Ak sa napríklad pokúsite získať informácie o protestoch na Námestí Tchien-an-men v roku 1989, počas ktorých režim zavraždil stovky civilistov, chatbot odpoveď jednoducho odmietne. DeepSeek teda kopíruje fungovanie čínskeho internetu, ktorý je nastavený tak, aby vopred filtroval a cenzuroval podobný obsah," upozorňuje NBÚ.

(Zdroj: TASR, NBÚ)

Komentár odborníka: Kyberútoky na slovenský kataster a Všeobecnú zdravotnú poisťovňu sú výstrahou pre štát aj pre občanov

JUDr. Jakub Pavčík
konateľ spoločnosti osobnyudaj.sk a expert na kybernetickú bezpečnosť

Vo veľkej väčšine prípadov kyberútokov nie je slabinou technológia ako taká, ale procesy a neexistujúce alebo slabé krízové scenáre. Mnoho štátnych organizácií nemá pravidelné penetračné testy, školenia personálu a ani vypracované reakčné plány. Kybernetické incidenty sa spájajú s dôverou občanov, so stabilitou štátu a schopnosťou zachovať kontinuitu fungovania krajiny aj v digitálnom svete. Zmena je nutná.

V posledných mesiacoch sme na Slovensku boli svedkami dvoch kybernetických incidentov, ktoré otriasli dôverou verejnosti v schopnosť štátu zabezpečiť kritické systémy. Kyberútok na systém katastra nehnuteľností a potom aj na Všeobecnú zdravotnú poisťovňu (VŠZP) ukázali, že digitálna odolnosť štátu je na poväženie a nepostačujúce zabezpečenie sa môže premietnuť do reálnych problémov občanov.

Čo sa stalo a prečo to nie je maličkosť?

V januári 2025 zaútočil neznámy aktér na systém Úradu geodézie, kartografie a katastra SR, hovorovo kataster. Kataster nehnuteľností, ktorý má kľúčový význam pre zaručenie vlastníckych práv, sa tak stal na **niekoľko dní až týždňov nedostupným**. Podľa doteraz dostupných informácií šlo o kombináciu DoS útoku a phishingovej kampane, **ktorá môže byť „predstupňom" väčšej kompromitácie**. O niekoľko týždňov neskôr zasiahol kybernetický útok aj Všeobecnú zdravotnú poisťovňu. Poisťovňa preventívne odstavila mobilné aplikácie a niektoré online systémy, aby zabránila šíreniu útoku. V oboch prípadoch šlo o incidenty, ktoré si vynútili pozornosť odborníkov aj verejnosti.

> Nefunkčný kataster neznamená iba pozastavenie prevodov nehnuteľností, ale aj nemožnosť získať výpisy a ohrozenie dôvery v stabilitu štátu.

Dôsledky: väčšie ako len „nefunkčný web"

Na prvý pohľad je možné tieto útoky vnímať ako technickú záležitosť IT oddelenia, no v skutočnosti ide **o zásah do bežného života občanov**. Nefunkčný kataster neznamená iba pozastavenie prevodov nehnuteľností, ale **aj nemožnosť získať výpisy a ohrozenie dôvery v stabilitu štátu**. Koho tento útok ešte ovplyvnil? Pocítili to aj desaťtisíce ľudí naprieč profesiami. Od geodetov, ktorí nevedeli zameriavať médiá, cez realitných maklérov, súdnych znalcov a bežných predávajúcich a kupujúcich až po farmárov, ktorých GPS v poľnohospodárskej technike je takisto napojené na systémy a mapy katastra.

V prípade VŠZP mohli útoky ohroziť dostupnosť zdravotných služieb, elektronických receptov či citlivých osobných údajov poistencov. To, že nedošlo k úniku údajov ani ku kompromitácii účtov, je dobrá správa. Otázka však zostáva: Je to dôsledok dobre nastavenej obrany alebo skôr šťastnej zhody náhod?

Kde je skutočný problém: V technológii? Nie, v procesoch a kultúre

Skúsenosti ukazujú, že vo veľkej väčšine prípadov nie je slabinou technológia ako taká, ale procesy a neexistujúce alebo **slabé krízové scenáre**. Mnoho štátnych organizácií nemá:

- pravidelné penetračné testy,
- školenia personálu v oblasti phishingu,
- vypracované reakčné plány.

Niektoré rezorty či príspevkové organizácie fungujú s minimálnym IT personálom, často bez manažéra kybernetickej bezpečnosti. Práve tieto slabiny sa ukážu a často rozhodujú v krízovej situácii.

Čomu sa môžeme naučiť?

Každý incident je aj príležitosťou. Udalosti z jari 2025 ukazujú niekoľko dôležitých bodov:

- **Bezpečnosť musí byť prioritou aj mimo kríz.** Investície do prevencie sú efektívnejšie než riešenie dôsledkov. **Obnova takýchto rozsiahlych systémov je vždy niekoľkonásobne drahšia než preventívne opatrenia.** Žiaľ, veľké množstvo organizácií (a hlavne štatutárov) rieši otázku kybernetickej bezpečnosti až vo chvíli, keď sa niečo stane. Často hľadajú vinníka. „Ako je možné, že nás nikto neupozornil, že sa to môže stať?" Tie upozornenia tu boli, žiaľ, vy ste neboli pripravení počúvať.
- **Vzdelávanie a povedomie zamestnancov sú rovnako dôležité ako firewall.** Podľa dostupných štatistík **až 52 % bezpečnostných incidentov v oblasti kybernetickej bezpečnosti vzniká práve z dôvodu pochybenia zamestnanca**. A ako pochybí? Jednoducho klikne na škodlivý odkaz, pretože chce vyhrať najnovší mobilný telefón, alebo si v rámci dlhých hodín v práci pozrie online film.
- **Komunikácia s verejnosťou by mala byť jasná, rýchla a otvorená.** Prvý dojem v kríze ovplyvňuje dôveru. Práve v tomto bode je kľúčové, aby sa **vedúci predstavitelia postavili k problému čelom a jasne komunikovali** (a predovšetkým upokojili) verejnosť. V prípade útoku na kataster boli občania právom vystrašení, začali sa obávať o svoje vlastnícke práva. Takéto situácie sú **živnou pôdou pre dezinformátorov**, ktorí sa na takýchto kauzách prižívujú a publikujú neoverené informácie a hoaxy. Prečo to robia? Jednoducho sa chcú zviditeľniť a získať pozornosť publika. Dôsledky sú však často katastrofálne.
- **Záznamy a logovanie sú kľúčom k vyhodnoteniu útokov a ich zdroja.** Aké záznamy a logy existujú z útoku na kataster a VŠZP, to si autor článku nedovolí hodnotiť, keďže týmito informáciami nedisponuje (a nechce šíriť hoaxy). Ak však kataster a VŠZP fungovali v režime zákona o kybernetickej bezpečnosti, a teda napĺňali jeho účel, dostupnosť záznamov a logov by nemala byť problém. Ak však naozaj fungovali v tomto režime, nemal nastať ani spomínaný incident, či nie?

