

**|VIAVIS|** střežíme podstatné

**CACIO**

S hackery se nevyjednává?

Vladimír Lazecký

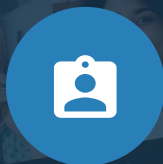
Jan Bonczek

# Úrodný rok 2021

Naše zkušenost – bez nároku na generalizaci



Dramatický nárůst útoků



99% z nich využilo zranitelností



V 50% případů bylo nutno vyjednávat

# V čem jsou útočníci dobří

## Exploitace a obcházení AV

Jsou dobří ve zneužívání zranitelností a v tom jak obejít AV.

## Eskalace privilegií

Jsou velice dobří v tom jak získat domain admin přístup.

## Mazání záloh

Zaměřují se na mazání a šifrování záloh.

## Rychlost

Vše zvládnou velice rychle.



# Příklad první

# Magistrát města Olomouc

## Kyberútok na olomoucký magistrát, agendy úřadů jsou mimo provoz

7.4.2021



Michal Kovář



Daniela Tauberová



Datové systémy olomouckého magistrátu napadli ve středu ráno hackeři. Kybernetický útok byl podle radnice velmi silný a navíc přišel v den, kdy chodí na úřad více lidí. Agendy byly po celý den mimo provoz.



Budova olomouckého magistrátu v Hynaisově ulici | Foto: DENÍK

# Magistrát města Olomouc



Statutární město Olomouc

26. dubna v 16:39 · 🌐



## 1 Magistrát funguje. 2 Hackeři znovu útočili

👉 Dva a půl týdne od začátku kybernetického útoku jsou veřejnosti k dispozici služby téměř všech agend magistrátu. Výjimkou je zatím živnostenský úřad, ale na zprovoznění jeho agendy se intenzivně pracuje. V případě některých odborů, jako je majetkoprávní, stavební, životního prostředí, dopravy či místní zeleně a odpadového hospodářství, zatím neběží plnohodnotně softwarová podpora. Vyřizování příslušné žádosti může proto být v některých případech zdlouhavější. IT specialisté pracují na tom, aby bylo fungování magistrátní digitální infrastruktury a všech speciálních aplikací každým dnem lepší, rychlejší a bezpečnější.

👉 O víkendu došlo také k útoku na webové stránky města, kdy stejná hackerská skupina cíleně útočila na webové servery s cílem eliminovat jejich dostupnost. IT tým útok rychle odhalil, provedl protipatření, a preventivně příslušné servery odstavil. Webové portály budou zatím omezeny co do funkčnosti. Podle odborníků se jednalo o jiný typ útoku – tzv. DDoS, k němuž se ale hlásí stejná skupina útočníků – dle jejího vyjádření jde o mstu za obnovení infrastruktury vlastními silami, aniž by město útočníkům platilo požadované výkupné.





### New companies

FEBANCOLOMBIA

Next update: 4 Days 22 : 31 : 40

DDOS

Cube Audit Ltd

Next update: 4 Days 22 : 11 : 11

DDOS

Halwani Bros Ltd

Next update: 4 Days 23 : 19 : 33

DDOS

Rate Rabbit Inc

Next update: 4 Days 23 : 11 : 11

DDOS

JetSJ

Next update: 4 Days 23 : 04 : 21

DDOS

Maryan beachwear group GmbH

Next update: 4 Days 22 : 50 : 34

DDOS

360 InStore

Next update: 4 Days 22 : 23 : 08

Company:

Address:

Website:

Email:

Phone:

Files:

[REDACTED]

[REDACTED] Czech Republic

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].7z 165.64 MiB

[REDACTED].mp.zip.003 1000 MiB

[REDACTED].mp.zip.002 1000 MiB

[REDACTED].mp.zip.005 1000 MiB

[REDACTED].mp.zip.001 1000 MiB

[REDACTED].mp.zip.004 1000 MiB

[REDACTED].mp.zip.008 1000 MiB

[REDACTED].mp.zip.006 1000 MiB

[REDACTED].mp.zip.007 1000 MiB

### Full dumps

TAIWAN SURFACE MOUNTING TECHNOLOGY CORP.

