ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 4:
Zodpovednostné vzťahy osôb pre vybrané bezpečnostné role, Časť 2.

JUDr. Michal Rampášek

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

CUSEC

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

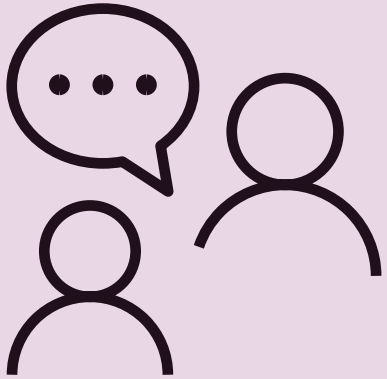
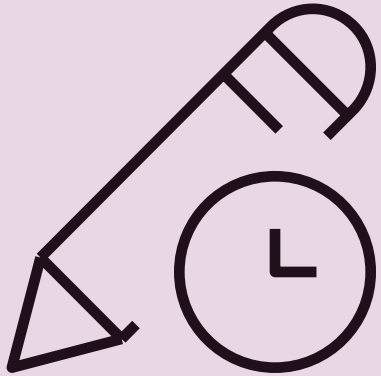
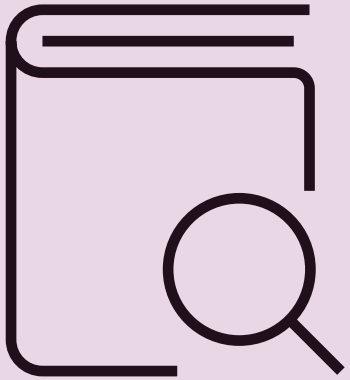
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

ÚVOD

- Rozhodnutia súdov a iných autorít z EÚ a USA
- Zodpovednosť fyzických a právnických osôb z oblastí: Civilné právo, Správne právo, Trestné právo
- Modelové prípady

ÚVOD

Rozhodnutia z oblasti civilného práva

CUSEC

PLÁN OBNOVY

Rozhodovacia prax

- Doterajšia judikatúra ukazuje, že súdy

1. v civilnom práve typicky neposudzujú kyberbezpečnosť ako abstraktnú povinnosť, ale cez otázky: (i) aka bola povinnosť odbornej starostlivosti či zmluvný záväzok, (ii) či došlo k porušeniu, (iii) či je preukázaná príčinná súvislosť, a (iv) rozsah škody.
2. v trestnoprávnych spravidla postihujú až konkrétne úmyselné neoprávnené konanie (neoprávnený prístup, zásah do údajov či systému, podvod, neoznámenie trestného činu, apod.)

- V konaniach sa pravidelne používajú ako listinné ale aj elektronické dôkazy napr. logy, konfigurácie, správy, a v zmluvných vzťahom medzi objednávateľom a dodávateľom je skúmaný dohodnutý rozsah rozdelenia zodpovedností

Hof van Twente (NL): IT dodávateľ nebol zodpovedný

Išlo o spor obce **Hof van Twente** proti poskytovateľovi riadených IT služieb (MSP) , Switch IT Solutions B.V. a Dustin Group AB po ransomvérovom útoku z roku 2020.
Odvolací súd **Arnhem-Leeuwarden (25. 2. 2025,** ECLI:NL:GHARL:2025:1046) potvrdil záver súdu prvej inštancie, že obec nepreukázala, že škoda bola **spôsobená chybou dodávateľa**
okresný súd, aj odvolací súd dospel k záveru, že kybernetický útok nebol výsledkom chýb spoločnosti Switch IT Solutions. Spoločnosť Switch IT Solutions a jej materská spoločnosť Dustin Group preto nenesú zodpovednosť za škody, ktoré obec utrpela v dôsledku kybernetického útoku.

K útoku prispel otvorený RDP port a zmena hesla k účtu zo strany zamestnanca obce, pričom súd neprijal argument, že príčinou boli nedostatky MSP. Ide o ukážkový post-incident spor, kde aj pri existencii outsourcingu zostáva pre žalobcu kľúčové **unesenie dôkazného bremena ohľadom príčinnej súvislosti** a konkrétneho porušenia zmluvných povinností.

Hof van Twente (NL) - IT dodávateľ nebol zodpovedný

Spoločnosť Switch IT Solutions bola poverená poskytovaním správy systému a súvisiacich služieb správy IKT pre obec. Umiestnenia IKT infraštruktúry v sídle obce bolo zachované, a to v kombinácii s externým uložením kópie záložných údajov. Služby správy IKT zahŕňali okrem iného zabezpečenie adekvátneho fungovania systémového softvéru, zálohovanie a obnovu údajov, antivírusové opatrenia a konfiguráciu firewallu. Spoločnosť Switch IT Solutions sa stala zodpovednou za správu konfigurácie serverov, úložísk a sieťových zariadení. Obec zostala zodpovedná za ostatné zariadenia. Technickí správcovia aplikácií obce si ponechali plné správcovské práva. Obec výslovne stanovila, že si ponechá svoj vlastný účet, ktorý si sama spravuje, aby externým dodávateľom umožnila prístup do svojej siete. S týmto účtom boli prepojené najvyššie správcovské práva. Okrem toho požiadavky obce zahŕňali nepretržitý prístup k zálohám..

