Hewlett Packard Enterprise

Zvyšování kybernetické odolnosti:

Neopakujte v kybernetické bezpečnosti chyby druhých

Martin Zich

CISSP, CCSP, C|CISO assoc.

Duben 2024

O mně

- HPE Services Worldwide – konzultant kybernetické bezpečnosti

- CISSP, CCSP, CCISO assoc., CEHv10 exp.
- 15+ let v kybernetické bezpečnosti

- Pracuji v organizacích po celém světě včetně Středního východu, USA, Evropy a dalších.

- Kybernetickou bezpečnost jsem konzultoval a konzultuji ve společnostech, které těží suroviny, rafinerie, nemocnicích, bankách, pojišťovnách, mobilních operátorech, prodejních řetězcích, atd.

Hewlett Packard Enterprise

Kybernetický útok

Není otázkou „jestli“, ale „kdy“

Aktuální výzvy

ZVĚTŠOVÁNÍ „ATTACK SURFACE“

BALANCOVÁNÍ BEZPEČNOSTI A RYCHLOSTI

ÚTOKY JSOU STÁLE SOFISTIKOVANĚJŠÍ

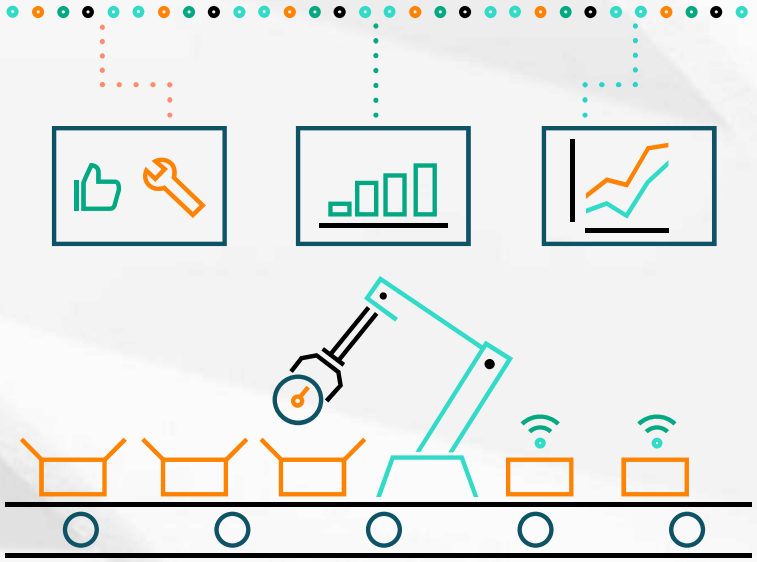
CENA ZA OPATŘENÍ A KOMPLEXITA PROSTŘEDÍ

NEDOSTATEK EXPERTŮ

ZABEZPEČENÍ DAT, KTERÁ JSOU ÚPLNĚ VŠUDE

Kybernetická odolnost

Schopnost včas detekovat a „ustát“ kybernetický útok
(třeba i za cenu dočasné degradace poskytovaných služeb)



Chyby, které nechcete opakovat: příčina vs. následek

Kybernetická odolnost

Jak vypadá špatná praxe…

Core-banking databáze přímo spojená s Internetem

„Jumpboxy“/“bastiony“, které lze jednoduše obejít

Blacklisting veřejného cloudu („self DoS“)

Domácí sklep (CEO) jako sekundární úložiště pro zálohy (nešifrované)

Přístup k zálohám po ověření z centrálního AD bez PAM

Nešifrované a úhledně popsané zálohovací pásky čekající vedle recepce na vyzvednutí...

Admin nastavující infrastrukturu „napřímo“ přes VPN ze svého domácího počítače

Univerzální root heslo…umožňující jakékoliv změny

Spojení výrobníky linky s IT infrastrukturou a Internetem bez jakéhokoliv systematického oddělení

„Hardcoding“ hesel do skriptů a „yamlů“ … a jejich nahrání do veřejného „gitu“

Digitalizace DR plánů…před útokem ransomwaru

Root přístup spravovaným jedním člověkem v jeho „KeePass“

Spolupráce s třetí stranou, která si najímá další subdodavatele a Ti spolupracují s externisty.... a... Ti pracují na napadených počítačích v kavárně

Potřeba emailové komunikace při napadení ransomwarem

Windows XP na POS spojených s Internetem

Jak vypadá špatná praxe…

Ve většině případů jde jen o důsledky... kde hledat příčiny?