> Niektoré rezorty či príspevkové organizácie fungujú s minimálnym IT personálom. Tieto slabiny rozhodujú v krízovej situácii.

A čo súvislosti a budúcnosť?

Kybernetické prostredie je dnes najrizikovejšou oblasťou kritickej a inak dôležitej infraštruktúry. **Spolu s príchodom smernice NIS 2 a novelizovaným slovenským zákonom o kybernetickej bezpečnosti majú štátne inštitúcie povinnosť zabezpečiť ochranu aktív na výrazne vyššej úrovni.**

V kybernetickej bezpečnosti platí staré známe pravidlo: *„Požiaru je lepšie predchádzať, ako ho potom hasiť."* Je teda najvyšší čas:

- zmapovať systémy,
- vyhodnotiť riziká,
- systematicky budovať odolnosť.

Bez toho budeme ďalej hasiť požiare, ktoré nikdy nemuseli nastať.

Záver: Nejde len o čísla, ale o dôveru

Na záver treba povedať, že kybernetické incidenty nesúvisia len s technickými parametrami a šifrovanými databázami. Spájajú sa **aj s dôverou občanov, so stabilitou štátu a schopnosťou zachovať kontinuitu fungovania krajiny aj v digitálnom svete**. Verme, že tieto prípady budú nielen varovaním, ale aj impulzom na zmenu.

VZOR: Správa o kybernetickom útoku

Mgr. Ján Bezpečný
manažér kybernetickej bezpečnosti

Kliknite a stiahnite si VZOR

1. Identifikácia incidentu

- **Dátum a čas zistenia incidentu:** 4. 6. 2025, 08:15
- **Dátum a čas začiatku incidentu (odhad):** 3. 6. 2025, cca 23:00
- **Nahlasujúca osoba:** Ing. Ján Novák, správca IT infraštruktúry
- **Zasiahnutý systém:** Interný server účtovníctva (srv-ucto01)
- **Kategória kybernetického incidentu:** Neoprávnený prístup, ransomvér

2. Popis incidentu

Dňa 4. 6. 2025 v ranných hodinách bola zaznamenaná anomália pri pokuse o prístup k účtovnému serveru. Používateľ nevedel otvoriť žiadne dokumenty a na disku sa nachádzal súbor s názvom „READ_ME.txt“, v ktorom bolo uvedené, že všetky súbory boli zašifrované a k ich obnove je potrebné zaplatiť výkupné v kryptomene.

Predbežnou analýzou logov sa zistilo, že útočník pravdepodobne získal prístup prostredníctvom služby vzdialenej plochy (RDP), ktorá bola prístupná z internetu bez obmedzení a bez použitia viacfaktorového overenia. Útočník sa následne prihlásil na administrátorské konto, nainštaloval škodlivý softvér a zašifroval obsah disku.

Incident zasiahol aj lokálne zálohy, ktoré boli pripojené k systému a takisto zašifrované.

3. Dopad incidentu

- **Dotknuté údaje:** osobné údaje zamestnancov a klientov (meno, priezvisko, adresa, e-mail, čísla zmlúv, čísla účtov)
- **Predbežný počet dotknutých osôb:** cca 830
- **Dopad na prevádzku:**
  - — Úplné prerušenie prístupu k účtovným údajom
  - — Nedostupnosť fakturačného systému
  - — Ohrozenie integrity údajov
- **Možné porušenie ochrany osobných údajov (GDPR):** Áno
- **Vplyv na dôveru verejnosti / reputáciu:** potenciálne negatívny

4. Prijaté opatrenia

Bezprostredné opatrenia po zistení incidentu:

- Zasiahnutý server bol okamžite odpojený z internej siete
- Zamedzenie prístupu z externého prostredia cez RDP na všetkých zariadeniach
- Informovanie zodpovednej osoby pre ochranu osobných údajov
- Oznámenie incidentu Národnému bezpečnostnému úradu (NBÚ) a Úradu na ochranu osobných údajov SR
- Vykonaná záloha systémov z predchádzajúceho funkčného bodu (z 1. 6. 2025) a obnovenie na nový server
- Všetky prístupové údaje boli zmenené a heslá boli vynútené ako silné
- Bol vykonaný úplný antivírusový a antimalvérový sken celej siete

Doplňujúce technické opatrenia:

- Zavedenie viacfaktorového overovania pre všetkých administrátorov
- Vypnutie nepotrebných služieb a portov
- Zavedenie tzv. „least privilege" princípu pre všetky používateľské kontá
- Presun záloh na oddelené offline úložisko s fyzickým odpojením mimo produkčnej siete
- Zazmluvnenie bezpečnostného auditu externou spoločnosťou

Organizačné a preventívne opatrenia:

- Vnútorné vyškolenie všetkých zamestnancov o rizikách phishingu a sociálneho inžinierstva
- Aktualizácia bezpečnostnej dokumentácie a havarijného plánu
- Vytvorenie samostatnej politiky pre manažment kybernetických incidentov
- Pravidelné testovanie záloh a simulácie kybernetických incidentov

5. Analýza a poučenie

- **Identifikovaná slabina:** Nezabezpečený RDP prístup, slabé heslo, chýbajúce 2FA
- **Závažnosť incidentu:** Vysoká (zásah do osobných údajov, prerušenie prevádzky, poškodenie systémov)
- **Opatrenia do budúcnosti:**
  - — Zaviesť pravidelný penetračný test a audit kybernetickej bezpečnosti
  - — Zaviesť systém na detekciu a reakciu na incidenty (EDR)
  - — Sledovanie logov v reálnom čase a nasadenie SIEM nástroja

6. Záver

Kybernetický útok bol identifikovaný a izolovaný včas, vďaka čomu bolo možné minimalizovať jeho dopad na organizáciu. Napriek tomu išlo o vážny incident s dopadom na dôvernosť a dostupnosť údajov. Organizácia prijala okamžité aj systémové opatrenia s cieľom posilniť odolnosť IT infraštruktúry a zabrániť opakovaniu podobných útokov.

