RADA PRO VEŘEJNÝ DOHLED
NAD AUDITEM

Podvody, kyberpodvody a jejich forenzní šetření

Dan Bican & Jiří Diepolt

Konference NKÚ

23. 9. 2021

RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

Obsah

RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

Podvody – „zbytečný“ crash kurz

Studie ACFE uvádí, že běžná organizace **v průměru** kvůli podvodům **přichází o 5 % svých ročních tržeb**

V případech podvodů vlastníků nebo top manažerů byl **medián ztráty 8,5 krát vyšší** než u podvodů spáchaných řadovými zaměstnanci

Malé společnosti přichází kvůli podvodům o téměř dvakrát více prostředků než velké korporace

Čím víc pachatelů bylo zapojených do firemního podvodu, **tím vyšší** byly způsobené **škody**

ACFE Report to the Nations 2018

Podvody – „zbytečný" crash kurz (pokr.)

ACFE:

- Podvod je definovaný jako lidská činnost, která je využívaná jednotlivcem či skupinou s cílem získat neoprávněnou finanční či nefinanční výhodu anebo její příslib na úkor jiného jednotlivce/skupiny uvedení nepravdivých skutečností, zatajením pravdy či hmotnou anebo nehmotnou manipulací. Ta zahrnuje neočekávané, klamavé, falešné a další podvodné jednání, kterým je oklamaná
- Podvod ve své podstatě zahrnuje každý úmyslný a připravený čin vykonaný se záměrem připravit někoho o majetek nebo peněžní prostředky uvedením v omyl nebo jiným pochybným způsobem.

§ **209 Zákona 40/2009 Sb. trestního zákoníku – Podvod:**

- *„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 (nejméně 5.000,- Kč), bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty."*

§ **216 TZ – Legalizace výnosů z trestné činnosti**

§ **220 TZ – Porušení povinnosti při správě cizího majetku**

§ **240 TZ – Zkrácení daně, poplatku a podobné povinné platby**

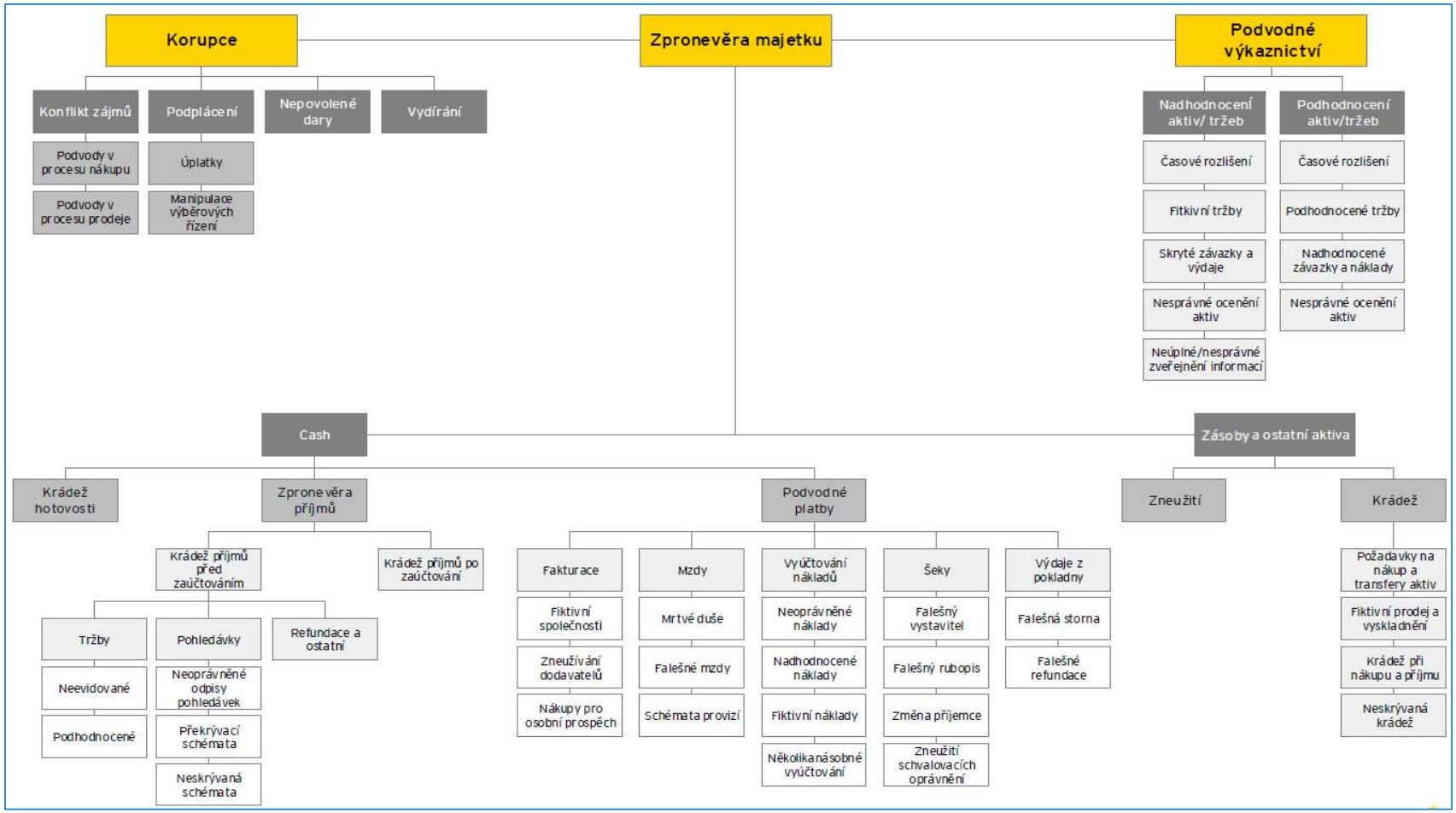
§ **254 TZ – Zkreslování údajů o stavu hospodaření a jmění**

