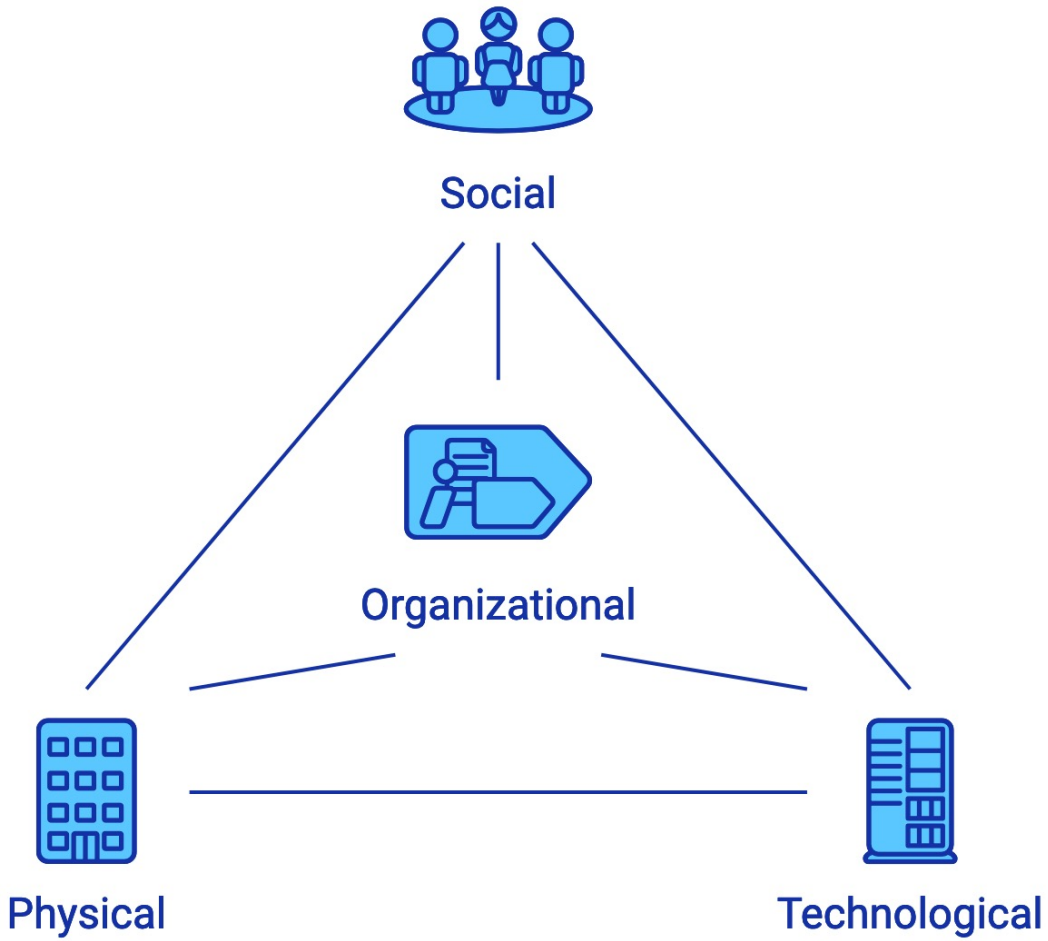
Cílený kybernetický útok