Tlačiareň ako extra slabé miesto vašej kyber-ochrany: bez softvéru to už neriskuje

Patrik Porubčan
riaditeľ divízie IT, PRESMONT.IT

Pre útok na tlačový server bola obmedzená prevádzka univerzity v Marylande, v nemocničnom prostredí bola pre tlačiareň závažne ohrozená citlivá zdravotná dokumentácia. Tlačiarne nie sú samostatnou jednotkou, musíme ich vnímať ako plnohodnotnú súčasť celej firemnej infraštruktúry, ktorú treba riadne chrániť. Ešte nemáte tlač zabezpečenú správnym serverom? Včera bolo neskoro. Na čo si pri jeho výbere dať pozor?

Tlačové zariadenia, ktoré sa kedysi považovali za bežnú techniku s okrajovým významom pre IT bezpečnosť, dnes čelia zásadnej transformácii. Stali sa integrálnou súčasťou dátových tokov a každá ich interakcia môže mať vplyv na kybernetickú bezpečnosť organizácie. V súčasnosti už nejde len o to, či tlačiareň dokáže tlačiť kvalitne a ekonomicky, ale aj o to, ako je integrovaná do siete, ako komunikuje s inými systémami, ako spracúva údaje používateľov a či tieto údaje dokáže chrániť pred zneužitím. Vzhľadom na rastúci počet kybernetických útokov, regulácie ako GDPR alebo smernica NIS 2 sa aj tlač musí prispôsobiť novým pravidlám. Súčasnosť je zároveň výzva. Rôzne spoločnosti, vrátane tej našej, sa snažia poskytnúť a nájsť riešenia, ktoré reflektujú potreby dnešných komplikovaných časov a môžu slúžiť ako inšpirácia na modernizáciu aj vo vašom prostredí. Investícia pritom nemusí byť obrovská a v niektorých prípadoch stačí iba minimálna, no výsledkom môže byť aj obrovské šetrenie nákladov a času.

Prečo sa tlač stala slabým miestom kybernetickej ochrany?

Zraniteľnosti tlačového prostredia sa často prehliadajú. Neautentifikované tlačové úlohy, nezabezpečené prístupy k multifunkčným zariadeniam, chýbajúce šifrovanie dát pri prenose či absencia logovania – to všetko sú riziká, ktoré môžu viesť k únikom údajov alebo k zneužitiu infraštruktúry. V korporátnom prostredí, ale, samozrejme, aj na úradoch či v menších spoločnostiach môže nezabezpečená tlačiareň slúžiť ako bod vstupu do siete. Rovnako mnohokrát môže ísť aj o únik osobných údajov, prípadne obchodných tajomstiev, ako napr. známok žiakov alebo identifikačných údajov občanov, či interných dát spoločnosti.

> V nemocničnom prostredí bola multifunkčná tlačiareň pripojená k rovnakej sieti ako zdravotnícke systémy, čím vznikol potenciálny bod pre prienik do elektronickej zdravotnej dokumentácie.

Mnohé organizácie si neuvedomujú, že nezabezpečená tlačiareň môže byť vstupnou bránou pre útočníka. V praxi sa už objavili prípady, keď došlo k incidentom práve kvôli nezabezpečenej tlači respektíve prostrediu. Napríklad strata dokumentu na výstupe z tlačiarne, nezabezpečené USB porty alebo nevhodné procesy digitalizácie môžu viesť k únikom údajov. V jednom z prípadov bola škodlivá aktivita spustená cez nezabezpečené multifunkčné zariadenie. Na istom úrade unikli osobné údaje občanov vinou výtlačku, ktorý zostal na výstupe z tlačiarne a bol omylom odnesený. Pri digitalizácii zmlúv došlo k neúmyselnému zverejneniu osobných údajov z dôvodu chýbajúcej klasifikácie dokumentov. V nemocničnom prostredí bola multifunkčná tlačiareň pripojená

k rovnakej sieti ako zdravotnícke systémy, čím vznikol potenciálny bod pre prienik do elektronickej zdravotnej dokumentácie. V inom prípade pracovník nechtiac naskenoval dokumenty s citlivými údajmi na verejne prístupný e-mail. Tieto prípady sú len špičkou ľadovca. Prípadne medializované útoky zo sveta, napríklad v roku 2018 sa podarilo etickému hackerovi zneužiť tisíce nezabezpečených tlačiarní po celom svete (tzv. PewDiePie útok), čím demonštroval, ako jednoducho sa dajú ovládať zariadenia dostupné z internetu. V Británii zase unikli zdravotné údaje pacientov Národnej zdravotnej služby (NHS), keď zostali výtlačky s osobnými informáciami vo verejne prístupných častiach nemocníc. Na americkej univerzite v Severnej Karolíne získal útočník prístup k internej sieti cez USB port na multifunkčnom zariadení. Spomenúť môžeme ešte DDoS útok cez tlačový server na univerzite v Marylande, kde nezabezpečený tlačový server poslúžil na útok, čoho výsledkom boli hromadné výpadky služieb univerzity. Špeciálnu pozornosť si zaslúži aj prípad „žltých bodiek" – niektoré zariadenia už v roku 2005 v USA automaticky tlačili identifikátory (dátum, čas, sériové číslo), ktoré mohli byť zneužité na sledovanie používateľov.

> Správny tlačový softvér by mal podporovať hlavne šifrovanie TLS, segmentáciu prístupu, viacúrovňové overovanie a zachytávať všetky operácie do logov.

Tieto prípady ukazujú, že podcenenie zabezpečenia tlače môže viesť nielen k úniku údajov, ale aj k systémovým kompromitáciám. Tlačové prostredie sa dnes musí správať ako štandardizovaná a kontrolovaná súčasť IT bezpečnosti – so šifrovaním, s auditovaním a riadeným prístupom.