§ **255 TZ – Zneužití informace a postavení v obchodním styku**

Činy uvedené v paragrafech výše jsou relevantní dle 418/2011 Sb. o trestní odpovědnosti právnických osob!

RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

Podvody – „zbytečný" crash kurz (pokr.)



Podvodná symbióza

MOTTO: Kybersvět akceleruje rychlost a úspěch byznysu, ale i podvodníků. Progresivně.

- Phishing a DDoS („distributed denial-of-service") jsou pouze špičkou ledovce
- Manipulace účetních a jiných obchodních výkazů pomocí účetních programů, Adobe atd.
- Social engineering / Whaleing (falešné faktury a konta, kontakt jménem CEO atd.)
- Zneužití výzvědných technik pro zjištění obchodního tajemství – také geopolitický problém

- *Phishing = (někdy převáděno do češtiny jako „rybaření") je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.)*

Aktuální případy - podvody

Commerzialbank Mattersburg, Rakousko

- Regionální banka v červenci 2020 ohlásila insolvenci v důsledku chybějících cca 680 mil. EUR z celkové bilanční sumy cca 800 mil. EUR (85%)
- Skandál malé rakouské banky medializován od července 2020, nicméně indikace zřejmé již nejméně od roku 2015
- Podstata:
  - Manipulace s cenou akcií
  - Lživé údaje na žádostech o úvěry fiktivním firmám (min 570)
  - Nadhodnocování cestovních a jiných nákladů
- Klíčové motivy:
  - Moc a prestiž (politika i bafuňářství), ovládání lidí
  - Peníze
- Zajímavé – velmi podobné českým bankám v 90. letech a kampeličkám donedávna, vč. afinity šéfa k fotbalu!

Aktuální případy - podvody (pokr.)

Wirecard, Německo

- Globální procesor online plateb pro Aldi, Lidl, Siemens atd.
- Ve 2018 byla třetí nejhodnotnější finanční skupinou Německa, měla politickou podporu a lesk
- V červnu 2020 byl zatčen majitel a CEO a po měsících spekulací potvrdilo, že na účtech německého „fintechového šampiona" chybí téměř 2 mld. EUR a má zmanipulované tržby a další klíčové finanční údaje.
- Podstata:
  - Manipulace s účetními údaji a jejich „odpovídající komunikace" investorům, auditorovi atp.
  - Vymyšlené fakturace služeb, nadhodnocené akvizice, praní špinavých peněz
  - Předkládané finanční výkazy prošly auditním procesem, BaFin i přijetím do DAX
- Klíčové motivy:
  - Moc a prestiž, ovládání lidí
  - Peníze
- Zajímavé
  - Již v lednu 2019 publikovaly FT výpověďmi podložená podezření, že vysoce postavený manažer firmy je podezřelý z falšování účtů, k čemuž měl použít padělané a antedatované smlouvy. Redaktory FT však dokonce začala vyšetřovat v Německu policie!
  - česká stopa: Jan Maršálek, dnes ukrývaný ruskými tajnými službami.

