# Kyberneticky odolné IT v různé fázi transformace do cloudu

Michal Svoboda
Martin Zich

eGovernment, Mikulov 2023

# Kdo jsme? – nadšenci do IT technologií, jejich organizace a také bezpečnosti

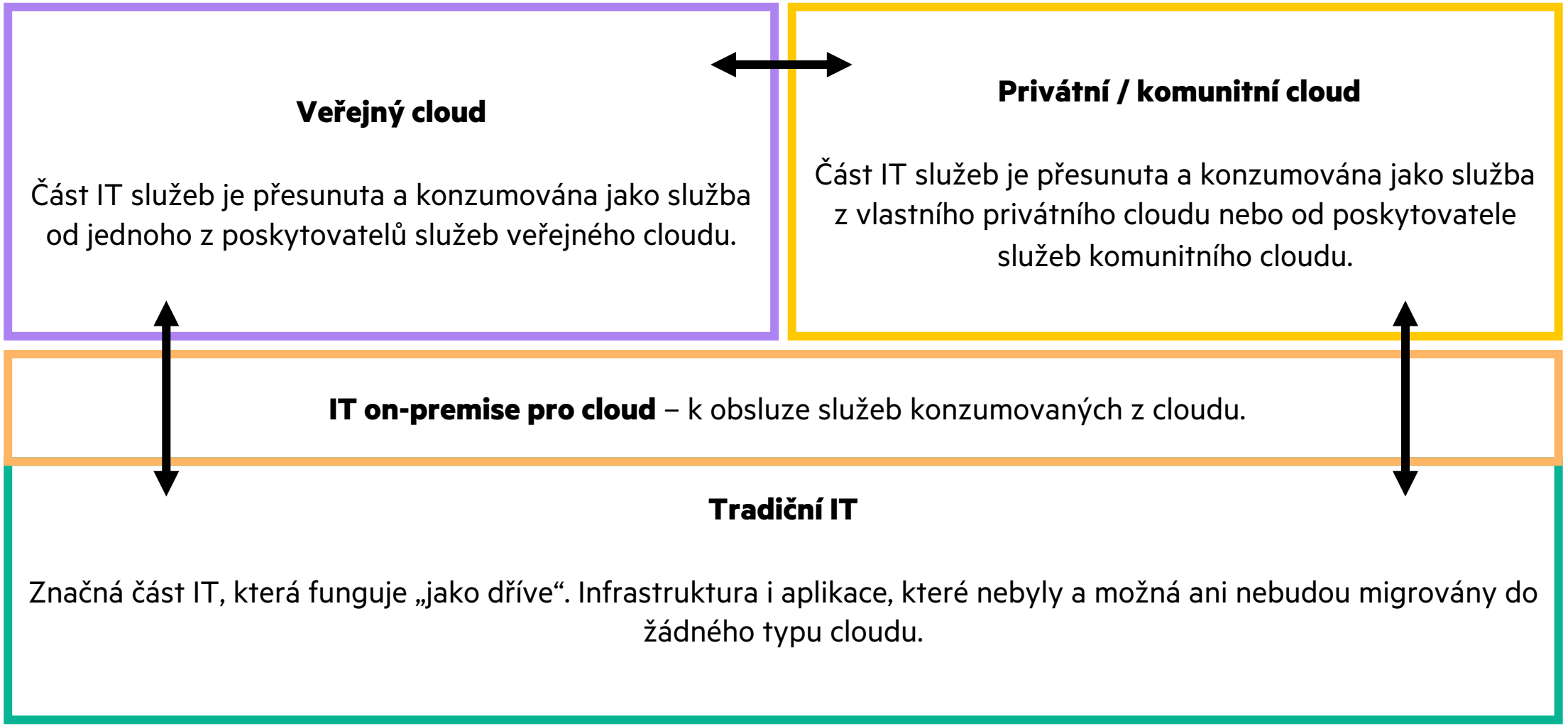
## Martin Zich

CISSP, CCSP, CEH
15 let na trhu konzultací kybernetické bezpečnosti
v největších projektech, které HPE celosvětové dodává v
USA, na Blízkém východě, Evropě, atd.

## Michal Svoboda

Country manažer české části divize HPE Aruba.
Vedoucí konzultantů dodávajících bezpečné síťové
technologie množství zákazníků v ČR.