Softvérový základ bezpečnej tlače a skenovania

Správny print admin systém by mal byť centralizovaný nástroj na správu a zabezpečenie tlače. Mal by byť vhodným práve pre vaše použitie, tj buď malú kanceláriu s pár počítačmi, alebo korporátne prostredie. Softvér by mal umožňovať napríklad aj tieto funkcie:

- autentifikáciu používateľov prostredníctvom čipovej karty, PIN kódu alebo prihlasovacieho mena a hesla napr. prostredníctvom AD/LDAP, Google Workspace a iných platforiem,
- zabezpečené uvoľnenie tlačových úloh až po prihlásení používateľa,

- podrobný audit všetkých operácií – kto tlačil, čo tlačil, odkiaľ, kedy a akou formou používal zariadenie,
- nastavenie bezpečnostných politík – napr. zakázanie farebnej tlače, nastavenie kvót, časové obmedzenia či v prípade skenovaní možnosť definovať oprávnenia podľa oddelenia alebo úrovne zamestnanca,
- integráciu s Active Directory alebo LDAP, čo umožňuje centrálne riadenie identity a oprávnení,
- prednastavené profily skenovania – dokumenty idú presne tam, kam majú: do správnej zložky, e-mailu, systému, navyše vďaka OCR obsahujú aj rozpoznanie textu a zvyšujú efektivitu pri digitalizácii,
- šifrovaná komunikácia cez TLS a možnosť integrácie s firewallmi, so systémami SIEM a DLP.

V korporátnom či väčšom prostredí možno takýto softvér nasadiť aj ako súčasť komplexného systému zabezpečenia, ktorý sleduje dodržiavanie takzvaných compliance politík. V školách a na úradoch môže slúžiť ako prostriedok ochrany osobných údajov GDPR a zároveň ako nástroj na optimalizáciu nákladov. Na úradoch bráni nedopatreniam, ktoré by inak mohli mať právne dôsledky.

Nehovoriac o tom, že samotné zariadenia, teda tlačiarne, by mali byť chránené. Spôsoby ochrany môžu byť napríklad tieto:

- digitálne podpísaný firmvér – každá aktualizácia firmvéru je digitálne podpísaná, čím sa zabezpečí, že zariadenie prijíma len autentické a dôveryhodné aktualizácie. Tým sa eliminuje riziko zavedenia škodlivého kódu,
- kontrola integrity firmvéru (Firmware Integrity Check) – pravidelná automatická kontrola integrity zaručuje, že firmvér nebol manipulovaný ani napadnutý neoprávnenou modifikáciou,

> Nezabezpečená tlačiareň môže slúžiť ako bod vstupu do siete.

- bezpečný bootovací proces (Secure Boot) – proces spúšťania tlačiarne je chránený a monitorovaný tak, aby sa zabránilo načítaniu škodlivých alebo neoprávnených verzií firmvéru,
- šifrovanie pevného disku (Data Encryption) – tlačiarne obsahujú interné disky so vstavaným šifrovaním (AES-256), čo chráni všetky citlivé údaje uložené v zariadení pred neoprávneným prístupom,
- šifrovanie komunikácie (TLS/IPsec) – komunikácia medzi tlačiarňou a ostatnými zariadeniami alebo servermi je zabezpečená protokolmi TLS a IPsec, čím sa zabráni odpočúvaniu dát a kybernetickým útokom typu „man-in-the-middle“,
- bezpečné vymazanie údajov (Secure Data Erase) – možnosť bezpečne vymazať údaje z pevného disku zariadenia po dokončení tlačovej úlohy alebo pri vyradení zariadenia z prevádzky, čím sa predchádza riziku úniku citlivých údajov.

Riešenie pre každého – škola, úrad aj priemyselno-korporátne prostredie

V rámci našej praxe sme úspešne nasadili takéto riešenia v rôznych prostrediach:

- základná škola – po incidente, keď sa výtlačky so známkami a s osobnými údajmi ponechali na výstupe, zaviedla škola implementáciou overovanie cez RFID karty učiteľov. Výsledkom je nulový počet incidentov a spokojnosť vedenia aj rodičov. V neposlednom rade aj obrovské zníženie nákladov, keďže už nie je dostupné kopírovanie či tlačenie bez akejkoľvek kontroly, ale aj zjednodušenie pre učiteľov v podobe profilového skenovania testov a ďalších dokumentov,
- mestský úrad – nasadenie softvéru ako súčasti projektu digitalizácie agendy. Prostredníctvom tlačového softvéru sme prepojili tlač a skenovanie s prihlasovaním do mestského IS. Prístup ku kopírovaniu majú len vybrané oddelenia a zamestnanci, čím sa znížili riziká neoprávneného úniku dokumentov, ale aj náklady na tlač, čo pomohlo k zelenšej samospráve. Zefektívnila sa aj digitalizácia a zverejňovanie povinných dokumentov s dôrazom na automatizáciu a citlivosť dokumentov a údajov v týchto dokumentoch,
- výrobný podnik – implementácia tlače podľa ID zamestnanca vo výrobnom závode eliminovala straty dokumentácie a zrýchlila logistiku. Po migrácii na hybridný pracovný model sa zvýšila potreba vzdialeného tlačového manažmentu a bezpečnosti. Vďaka tlačovému softvéru sa tlačové úlohy ukladajú na server a uvoľňujú sa iba po fyzickej autentifikácii – minimalizuje sa tak riziko zneužitia dokumentov. Podarila sa aj centralizácia

> Ak má byť vaša infraštruktúra bezpečná, spoľahlivá a efektívna, tlač a digitalizácia formou skenovania dokumentov musia do nej patriť ako jej plnohodnotná súčasť.

tlače a výrazne sa znížili náklady na tlač až o 60 percent aj vďaka efektívnemu riešeniu a správnej technológii pri zvolenej značke tlačiarní, rovnako ako uhlíková stopa danej spoločnosti v oblasti tlačových riešení.

NIS 2 a Zero Trust – tlač patrí do bezpečnostného rámca

Norma NIS 2 zaväzuje k tomu, aby organizácie chránili všetky technické aktíva – vrátane tlače. Správny tlačový softvér by mal podporovať hlavne šifrovanie TLS, segmentáciu prístupu, viacúrovňové overovanie a zachytávať všetky operácie do logov. To umožňuje nielen predchádzať incidentom, ale aj preukázať, že sa prijali primerané technické a organizačné opatrenia.