Top 10 příčin, na které pravidelně narážíme

Opakující se příklady špatné praxe, která způsobuje značný negativní dopad

#1: Kybernetická bezpečnost jako „black box“ (změť technologií)

- Chápána jako nestrukturovaný problém řešený v reaktivním módu:
  - Náhodná implementace opatření ve snaze zabezpečit „vše potřebné“
  - Není jasné kde kybernetická bezpečnost v organizaci „začíná a končí“
  - Neschopnost strukturovat daný problém vede jistě k zanedbání priorit
  - Neschopnost odhlédnutí od technologií k systematickému řešení problému (získání návyků, které nenastavuje provoz)

Ukázka: Dáváme kybernetické bezpečnosti strukturu

0. Cybersecurity Governance
1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. **Data Recovery**
12. Network Infrastructure Management
13. **Network Monitoring and Defense**
14. Security Awareness and Skills Training

...

atd.

LIDÉ

POLITIKY

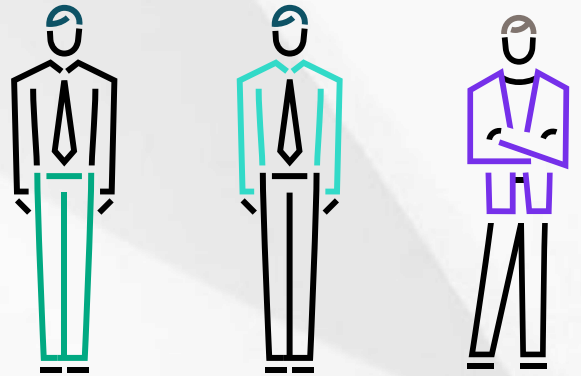
PROCESY

TECHNOLOGIE

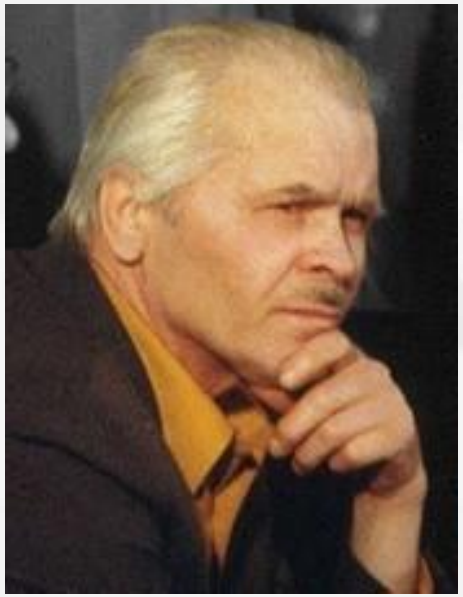
METRIKY

#2: (Ne)systém řízení kybernetické bezpečnosti

- Chybějící zdravá rovnocenná spolupráce IT & IT bezpečnosti (pomáhá!) > nejde o podřízenost (ideálně C-level prezence)
- Opatření kybernetické bezpečnosti nastavované technickým provozem
- Chybějící celkový koncept řízení – „shora-dolů“ ve spolupráci se „zdola-nahoru“
- Pohled na politiky a standardy jako na hromadu zbytečných papírů, které leží ve své neaktuální verzi na filesharech jako „potrava“ pro auditory



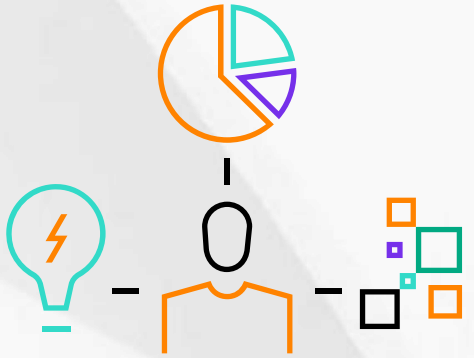
#3: Absence i základní práce s rizikem („risk culture“)



