Avast Business

Bezpečnostní hygiena pro neziskovky

aneb centrální správa a proč se vyplatí

Jiří Zlámal

Avast Business Sales Engineer

2 hlavní vektory útoku...

...a 3 oblasti které je potřeba chránit

Útočná plocha jakékoliv organizace je:

1. **Lidé**
2. **Zařízení**

Potřeba chránit:

1. Zaměstnance

2. Zařízení

3. Data

Lidé jako vektor útoku

Sociální inženýrství, nejčastěji ve formě phishingu, je primární hrozbou

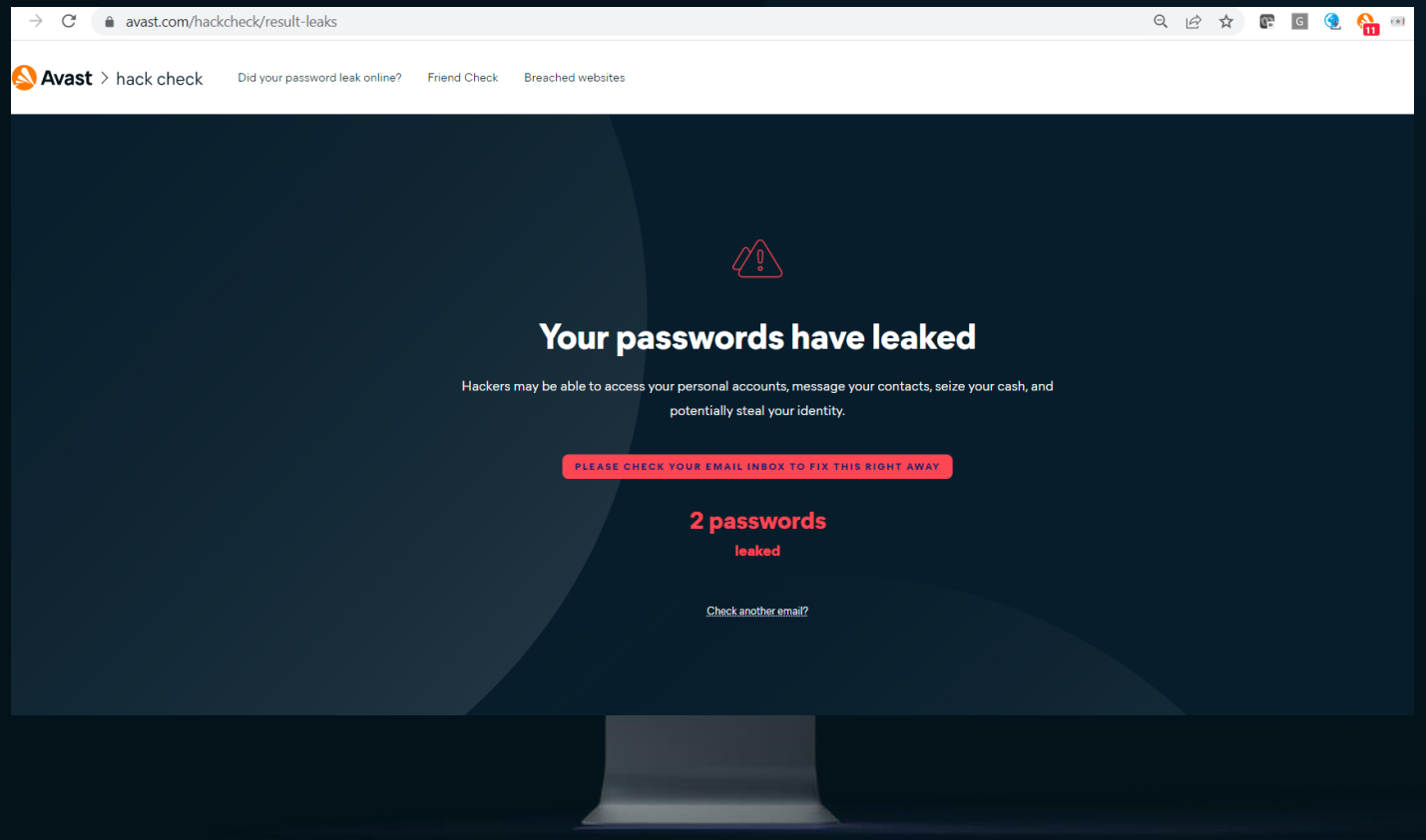
- **Phishing** - útočník odešle podvodnou zprávu, jejímž účelem je přimět osobu, aby prozradila útočníkovi citlivé informace nebo nasadit škodlivý software do infrastruktury oběti, např. ransomware.
- **Spear Phishing** - Pokusy o phishing zaměřené na konkrétní jednotlivce nebo společnosti. Na rozdíl od hromadného phishingu často útočníci již mají nějaké osobní údaje o svém cíli, které využijí ke zvýšení pravděpodobnosti úspěchu.
- **Whaling** - Spear phishingový útok zaměřený konkrétně na vedoucí pracovníky a další významné cíle. V těchto případech bude obsah vytvořen tak, aby se zaměřoval na specifického vyššího manažera.
- **Clone Phishing** – Legitimní, dříve doručený e-mail obsahující přílohu nebo odkaz, který byl použit k vytvoření téměř identického nebo klonovaného e-mailu. Příloha nebo odkaz v e-mailu je nahrazen škodlivou verzí a odeslán z e-mailové adresy podvržené tak, aby se zdálo, že pochází od původního odesílatele.