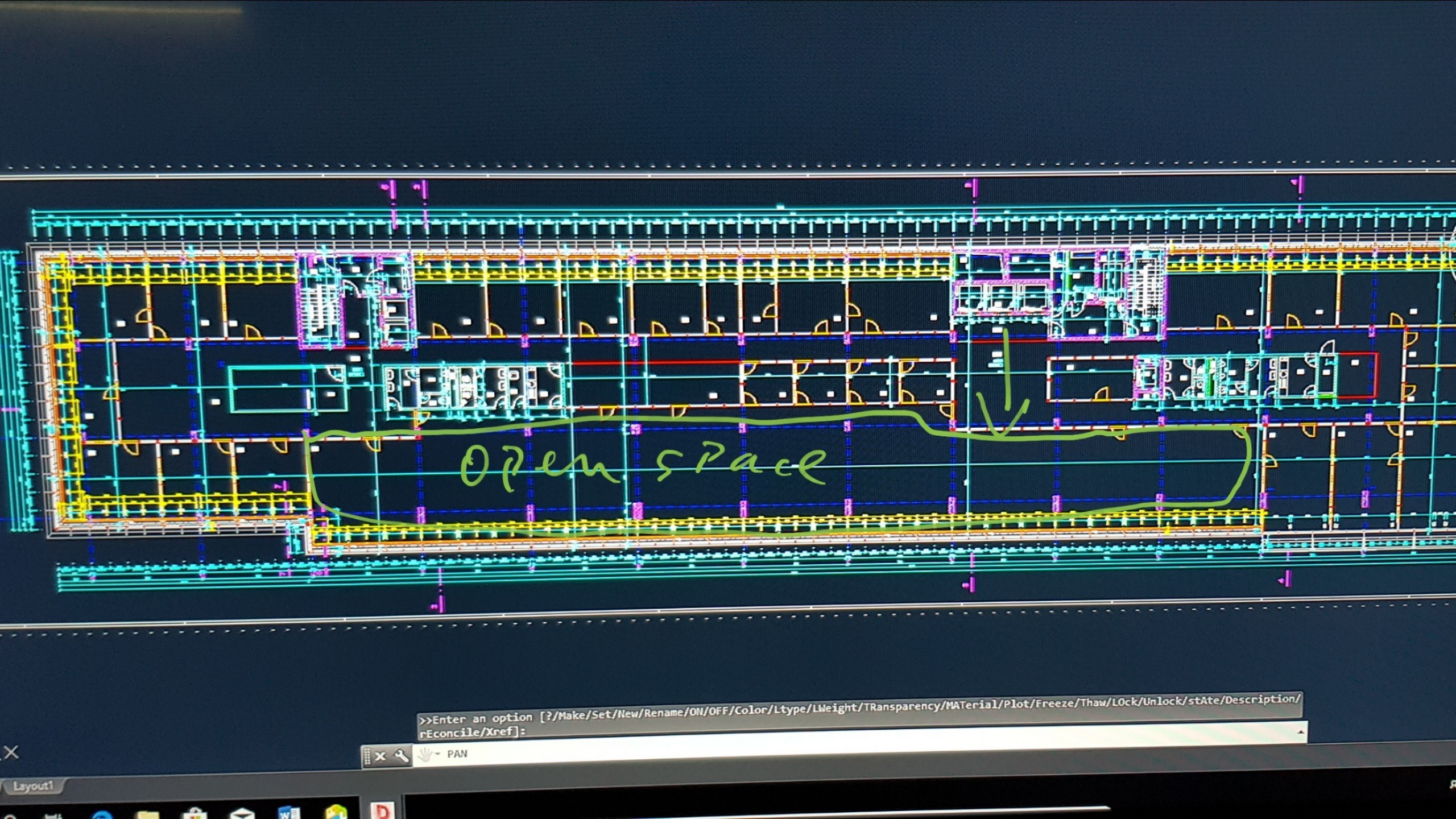
Jak operují APT skupiny a jak se jim bránit