Ilustrace:
https://en.wikipedia.org/wiki/Anatoly_Dyatlov

#3: Absence i základní práce s rizikem v IT

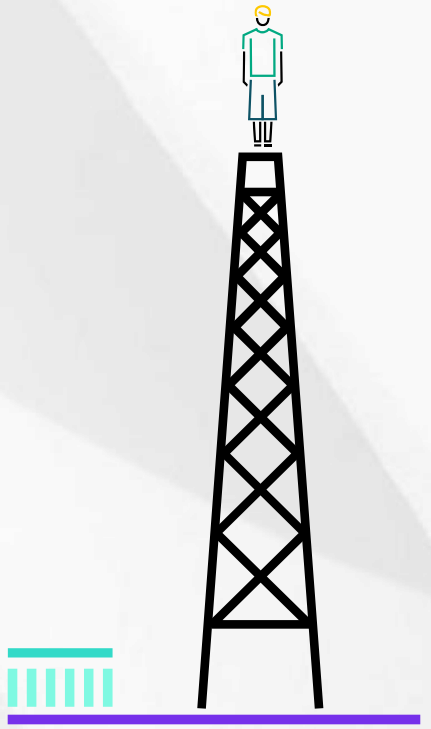
- Často na spodku seznamu priorit (nebo mimo seznam)
- Základní stavební kámen – povědomí (budování „risk culture“)
- Neschopnost uchopit základní pojmy – např. „risk appetite, risk tolerance“
  - Umění zjednodušit si život
  - Definice vlastních hranic a způsobů jak je dosáhnout v praxi
- Zdůvodnění („proč?“): nalezení formálního důvodu k nasazení opatření
- Nasazení nových technologií a změn, které „nepřiléhají“ (neřeší daný problém)



RIZIKO = HROZBA * ZRANITELNOST

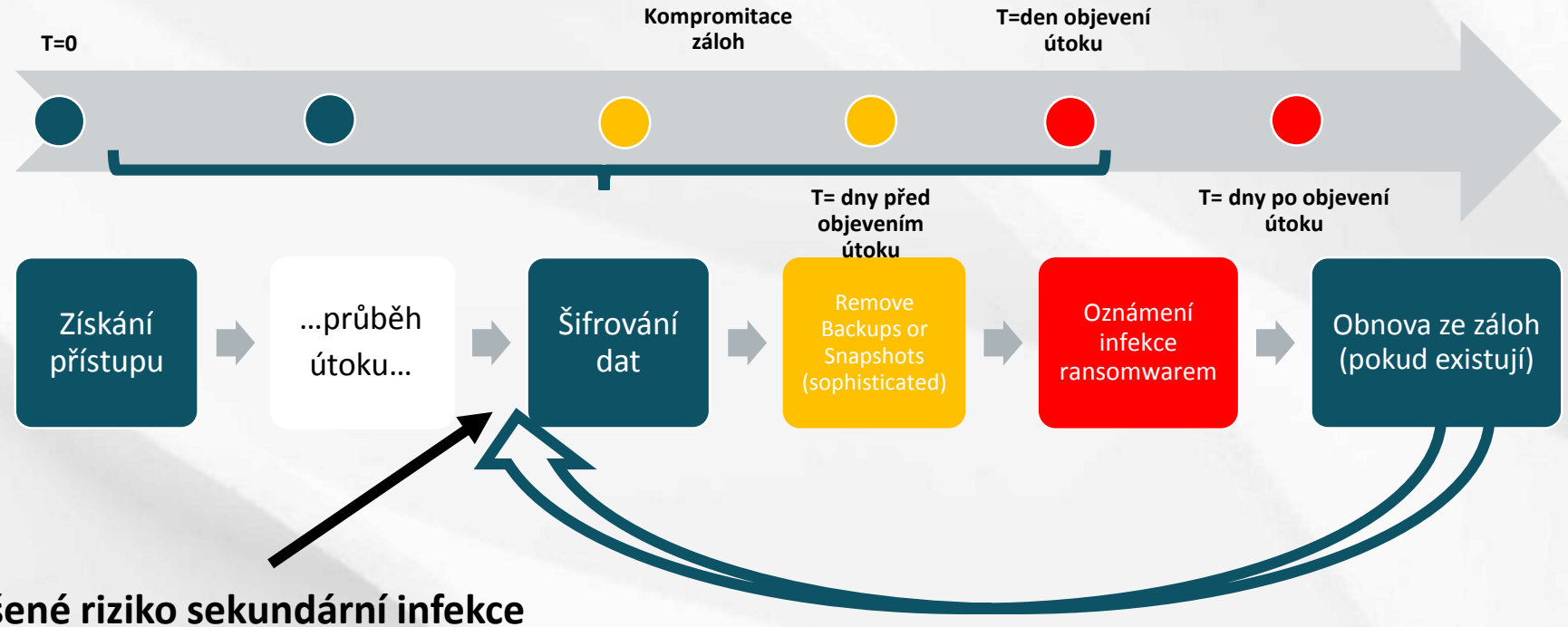
#4: Zálohování jako ultimátní ochrana před kybernetický útokem

- **Modelová situace:** „bungee jumping“
- **Zálohy:** voda pod věží, ze které se skáče
- **Kybernetická odolnost:** lano, které zadrží padajícího člověka



