Transformace přístupu k zvládání hrozeb informační bezpečnosti: interní hrozby jako nová priorita

Redefining Threats: Extending the Threat Response Focus from External to Internal in Threats

Jiří Hološka [0009-0009-6559-8289*](jiri.holoska@vse.cz) – Incident Response and Insider Threat Manager at PwC, Assistant Professor at University of Economics, Prague., Petr Doucek[0000-0002-5647-661X] (petr.doucek@vse.cz) – Head of the Department of System Analysis, University of Economics, Prague, full professor since 2007 in Informatics.

ABSTRAKT

Cílem článku je analyzovat vzrůstající nebezpečí interních hrozeb a jejich dopadů pro bezpečnost podnikových informačních systémů a ukázat vybrané způsoby jejich možných řešení v podmínkách České s Slovenské republiky.

Podíl a význam insider incidents v současné podnikové praxi, zejména ve velkých organizacích, narůstá. Stejně tak roste motivace tyto incidenty vyšetřovat, jak ukazují presentované trendy z období 2016 – 2022. Stejně tak narůstají i finanční objemy jejich dopadů na organizace. Organizace se při řízení bezpečnosti informací věnují zejména řízení externích hrozeb, neboť insider incidents bývají presentovány jako snaha organizací zasahovat do soukromí změstnanců. Tento trend se začíná otáčet a metody vyšetřování incidentů způsobené zaměstnanci se dostávají do standardních vyšetřovacích procesů.

Článek rozebírá trendy v oblasti interních hrozeb, možnosti řešení a doporučení, jak se mohou organizace proti těmto hrozbám chránit, včetně podpory těchto vyšetřování z pohledu místní legislativy.

Category: Research paper

Keywords: informační bezpečnostní management; interní hrozby; informační bezpečnost; digitální stopy

Research Areas: Management of Technology and Innovation, ICT Security Management

ABSTRACT

Purpose of this article is to analyze the growing danger of insider threats and their impact on the security of company information systems and to show the select ways of their potential solutions in the Czech Republic and the Slovak Republic.

The volume and significance of insider incidents in today's corporate practice, particularly in large organizations, is increasing. At the same time, the motivation to investigate these incidents is also growing, as demonstrated by the trends observed during the period 2016–2022. The financial impact of such incidents on organizations is likewise on the rise.

Organizations primarily focus on managing external threats within their information security frameworks, as insider incidents are often perceived as an attempt to infringe on employee privacy. However, this perception is beginning to shift, and methods for investigating incidents caused by employees are gradually becoming part of standard investigative procedures.

The article focuses on insider threat trends, options and recommendations on how organisations can protect themselves against threats, including support for these investigations from the perspective of local legislation.

Keywords: Internal Threats; ICT Security; Digital Evidence; Insider Incident.

Research Areas: Management of Technology and Innovation, ICT Security Management

1 ÚVOD

Z pohledu zajištění bezpečnosti ICT organizace je možné identifikovat dva základní typy hrozeb – interní a externí (ISO/IEC 27005). Většina pozornosti útvarů ochrany informací a dat v organizacích je zaměřena na externí hrozby. Ale současný vývoj upozorňuje i na vážná nebezpečí hrozeb interních, a to zejména od vlastních zaměstnanců (Catrantzos, 2022). Mezi první organizace, které identifikovaly dopady interních hrozeb celosvětově, a to i mimo informační a komunikační technologie (ICT), patří informační služby. Infiltrace organizace, nebo únik informací měl sílu vyřadit operační schopnosti organizace v daném regionu, nebo ohrozit životy agentů (Hellberg, 2013). Na identifikaci interních hrozeb rychle navázaly organizace zapojené do technologických inovací, zejména pak do vývoje technických výrobků s důrazem na vojenskou techniku. Důkazem může být, že na základě vizuálního porovnání lze jasně identifikovat společné rysy různých plagiátorských výrobků s jejich původními originály. Příkladem může být vzhled některých nově vyvíjených dronů nebo dokumentace ponorek (Bing, 2018). Dalším důkazem nebezpečnosti úniku dat prostřednictvím vlastních zaměstnanců je pak případ letadel F-35 (Gady, 2015). Tyto dokumenty se objevily na „dark webu“ a byly předmětem obchodování.

Tento trend se s rozvojem mobilních technologií, jako jsou chytré telefony, notebooky a osobní cloudové služby přelil do ostatních organizací napříč celým technologickým spektrem. Uživatelé ve výpovědní lhůtě kopírují celé složky k projektům, na kterých pracovali, nebo o kterých si myslí, že jim v nové organizaci přinesou konkurenční výhodu.