1. decembra 2020 došlo v obci ku kybernetickému útoku. Okrem toho boli systémy siete obce a zálohy zašifrované a zneprístupnené a mnohé servery boli vymazané. Vyšetrovanie po kybernetickom útoku odhalilo, že rok pred útokom zamestnanec obce upravil pravidlo vo firewalle, čím otvoril RDP (remote desktop) port, ktorý sa neskôr ukázal ako prístup do zvyšku siete. Niekoľko týždňov pred útokom bolo heslo k účtu obce zmenené na ľahko uhádnuteľné heslo. Je pravdepodobné, že heslo bolo uhádnuté počas následných útokov. Keďže účet mal najvyššie práva v sieti obce, útočníci sa následne mohli voľne pohybovať po sieti. To im tiež umožnilo vymazať zálohy.

O'Cliance (NL) – IT dodávateľ čiastočne zodpovedný

V rozhodnutí Okresný súd Amsterdam (ECLI:NL:RBAMS:2018:10124) súd priznal, že IT dodávateľ môže niesť významnú časť škody po ransomvéri, ak ako profesionál nevaroval dostatočne jasne a opakovane pred rizikami a pokračoval v poskytovaní služby bez primeraných bezpečnostných opatrení. Zároveň súd zohľadnil aj spoluzavinenie klienta (napr. slabé heslá) pri výške náhrady.

O'Cliance (účtovnícka firma) si od roku 2009 objednala od IT dodávateľa návrh, vybudovanie a následnú správu/údržbu IT infraštruktúry (mesačný paušál,).
Abstovala písomná zmluva. IT dodávatreľ na pojednávaní uznal, že v mene spoločnosti O'Cliance nainštaloval kompletnú IT infraštruktúru a zabezpečoval jej správu a údržbu na požiadanie. Preto nie je sporné, že medzi stranami existovala dohoda, ktorá stanovovala, že [žalovaný] dodá „kompletný balík".
O'Cliance tvrdí, že svoju IT infraštruktúru úplne zverila do rúk [žalovaného] a že bezpečnosť bola jej prirodzenou súčasťou.
[Žalovaný] vo svojej argumentácii tvrdí, že navrhol bezpečnostné opatrenia, ale že všetky jeho návrhy spoločnosť O'Cliance zamietla. Jeho pôvodný návrh zahŕňal okrem iného inštaláciu firewallu.

Toto rozhodnutie sa často používa ako protipól k rozhodnutiu Hof van Twente. Pri úplnej správe infraštruktúry môže súd vyvodiť silnejšiu povinnosť profesionála, najmä povinnosť aktívneho upozornenia, návrhu alternatív alebo odmietnutia rizikového plnenia

O'Cliance (NL) – IT dodávateľ čiastočne zodpovedný

Súd uznal, že ak dodávateľ dodáva „kompletný balík" infraštruktúry, je ťažko predstaviteľné, aby do toho nepatrila aj primeraná bezpečnosť, najmä keď klient pracuje s citlivými údajmi a dodávateľ o tom vedel.

Dodávateľ infraštruktúru zriadil bez firewallu a bez správnej externého backup režimu. Obrana dodávateľa (argument, že klient to nechcel, bolo to drahé, bolo to komplikované) neuspela, lebo dodávateľ nepreukázal, že klienta dostatočne a opakovane upozornil, ako profesionál nemal len ustúpiť a následne ponechať systém v zjavne rizikovom stave.

Súd prijal, že lepšie zabezpečenie by útok aspoň výrazne sťažilo alebo mohlo odradiť, a najmä správne nastavené externé zálohy by znamenali, že firma by sa vedela obnoviť bez platenia výkupného alebo s menšími dopadmi. Súd však zároveň uznal, že klient prispel k riziku tým, že si výslovne vyžiadal zjednodušenie hesiel (a vedel, že je to rizikové).

Toto rozhodnutie sa často používa ako protipól k rozhodnutiu Hof van Twente.

Smart Connections Factory (NL) – IT dodávateľa odborná starostlivosť

V ďalšom rozhodnutí okresný súd Amsterdam (ECLI:NL:RBAMS:2019:9635) rozhodol, že zákazník profesionálneho poskytovateľa IT služieb môže očakávať, že tento **bude pracovať s náležitým dodržiavaním normy ISO/IEC 25010 pre kvalitu softvéru, aj keďto nebolo výslovne dohodnuté.**

Allsafe si objednala u Smart Connections vývoj CRM systému po neúspešnej predchádzajúcej spolupráci s iným dodávateľom. Hoci absentovala písomná zmluva, obsah zmluvného vzťahu bol založený na prezentácii (PowerPoint) s rozsahom (fázy 1–2), cenami a plánom, Smart Connections tvrdila aj uplatnenie všeobecných podmienok.