Sociální inženýrství je v kontextu informační bezpečnosti manipulace lidí k provádění akcí nebo prozrazení důvěrných informací.

Liší se od tradičního podvodu v tom, že je často **jedním z mnoha kroků ve složitém podvodném schématu**.

Obecně řečeno, sociální inženýrství bylo také definováno jako jakýkoli akt, který ovlivní osobu, aby učinila akci, která může, ale nemusí být v jejím nejlepším zájmu.

Osobní kyberbezpečnost



Relevantní jak pro firmu, tak pro zaměstnance osobně

https://haveibeenpwned.com/

https://www.avast.com/hackcheck

Hlavně v případě BYOD jsou osobní a firemní kyberbezpečnost přímo spojené.

Hlavní body pro kyberbezpečnost

Zajistit Ověřování Identity

Definovat zásady hesel a zavést SSO a MFA

Zabezpečení práce na dálku

VPN který zašifruje veškerý provoz, bezpečný přístup k firemním údajům a aplikacím.

Zajistit vzdělávání zaměstnanců

Lidé se nemohou bránit proti hrozbám, které si neuvědomují.

Zálohování

Navzdory všem opatřením, zálohování je stále poslední nejspolehlivější záchrana

Antivirus

Instalace a sledování antiviru na všech zařízeních je stále základním kamenem ochrany

Pravidelné Vyhledávání Zranitelností

Mělo by se dělat pravidelně a zahrnovat stav antiviru, hesla, aktualizace, př. penetrační testování