Vnitřní hrozby se neomezují pouze na ztrátu dat jako takovou, ale mohou nabývat i čistě destruktivní podoby (Payne, 2022). Frustrovaní privilegovaní uživatelé, se mohou jednoho dne rozhodnout provést neutorizované změny ve firemní, nebo výrobní infrastruktuře s cílem ventilovat frustraci, poukázat na neřešené problémy, nebo poškodit dobré jméno firmy (Press Relaese, 2022). Zejména zranitelné jsou oblasti zpracování a dodávek pitné vody, nebo distribuce pohoných hmot a elektrické energie (Abrams, 2008).

Další oblastí, kde mohou mít vážné dopady interní hrozby, je únik intelektuálního vlastnictví. Ty mohou být pro společnost z pohledu konkurenceschopnosti likvidační. Roky výzkumu se během několika dní dostanou ke konkurenci a konkurenční výhoda

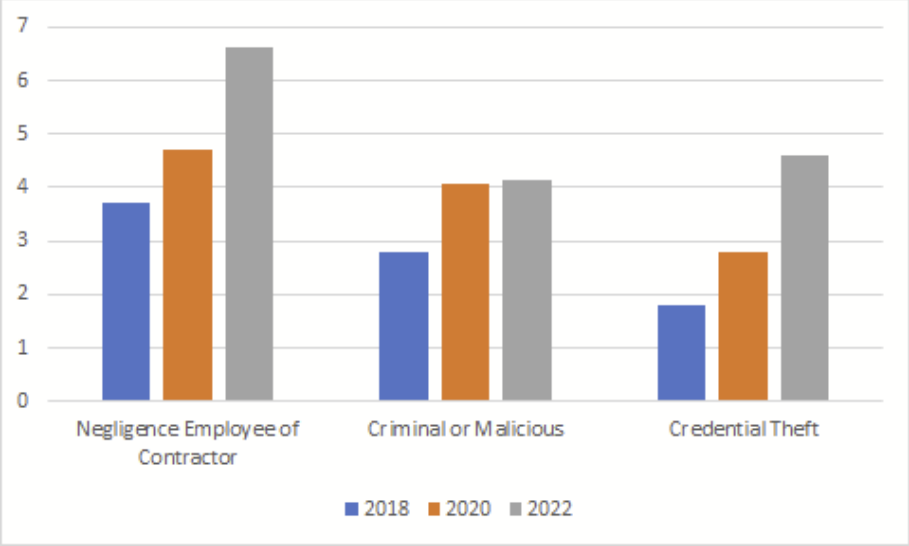
na trhu zmizí přes noc. Ekonomické dopady v podobě ztrát na burze mohou během několika měsíců vymazat roky práce organizace a dlouhé období pozitivních ekonomických výsledků (Bunn, 2017).

Příkladem takového jednání je i bývalý zaměstnanec organizace Ubiquity pan Nickolas Sharp , který odcizil 10 GB důvěrných dat. Následně se pokusil firmu anonymně vydírat a vyhrožoval zveřejněním dokumentů, pokud nedostane zaplaceno $1.9 milionu dolarů. Společnost Ubiquity se rozhodla výkupné nezaplatit a začala spolupracovat s FBI. Vyšetřování odhalilo Sharpa jako strůjce úniku dat, ten se obratem začal stylizovat do role whisleblowera a přes média nepravdivě publikoval informace o interním vyšetřování jím způsobeného úniku informací. Výsledkem byl propad ceny akcií o zhruba 20 % a ztráta čtyř miliard USD tržní hodnoty pro Ubiquity. V květnu 2023 byl Sharp odsouzen k šestiletému vězení, tříletá podmínka po propuštění a dále mu bylo uloženo zaplatit více jak $1.5 milionu USD na odškodném (Press Relaese, 2023; Belanger, 2023).

Je tedy zřejmé, že s postupem digitalizace se otvírají nové možnosti pro úmyslné, ale i nedbalostní incidenty s dopadem na koncové uživatele.

Společnost Cybersecurity Ventures očekává, že celosvětové náklady na kybernetickou kriminalitu porostou v příštích pěti letech o 15 % ročně a do roku 2025 dosáhnou 10,5 bilionu USD ročně, přičemž v roce 2015 činily 3 biliony USD. To představuje největší přesun ekonomického bohatství v historii, ohrožuje pobídky k inovacím a investicím, je exponenciálně větší než škody způsobené přírodními katastrofami za rok a bude výnosnější než celosvětový obchod se všemi hlavními nelegálními drogami dohromady (Morgan, 2021).

Náklady, které vznikají na řešení insider incidents také meziročně permanentě stoupají, a to nejen v jednotivých kategoriích, ale i celkově. Jejich vývoj ve velkých organizacích v letech 2018-2022 můžeme vidět na následujícím Obr. 1.



