POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra managementu a informatiky

Možnosti, formy a nástroje pro zajištění bezpečnosti podniku v současných podmínkách

Bakalářská práce

Possibilities, forms and tools for ensuring the security of the company in the current conditions

Bachelor thesis

VEDOUCÍ PRÁCE

Dr. Nový Jindřich Ph.D.

AUTOR PRÁCE

Kateřina Bžatková

Praha

2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 3.9. 2023

Kateřina Bžatková

ANOTACE

Bakalářská práce se zaměřuje na zajištění podnikové bezpečnosti v současných podmínkách.
V práci je vysvětleno, jaké jsou pro podnik možnosti při zajištění bezpečnosti, jakými způsoby se podnik může bránit a čím musí podnik disponovat, aby byla bezpečnost zajištěna.
Na základě dostupných analýz je uvedeno, jakým způsobem jsou podniky okrádány nejčastěji. Dále se práce více zaměřuje na podvody ze strany zákazníka a na kybernetické útoky, přičemž u obou případů jsou podrobněji popsány konkrétní způsoby, jakými mohou podniky těmto hrozbám zamezit.

KLÍČOVÁ SLOVA

Bezpečnost podniku, podvod, zpronevěra, audit, datová analýza, kybernetická bezpečnost, Bezpečnostní softwary, systémy řízení identit

ANNOTATION

The bachelor's thesis is focused on ensuring company security under current conditions.
The thesis explains the options available to a business for ensuring security, the methods a business can employ to defend itself, and the resources it must possess to guarantee security.
Based on available analyses, it outlines the most common ways in which businesses are frequently targeted. Furthermore, the thesis delves into customer fraud and cyberattacks, providing detailed descriptions of specific measures that businesses can take to mitigate these threats in both cases.

KEYWORDS

Security of the company, fraud, misappropriation, audit, data analysis, cyber security, computer security software, identity management

Obsah

Úvod

Úspěch každého podniku závisí na řadě faktorů, přičemž jedním z podstatných je, jakým způsobem se podnik dovede bránit před hrozbami ohrožující jeho zájmy. Když se řekne pojem bezpečnost podniku, řada lidí si pod tím představí BOZP - bezpečnost a ochrana zdraví při práci. Nicméně pojem bezpečnost podniku je daleko širší a zahrnuje velkou škálu procesů, jejichž výsledkem je zajištění bezpečnosti v mnoha oblastech.

Bezpečnost podniku je neustále zkoumané téma, na které se pravidelně zpracovávají analýzy ukazující, že hrozby mají ve spoustu oblastech stále vzestupnou tendenci. Technologický vývoj a rostoucí propojenost prostřednictvím digitálních kanálů otevírají nové cesty pro kybernetické útoky a další formy hrozeb.

Zároveň analýzy upozorňují, že bezpečnostní opatření zaváděné podniky nejsou dostatečné, a proto je potřeba se na zajištění bezpečnosti více zaměřit.

Cílem této práce je na základě rešerše materiálů vysvětlit problém bezpečnosti podniku. Uvést jaké mají podniky možnosti, jakou formou a jaké používají nástroje, k tomu, aby zajištění podnikové bezpečnosti dosáhly.

Název práce určuje zajištění bezpečnosti v současných podmínkách, proto zdroje ze kterých tato práce čerpá, jsou především průzkumy a analýzy z posledních let, které zachycují současnou situaci. Na základě zdrojů je nejprve zpracován úvod do problematiky. Protože téma se zdá značně široké, je v další části práce potřeba si vybrat jen určité oblasti podnikové bezpečnosti, které se v úvodu práce ukáží jako nejvíc klíčové.

Nejprve je potřeba uvést stěžejní pojmy, na které se tato práce zaměřuje.

Podnik

Podnikem se rozumí každý subjekt vykonávající hospodářskou činnost, bez ohledu na jeho právní formu. K těmto subjektům se řadí osoby samostatně výdělečně činné, rodinné podniky vykonávající řemeslné či jiné činnosti, obchodní

společnosti, organizace a sdružení, která běžně vykonávají hospodářskou činnost.[1]

Chráněné zájmy podniku

Chráněné zájmy či základní zájmy podniku jsou cíle podniku, které jsou prioritně ochraňovány.
Jedná se o široký pojem, mezi chráněné zájmy podniku se řadí ochrana hmotného majetku, ochrana nehmotného majetku a ochrana osob.

Ochrana hmotného majetku zahrnuje ochranu jak movitého, tak nemovitého majetku, jako jsou objekty, prostory, výrobní zařízení, pracovní pomůcky, materiál a polotovary. Cílem je předcházet rozkrádání, ztrátám a zpronevěře.

Oblast nehmotného majetku zahrnuje ochranu důležitých obchodních informací, provozně výrobních dat, know-how firmy, vynálezů, výzkumu, osobních údajů zaměstnanců a patentových práv.

V případě ochrany osob se podnik stará o bezpečnost majitelů podniku a jejich rodinných příslušníků, vedení firmy, zaměstnanců a i návštěvníků.

Celkově zabezpečení těchto různých cílů je klíčové pro udržení stability, dobrého jména a trvalého úspěchu podniku.[2]

Hrozby, rizika

Hrozba je jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné podnikem. Na konkrétní hrozbu se vždy vtahuje i riziko.[3]

Riziko je definováno jako možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí.[4]

---

[1] DEFINICE PODNIKU. *Technologická agentura ČR* [online]. 2020, 3 [cit. 2023-09-03]. Dostupné z: https://www.tacr.cz/wp-content/uploads/documents/2020/02/24/1582544648_definice_podniku.pdf
[2] Základní pojmy pro krizové řízení. Specifické pojmy používané v krizovém řízení. *Oborový portál pro BOZP* [online]. 2003, 3 [cit. 2023-09-03]. Dostupné z: https://www.bozpinfo.cz/zakladni-pojmy-pro-krizove-rizeni-specificke-pojmy-pouzivane-v-krizovem-rizeni
[3] Obecné pojmy - Hrozba. *Policie.cz* [online]. 2003 [cit. 2023-09-03]. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx
4 Obecné pojmy - Riziko. Policie.cz [online]. 2003 [cit. 2023-09-03]. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx

Bezpečnost podniku

Bezpečnost podniku lze definovat jako stav, ve kterém ekonomika objektu, jehož bezpečnost má být zajištěna, není ohrožena hrozbami, které výrazně snižují nebo by mohly snížit ekonomickou výkonnost potřebnou k zajištění kapacit, sociálního smíru a konkurenceschopnost objektu i jeho jednotlivých složek na vnějších i vnitřních trzích.[5]

Dříve než podnik zavádí jakýkoliv bezpečnostní systém, je potřeba vědět co chce chránit a proč to chce chránit.

Pokud chce podnik svoji bezpečnost zajistit, musí si položit tři klíčové otázky. Jestli má vůbec možnost podnikovou bezpečnost ovlivnit, jakými způsoby lze bezpečnosti dosáhnout a jaké nástroje k tomu může použít. Odtud plyne i význam tří důležitých pojmů pro tuto práci.

Možnosti pro zajištění bezpečnost podniku

Možnostmi zajištění podnikové bezpečnosti se rozumí proč a jestli vůbec se podnik může podnik proti hrozbám bránit.

Formy pro zajištění bezpečnost podniku

Forma udává jakým způsobem je bezpečnost podniku zajištěna. Mezi konkrétní formy například patří systém řízení rizik podvodů, interní audity, vytváření datových analýz, proškolování zaměstnanců.

Nástroje pro zajištění bezpečnost podniku

Nástroji se rozumí prostředky, kterými musí podnik disponovat a investovat, aby byla konkrétní forma naplněna.

V dalších kapitolách této práce budou jednotlivé formy a nástroje více vysvětleny v souvislosti s tím, proti konkrétním jakým bezpečnostním hrozbám bezpečnost zajišťují.

---

5 Česká bezpečnostní terminologie Výklad základních pojmů [online]. 2003, 20 [cit. 2023-09-03]. Dostupné z: https://moodle.unob.cz/pluginfile.php/11277/course/section/3043/%C4%8Cesk%C3%A1%20bezpe%C4%8Dnostn%C3%AD%20terminologie.pdf

1. Možnosti zajištění podnikové bezpečnosti

Jak lze vymezit podnikovou bezpečnost v kontextu zajištění bezpečnosti státu nebo bezpečnosti jednotlivce?

Bezpečnost státu je zajišťována prostřednictvím státních institucí jako jsou Ministerstva a jejich úřady, Bezpečnostní informační služba (BIS) a další. Tyto instituce mají za úkol monitorovat a ochraňovat národní bezpečnost a zajišťovat ochranu proti různým hrozbám, včetně kybernetických útoků, terorismu a dalších hrozeb.

Podniky mají v možnosti zajištění své bezpečnosti větší míru autonomie. Je zodpovědností managementu každého podniku, zda a kolik zdrojů investuje do zabezpečení.

Bezpečnost jednotlivce je kombinací úsilí státu a jednotlivce. Stát má své zákony, státní policii, obecní policii a jiné bezpečnostní, které mají za úkol udržovat veřejný pořádek a chránit občany před nebezpečím. Nicméně každý jednotlivec také nese zodpovědnost za svou vlastní bezpečnost a měl by dbát na to, aby se nestal snadným cílem pro různé formy kriminality.

Je důležité zdůraznit, že bezpečnost podniku není institucionálně zajištěna jako u stát, či jednotlivce a každý podnik si bezpečnost musí řídit sám.

Podniková bezpečnost je ovlivněna následujícími aspekty:

- Legislativní opatření
- Organizační opatření
- Technická opatření
- Lidský faktor

Do legislativního opatření podnik zasahovat nemůže. Stejně tak nemůže ovlivnit lidský faktor. Podnik má tedy možnost zajistit bezpečnost pomocí zavádění organizačních a technických opatření.[6]

[6] JINDŘICH, Nový. Manažerská ekonomie [online]. Praha, 2023 [cit. 2023-09-03]. Studijní materiály. PAČR.

V rámci organizačních technických opatření je potřeba zahrnout základní principy, kterými jsou prevence, vyhledávání klíčových míst a kontrola.

V rámci prevence by podniky měly aktivně sledovat aktuální bezpečnostní hrozby a reagovat, pokud jsou pro ně relevantní. Prevence také zahrnuje vypracovaný a aktualizovaný systém bezpečnostní politiky, nebo zavedení oddělení investigativních služeb a řešení sporů.

Vyhledání klíčových míst spočívá ve zdůraznění důležitých a kritických míst, činností, nebo pracovních pozic, které by mohly být cílem útoků. Identifikace klíčových míst umožňuje zaměřit zabezpečení na tyto oblasti a zajistit, že jsou řádně chráněny a monitorovány.

Princip kontroly zahrnuje pravidelné monitorování a auditování různých podnikových procesů. Interní kontroly a audity pomáhají identifikovat nedostatky, zranitelnosti a případné neobvyklé události. Tímto způsobem lze rychle reagovat na potenciální problémy a minimalizovat rizika.

Odpovědnost za řízení bezpečnosti

Řízení bezpečnosti je soustavná, opakující se sada navzájem provázaných činností, jejichž cílem je zajistit bezpečný provoz a zamezit bezpečnostním rizikům a hrozbám, jako jsou ohrožení či poškození života a zdraví, hmotných a nehmotných aktiv organizace**.**

Zodpovědnost za bezpečnost spočívá především na vlastníkovi podniku, statutárním orgánu a nejvyšším managementu dané organizace. V případě rozsáhlých institucí se vyčleňuje role manažera bezpečnosti (CSO – Chief Security Officer), který zajišťuje celkovou bezpečnostní strategii. Ve větších podnicích se navíc zavádí pozice manažera informační bezpečnosti (CISO), který se soustředí na zabezpečení informací a bezpečnost ICT (informační a komunikační technologie). U větších subjektů se rovněž objevují specializovaní experti na konkrétní oblasti kybernetické bezpečnosti.[7]

[7] JINDŘICH, Nový. Manažerská ekonomie [online]. Praha, 2023 [cit. 2023-09-03]. Studijní materiály. PAČR.

Manažer bezpečnosti

Úkoly manažera bezpečnost spočívají v plánování, organizování, a rozhodování o procesech, které se týkají řízení bezpečnosti. Provádí analýzy bezpečnosti a stanovuje strategie, přičemž může delegovat část svých pravomocí a odpovědností na další manažery nižších úrovní z jiných oddělení. Dále jeho role zahrnuje vedení a kontrolování svých podřízených zaměstnanců.

2. Současná situace

Tato kapitola je věnována analýze rizik, se kterými se podniky nejčastěji setkávají v současné době. Jak už bylo zmíněno, bezpečnost podniku je široký pojem zahrnují spoustu oblastí. Následující průzkum však odhaluje, které hrozby jsou v současnosti pro podniky nejzávažnějšími.

2.1. Celosvětová situace

PwC je mezinárodní společnost, která se zaměřuje na poradenskou a auditorskou činnost. Mimo jiné zpracovává každoročně zprávu stavu bezpečnosti a současných hrozeb napříč podniky z celého světa.

Do průzkumu bylo zapojeno přes 1200 dotázaných podniků z více jak 53 zemí věta, přitom většina s ročním obratem nad 2 miliardy.

Průzkum uvádí porovnání napříč lety, které prokazuje, že navzdory současné geopolitické nestabilitě a s tím i pramenící nejistá ekonomická situace, má výskyt podvodů vůči podnikům mírně klesající tendenci.