Data Loss Prevention

DLP řešení brání uživatelům ve sdílení citlivých dat mimo společnost

Správa Aktualizací

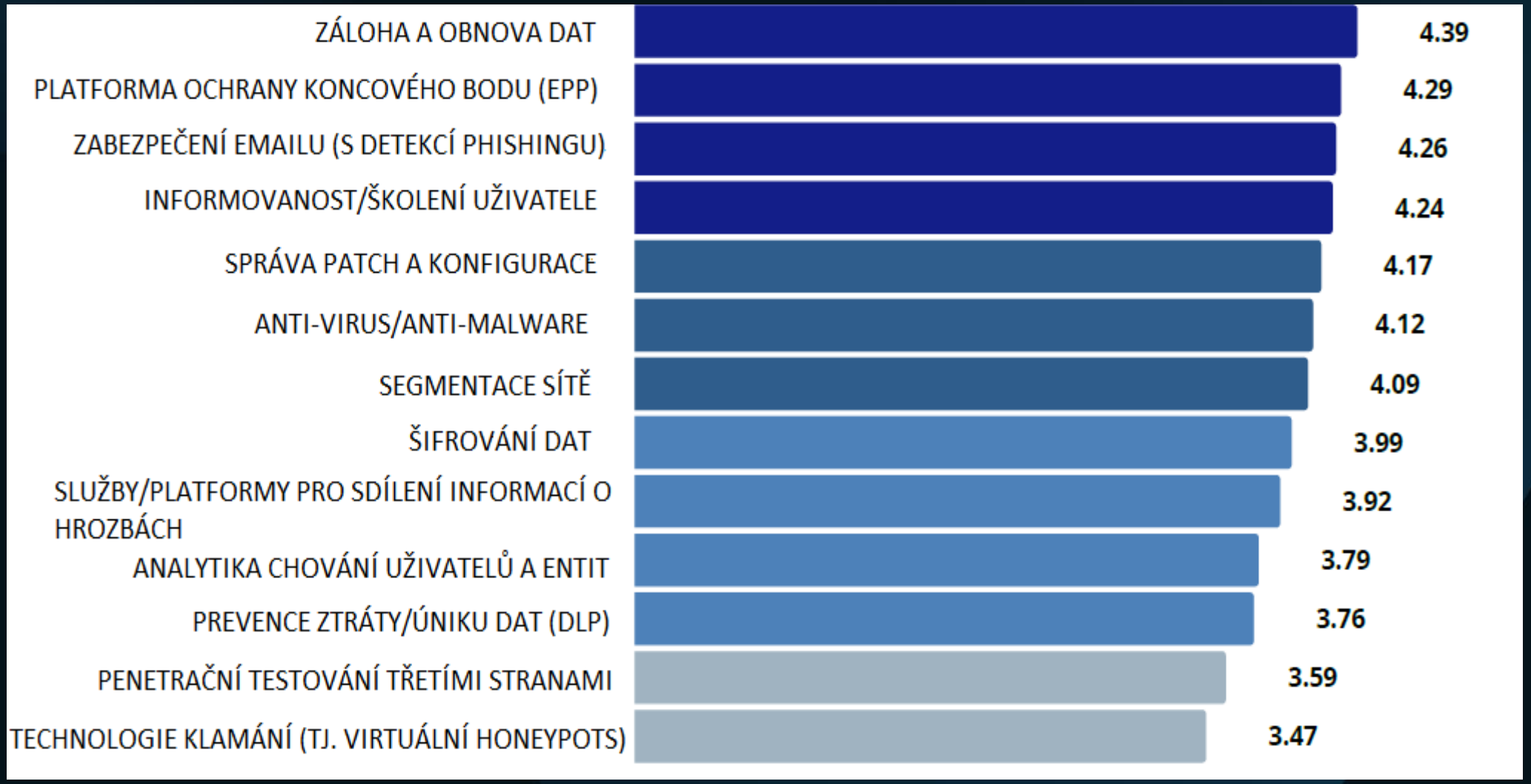
Každý software může být zranitelný, včasná instalace aktualizací je kritická

Definovat Vymahatelná Pravidla a Procesy

Jaká data je třeba chránit a jak. Zaměstnanci musí rozumět jejich roli ve kyberbezpečnosti organizace.