Obr. 1. Dopady Insider Incidents v letech 2018 – 2022 v mio USD zdroj: (Ponemon, 2023)

1.1 Kompetence při vyšetřování dopadů interních hrozeb

Agentura pro kybernetickou bezpečnost a bezpečnost infrastruktury (CISA) definuje interní hrozbu jako hrozbu, kdy osoba s oprávněným přístupem úmyslně nebo neúmyslně zneužije tento přístup k poškození poslání, zdrojů, personálu, zařízení, informací, vybavení, sítí nebo systémů daného úřadu. Interní hrozby se mohou projevovat různými způsoby: násilím, špionáží, sabotáží, krádeží nebo kybernetickými útoky (CISA, 2023). Insider je tedy jedinec nebo dodavatel s lokální znalostí organizace, jejichž autorizovaný přístup je vědomě nebo i nevědomě zneužit k získání a exfiltraci zájmových dat. Případně se jedná o interní bezpečnostní týmy s rozšířenou působnosti a přístupy k auditovaní uživatelských aktivit, nebo specializované firmy poskytující služby odhalování a vyšetřování interních hrozeb.

Vyšetřování interních hrozeb je doménou komerčních organizací, které si v konkurenčním prostředí musí chránit svoje duševní a průmyslové vlastnictví, know-how, informace o klientech, nebo jakékoliv jiné informace, které jsou přímo nebo nepřímo využívány k získání konkurenční výhody a finančního zisku.

V praxi se obvykle setkáváme se třemi hlavními skupinami uživatelů podle motivace:

- Nespokojený/zákeřný uživatel.
- Nedbalý uživatel.
- Infiltrátor.

Vyšetřování zaměstnanců spadá primárně do kompetence daných organizací, za určitých okolností může ovšem vyšetřování provádět externí firma. Vyšetřovací tým je složený z bezpečnostních analytiků, kteří mají na starost zajištění, zpracování a interpretaci digitálních stop. Personální oddělení, má na starosti komunikaci se zaměstnancem, zajištění nestranného a důstojného zacházení s ním. Stejně tak i koordinaci s ostatními týmy, dokumentaci vyšetřování, eskalaci a reportování vedoucím pracovníkům. Dále osobní oddělení provádí závěrečné hodnocení vyšetřování s ohledem k platným vnitřním předpisům a doporučením společnosti a případné zahájení disciplinárního řízení. Právní oddělení garantuje, že vyšetřování probíhá v souladu se zákony a předpisy platnými pro daný stát a odvětví. Dále právní oddělení provádí vyhodnocení nálezů a poskytují doporučení, nebo přímo sděluje příslušným organizačním jednotkám povinnost informovat o incidentu orgány státní správy, jako tomu je například u nařízení o ochraně osobních údajů (GDPR). Stejně tak je tomu i u incidentů zahrnujících ztrátu osobních informací, kdy je ze zákona nutné tuto skutečnost bez zbytečného odkladu oznámit Úřadu pro ochranu osobních údajů.

Vyšetřování se obvykle účastní i nadřízení zaměstnance, kteří poskytují kontext ke zjištěným uživatelským aktivitám.

1.2 Cíl článku

Cílem tohoto článku je poukázat na rostoucí nebezpečí vnitřních hrozeb a jejich významu pro bezpečný chod podnikových informačních systémů v celosvětovém kontextu. Interním hrozbám se z různých důvodů, jako jsou např. ochrana soukromí vlastních zaměstnanců, jejich diverzita a loajalita vůči zaměstnavateli, až taková pozornost nevěnuje. To ovšem v praxi může způsobit úniky dat, komplikované právní

situace a následně celkovou ztrátu konkurenceschopnosti dané organizace. Kromě toho se článek zabývá i vybranými způsoby, jak vnitřním hrozbám metodicky předcházet s přihlédnutím k legislativě České a Slovenské republiky.

2 METODOLOGIE

Pro zpracování podkladů toho článků jsme využili tří hlavních zdrojů. Prvním z nich jsou kvantitativní data, která jsou uvedena za roky 2016-2022 např. ve studii, která je výsledkem dotazníkového šetření Ponemon Institutem v roce 2023. Zde vycházíme z metodiky použité při studii (Ponemon, 2023), kdy jsme data získaná z firem rozdělili podle tří typů incidentů:

- relating to negligence,
- relating to criminal insider,
- relating to user credential theft.

Druhým zdrojem pro tuto studii jsou závěry a zkušenosti z celé řady komerčních i vědeckých projektů v oblasti bezpečnosti.

Třetím zdrojem je pak studium odborné literatury a dokumentů, které se zabývají problematikou bezpečnosti informací v organizacích.

