Hewlett Packard Enterprise

Kybernetická odolnost – jak špatný bývá stávající stav a co s tím?

HPE

Mikulov 2024

Představení

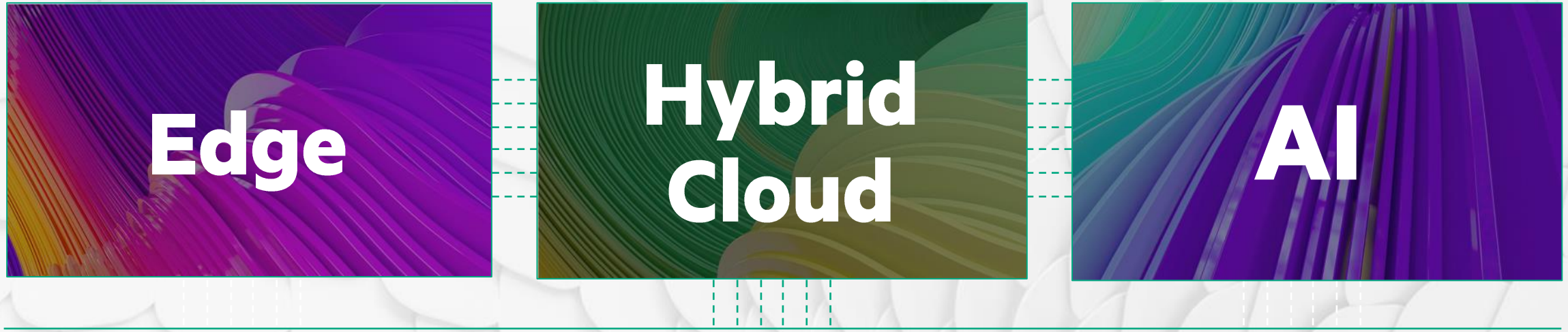
Martin Zich CISSP, CCSP, CCISO assoc.

Konzultant kybernetické bezpečnosti

Michal Svoboda HPE aruba networking

Country manažer české části divize HPE Aruba

HPE GreenLake



Data | Sustainability | Security

Security: Odolnost před kybernetickými hrozbami

Chyby, které nechcete opakovat

Provozovaná prostředí stále nebývají v dobrém stavu...

Administrátoři spravují systémy z domácích počítačů „napřímo“ přes VPN.

„Plochá“ sítě bez jakékoliv segmentace.

Analýza rizik... bohužel ji nemáme.

„Core- databáze“ je přístupná z Internetu.

Hesla jsou v některých předpisech kontejnerů, které se synchronizují do GitHub.

Windows XP na POS systémech spojených do internetu.

IT systémy si každý provozní tým řídí a ochraňuje sám...

Nemáme žádné napsané standardy bezpečnosti ani IT.

„Root“ oprávnění má pouze jeden člověk.

Máme jednofaktorové přihlášení.... včetně administrátorů.

DR plány jsme digitalizovali ... pak přišel ransomware.

Do prostředí se připojují třetí strany. Jejich seznam ani úroveň jejich bezpečnosti neznáme.

Útočníci umí takových chyb trpělivě využít

Kybernetický útok

Kybernetický útok

Útočník napadne koncovou stanici a pohybuje se po síti.

Dostupné IT v cloudu (IaaS, PaaS, SaaS)?