Avast Business

Opatření dle důležitosti



Bezpečnost vs. Praktičnost

- Admin jenom pro IT a vyvolené
- Zálohy několikanásobně klonované, cloudové
- Jenom HW a SW společnosti

- Admin přístup (skoro?) pro všechny
- Místní zálohy serverů
- BYOD

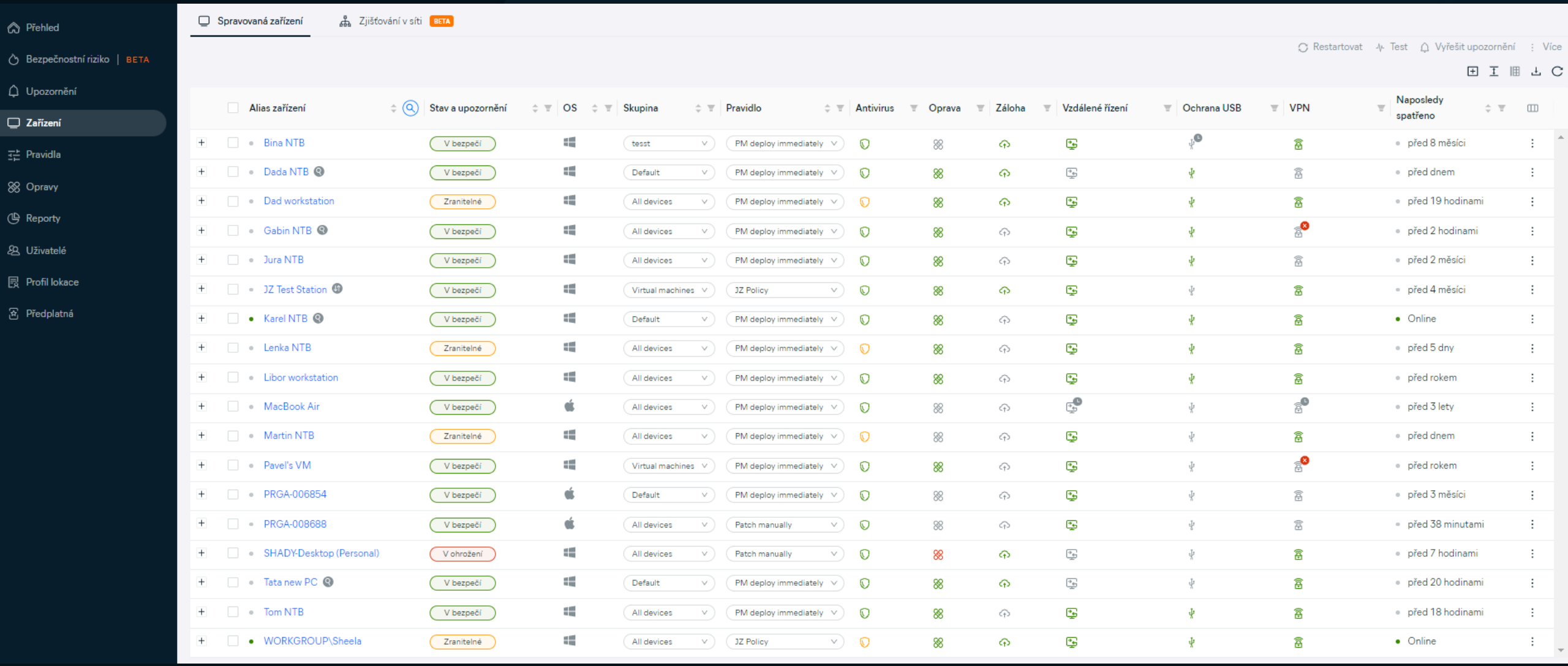
Vše on-premise na HW organizace
vs.
Cloudové služby

Základní “Hygiena”