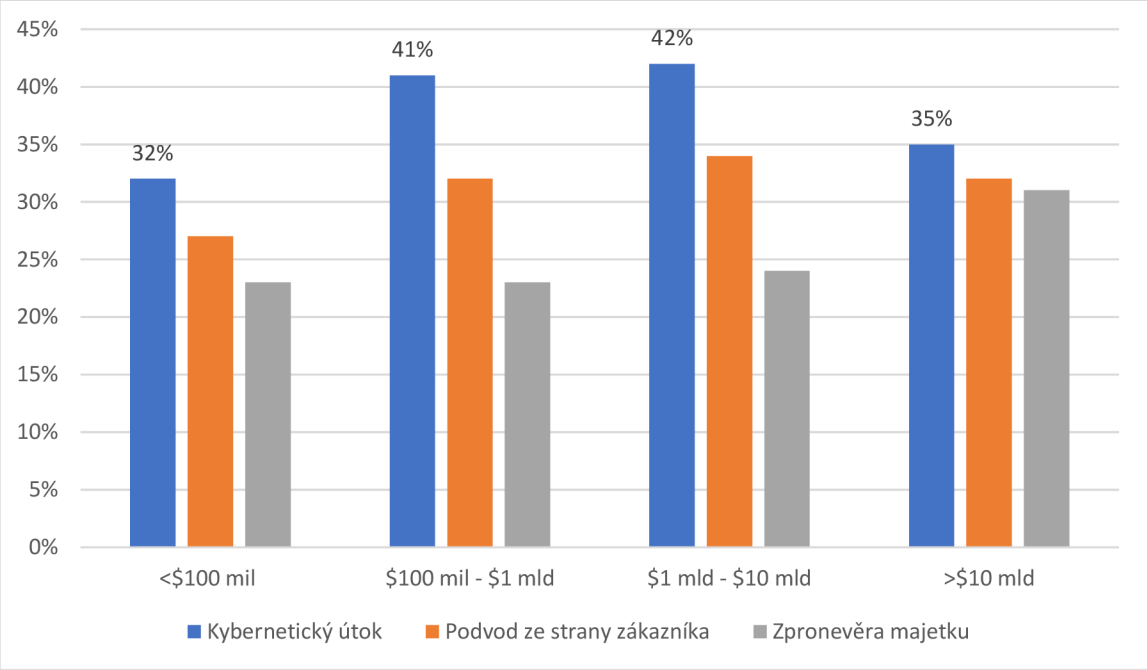
Z analýzy vyplývá, že zatímco v roce 2018 se podvodem potkalo 49% podniků, v roce 2022 je uvedeno 47% podniků a během roku 2022 se počet lehce snížil na 46%.

Tento lehce optimistický trend není dodržen u podniků v oblasti energetiky, médií a telekomunikačních společností. Jak bude v této práci ukázáno, na vzestupu jsou stále kybernetické hrozby, které právě tato odvětví nevíce postihují.

Analýza dále ukazuje na rozdíly výskytů podvodů u velkých a malých podniků. Konkrétně 52% větších podniků, které uvádí roční příjem nad 200 miliard ročně, se během roku 2022 potkalo s podvodem. U menších podniků, jejichž roční obrat činí pod 2 miliardy, je procento případů nižší jen 38%.

Pro tuto práci nejdůležitější analýza přináší porovnaní podvodů vzhledem k typu provedení.

Následující graf z roku 2022 ukazuje, že napříč všemi podniky, co do velikosti z hlediska ročního obratu, dominují tři typy podvodů – kybernetické útoky, podvod ze strany zákazníka a zpronevěra majetku.[8]



Graf č.1: Srovnaní četnosti třech nejčastějších typů podvodů v závislosti na velikosti podniku (podle ročního obratu)

Vývoj během pandemie COVID-19

Jedním z dopadů celosvětové pandemie bylo přenesení velké části dění do digitálního světa, což vedlo k zvýšení rizika kybernetických útoků. Naopak pokles byl zaznamenám u zpronevěry podnikového majetku, protože k němu měli zaměstnanci během této doby omezenější přístup. Vedle kybernetických útoků podniky zaznamenaly i zvýšení případů vydírání, nebo zvýšení šíření podvodů plynoucích z desinformací.[9]

[8] *PwC's Global Economics Crime and Fraud Survey 2022* [online]. 2022, 3-6 [cit. 2023-09-05]. Dostupné z: https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

[9] *PwC's Global Economics Crime and Fraud Survey 2022* [online]. 2022, 7 [cit. 2023-09-05]. Dostupné z: https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

Vnější a vnitřní pachatelé

Další statistiky byly zpracovány z pohledu, zda byl podvod spáchán pachatelem, který v podniku nepracuje, nebo zda byl proveden zaměstnancem podniku. Pachatele z vně podniku tvořili 43%, zatímco 31% podvodů bylo spácháno vlastními zaměstnanci, zbylých 26% podvodů bylo provedeno ve spolupráci zaměstnance a externího pachatele.[10]

2.2. Situace v České republice

V roce 2018 vydala společnost PwC zatím nejaktuálnější takto komplexní analýzu podvodů, kterým musí české podniky čelit.

Průzkum uvádí, že během roku 2018 se s podvodem setkala třetina českých podniků. V porovnání se zbytkem světa, se jedná o nízké číslo, protože v rámci střední a východní Evropy je číslo 47% a celosvětově dokonce 49%.

Dalším zajímavým ukazatelem je, téměř každý druhý český podnik přišel v důsledku podvodného jednání o více než 100 000 Kč. Každá čtvrtý pak za následné vyšetřování podvodu utratil více než dvojnásobek sumy, o kterou kvůli podvodu přišel.

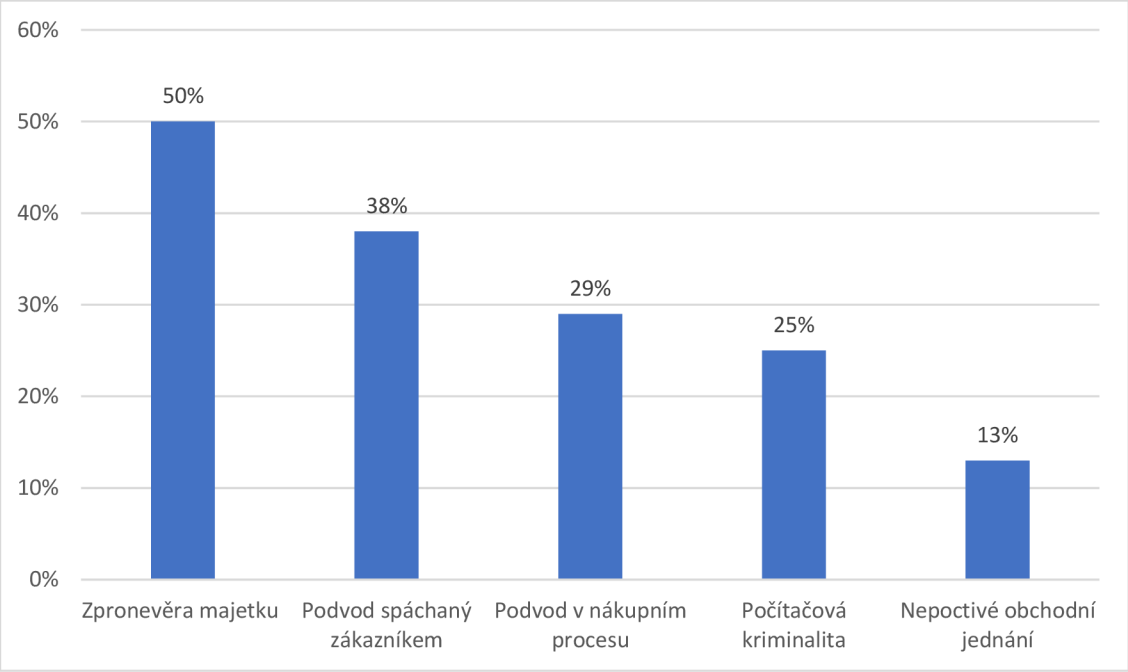
Druhy nejčastějších podvodů přibližně kopírují celosvětový trend. Mezi nejčetnější podvody opět patří zpronevěra majetku, podvody spáchány zákazníky a kybernetická kriminalita. Oproti světovým průzkumům významný podíl plní také podvody v nákupním procesu a praní špinavých peněz s nepoctivým obchodním jednání.

V oblasti kybernetické kriminality, 41 % respondentů uvedlo phishing jako nejčastější techniku použitou ke kybernetickému útoku. Phishing je těsně následován útoky malwarem, které jako nejčastější označilo 37 % respondentů.

---

[10] *PwC's Global Economics Crime and Fraud Survey 2022 [online]. 2022, 8-9 [cit. 2023-09-05]. Dostupné z: https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf*

Průzkum také uvádí, jestli se českým podnikům vyplácí vynaložit finance do vyšetření uskutečněného podvodu. Přibližně 63% podniků utratilo za vyšetřování minimálně stejnou částku, o kterou kvůli danému podvodu přišla a vyšetřování se vyplatilo pouze 33% podnikům.



Graf č.2: Nejčastější typy podvodů registrovaných u českých podniků

Analýza ukázala, že přesně v polovině případů podvodů byla zaznamenána zpronevěra podnikového majetku, ve 38% byl podvod spáchán zákazníkem, ve 29% šlo o podvod v nákupním procesu, 25% případů představuje počítačová kriminalita a 13% praní špinavých peněz a nepoctivé obchodní jednání, jako je například korupce.

Pro shrnutí podniky čelí široké škále podvodů, které ohrožují jejich ekonomické zájmy. Tato práce je dále zaměřena jen na dvě kategorie podvodů, které, jak potvrzují zmíněné průzkumy, patří k nejčastějším.

Následující kapitola je věnována podvodům, které páchají samotní zaměstnanci, kam spadají zpronevěry, krádeže, nebo účetní podvody. Další kapitola se pak zaměřuje detailněji na kybernetickou kriminalitu.[11]

[11] *Global Economic Crime and Fraud Survey 2018 Czech Republic. Global Economic Crime and Fraud Survey 2018 [online]. 2018, 1-32 [cit. 2023-09-03]. Dostupné z: https://www.pwc.com/cz/en/hospodarska-kriminalita/assets/pdf/gecs-survey-report-pro-cr-2018.pdf*

3. Podvody ze strany zaměstnance

Jak plyne ze závěrů analýz zmíněných v minulé kapitole, podvodné jednání ze strany zaměstnance, patří k vůbec k nejčastější hrozbě, se kterou musí podniky počítat.

Podvodné jednání může mít pro podnik vážné dopady, nejedná se jen o materiální škody v podobě ztráty financí a podnikového majetku, ale podnik může utrpět i nemateriální újmu. Následky podvodu můžou znamenat špatné jméno a pověst podniku, poškození obchodní vztahů a ztrátu důvěry ze strany zákazníků, partnerů a investorů, čímž je do budoucna ohroženo postavení podniku na trhu.

V této kapitole je podvod chápán v širším slova smyslu. Podvodem se rozumí jakékoliv škodlivé jednání ze strany zaměstnance vůči podniku, kde pracuje. V další kapitole jsou představeny jednotlivé druhy podvodných jednání jako je krádež, zpronevěra, fraud (podvod v užším významu) a korupce.

3.1. Druhy podvodného jednání ze strany zaměstnance

Způsobů, jakými se může zaměstnanec dopustit podvodného jednání, je široká škála. Je důležité zmínit, že podniky jsou okrádány i podvodným jednáním, které není klasifikováno jako trestný čin. Platí, že i mnoho podvodů menšího rozsahu, může způsobit podniku velké ztráty.

Samozřejmě ne všechna podvodná jednání jsou přímo trestnými činy, protože nesplňují míru škodlivosti. Například u krádeže do 10 000 Kč, se nejedná o trestný čin, ale přestupek. Nicméně pokud by míra škodlivosti splněna byla, podvody by byly klasifikovány jako trestný čin spadající pod majetková trestnou činnost.

V této kapitole, je pozornost zaměřena na škodlivé činy, které ohrožují podniky v největší míře. Jedná se o činy směřují proti podnikovému vlastnictví (např. krádež, zpronevěra) a podnikovému majetku (např. podvod).

Vedle majetkové trestné činnosti je v této kapitole také více vysvětlena korupce, jež nemá v trestním zákoníku svoje konkrétní místo, ale většinou spadá pod trestné činy proti pořádku ve věcech veřejných.

a) Krádež

Krádeže se dopustí ten, kdo si neoprávněné přisvojení cizí věc či hodnotu. Od zpronevěry se liší především tím, že odcizená věc nebyla pachateli předtím svěřena.

V rámci podniku jsou zaměstnancům svěřovány různé formy podnikového majetku, ať už se jedná o manažery, kteří spravují podnikové úspory, nebo o řadové zaměstnance, kteří využívají služební vozidla, kopírky a další podniková vybavení.

Z tohoto důvodu není krádež mezi častými formami podvodných jednání a v rámci podniku a jde spíše zpronevěru.

b) Zpronevěra

Podle trestního zákoníku České republiky je zpronevěra trestný čin, kterého se pachatel (defraudant) dopustí, pokud si přisvojí věc, která mu byla svěřena, a způsobí tak na cizím majetku škodu nikoli nepatrnou.[12]

Od ostatní majetkové trestních činnosti se liší především tím, že daná věc byla pachateli majitelem výslovně svěřena.

Konkrétně od podvodu se liší, že pachatel získá z zpronevěry faktickou moc nad věcí bez vyvolání, či využití cizího omylu.[13]

Příznivé podnikové prostředí pro zpronevěru je takové, kde neexistuje propracovaný vnitřní kontrolní systém, nebo pokud chybí korektní etická kultura podniku. Špatnou etickou kulturou se rozumí, že zaměstnanci nemají k podniku bližší vztah, nejsou seznámení s interním etickým kodexem, nebo mají dojem, že ostatní zaměstnanci se dopouští do jisté míry zpronevěry taky.

---

[12] *Zákon č. 40/2009 Sb. Zákon trestní zákoník* [online]. 2009 [cit. 2023-09-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40#p206

Zpronevěra může nabývat různých podob a rozsahů.

Falšování zpráv o výdajích: To zahrnuje například předkládání falešných účtů za služební cesty, nebo účelové nákupy levných vstupenek či jízdenek, které jsou následně uplatněny jako drahé.

Zpronevěra malého rozsahu: Sem spadá zpronevěra drobných předmětů, kopií či tisku soukromých materiálů. Zpronevěry menšího rozsahu jsou většinou těžko zaznamenatelné, ale jejich akumulace může zapříčinit pro podnik velké ztráty.