Aktuální případy – podvody (pokr.)

Podvody ve státní správě, ČR

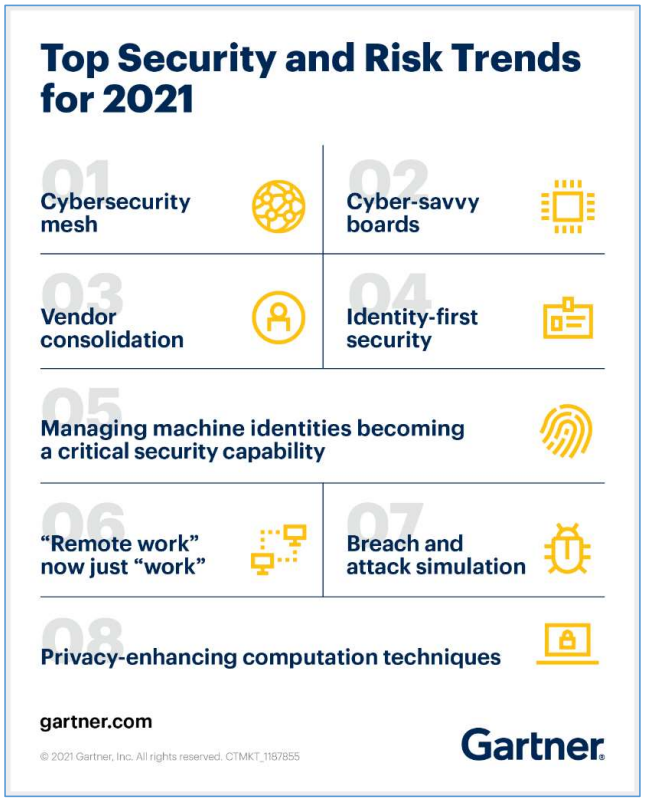
- Infrastrukturní
- Manipulace výběrových řízení
- Politicky motivované
- Metrostav, Kapsch, JCDecaux atd.

Další stovky významných podvodů ve světě každý rok

- Dieselgate – aktivní vytváření managementem
- NMC Health – aktivní podpora auditorem
- Tata Steel – falšování klíčovými zaměstnanci

Trendy v oblasti rizik a bezpečnosti

1) Zavedení bezpečnostních opatření v komplexním prostředí (např. privátní cloudy)
2) Nárůst významu role CISO ve společnosti
3) Konsolidace bezpečnostních nástrojů
4) Řízení identit prioritní
5) Správa identit zařízení (IOT)
6) Testování externích průniků
7) Práce z domova
8) Ochrana dat při užití



Trendy v oblasti rizik a bezpečnosti (pokr.)

Aktuální kurzy TOP kryptoměn

	Kryptoměna	Aktuální cena	Změna (24h)	Baserank rating™	Tržní kap.	Graf (7 dní)	
	Bitcoin (BTC)	$43 148	-3,7%	0	$815,2 mld.		Koupit!
	Ethereum (ETH)	$3 063	-2,7%	0	$359,9 mld.		Koupit!
	Tether (USDT)	$1	+0,13%	–	$69,77 mld.		Koupit!
	Cardano (ADA)	$2,14	-0,27%	0	$68,18 mld.		Koupit!
	Binance Coin (BNB)	$369,4	-3,3%	0	$57,14 mld.		Koupit!
	Ripple (XRP)	$0,95	-1,7%	0	$44,3 mld.		Koupit!
	Solana (SOL)	$143,3	+0,9%	0	$39,21 mld.		Koupit!
	Dogecoin (DOGE)	$0,21	-3,5%	0	$27,81 mld.		Koupit!
	USD Coin (USDC)	$1	-0,06%	–	$25,33 mld.		Koupit!
	Polkadot (DOT)	$29,19	-2,5%	0	$25,73 mld.		Koupit!
	Avalanche (AVAX)	$62,28	-3,1%	0	$13,72 mld.		Koupit!
	Uniswap (UNI)	$21,11	-4,4%	0	$12,38 mld.		Koupit!
	Terra (LUNA)	$28,83	-5,8%	0	$12,03 mld.		Koupit!
	Litecoin (LTC)	$159,7	-2,5%	0	$11,02 mld.		Koupit!