Published data: 125.25 GiB

Cinov Federation

Published data: 22.98 GiB

Glasbau Wiedemann GmbH

Published data: 58.58 GiB

Cocal

Published data: 114.03 MiB

SPINE & DISC

Published data: 2.19 GiB

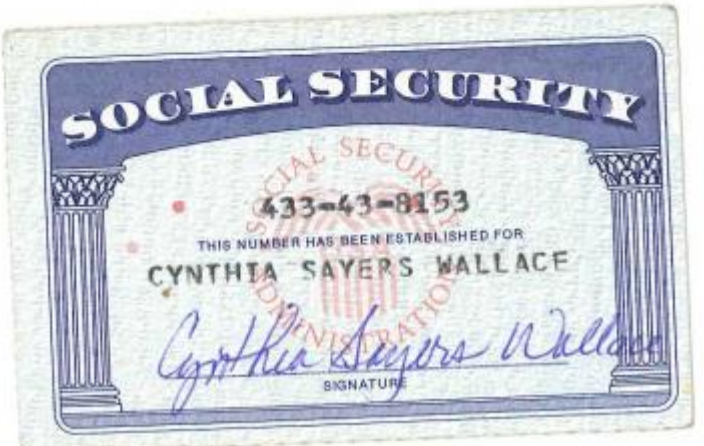
EUROMAIS - PEÇAS E PNEUS, LDA

Published data: 21.39 GiB

Schepisi Communications

Published data: 2.88 GiB

# CEO TAX, SOCIAL SECURITY NUMBER + DRIVER LICENSE



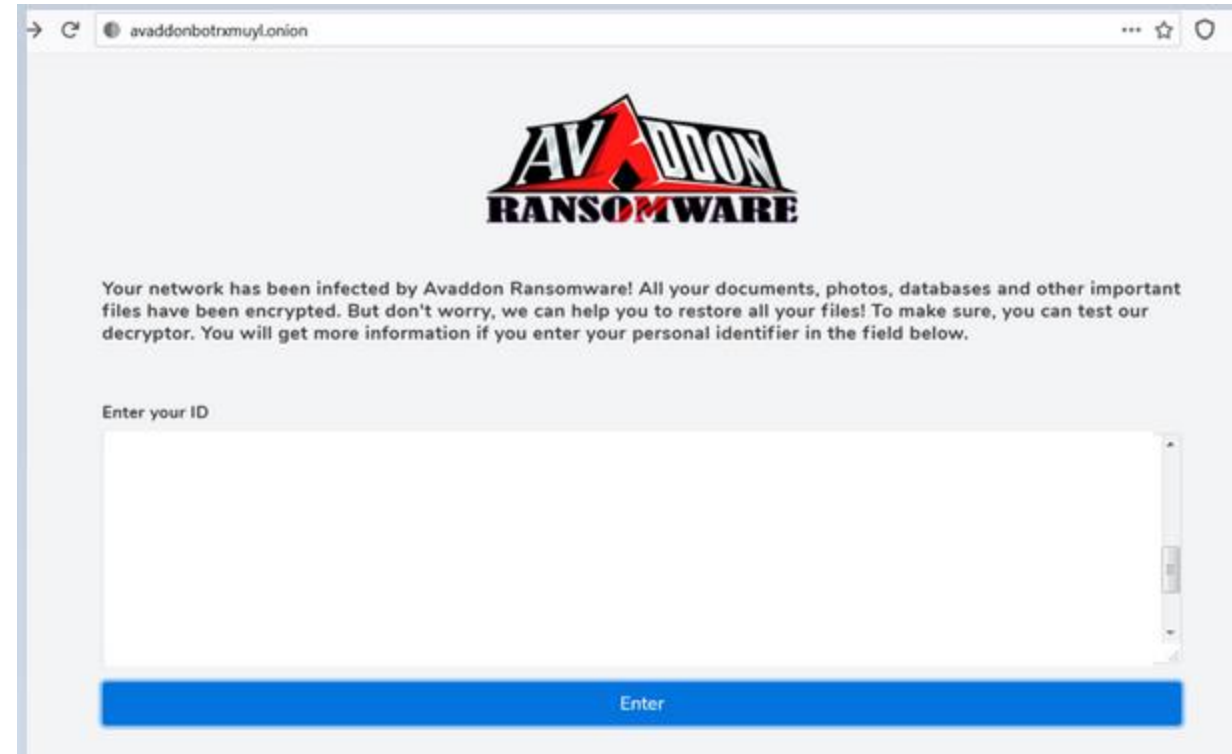
Ejercicio: 2018

Cuenta	Contrapartida	Comentario	Debe	Haber	Saldo
<b>DETERIORAMIENTO PARCELA (1296242CG7819N0000XX)</b>					
27	69100010015	DETERIORAMIENTO TERRENOS I BIENES NATURA		71860,84	-71860,84
27	79100010015	REVERSION TERRENOS Y BIENES NATURALES	5282,18		-66578,66
29		Cierre contabilidad 2017	66.578,66		
<b>tos ...</b>			<b>71.860,84</b>	<b>71.860,84</b>	
<b>DETERIORAMIENTO PARCELA (1296248CG7819N0000UX)</b>					
27	69100010015	DETERIORAMIENTO TERRENOS I BIENES NATURA		51462,94	-51462,94
27	79100010015	REVERSION TERRENOS Y BIENES NATURALES	3585,94		-47877
29		Cierre contabilidad 2017	47.877,00		
<b>tos ...</b>			<b>51.462,94</b>	<b>51.462,94</b>	
<b>DETERIORAMIENTO PARCELA (1296249CG7819N0000HX)</b>					
27	69100010015	DETERIORAMIENTO TERRENOS I BIENES NATURA		51223,86	-51223,86
27	79100010015	REVERSION TERRENOS Y BIENES NATURALES	3566,57		-47657,29
29		Cierre contabilidad 2017	47.657,29		
<b>Suma Movimientos ...</b>			<b>51.223,86</b>	<b>51.223,86</b>	
<b>291000000158 DETERIORAMIENTO PARCELA (1296250CG7819N00000ZX)</b>					
01/01/2017	27	69100010015		51974,89	-51974,89
31/12/2017	27	79100010015	3547,22		-48427,67