# Transformace do cloudu – příklad „běžné“ skladby IT



# Transformace do cloudu – příklad zastoupení jednotlivých částí

**20%**

**Veřejný cloud**

Část IT služeb je přesunuta a konzumována jako služba od jednoho z poskytovatelů služeb veřejného cloudu.

**5%**

**Privátní / komunitní cloud**

Část IT služeb je přesunuta a konzumována jako služba z vlastního privátního cloudu nebo od poskytovatele služeb komunitního cloudu.

**10%**

**IT on-premise pro cloud** – k obsluze služeb konzumovaných z cloudu.

**65%**

**Tradiční IT**

Značná část IT, která funguje „jako dříve“. Infrastruktura i aplikace, které nebyly a možná ani nebudou migrovány do žádného typu cloudu.

# Privátní cloud – např. HPE GreenLake

**Veřejný cloud**

Část IT služeb je přesunuta a konzumována jako služba od jednoho z poskytovatelů služeb veřejného cloudu.

HPE GreenLake

**Privátní / komunitní cloud**

Část IT služeb je přesunuta a konzumována jako služba z vlastního privátního cloudu nebo od poskytovatele služeb komunitního cloudu.

IT on-premise pro cloud – k obsluze služeb konzumovaných z cloudu.

**Tradiční IT**

Značná část IT, která funguje „jako dříve“. Infrastruktura i aplikace, které nebyly a možná ani nebudou migrovány do žádného typu cloudu.

# IT „on-premise“

**Veřejný cloud**

Část IT služeb je přesunuta a konzumovaná jako služba od jednoho z poskytovatelů služeb veřejného cloudu.

**Privátní / komunitní cloud**

Část IT služeb je přesunuta a konzumovaná jako služba z vlastního privátního cloudu nebo od poskytovatele služeb komunitního cloudu.

**IT on-premise pro cloud** – k obsluze služeb konzumovaných z cloudu.

**Tradiční IT**

Značná část IT, která funguje „jako dříve“. Infrastruktura i aplikace, které nebyly a možná ani nebudou migrovány do žádného typu cloudu.