Tlač v koncepte Zero Trust znamená, že nikto nemá implicitne dôveru – ani používateľ, ani zariadenie. Každá požiadavka na tlač, kopírovanie či skenovanie sa musí overiť a autorizovať – bez výnimiek. Tlačiareň by nemala byť dostupná „na voľno" každému v sieti. Používateľ musí byť autentifikovaný (napríklad kartou, PIN-om alebo sieťovým účtom) a zariadenie, z ktorého požiadavka prichádza, by malo byť dôveryhodné – napríklad registrované v MDM (Mobile Device Management) systéme alebo patriť do bezpečnostnej zóny akou je napríklad doména.

V prostredí Zero Trust sa všetky činnosti zaznamenávajú (auditujú), čím sa výrazne znižuje riziko zneužitia, či už náhodného alebo úmyselného. Systém by mal vedieť okamžite rozpoznať, kto, kedy, aký dokument tlačil, kam ho poslal, či bol výstup fyzicky uvoľnený, a kým.

Princíp „never trust, always verify" (nikdy never, vždy overuj) v praxi znamená, že aj tlačová infraštruktúra podlieha rovnakej úrovni ochrany ako servery, cloudové služby alebo prístup do firemných aplikácií. V takomto softvéri je každá interakcia riadená, overená a zaznamenaná. Takýto prístup významne redukuje priestor na ľudské chyby alebo na úmyselné obchádzanie systému.

Jednoduchosť a dostupnosť

Napriek robustnosti riešenia by sme mali myslieť aj na koncových používateľov, softvér by mal byť jednoduchý na používanie. Taktiež existujú softvérové riešenia dostupné aj vo verziách bez licenčných poplatkov pre menšie organizácie, školy či úrady. Základom je, aby bol softvér moderný a prehľadný a ponúkal prostredie, kde si môžu administrátori sami upravovať pravidlá a používatelia majú istotu, že pracujú bezpečne.

A čo povedať na záver?

Bezpečnosť tlače, automatizácia úloh a digitalizácia sú dnes nevyhnutnosťou. Správnym výberom tlačiarní a softvéru môžete pomáhať chrániť údaje, optimalizovať náklady a zvyšovať komfort aj kontrolu nad dokumentmi. V spojení so spoľahlivými zariadeniami a s odborným servisom a poradenstvom dokážete priniesť reálnu hodnotu pre každú IT stratégiu a IT prostredie. Ak má byť vaša infraštruktúra bezpečná, spoľahlivá a efektívna, tlač a digitalizácia formou skenovania dokumentov musia do nej patriť ako jej plnohodnotná súčasť.

Keď odíde zamestnanec, odídu aj dáta?

JUDr. Jakub Pavčík
konateľ spoločnosti osobnyudaj.sk a expert na kybernetickú bezpečnosť

Napadlo vám, že e-maily, ktoré váš zamestnanec posiela sám sebe, môžu byť po jeho odchode z firmy zdrojom úniku dát s devastačným a nenávratným reputačným vplyvom? Myslíte na to, že zamestnanec odchádza z vašej firmy s databázou klientov? A teraz si predstavte, že začne pracovať v druhej spoločnosti, použije databázu, vy prídete o desiatky tisíc eur a nebudete s tým môcť nič urobiť! Zabudnite na to, že kybernetickú bezpečnosť rieši len IT oddelenie, spolupracovať musíte všetci. Čo urobiť pred tým, než odíde zamestnanec z vašej spoločnosti?

Zobral si len pár súborov, to je v pohode... Nie, nie je. A ak si to myslíte, je najvyšší čas sa prebudiť. Odchod zamestnanca nie je len HR udalosť. Je to **kybernetický incident**, ak nie sú nastavené správne pravidlá.

Reálny príklad z praxe

Firma XYZ (názov úmyselne zmenený) bola úspešná IT spoločnosť. Jeden z obchodníkov dal výpoveď a o dva mesiace sa objavil v konkurenčnej firme. Tá začala náhle oslovovať rovnakých klientov s rovnakou prezentáciou. Vysvitlo, že odchádzajúci zamestnanec si pred odchodom **skopíroval kompletný CRM export, prezentácie a obchodné podklady** na USB. Mal k nim prístup, heslo mu fungovalo ešte tri dni po odchode. Nikto ho neskontroloval, nikto nič nezablokoval. **Škoda vyše 80 000 eur.** A nič s tým nemohli robiť – nebolo to právne ošetrené.

Prečo je to problém?

Odchádzajúci zamestnanec **často neodchádza len s pracovnými skúsenosťami**, ale aj s:

- databázami klientov,
- firemnými cenovými politikami,
- prístupmi do systémov,
- dokumentmi, ktoré si posielal sám sebe e-mailom,
- heslami, ktoré poznal,
- zariadením, ktoré nikto nepremazal.

> Odchod zamestnanca nie je len HR udalosť. Je to kybernetický incident, ak nie sú nastavené správne pravidlá.

Ak nemáte nastavený proces, je to **ideálna situácia na únik citlivých údajov** – často úplne legálne (z vášho pohľadu), ale s devastačným a nenávratným reputačným vplyvom.

Časté situácie, ktoré sa dejú denne:

- Zamestnanec si pred výpoveďou preposiela dôležité súbory na svoj súkromný e-mail.
- Pripojí si USB disk a stiahne si 3 GB firemných dát.

CHECKLIST: Čo urobiť pri odchode zamestnanca?

Toto nie je IT úloha. Je to firemná povinnosť – HR, manažér, IT musia spolupracovať.

Pred odchodom (ideálne pri výpovedi):

- Informujte IT o presnom dátume posledného pracovného dňa.
- Vyhodnoťte prístupy, ktoré daný človek má (e-maily, servery, cloud, aplikácie).
- Zablokujte možnosti externého ukladania dát (USB, cloud, e-mail).
- Preverte, či nemá zdieľané disky alebo súkromné zálohy.
- Vykonajte kontrolu zariadení, ktoré používa – čo má uložené, či neodnáša údaje.