Zpronevěra velkého rozsahu: Pachatelem je zaměstnanec zpravidla na vyšší pozici, který zpronevěří podnikové peníze tím, že místo k účelu, ke kterému mu byly peníze svěřeny, je použije na soukromé investice, nebo osobní spotřebu. Zaměstnanec může také zpronevěřit cenný majetek, jako jsou drahá zařízení, technologie nebo samotné produkty, a následně tento majetek prodat nebo využít pro osobní prospěch.

V následující kapitole bude více rozebrán popis typického pachatele dopouštějícího se zpronevěry. Pro úvod, mezi nejčastější pachatele patří zaměstnanci na vyšších pozicích (bílé límečky), protože právě ti mají největší zodpovědnost a přístup k podnikovému majetku.

Ve všech podnicích musí být podnikový majetek a další finanční prostředky svěřeny do rukou zaměstnanců, aby s ním nakládali na vlastní zodpovědnost a jak je vyžadováno v souvislosti s jejich pracovní pozicí. To je důvod, proč riziku zpronevěry budou podniky čelit neustále, ale existuje několik nástrojů a postupů, jak rizika zpronevěry účelně eliminovat.

Podniky by měly mít vytvořený jasný interní etický kodex a také následné mechanismy pro kontrolu finančních toků a nakládání s podnikovým majetkem.

Kromě samotné existence etického kodexu, je důležitá i následná komunikace, případně školení zaměstnanců, aby měli o důležitosti etických hodnot povědomí. Obecně se dá říct, že pro prevenci proti zpronevěře je důležité vytvořit integrované prostředí založeného na transparentnosti a etických hodnotách podniku.

Pokud přece jen k zpronevěře dojde, musí ji podnik odhalit pomocí jednoho z kontrolních mechanismů. Těmi jsou vnitřní audity a forenzní audity.

c) Podvody (Fraudy)

Definice podvodu z trestního zákoníku zní: „Trestný čin, jehož se dopustí ten, kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou."

V případě podnikových podvodů je ten, kdo je uveden v omyl, podnik. Škoda nikoli nepatrná vznikla právě na podnikovém majetku. Důležitý je zde podmínka vyvolání nebo využití omylu, tím se liší od ostatní majetkové trestné činnosti.

Mohlo by se zdát, že podvodů se dopouštějí zákazníci, dodavatelé, nebo konkurenční podniky, tedy pachatelé pocházejí z vně podniku. Nicméně, jak už bylo ukázáno v analýzách z předchozí kapitoly, skutečností je, že pokusy o podvod nevznikají vždy pouze ze strany vnějších pachatelů, ale s velikostí podniku roste i četnost podvodů ze strany vlastních zaměstnanců.

Fakturační podvody

Zaměstnanec vytvoří falešnou fakturu za služby či zboží, které ve skutečnosti nebyly poskytnuty. Tímto způsobem se snaží získat platbu od podniku za něco, co vlastně neexistuje nebo nebylo provedeno. Falešnou fakturu může následně zpracovat v podniku tak, aby se zdálo, že jde o legitimní transakci.

Účetní podvody

Účetní podvody spočívající ve zmanipulování, zfalšování nebo pozměnění účetní evidence nebo příslušných podkladů, podle nichž se zpracovává účetní závěrka.

Zaměstnanec může v účetní uzávěrce nesprávně uvést události, transakce nebo jiné závažné informace. Dále může nerespektovat účetní principy vztahujících se k částce nebo klasifikaci.[14]

---

[14] WIEDOVÁ, Zuzana. *PROBLEMATIKA ZKRESLOVÁNÍ ÚČETNÍCH INFORMACÍ A MANIPULACE S ÚČETNÍMI VÝKAZY*. Praha, 2012. Diplomová práce. Univerzita Karlova.

d) Korupce

Podle PwC analýzy je 13% ze všech podvodů právě korupční jednání. Stejně jako ostatní podvody je korupce motivována snahou po materiálním zisku nebo získání jiných výhod. Korupci lze definovat jako projevem zneužití postavení nebo pravomocí v rozhodovacím a řídícím procesu k osobnímu prospěchu, přičemž je porušen princip nestrannosti. Projevuje se protěžováním, podplácením, vydíráním, zastrašováním, nebo podvody při využívání dotací.

Samotný termín korupce není v trestním zákoníku použit, ale namísto toho je část korupčního jednání zahrnuta v termínu „úplatkářství“, jenž spadá pod „Trestné činy proti pořádku ve věcech veřejných“. Do úplatkářství jsou zahrnuty tyto trestné činy:

- Přijetí úplatku,
- Podplácení,
- Nepřímé úplatkářství,

Kromě úplatkářství je v právním řádu zakotveno několik dalších skutkových podstat trestných činů, které zahrnují korupční chování. Jedná se o následující trestné činy:

- Neoprávněné nakládání s osobními údaji
- Zneužití informace a postavení v obchodním styku,
- Sjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě,
- Pletichy při zadání veřejné zakázky a při veřejné soutěži,
- Pletichy při veřejné dražbě.[15]

V roce 2018 vypracovala poradenská společnost EY průzkum zaměřen na problematiku vnímaní korupce. V projektu byli osloveni vrcholní manažeři, obchodní ředitelé, nebo vedoucí interních auditů z více než 50 zemích celého světa.

---

[15] Co je korupce. *Policie.cz* [online]. 2023 [cit. 2023-09-04]. Dostupné z: https://www.policie.cz/clanek/co-je-korupce.aspx

Výsledkem průzkumu bylo mimo jiné odhalení, že korupce je do velké míry běžná součást české podnikové kultury.

Benevolentní vnímaní korupce přispívá k faktu, že šest z deseti dotázaných českých manažerů je ochotno při boji o zakázky podvádět. Přestože dotazovaní připouští, že jsou si vědomi, že se jedná o neetický postup pro získání zakázky, mezi často používané praktiky při získávání zakázek uvádí úplatky, nabízení jiných hodnotných darů nebo poskytnutí zábavy obchodním partnerům či zákazníkům.

Ve shrnutí, Česká republika patří dlouhodobě mezi státy s největším procentem rizika korupce v Evropě. Přibližně 36% českých respondentů shledává korupci jako velkou hrozbu pro jejich podnik. Pro porovnání a nastínění rozdílů mezi ostatními regiony, ve státech západní Evropy, považuje korupci za riziko 20% manažerů, na území střední a východní Evropy se jedná 47% manažerů, v zemích latinské Ameriky je to dokonce 74% dotazovaných.

Na druhou stranu, pouze 6% českých podniků uvádí, že se během dvou let stalo obětí závažného podvodu ve spojení s korupčním jednáním.

Mohlo by se zdát, že jde o dobré výsledky, nicméně Radim Bureš, manažer oddělení investigativních služeb a řešení sporů společnosti EY se zaměřením na veřejný sektor, byl ve svém vyjádření zdrženlivější: *„Nízký počet odhalených podvodů v českých a slovenských firmách není důkazem vyšší integrity. Naopak ukazuje, že naše firmy stále neumí podvody správně detekovat. Relativně malé náklady na zavedení preventivních a detekčních mechanismů mohou později firmám ušetřit velké prostředky.“* [16]

[16] *Jak jsou na tom čeští manažeři v tolerování korupčních praktik?* [online]. 2018 [cit. 2023-09-03]. Dostupné z: https://roklen24.cz/?quick_news=jak-jsou-na-tom-cesti-manazeri-v-tolerovani-korupcnich-praktik

3.2. Analýza typického pachatele

3.2.1. Hlavní faktory vedoucí k podvodnému jednání

Podvody jsou páchány z různých důvodů, nicméně odborné studie se shodují a následně i z průzkumů vyplývá, že pro podvod existují tři hlavní faktory.

Souhrnně pro faktory existuje i odborný název “fraud triangle“ a zahrnuje příležitost spáchat podvod, tlak na spáchání podvodu a schopnost zdůvodnit si (racionalizace) spáchání podvodu.

Podle PwC analýzy 59% respondentů, uvedlo že hlavní faktorem k uskutečnění podvodu je pocítění příležitosti. Podle dalších 21% dotázaných je hlavním důvodem tlak na spáchání podvodu, 11% dotázaných si myslí že pro pachatele je nejdůležitější, aby si podvod dokázali racionálně odůvodnit.

Zaměstnanci se mohou pod tlakem ocitnout z důvodu finančních potřeb spojených se stresovými situacemi. Tento tlak může vyvolat různé reakce, včetně závislostí (alkohol, drogy, hazard), životního stylu mimo možnosti jednotlivce, touhy po rychlém obohacení či vysokého osobního zadlužení. Tyto faktory mohou přivést k neetickému chování včetně nečestného přístupu na pracovišti.

Samotný tlak však často nestačí k tomu, aby zaměstnanec začal s podvodem, pokud nemá konkrétní příležitost. Důležitý faktor představuje pocítění naskytnuté příležitostí, zaměstnanci se často rozhodují k podvodu v domnění, že jejich činnost nevyjde najevo. Mezi typické příležitosti pro páchání podvodu patří nedůsledné kontrolování managementu, například dozorčí radou, dále pokud je organizační struktura v podniku složitá, nestabilní a celkově pokud nedostatečně funguje vnitřní kontrolní systém.

Racionalizace neetického chování může zahrnovat myšlenky, že takové jednání nikomu neublíží, jako například neškodná krádež, kdy má podnik dostatek prostředků. Tento postoj může také vyvstat z pocitu, že zaměstnancův plat není v souladu s jeho schopnostmi, nebo si podvod může zdůvodňovat tím, že v podniku podvádí každý druhý.

Pro zajištění podniku proti podvodům ze strany zaměstnance je stěžejní co nejvíce eliminovat všechny tři faktory, nicméně největší vliv má vedení podniku právě na snížení příležitosti spáchání podvodu.

3.2.2. Profil typického pachatele

Následující studie se zaměřují na pachatele z oblasti interního podvodu, tedy kdy se podnik pokusili okrást vlastní zaměstnanci.

Přestože je podoba podvodů velice rozmanitá, lze sestavit typický profil takového pachatele.

V minulé podkapitole bylo zmíněno, že pachatel musí být pod tlakem, umět podvod racionalizovat a cítit příležitost podvod provést. K těmto třem aspektům se přidává ještě jeden faktor, a to že pachatel musí mít schopnosti podvádět, ať už to zahrnuje jeho zkušenosti v podniku, pracovní pozici nebo celkově jeho povahu.

Následující analýza vychází ze studie mezinárodní poradenské společnosti KPMG z roku 2016. Studie byla zpracována na základě skutečných případů podvodů během let 2013 až 2015. Do průzkumu bylo zahrnuto 750 podvodných případů z 81 zemí světa, kde zaměstnanci okradli vlastní podnik. Kromě základních charakteristik byla zkoumána povaha pachatele, jeho motivace k provedení podvodu a jeho vazby na podnik, kde podvod uskutečnil. Studie byla vypracována podle dostupných statistických dat a výsleších pachatelů.[17]

Profil typického pachatele:

- převažují muži (79 %)
- ve věku 36 až 55 let (69 %)
- na pozici manažera nebo ředitele (35%)
- v podniku dlouhodobě zaměstnaný - více jak 6 let (38%)

[17] *Global profiles of the fraudster: Technology enables and weak controls fuel the fraud* [online]. 2016, [cit. 2023-09-03]. Dostupné z: https://www.vyrostli-jsme.cz/profil-typickeho-podvodnika

- tajně spolupracuje s dalšími stranami (60%)
- okolím nahlížen jako respektovaný a přátelský
- nejčastěji motivován osobních prospěchem (60%), nenasytností (36%), pocitem „protože mohu" (27%)

Detailnější studie zaměřená na pachatele v České republice ukazuje, že profil českého pachatele se odráží v profilu globálním jen s drobnými rozdíly. Jedná se o průměrově starší muže, kteří v podniku působí kratší dobu než jak je tomu ve celosvětovém měřítku.

Profil typického pachatele v České republice:

- muž (85%)
- ve věku mezi 46 až 55 lety (48%)
- ve podniku působí více jak 3 roky
- pracovníci na vrcholných pozicích v oblasti financí, prodeje, nebo provozu
- tajně spolupracuje s dodavateli nebo zákazníky
- nejčastěji se dopouští zpronevěry majetku, podvodu spojeným s manipulací s účetních výkazů (83%)

Ze statistik vyplývá, že se jedná nejčastěji o dlouhodobě pracující zaměstnance a zaměstnance na vysokých pozicích. Oba typy pracovníků spojuje dobrá znalost fungování oddělení. Vedoucí pracovníci mají přístup k citlivým informacím podniku a informacím, které mohou zneužít k obejití vnitřních kontrol. Mají vliv na chod svého oddělení, což mohou využít k zamaskování vlastního podvodu.

Zaměstnanec, který v podniku pracuje dlouhodobě, zná dobře procesy a fungování svého oddělení. Ví, jaká panuje v podniku atmosféra, co si může dovolit a kde je potenciální slabé místo z hlediska kontroly.

S vedoucí pracovní pozicí souvisí věk a pohlaví pachatele. V České republice, ale i celosvětově, se na vedoucí pozice zpravidla obsazují muži s letitými pracovními zkušenostmi. Tento faktor výrazně přispívá k tomu, že větší procento mezi pachateli zaujímají muži.

Z průzkumu dále vyplývá, že pachatelem je nejčastěji zaměstnanec, který působí na ostatní věrohodným dojmem. Pachatel pracuje často přesčasy, nebere si moc dovolené, působí svědomitě. Pro podniky je těžké takového zaměstnance z něčeho podezřívat a k většině odhalení dojde náhodou, nebo na základě neobvyklé události.

