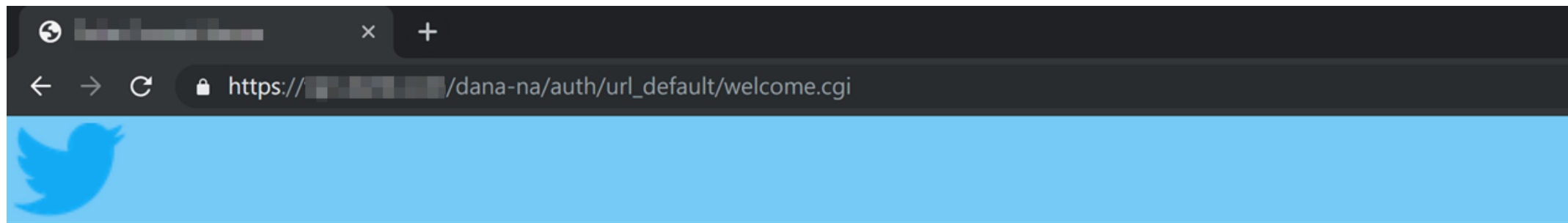




Martin Haller

《 Teorie vs. praxe: naše postřehy z auditů 》



Welcome to the Twitter VPN Access Portal

username
password
Realm

Please sign in to begin your secure session.

Sign In

Zdroj: <https://devco.re/blog/2019/09/02/attacking-ssl-vpn-part-3-the-golden-Pulse-Secure-ssl-vpn-rce-chain-with-Twitter-as-case-study/>

I velká organizace s velkým rozpočtem může
dělat „základní“ chyby.

Martin Haller

- PATRON-IT s.r.o.
(MSP / MSSP)
- Etický hacker
- Blog MartinHaller.cz



Problematická místa

- Návrh zabezpečení
- Realizace návrhu

Chyby v návrhu

Podle čeho se navrhuje architektura zabezpečení?

Návrh – podle toho, co koho napadne



Autor: Josef Čapek

Návrh – podle toho s čím si kdo chce hrát



Zdroj: <https://www.pexels.com/photo/a-toddler-playing-with-in-the-room-5247758/>

Návrh – podle toho co nabídne dodavatel



Zdroj: <https://www.pexels.com/photo/man-wearing-an-apron-helping-a-elderly-man-8422706/>

Návrh

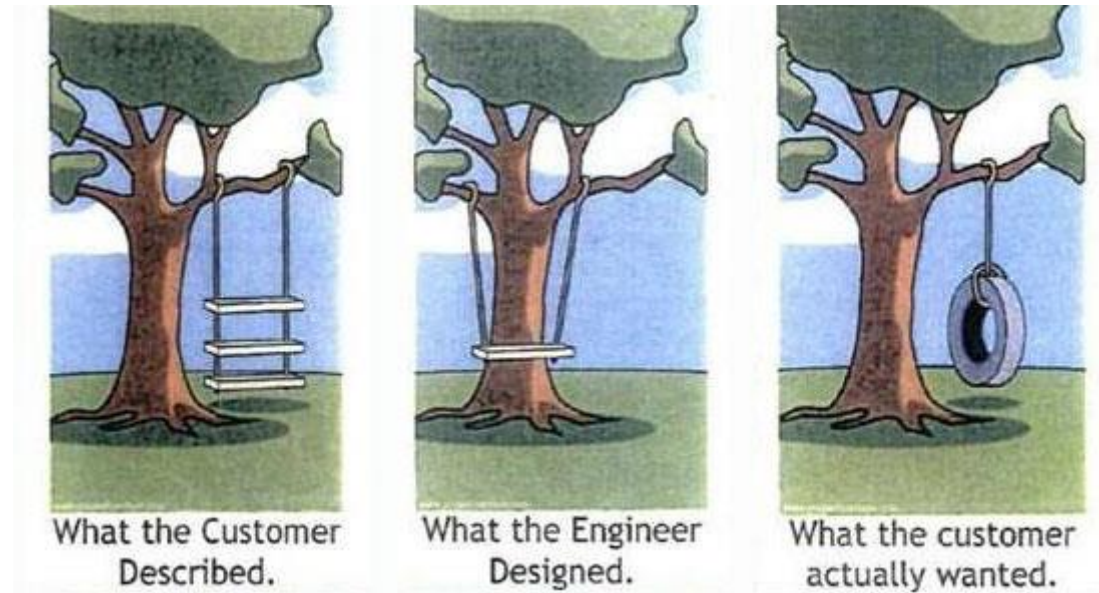
- Neoptimální výsledky
- Nedostatek lidí
- Každý vymýšlí kolo
- Problém neznámých neznámých