V deň odchodu:

- Zablokujte alebo vymažte účty vo všetkých systémoch (Microsoft, GSuite, CRM, ERP...).
- Zrušte alebo presmerujte e-mail (nastavte automatickú odpoveď).
- Zabezpečte vrátenie firemných zariadení – notebook, mobil, USB, kľúče, prístupové karty.
- Odoberte ho zo všetkých tímových četov, skupín, nástrojov.

Po odchode:

- Skontrolujte logy prihlásení a prenosov dát (sťahovanie, odosielanie).
- Informujte kľúčových klientov, že prišlo k zmene kontaktnej osoby.
- Vyhodnoťte riziká – čo by mohol vedieť, čo si mohol zobrať, či má NDA.

Právne riešenia

- Dohoda o zachovaní mlčanlivosti (NDA) – aj po odchode, ideálne ako súčasť pracovnej zmluvy.
- Dohoda o ochrane dôverných informácií – samostatný dokument, ktorý pretrvá.
- Sankčné ustanovenia – pri porušení, napríklad odcudzení obchodného tajomstva, know-how.
- Zmluvné doložky o vrátení zariadení a údajov – všetko treba vrátiť bez kopírovania.

- Má stále prístup do e-mailu, SharePointu či do cloudového úložiska aj týždne po odchode.
- Nikto neodstránil jeho prístup do účtovného softvéru alebo do CRM.
- Má firemný notebook a ešte dva týždne ho používa, kým to niekto rieši.

> Nezáleží na tom, či ide o IT špecialistu alebo o recepčnú. Každý má prístup k nejakým údajom, ktoré nemajú opustiť firmu.

Dôležité ponaučenie

Nie každý zamestnanec odchádza s úmyslom poškodiť firmu. Ale každý odchod je bezpečnostné riziko, ak nie sú nastavené procesy. A to platí bez ohľadu na to, či ide o IT špecialistu alebo o recepčnú – **každý má prístup k nejakým údajom, ktoré nemajú opustiť firmu**.

Kybernetická bezpečnosť nie je len o hekerovi za notebookom v tmavej kapucni. Ide pri nej aj o to, či **máte kontrolu nad vlastnými ľuďmi – ich prístupmi, správaním a následkami, keď odchádzajú**.

Tip na záver

Bez formalizovaného postupu bude každý odchod chaos. Preto si zaveďte jednoduchý **„odchodový protokol" – jeden formulár alebo digitálny checklist**, v ktorom si každé oddelenie (HR, IT, manažér) odškrtne svoju časť:

- **IT oddelenie:** odstránenie prístupov, spracovanie logov, návrat zariadení.
- **HR/právne oddelenie:** preverenie zmluvných náležitostí, NDA, spracovanie citlivých údajov.
- **Nadriadený:** vyhodnotenie, aké know-how alebo citlivé dáta by zamestnanec mohol odniesť.

Urobte tento protokol ako súčasť interného predpisu. A nezabudnite – nestačí ho mať. **Musí sa aj reálne používať.**

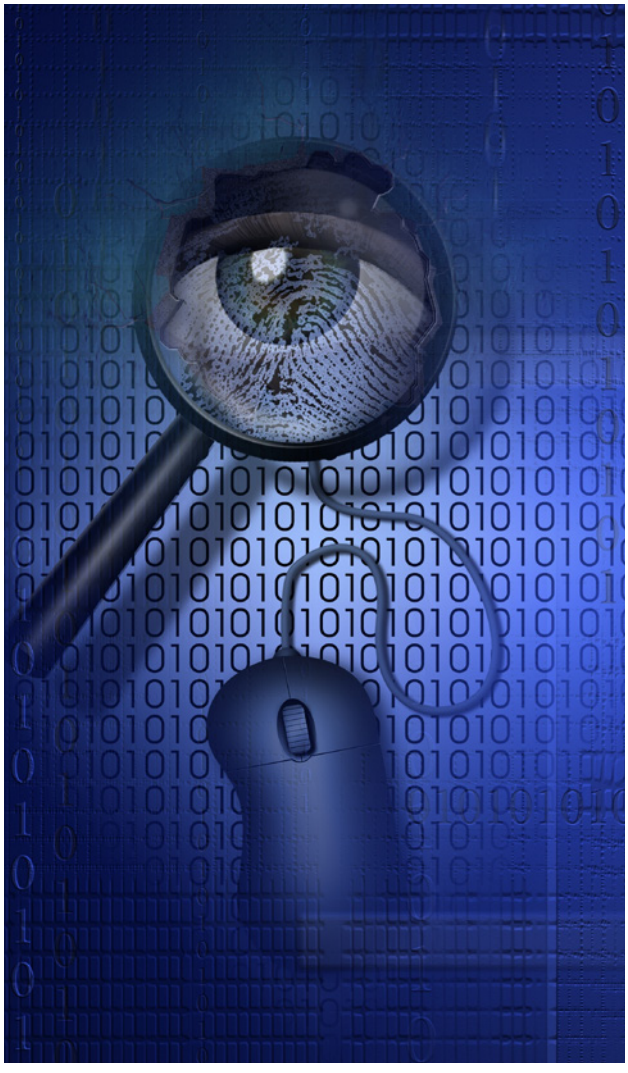
Nový zákon o kyberbezpečnosti pritvrdzuje: Máte povinnosť, nie voľbu

Redakcia

Šibeničné lehoty na hlásenie kybernetických útokov, povinný kybernetický audit, analýza rizík a množstvo ďalších opatrení priniesol nový kyberzákon a smernica NIS2. Po novom musia riešiť kyberbezpečnosť stovky nových subjektov. Čo všetko ste povinný zariadiť a v akých lehotách?

Od 1. 1. 2025 je na Slovensku účinná novela zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorou sa do slovenskej legislatívy implementujú prísne požiadavky európskej smernice NIS2. Tento právny predpis zásadne rozširuje okruh subjektov, ktoré sú povinné zaviesť robustné bezpečnostné opatrenia, chrániť svoju IT infraštruktúru, reagovať na incidenty v zákonom stanovených lehotách a podrobiť sa auditu alebo samohodnoteniu.

Nejde už len o odporúčanú prax – ide o právne záväzné kroky, ktorých nesplnenie môže mať pre organizácie vážne dôsledky. A to aj vo forme pokút, ktoré môžu dosahovať miliónové sumy. Čo všetko nový zákon prináša?