Stále vysvětlujeme, kde Vás zálohy už nezachrání

- Podobný útok může probíhat minuty / dny / měsíce / roky…



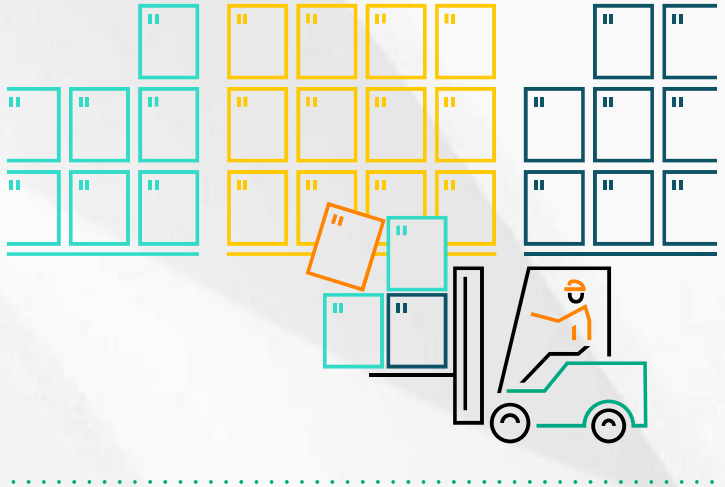
Zvýšené riziko sekundární infekce

RTP – Recovery Time Objective = za jak dlouho obnovím normální fungování

RPO – Recovery Point Objective = o kolik dat potenciálně přijdu!

#5: Nepořádek v „assetech“ a jejich stavu

- Neschopnost říci co a kde provozujeme
- Co je kritičtější než to ostatní?
- Chybí zcela vitální podklad pro bezpečnost i vše ostatní
  - Sledování stáří, typu, stavu, compliance, atd.
- Dle našich subjektivních zjištění 9 z 10 organizací toto nemá v pořádku

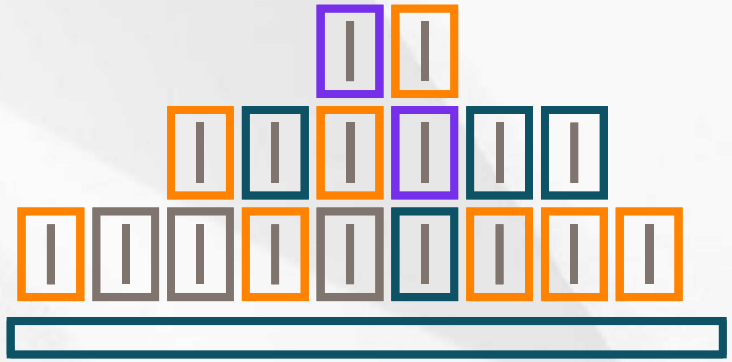


#6: Chaotická reakce na incidenty

- Málokdo se připravuje – „kdo je připraven, není překvapen“
  - „Tabletopy“ jako minimum
- Chybějící příprava scénářů – detailní „runbooks“ a to včetně technických i komunikačních
  - Pamatujete na „Covid-19“ a volání po krizových scénářích?
- Schopnost incidenty odlišit a prioritizovat – kdo např. rozhodne, že jde o „disaster“
- Vymýšlení věci za běhu jako „cesta do pekel“ – kdo se sejde, kde se sejde, co budeme dělat, jak budeme komunikovat

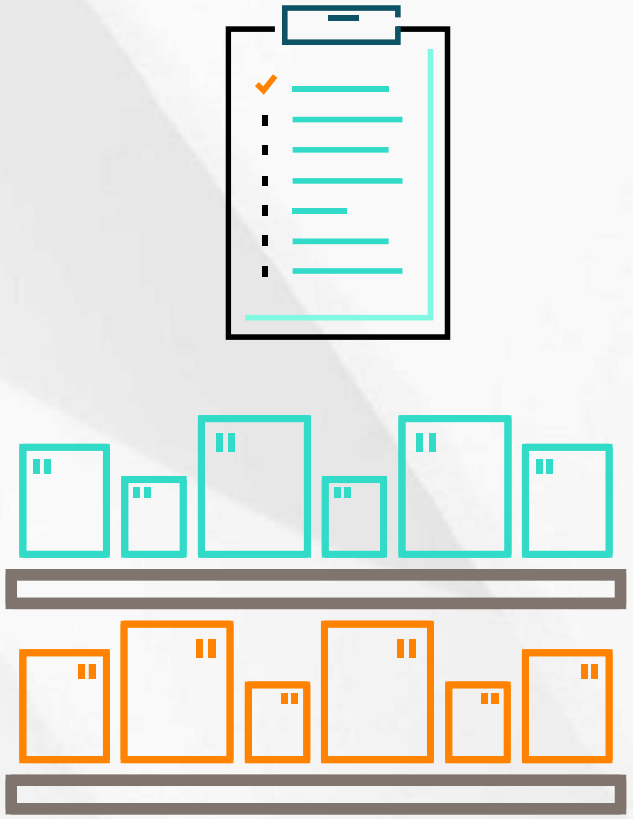
#7: Odpor k dokumentaci a vůbec formálnímu „vybavení“ řízení bezpečnosti