Kryptoměny přináší nové možnosti „investování", plateb za zboží a služby, a s tím i nové typy rizika zneužití.

Aktuální případy – nejznámější kyberpodvody

Zneužití přístupových oprávnění - Microsoft

Od roku 2016 do roku 2018 se softwarovému inženýrovi společnosti Microsoft podařilo podvést společnost o více než 10 milionů dolarů. **Útočník byl členem testovacího týmu** Microsoftu, který pracoval na řešeních elektronického obchodování, a dokázal vytvořit fiktivní účty v obchodě, aby simuloval nákupy zákazníků (digitální dárkové karty).

Prevence: speciální režim privilegovaných účtů, zabezpečení informaci a dat dle hodnoty.

Útoky zaměstnanců třetích stran – Jet2

Subdodavatelé mají často stejná přístupová práva jako interní uživatelé. V roce 2018 bývalý subdodavatel nelegálně získal přístup k doménám Dart Group PLC a její dceřiné společnosti Jet2, jedné z největších leteckých společností ve Velké Británii. Pomocí účtu služby tiskárny na interní síťové doméně Jet2 zahájil útočník relaci vzdálené plochy a přistoupil ke složce souborů s pověřeními zaměstnance letecké společnosti. Muž odstranil všechna data z napadené složky, čímž znemožnil více než 2 000 lidem přístup k jejich online účtům a firemní e-mailové službě.

Prevence: omezení přístupových práv subdodavatelům, pravidelná revize přístupových práv.

Aktuální případy – nejznámější kyberpodvody (pokr.)

Phishing – Twitter

V polovině července 2020 došlo na Twitteru k masivnímu útoku typu phishing. Kybernetičtí zločinci kompromitovali administrátorský panel sociální sítě, získali kontrolu nad účty známých uživatelů Twitteru, soukromých i firemních, a jejich jménem zinscenovali zaslání falešného dárku ve formě bitcoinové platby.

Podle Zprávy o vyšetřování narušení dat společnosti Verizon 2021 přibližně **80% incidentů** souvisejících se sociálním inženýrstvím je **způsobeno phishingem.**

Prevence: školení, reálné testování uživatelských znalostí.

Krádež dat interním zaměstnancem – Shopify

Dva zaměstnanci Shopify dostali zaplaceno za krádež záznamů o transakcích téměř 200 online obchodníků.

Prevence: omezení uživatelských práv, zrychlení/zautomatizování procesů řízení bezpečnostních incidentů.

Aktuální případy – nejznámější kyberpodvody (pokr.)

This is just a small section of what sensitive information lies on the servers, unfortunately, since we had to dump manually we didn't dump everything,
to get the full dump simply log into http://www.gfmc.foxconn.com with admin as the username and password1 as the password, then go here http://www.gfmc.foxconn.com/webpage/APOnlineVendor_s.asp and search for the company you want. You can then go back to login and get some sensitive information as we posted directly below.

VendorGroup: Vendor Code: 2502
Vendor Name: MISSION HILLS CHINA LTD Address: 中國深圳市觀瀾鎮高爾夫大道
Country: RGC ContactPerson:
TelephoneNo: 802-2931-1326 VendorAccNo: 01287510962295
Beneficiary: Bank: BANK OF CHINA (HONG KONG) LIMITED
PostalCode: MailAddress:
PaymentKey: M0102 PaymentName:

