Kybernetická bezpečnost

VIAVIS střežíme podstatné

Ing. Jan Bonczek

Konzultant v oblasti kybernetické bezpečnosti
Etický hacker

Dnešní témata

Z praxe

30 minut

Co je dobré znát?

Zdroj: https://www.youtube.com/watch?v=u8qgehH3kEQ

Motivace útočníků

Testování obranyschopnosti

První kybernetická zbraň, útoky státu na stát v rámci tajných služeb nebo odplaty. Příprava na kyberrnetickou válku

Finanční motivace

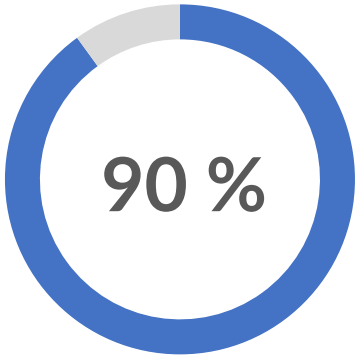
Vydírání, krádeže informací a know how, útoky na konkurenci.

Pomsta, zábava a další

Propuštění zaměstnanci, nespokojení klienti, naštvaný podřízený. Člověk kterého to pouze baví a další.

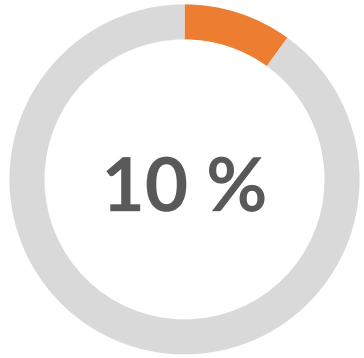
Kdo je útočník?

Jak?



Phishing

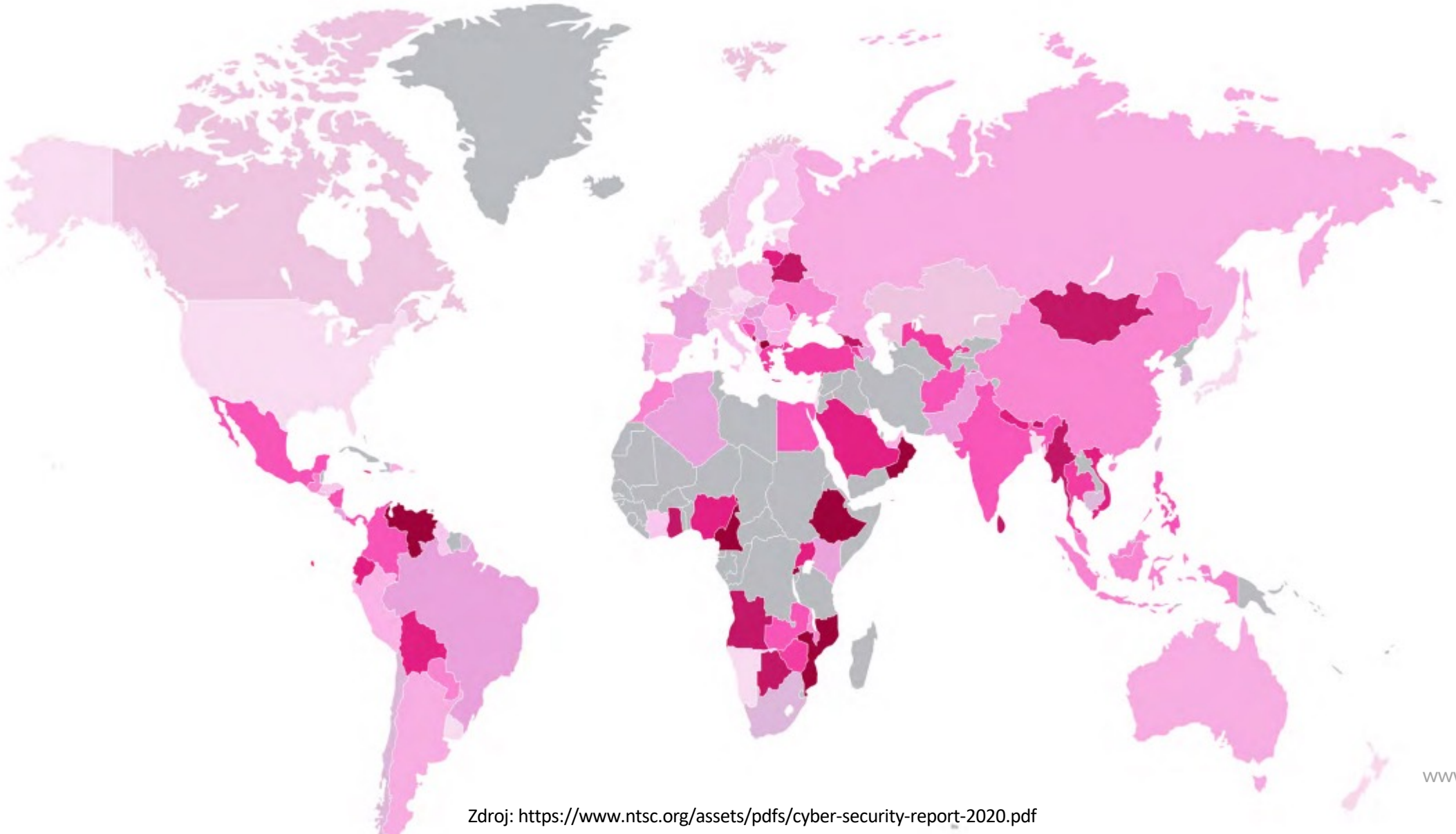
E-maily, „flešky“, vydávání se za…, malware,