31/12/2017	29		48.427,67		
<b>Suma Movimientos ...</b>			<b>51.974,89</b>	<b>51.974,89</b>	
<b>291000000159 DETERIORAMIENTO PARCELA (1296241CG7819N0000DX)</b>					
01/01/2017	27	69100010015		69967,28	-69967,28
31/12/2017	27	79100010015	5062,88		-64904,4
31/12/2017	29		64.904,40		
<b>Suma Movimientos ...</b>			<b>69.967,28</b>	<b>69.967,28</b>	
<b>291000000160 DETERIORAMIENTO PARCELA (1296243CG7819N0000IX)</b>					
01/01/2017	27	69100010016		73987,61	-73987,61
31/12/2017	27	79100010016			



# Vyjednávání s útočníky

```
----- Your network has been infected! -----
***** DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED *****
All your documents, photos, databases and other important files have been encrypted and have the extension: .beDBDd
You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!
The only way to restore your files is to buy our special software. Only we can give you this software and only we c
restore your files!
We have also downloaded a lot of private data from your network.
If you do not contact as in a 3 days we will post information about your breach on our public news website
(avaddongun7ngel.onion) and after 7 days the whole downloaded info.
You can get more information on our page, which is located in a Tor hidden network.
How to get to our page
-----
|
| 1. Download Tor browser - https://www.torproject.org/
|
| 2. Install Tor browser
|
| 3. Open link in Tor browser - avaddonbotrxmuy1.onion
|
| 4. Follow the instructions on this page
|
-----
Your ID:
```



# Jak to dopadlo

## Windows zašifrované

Windows zašifrované. Linuxy přežily.