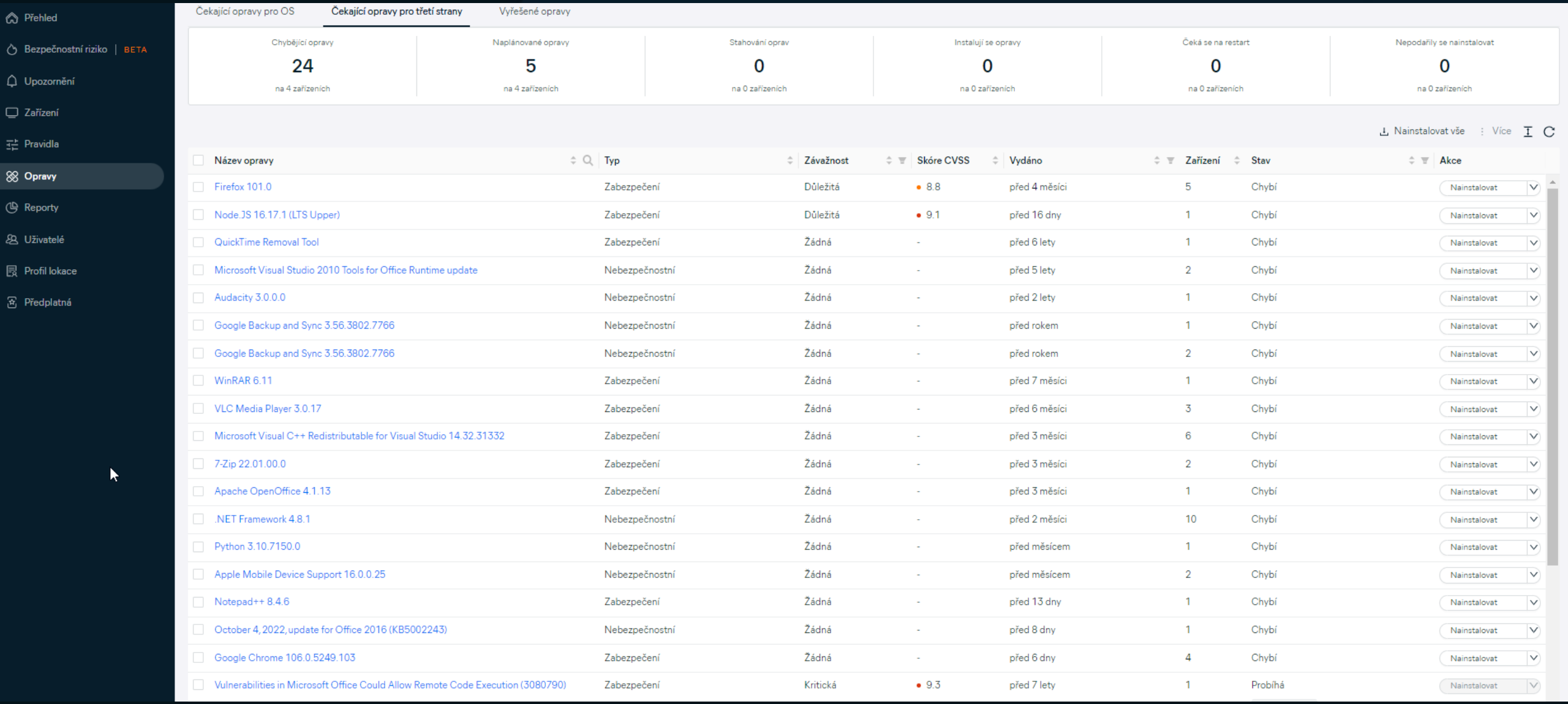
Každá organizace by měla provozovat:

1. Diverzifikované zálohování
2. Základní kyberbezpečnostní školení zaměstnaců
3. Plánování postupu pro případ narušení kyberbezpečnosti
4. Ochranu koncových bodů (AV) s centrální správou
5. Centrální správu aktualizací softwaru