Dalším z ukazatelů může být nepřiměřený životní styl pachatele vzhledem k jeho platu a pozici. Tento ukazatel se týká spíš méně opatrných pachatelů, kteří na sebe upozorňují drahými auty nebo exotickými dovolenými. Je na každém podniku, jak tyto signály vyhodnotí. I v tomto případě je potřeba najít rovnováhu mezi kontrolou svých zaměstnanců a nevstupováním do jejich soukromých záležitostí.[18]

Využití znalosti typického pachatele

Znalost profilu typického pachatele pomáhá při odhalování podvodů, ale důležitější roli má už i při prevenci před podvody. Znalost profilu pachatele pomůže podniku při rozhodování, pro které pozice je potřeba zavést bezpečnostní prověrku, kde je potřeba více zaměřit vnitřní kontroly a pravidelné audity. V rámci forenzního auditu může být profil taktéž nápomocný při vytipování okruhu pachatele.

3.3. Formy zajištění bezpečnosti proti podvodům

Některé nástroje a postupy pro účinný boj proti podnikovým podvodům byly zahrnuty v předchozí kapitole s vymezením podvodných jednání.

V souvislosti se zpronevěrou bylo zmíněno vypracování etického kodexu, školení zaměstnanců a kontrolní mechanismy, jako jsou interní a forenzní audity. Za jeden z účinných nástrojů při boji s korupcí se považuje sankciování, nebo prověřování rizik vyplývajících ze smluvních vztahů s třetími stranami.

Podniky mají celou řadu možností a nástrojů, jak podvodným jednáním zabránit. Způsoby odhalení podvodů lze rozdělit do tří kategorií, podle toho, jestli k odhalení

[18] *Profil typického podvodníka* [online]. 2016 [cit. 2023-09-04]. Dostupné z: https://www.vyrostlijsme.cz/profil-typickeho-podvodnika.

došlo uvnitř podniku v rámci kontrolních systémů, nebo jestli odhalení vyplynulo ze správně nastavené podnikové kultury. Poslední kategorií jsou způsoby odhalení podniku mimo oblast vlivu vedení společnosti, které sice podnik nemůže přímo ovlivnit, nicméně k odhalení podvodu napomáhají.

Firemní kontrolní systémy

- interní audit
- systém řízení rizik
- datová analýza
- podniková bezpečnost
- rotace zaměstnanců
- rozdělení kompetencí

Podniková kultura

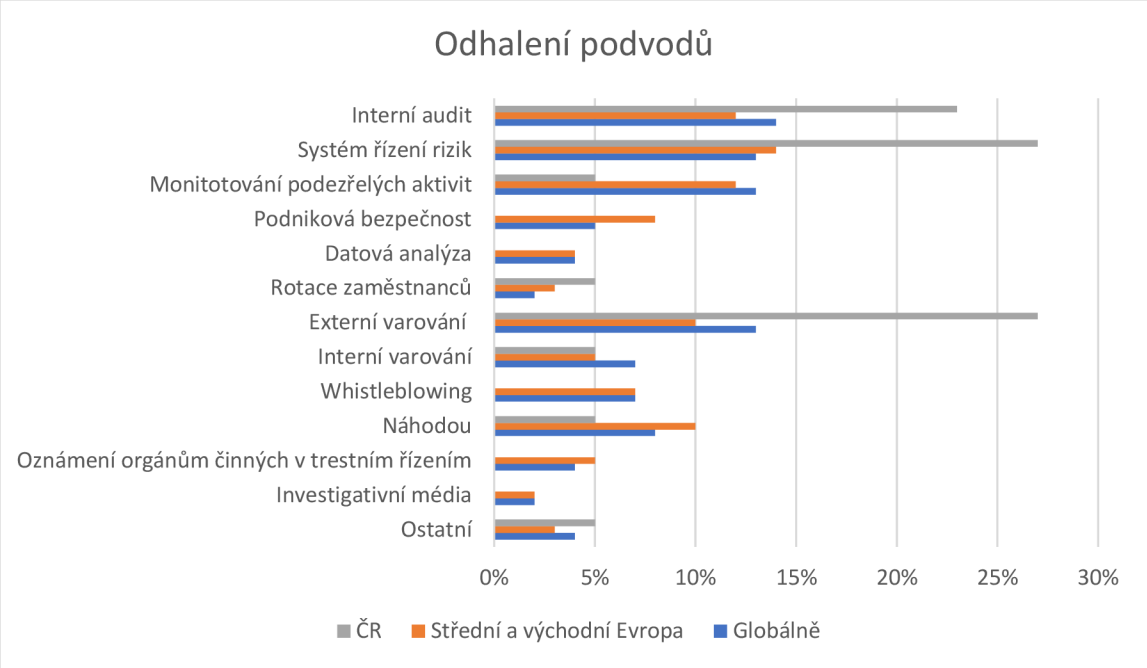
- interní varování
- externí varování
- anonymní informační linka

Mimo oblast vlivu vedení společnosti

- náhodou
- oznámením orgánů činných v trestním řízením
- investigativní média

Na následujícím grafu je znázorněno, co nejčastěji napomáhá k odhalení podvodu. Trend v České republice přibližně odpovídá trendu celosvětovému, nicméně jsou zde vidět určité rozdíly. Například ve světě už využívaný whistleblowing, je v Česku stále nepopulární.

Podobně jako ve světě, se v Česku nejvíce podvodů odhalilo díky upozornění zaměstnancem podniku na jisté podezřelé události. Dalším klíčovým nástrojem pro odhalení podvodů se ukazuje řízení rizika podvodů a interní audity.



Graf č.3: Způsoby odhalení podvodů, globální srovnání se situací v ČR a ve střední a východní Evropě

a) Systém řízení rizik podvodu

Systém řízení rizik podvodu je nedílným mechanismem, který pomáhá eliminovat podvody v podniku.

Řízení rizika podvodu zahrnuje systematický proces identifikace, porozumění a zpracování rizik spojených s podvody v organizaci. Zahrnuje vytváření strategií pro detekci, prevenci a omezení jak interních, tak externích podvodů v rámci organizace.

Efektivní řízení rizika podvodu slouží k minimalizaci pravděpodobnosti všech druhů podvodů, včetně krádeží, korupce, zpronevěry, praní špinavých peněz, úplatkářství, vydírání a dalších forem podvodných aktivit. Také pomáhá odhalit bezpečnostní slabá místa, skrz která by mohl být podnik nejvíce ohrožen.

Systém řízení rizik stojí na následujících principech:

Vedení rizika podvodu

Vedení rizika podvodu zahrnuje vytvoření rámce pravidel, postupů a procesů pro řízení rizik spojených s podvody ve firmě a také průběžně monitorovat rizika podvodu a přizpůsobovat strategie dle potřeby.

Posouzení rizika podvodu

Posouzením rizika podvodu se rozumí identifikace nejzávažnějších rizik spojených s podvody v daném podniku a lokalizace zranitelných míst a klíčových pracovních pozic.

Prevence podvodů

Snaha je o minimalizaci třech hlavním motivů ke spáchání podvodu – tlak, racionalizace a pocit příležitosti. Snížením těchto tří prvků se snižuje i riziko podvodných činností.

Mechanismy detekce rizik

Implementace automatizovaných mechanismů pro hlášení, které monitorují podezřelé chování, jako jsou hlášení výjimek a analýza dat.

Monitorování a hlášení rizik

Vytvoření prostředí, kde se zaměstnanci nebojí podvody nahlásit. Poskytnutí vzdělávání o podnikové kultuře, anonymní horké linky a podpory kultury transparentnosti a otevřenosti.[19]

b) Dělba kompetencí

Je klíčové, aby podniky rozdělovaly různé úkoly a povinnosti mezi více zaměstnanců či oddělení. Tímto krokem výrazně snižují možnost vzniku koncentrované zpronevěry, kde by jediná osoba mohla zneužít své postavení k neoprávněnému získávání prostředků.

Rozdělením povinností vytvářejí tzv. vrstvu kontroly, kde každý krok procesu je svěřen jiné osobě nebo týmu. To znamená, že žádný jednotlivý zaměstnanec

[19] *5 Fraud Risk Management Principles & Assessment Strategies* [online]. 2022, 1 [cit. 2023-09-03]. Dostupné z: https://datadome.co/threats/fraud-risk-management/

nemá absolutní kontrolu nad všemi fázemi transakce, účetních záznamů nebo jiných důležitých procesů.

Tato strategie ochrany před zpronevěrou přispívá k celkové bezpečnosti finančních toků v organizaci a posiluje důvěru v systém interních kontrol.

c) Datová analýza

Cílem datové analýzy je objevení podezřelých aktivit, anomálií, které se naskytnou napříč celým podnikem, a to na základě zpracování většího množství dat získaného během určitého období fungování podniku.

Do nasbíraných dat lze zahrnout sice jen digitální stopy, ale i ty mohou pomocí datové analýzy vést k identifikaci pachatele, nebo napomoct při prevenci proti dalšímu protiprávnímu jednání.

Obecně lze uvažovat jakékoliv zpracování dat včetně manuálního vyhodnocování a databázových nástrojů. Nicméně v dnešní době se nabízí využívat výpočetní technologie s propracovanými statistickými modely nebo modely využívající strojové učení. Moderní technologie tak umožňují identifikovat i případy škodlivého jednání, které v minulosti zůstaly neodhalena.

Podle PwC průzkumu se v podnicích, které využívají specializované softwary pro forenzní datovou analýzu, daří dříve odhalovat potenciální škodlivé jednání. Konkrétně je to o 15% více podniků, oproti těm, které datovou analýzu pomocí moderních technologií nezavádí.

Klasický postup při datové analýze zahrnuje přípravu, vlastní analýzu a následnou interpretaci dat.

Příprava zahrnuje sběr relevantních dat, která se nashromáždí během určitého časového úseku fungování podniku. Může se jednat o platební transakce, které jsou navíc samostatně zmíněny v další části této práce, jiných digitálních dat jako jsou záznamy ze serverů, síťových logů, nebo údaje o zaměstnaneckých aktivitách. Vždy je však dodržovat pravidlo o zpracovávání osobních údajů a nezneužívat nasbíraná data pro jiné účely.

Následná analýza dat zahrnuje spuštění statistických a jiných výpočetních modelů na nasbíraných datech. Samotné výsledné hodnoty, které vrátí výpočetní model nestačí. Je potřeba, aby výsledky byly správně vyhodnoceny a odfiltrovány všechny případy, které nejsou pro podnik podvodná jednání, ale model je z nějakého důvodu tak vyhodnotil.

d) Automatické hlášení podezřelých finančních transakcí

Obvykle se využívají dva způsoby, jakými podezřelé transakce detekovat.

Prvním způsobem je, přistupovat k problému, jako ke klasické datové analýze. Nutným předpokladem je velký objem dat, v tomto případě transakcí, které jsou následně analyzovány počítači pomocí výpočetních modelů. Výpočty zachytí nestandartní převody oproti ostatním transakcím a poukážou na potenciální problém.

Druhým způsobem je provést datovou analýzu předem a na základě výsledků nastavit jasná kritéria, které transakce jsou už podezřelé a které naopak ještě odpovídají podnikovým normám.

Tato kritéria se mohou pro každý podnik lišit, ale typická jsou kritéria pro často se opakující menší transakce směřující na jeden účet. Dalším příkladem mohou být definované podezřelé výše převáděných částek, ať už se jedná o vysoké částky, nebo podezřele zaokrouhlené sumy.

Příkladem může být detekce podezřelých finančních transakcí u dodavatelů. Podnik se rozhodne provést datovou analýzu finančních transakcí u svých dodavatelů s cílem odhalit podezřelé aktivity:

Nastavení kritérií: V podniku je zaměstnáno více nákupců od dodavatelů a dřívější analýza ukázala, že platby jsou od každého z nich typicky rovnoměrně rozesílány mezi více dodavatelů.

Analýza dat: Na základě těchto kritérií je každá transakce monitorována a pokud jsou kritéria porušena, je automaticky nahlášeno, že se může jednat o potenciální podvod.

Interpretace: V průběhu analýzy jsou identifikovány transakce, u kterých neodpovídá rozložení platby od jednoho nákupce mezi více dodavatelů. Je potřeba následně vyhodnotit, z jakého důvodu k tomu došlo a zda nedošlo k podvodnému jednání ze strany nákupce .

Opět je potřeba zdůraznit, že ohlášení podezřelých transakcí je pouhým ukazatelem. Následně je nutná kontrola, zda pro tuto událost neexistuje legitimní vysvětlení. Kontrolu zpravidla provádí manažer zodpovědný za dané oddělení, auditor, nebo nezávislá třetí osoba.

e) Whistleblowing

Whistleblowing je označení pro podání upozornění oprávněné instituci nebo orgánu k prověření na nelegální, neetické nebo nezákonné praktiky ve svém podniku. Whistleblowing lze uvažovat v širokém významu pro oznamování jakýchkoliv podvodů včetně zpronevěry, klíčovou roli hraje zejména při odhalování korupce.

Whistleblower je z anglického "ten, kdo hvízdá na píšťalku", neboli veřejně oznámí nezákonné chování, a to i přes možný tlak nebo hrozbu represí ze strany nadřízených nebo kolegů. Role whistleblowera je pro podniky zásadní a měla by být respektována a chráněna.[20]

Některé země mají zákony a předpisy, které chrání whistleblowery před odvetnými opatřeními ze strany zaměstnavatele za jejich oznámení. K těmto státům se řadí od roku 2023 i Česká republika, když v srpnu 2023 nabyl účinnosti zákon o ochraně oznamovatelů a zákon, kterým se mění některé starší zákony v souvislosti s ochranou oznamovatelů. Oba zákony poskytují osobám, jež oznamují protiprávní jednání, účinnou ochranu před odvetnými opatřeními.

Všechny organizace, kterých se týká zákon o ochraně oznamovatelů, by měly o této problematice sepsat interní směrnici. V soukromém sektoru se to týká všech podniků s více jak 50 zaměstnanci. Interní směrnice by měla obsahovat popis

[20] *Whistleblowing* [online]. 2023 [cit. 2023-09-03]. Dostupné z: https://cs.wikipedia.org/wiki/Whistleblowing

procesů podávání oznámení, jeho přijímání, posouzení, řešení a také evidenci oznámení.[21]

Jak už bylo ukázáno výše, v České republice se stále jedná o nepopulární metodu, české podniky případy whistleblowing vůbec nezaznamenávají a oproti světovému nebo i evropskému trendu v tomhle ohledu zaostává.

f) Vnitřní audit

Zatímco předchozí metody představovaly nástroje pro prevenci před podvodnými jednáními. Vnitřní audity a následně uvedený i forenzní audit patří ke kontrolním mechanismům pro odhalení podvodů v podniku.