Vulnerabilities

Exchange, Fortinet, F5, WatsApp, Android, iOS,

Odkud?



Zdroj: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

Problémy obránce a útočníka

- Pouze technické prostředky a vybavení nestačí
- Bezpečnost nejde vidět

Proč řešíme kybernetickou bezpečnost

- Právní předpisy
- Ochrana dobrého jména a pověsti
- Ochrana zdraví a životů
- Vydíratelnost
- Ochrana firemního know how
- Ochrana vlastního soukromí a majetku

Pár případů, kdy se to nepovedlo

Emotet

Kyberútok v benešovské nemocnici: podle policie nešlo o vydírání, oprava potrvá nejméně do pátku

Benešovská nemocnice bude fungovat v omezeném režimu nejméně do pátku. IT specialisté v pondělí v poledne začali znovu instalovat všechny servery a koncové IT stanice napadené počítačovým virem. Většinu zálohovaných dat nemocnice zřejmě bude možné obnovit. Policie v pondělí uvedla, že útok nebyl vyděračský a nešlo o výkupné, vyšetřování pokračuje. Chod bude nemocnice podle hejtmanky Jaroslavy Pokorné Jermanové (ANO) obnovovat pomalu a postupně.

Praha 16:48 16. prosince 2019

ZPRÁVY, KTERÉ JSTE NEČETLI

Kdo podle Filipa napadl nemocnici v Benešově? ‚Nejen Milion chvilek. Prostě ti, kteří to zorganizovali'

Snímky Nabarvené ptáče a Dcera se dostaly do užších nominací na Ceny Akademie

Emotet

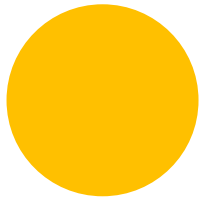
Phishingový e-mail

**Šíření, extrakce dat,
krádeže credentials.**

Napadení uživatelského PC

Mazání záloh a stop

Ransomware



Ransomware

Make a type specimen book unknown printer took type and scrambled it to make a type specimen book

Z praxe

Limity

- Právní předpisy
- Peníze a čas
- Morálka
- Metodiky
- Reporty
- Držíte se scénáře