3 RESUTLS

Výsledky jsme rozdělili do dvou relativně samostatných částí. V prvním bloku jsou dílčí závěry z vyhodnocených dat 278 velkých organizací ve světě, kde formulujeme některé základní trendy v insider incidents v letech 2016-2022. Velké organizace jsou regionálně procentně zastoupeny následujícím způsobem – Severní Amerika 44 %, Evropa 27 %, Asie 19 %, Afrika a Arábie 10 %.

Druhý blok pak obsahuje návrhy na řešení tohoto typu incidentů v konkrétních podmínkách České a Slovenské republiky.

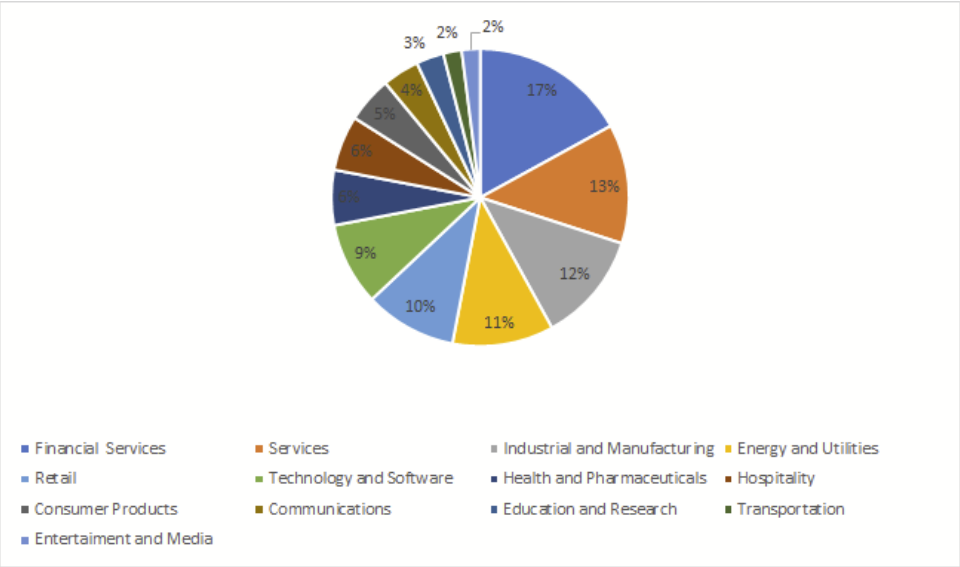
3.1 Stav Insider Incidents a trendy jejich vývoje

Prvními výstupy jsou elementární charakteristiky získaných dat. Při studii byly získány podklady od celkem 278 firem, které prošly 6.803 insider incidents s celkovými ztrátami 15,4 milionů USD. Členění insider incidents podle typu je uvedeno v následující Tab. 1

Tab. 1. Členění analyzovaných insider incidents podle typu. Zdroj: (Ponemon, 2023)

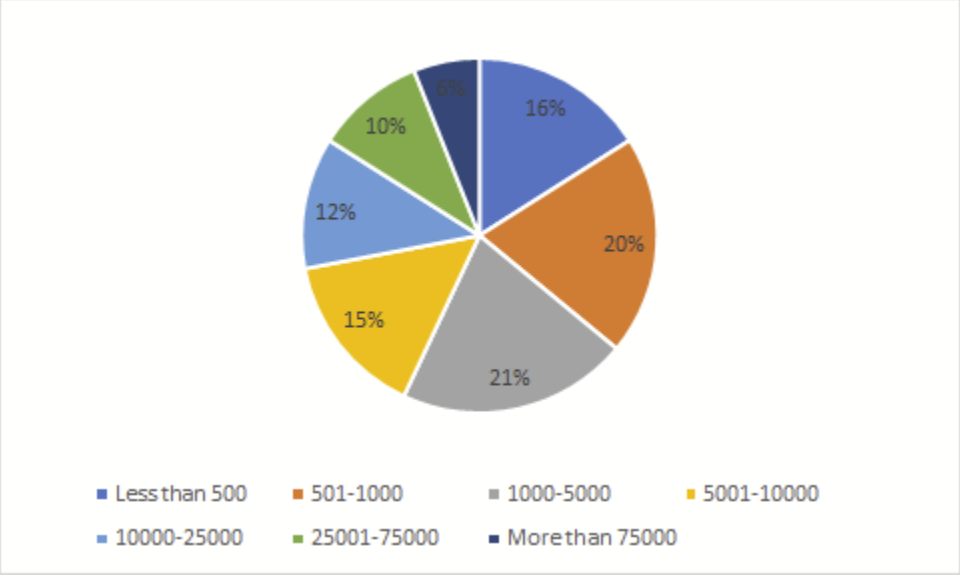
Incidents Relating to	Percentage	Annual Costs in Mio USD
Negligence	56	6.6
Criminal Insider	26	4.1
Credential Theft	18	4.6
Sum	100	15.3

Na následujícím Obr. 2 je uvedena struktura dotázaných organizací podle sektoru ekonomiky, kde vyvíjejí svoji hlavní činnost.