## Výkupné nezaplaceno

Požadováno 100 000 dolarů.

## Následovaly DDoS

Jako pomsta za nezaplacení následoval dlouhotrvající DDoS.

## Napadení webového serveru

Exploitace a smazání.

## Zveřejnění dat

Byla zveřejněna ukradená data.



# Příklad druhý



# Centrální konzole AV

## Endpoint Protection - Dashboard

[Overview](#) / [Endpoint Protection Dashboard](#)

Help  
Central Demo

### Recent threat graphs

[Sophos generated](#) | [Admin generated](#)

**i** As an MTR customer, these graphs are for information only for all devices with an MTR assigned license. Our MTR team will contact you if you need to take action.

Time created	Priority	Name	User	Device
Oct 16, 2021 7:20 AM	High	CryptoGuard	Frank Castle	Win7-desktop-3
Oct 16, 2021 6:32 AM	Medium	PrivGuard	Frank Castle	Win7-desktop-3
Oct 16, 2021 5:46 AM	Medium	CodeCave	Frank Castle	Win7-desktop-3
Oct 16, 2021 1:49 AM	Medium	ATK/Shellter-B	Frank Castle	Win7-desktop-3
Oct 16, 2021 12:56 AM	Medium	HeapHeapProtect	Frank Castle	Win7-desktop-3

## Threat Analysis Center - CryptoGuard

[Overview](#) / [Threat Analysis Center Dashboard](#) / [Threat Graphs](#) / [CryptoGuard](#)