Oblasti PT

Externí PT

Interní PT

Socio PT

Etapy penetračních testů

- Pre-attack, T+7
- Attack, T+28
- Post-attack, T+35

Etapy hackování

- Skenování
- Získání přístupu
- Udržení přístupu
- Čištění stop, destrukce

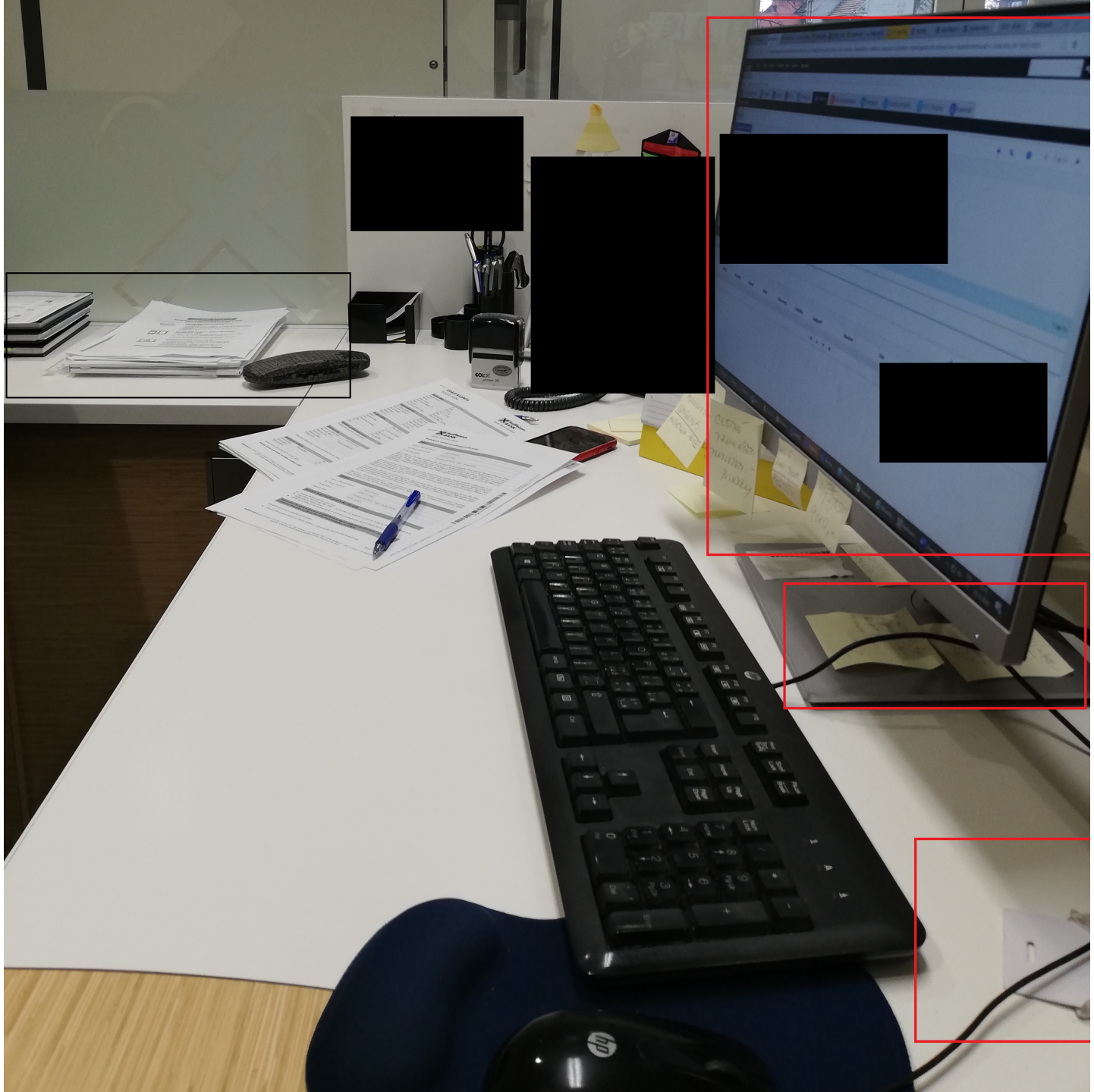
- Etický hacker simuluje techniky používané útočníky k nalezení exploitovatelných zranitelností.

https://twitter.com/thecrazyprogrmr/status/664378844393046016/photo/1

Pátek 6. března

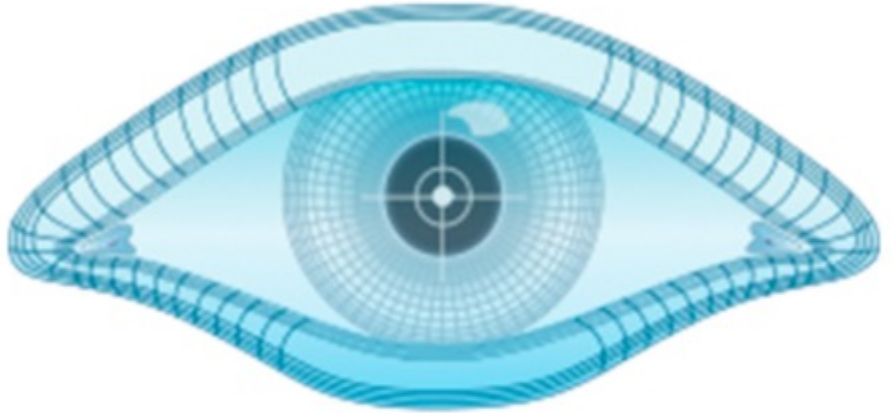
- https://www.ceskatelevize.cz/porady/10095426857-interview-ct
- https://www.ceskatelevize.cz/porady/10101491767-studio-ct24


SLOUČÍM SI PŮJČ...
A ROZLOUČÍM SE
S VYSOKÝMI ÚROKY



Nejběžnější nástroje

- NMAP
- Google Hacking
- Shodan
- Binaryedge
- dnsdumpster
- Whois
- Maltego



NMAP

MALTEGO

Google Transparency Report

Whois
Identity for everyone

OSINT Framework

SHODAN

Jak nám hackli ministerstvo?