Jiří Vaněk

Security Unit Manager

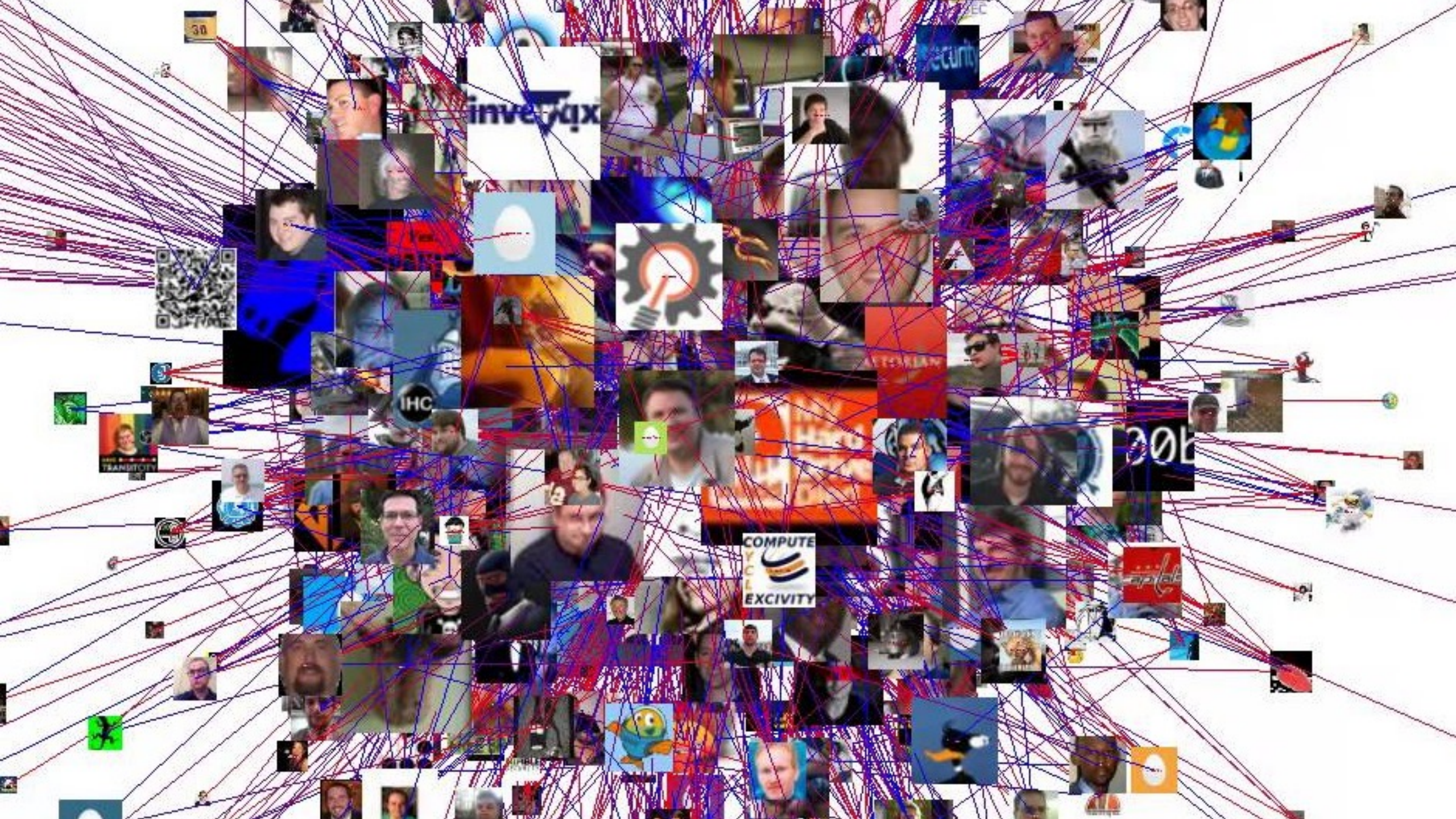
13.05.2022




Open space
>>Enter an option [?/Make/Set/New/Rename/ON/OFF/Color/Ltype/LWeight/TRansparency/MATerial/Plot/Freeze/Thaw/LOck/Unlock/stAte/Description/
rEconcile/Xref]:
PAN
Layout1

```
sh-3.2# nmap -sS -sV -O --min-parallelism 64 -oX output -v plus4u.net
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-08 15:18 CEST
NSE: Loaded 43 scripts for scanning.
Initiating Ping Scan at 15:18
Scanning plus4u.net (193.85.156.207) [4 ports]
Completed Ping Scan at 15:18, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:18
Completed Parallel DNS resolution of 1 host. at 15:18, 0.01s elapsed
Initiating SYN Stealth Scan at 15:18
Scanning plus4u.net (193.85.156.207) [1000 ports]
Discovered open port 80/tcp on 193.85.156.207
Discovered open port 443/tcp on 193.85.156.207
Completed SYN Stealth Scan at 15:18, 4.01s elapsed (1000 total ports)
Initiating Service scan at 15:18
Scanning 2 services on plus4u.net (193.85.156.207)
Completed Service scan at 15:18, 12.08s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against plus4u.net (193.85.156.207)
Retrying OS detection (try #2) against plus4u.net (193.85.156.207)