Help  
Central Demo Sophos In



Win7-desktop-3  
10.108.209.253



Root Cause  
Outlook



Beacon  
e33dj3o.exe



Detected  
Oct 16, 2021 7:18 AM



Clean

Summary

Suggested next steps

# Analýza OS

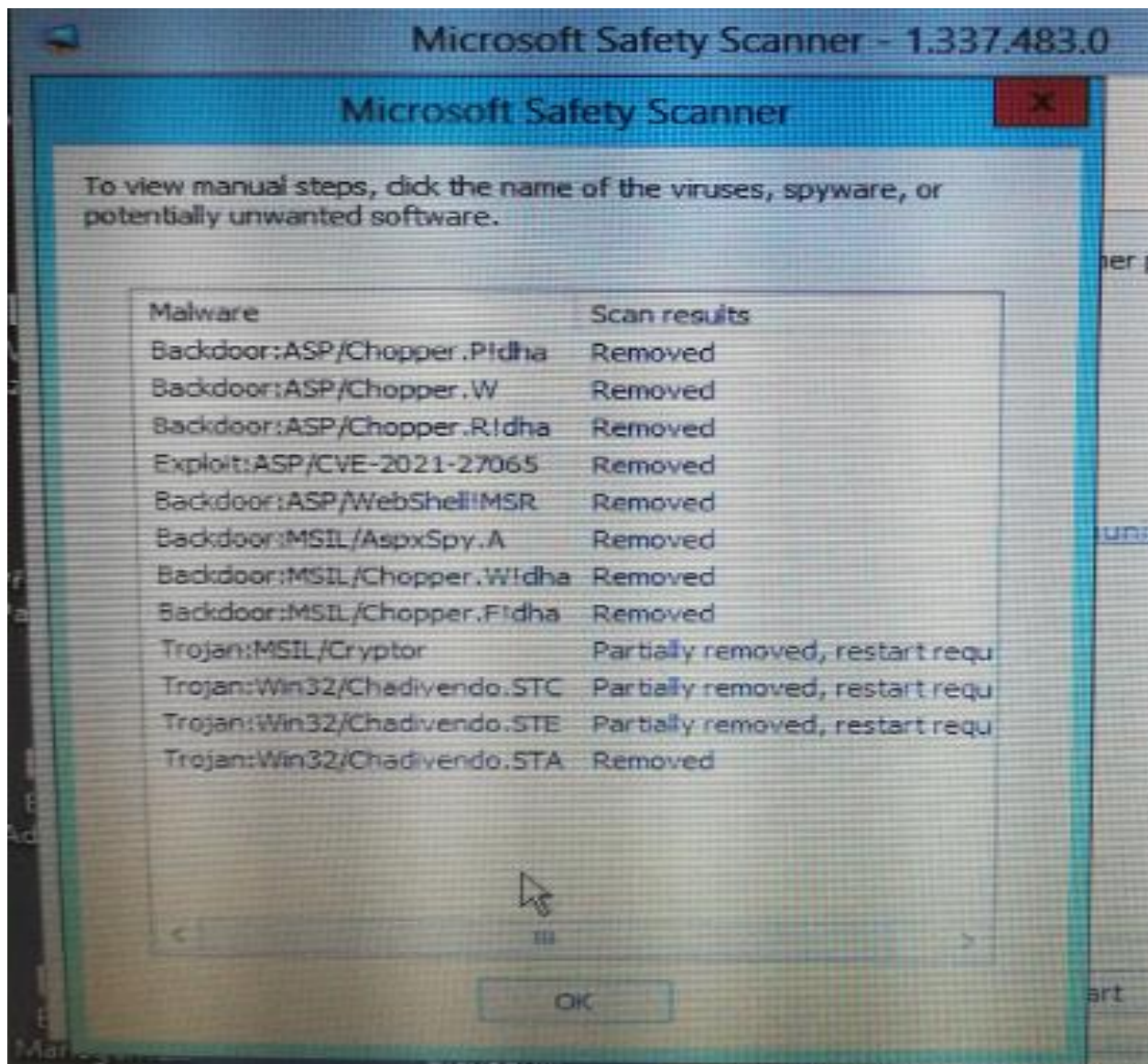
4-04-2021 - VMware Remote Console

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Users\administrato[REDACTED] cd .\Desktop
PS C:\Users\administrato[REDACTED]esktop> cd e:
PS E:\> .\Test-ProxyLogon.ps1.txt -OutPath $home\desktop\logs
PS E:\> .\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
ProxyLogon Status: Exchange Server [REDACTED]
Log age days: Oabgen 59,5 Ecp 43,7 Nutod 59,7 Eas 59,7 EcpProxy 45,9 Ews 59,7 Mapi 49,5 Oab 45,9 Owa 59,
PowerShell 59,7 RpcHttp 59,7
Report exported to: C:\Users\administrato[REDACTED]ktop\logs[REDACTED]ogAgeDays.csv
[CVE-2021-26855] Suspicious activity found in Http Proxy log!
Report exported to: C:\Users\administrato[REDACTED]esktop\logs[REDACTED]ve-2021-26855.csv