Návrh – na co se zaměřujeme

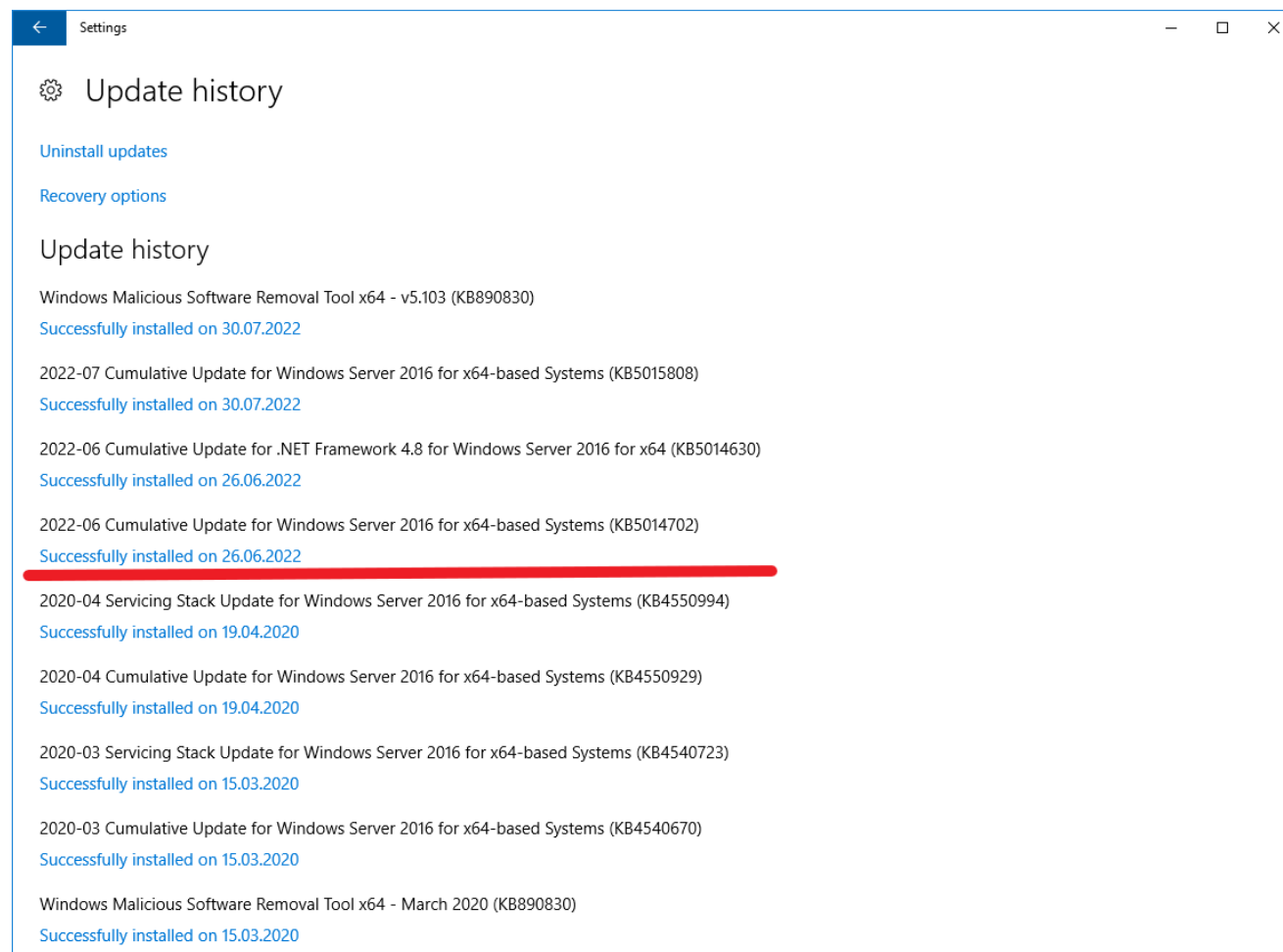
Podle toho co dělají útočníci:

- Ransomware -> **zálohy** – nesmazatelnost, úplnost, obnovitelnost, monitorování
- Lateral movement -> **síťová segmentace** (produkce, virtualizace+zálohy, management), **LAPS, seznam privilegovaných účtů v AD, identifikace kritických serverů, používání Domain Admins účtů, aktualizace, AV a jeho monitorování.**
- Initial foothold -> **2FA, veřejně dostupné služby, AV a jeho monitorování**

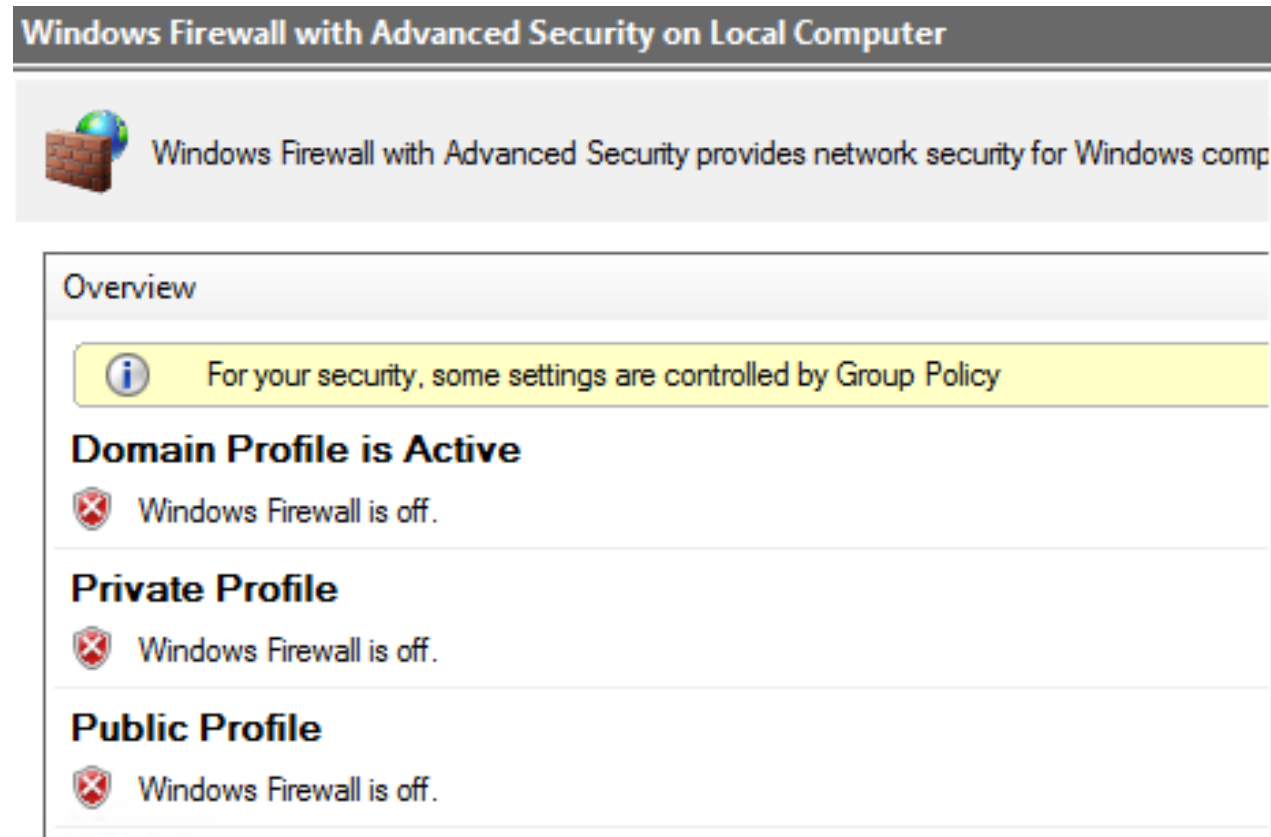
Realizace opatření



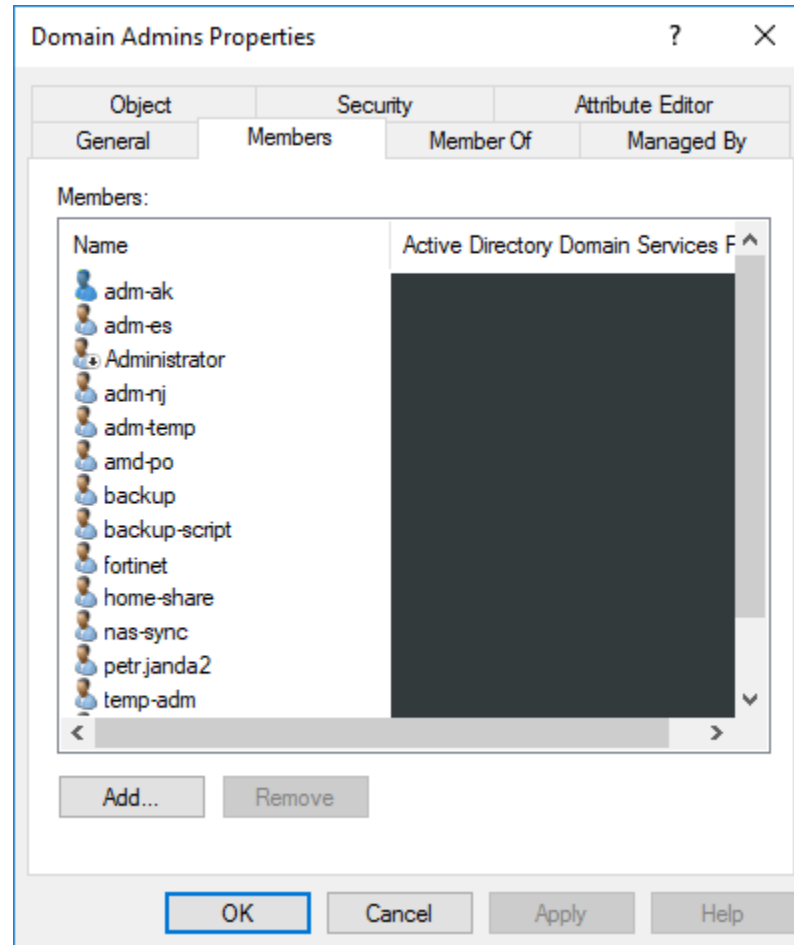
Realizace - Aktualizace



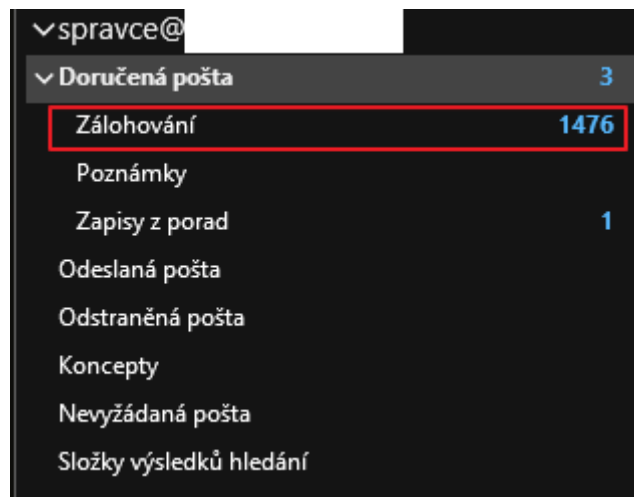
Realizace – AV / firewall



Realizace – Mnoho privilegovaných účtů



Realizace – Monitorování



▼ spravce@	
▼ Doručená pošta	3
Zálohování	1476
Poznámky	
Zapisy z porad	1
Odeslaná pošta	
Odstraněná pošta	
Koncepty	
Nevyžádaná pošta	
Složky výsledků hledání	

Realizace – nakoupené technologie



Realizace - zálohy

The screenshot displays the Veeam Backup and Replication console. The 'Jobs' tab is active, showing a list of backup jobs. The 'Servers Backup to Cloud' job is selected, and a context menu is open over it, with the 'Stop' option highlighted. The job progress bar indicates 48% completion. The summary section shows the job duration, processing rate, and bottleneck. The status section shows the job is successful, with no warnings or errors. The throughput graph shows a peak in activity.

Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Agent Backup Copy	Linux Backup Copy	0	Stopped			<As new restore...	Default Backup...	Created by SRV16...
Backup Copy	Windows Backup Copy	0	Stopped			<As new restore...	Default Backup...	Created by SRV16...
DB Backup	Windows Agent Backup	1	Stopped	19 hours ago	Success	2/21/2021 9:00...	Default Backup...	Backup of MS SQL...
PosgreSQL DB Backup	Linux Agent Backup	1	Stopped	23 hours ago	Success	<not scheduled>	Default Backup...	Created by SRV16...
QWE Fileserver Backup	VMware Backup	1	Stopped	23 hours ago	Success	<not scheduled>	Cloud reposito...	Created by SRV16...
Server Backup	Windows Agent Backup	1	Stopped	34 minutes ago	Success	<not scheduled>	Default Backup...	Veeam Agent for W...
Servers Backup to Cloud	Windows Agent Backup	1	48% com...	6 minutes ago		2/22/2021 2:00...	Cloud reposito...	Created by SRV16...
Windows Servers Backup	Windows Agent Backup	1	Stopped	18 hours ago	Success	2/21/2021 10:00...	Default Backup...	Created by SRV16...
Workstations Backup to Cloud	Windows Agent Backup	1	Enabled	21 minutes ago	N/A	N/A	Cloud reposito...	Created by SRV16...