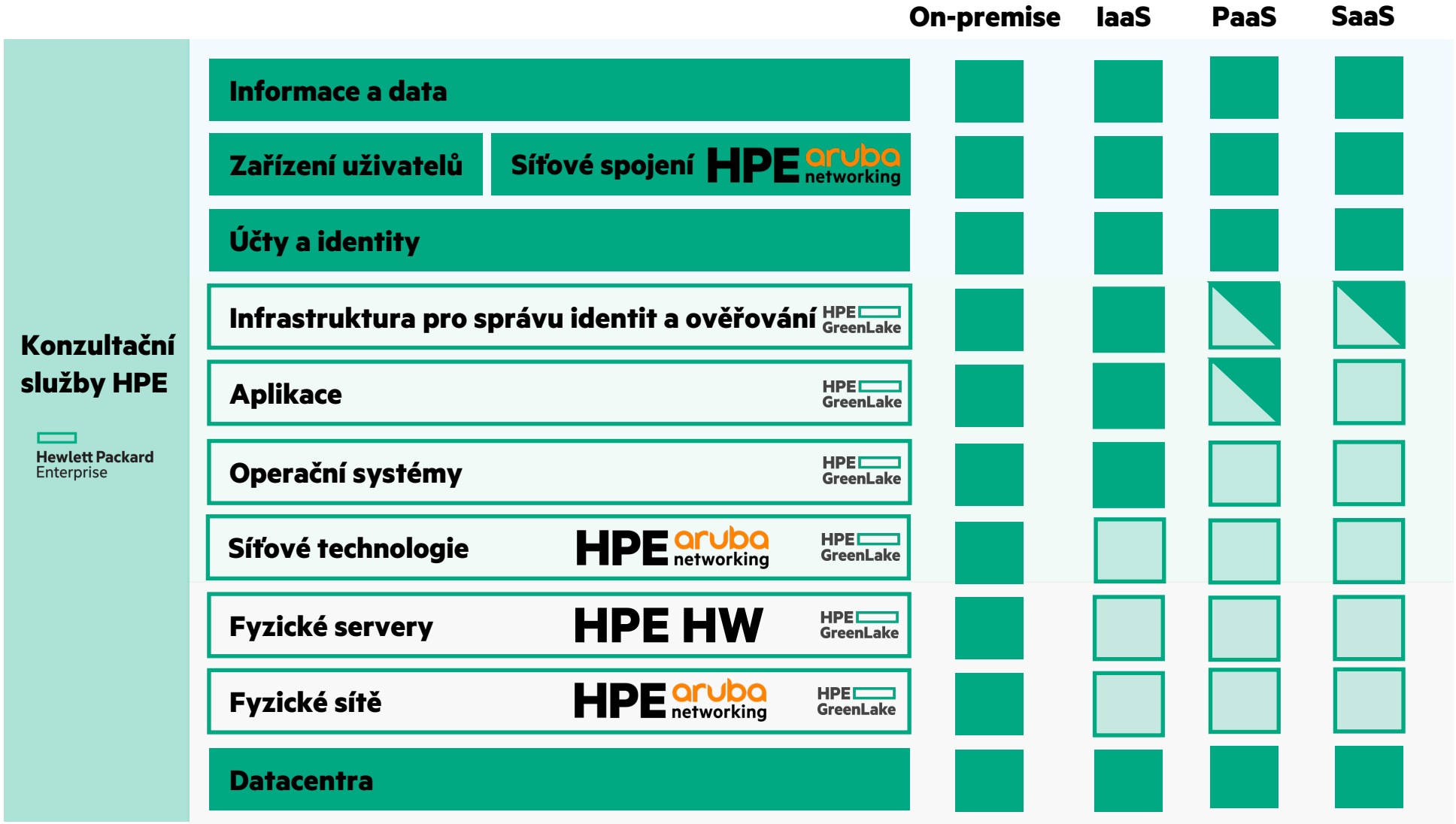
# Pizza as a Service Example

| | Traditional On-Premises (Legacy) | Infrastructure as a Service (IaaS) | Containers as a Service (CaaS) | Platform as a Service (PaaS) | Function as a Service (FaaS) | Software as a Service (SaaS) |
|---|---|---|---|---|---|---|
| Configuration | Conversation | Conversation | Conversation | Conversation | Conversation | Conversation |
| Functions | Friends | Friends | Friends | Friends | Friends | Friends |
| Scaling | Drink | Drink | Drink | Drink | Drink | Drink |
| Runtime | Pizza | Pizza | Pizza | Pizza | Pizza | Pizza |
| OS | Fire | Fire | Fire | Fire | Fire | Fire |
| Virtualisation | Oven | Oven | Oven | Oven | Oven | Oven |
| Hardware | Electric / Gas | Electric / Gas | Electric / Gas | Electric / Gas | Electric / Gas | Electric / Gas |
| | Homemade | Communal Kitchen | Bring Your Own | Takeaway | Restaurant | Party |

You Manage

Vendor Manages

# „Shared responsibility model“ – privátní cloud




HPE GreenLake

**Private Cloud Enterprise**

- bare metal
- virtuální stroj
- kontejner

**jako služba**

Řídíte a staráte se Vy

Řídí a stará se poskytovatel

# „IT on-premise pro cloud“ i tradiční IT nebývá v dobrém stavu… ukázka reality

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

„Plochá“ sítě bez jakékoliv segmentace.

Analýza rizik… aha, to nemáme.

„Core-banking“ databáze je přístupná z Internetu.

Hesla jsou v některých skriptech, které se synchronizují do GitHub.

Windows XP na POS systémech spojených do internetu.

IT systémy si každý provozní tým řídí a ochraňuje sám…

„Root“ oprávnění má pouze jeden člověk.

Nemáme žádné standardy bezpečnosti ani IT.

Máme jednofaktorové přihlášení…. včetně administrátorů odkudkoliv.

DR plány jsme konkrétně digitalizovali … pak přišel ransomware.

Do prostředí se připojují třetí strany. Jejich seznam ani úroveň jejich praxi bezpečnosti není znám.

Existuje jednotné heslo … ke administraci „všeho“.