NSE: Script scanning 193.85.156.207.
Initiating NSE at 15:18
Completed NSE at 15:18, 0.12s elapsed
Initiating NSE at 15:18
Completed NSE at 15:18, 0.00s elapsed
Nmap scan report for plus4u.net (193.85.156.207)
Host is up (0.0036s latency).
Not shown: 996 filtered ports
PORT    STATE  SERVICE  VERSION
25/tcp  closed smtp
80/tcp  open   http     Apache httpd
443/tcp open   ssl/http Apache httpd
465/tcp closed smtps
Device type: WAP|general purpose|firewall|router|load balancer
Running (JUST GUESSING): Linksys embedded (93%), Linux 2.6.X (89%), Palo Alto embedded (87%), Synology embedded (85%), F5 Networks TMOS 11.1.X (85%)
OS CPE: cpe:/h:linksys:befw11s4 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:paloalto:pa-500 cpe:/h:synology:rt1900ac cpe:/o:f5:tmos:11.1
Aggressive OS guesses: Linksys BEFW11S4 WAP (93%), Linux 2.6.32 (89%), Palo Alto PA-500 firewall (87%), Synology RT1900ac router (85%), F5 3600 LTM load balancer (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.000 days (since Mon Apr  8 15:18:11 2019)
TCP Sequence Prediction: Difficulty=250 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.56 seconds
           Raw packets sent: 2046 (93.748KB) | Rcvd: 39 (2.232KB)
sh-3.2#
```