Už ste začali s auditom?

Legislatívna zmena je odpoveďou na rastúci počet kybernetických hrozieb a útokov, ktoré nezasahujú len veľké technologické firmy, ale čoraz častejšie aj kľúčové oblasti ako energetiku, zdravotníctvo, dopravu či digitálnu infraštruktúru.

Zákon zavádza dve hlavné kategórie povinných subjektov: **prevádzkovateľov základných služieb** a **prevádzkovateľov kritických základných služieb**. Kým medzi prevádzkovateľov kritických základných služieb patria najmä veľkí hráči v sektoroch ako energetika, financie alebo zdravotníctvo, medzi prevádzkovateľov základných služieb spadajú aj menšie firmy, verejné inštitúcie, poskytovatelia digitálnych a cloudových služieb, telekomunikácií a mnohých ďalších.

Povinnosť zabezpečiť kybernetickú ochranu teda nespadá len na veľké korporácie – **zákon sa týka aj malých**

firiem, ktoré sú súčasťou dodávateľských reťazcov alebo podporujú kritické sektory.

Organizácie majú podľa zákona jasne stanovený harmonogram: **do 60 dní** od začatia činnosti sa musia **identifikovať Národnému bezpečnostnému úradu (NBÚ)**, následne sa zapísať do príslušného registra a **do 12 mesiacov implementovať technické aj organizačné opatrenia**. **Do dvoch rokov** musia absolvovať **nezávislý audit alebo samohodnotenie**, v závislosti od kategórie.

Prísne opatrenia

Kybernetická bezpečnosť je stále často nesprávne vnímaná len ako „záležitosť IT oddelenia". Nová legislatíva však kladie dôraz na to, aby ju firmy a organizácie vnímali ako **neoddeliteľnú súčasť strategického riadenia**. Právna zodpovednosť sa rozširuje až na úroveň štatutárnych zástupcov. Tí môžu v prípade závažného zlyhania **niesť osobnú zodpovednosť**, vrátane možného zákazu výkonu funkcie.

Subjekty musia preukázať schopnosť **aktívne riadiť riziká, pravidelne vyhodnocovať zraniteľnosti** a implementovať moderné bezpečnostné technológie – od viacfaktorového overovania (MFA), cez šifrovanie až po monitorovanie infraštruktúry pomocou SIEM systémov.

Veľmi dôležitou povinnosťou je aj **pripravený a zdokumentovaný plán reakcie na incidenty**, ktorý musí byť aj personálne zabezpečený. V prípade vážneho kybernetického incidentu je potrebné **informovať NBÚ do 24 hodín**, **do 72 hodín** doplniť ďalšie detaily a **do 30 dní zaslať záverečnú správu**.

Zákon kladie dôraz aj na bezpečnosť **dodávateľského reťazca**. Organizácie musia zabezpečiť, aby ich partneri spĺňali požadovanú úroveň ochrany – to si vyžaduje **zmluvné revízie, bezpečnostné klauzuly a pravidelné kontroly tretích strán**.

Popri technických a procesných opatreniach je **kľúčové aj vzdelávanie**. Zákon očakáva, že organizácie zabezpečia **pravidelné školenia** nielen pre IT špecialistov, ale aj pre manažment a bežných zamestnancov, ktorých správanie môže výrazne ovplyvniť celkovú bezpečnostnú kultúru.

Získajte odborný e-magazín **Profesionál kybernetickej bezpečnosti**

Získajte odborný e-magazín

V ďalších vydaniach odborného e-magazínu Profesionál kybernetickej bezpečnosti vám prinesieme podrobné vysvetlenia nového zákona a praktické návody na jeho zavádzanie – priamo od expertov z praxe.

Tešiť sa môžete na témy ako:

- **Samohodnotenie vs. audit:** Ako vyzerá kontrola kybernetickej pripravenosti?
- Povinný kybernetický audit od A po Z
- Nástrahy a **povinnosti manažéra kybernetickej bezpečnosti** podľa nového kyberzákona
- Implementácia vyše **80 nových povinností nového kyberzákona** do praxe
- **Nová kategorizácia subjektov:** Povinnosti prevádzkovateľa základnej služby a prevádzkovateľa kritickej základnej služby
- Monitoring a ukladanie logov
- **Technické opatrenia:** Čo všetko musí organizácia zaviesť, aby vyhovela zákonu? (Prehľad požadovaných technických riešení – od MFA po SIEM systémy.)
- **Kybernetické školenia a osveta:** Čo musí váš zamestnanec vedieť podľa zákona aj o polnoci?
- **Dodávateľský reťazec pod kontrolou:** Nové pravidlá pre spoluprácu s partnermi + ktorých dodávateľov musíte nahlásiť NBÚ?
- **A ešte oveľa viac...**

AKO PRACOVAŤ S NEWSLETTROM KYBERSTRÁŽCA?

Ako tomu rozumieť?

Každý mesiac nájdete v novom vydaní e-magazínu Profesionál kybernetickej bezpečnosti aj NEWSLETTER KYBERSTRÁŽCA. Môžete si ho pohodlne stiahnuť v PDF verzii a využiť hneď na niekoľko spôsobov.

Čaká vás vždy nová aktuálna téma, ktorú pripravia experti na kyberbezpečnosť. Newsletter pomôže vašim zamestnancom chrániť firmu pred čoraz sofistikovanejšími kyberútokmi či hrozbami a Vám ušetrí čas aj peniaze.

Vyťažte z NEWSLETTRA KYBERSTRÁŽCA maximum

Tu je niekoľko tipov, ako ho efektívne využiť:

1. **Zdieľajte KYBERSTRÁŽCU e-mailom celej firme** – jednoduchý spôsob, ako zabezpečiť, že každý dostane porciu odborných informácií a naučí sa vyhnúť sa kyberútokom.

2. **Zaraďte KYBERSTRÁŽCU do mesačného interného školenia** – newsletter pokryje vždy aktuálnu tému zrozumiteľne a stručne. Teoretickú nudu nečakajte, je plný príkladov z praxe!

3. **Zverejnite KYBERSTRÁŽCU na internom portály a doplňte testy** – vytvorte si vlastné kyber-bezpečnostné centrum pre zamestnancov. Ak chcete portál oživiť, doplňte jednoduché testy, ktoré na pár klikov overia znalosti, ktoré KYBERSTRÁŽCA naučil vašich zamestnancov.