Internet/privátní linka

Neexistující segmentace

Malware se snaží šířit

Koncová stanice

Bezpečnostní zóny se neřeší

Servery

Doménový Řadič

Enterprise administrátor

Žádná detekce neobvyklé aktivity

Bolestivý úder

Specializované části malwaru napadají v podstatě vše. Zálohy nevyjímaje…

Doménový Řadič

Enterprise administrátor

Online ZÁLOHY…“ouch“

Koncové stanice

Produkční systémy

Třetí strany…

Internet

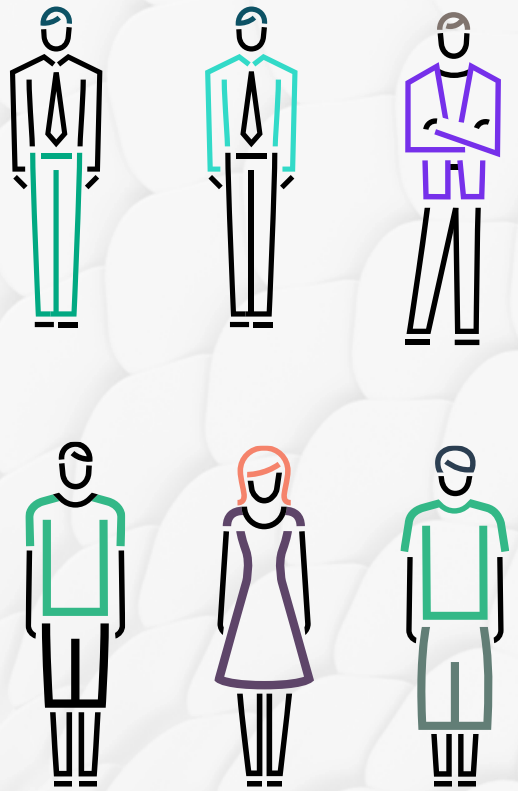
Dostupné IT v cloudu (IaaS, PaaS, SaaS)?

10 nejčastějších chyb

Jak je řešit

#1: Chybějící nebo neúplný systém řízení kybernetické bezpečnosti

- Implementace opatření bez celkové koncepce
- Není jasné kde bezpečnost v organizaci „začíná a končí“
- Buduje se „zdola-nahoru“ bez spolupráce s „shoda-dolů“



Pomáháme dát kybernetické bezpečnosti strukturu

Hewlett Packard Enterprise

HPE Services

Rapid Cybersecurity Assessment

Např.:

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: Absence kvalitní práce s rizikem v IT

- Často na konci seznamu priorit
- Neschopnost uchopit základní pojmy jako „risk appetite“ nebo „risk tolerance“
- Riziko zřídka formálním důvodu k nasazení bezpečnostního opatření

NIS2 DORA Digital Operational Resilience Act ...

Nový zákon o kybernetické bezpečnosti – poskytovatel regulované služby má v režimu **vyšších povinností:** vyhodnocení rizik, zavedení opatření ke snížení rizika.

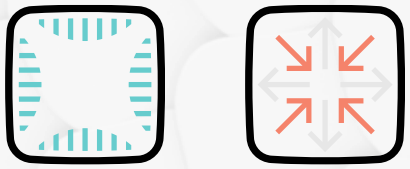
DORA – mezi povinnosti patří řízení rizik, nebo povinnost vrcholového vedení stanovit úrovně tolerance rizik.

#3: Slabá segmentace síťové infrastruktury

- Plochá topologie bez bezpečnostního rozlišení zón, neznámá telemetrie
- Snadnější šíření kybernetického útoku

- **Řešení:**
  - HPE má konzultanty pro analýzu a návrh konkrétního řešení
    - Porozumíme aplikačním tokům, nasadíme řízení, vytvoříme pravidla
  - Mnohdy není potřeba rekonfigurovat síť nebo měnit síťové nastavení
    - Konfigurace realizovaná na switchi

#4: Stále vidíme tradiční VPNky (i na místech k tomu nevhodných)



- Nevhodné pro hybridní model práce
- „Úzké hrdlo“, které navíc může zvýšit riziko kybernetického útoku

HPE aruba networking

- **SSE (Security Service Edge):**
  - Tradiční VPN připojení vzdálených uživatelů zaznamenává příklady zneužití
  - Po Covidu existuje masivní počet uživatelů s hybridním modelem práce
  - Je třeba zajistit stejný stupeň ochrany uživatelů pracujících „odkudkoliv“

#5: Podceněná ochrana privilegovaných identit

- Lokální nebo o Active Directory „opřené “ privilegované účty
- Absence více-faktorové autentizace
- Snadnější šíření kybernetického útoku

- **Řešení:**
  - Implementace „Privileged Access Management“ (PAM)
  - Monitoring přístupů, rotace hesel, silnější autentizace, atd.)

Hewlett Packard Enterprise

HPE Services

Implementační projekty na různá technická i netechnická témata.