Vnitřní audity jsou pořádány pravidelně za účelem kontroly veškerých podnikových činností, přičemž auditorem je zaměstnanec podniku, jenž má tuto funkci přiřazenou.

Z důvodu komplexnosti a rozsahu této činnosti je důležité, aby interní auditoři měli vysokou odbornost, kvalifikaci a schopnost analyzovat různorodé aspekty organizace. Role auditorů spočívá v poskytování nezávislého pohledu.

Pravidelnost i na které oblasti se audit zaměřuje, si určuje podnik sám, podle zaměření podniku a oblastí, které jsou vnímány jako kritické.

Interní audit poskytuje vedení organizace informace, hodnocení, analýzy, doporučení a konzultace, které jim pomáhají lépe plnit své úkoly. Tím zajišťuje efektivní zavedení systému řízení rizik a jiných kontrolních mechanismů.[22]

g) Forenzní audit

Forenzní audit je důkladné vyšetřování, které se provádí na základě podezření z podvodného jednání v podniku, čímž se odlišuje od pravidelných interních auditů, které se dělají bez ohledu na podezření.

---

[21] *KORUPCE* [online]. 2023 [cit. 2023-09-03]. Dostupné z: https://korupce.cz/ministerstvo-spravedlnosti-spustilo-medialni-kampan-na-podporu-informovanosti-o-ochrane-oznamovatelu-protipravniho-jednani/

[22] *Interní audit* [online]. 2022 [cit. 2023-09-03]. Dostupné z: https://cs.wikipedia.org/wiki/Intern%C3%AD_audit

Cílem je získat objektivní důkazy o podvodu, nebo jej vyvrátit. Provádí ho nezávislá třetí strana, což znamená někdo z v ně podniku, než kde se podvodné jednání vyšetřuje. Forenzní audit se využívá u všech typů podvodů, jako jsou účetní podvody, korupce a zpronevěra majetku.

Na začátku forenzního auditu se zajišťují důkazní předměty**.** Detailněji se zkoumají finanční a obchodní dokumenty, účetní záznamy, výroční zprávy, ale i vztahy a finanční transakce všech zainteresovaných osob.

Důkazní materiály se podrobí důkladné analýze, a následně se získané výsledky interpretují. Celý průběh a výsledky auditu jsou následně zdokumentovány ve formě znaleckého posudku.[23]

h) Prověrky zaměstnanců

Některé klíčové pracovní pozice, jako jsou manažerské pozice, nebo obchodní ředitelé, mají přístup k velké části podnikových peněz a zároveň jim je svěřena velké pravomoc rozhodovat o podnikovém majetku.

Proto tito zaměstnanci představují pro podnik velké riziko potenciálních podvodů a podnik by vzniklé škody mohly stát nemalé peníze.

Zaměstnance na těchto klíčových pozicích je potřeba cíleně a pravidelně prověřovat. Přičemž rozsah prověřování se odvíjí od důležitosti dané pracovní pozice a závažnosti rizik, která jsou s ní spojená. Prověrky nejsou potřeba jen u stávajících zaměstnanců, ale také u nových uchazečů o klíčovou pracovní pozici.

Mezi základní informace, které jsou prověřovány patří trestní minulost, ověření referencí z předchozích zaměstnání, či posouzení rodinných vazeb. U prověrek pokročilejšího charakteru se prověřuje například finanční situace, volnočasové aktivity, blízký okruh přátel nebo kontakty s jinými zaměstnanci z konkurenčních společností. Všechny tyto prvky jsou klíčové pro zhodnocení spolehlivosti a integritního chování prověřované osoby v pracovním prostředí.

[23] JINDŘICH, Nový. *Manažerská ekonomie* [online]. Praha, 2023 [cit. 2023-09-03]. Studijní materiály. PAČR.

i) Nástroje proti korupčnímu jednání

Účinným nástrojem v boji s korupcí je systematické prověřování rizik vyplývajících ze smluvních vztahů s třetími stranami. Z průzkumů ovšem vyplývá, že tento postup aplikuje pouze 28% českých podniků. Pro srovnání celosvětový průměr se pohybuje kolem 60%.

Dalším způsobem, jak se bránit proti korupci je uvalení účinných sankcí u svých zaměstnanců v případě, že se prokáže jejich porušení podnikových pravidel. Česká republika opět zaostává za celosvětovým průměrem. Zatímco celosvětově 57% firem své zaměstnance sankcionuje, v České republice je to 46% firem.

V rámci kontrolních mechanismů hrají opět důležitou roli audity a forenzní audity.

ISO 37001

ISO 37001 je mezinárodní norma pro systémy protikorupčního managementu. Poskytuje podnikům působícím kdekoli na světě rámec, jak vyhodnotit jejich interní protikorupční procesy a vyřešit případné slabiny. Norma uvádí řadu konkrétních opatření, která pomáhají podnikům při prevenci, odhalování a řešení korupce.

Přestože certifikace ISO 37001 není povinná, díky jejímu získání, je podnik ostatními vnímán jako důvěryhodnější.[24]

[24] *ISO 37001 Systémy protikorupčního managementu* [online]. 2023 [cit. 2023-09-03]. Dostupné z: https://www.tuvsud.com/cs-cz/cinnosti/audity-a-certifikace-systemu/iso-37001-protikorup%C4%8Dn%C3%AD-management

4. Kybernetická bezpečnost

Z analýz ve druhé kapitole vyplývá, že kybernetické útoky představují 25 % všech podvodů spáchaných vůči podnikům a řadí se tedy v dnešní době mezi nejčastější druhy útoků, kterým podniky musí čelit. Je jisté, že vzhledem k neustálé rozvíjející se digitální době, bude mít problematika kybernetické bezpečnosti stále vzestupnou tendenci a podniky budou muset stále více řešit, jakým způsobem se proti kybernetickým hrozbám bránit. Nejdříve je potřeba upřesnit, co se pod pojem kybernetické bezpečnost rozumí.

Kybernetická bezpečnost je obor zabývající se ochranou počítačových systémů a sítí před kybernetickými útoky. Rozdělení a specifice jednotlivých kybernetických útoků se nachází až v nadcházející části, takže jen pro úvod, kybernetické útoky zahrnují neoprávněné přístupy k systémům, poškození softwaru, či hardwaru nebo poškození dat a elektronických údajů.

Základem kybernetické bezpečnosti je dosažení důvěrnosti, integrity a dostupnosti počítačových sítí a systémů.

Důvěrností se rozumí, že k podnikovým informacím se dostane pouze ten, kdo má oprávněný přístup, a naopak všem neoprávněným osobám je číst informace znemožněno.

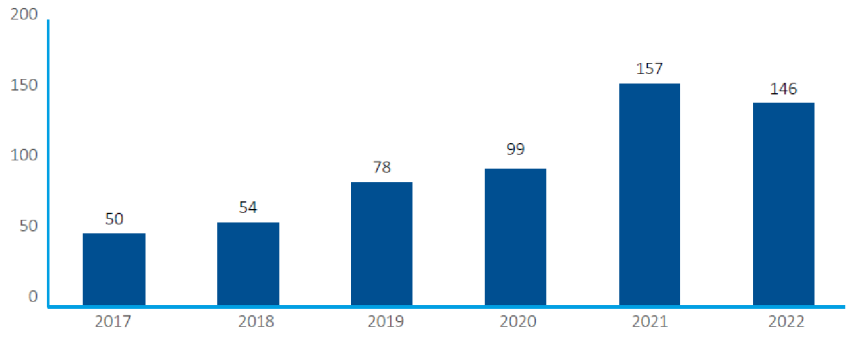
Integrita souvisí i s důvěrností a znamená, že informace nejsou nekontrolovaně, nebo neoprávněně změněny.

Dostupnost spočívá v zajištění nepřetržitého fungování počítačových systémů, nebo alespoň s výpadky, se kterými podnik počítá, nebo jsou pro něho akceptovatelné.

4.1. Trend kybernetických útoků v roce 2022

Kybernetická bezpečnost v České republice spadá pod dohled Národního ústavu pro kybernetickou bezpečnost (NÚKIB), jenž každý rok vydává souhrnnou zprávu o jejím stavu. Jsou zde zmíněné významné bezpečnostní incidenty, statistiky, četnost útoků, jejich nahlášení a rady, čeho se v příštím roce vyvarovat.

Následující kapitola popisuje stav kybernetické bezpečnosti v roce 2022. V roce 2022 bylo NÚKIBem evidováno 146 kybernetických incidentů, což je lehký pokles oproti roce 2021 s počtem 157 incidentů.
Dlouhodobě má však počet detekovaných kybernetických incidentů vzestupnou tendenci. Vývoj počtu kybernetických incidentů je znázorněn na následujícím grafu.



Graf č.4: Meziroční srovnání počtu kybernetických incidentů

Pokles oproti roku 2021 může být zapříčiněný skutečností, že během roku 2022 neproběhla žádná významná kampaň pro odhalení zranitelností, které by byly následně zneužívány. Oproti tomu v roce 2021 se takové kampaně uskutečnily dvě a konkrétně byly zneužívány zranitelnosti ProxyLogon, ProxyShell a jedna z nekritičtějších zranitelností posledních let Log4Shell. Oba útoky jsou postavené na neautorizovaném vzdáleném spuštění kódu na napadnutém serveru.

Ovšem je vysoce pravděpodobné, že evidované kybernetické incidenty tvoří jen procento reálného počtu incidentů, který se odhadem pohybuje ve vyšších stovkách.[25]

Kybernetická aktivita v souvislosti s geopolitickými událostmi

Kybernetická aktivita je ovlivněna mnoha faktory, jedním z nich je i geopolitický faktor, který v roce 2022 představuje především počátek ruské invaze na Ukrajinu. Přestože invaze začala na konci února, nejvíc kybernetických útoků bylo zaznamenáno v dubnu a říjnu. Jednalo se především o DDoS útoky, tedy o pokusy o zahlcení serverů.

Během roku 2022 došlo k několika vlnám DDoS útoků, ke kterým se přihlásili ruskojazyční hackerské skupiny. Jejich cílem byly hlavně subjekty veřejného sektoru, ale i řada soukromých organizací.

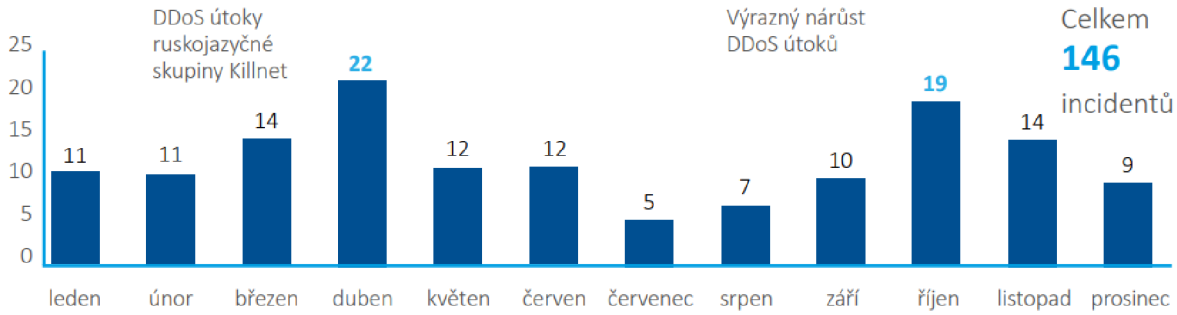
V dubnu 2022 proběhly dvě série DDoS útoků ruskojazyčné hackerské skupiny Killnet. Celkem bylo zasaženo 22 významných subjektů včetně řady ministerstev. Tento útok je označován jako reakce na oznámení oprav ukrajinské těžké vojenské techniky na území ČR.

V říjnu hackerská skupina Anonymous Russia oznámila rozsáhlý DDoS útok na vládní instituce, média, banky a letiště. Reálně bylo zasaženo jen zlomek vytyčených cílů. V tomto případě nebylo prokázáno žádné spojení s konkrétní činností či vyjádřením v souvislosti s děním na Ukrajině.
Na následujícím grafů lze vidět, jakým způsobem se vyvíjel počet DDos útoků během roku 2022.[26]

---

[25] *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022* [online]. 2022, 7-8 [cit. 2023-09-04]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

[26] *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022* [online]. 2022, 7-8 [cit. 2023-09-04]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/



Graf č.5: Četnost DDoS útoků během roku 2022

4.2. Klasifikace kybernetických incidentů

Kybernetické incidenty lze z hlediska cíle útoku rozdělit do několik skupin. Existuje více pohledů na klasifikovaní kybernetických incidentů, v této práci je dodržena klasifikace dle výroční zprávy NÚKIB.

Následující tabulka nabízí porovnání míry zastoupení jednotlivých typů kybernetických incidentů, které byly nahlášeny NÚKIB v letech 2021 a 2022.

Typ kybernetického incidentu	**Procentuální zastoupení 2021**	**Procentuální zastoupení 2022**
Dostupnost	34%	58%
Malware	25%	8%
Průnik	22%	12%
Podvod	10%	11%
Informační bezpečnost	8%	10%
Pokus o průnik	1%	0%
Sběr informací	0%	0%
Urážlivý obsah	0%	0%
Ostatní	0%	3%

Z tabulky lze vyčíst vysoký podíl kybernetických útoků na dostupnost. Jak už bylo výše zmíněno, nárůst souvisí i se dvěma masivními DDoS útoky, ke kterým se přihlásily ruskojazyčné hackerské skupiny.