Obr. 2. Zastoupení organizací v průzkumu podle sektoru ekonomiky zdroj: (Ponemon, 2023)

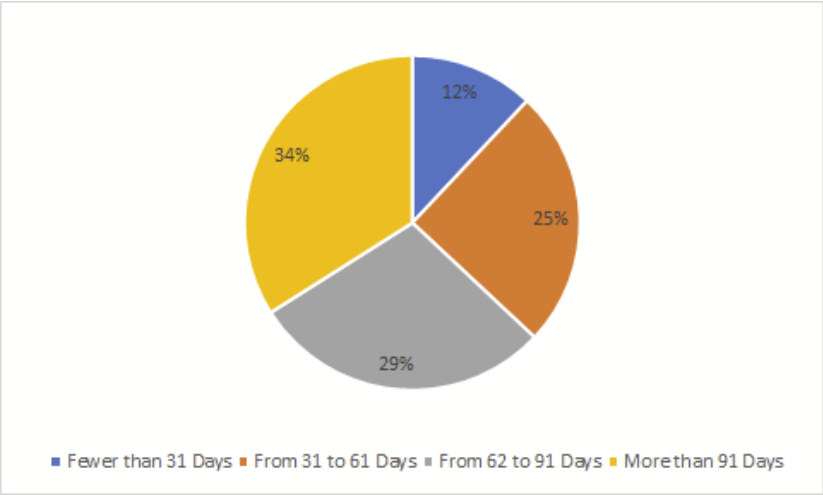
Obr. 3 prezentuje u organizací, jejichž data jsme měli ve výzkum k dispozici, jejich velikost podle počtu zaměstnanců, jejichž data jsme ve výzkumu zpracovávali. Z obrázku je jasně patrné, že se jedná zejména o větší a velké společnosti nad 500 zaměstnanců.



Obr. 3. zastoupení společností podle počtu zaměstnanců zdroj: (Ponemon, 2023)

Jak je také vidět z Obr. 3, jedná se především o velké organizace, jak je klasifikuje Evropská Unie. Proto ani další naše úvahy a doporučení se primárně netýkají mikrofirem a malých a středních firem (SMEs). SMEs jsou ve vzorku zastoupeny pouze 16 %.

Dalším velmi významným rizikem insider incidents je doba, která uplyne od jejich zjištění a uvedení systému organizace do původního stavu. Po tuto dobu je organizace vystavena hrozbám, které incident aktivoval. Průměrná doba „životnosti“ incidentu a tedy i průměrná doba do jeho odstranění jsou uvedeny na následujícím Obr. 4.

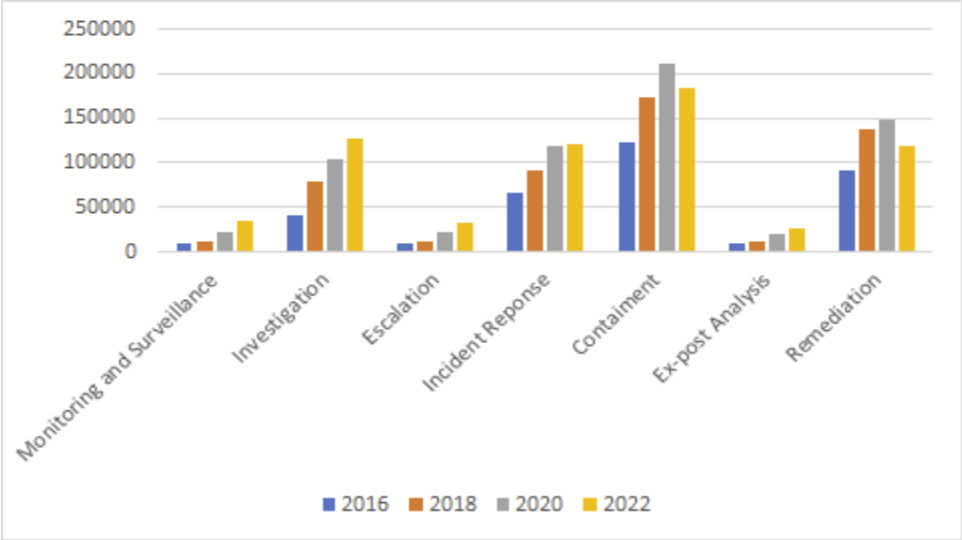


Obr. 4. Průměrné doby do vyřešení insider Incidents zdroj: (Ponemon, 2023)

Zde je základním problémem identifikace takového incidentu, protože interní uživatel může využívat informační systém organizace ke svému osobnímu prospěchu (v minulosti to byla nejčastěji těžba kryptoměny nebo retailové aktivity pro jiné subjekty, než je zaměstnavatel).