Last Detected	2020-12-23T15:26:14.349000
Link	https://91.214.157.10/owa/auth/logon.aspx?url=https%3a%2f%2f91.214.157.10%2fowa%2f&reason=0
HTTP Status	**200 OK**
Title	Outlook

Body Hash (web.body.sha256): 36ada3460352992441a88daa86693369d088bbd5bcd49a2787ed235d40a32c5d

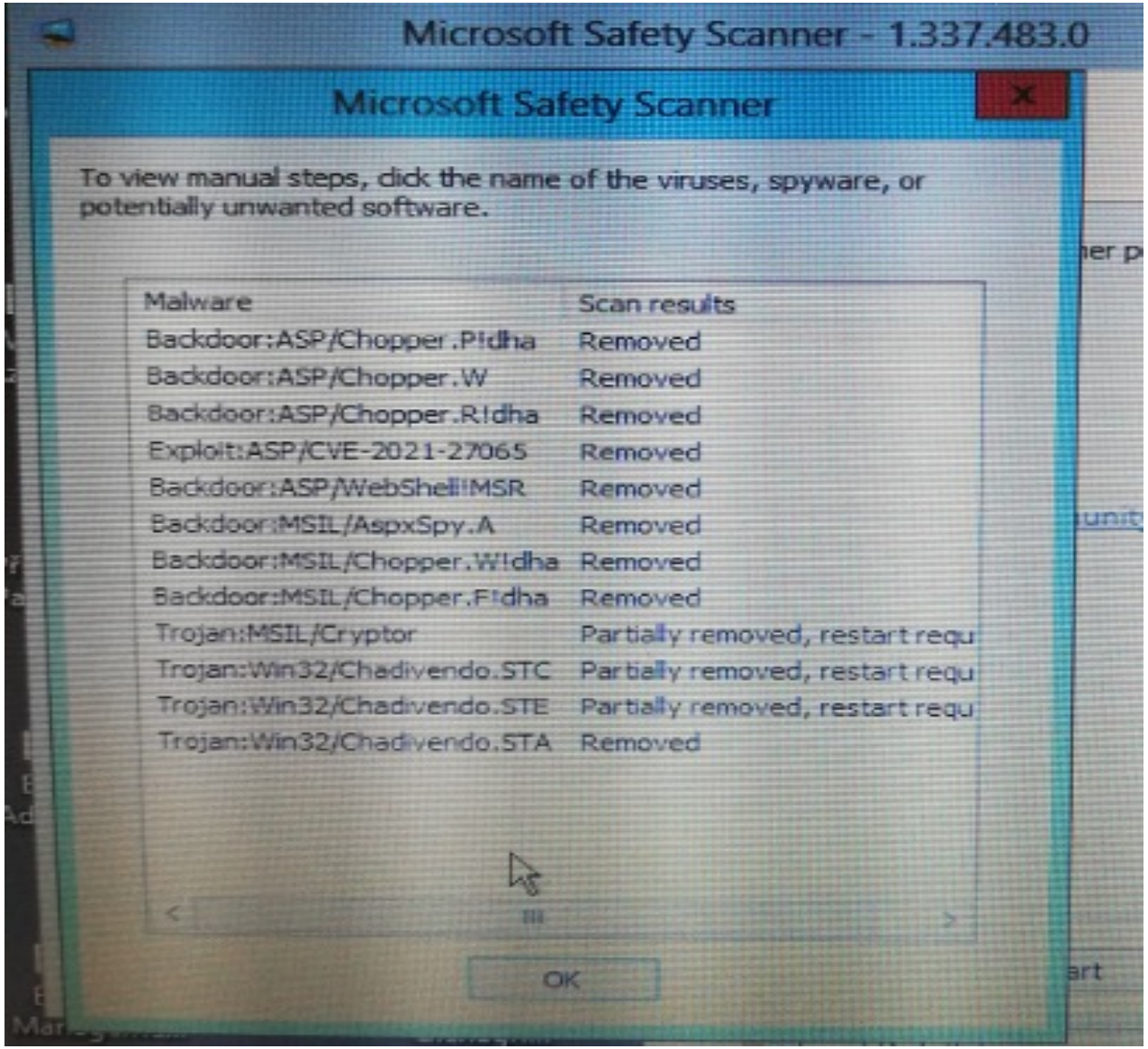
web.body.content:

```
 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<!-- Copyright (c) 2011 Microsoft Corporation.  All rights reserved. -->
<!-- OwaPage = ASP.auth_logon_aspx -->

<!-- {57A118C6-2DA9-419d-BE9A-F92B0F9A418B} -->
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=10" />
<link rel="shortcut icon" href="/owa/auth/15.1.1779/themes/resources/favicon.ico" type="image/x-icon">
<meta http-equiv="Content-Type" content="text/html; CHARSET=utf-8">
<meta name="Robots" content="NOINDEX, NOFOLLOW">
<title>Outlook</title>
<style>
@font-face {
    font-family: "wf_segoe-ui_normal";
    src: url("/owa/auth/15.1.1779/themes/resources/segoeui-regular.eot?#iefix") format("embedded-opentype"),
         url("/owa/auth/15.1.1779/themes/resources/segoeui-regular.ttf") format("truetype");
}
```