#6: Zálohování jako jediné řešení dopadu kybernetického útoku

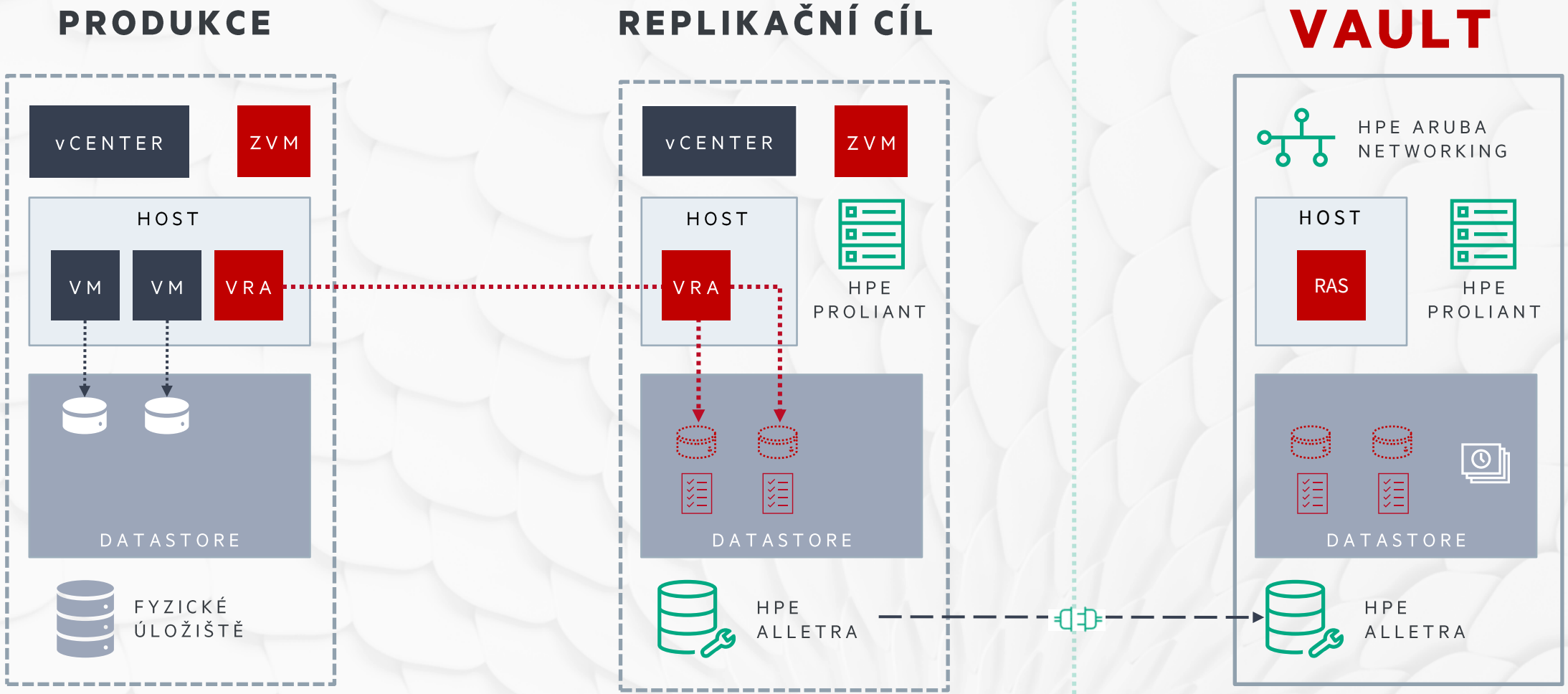
Program pro kybernetickou bezpečnost (odolnost)

Illustrations: Pixabay – free Commercial use

Zálohy (“záchranná síť”)

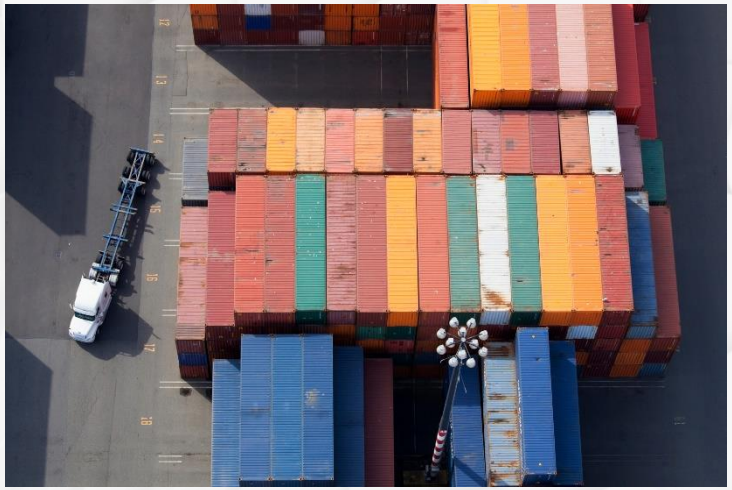
Zálohy by měly být odolné – koncept „Cyber-vault“