3.2 Návrhy na ochranu proti Insider Incidents

Pro organizace jsou dalším klíčovým faktorem náklady, které jsou spojené s řešením insider incidents. Na jejich vývoj mezi lety 2016-2022 se podívejme na Obr. 5.



Obr. 5. Náklady v životním cyklu řešení incidentu zdroj: (Ponemon, 2023)

Data zde uvedená představují průměrné náklady na jeden bezpečnostní insider incident, jak jej identifikovalo sedm security operation centres. Mezi nejnákladnější etapy životního cyklu incidentu patří vyšetřování, reakce na incident, izolace a obnovení běžné funkce organizace.

Pojďme se podívat podrobněji na to, jak se preventivně chránit před insider incidents.

Ochranu před externími hrozbami jsou organizace často nuceny řešit už na legislativní úrovni (Gelles, 2016), ochrana před interními hrozbami je stále spíše tabuizované téma,

na které je nahlíženo jako na narušení soukromí zaměstnanců. Důvěrnost a zabezpečení citlivých informací je potřeba řešit nejen na technologické úrovni, ale taktéž řádným (nikoli formálním) proškolením v oblasti bezpečného používání firemních informačních a počítačových systémů. Potvrzení uživatelů o akceptování práv, povinností a odpovědnosti zaměstnanců ve vztahu k informačním technologiím je klíčové k dosažení přijatelné míry informační bezpečnosti.

Jaké jsou základní nástroje administrativní bezpečnosti proti insider threats.

Etický kodex (tzv. „Code-of-Conduct“) je závazný soubor zásad chování a společenských norem, u nichž organizace očekává, že budou její zaměstnanci dodržovat. Konrétní obsah etického kodexu je specifický pro každou organizaci. Společným obsahem bývá čestné prohlášení o znalosti a dodržování platné legislativy pro daný obor činnosti. Odpovědnost a povinosti zaměstnanců identifikovat a hlásit škodní a nestandardní události. S ohledem na ochranu citlivých informací by měl etický kodex obsahovat obecná pravidla pro nakládání s daty, kontrolu přístupů, šifrování a hlášení incidentů s odkazem na směrnici o informační bezpečnosti, která obsahuje detailní pokyny pro správné používaní podnikových informačních systémů a ochranu proti neoprávněnému přístupu k datům.

Dohoda o mlčenlivosti – Non-Disclosure-Agreement (NDA) je právně závazná smlouva mezi dvěma, nebo více stranami, která definuje důvěrnost ve vztahu ke spřístupněným informacím, včetně pokut za její porušení. Jedná se o způsob, jak chránit citlivé informace, nebo data, která nejsou chráněna jinými zákony, jako je například autorský zákon. NDA je vhodný doplněk k pracovní smouvě pro zaměstnance, kteří přicházejí do styku s důvěrnými firemními informacemi a dokumenty.

Klasifikace dokumentů podle úrovně důvěrnosti obsahu. Daná úroveň důvěrnosti dokumentu následně určuje uživatelům způsoby práce s dokumentem, komu mohou dokument sdílet, kde a jakým způsobem muže být dokument uložen.

Dokumenty označené správnou úrovní důvěrnosti, lze sledovat pomocí nástrojů Data Loss Prevention (DLP) a neoprávněný přístup k dokumentům reportovat jako incidenty pro Data Security tým.

Úroveň zabezpečení lze zvýšit proaktivními opatřeními omezujícími možnosti uživatele exfiltrovat data. Mezi ně se řadí omezení přístupu k osobnímu emailu, tisku dokumentů, nebo blokovanání zápisu na externí USB disky a cloudová úložiště. Pokud není možné tato opatření nasadit plošně, je vhodné je použít alespoň pro uživatele ve výpovědní lhůtě.

Vyhodnocování vzorů chování uživatelů – User behavioral analysis (UBA) funguje na základě dlouhodobého sledování chování uživatelů a vytváření vzorů pro detekci jejich nestandartního chování. Specificky lze idenfikovat zda se uživatel nezajímá o dokumeny z projektů se kterými bežně nepracuje, nebo identifikovat zvýšený výskyt stahovanání dokumentů z centrálních úložišť na pracovní stanici.

Efektivní řešení pro ochranu dat proti úniku se skládá z kombinace formálních smluv (Veber, 2016) se zaměstnanci s přístupem k důvěrným dokumentům, kvalitním školením zameřeným na bezpečné nakládání s daty a technickými prostředky pro prevenci a detekci neautorizovaných operací s důvermými daty.