# Je užitečné zaujmout perspektivu útočníka

„Příběh podle skutečných událostí....“

# Jak to celé typicky začíná – útok na zařízení uživatele cloudu

**Uživateli je doručen email, který obsahuje nebezpečnou přílohu.**

**Škodlivý email**

**Slabá Messaging Gateway**

**Email server (schránka)**

**Chybějící analýza obsahu, atd.**

HPE aruba networking
**Aruba ClearPass**

| | |
|---|---|
| **Valid Accounts** | **Phishing** |
| Drive-by Compromise | Replication Through Removable Media |
| Exploit Public-Facing Application | Supply Chain Compromise |
| External Remote Services | Trusted Relationship |
| HW Additions | |



**Illustrations:** Pixabay

# Útok pokračuje napadením koncové stanice

**Uživatel otevře přílohu a spustí makro. Malware se spouští.**

Koncová stanice

**Malware přebírá vládu nad koncovým bodem**

Bezpečnost OS „by design“ se nevyužívá

Bezpečná konfigurace (hardening) není standardem

Slabá ochrana koncové stanice

Neexistuje „Whitelisting“ aplikací

Analýza dle vzorů

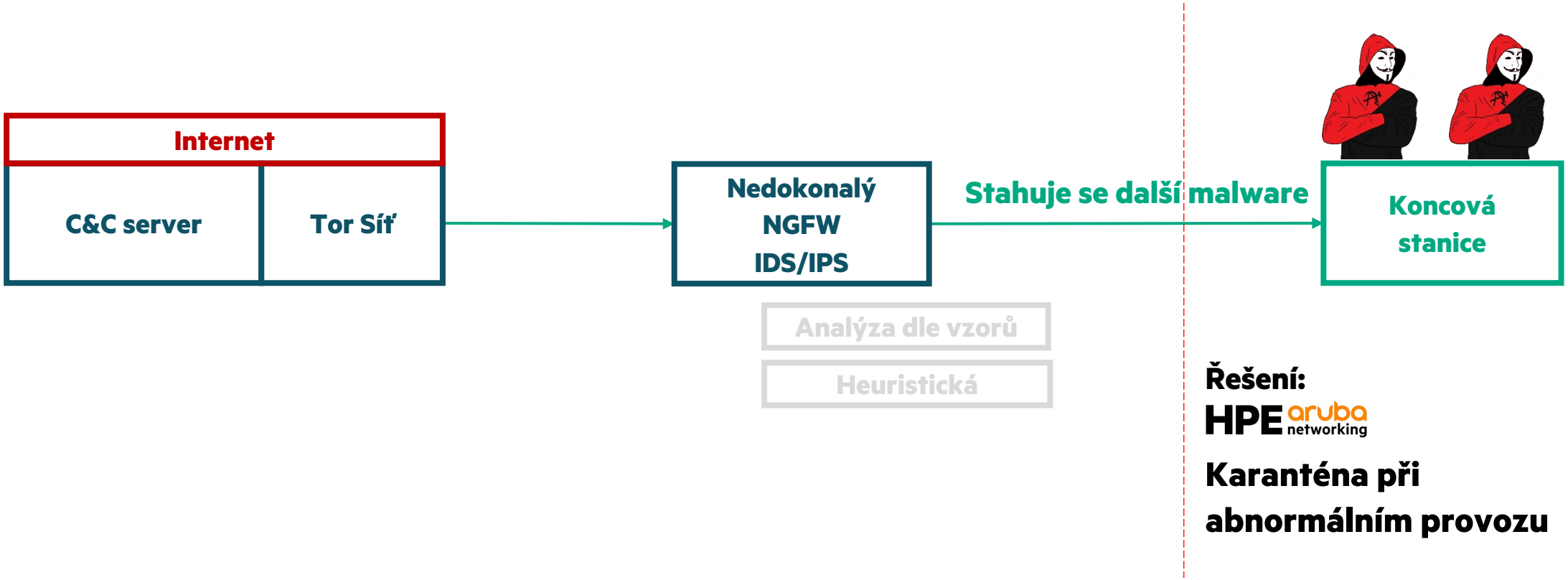
Heuristická



**Illustrations:** Pixabay

# Malware volá domů

**Malware se připojuje na svoji mateřskou loď a stahuje další „pomocníky“.**




**Řešení:**

HPE aruba networking

**Karanténa při abnormálním provozu**



**Illustrations:** Pixabay

# Nákaza se začíná šířit

**Malware se snaží pohybovat po síti. Typickým cílem je najít doménový řadič.**

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