Projekt bežal 2016–2018, no Allsafe dlhodobo reklamovala:slabú použiteľnosť (UI), nekonzistentné obrazovky, nezodpovedajúce procesom, chyby, výpadky, nefunkčnosť kľúčových úkonov, nesplnenie účelu (podpora predaja/marketingu). Allsafe neplatila časť faktúr a následne zmluvu okamžite vypovedala/odstúpila.

Allsafe predložila odborný posudok SQMI, ktorý hodnotil systém podľa ISO/IEC 25010:2011 a konštatoval závažné nedostatky v použiteľnosti, spoľahlivosti, výkonnosti, kompatibilite a udržiavateľnosti.

Blauw (NL) - zmluva o spracúvaní údajov ako nástroj post-incident povinností

V rozhodnutí Rechtbank Rotterdam (ECLI:NL:RBROT:2023:2931) súd riešil spor po ransomvéri a exfiltrácii údajov, kde zákazník požadoval od dodávateľa(sprostredkovateľa) informácie a spoluprácu na základe zmluvy o spracúvaní osobných údajov. Súd v skrátenom konaní z veľkej časti vyhovel (vrátane požiadaviek na poskytnutie informácií a umožnenie nezávislého technického skúmania).

Blauw (prevádzkovateľ) využíval ICT služby Nebu (sprostredkovateľ), pričom Nebu spracúva osobné údaje podľa GDPR.

Zmluva obsahovala široko formulovanú povinnosť sprostredkovateľa:

- **okamžite informovať** o incidente (najneskôr do 24h),
- **plne spolupracovať** a **riadiť sa pokynmi** prevádzkovateľa,
- poskytnúť postupy a protokoly incident managementu navyžiadanie.

Blauw mala dlhšie len fragmentárne informácie a potrebovala ich pre plnenie vlastných právnych povinností (notifikácie, posúdenie dopadov, komunikácia so zákazníkmi).

Podľa súdu **právo a povinnosť spolupráce podľa DPA sa majú vykladať široko,** lebo ich cieľom je umožniť prevádzkovateľovi incident riadne vyšetriť, zvoliť primeranú reakciu, a prijať následné kroky (vrátane notifikácií a mitigácie).

Blauw (NL)

Čo súd Blauw priznal

a) Povinnosť poskytnúť detailné informácie o incidente (do 2 pracovných dní) vrátane priebehu útoku , obnovy systémov a použitých metód a nástrojov na skenovanie zvyškov malvéru a zraniteľností, analýzy exfiltrácie dát a určenia, či boli dotknuté údaje Blauw a jej klientov, informácií o útočníkoch (vrátane zanechaných správ), bezpečnostných opatrení prijatých/plánovaných po incidente, stav implementácie, dát a podkladov k internému vyšetrovaniu .

b) Povinnosť poskytovať informácie aj do budúcna, do 4 hodín pri kľúčových nových zisteniach: nový incident, potvrdenie či boli údaje Blauw exfiltrované, identita páchateľov (časovo obmedzené do októbra 2023), inak denná aktualizácia o 18:00 (do júna 2023).

c) Nebu musí zadať nezávislé forenzné vyšetrovanie (zistenie root cause, rozsah exfiltrácie), lebo po niekoľkých týždňoch stále nedokázala spoľahlivo potvrdiť rozsah exfiltrácie, počet dotknutých údajov bol veľký, Nebu poskytovala spočiatku limitované informácie.

d) Súd určil povinnosť uchovať konkrétne typy logov a artefaktov (AD timeline, auth logy, FW logy, Google Cloud Platform admin activity log, data access audit log, system event audit log, policy denied audit log a SQL logs, ako aj z endpointov/počítača, z ktorého bol získaný prístup: (i) systémové protokoly systému Windows, (ii) zoznamy odkazov (zobrazenie naposledy alebo často používaných dokumentov), (iii) priečinky s názvom „shellbags" , (iv) položky automatického spúšťania, (v) súbory LNK (automaticky vytvorené systémom Windows pri otvorení priečinka alebo súboru alebo pri spustení programu), (vi) pamäť, (vii) súbory predbežného načítania, (viii) register, (ix) kôš a (x) služby systému Windows, atď.) pre možné forenzné vyšetrovanie.

Delaware Supreme Court (Travelers v. Blackbaud, USA 2026)

Prípad Blackbaud zásadne mení sporové riziko pri kybernetických incidentoch u SaaS poskytovateľov a MSP incidenty majú po novom výrazne vyššiu šancu v civilnom konaní.