Avast Business Hub: Centrální přehled připojených stanicí



Avast Business Hub: Centralizace správy aktualizací



Název opravy	Typ	Závažnost	Skóre CVSS	Vydáno	Zařízení	Stav	Akce
Firefox 101.0	Zabezpečení	Důležitá	8.8	před 4 měsíci	5	Chybí	Nainstalovat
Node.JS 16.17.1 (LTS Upper)	Zabezpečení	Důležitá	9.1	před 16 dny	1	Chybí	Nainstalovat
QuickTime Removal Tool	Zabezpečení	Žádná	-	před 6 lety	1	Chybí	Nainstalovat
Microsoft Visual Studio 2010 Tools for Office Runtime update	Nebezpečnostní	Žádná	-	před 5 lety	2	Chybí	Nainstalovat
Audacity 3.0.0.0	Nebezpečnostní	Žádná	-	před 2 lety	1	Chybí	Nainstalovat
Google Backup and Sync 3.56.3802.7766	Nebezpečnostní	Žádná	-	před rokem	1	Chybí	Nainstalovat
Google Backup and Sync 3.56.3802.7766	Nebezpečnostní	Žádná	-	před rokem	2	Chybí	Nainstalovat
WinRAR 6.11	Zabezpečení	Žádná	-	před 7 měsíci	1	Chybí	Nainstalovat
VLC Media Player 3.0.17	Zabezpečení	Žádná	-	před 6 měsíci	3	Chybí	Nainstalovat
Microsoft Visual C++ Redistributable for Visual Studio 14.32.31332	Zabezpečení	Žádná	-	před 3 měsíci	6	Chybí	Nainstalovat
7-Zip 22.01.00.0	Zabezpečení	Žádná	-	před 3 měsíci	2	Chybí	Nainstalovat
Apache OpenOffice 4.1.13	Zabezpečení	Žádná	-	před 3 měsíci	1	Chybí	Nainstalovat
.NET Framework 4.8.1	Nebezpečnostní	Žádná	-	před 2 měsíci	10	Chybí	Nainstalovat
Python 3.10.7150.0	Nebezpečnostní	Žádná	-	před měsícem	1	Chybí	Nainstalovat
Apple Mobile Device Support 16.0.0.25	Nebezpečnostní	Žádná	-	před měsícem	2	Chybí	Nainstalovat
Notepad++ 8.4.6	Zabezpečení	Žádná	-	před 13 dny	1	Chybí	Nainstalovat
October 4, 2022, update for Office 2016 (KB5002243)	Nebezpečnostní	Žádná	-	před 8 dny	1	Chybí	Nainstalovat
Google Chrome 106.0.5249.103	Zabezpečení	Žádná	-	před 6 dny	4	Chybí	Nainstalovat
Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)	Zabezpečení	Kritická	9.3	před 7 lety	1	Probíhá	Nainstalovat

Avast Business

Správa aktualizací - Patch Managment

Proč a jak centralizovat tento klíčový aspekt kyberbezpečnosti

57%

případů narušení dat se připisuje špatné správě aktualizací[1]

102 dní

je průměrná doba pro podnik nasadit kritické softwarové aktualizace[1]

86%

nahlášených chyb zabezpečení pochází z aplikací třetích stran[2]

[1]Ponemon. [2]National Vulnerability Database.

… přesto, málo společností pravidelně aktualizuje software

Avast provedl posouzení bezpečnosti 500 000 koncových bodů, pouze

29%

prošlo všemi testy aktualizace softwaru

Z 500 000 analyzovaných zařízen

304

byly 100% aktualizovány

55%

všech softwarových aplikací na celém světě nejsou aktualizované

15%

Windows 7 instalací nejsou aktualizované

8%

Windows 10 instalací nejsou aktualizované

Nebezpečí nedostatečné pozornosti věnované aktualizacím je jasné:

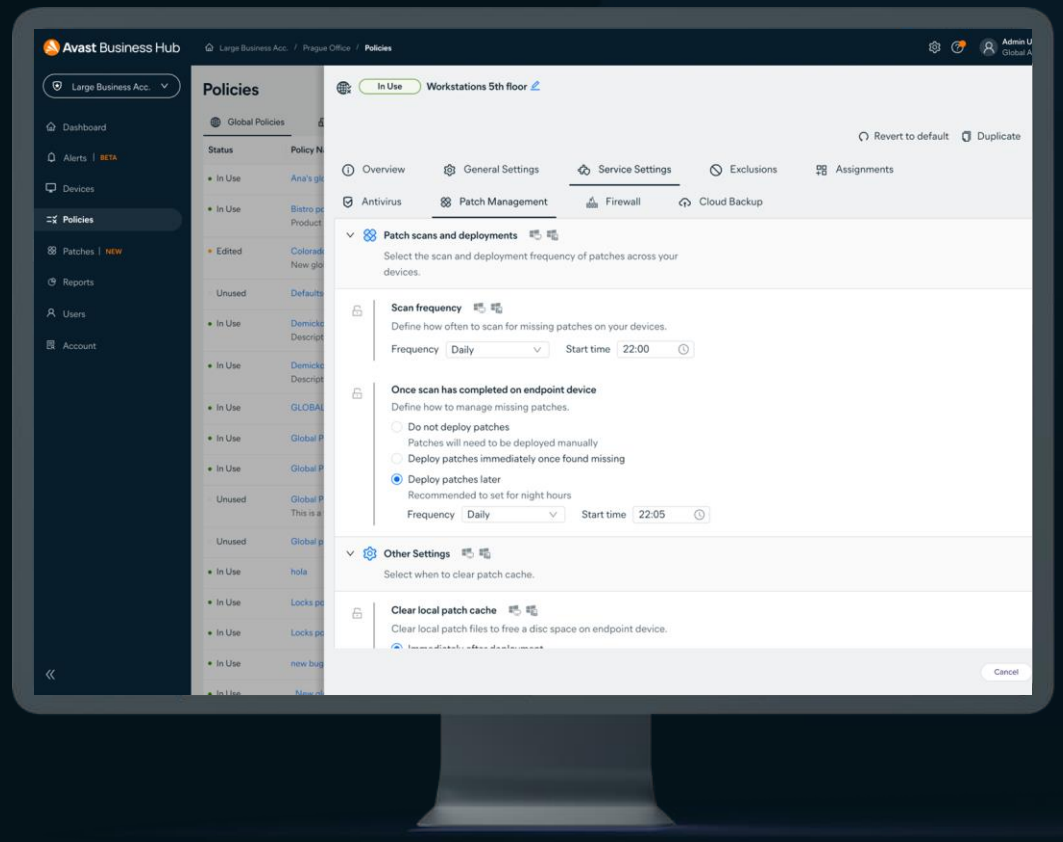
- Ransomware
- Ztráta nebo krádež dat
- Ztráta času pro obnovení provozu
- Právní následky, odpovědnost k zákazníkům, partnerům a státním regulátorům
- Narušení integrity dat
- Ztráta důvěryhodnosti

Hlavní nebezpečí ale nečíhá ve velkých 0-day zranitelnostech ktere jsou často medializované. Útočníci spoléhají hlavně na:

- Automatizované útoky
- Zneužití zranitelností, na které již existuje oprava
- Dostatek času mezi vydáním aktualizace a jejím nasazení
- Schopnost pokrýt velké množství systémů v krátkém čase, vyhledávat zranitelné

Životní cyklus zranitelnosti

Patch Managment v Avast Business Hub



Rychlé řešení zranitelností s centrálním managmentem aktualizací

- Centralizuje kontrolu nad aktualizacemi jak OS Windows, tak aplikací třetích stran
- Výrazně snižuje úsilí potřebné k udržování softwaru v aktuálním stavu
- Minimalizuje závislost na jednotlivých uživatelých

- 400+ aplikací, tisíce patchů
- Testované a ověřené opravy
- Intuitivní ovládání
- Manuální nebo automatické nasazování, plánování
- Místní aktualizační agent pro úsporu šířky pásma

Děkuji za pozornost!