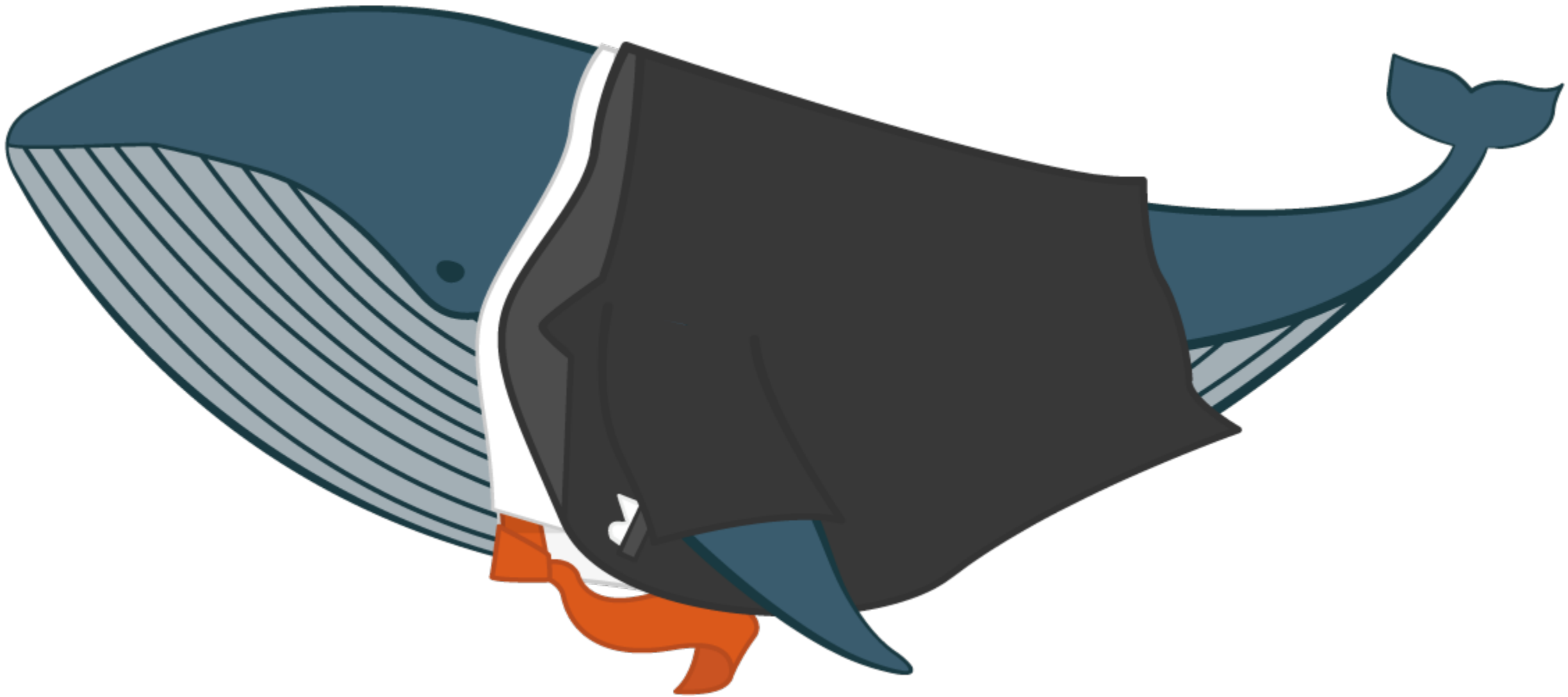

COMPUTE
CYCLE
EXCIVITY

- Školení k publikování interních informací
- Školení k používání SM
- Monitoring SM
- Monitoring veřejných zdrojů
- Monitoring veřejných úložišť
- Pravidelné provádění OSINT
- Pravidelné skenování perimetru
  - Pozor na „shadow IT“ a zdroje v cloudech

- **30% phishingových zpráv** je otevřeno cílovým uživatelem
- **12% těchto uživatelů klikne** na škodlivý odkaz či přílohu
- **95% všech útoků** je výsledkem úspěšného spear phishingu

„Množství osobních informací, které jsou lidé ochotni sdílet na sociálních sítích, pomáhá útočníkům perfektně profilovat své cíle.

Detaily jako data narození, jména rodinných příslušníků a mazlíčků, detaily o zaměstnáních a zaměstnavatelích či nedávné důležité události jsou bezednou studnicí k zacílení útoku.“



Hi Tatrabanka security!

Please read this email carefully!

We have dumped credentials to your mobile banking! Complete database of PIDs, passwords, names, addresses and other personal data now belong to us. As proof, we have hidden the complete dump at your server ”uat.tatrabanka.sk". If you're good enough you must find it in no time:)

And by the way, we also have access to these your servers:

dev.tatrabanka.sk

hadoop.tatrabanka.sk

red.tatrabanka.sk

We are ready to negotiate the price for our silence. Expect further

instructions in 24 hours.

Do not try to cut off the servers! If our backdoor does not reach our C&C it will automatically encrypt whole server!

Best regards,

z3r0bytes team

Podporovať výnimočné zamestnanca je pre nás dôležité.

Sme radi, že máme veľa ľudí, ktorí každý deň pomáhajú napĺňať naše ciele a posúvať sa bližšie našim zákazníkom.

Preto sme sa rozhodli tie najlepšie odmeniť. Choďte na https://tvojatatrabanka.sk a vyberte si svoj vianočný darček!

Vaša Tatra banka
#prirodzenenajlepsi

https://tvojatatrabanka.sk/auth/login

MSN International Edition - W...

Premium banking academ...

TATRA BANKA

Login

Heslo

Prihlásenie

Zabudnuté heslo

Prosím prihláste sa vašimi údajmi do domény. V prípade problémov s prihlásením nás prosím kontaktujte

KONTAKTOVAŤ

Vážení,

z dôvodu nedávno prebehnutých phishingových útokov na našu spoločnosti musíme vykonať urgentnú kontrolu prístupov do informačných systémov. Preto prosím vyplňte priloženú tabuľku, v ktorej špecifikujete, na aké informačné systémy máte aktuálne prístup. Tieto informácie budú použité pre porovnanie s našou internou databázou.

Pre zjednodušenie sme do tabuľky vložili makro, ktoré nahrá vyplnené údaje do nášho systému. Preto prosím povoľte spustenie makier.

Ďakujem za spoluprácu a prajem Vám veľa síl v tomto hektickom predvianočnom čase.