Spoločnosť Blackbaud (SaaS s citlivými údajmi darcov) čelil ransomware útoku. Zákazníci (neziskové organizácie a školy) museli robiť vlastné vyšetrovania a znášali právne, forenzné a notifikačné náklady. Poisťovne vyplatili milióny a následne žalovali Blackbaud. Prvostupňový súd žaloby dvakrát zamietol, no Najvyšší súd Delaware to zvrátil a umožnil pokračovať v žalobe pre porušenie zmluvy.

Kľúčové závery : nižšie nároky pre žalobcov (vrátane poisťovní) pri formulovaní žaloby, príčinná súvislosť nie je bariéra v úvodnej fáze , agregované žaloby naprieč viacerými zákazníkmi sú prípustné, vyššie náklady na spory a tlak na rýchle urovnanie , vyššie očakávania, od dodávateľov pri reakcii a vyšetrovaní incidentov
„Komerčne primeraná" kybernetická bezpečnosť

Delaware Supreme Court (Travelers v. Blackbaud, USA 2026)

„Komerčne primeraná" kybernetická bezpečnosť, súdy USA implicitne zahŕňajú :

- MFA (najmä pre vzdialený prístup a prístup správcov)
- Šifrovanie citlivých údajov (v úložisku aj pri prenose)
- Správa aktualizácií a odstraňovanie zraniteľností
- Segmentácia siete a kontroly prístupu
- Funkcie logovania, monitorovania a detekcie
- Formálne plány reakcie na incidenty
- Obmedzovanie objemu údajov a kontroly uchovávania údajov

Odborná starostlivosť

Podľa § 537 (1) Obchodného zákonníka „Zhotoviteľje povinný vykonať dielo na svoje náklady a na svoje nebezpečenstvo v dojednanom čase, inak v čase primeranom s prihliadnutím na povahu diela." a podľa § 537 (3) Obchodného zákonníka „pri vykonávaní diela postupuje zhotoviteľ samostatne a nie je pri určení spôsobu vykonania diela viazaný pokynmi objednávateľa, ibaže sa výslovne zaviazal plniť ich."

Zhotoviteľje povinný vykonávať dielo samostatne, riadne, poctivo a odborne, na svoje náklady a nebezpečenstvo. Prvok samostatnosti sa primárne odvodzuje z vymedzenia podnikania (§ 2 ods. 1) a explicitnej úpravy v ustanovení § 537 ods. 3.

Zo samostatnosti zhotoviteľa vyplýva zodpovednosť za odborný postup vo všetkých súvislostiach, ktoré je možné subsumovať pod odbornú starostlivosť podnikateľa. Zákon akcentuje prvok samostatnosti a odbornosti tým, že pre relevanciu príkazov objednávateľa ustanovuje výslovný prejav vôle zhotoviteľa obsahujúci záväzok zhotoviteľa zachovávať pokyny objednávateľa. Napriek platnému záväzku s takýmto obsahom je zhotoviteľ povinný s odbornou starostlivosťou preveriť pokyny objednávateľa a notifikovať ich nedostatky (§ 551).

(DURAČINSKÁ, Jana, PATAKYOVÁ, Mária. § 537 [Základné povinnosti zmluvných strán]. In: PATAKYOVÁ, Mária a kol. Obchodný zákonník. 1. vydanie. Bratislava: C. H. Beck, 2022, s. 1524–1525, marg. č. 2.)

NAP (SDEÚ 2023) – dôkazné bremeno a TOMs

Vec C-340/21 (Natsionalna agentsia za prihodite) je jeden z najdôležitejších pre aj sporovú agendu po kyberútoku.

Rozsudok patrí medzi najdôležitejšie rozhodnutia SDEU k civilným nárokom po kyberútokoch podľa GDPR, lebo zjednocuje výklad toho, čo znamenajú primerané technické a organizačné opatrenia, ako sa rieši dôkazné bremeno a čo môže byť nemajetková ujma.

(i) Primeranosť opatrení (TOMs): Súd potvrdil, že posúdenie primeranosti je vždy kontextové (založené na riziku) – hodnotí sa vzhľadom na riziká spracúvania, povahu údajov a pravdepodobnosť/závažnosť dopadov; nejde o „formálnu" požiadavku, ale o reálnu schopnosť opatrení chrániť údaje.

(ii) (Dôkazné bremeno: Prevádzkovateľ má vedieť preukázať, aké opatrenia zaviedol a prečo boli primerané .

(iii) Súd pripustil, že aj obava či strach z budúceho zneužitia osobných údajov môže predstavovať nemajetkovú ujmu, ak je skutočná a primerane preukázaná, nie čisto hypotetická alebo abstraktná.