PS E:\> _
```

# Analýza OS



# Analýza komunikace

47	[REDACTED]	11:27	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	22.2 KB/20.0 KB	[REDACTED]
48	[REDACTED]	11:25	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	21.2 KB/19.1 KB	[REDACTED]
49	[REDACTED]	11:23	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	20.2 KB/18.1 KB	[REDACTED]
50	[REDACTED]	11:21	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	19.2 KB/17.2 KB	[REDACTED]
51	[REDACTED]	11:19	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	18.1 KB/16.3 KB	[REDACTED]
52	[REDACTED]	11:17	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	17.1 KB/15.3 KB	[REDACTED]
53	[REDACTED]	11:15	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	16.1 KB/14.4 KB	[REDACTED]
54	[REDACTED]	11:13	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	15.1 KB/13.4 KB	[REDACTED]
55	[REDACTED]	11:11	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	14.1 KB/12.5 KB	[REDACTED]
56	[REDACTED]	11:09	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	13.1 KB/11.6 KB	[REDACTED]
57	[REDACTED]	11:07	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	12.1 KB/10.6 KB	[REDACTED]
58	[REDACTED]	11:05	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	11.0 KB/9.7 KB	[REDACTED]
59	[REDACTED]	11:03	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	10.0 KB/8.8 KB	[REDACTED]
60	[REDACTED]	11:01	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	9.0 KB/7.8 KB	[REDACTED]
61	[REDACTED]	10:59	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	8.0 KB/6.9 KB	[REDACTED]
62	[REDACTED]	10:57	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	7.0 KB/5.9 KB	[REDACTED]
63	[REDACTED]	10:55	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	6.0 KB/5.0 KB	[REDACTED]
64	[REDACTED]	10:53	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	4.9 KB/4.1 KB	[REDACTED]
65	[REDACTED]	10:51	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	3.9 KB/3.1 KB	[REDACTED]
66	[REDACTED]	10:49	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	2.9 KB/2.2 KB	[REDACTED]
67	[REDACTED]	10:47	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	1.9 KB/1.3 KB	[REDACTED]
68	[REDACTED]	10:45	FC	[REDACTED]	9706	✓	[REDACTED]	[REDACTED]	HTTP	HTTP	904.0 B/332.0 B	[REDACTED]

**Destination**

- Country: Singapore
- End User ID: 0
- Endpoint ID: 101
- IP: [REDACTED]
- Interface: WAN1
- Interface Role: undefined
- Port: 80

**Action**

- Action: ✓
- Firewall Action: ✓ accept
- Policy ID: [REDACTED]
- Policy UUID: [REDACTED]

**Application**

- Application: HTTP
- Application Category: unknown
- Application Control List: block-nonprod-im-file-transfer
- Protocol: 6
- Service: HTTP

**Data**

- Duration: 243 seconds
- Received Packets: [REDACTED]
- Sent Packets: [REDACTED]
- Sent/Received: [REDACTED]

**Type**

- Sub Type: forward

# Jak to dopadlo

## Vše zašifrované

Windows zašifrované. Linuxy smazané.

## Technologická síť přežila

Uživatelská doména posloužila jako honeypot.

## Zaplacení výkupného

Zaplaceno 1,5 BTC.

## Existovala druhá lokalita

V době útoku byla téměř připravena nová serverovna.

## 18 TB dat

V době útoku nebyly dostupné SSD.



# Co s tím?

## Důsledná segmentace

Přístup všude jen na základě nutného minima.

## Řídit vzdálené přístupy

Více faktorová autentizace je „must have“.

## Zálohy

Co je doma, to se počítá.

## Za všechno může uživatel?

Platí i pro IT. Bez kvalitních lidí na IT pozici to nepůjde.

# Útoky z pohledu managementu

❓ Uspěl management?

- Formální/reálná připravenost
- Zvyšování časového stresu
- Řešení nepodstatných problémů

# Veselé příhody z natáčení



„Jak dlouho budeme obnovovat? Hmm, to raději zaplatíme...“



„Může za to informatika, potrestáme je. Zkrátíme jim rozpočet...“



„Tak dáme zálohy do cloudu, nemůže se nic stát... “



Poslední vlna útoku

# Workshop – jak zvládnout kyber útok

Simulace reálného útoku

Tým managementu a tým IT

Reakce na jednotlivé fáze a vlny útoku



## Co si odnesete

Jak řešit situace, o kterých se nedočtete



## Ukázka pro CACIO

14.4.2022

Registrace: [jan.heisler@cacio.cz](mailto:jan.heisler@cacio.cz)

Prostor pro vaše dotazy...

## Děkujeme za pozornost

Za tým VIAVIS a.s.

- Jan Bonczek
- Vladimír Lazecký