Job progress: 48% (0 of 2 hosts)

SUMMARY

Duration: 06:06
Processing rate: 318 MB/s
Bottleneck: Source

STATUS

Success: 0
Warnings: 0
Errors: 0

THROUGHPUT (LAST 5 MIN)

Speed: 0 KB/s

1 job selected

Connected to: localhost Build: 11.0.1.1261 Enterprise Plus Edition Support expires: 258 days remaining

Realizace – další postřehy

- Lidé spolu nekomunikují – vznikají mezery, není daná odpovědnost
- Chyby v segmentaci

Co s tím?



Co s tím

- Nutnost se vzdělávat !!!
- Udržovat se v obraze:
 - <https://thehackernews.com/> - zpravodajství ze světa IT bezpečnosti
 - <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> - seznam zranitelností, které patchovat
 - <https://www.akamai.com/blog/security/conti-hacker-manual-reviewed#access> – přečíst si něco o nepříteli
 - <https://www.cisa.gov/uscert/ncas/alerts> - přihlásit se k odběru varování od americké CISA
 - <https://www.nukib.cz/cs/infoservis/hrozby/> - varování od NUKIBu
 - <https://www.nukib.cz/cs/infoservis/doporuceni/1511-doporuceni-nukib-pro-administratory-verze-4-0/> - nevymýšlet znovu kolo
- Občas si zkontrolovat že věci odpovídají tomu co bylo domluveno
- Společně spolupracovat



Děkuji za
〈pozornost〉