Internet

Řešení:
HPE aruba networking
Aruba – cx10000

Neexistující segmentace

Malware se snaží šířit

Koncová stanice

Analýza dle vzorů

Heuristická

Bezpečnostní zóny se neřeší

Servery

Doménový Řadič

Enterprise administrátor

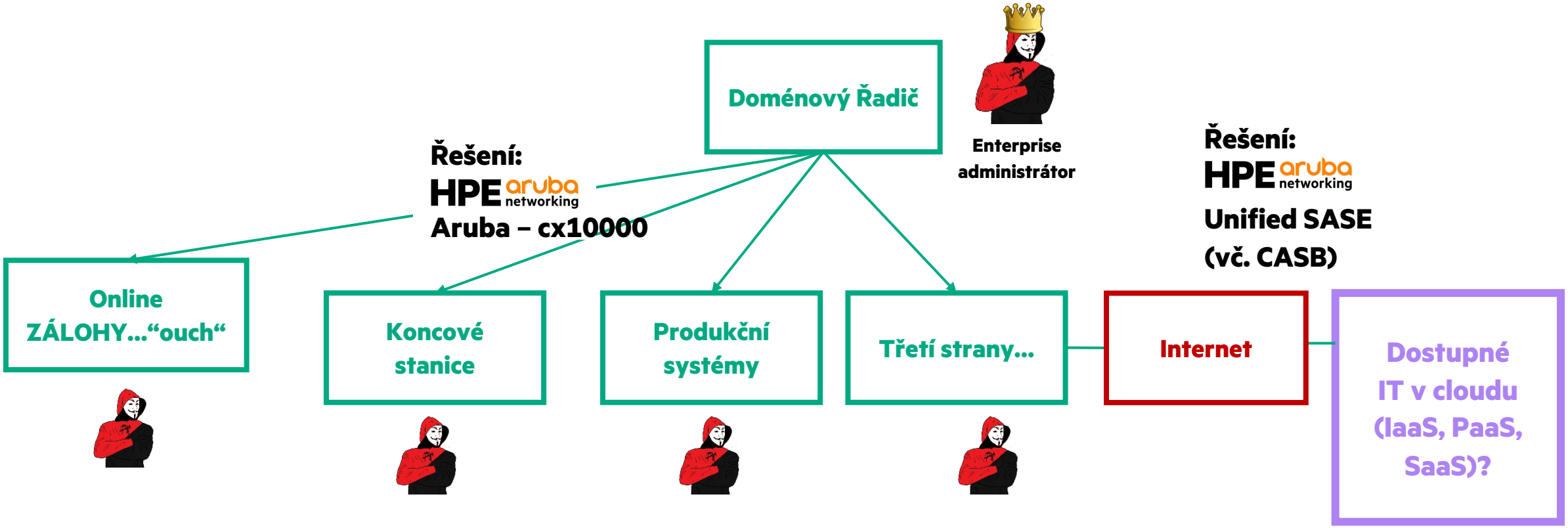
Žádná detekce neobvyklé aktivity



**Illustrations:** Pixabay, Rawpixel

# Závěrečný bolestivý úder

**Specializované části malwaru napadají všechno možné. Zálohy nevyjímaje…**






**Illustrations:** Pixabay, Rawpixel

# Co v této souvislosti nabízíme?

Rekapitulace

# Co si odnést?

## HPE HW technologie, včetně „as a service“

HPE GreenLake

**IaaS, PaaS, SaaS**

Bezpečný privátní flexibilní cloud provozovaný u Vás, případně v konkrétní „co-location“

HPE aruba networking

Síťové technologie k budování bezpečných hybridních prostředí, které zabrání kybernetickému napadení

**HPE Serverový HW** – se zabudovanou bezpečností

## HPE konzultační služby

Konzultační služby na míru – řešící „problém“, nikoliv jen nastavení konkrétní izolované technologie

**Kybernetická bezpečnost:**

- Rychlá a přehledová analýza existující praxe bezpečnosti
- Ransomware awareness
- Analýza těch nejtypičtějších chyb využívaných při reálných útocích
- Bezpečnost prostředí postavených na různých technologiích
- Table-top simulace napadení
- atd.

# Děkujeme za pozornost.

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