4 VÝSLEDKY A DISKUZE

Zneužívání neveřejných informací k osobnímu obohacení, je koncept značně předcházející informační technologie, ale právě rozvoj osobních počítačů a internetu, otevřel nové možnosti k získání finanční nebo konkureční výhody.

Zneužívání neveřejných informací na burzovním operacích a obecně investic do akcií patří mezi první typ monetizace informací, který byl ošetřen zákonem. Ve Spojených státech Amerických byly první zákony regulující burzovní operace a obchody s investičními nástroji v roce 1933. Nejpve byl přijat Securities Act a následně Securities Exchange Act, cílem bylo dosáhnout prostředí, kde budou mít všichni účastnící stejnou šanci dosáhnout zisku. V České Republice byl v roce 1991 ustanoven §128 trestního zákoníku č. 557/1991 Sb, zneužívání informací v obchodním styku, který v důvodové zprávě pokrývá právě "Insider Trading"[1]. Aktuálně "Insider Trading" patří v české legislativě pod § 255 trestního zákoníku č. 40/2009 Sb., Zneužití informace v obchodním styku a Zákon č. 300/2005 Z. z. – § 265 Zneužívanie informácií v obchodnom styku dle slovenské legislativy.

Firemní informace a data, které lze klasifikovat jako umělecká, nebo vědecká díla, jsou chráněny autorským zákonem č. 121/2000 Sb. v České republice a 185/2015 Z.z. na Slovensku[2,3]. Důležitým aspektem těchto děl je požadavek na vyjádření tvůrčí činnosti. Český i Slovenský právní řád považuje za autorské dílo také počítačové programy[4], nebo například databáze a to i za předpokladu že postrádají prvky originality[5]. U databází je brána v úvahu časová a finanční investice, potřebná k vytvoření dané databáze (právo sui generis)[6]. Technická řešení, na něž je udělen patent, nebo technická řešení zapsaná v rejstříku užitných vzorů jsou chráněna zákonem zákonem č. 221/2006 Sb., Zákon o vymáhání práv z průmyslového vlastnictví a ochraně obchodního tajemství.

Obecně přijatelným řešním pro ochranu firemních dokumentů a intelektuláního vlastnicví je uzavření dohody o mlčenlivosti včetně jasně uvedených sankcí v případě porušení smouvy.

Specifickými případy vyšetřování jsou incidenty spojené s legislativou GDPR, telekomunikačního[7,8], obchodního[9,10] a bankovního tajemství[11,12], nebo kybernetického zákona[13,14], které se konkrétně vyjadřují k jednotlivým typům chráněných informací.

---

[1] Zákon č. 557/1991 Sb., zákon, kterým se mění a doplňuje zákon č. 140/1961 Sb., trestní zákoník
[2] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů
[3] Zákon č. 185/2015 Z. z. - Autorský zákon
[4] Směrnice 2009/24/ES o právní ochraně počítačových programů
[5] Zákon č. 185/2015 Z. z. - Autorský zákon, ŠTVRTÁ ČASŤ, PRÁVA K DATABÁZE
[6] KOHUTOVÁ, PhDr. et Mgr Radka. Právní ochrana databází. Praha, 2012. Rigorózní práce. Univerzita Karlova v Praze.
[7] Zákon 151/2000 Sb. - zákon o telekomunikacích
[8] Zákon č. 452/2021 Z. z. - Zákon o elektronických komunikáciách,§ 117 Telekomunikačné tajomstvo
[9] Nový občanský zákoník č. 89/2012 Sb., § 504 Obchodní tajemství
[10] Zákon č. 513/1991 Zb. - Obchodný zákonník, Diel V, Obchodné tajomstvo
[11] Zákon č. 21/1992 Sb. - Zákon o bankách, § 38 odst. 1 - bankovní tajemství
[12] Zákon č. 483/2001 Z. z. - Zákon o bankách, štrnásta časť, ochrana klientov a bankové tajomstvo
[13] Zákon č. 181/2014 Sb. - Zákon o kybernetické bezpečnosti
[14] Zákon č. 69/2018 Z. z. - Zákon o kybernetickej bezpečnosti

V obecné rovině se poškozováním a zneužíváním počítačových systémů a v nich uložených informací zabývá trestní zákoník § 230 (Česko), a Trestný zákon § 247 (Slovensko) zaměřený na neoprávněný přístup k počítačovému systému a nosiči informací [15, 16].

5 ZÁVĚR

Postupy uvedené v kapitole výsledky a diskuze lze volně aplikovat na neuatorizované přístupy uživatelů k informačnímu systému s cílem zjišťovat informace o zákaznících, nebo jejich službách.