Naopak významný pokles zaznamenaly kybernetické incidenty použití malwarů. Opět už bylo výše zmíněno, že v roce 2021 se ve velkém měřítku využívaly známé zranitelnosti, které právě zahrnovaly nahrání škodlivých kódů na napadnutých serverech. V roce 2022 se žádná významná a kritická zranitelnost neukázala, čímž lze vysvětlit znatelný pokles v této oblasti kybernetických incidentů.[27]

a) Útoky na dostupnost

Do typu kybernetického incidentu ohrožující dostupnost spadají útoky, které přerušují, nebo výrazně omezují provoz napadnutého serveru.

Nejrozšířenější jsou tzv. DoS (Denial-of-Service) a ještě specifičtější DDoS (Distributed denial-of-service) útoky, které přehlcují servery obrovským množstvím dotazů a tím znemožňují, anebo aspoň výrazně zpomalují fungování serveru pro jeho skutečné klienty.

V případě, že je útok prováděn z jednoho místa, jedná se o DoS útok (Denial-of-Service). K zneškodnění takového útoku je potřeba odhalit a zablokovat jen jeden konkrétní zdroj.

Mnohem častějším a účinnějším útokem je DDoS, (Distributed denial-of-service), kdy zahlcující dotazy pochází z více zdrojů, neboli z distribuované sítě. V případě DDoS se často využívají tzv. botnety, neboli sítě počítačů infikovaných škodlivým softwarem řízeným z jediného centra. Takto infikované počítače se potom bez vědomí majitelů podílí na DDoS útoku nebo jiných kybernetických trestných aktivit.

---

[27] *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022* [online]. 2022, 8-10 [cit. 2023-09-04]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

DDoS útok je oproti DoS efektivnější a pro útočníky výhodnější metodou. První výhoda spočívá v tom, že větší počet útočníků dokáže vygenerovat mnohem větší množství zpráv, a tím více a efektivněji zahltit síťový provoz než jediný počítač.

Další výhodou DDoS s více útočníky je složitější odvrácení útoku, protože je potřeba detekovat a zamezit přístup více zařízením. Složitější detekce souvisí i s tím, že jednotliví útočníci mohou být méně nápadní, protože tok zahlcujících dat se rozdělí mezi více útočících zařízení.
Existuje více metod, jak DDoS a DoS útoky provést. Všechny způsoby ale mají několik společných rysů. Zaplavují síť náhodnými daty, čímž způsobují nadměrnou zátěž operačního systému na cílovém serveru a brání tak přenosu oprávněných informací. Cílem je přerušit přístup určitého uživatele k službě. Mění konfigurační nastavení a vkládají falešná chybová hlášení, čímž mohou narušit stabilitu operačního systému a v nejhorším případě mohou způsobit jeho úplné selhání.

Proti DoS, DDoS útokům se lze bránit zahrnutí implementace bezpečnostních opatření v síti a filtrováním provozu. Typickým a účinným nástrojem jsou firewally, které blokují požadované IP adresy.
Dále existují specializované softwary proti DDoS útokům, které například znemožňují nebo upozorňují na skenování portů, anebo omezují tzv. ping dotazy.

K navýšení bezpečnosti je také vhodné pravidelně aktualizovat používané systémy, protože aktualizace v sobě často zahrnují nově ošetřené zranitelnosti.[28]

b) Průnik a informační bezpečnost

Průnikem se rozumí kompromitace zaměstnaneckého uživatelského účtu nebo samotného informačního systému, který podnik používá.
Průnik zpravidla navazuje na nějaký předchozí jiný kybernetický útok, například díky úspěšnému phishingu útočník získá zaměstnanecké přihlašovací údaje, které potom zneužije k přihlášení do podnikového informačního systému.

[28] *Denial-of-service attack* [online]. 2023 [cit. 2023-09-04]. Dostupné z: https://en.wikipedia.org/wiki/Denial-of-service_attack

Pod kybernetickými útoky na informační bezpečnost se rozumí neautorizovaný přístup k datům nebo neautorizovaná změna informace.

Útočníci nevyužívají kompromitovaných přístupových údajů jako je tomu u průniku, ale podaří se jim i přesto využít slabin autentizačních systémů a dostanou se k datům, ke kterým jinak nemají přístupové právo. Už jen samotné neautorizované prohlížení nebo kopírování dat se považuje za úspěšný útok, další podobou útoku je pozměnění dat.

c) Malware

Malware (zkratka z anglického "malicious software") je termín používaný pro označení počítačového softwaru, který byl vytvořen s úmyslem způsobit škodu, odcizení dat, nebo provádět jiné nelegitimní činnosti na cílovém systému, zařízení nebo síti.

Malware zahrnuje různé druhy škodlivých programů, jako jsou viry, červi, trojské koně, ransomware, spyware, adware a další. Jeho cílem může být ovládnutí systému, krádež citlivých informací, šíření spamu, vyřazení systému z provozu nebo jiné formy poškození. Malware může být šířen pomocí infikovaných souborů, e-mailových příloh, škodlivých odkazů nebo zranitelností v softwaru.

Ransomware

Ransomware je složenina dvou anglických slov – ransom a software. Jak napovídá překlad, jedná se o škodlivý program, který způsobí škody v počítačovém systému a následně se po podniku, který systém využívá, požaduje výkupné pro navrácení systému do původního stavu.

Ransomware počítačový systém typicky zablokuje, nebo zašifruje uživatelská data. Odblokování nebo odšifrování dat je i pro technické znalce nemožné. Například k odšifrování je potřeba znalosti kryptografického klíče, kterým disponuje pouze útočník. Napadenému podniku nezbývá nic jiného, než požadované výkupné zaplatit.

Nejčastěji jsou ransomware útoky prováděny na podniky státní správy nebo kritické infrastruktury, kde jakýkoli výpadek počítačového systému může mít fatální důsledky.

V Česku bylo NÚKIBem během roku 2022 zaznamenáno 27 kybernetických incidentů, které způsobil ransomware. Kolem 15 % dotazovaných podniků uvedlo, že se setkaly buď s úspěšným útokem nebo aspoň s pokusem o ransomwarový útok.

Malware jako služba

Škodlivé softwary jsou využívány také jako samostatný produkt. Ovšem protože jde o kriminální aktivitu, nejsou nabízeny oficiální cestou. Kyberkriminální skupiny nabízejí za peníze svoje služby na tzv. darkwebu, (část webu, která není přístupná přes obyčejné prohlížeče, ale je za potřebí specializovaného softwaru a konfigurace).

Obecně je možno na darkwebu zakoupit jakoukoliv kyberkriminální službu, pro což se používá termín cybercrime-as-a-service. Ke koupi jsou nabízeny ransomware (ransomware-as-a-service), což je speciální druh malwaru, kompletní phishingové (phishing-as-a-service), vishingové (vishing-as-a-service) kampaně, nebo přístupy k infikovaným zařízením za účelem provádění DDoS útoků (DDoS-as-a-service).

Speciálně u ransomwaru se od roku 2019 eviduje převažování ransomwaru ve formě služby. Specifické pro tento druh ransomwaru je víceúrovňové vydírání. Kromě klasického zašifrování dat je na napadenou oběť vyvíjen tlak hrozbou zveřejnění citlivých interních dat, DDoS útoky a kontaktování dalších partnerů nebo zákazníků.

Model prodeje na darkwebu umožňuje se zúčastnit trestní kybernetické činnosti i méně technicky zdatným útočníkům. Naopak pro poskytovatele těchto služeb plyne z prodeje velký zisk. Vzhledem k narůstající popularitě je se stávají produkty pro kyberkriminální činnost stále dostupnějšími.

d) Podvody

Podvodné kampaně patří k nejčastějším způsobům kybernetického útoku. Do statistik spadají více i méně sofistikované kampaně, ale aspoň s nějakým pokusem o podvod se setkaly skoro všechny dotazované podniky.
Během roku 2022 se s pokusem či úspěšným phishingovým útokem setkalo 92 % dotazovaných podniků a vishing zaznamenalo 20 % podniků.

Phishing

Phishing je forma kybernetického útoku, při kterém se útočníci vydávají za důvěryhodnou stranu, přičemž se snaží získat citlivé informace, jako jsou hesla, osobní údaje nebo platební údaje. Útoky jsou zpravidla prováděny rozesíláním podvodných e-mailů, zpráv, nebo přesměrováním na falešné webové stránky.

Typickými phinshingovými zprávami, které cílí na zaměstnance podniku, jsou falešné e-maily od nadřízeného, kolegy, od externího dodavatele, nebo od IT oddělení. Emaily jsou typicky posílány z jiné jen neznatelně upravené emailové adresy, čehož si zaměstnanci nemusí na první pohled všimnout a mohou na takový e-mail reagovat. V emailu se potom objevuje odkaz na falešnou stránku, kterou už mají pod kontrolou útočníci.

Emaily od IT oddělení mají v příloze ke stažení softwary pro aktualizaci, které ve skutečnosti obsahují malware. Ve falešné zprávě o bezpečnosti bývá například uvedeno, že došlo k porušení bezpečnosti a že zaměstnanci musejí okamžitě změnit svá hesla na odkazu uvedeném v e-mailu. Odkaz vede na falešnou stránku, kde útočníci získají nová hesla.

Vishing

Termínem vishing se rozumí podvodné telefonáty, při kterých se útočníci snaží získat přihlašovací údaje a tím získat přístup do informačních systémů podniku. V oblasti podnikové bezpečnosti se nejedná o takovou hrozbu v porovnání s phishingovými útoky. Nicméně popularita vishingu má vzestupnou tendenci a oproti 2021 byl zaznamenán větší nárůst než nárůst u phishingových útoků.

4.3. Současné možnosti zajištění kybernetické bezpečnosti

4.3.1. Aktuální průzkumy

Pro uvedení současné situace, jak jsou podniky schopny se vypořádat s kybernetickými hrozbami, jsou v této kapitole uvedeny dva průzkumy, které se kromě vnímání závažnosti kybernetických hrozeb zaměřily na investice podniků do kybernetické bezpečnosti.

EY průzkum zájmu o kybernetickou bezpečnost

V roce 2018 společnost EY zveřejnila průzkum, který ukázal stále rostoucí zájem o kybernetickou bezpečnost mezi podniky. Zjistilo se, že 87 % dotazovaných podniků má jen omezené prostředky pro čelení kybernetickým hrozbám. Přestože byly tyto podniky informovány o rizicích kybernetických útoků, jen méně než pětina z nich měla propracovanou strategii týkající se kybernetické bezpečnosti. Více než 60 % firem nepřiřadilo přímou odpovědnost za kybernetickou bezpečnost členu výkonného vedení.

V průzkumu se ukázalo, že více než 65 % respondentů z větších podniků považuje stávající bezpečnostní opatření proti kybernetickým hrozbám za nedostatečná. Většina těchto firem plánovala v následujících dvou letech zvýšit investice do kybernetické bezpečnosti.

Jako největší slabina byla identifikována lidská chyba, za kterou stála 34 % nejzávažnějších hrozeb. Dalšími častými příčinami byly zastaralé bezpečnostní kontroly (26%), neoprávněné přístupy (13%) a nesprávné zacházení s využíváním cloudových služeb (10%).

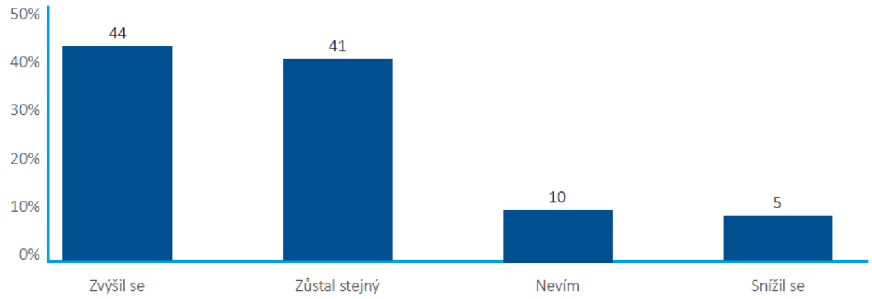
Z průzkumu rovněž vyplývá, že mnoho firem bylo k implementaci bezpečnostních systémů donuceno až vlastními zkušenostmi. Tyto podniky se dříve setkaly s útoky a vysoké náklady na odstranění škod je motivovaly k zavedení opatření, která by omezovala podobné incidenty v budoucnosti.

V oblasti investic se podniky zaměřovaly zejména na moderní technologie, včetně využívání cloudových služeb a softwarů analyzujících a odhalujících kybernetické hrozby.[29]

4.3.2. Finance vynaložené na kybernetickou bezpečnost

Fakt, že podniky jsou si pořád více vědomy kybernetického nebezpeční odráží i trend neustálého navyšováním výdajů do kybernetické bezpečnosti. Děje se tak i navzdory složité ekonomické situaci spojené s vysokou inflací a vysokými cenami za energie.

Na následujícím grafu je znázorněno, že drtivá většina podniků dotázaných NÚKIBem uvedla, že do kybernetické bezpečnosti investovala v roce 2022 více nebo stejně peněz v porovnání s rokem 2021.

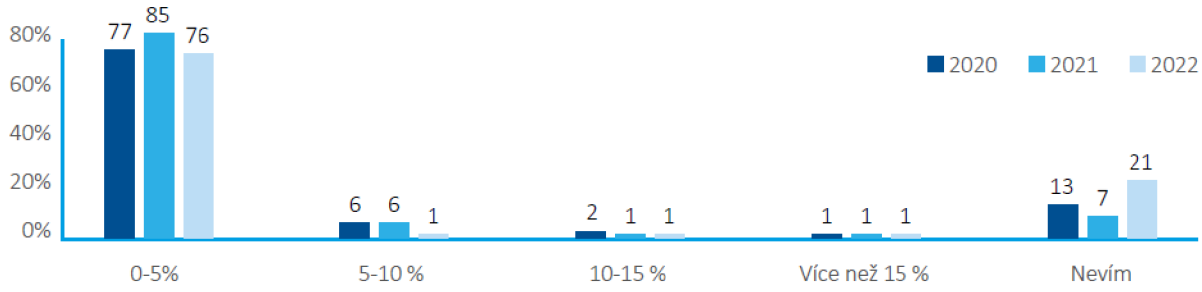


Graf č.6: Vývoj rozpočtů respondentů alokovaných na kybernetickou bezpečnost oproti roku 2021 (% respondentů)

I přes zvýšené výdaje stále více jak polovina dotázaných zástupců podniků vnímá tyto prostředky jako nedostatečné.