Samotné porušenie ochrany osobných údajov (data breach) automaticky nedokazuje, že prevádzkovateľ porušil povinnosť prijať primerané technické a organizačné opatrenia

Rozhodnutia z oblasti trestného práva

CUSEC

PLÁN OBNOVY

Uber a Sullivan

- po prvýkrát CISO odsúdený v trestnom konaní (2023)
- Uber bol opätovne napadnutý v dôsledku rovnakých nedostatočných bezpečnostných postupov, ktoré viedli k incidentu ktorý práve prešetrovala Federálna obchodná komisia (FTC)
- Sullivan vo výpovedi pred FTC nepravdivo opísal bezpečnostné postupy Uber
  - vedome zatajil informácie o narušení bezpečnosti, pri ktorom hackeri získali prístup k údajom približne 57 miliónov používateľov a vodičov Uberu
  - namiesto nahlásenia incidentu, CISO zabezpečil, aby hackeri dostali výkupné vo výške 100 000 dolárov z bug bounty programu spoločnosti Uber
  - vedome nepodal trestné oznámenie a podnikol kroky na utajenie trestného činu
  - klamal a skresľoval informácie novému vedeniu spoločnosti (CEO) a internýmvyšetrovateľom
- podmienečný trest odňatia slobody na 3 roky odňatia slobody, trest verejnoprospešných prác 200 hodín a pokuta 50 000 dolárov

Uber a Sullivan

- Odvolací súd Spojených štátov pre deviaty obvod 13. marca 2025 potvrdil rozsudok odsudzujúci bývalého CISO spoločnosti Uber, Joea Sullivana a zamietol jeho odvolanie

SolarWinds a Brown

- po prvýkrát čelí CISO žalobe regulačného orgánu (2023,)
- Orion (45% príjmu SolarWinds v 2020) = „crown jevel"
- kompromitácia viac ako 18 000 zákazníkov
- Komisia pre cenné papiere (SEC) tvrdí, že

A. podvádzali investorov a zákazníkov SolarWinds prostredníctvom nepravdivých a skresľujúcich verejných vyhlásení („Security Statement"), ktoré zakrývali nesprávne a nedostatočné opatrenia a riziká

B. podávali skreslené informácie o bezpečnosti a rizikách v písomných podaniach (formulároch) pre SEC

C. Brown bol tvorcom vyhlásení a riadiacim pracovníkom SolarWinds, vedúceho skupiny InfoSec, a doslova "tvárou" kyberbezpečnosti

- SEC žiada aj

➢ vydanie všetkých neoprávnene nadobudnutých príjmov

➢ trvalý zákaz Brownovi pôsobiť ako vedúci alebo riaditeľ akéhokoľvek emitenta

SolarWinds a Brown

- **Komisia SEC 20. novembra 2025 dobrovoľne stiahla žalobu proti spoločnosti SolarWinds a jej CISO Timothy Brownovi.**

- "When you don't have rules to follow, it's very hard to follow them,"
- "It puts pressure on, but it's also an inflection point," he said. "It has elevated the [chief information security officer] position and made sure that boards are having these conversations."

SolarWinds security chief calls for tighter cyber laws

Tim Brown was first cyber executive to face SEC charges after a massive Russian hack

The complaint against Tim Brown, chief information security officer at SolarWinds, was largely thrown out by a federal court in July

The Financial Times, https://www.ft.com/content/a9645282-70f0-40ac-bfa2-c77f485d33fd

Vybrané rizikové scenáre v slovenskej praxi

1) Formuláre a samohodnotenia prijatých bezpečnostných opatrení a plnenia zákonných požiadaviek voči regulačným orgánom (najmä NBÚ)
2) Verejné vyhlásenia a zmluvné záväzky týkajúce sa kybernetickej bezpečnosti organizácie a/alebo produktov
3) (Ne)oznámenie incidentu, (ne)podanie trestného oznámenia
4) Nezabezpečenie a/alebo zničenie digitálnych stôp (dôkazov)

Drizzly a Rellas

Prípad Drizly (FTC, 2022): FTC zasiahla proti spoločnosti Drizly a jej CEO (James Rellas) po úniku osobných údajov približne **2,5 mil. spotrebiteľov**.
Kľúčový kontext: Drizly **nemala CISO** – úlohy informačnej bezpečnosti vykonával **CEO** (osobná zodpovednosť za nastavenie bezpečnosti).
Spracúvané údaje: údaje zákazníkov ukladané v **AWS** (e-mail, heslá, geolokácia, poštové adresy).
Kritická chyba: Drizly používala **GitHub** ako nezabezpečené „úložisko" a ukladala tam aj **prístupové údaje k AWS**(credentials), ktoré umožnili prístup k databáze/heslám.
Incident 2018: prístup do GitHubu zostal aktívny po odchode vedúceho pracovníka; útočník využil jeho prihlasovacie údaje a našiel **AWS credentials**.
Incident 2020: podobný scenár – útočník získal AWS credentials cez GitHub, prenikol do databázy a **odcudzil zákaznícke údaje**.