- Pokud absentuje řízení, vždy nakonec vyhrává přirozený odpor k dokumentování
- Fatální potřeba „reverse engineeringu“ – často nemožný vedoucí na značný počet zranitelností, což se v čase dále zhoršuje
- Chybějící standardy umožní jednotlivcům zvyšovat riziko napadení s fatálními dopady



#8: Přeceňování/desinterpretace výsledků auditu

- Auditor chápe audit jako srovnání – „papír“ vs. realita
  - Assessment vs. audit
- Interní audit nám dopadl dobře – “soulad s neexistujícími nebo standardy v katastrofálním stavu je zajištěn…”
- Audit souladu s normou, která nestanovuje „baseline“ je také „ok“
- Audit nás prověřil, tedy prověřil to, co mu pracovníci řekli jako jejich popis reality (otázka / odpověď)
- Framework, který nenastavuje „baseline“ máme implementovaný

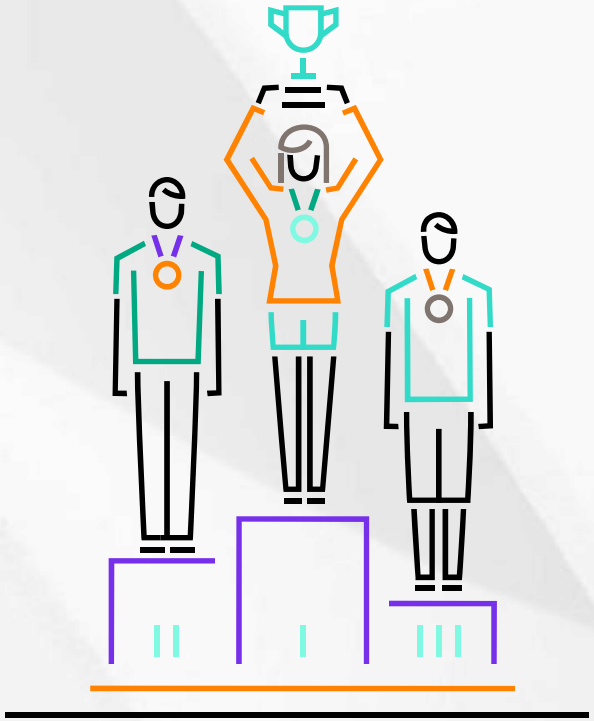


#9: Neuřízené změny (nasazení nových technologií) a výjimky

- Dočasná nastavení jako „dar z nebes“ pro útočníka – absentující řízení změn a výjimek
- Nekompatibility a změny vytvářející nerozpoznané riziko
  - „Change Review Board“ – je to dobrý nápad?
- Neformálně implementované výjimky pro vysoký management a další
- Živelné adopce cloudových řešení (zvýrazněno během „covidové“ krize)
- Živelná adopce AI – data unikají do učících se modelů jako na běžícím pásu
- Zapnutí AI v nástrojích ochrany „bez rozmyslu“
- Připojení OT a IIOT k IT – je opravdu potřeba speciální přístup?

#10: Chybějící expertíza

- Tohle je samozřejmě to nejtěžší
- Chybějící kompetence, kompetence, kompetence
- Často se budují systémy závislé na konkrétních lidech, nikoliv rolích
- Governance je také „řemeslo“ a je třeba ho zdokonalovat (ne nechat „zemřít“)



Cesta k pevným základům kybernetické bezpečnosti – HPE Services

Rychlý úvod a základní kontrola

- Workshop s vysvětlením problému ransomware a obraně proti němu
- Kontrola hlavních kritických indikátorů

Možné navazující aktivity

- HPE Rapid Cybersecurity Assessment
- Storage and Backup Security Assessment
- Obecně: Konzultace k nasazení nebo zdokonalení konkrétních opatření (vč. technologií)

Další – ve speciální situaci

- Table-Top: reakce na incident
- Forenzní analýza kybernetického útoku

Děkuji.

martin.zich@hpe.com