Stejně jako v předchozích letech, většina organizací alokuje na oblast kybernetické bezpečnosti mezi 0 a 5 % svého celkového rozpočtu.

[29] EY: 82 % firem netuší, zda jejich metody odhalování bezpečnostních incidentů fungují. *Channel World* [online]. 2018 [cit. 2023-09-04]. Dostupné z: https://www.channelworld.cz/clanky/ey-82-firem-netusi-zda-jejich-metody-odhalovani-bezpecnostnich-incidentu-funguji/



Graf č.7: Podíl rozpočtu alokovaného na kybernetickou bezpečnost z celkového podnikového rozpočtu v letech 2020 – 2022 (% respondentů)

4.3.3. Odborníci na kybernetickou bezpečnost

Vytvořit v podniku specializované odvětví pro kybernetickou bezpečnost je jedním ze stěžejních předpokladů pro zajištění ochrany před kybernetickými útoky. Nestačí totiž jen nakoupit antiviry, a další bezpečnostní softwary, nebo pořádat pravidelná školení zaměstnanců. Kybernetická bezpečnost podniku je potřeba neustále monitorovat a reagovat na nastalé incidenty, k čemuž je potřeba zaměstnat odborníky v dané oblasti.

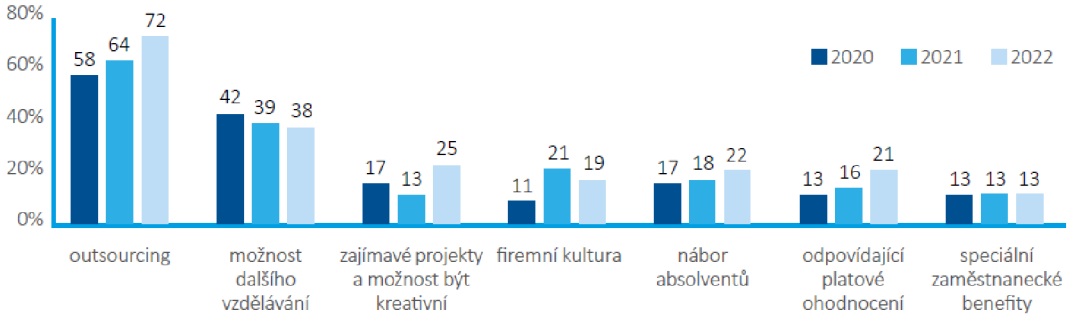
Přestože kybernetická bezpečnost se stává stále důležitějším a aktuálnějším tématem, odborníků je v této oblasti značný nedostatek. S tím úzce souvisí i vysoké finanční požadavky uchazečů na pozice v tomto odvětví. Přes 70 % dotázaných podnikových zástupců uvedlo, že nižší nabízené finanční ohodnocení je hlavním důvodem, které uchazeče odrazuje při pracovních náborech.

Podniky mají na výběr několik řešení. Nejčastějším způsobem je outsourcing, který oproti roku 2020 vzrostl o téměř 15 %, přestože už tehdy uplatňovala toto řešení více jak polovina respondentů.

Dalšími častými způsoby, jak se podniky vypořádávají s nedostatečným zájmem o pracovní pozice je nabízení možnosti dalšího vzděláván a příležitostí zapojit se

do zajímavých projektů. Souvisí to s tím, že tato oblast je rychle měnící se a pro uchazeče je důležité zůstat v kontaktu s novými technologiemi a trendy.

22 % podniků si může dovolit nabírat absolventy, což je jedním ze stěžejních předpokladů pro rozvíjení této oblasti do budoucna. [30]



Graf č.8: Jak se podniky v letech 2020-2022 snažily vypořádat s nedostatkem odborníků v oblasti kybernetické bezpečnosti (% respondentů)

4.4. Nástroje a formy pro zajištění kybernetické bezpečnosti

Rámec, jakým způsobem můžou podniky dosáhnout zajištění bezpečnosti před kybernetickými hrozbami udává mezinárodní standard ISO 27001. Požadavky, které podniky musí kybernetickou bezpečnost řešit, zase udává evropská směrnice NIS2.

a) NIS2

V rámci Evropské unie je legislativa zabývající se kybernetickou bezpečností upravena směrnicí NIS2. Směrnice se především zaměřuje na povinnost zavedení technologií zabezpečující podnikové informační systémy proti kybernetickým hrozbám, nebo na zlepšení schopnosti reagovat na nové hrozby v digitálním

[30] *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022* [online]. 2022, 13-14 [cit. 2023-09-04]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

prostoru. Nově je také pozornost věnována bezpečnosti IoT (Internet of Things) zařízení.

Obecně je vyžadováno, aby pro informační systémy byly zajištěny tři základní požadavky - dostupnost, důvěrnost a integrita. Z hlediska dostupnosti je vyžadováno, aby informační systémy běžely nepřetržitě, což souvisí s požadavkem na zálohovaní dat a zdrojů, na kterých systémy běží. Pro splnění důvěrnost a integrity je konkrétně vyžadováno zabezpečení systémů pomocí hesel, digitálních certifikátů nebo jiných autorizací.

V případě zjištění bezpečnostního incidentu musí být podáno hlášení příslušnému úřadu. V České republice je k tomuto účelu pověřen NÚKIB.

Směrnice se vztahuje především na vybrané podniky, které spadají do kritické infrastruktury, nebo jsou regulovány kvůli své významnosti nebo zranitelnosti.

Oproti předchozí směrnici NIS z roku 2016 je regulována mnohem širší oblast podniků. Mezi nově regulované oblasti spadají například potravinářství, poskytovatelé služeb a sítí elektronických komunikací.

Celkem je směrnicí regulováno přibližně 60 služeb v 18 odvětvích. Podniky spadají do dvou kategorií podle míry regulovanosti a vyplývajících povinností. Do více regulované kategorie tzv. „essential“ spadají například odvětví energetiky, dopravy, bankovnictví, zdravotnictví, digitální infrastruktury nebo veřejné správy. Druhá méně regulovaná skupina tzv „important“ zahrnuje poštovní služby, odpadové hospodářství, chemický průmysl, potravinářství, poskytování digitálních služeb.

Nicméně je stanoveno pravidlo, že regulace platí jen pro podniky zaměstnávající více než 50 zaměstnanců, nebo pokud jejich roční obrat překračuje 250 miliónů korun.

Oproti předchozí úpravě je důraz je kladen i na zvýšenou spolupráci mezi členskými státy, nebo na rozšířenou povinnost hlášení kybernetických incidentů. V České republice jsou kybernetické incidenty zpravidla registrovány NÚKIBem.

Směrnice NIS2 byla publikována v prosinci 2022 a v platnost vyjde v říjnu 2024. Do té doby je povinností všech členských států zařadit obsah směrnice do vlastní legislativní úpravy. Do české legislativy je směrnice NIS2 implementována v rámci nového zákona o kybernetické bezpečnosti a osmi prováděcích vyhlášek.[31]

b) ISO 27001

Mezinárodní standard ISO 27001 byl naposledy revidován v roce 2022 a uvádí aktuální rámec, jakým způsobem mají být spravovány informační systémy.

Standard vyžaduje, aby management, nebo jiné příslušné oddělení podniku systematicky zkoumalo rizika informační bezpečnosti s ohledem na hrozby a eventuální dopady pro podnik.

Standard zahrnuje požadavky na fyzickou bezpečnost, firewally, autorizované softwary nebo požadavky na zajištění autentizace při přihlašování do informačních systémů.

c) Zálohování dat

Zálohování dat je jedním z klíčových požadavků pro zajištění bezproblémového fungování podnikových informačních systémů.

Existuje několik důvodů, proč je nezbytné pravidelně zálohovat data. Podniková data mohou být napadena útočníky, kteří se mohou pokusit odcizit, zašifrovat po napadením systému ransomwarem nebo k datům znemožnit přístup.

Kybernetické útoky ale nejsou jediným způsobem, jako mohou podniky o svá data přijít. Ke ztrátě dat mohou vést i technické poruchy, chyby v systémech, nebo

[31] *NÚKIB spouští webové stránky ke směrnici NIS2* [online]. 2022 [cit. 2023-09-05]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1869-nukib-spousti-webove-stranky-ke-smernici-nis2/

fyzické poškození hardwaru. Všechny tyto události jsou nepředvídatelné a podnik by měl počítat, že nastanou.
V některých odvětvích je přímo v rámci právních předpisů vyžadováno, aby podniky uchovávaly zálohy dat. Do těchto odvětví spadá kritická infrastruktura, bankovnictví a další podniky, které jsou regulovány evropskou směrnicí NIS2. Správně provedené zálohování může podnikům pomoci splnit tyto požadavky.

Data se mohou zálohovat v režimu online, neboli počítač se zálohuje za jeho běžného chodu. Dalším způsobem je zálohovat data offline, kdy zálohování je prováděno mimo běžný provoz počítače a obvykle za pomoci zavedení speciálního média. V dnešní době se kromě klasického zálohování na pevné disky často využívá možnosti zálohovat dat na cloudových úložištích.

Důležitým principem, který se při zálohování uplatňuje je "3-2-1" pravidlo, které znamená, že by měly existovat minimálně tři kopie dat, uložené na alespoň dvou různých typech médií a minimálně jedna z těchto kopií by měla být fyzicky umístěna na jiném místě než původní data.

Statistiky ukazují, že podniky do systematického, a hlavně pravidelného zálohování neinvestují dostatečně, přestože mohou mít významně vyšší náklady a problémy v případě, že data ztratí.

d) Bezpečnostní softwary

Antivirový program, též známý jako anti-malware, je softwarový nástroj používaný k prevenci, detekci a odstraňování škodlivého softwaru, zvaného malware. Tento program má schopnost identifikovat a neutralizovat různé typy hrozeb, včetně virů, trojských koní, spywaru a ransomwaru.

Nejběžnějším případem, že antivirus běží lokálně na jednotlivých počítačích, ale stále častěji je využívané cloudové antivirové řešení, kde je na uživatelském zařízení nainstalována lehčí verze a většina analýz probíhá na cloudových serverech.

Kromě základní ochrany proti malwaru mnohé antivirové produkty zahrnují také ochranu proti škodlivým URL adresám, spamu a phishingu.

Dalším způsobem, jak chránit informační systémy proti kybernetickým hrozbám, je implementace firewallu, který podle definovaných pravidel zamítá všechny přístupy z adres, které nejsou povoleny.

Protože samotné antivirové programy nemusí být dostatečné, a navíc bývají prvním, co škodlivé programy napadají, je užitečné mít systémy monitorované ještě z jiného místa. K tomu slouží online skenování, které umožňuje provést kontrolu počítače pomocí online zdroje a detekuje hrozby, přestože už antivirový program nefunguje.

K identifikování DDoS útoků jsou určeny IDPS systémy, neboli systémy detekce a prevence narušení, které monitorují síťový provoz a detekují neobvyklé aktivity a pokusy o neoprávněný vstup do systémů.

Pokročilejším řešením proti sofistikovaným hrozbám jsou Security Information and Event Management (SIEM) systémy, které se zaměřují na dlouhodobé ukládání událostí, jejich analýzu a vytváření upozornění. SIEM systémy monitorují infrastrukturu, korelují události a poskytují v reálném čase varování o potenciálních problémech.

e) Systémy řízení identit

Při každém informačním systému je potřeba zajistit, aby k němu neměl přístup nikdo neoprávněný. Jednak, aby k informačním systémům neměl mít přístup nikdo z venku podniku, ale také v rámci podniku je potřeba řídit oprávnění a role zaměstnanců.

K tomuto účelu slouží systémy řízení identit. Tyto systémy mají za cíl spravovat informace o uživatelích, zajišťovat identifikaci, autentizaci, autorizaci a oprávnění uživatelů na základě stanovených politik.

Identifikace neboli ztotožnění uživatele znamená určení, kdo daný uživatel je. Tento krok je se provádí při přihlašování nebo při vyhledávání informací v databázích.

Systémy řízení identit se dále zabývají autentizací, což je proces ověření, že uživatel je skutečně tím, za koho se vydává. Zaměstnancům jsou uděleny jejich přihlašovací údaje, které jsou pro každý informační systém specifické. Typicky je požadované přihlašovací jméno a heslo, ale čím více jsou využívané také speciální hardwary v podobě bezpečnostní tokenů, nebo prokazování se biometrickým údaji. Systémy řízení identity potom při přihlašování tyto údaje ověřují ve vlastní databázi a poskytnou, nebo odmítnou k informačnímu systému přístup.
Pro zajištění větší bezpečnosti je vhodné zavést více faktorovou autentizaci, což znamená, že uživatel musí znát nejen heslo, ale ve druhé fázi připojit například bezpečnostní token.

Další důležitou funkcí systémů řízení identit je autorizace, spočívající v udělení jednotlivým uživatelům oprávnění, jakým způsobem mohou informační systém využívat. Oprávnění a zaměstnanecké role musí vyplývat z podnikové politiky.

Systémy řízení identit však sami o sobě neochraňují podnik před kybernetickým útokem krádeže identity. Jakmile se útočník phishingovým útokem, nebo jiným způsobem dostane k heslům a jiným přihlašovacím údajům oprávněných uživatelů, systémy řízení identit jej nezachytí a útočník má přístup k interním podnikovým datům.