**** ****

Head of **** department

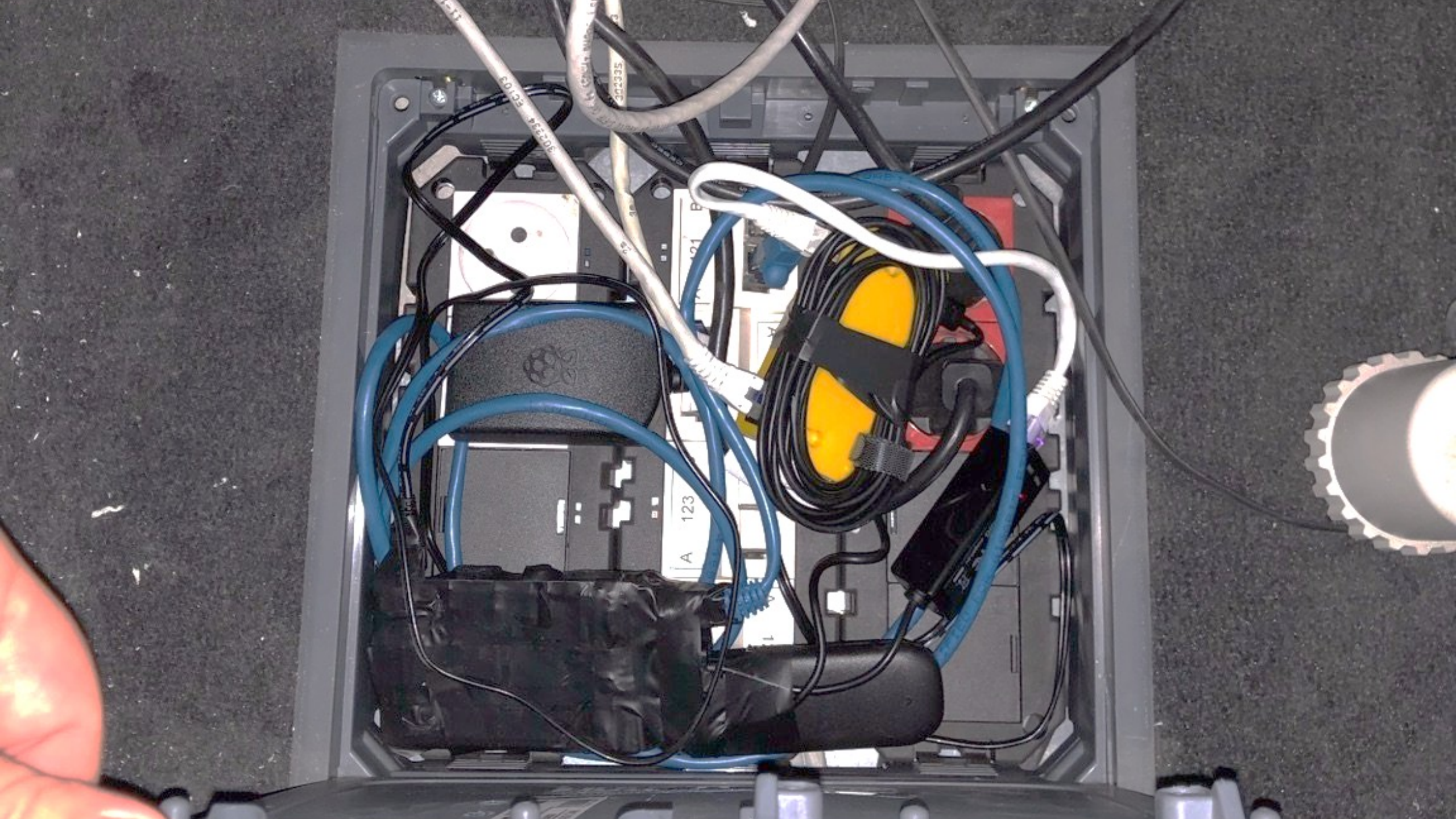
- Školení k sociálnímu inženýrství
- Pravidelné phishingové kampaně
  - Jednoduché, generované nástrojem – často
  - Cílené, realizované externím dodavatelem – alespoň kvartálně, ale náhodně
- Monitoring podvodných domén
- Monitoring kampaní v sektoru
- Minimalizace doručení phishingu k uživatelům
  - Hardening a testování e-mailové infrastruktury
  - Vhodné anti-phishingové nástroje
  - Pozor na další kanály (telefon, SMS, Teams…)


BMW

- Striktní oddělení wifi pro hosty
- Hardening a pravidelné patchování wifi sítí a prvků
- Aktivní monitoring Wifi a detekce Rouge AP
- Podpora moderních standardů WPA3
- Nepoužívat hesla
- Když už hesla, pak opravdu silná
- Pravidelné testování

- Nasazení moderního PACS a jeho správná konfigurace
- Výběr vhodných turniketů
- Vhodná architektura vstupních míst
- Nasazení odrazujících opatření
- Školení zaměstnanců
- Školení ostrahy a recepčních
- Aktivní monitoring citlivých oblastí
- Pravidelné testování


DT50
8GB




Network print accelerator
Do not disconnect!