Zerto
a Hewlett Packard Enterprise company



#7: Nepořádek v „assetech“ a jejich stavu

- Chybí jednoduchá orientace v tom co je provozováno
- Kritické prostředky nejdou identifikovány
- V důsledku schází vitální podklad nejen pro proces zabezpečování



#8: Nepřipravená reakce na incidenty

- Málokdo se připravuje – „kdo je připraven, není překvapen“
- Chybějící příprava scénářů včetně technických i komunikačních
  - Pamatujete na „Covid-19“ a volání po krizových scénářích?
  - Vymýšlení za běhu je „cesta do pekel“
- Schopnost incidenty odlišit a prioritizovat
  - kdo např. rozhodne, že jde o „disaster“
- **Řešení:**
  - Simulace kybernetického incidentu (např. útok ransomwaru)
  - Navazující příprava

Hewlett Packard Enterprise

HPE Services

Table-Top: Simulace kybernetického incidentu

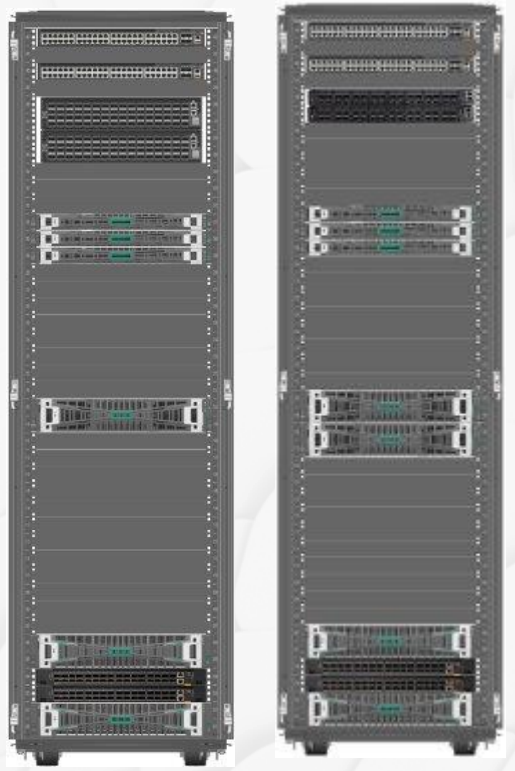
#9: Výběr nových technologií – např. platformy pro AI

- **Příklad: Nasazení AI řešení**
  - Důvěra
  - Suverenita dat – „můžeme opravdu svá data nahrát do veřejného cloudu?“

- **Řešení – AI platforma „on-premise“**
  - HPE for Private Cloud AI (PCAI) – nová platforma pro AI ve spolupráci s NVIDIA
  - Další řešení platforem pro AI od HPE – Ezmeral Unified Analytics, MLDE, MLDM, atd.

  - **Je možné vybrat tu vhodnou pro Vaši situaci, Váš plán pro AI**

NVIDIA AI Computing by HPE

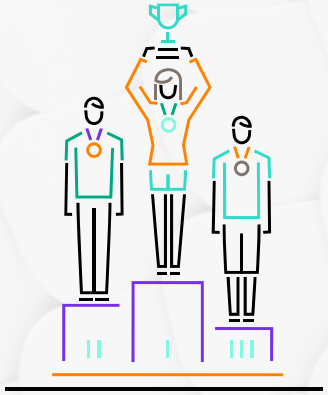


NVIDIA. Hewlett Packard Enterprise

#10: Chybějící expertíza

- Chybějící kompetence
- Neúplné a nesystematické vzdělávací plány
- Standardizované požadavky na kvalifikace/certifikace pro různé části IT

- **Řešení:**
  - Spolupráce s externími kvalifikovanými konzultanty
  - Poptávka technického a dalšího vzdělávání



Hewlett Packard Enterprise

HPE Education

Např.:

- ITSM
- DevSecOps
- AI
- FinOps

HPE – kam nás zařadit?

Hewlett Packard Enterprise

HPE GreenLake

IaaS, PaaS, SaaS

Bezpečný privátní flexibilní cloud provozovaný u Vás

HPE aruba networking

Síťové technologie k budování bezpečných hybridních prostředí

HPE Serverový a Storage HW

Konzultační služby na míru – řešící konkrétní „problém

Konzultační služby pro kybernetickou bezpečnost

Děkujeme za pozornost.

michal.svoboda@hpe.com
martin.zich@hpe.com