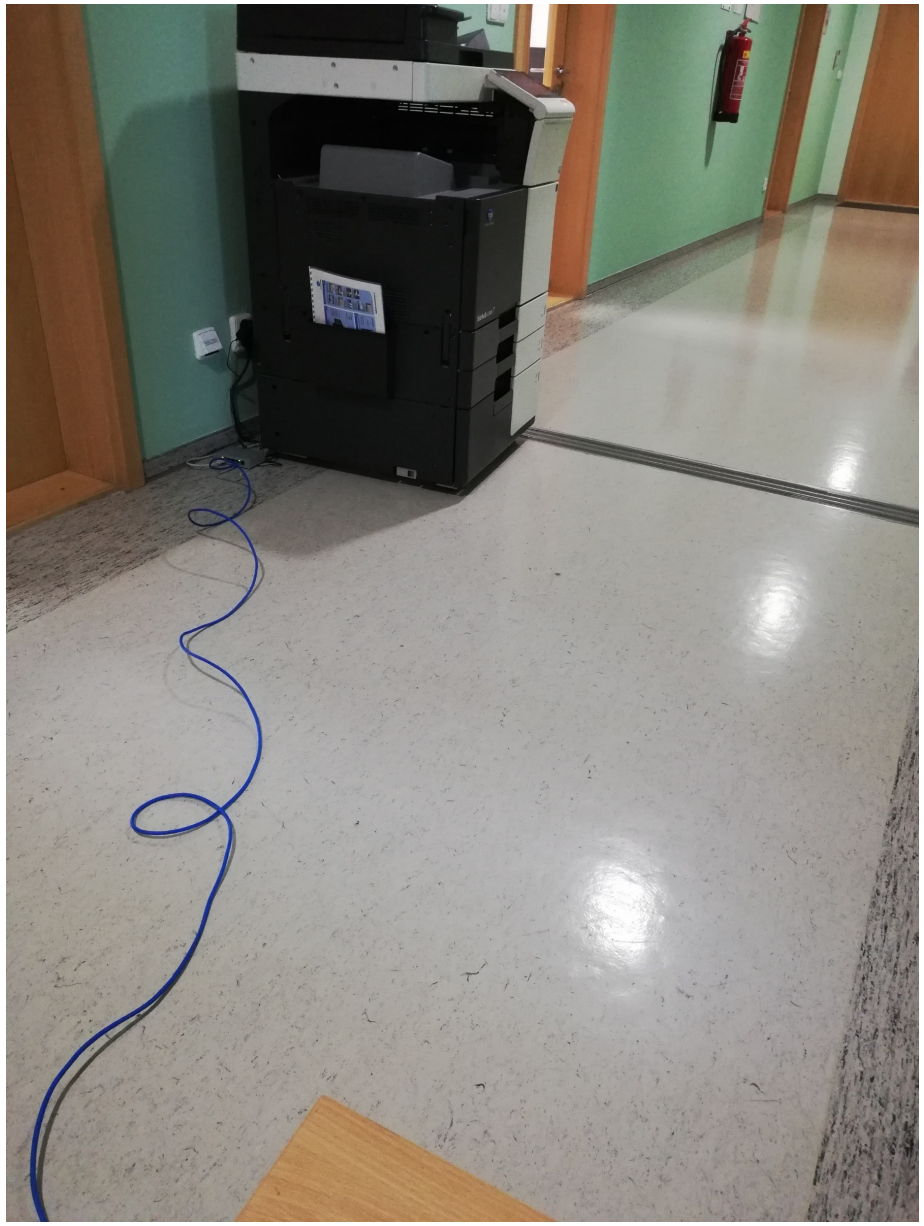
Technologické sítě a odposlechy

```
[*] 192.168.235.0/24:502  - Scanned  26 of 256 hosts (10% complete)
[+] 192.168.235.41:502    - 192.168.235.41:502 - MODBUS - received correct MODBUS/TCP
header (unit-ID: 1)
[+] 192.168.235.42:502    - 192.168.235.42:502 - MODBUS - received correct MODBUS/TCP
header (unit-ID: 1)
[+] 192.168.235.43:502    - 192.168.235.43:502 - MODBUS - received correct MODBUS/TCP
header (unit-ID: 1)
[+] 192.168.235.44:502    - 192.168.235.44:502 - MODBUS - received correct MODBUS/TCP
header (unit-ID: 1)
[+] 192.168.235.45:502    - 192.168.235.45:502 - MODBUS - received correct MODBUS/TCP
header (unit-ID: 1)
[+] 192.168.235.46:502    - 192.168.235.46:502 - MODBUS - received correct MODBUS/TCP
header (unit-ID: 1)
[+] 192.168.235.50:502    - 192.168.235.50:502 - MODBUS - received correct MODBUS/TCP
header (unit-ID: 1)
[+] 192.168.235.51:502    - 192.168.235.51:502 - MODBUS - received correct MODBUS/TCP
header (unit-ID: 1)
[*] 192.168.235.0/24:502  - Scanned  52 of 256 hosts (20% complete)
[*] 192.168.235.0/24:502  - Scanned  77 of 256 hosts (30% complete)
[*] 192.168.235.0/24:502  - Scanned 103 of 256 hosts (40% complete)
[*] 192.168.235.0/24:502  - Caught interrupt from the console...


Nmap scan report for 192.168.235.41
Host is up (0.012s latency).

PORT    STATE SERVICE
502/tcp open  modbus
| modbus-discover:
|   sid 0x1:
|     error: ILLEGAL FUNCTION
|_    Device identification: Schneider Electric TM258LF66DT4L V04.00.02.51
```