Drizzly a Rellas

FTC vytýkala najmä tieto zlyhania (Drizly aj CEO):
Nesúlad medzi deklaráciami a realitou: firma tvrdila, že používa primerané bezpečnostné postupy, no **nezaviedla primerané opatrenia**.
Chýbajúce základné kontroly: nevyžadovala **2FA** pre GitHub, neobmedzila prístupy k osobným údajom, nemala **písomné bezpečnostné politiky** a **neškolila** zamestnancov.
Zlé nakladanie s tajomstvami: ukladanie prihlasovacích údajov na GitHub v rozpore s odporúčaniami a napriek známym incidentom (secrets management fail).
Slabé monitorovanie/detekcia: bez CISO a bez monitoringu pokusov o neoprávnený prístup či exfiltráciu dát.
Nápravné opatrenie FTC – dopad na CEO osobne:
povinnosť zaviesť a udržiavať **program informačnej bezpečnosti** počas **10 rokov** v každej budúcej spoločnosti, kde bude väčšinovým vlastníkom, CEO alebo zodpovedný za informačnú bezpečnosť, ak firma spracúva údaje **> 25 000 osôb**.

Ak organizácia nemá CISO alebo CEO preberie rolu kyberbezpečnosti, zvyšuje sa riziko **osobnej zodpovednosti** za zlyhania (a opatrenia môžu „nasledovať" manažéra aj do ďalšej firmy).

Ďalšie informácie

Časopis pro Právní Vědu a Praxi (MUNI Brno)

č. 3/2024 str. 483–513

„Trestnoprávna zodpovednosť manažéra kybernetickej bezpečnosti v českom a slovenskom právnom poriadku"

Jozef Čentéš, Michal Rampášek
https://doi.org/10.5817/CPVP2024-3-5

Modelový prípad -ransomvér

- Poskytovateľ digitálnych služieb pre ambulancie spracúva veľké objemy osobných údajov vrátane údajov o zdraví.
- **Incident:** útočník sa dostane do siete cez kompromitovaný účet (bez MFA), zašifruje dáta a podarí sa mu **exfiltrovať údaje**.
- **Požiadavka útočníka:** zaplatiť do 72h v **kryptomene,** inak zverejní dáta

1. útočník tvrdí, že „operuje z jurisdikcie", na ktorú sa vzťahujú **medzinárodné sankcie,** alebo používa jazyk/časové pásmo a infraštruktúru typickú pre taký štát,
2. v správe uvádza, že ak sa bude kontaktovať polícia, „zapojí štátnu ochranu" ,
3. poskytne **krypto adresu,** ktorú komerčné nástroje na analýzu blockchainu alebo poskytovateľ služieb virtuálnych aktív (VASP) označia ako „high risk / linked to sanctioned entity" (napr. napojenie na sankcionovanú burzu alebo službu),
4. platbu chce viesť cez konkrétnu službu, ktorá je známa obchádzaním sankcií alebo je v niektorých režimoch obmedzená.

- **Rozhodnutie manažmentu:** incident **neohlásiť** „kým nebudeme mať viac informácií" (obavy o reputáciu) a zvážiť **úhradu výkupného** pre obnovenie prevádzky.

Riziká

- Väčšina ransomvérových útokov prebieha anonymne.
- V podmienkach SR doposiaľ nie je známy prípad stíhania konkrétnej osoby.
- Existujú čiastočné možnosti atribúcie, napríklad na základe technických znakov útoku, komunikácie, alebo kryptopeňaženiek, ktoré môžu odkazovať na známe skupiny.
- Tri rizikové oblasti, ktoré aj zahraničná odborná literatúra opakovane označuje ako problematické pri platbe výkupného:

1) **Možné porušenie medzinárodných sankčných režimov,**
2) **Financovanie terorizmu,**
3) **Legalizácia výnosu z trestnej činnosti**.

Regulácia

- Závažný KB incident a povinnosť oznámiť podľa ZoKB
- SR je členom medzinárodnej iniciatívy proti ransomvéru (***Counter Ransomware Initiative*** **- CRI**)
- EU a Návrh revízie NIS2 (COM(2026) 13 final) zavedenie harmonizovaného zberu údajov o ransomvérových útokoch
- a) či subjekt odhalil ransomvérový útok; b)aký bol vektor útoku v prípade ransomvérového útoku; c) či boli vykonané zmierňujúce opatrenia a v prípade významného incidentu spôsobeného ransomvérovým útokom dotknuté subjekty na žiadosť uvedú a)či subjekt dostal žiadosť o výkupné a prípadne od koho; b)či bolo výkupné zaplatené, a ak áno, v akej výške, akým platobným prostriedkom a akému príjemcovi alebo prijímajúcej strane, prípadne vrátane kryptoaktíva a poskytovateľa služieb kryptoaktív.
- **Spojené kráľovstvo predstavilo v 2025 návrh legislatívy**
  - **cieleného zákazu** platieb výkupného pre všetky **orgány verejného sektora** vrátane miestnej samosprávy a pre vlastníkov a prevádzkovateľov **kritickej infraštruktúry**.
  - **režimu prevencie platieb,** kde každá obeť ransomvéru (okrem vyššie uvedených) by povinne oznámila svoj úmysel vykonať platbu výkupného a orgány by preskúmali či by mohla ísť sankcionovaným subjektom, alebo či ide o financovanie terorizmu (rozhodnutie o blokovaní)
  - povinné oznámenie incidentu do 72 hodín od zistenia