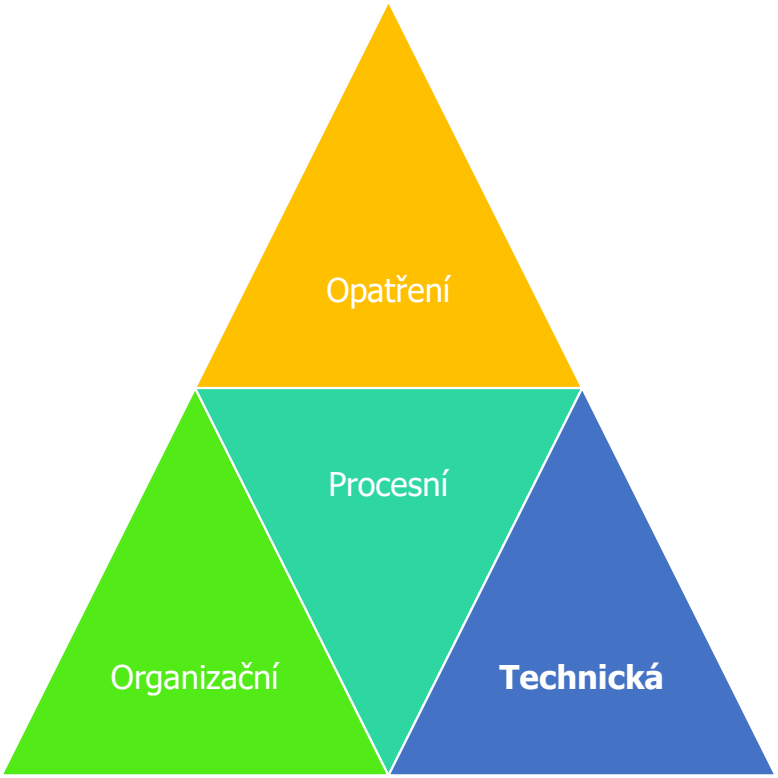
FirstName: Terry
LastName: Gou
ShortName: terrygou
HTTPPassword: (GEd/mzYRx4Q98Z6wpQ47)

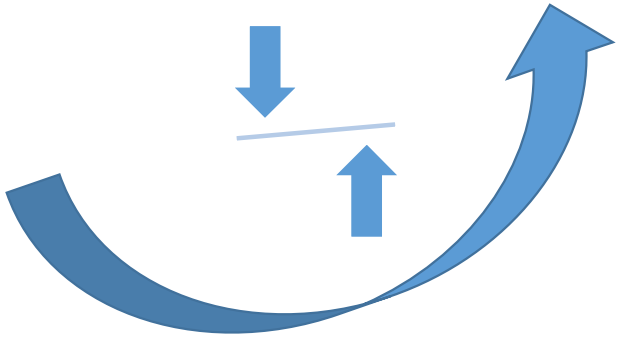
[http://x/.../$defaultview/01738F812EBC6F45BBE98FC024D560DD]

NO.	User ID	User Name	Password	Vendor Code	Company Name	User Ty
1	APPLE	APPLE COMPUTER INC.	foxconn2	APPLE		Vendor

Swagg Security
@SwaggSec
Swagg Security® (SwaggSec), Hacking Today for an Entertaining Tomorrow.

Ochrana informací & dat
Prevence vs detekce





Společné příznaky a hybatele

Nové technologie a online prostředí
- Real-time access & handling (online půjčky)
- Nové aplikace, programy, prostředí (Revolut)
- Laxnost, nevědomost, ignorace faktů (Theranos, Nikola, …)

GDPR
- Od května 2018 klíčová regulatorika pro ochranu osobních údajů EU
- Propojuje boj s podvody v IT prostředí

FSI regulatorika
- Pro finanční sektor vzhledem k podvodům zřejmě nejrozsáhlejší
- Komplexní a komplikovaná
- Pro organizace v sektoru velmi náročné a nákladné postihnout vše v různých oblastech (hospodářské) kriminality
- Často zdrojově poddimenzované zároveň čelící skvěle organizovaným mezinárodním strukturám

Ostatní
- Obchodní tajemství / konkurenční prostředí
- Home-office

Paradoxy
- Napadají vás zásadní paradoxy hospodářské kriminality v dnešním světě?

RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

Role Risk managementu, IA a Externího auditu

Risk management	Interní audit	Externí audit
• Preventivní i reaktivní • Systematický • Komplexní • Systémový	• Preventivní i reaktivní • Systematický • Výběrový	• Reaktivní • Systematický • Výběrový

KLÍČOVÝ PARAMETR PREVENCE: „TONE-AT-THE-TOP" !

RADA PRO VEŘEJNÝ DOHLED
NAD AUDITEM

Dotazy

RADA PRO VEŘEJNÝ DOHLED NAD AUDITEM

Kontakty

Dan Bican

DABRICON s.r.o.
dab@dabricon.com
737 235 534

Jiří Diepolt

RVDA
jiri.diepolt@rvda.cz
724 244 073