VIAVIS střežíme podstatné


Microsoft Safety Scanner - 1.337.483.0
Microsoft Safety Scanner
To view manual steps, dick the name of the viruses, spyware, or potentially unwanted software.
Malware
Scan results
Backdoor:ASP/Chopper.P!dha
Removed
Backdoor:ASP/Chopper.W
Removed
Backdoor:ASP/Chopper.R!dha
Removed
Exploit:ASP/CVE-2021-27065
Removed
Backdoor:ASP/WebShell!MSR
Removed
Backdoor:MSIL/AspxSpy.A
Removed
Backdoor:MSIL/Chopper.W!dha
Removed
Backdoor:MSIL/Chopper.F!dha
Removed
Trojan:MSIL/Cryptor
Partially removed, restart requ
Trojan:Win32/Chadivendo.STC
Partially removed, restart requ
Trojan:Win32/Chadivendo.STE
Partially removed, restart requ
Trojan:Win32/Chadivendo.STA
Removed
OK

Fyzický průnik



Odpověď: Zapojení zaměstnanců do rozvoje webové prezentace

MP [redacted]
Komu Zdeněk [redacted]

Odpovědět | Odpovědět všem | Přeposlat | ...

čt 05.11.2020 11:3

udělám přehled těch, co se ozvali a ty co byli osloveni a neozvou se zbijeme?

S pozdravem

Ing. Mi [redacted]
manažer kybernetické bezpečnosti

[redacted]

e-mail [redacted]
číslo datové schránky: [redacted]

Navštivte naše stránky na adrese:
[redacted]
sledujte nás na:
www.facebook.com [redacted]
zaregistrujte se do K [redacted] ce:
[redacted]

Email v karanténě

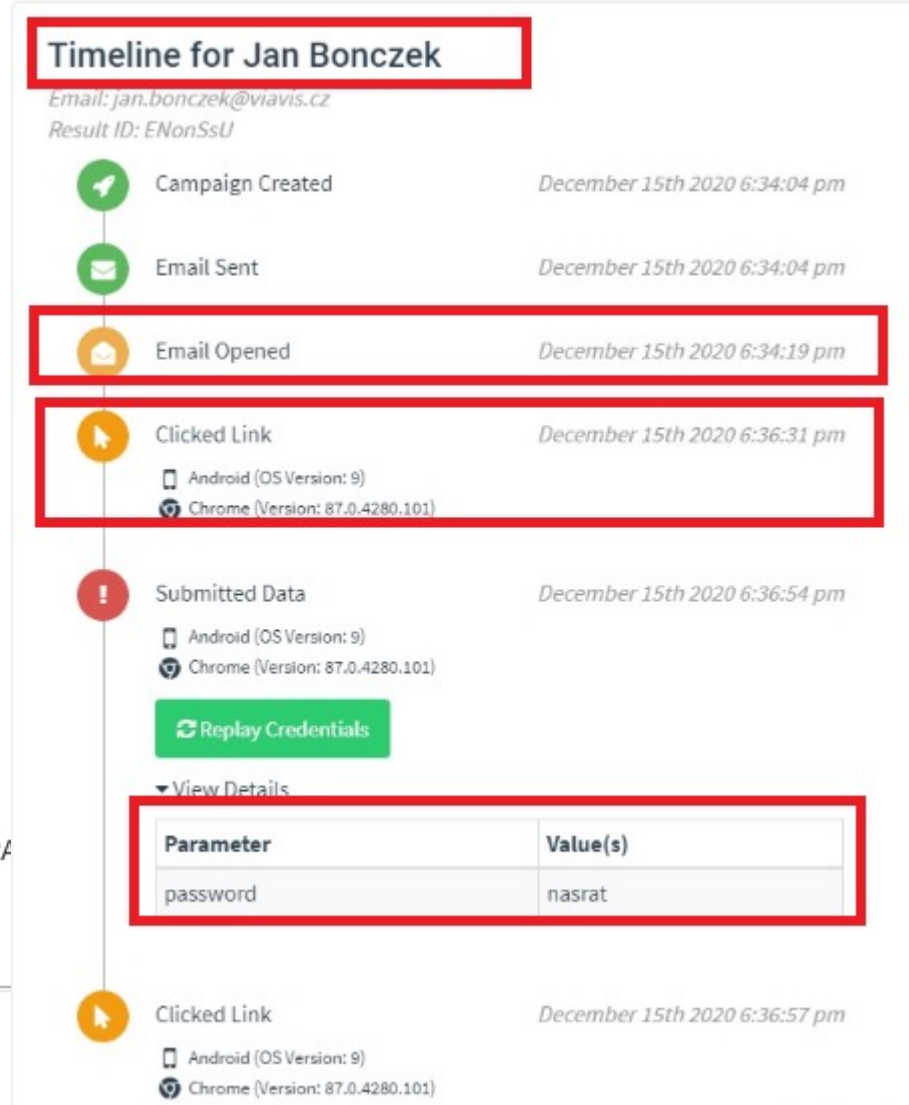
Antispamový filtr zařadil příchozí email do karantény na základě výsledku antivirové kontroly s výsledkem "SPA