Kybernetické sankcie

- **Rozhodnutie Rady č. 2019/797** o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty a **Nariadenie Rady (EÚ) 2019/796** o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty
- **Zakazuje** priame alebo nepriame **sprístupnenie finančných prostriedkov** alebo hospodárskych zdrojov osobám uvedeným na sankčnom zozname.
- Implementácia medzinárodných sankcií cez **zákon č. 289/2016 Z.z. o vykonávaní medzinárodných sankcií** - medzinárodná sankcia je aj právne záväzný akt Európskej únie.

Kryptoaktíva

- Súčasným trendom je žiadať o zaplatenie **výkupného v niektorej z kryptomien**.
- Tento model pozostáva z dvoch fáz. V prvej fáze sa pôvod peňazí zakrýva pomocou tzv. **mixovacích služieb**. V druhej fáze sa kryptomeny prevedú na **kryptomenové adresy jedného alebo viacerých sprostredkovateľov,** po čom skončia u páchateľov
- **Privacy coins,** ako Monero (XMR), vynikajú svojimi vylepšenými funkciami anonymity, ktoré zahmlievajú transakcie
- **Nariadenie o kryptoaktívach (MiCA)** významne ovplyvňuje platby výkupného pri ransomvérových útokoch tým, že ukladá prísne požiadavky na poskytovateľov služieb kryptoaktív, čím obmedzuje anonymitu transakcií

Porušenie sankcií

- **Nový trestný čin Porušenie reštriktívneho opatrenia podľa § 417a ods. 1 písm a.)** *„Kto poruší reštriktívne opatrenie v rozsahu najmenej 10 000 eur, tým že sprístupní finančné prostriedky priamo alebo nepriamo označenej osobe alebo v jej prospech...“* (najprísnejšia sadzba TOS až 8 rokov)
- Účinnosť 1.6.2025
- Transpozícia **Smernice EÚ č. 2024/1226** o vymedzení trestných činov a sankcií za porušenie reštriktívnych opatrení Únie
- Obeť ransomvérového útoku, ktorá uhradí výkupné sankcionovanej osobe, subjektu alebo orgánu, by mohla naplniť skutkovú podstatu trestného činu podľa návrhu § 417a ods. 1 TZ.

Legalizácia výnosu

- Trestný čin legalizácie výnosu podľa § 233 ods. 2 TZ (úmyselné konanie, najprísnejšia sadzba TOS do 10 rokov) alebo podľa § 233a ods. 2 TZ (z nedbanlivosti, najprísnejšia sadzba TOS do 5 rokov).
- Rizikovým scenárom je keď obeť ransomvérového útoku umožní zatajenie pôvodu finančných prostriedkov z nedbalivosti:

- Hodnota zatajených finančných prostriedkov musí presiahnuť sumu 20 000 eur (vec väčšej hodnoty)

- Konanie z nedbanlivosti, napríklad tým, že neoverí, či služby, použité na úhradu výkupného (napr. kryptomenové burzy alebo peňaženky), neumožňujú anonymizáciu transakcií alebo nasleduje pokyny útočníkov bez zohľadnenia potenciálnych dôsledkov, prípadne že tieto služby sú známe nedodržiavaním pravidiel

Dôležitými faktormi pri posúdení konania sú:

1. Použitie anonymizačných nástrojov alebo metód na utajenie transakcií.

2. Neoznámenie ransomvérového útoku (incidentu) orgánom činným v trestnom konaní a NBÚ.

3. Spôsob vedenie transakcií v účtovníctve.

Financovanie terorizmu

- Trestný čin financovania terorizmu podľa § 419c TZ:

  „kto sám alebo prostredníctvom iného *zhromažďuje alebo poskytuje* priamo alebo nepriamo veci, finančné prostriedky alebo iné prostriedky pre páchateľa terorizmu, pre teroristickú skupinu, jej člena, alebo na spáchanie niektorého z trestných činov terorizmu, alebo zhromažďuje veci, finančné prostriedky alebo iné prostriedky v úmysle, aby ich bolo možné takto použiť, alebo s vedomím, že na taký účel môžu byť použité" (najprísnejšia sadzba TOS až do 15 rokov).

- „Páchateľ terorizmu" aj osoba nie je nevyhnutne členom teroristickej skupiny.
- Základným predpokladom spáchania je, že obeť vedome poskytne finančné alebo iné prostriedky osobe, ktorá je označená ako „páchateľ terorizmu" alebo ktorá je evidovaná v teroristických zoznamoch OSN či EÚ, a to buď priamo, alebo sprostredkovane.