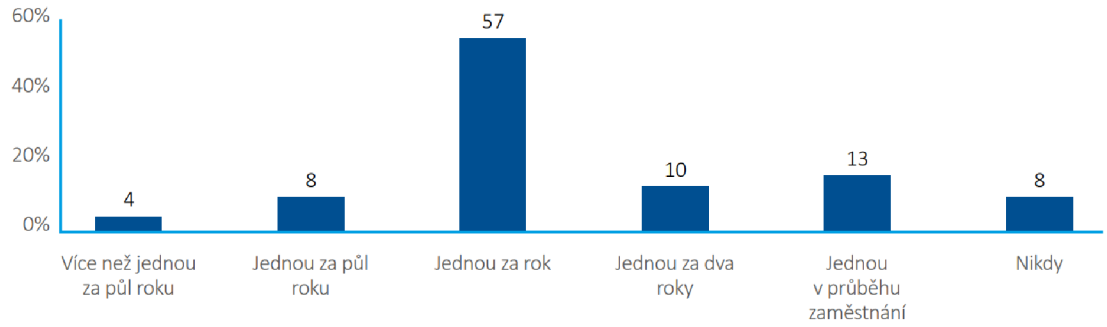
Proto i zde je důležité zmínit klíčový lidský faktor a zodpovědnost zaměstnanců za chránění svých osobních údajů pro přihlašování.

f) Školení, testování zaměstnanců

Lidský faktor hraje v kybernetické bezpečnosti velkou roli. Podstatná část kybernetických incidentů je zapříčiněna neopatrností, nevědomostí nebo jinou

chybou zaměstnance. Odtud plyne, že zásadní součástí zajištění kybernetické bezpečnosti je pravidelné testování a pořádání zaměstnaneckých školení.

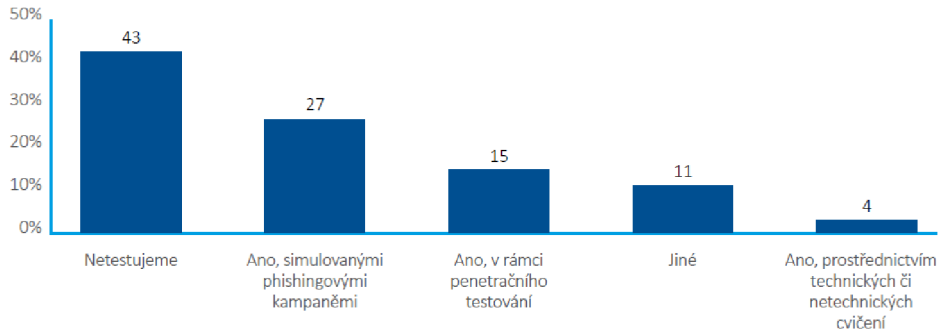
Více než polovina dotazovaných podniků uvedla, že organizuje školení více než jednou za rok, přičemž jen necelých 5 % neproškoluje své zaměstnance vůbec. Školení by mělo být zaměřeno především na technologie, se kterými podnik nebo konkrétní oddělení pracuje, a přizpůsobeno typu pracoviště a možnosti závažnosti kybernetických incidentů, se kterými se konkrétní zaměstnanci může setkat.



Graf č.9: Frekvence školení zaměstnanců v oblasti kybernetické bezpečnosti v podnicích za rok 2022 (% respondentů)

Nějakou formou provádí testování svých systémů přes polovina podniků. Technická bezpečnost systémů se nejčastěji ověřuje prostřednictvím penetračních testů, do kterých investuje přes 15 % podniků.

V oblasti organizační opatření se jednoznačně nejvíce pozornosti věnuje phishingovým útokům.
Oddělení zaměřené na kybernetickou bezpečnost rozešle ostatním zaměstnancům emaily se škodlivým obsahem a následně analyzuje, kolik procent zaměstnanců správně zareagovalo. Na základě výsledků takových testování se můžou upravovat školící materiály, nebo jiná bezpečnostní politika podniku.



Graf č.10: Formy testování odolnosti zaměstnanců proti kybernetickým hrozbám v podnicích za rok 2022. (% respondentů)

Zaměstnanci by měli být informováni o rizicích phishingu ve formě školení nebo v rámci jiných vzdělávacích programů. Obecně platí pravidlo, že je důležité klást důraz na kontrolování od koho email ve skutečnosti pochází a pokud obsahuje email jakýkoliv obsah ke stažení, ověřit si ještě z jiného zdroje, zda opravdu nejde o škodlivý obsah.

Další metodou, jak se proti phishingu efektivně bránit, je spolupráce zaměstnanců s IT oddělením podniku. Pokud zaměstnanci posoudí příchozí email za phishingový útok, pošlou upozornění na IT oddělení, které ověří, zda se o phishing skutečně jedná. Následně můžou varovat další zaměstnance, aby se tomuto útoku také vyvarovali. Dále můžou zablokovat konkrétní emailovou adresu, nebo dokonce celou doménu, pokud byl z této domény útok opakovaný. Tím se aspoň částečně předchází dalším potenciálním phishingovým útokům.[32]

g) Penetrační testování

Penetrační testování je metoda, která testuje a následně hodnotí míru zabezpečení počítačových zařízení, systémů nebo aplikací. Cílem testování není bezpečností hrozby opravit, ale jen na ně upozornit a odhalit slabá místa testovaného systému, či aplikace. Po provedeném testování se sepisuje

[32] *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022* [online]. 2022, 27-28 [cit. 2023-09-04]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

závěrečná zpráva, která by měla shrnout výsledky, v případě nálezu upozornit na nedostatky a přiložit informace o možných důsledcích v případě jejich neodstranění.

V celkové analýze bývají také posouzeny možné dopady na ekonomiku podniku, v případě, že by k došlo ke zneužití daného odhaleného slabého místa.
Testuje se především simulací možných útoků, které mohou být prováděny jak zvenku, tak zevnitř podniku.
Penetrační testování je široký pojem, zahrnuje jak prověřování technické oblasti, čímž se rozumí odolnost vůči známým softwarovým, či hardwarovým zranitelnostem, nastavení připojení k síti, přístupné porty, zabezpečení databází atd.

Mimo technické oblasti se penetrační testování zabývá i oblastí organizačních opatření, do které spadají podvody a sociální inženýrství vůči zaměstnancům.

Penetrační testování je prováděno odborníky v oblasti kybernetické bezpečnosti, kteří mají sice k dispozici zautomatizované procesy, které odhalí většinu známých a často prověřovaných chyb, ale vždy je také důležitý specifický přístup ke konkrétnímu testovanému systému.

Pro oblast technického zabezpečení existují volně dostupné nástroje (Kali-Linux, BlackArch), díky kterým si mohou uživatelé provádět penetrační testování sami, nicméně v mnoha odvětvích je vyžadováno, aby se testování provádělo nezávislou stranou a bylo součástí komplexního bezpečnostního auditu. Některá odvětví jako je energetika nebo bankovnictví vyžadují pravidelné penetrační testování opakující se každý rok, nebo kdykoliv po změně systému.

Závěr

Zajištění bezpečnosti podniku je rozsáhlý problém, který zahrnuje účelnou prevenci, a dostačující kontroly nad podnikovými procesy. Narozdíl od bezpečnosti jednotlivce, nebo státu, není podniková bezpečnost řízena institucionálně a je na zodpovědnosti managementu podniku, aby bezpečnost zajistil.

Podle dostupných analýz vypracovaných společnostmi PwC a EY, jsou nejčastěji zájmy podniku ohroženy podvody vlastních zaměstnanců, podvody ze stran zákazníka nebo kybernetickými útoky.

Mezi podvody způsobených vlastními zaměstnanci se řadí zejména zpronevěra podnikového majetku, ale také krádeže, různé druhy fraudů, nebo korupce. Přičemž podniky zajistí bezpečnost rámcově implementací systému řízení rizik podvodů, mezi konkrétní formy zajištění bezpečnosti patří dělba kompetencí mezi více zaměstnanců, vypracovaní datových analýz, pořádání pravidelných interních, nebo forenzních auditů. Nedílnou součástí je také vytvoření správné podnikové kultury, včetně prostoru pro whistleblowing.

Kybernetické hrozby představují útoky na dostupnost jako jsou DoS a DDoS útoky, útoky na informační bezpečnost, malwary nebo phishingové a vishingové podvody. Přičemž během posledních let jsou na vzestupu právě phishingové podvody.

Z výzkumu vyplývá, že v současné době podniky vnímají kybernetické hrozby jako velké riziko, nicméně pořád do kybernetické bezpečnosti dostatečně neinvestují. Navíc na trhu je pro tuto oblast nedostatek odborníků.

V roce 2023 vstupuje v platnost nová evropská směrnice NIS2, která určuje povinnost více podnikům implementovat bezpečnostní opatření proti kybernetickým hrozbám, než tomu bylo doposud.

Mezi konkrétní způsoby, jak se proti kybernetickým hrozbám bránit, patří zálohováni podnikových dat, instalace bezpečnostních softwaru, systémů řízení identit. Protože selhání lidského faktoru je v rámci kybernetických útoku znatelně slabým místem, je potřeba, aby podniky na toto téma pravidelně proškolovali a testovali své zaměstnance.

Seznam literatury

5 Fraud Risk Management Principles & Assessment Strategies [online]. 2022, 1 [cit. 2023-09-03]. Dostupné z: https://datadome.co/threats/fraud-risk-management/

Co je korupce. *Policie.cz* [online]. 2023 [cit. 2023-09-04]. Dostupné z: https://www.policie.cz/clanek/co-je-korupce.aspx

Česká bezpečnostní terminologie Výklad základních pojmů [online]. 2003, 20 [cit. 2023-09-03]. Dostupné z: https://moodle.unob.cz/pluginfile.php/11277/course/section/3043/%C4%8Cesk%C3%A1%20bezpe%C4%8Dnostn%C3%AD%20terminologie.pdf

DEFINICE PODNIKU. *Technologická agentura ČR* [online]. 2020, 3 [cit. 2023-09-03]. Dostupné z: https://www.tacr.cz/wp-content/uploads/documents/2020/02/24/1582544648_definice_podniku.pdf

Denial-of-service attack [online]. 2023 [cit. 2023-09-04]. Dostupné z: https://en.wikipedia.org/wiki/Denial-of-service_attack

EY [online]. 2021 [cit. 2023-09-04]. Dostupné z: https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

EY: 82 % firem netuší, zda jejich metody odhalování bezpečnostních incidentů fungují. *Channel World* [online]. 2018 [cit. 2023-09-04]. Dostupné z: https://www.channelworld.cz/clanky/ey-82-firem-netusi-zda-jejich-metody-odhalovani-bezpecnostnich-incidentu-funguji/

Global Economic Crime and Fraud Survey 2018 Czech Republic. *Global Economic Crime and Fraud Survey 2018* [online]. 2018, [cit. 2023-09-03]. Dostupné z: https://www.pwc.com/cz/en/hospodarska-kriminalita/assets/pdf/gecs-survey-report-pro-cr-2018.pdf

Global profiles of the fraudster: Technology enables and weak controls fuel the fraud [online]. 2016, [cit. 2023-09-03]. Dostupné z: https://www.vyrostli-jsme.cz/profil-typickeho-podvodnika

Interní audit [online]. 2022 [cit. 2023-09-03]. Dostupné z: https://cs.wikipedia.org/wiki/Intern%C3%AD_audit

ISO 37001 Systémy protikorupčního managementu [online]. 2023 [cit. 2023-09-03]. Dostupné z: https://www.tuvsud.com/cs-cz/cinnosti/audity-a-certifikace-systemu/iso-37001-protikorup%C4%8Dn%C3%AD-management

Jak jsou na tom čeští manažeři v tolerování korupčních praktik? [online]. 2018 [cit. 2023-09-03]. Dostupné z: https://roklen24.cz/?quick_news=jak-jsou-na-tom-cesti-manazeri-v-tolerovani-korupcnich-praktik

JINDŘICH, Nový. *Manažerská ekonomie* [online]. Praha, 2023 [cit. 2023-09-03]. Studijní materiály. PAČR.

KORUPCE [online]. 2023 [cit. 2023-09-03]. Dostupné z: https://korupce.cz/ministerstvo-spravedlnosti-spustilo-medialni-kampan-na-podporu-informovanosti-o-ochrane-oznamovatelu-protipravniho-jednani/

NÚKIB spouští webové stránky ke směrnici NIS2 [online]. 2022 [cit. 2023-09-05]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1869-nukib-spousti-webove-stranky-ke-smernici-nis2/

Obecné pojmy - Hrozba. *Policie.cz* [online]. 2003 [cit. 2023-09-03]. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx

Obecné pojmy - Riziko. Policie.cz [online]. 2003 [cit. 2023-09-03]. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx

Profil typického podvodníka [online]. 2016 [cit. 2023-09-04]. Dostupné z: https://www.vyrostlijsme.cz/profil-typickeho-podvodnika.

Pulling fraud out of the shadows Global Economic Crime and Fraud Survey 2018 [online]. 24 [cit. 2023-09-04]. Dostupné z: https://www.pwc.com/gx/en/news-room/docs/pwc-global-economic-crime-survey-report.pdf

PwC's Global Economics Crime and Fraud Survey 2022 [online]. 2022, 5 [cit. 2023-09-05]. Dostupné z: https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

The EY Global Information Security Survey 2021 finds CISOs and security leaders battling against a new wave of threats unleashed by COVID-19.
Zákon č. 40/2009 Sb. Zákon trestní zákoník [online]. 2009 [cit. 2023-09-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40#p206

WIEDOVÁ, Zuzana. *PROBLEMATIKA ZKRESLOVÁNÍ ÚČETNÍCH INFORMACÍ A MANIPULACE S ÚČETNÍMI VÝKAZY*. Praha, 2012. Diplomová práce. Univerzita Karlova.

Whistleblowing [online]. 2023 [cit. 2023-09-03]. Dostupné z: https://cs.wikipedia.org/wiki/Whistleblowing

Základní pojmy pro krizové řízení. Specifické pojmy používané v krizovém řízení. *Oborový portál pro BOZP* [online]. 2003, 3 [cit. 2023-09-03]. Dostupné z: https://www.bozpinfo.cz/zakladni-pojmy-pro-krizove-rizeni-specificke-pojmy-pouzivane-v-krizovem-rizeni

ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022 [online]. 2022, [cit. 2023-09-04]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/