4. **Využite KYBERSTRÁŽCU na tímových poradách** – je spoločenský a aj keď stráži, nesedí v kúte! Krátka prezentácia témy a diskusia pomôže zamestnancom prepojiť poznatky s praxou.

5. **Vytlačte KYBERSTRÁŽCU a vyveste v kuchynke alebo pri výťahu** – KYBERSTRÁŽCA nie je žiadna citlivka. Rád poslúži aj offline formou pre tých, čo radi čítajú bez obrazovky.

NEWSLETTER KYBERSTRÁŽCA

Váš osobný ochranca pred kybernetickými hrozbami v práci

Pozor na telefonát od šéfa

Klikni a stiahni si NEWSLETTER

ZAVOLAL „ŠÉF" A CHCEL RÝCHLU PLATBU

Kolegyňa mu to poslala. Firmu to stálo 28 000 eur.

Stalo sa to aj mnohým firmám.

V jeden pondelok dopoludnia prišiel firme XYZ (názov úmyselne zmenený) účtovníčke e-mail od generálneho riaditeľa.

Text znel dôveryhodne, bol písaný slušne, bez chýb, dokonca s jeho podpisom. V ňom ju žiadal o okamžité vybavenie mimoriadnej platby pre zahraničného partnera – „diskrétne, bez zdržania, ide o dôležitú akvizíciu".

Účtovníčka si e-mail prečítala, zavolala mu naspäť na číslo, ktoré bolo uvedené v správe. Ozval sa profesionálny mužský hlas, ktorý sa podobal na hlas jej nadriadeného. Pôsobil nátlakovo, ale dôveryhodne: *„Potrebujem, aby to odišlo dnes. Verím, že to zvládnete, nerobme okolo toho rozruch."*

Platbu vo výške 28 000 eur zadala. Až o dva dni zistila, že peniaze sú preč. Natrvalo.

ČO SA VLASTNE STALO?

Tento typ podvodu sa volá **CEO fraud** alebo **Business Email Compromise (BEC)**.

Útočníci sa vydávajú za osobu s vysokou autoritou – zvyčajne za:

- generálneho riaditeľa,
- finančného riaditeľa,
- právnika firmy.

Ich cieľom je **vytvoriť tlak, zneistiť, vyvolať pocit naliehavosti** a donútiť vás konať bez overenia.

Pracujú s detailmi – často vedia mená, štruktúru firmy, dokonca aj štýl komunikácie. Môžu:

- napodobniť e-mailovú adresu (napr. miesto riaditel@firma.sk napíšu r1aditel@firma.sk),
- poslať správu z falošnej adresy cez tzv. „spoofing" (ktorá vyzerá ako originál),
- zavolať z čísla, ktoré si pomocou technológií upravia, aby sa javilo ako interné.

AKO ROZPOZNAŤ CEO PODVOD?

Všímajte si tieto varovné signály:

- E-mail prišiel z **neznámej alebo podozrivej adresy**, hoci pôsobí dôveryhodne.
- Obsahuje **žiadosti o diskrétnosť** – „neinformuj o tom kolegov", „rieš to len ty".
- **Naliehavosť** – „dnes do 15.00", „sme pod časovým tlakom".
- **Žiadosť o nezvyčajnú alebo vysokú platbu**, ktorú bežne neriešite.
- **Netypický spôsob komunikácie** od nadriadeného – buď príliš formálny, alebo príliš neformálny.

ČO ROBIŤ, KEĎ DOSTANETE TAKÚTO ŽIADOSŤ?

1. **Nikdy nekonajte pod tlakom.** Aj keď sa zdá, že to „súri".
2. **Overte si požiadavku osobne alebo na známom čísle.** Nepoužívajte kontakt uvedený v e-maile.
3. **Ak sa vám niečo nezdá, povedzte to nahlas.** Nahláste podozrivý e-mail IT oddeleniu.
4. **Nespoliehajte sa len na podpis v e-maile.** Ten sa dá skopírovať alebo napodobniť.

ČO ROBIŤ, AK UŽ BOLA PLATBA ODOSLANÁ?

1. **Okamžite kontaktujte banku.** Ak zareagujete do niekoľkých hodín, ešte je šanca transakciu zablokovať.
2. **Nahláste incident nadriadenému a IT.**
3. **Zabezpečte dôkazy:** e-mail, telefónne číslo, IP adresu, všetko, čo môže pomôcť polícii.
4. **Podajte trestné oznámenie.**

AKO TOMU PREDÍSŤ VO FIRME?

Nastavte si v tíme tieto pravidlá:

- **Bez telefonického alebo osobného overenia sa nezasiela žiadna mimoriadna platba.**
- **Zamestnanci musia vedieť, že šéf nikdy nežiada citlivé veci cez e-mail.**
- **Väčšie prevody musia schváliť aspoň dve osoby (tzv. princíp štyroch očí).**
- **Pravidelne školte zamestnancov, ako vyzerajú moderné podvody.**
- **Zabezpečte e-mailové domény pred spoofingom (napr. pomocou SPF, DKIM, DMARC).**

ZÁVER

Útočník dnes nepotrebuje prelamovať heslá. **Stačí, že vás presvedčí, aby ste to urobili sami.** Nepotrebuje technológiu – stačí mu psychológia.

A keď sa zdá, že ide „len o e-mail od šéfa", ostražitosť ide bokom, kontrolné mechanizmy nefungujú a chyba je na svete.

Podvodníci nerobia chyby. Robia presne to, čo funguje. A funguje to preto, lebo zamestnanci nechcú vyzerať, že brzdia firmu, že zdržujú, že neveria vedeniu.

Ale pozor: **Overenie nie je zdržovanie. Overenie je ochrana.** Ochrana vašej práce, reputácie aj peňazí firmy.

PAMÄTAJTE:

- **Váš zdravý rozum** je silnejší než akýkoľvek firewall.
- **Päť sekúnd navyše** – keď si overíte e-mail, zodvihnete telefón, spýtate sa kolegu – môže firme **ušetriť desaťtisíce eur**.
- A najmä: **radšej byť opatrný, ako vysvetľovať, prečo chýba 28 000 eur.**