Prosím potvrďte co se má s emailem stát:

SENDER: vavrova@zpskoda.cz - SUBJECT: 'XXX Prohlášení vedení pojišťovny k nouzovému stavu COVID-19'

DORUČIT EMAIL / SMAZAT EMAIL

Děkujeme,
odbor organizace a informačního systému



TeamViewer - dobrý sluha, ale špatný pán.

RE: Zapojení zaměstnanců do rozvoje webové prezentace

MV Michaela [redacted]
Komu [redacted]

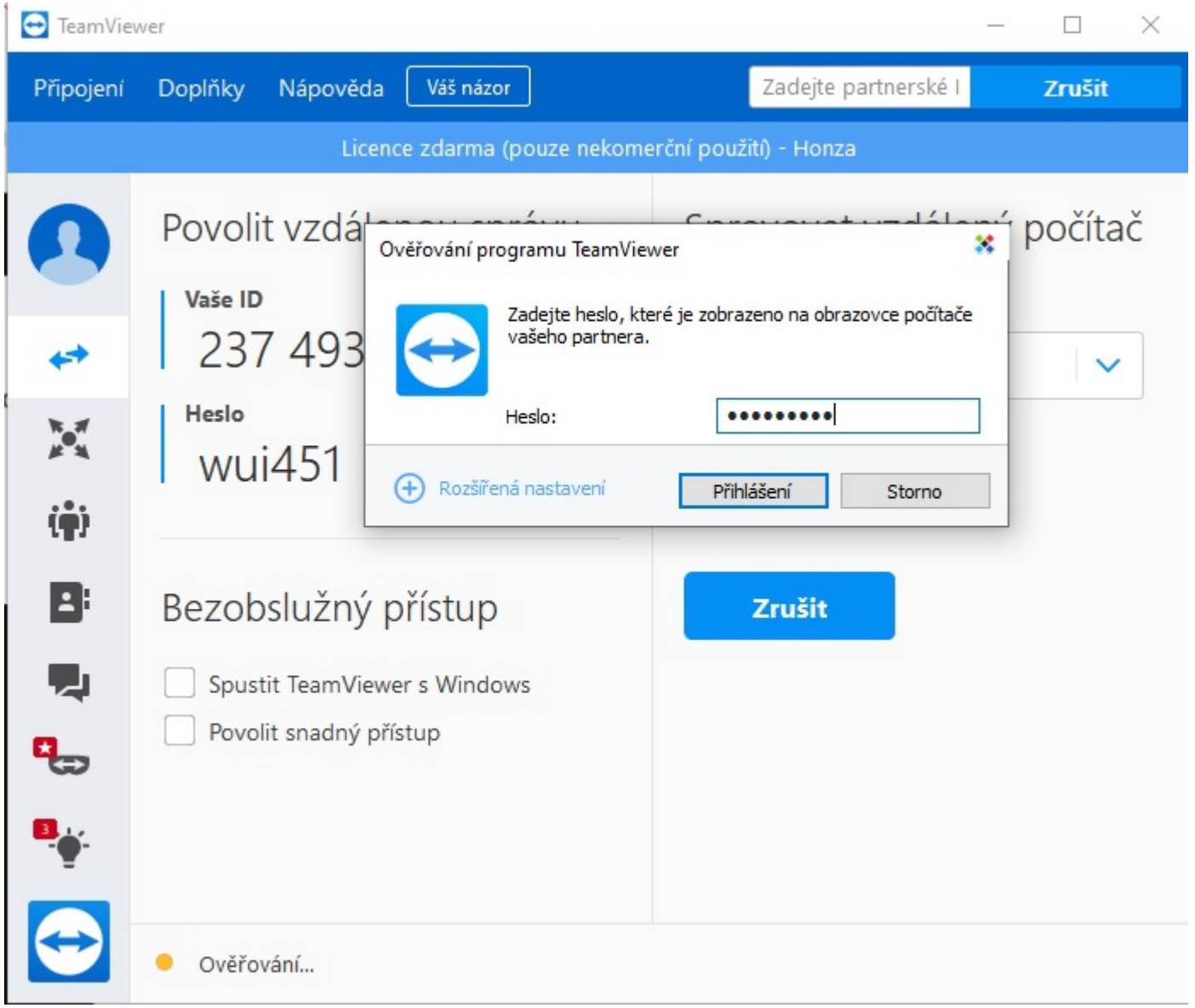
Dobrý den,

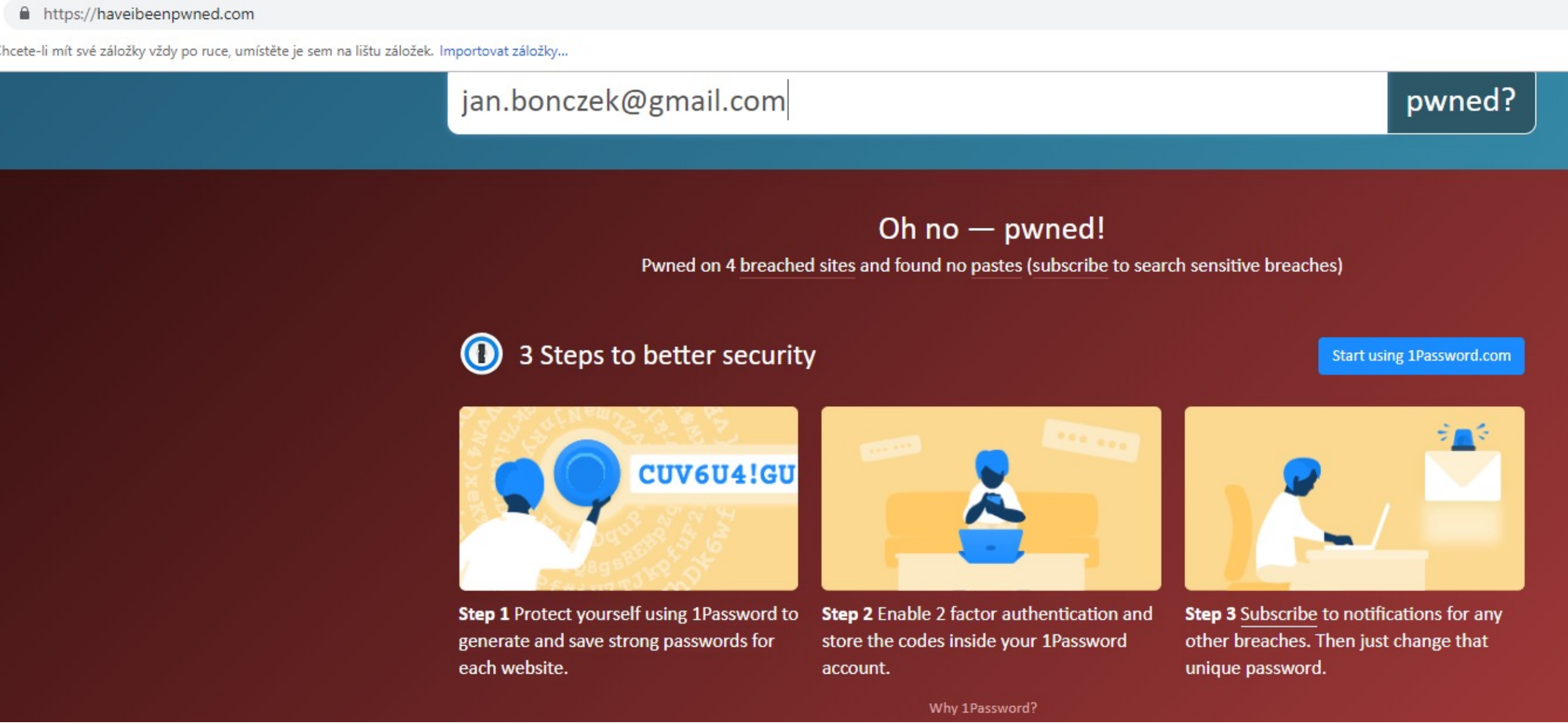
aplikaci teamviewer mám nainstalovanou. Můžete mě kontaktovat.

S přáním příjemného dne

Bc. Micha [redacted]
referent odd. [redacted]

[redacted]





- https://haveibeenpwned.com/

Vyzkoušejte si

955db0b81ef1989b4a4dfeae8061a9a6 inurl:sql

Vyzkoušejte si

- Jméno
- Adresa
- Počet dětí
- Výše dluhů
- Rodné číslo
- Jméno partnerky
- Vlastněné nemovitosti
- Osobní webové stránky
- Značka auta, stáří, barva, typ, cena

Úkoly

Najit exploit na kamery hikvision

MX servery pro doménu MPSV

Subdomény pro doménu MPSV

Jakou verzi exchagne používá MPSV