Zásadním rozdílem mezi externími hrozbami a těmi interními je znalost hodnoty jednotlivých informačních zdrojů a specifických dokumentů. V případě Tele Denmark Communications (TDC), byl rozhodujícím faktorem přístup k detailům informací v neveřejné nabídce firmy Ericsson pro výstavbu mobilní 5G sítě, v jiných případech to mohou být identifikační a lokalizační údaje zákazníků, nebo záznamy ze systémů státní správy.

Hodnocení rizik spojených s typy informací je v kompetenci daných organizací, včetně návrhu konkrétních protiopatření a procesů pro monitoring a vyšetřování. Český právní řád škodní události spojené s vnitřními hrozbami vcelku dostatečně pokrývá, nicméně konsolidace výše zmíněných zákonů a do jednotné právní úpravy, by byla přínosem zejména z pohledu rozdílových analýz a bezpečnostních auditů.

PODĚKOVÁNÍ

Paper was processed with support from institutional-support fund for long-term conceptual development of science and research at the Faculty of Informatics and Statistics of the Prague University of Economics and Business (IP400040).

ZDROJE

BING, Chris: Stolen U.S. drone documents found for sale on dark web, July 11, 2018, https://cyberscoop.com/us-drone-dark-web-us-air-force-recorded-future/), last accessed 2023/06/23.

MORGAN, S.: Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, last accessed 2023/06/23.

CATRANTZOS, Nick. Managing the Insider Threat: No Dark Corners and the Rising Tide Menace. 2nd Edition. Florida, USA: CRC Press, 2022. ISBN 978-1032274249.

PAYNE, Joe, Jadee HANSON a Mark WOJTASIAK. Inside Jobs: Why Insider Risk Is the Biggest Cyber Threat You Can't Ignore. New Yorku, USA: Skyhorse, 2022. ISBN 1510764488.

BUNN, Matthew. Insider Threats (Cornell Studies in Security Affairs). Ithaca, New York, USA: Cornell University Press, 2017. ISBN 978-1501705175.

ABRAMS, Marshall, Joe WEISS: Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia. https://www.mitre.org/sites/default/files/pdf/08_1145.pdf , https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire/

[15] Trestní zákoník 40/2009 SB. § 230 - Neoprávněný přístup k počítačovému systému a nosiči informací.
[16] Zákon č. 300/2005 Z. z. - Trestný zákon § 247 Neoprávnený prístup do počítačového systému.

CISA, 2023. Insider Threat Mitigation: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

GADY, Franz-Stefan: New Snowden Documents Reveal Chinese Behind F-35 Hack: Experts have long argued that China has copied the F-35 design for its own fighter jets. Is this the proof?, https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/, January 27, 2015 last accessed 2023/08/10

PRESS RELAESE (2022). PH.D. Chemist Sentenced To 168 Months For Conspiracy To Steal Traded Secrets, Economic Espionage, Theft Of Trade Secrets, And Wire Fraud, https://www.justice.gov/usao-edtn/pr/phd-chemist-sentenced-168-months-conspiracy-steal-traded-secrets-economic-espionage, May 9, 2022, last accessed 2023/08/05.

PRESS RELAESE, 2023. Former Employee Of Technology Company Sentenced To Six Years In Prison For Stealing Confidential Data And Extorting Company For Ransom, May 10, 2023, https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-sentenced-six-years-prison-stealing-confidential, last accessed 2023/08/05

BERLANGER, Ashley: Ex-Ubiquiti engineer behind “breathtaking” data theft gets 6-year prison term, https://arstechnica.com/tech-policy/2023/05/ex-ubiquiti-engineer-behind-breathtaking-data-theft-gets-6-year-prison-term/, 5/11/2023, last accessed 2023/08/05

HELLBERG, Magnus (7 December 2013). "Spionen Stig Bergling plågas av dödstankar" [The spy Stig Bergling tormented by thoughts of death]. Expressen (in Swedish). Retrieved 3 May 2016. https://www.expressen.se/nyheter/spionen-stig-bergling-plagas-av-dodstankar/

VEBER, Jaromír, NEDOMOVÁ, Lea, DOUCEK, Petr. Corporate Digital Incident Investigation. Quality Innovation Prosperity [online]. 2016, roč. 20, č. 1, s. 57–70. ISSN 1335-1745. DOI: 10.12776/QIP.V20I1.656.

PONEMON, 2023. 2022 Ponemon Cost of Insider Threats Global Report, 2022

GELLES, Michael G. Insider Threat: Prevention, Detection, Mitigation, and Deterrence. Butterworth-Heinemann, 2016. ISBN 978-0128024102.