Ďalšie informácie

Časopis pro Právní Vědu a Praxi (MUNI Brno)

č. 3/2025 str. 555 - 578

„Ransomvér a úhrada výkupného v kontexte trestného práva"

Jozef Čentéš, Michal Rampášek

https://doi.org/10.5817/CPVP2025-3-7

Modern Solutions (DE) – Oznamovanie zraniteľností

- Prípad sa týka bezpečnostného výskumníka/programátora, ktorý pri analýze softvéru zistil zraniteľnosť vedúcu k prístupu k databáze s osobnými údajmi koncových zákazníkov (cca 600–700 tis.).
- Bezpečnostná zraniteľnosť bola nájdená v middleware pre elektronický obchod od spoločnosti Modern Solution, ktorá bola navrhnutá tak, aby umožnila menším online obchodom ponúkať svoj tovar vo veľkých online obchodoch spoločností Kaufland, Otto, Check24 a ďalších. Modern Solution uchovávala údaje všetkých nakupujúcich, ktoré boli prostredníctvom tohto softvéru prenesené prevádzkovateľom softvéru Modern Solution, v jednej databáze. Heslo k tejto databáze na serveroch Modern Solution bolo uložené nešifrované v spustiteľnom súbore middleware softvéru a bolo rovnaké pre všetkých zákazníkov Modern Solution. To znamenalo, že ktokoľvek s prístupom k tomuto softvéru, ktorý bol v tom čase dostupný na stiahnutie z internetu, mohol tieto údaje ľahko získať.
- Amtsgericht Jülich (17. 1. 2024) ho uznal vinným zo skutku podľa § 202a StGB – Ausspähen von Daten (neoprávnené získanie prístupu k dátam) a uložil mu peňažný trest.
- Landgericht Aachen (4. 11. 2024) zamietol odvolanie a rozsudok AG Jülich potvrdil.
- Bundesverfassungsgericht (BVerfG) ústavnú sťažnosť neprijal na konanie, takže odsúdenie ostal oprávoplatné.

Modern Solutions (DE) – Oznamovanie zraniteľností

- Obžaloba strávila značnú časť pojednávania snahou dokázať, že obžalovaný dekompiloval kód softvéru spoločnosti Modem Solution, aby získal heslo pre pripojenie k databáze. Obžalovaný uviedol, že si predmetný súbor iba prezeral v textovom editore, a teda heslo k databáze prečítal v obyčajnom texte.
- Sudca uviedol, že samotná skutočnosť, že softvér mal heslo pre pripojenie, znamenala, že prezeranie nespracovaných údajov programu a následné pripojenie k databáze Modem Solution predstavovalo trestný čin.
- Odvolací súd zdôraznil, že obžalovaný sa mohol vyhnúť trestnej zodpovednosti, ak by prestal pristupovať k údajom hneď, ako si uvedomil, že má prístup k údajom zákazníkov, ktoré nemal vidieť. Skutočnosť, že tieto údaje zdokumentoval snímkami obrazovky, čo bolo počas súdneho konania nespochybniteľné, potvrdila jeho trestnú zodpovednosť.

Neoprávnený prístup do počítačového systému

- § 247 (1) Trestného zákona „Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.“

Cour de cassation (FR), 2. 9. 2025

- ECLI:FR:CCASS:2025:CR00934
- Obvinený bol zamestnanec – administrátor siete (správca IT) v spoločnosti a mal prístupové kódy k firemnej e-mailovej komunikácii všetkých zamestnancov vrátane konateľa. Súd mu preukázal, že tajne čítal archivované správy konateľa a deň pred disciplinárnym opatrením skryto nastavil automatické preposielanie e-mailov konateľa na svoju adresu.
- Bol odsúdený za trestný čin neoprávneného prístupu do počítačového systému alebo zotrvania v ňom podľa čl. 323-1 francúzskeho TZ
- Aj osoba s legitímnymi admin prístupmi môže spáchať trestný čin, ak tajne pristupuje k obsahu komunikácie mimo svojej pracovnej náplne

Neoprávnené nakladanie s počítačovými údajmi

- § 247b (1) Kto úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

- § 247a (1) Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti a) neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, alebo b) tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

- § 376 Kto neoprávnene poruší tajomstvo ... počítačových dát alebo iného dokumentu uchovávaného v súkromí iného tým, že ich zverejní alebo sprístupní tretej osobe alebo iným spôsobom použije a inému tým spôsobí vážnu ujmu na právach, potrestá sa odňatím slobody až na dva roky.

- § 264 (1) Kto vyzvedá obchodné tajomstvo, bankové tajomstvo, poštové tajomstvo, telekomunikačné tajomstvo alebo daňové tajomstvo v úmysle vyzradiť ho nepovolanej osobe alebo kto také tajomstvo nepovolanej osobe úmyselne vyzradí, potrestá sa odňatím slobody na šesť mesiacov až tri roky.