Network print accelerator
Do not disconnect!
TOJ-6097-05

- Školení zaměstnanců příklady
  - Co je normální a co už ne
  - Rozpoznání kolegy
  - Šňůrky ke kartám NEJSOU marketingový předmět!
- Striktní nasazení kontroly připojeného HW do datové sítě
- Šifrovaná komunikace bez výjimky!
- Důsledná segmentace sítě
- Datové zásuvky nepatří do veřejných prostor
  - Pokud musí být, pak *extrémní* opatření
- Pravidelné testování


SAN Volume Controller
Storage Management (SSVC)
User name:
Password:
Log in
IBM.

Hewlett Packard Enterprise

iLO 4
ProLiant DL360 Gen9

Local User:
iLO Hostname:

Expand All

- Information
  - Overview
  - System Information
  - iLO Event Log
  - Integrated Management Log
  - Active Health System Log
  - Diagnostics
  - Location Discovery Services
  - Insight Agent
- iLO Federation
- Remote Console
- Virtual Media
- Power Management
- Network
- Remote Support
- Administration
  - Firmware
  - Licensing
  - User Administration
  - Access Settings
  - Security
  - Management
  - Key Manager
  - iLO Federation

User Administration

Local Users

Login Name	User Name
Administrator	Administrator
QBm7Z1NC	QBm7Z1NC

New

Directory Groups

Group	SID
Administrators	
Authenticated Users	S-1-5-11

New

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username         Domain  LM                                NTLM                              SHA1
--------         ------  --                                ----                              ----
S4009DC001$      CZ                                        acc1a6f8[redacted]                8a13ba13d0b3679[redacted]
czadm.novak      CZ      25bc1f4[redacted]b                bef1d4f5[redacted]                48c728c8aa1ab9d6[redacted]
czadm.vagner     CZ      b59bba3[redacted]b                c1afb3b8[redacted]                f91c6e9c542d969a[redacted]
czsvc_SCOMS_MSAA CZ      660d6fb[redacted]3                8b9f8ce8[redacted]                f3908287ec90f0b6[redacted]

wdigest credentials
===================

Username         Domain  Password
--------         ------  --------
(null)           (null)  (null)
S4009DC001$      CZ      64 c0 fa 4a 6c 4e 7a 9b 03 60 5b 7f 00 38 c7 bb 49 61 41 26 c4 84 9f 24 16 1f 4c 6b 33 ef dc 22 b9 e6 dc 2a db
2 13 fb 97 88 65 98 c0 85 f4 0b ad 59 f9 e8 82 b5 fb 53 bb eb a5 2f 9c 03 a9 2f 0d db 32 1c 45 0f 39 f2 e8 c4 92 08 74 a4 f9 a8 b1 20 69
5 0a fb d3 f2 70 61 d7 d7 7f c9 77 60 53 d6 e6 3b 23 b7 05 32 9d 3d d4 96 65 b8 d1 c1 27 26 84 7b f2 40 39 ac ee e0 0f 36 4c 50 08 d8 52
9 dd aa f8 b3 d9 11 1a f5 5a 0b 1c 81 72 9e 90 78 dc
[redacted]       CZ      [redacted]
czadm.vagner     CZ
czsvc_SCOMS_MSAA CZ

tspkg credentials
=================

Username         Domain  Password
--------         ------  --------
czadm.novak      CZ      [redacted]
czadm.vagner     CZ      [redacted]
```

- SSDLC & DevSecOps & Zero Trust
- Školení & awareness raising
- Hardening
  - AD je by design zranitelné a SPOF!
- Segmentace sítě
- Patch management
- Honeypoty
- Monitoring, SOC
- Penetrační testování
  - Aplikace
  - Infrastruktura
  - Síť
- Pravidelná Red teamingová cvičení
- A mnoho dalšího …

Falešný **POCIT BEZPEČÍ**

Mentální **připravenost**

NEADEKVÁTNÍ stav **IT prostředí**

Nedostatečná podpora VEDENÍ

Díky za pozornost

UNICORN