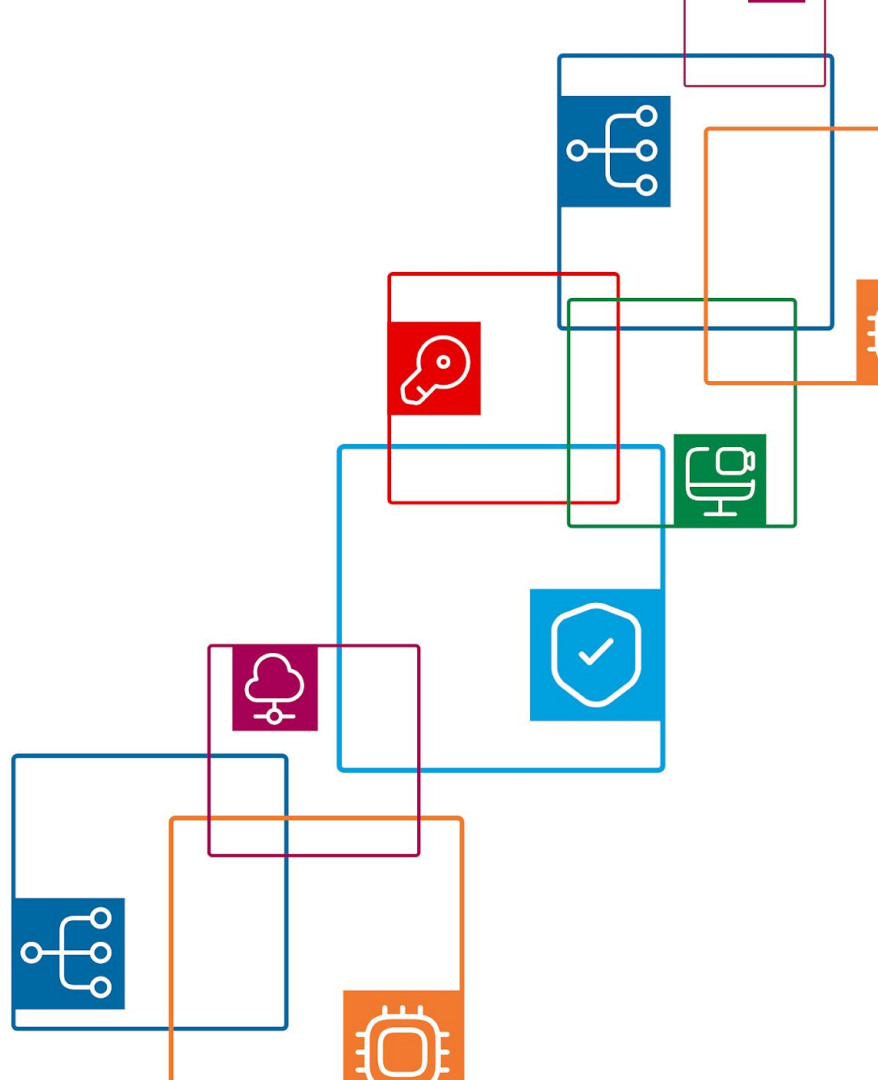




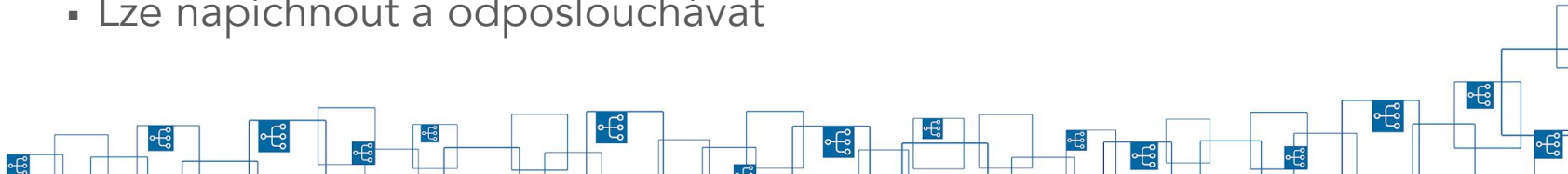
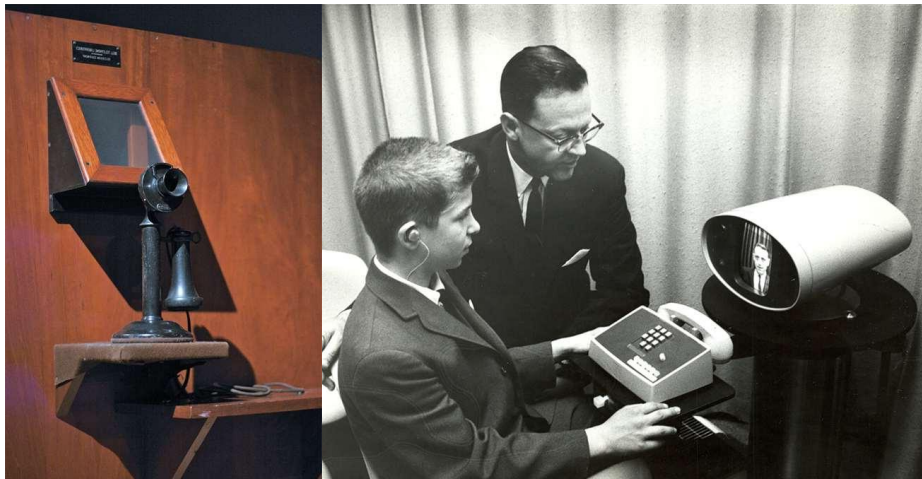
Co znamená bezpečnost v kontextu videokonferencí

Miloš Liška

Konference CESNET 1. 10. 2026



- Telefonní okruhy
 - 1927: AT&T úspěšně otestovalo přenos zvuku a obrázi mezi Washingtonem a New Yorkem.
 - 1964: AT&T Picturephone a veřejné videohovory.
- Bezpečnost? Žádná
 - Telefonní okruhy
 - Lze napíchnout a odposlouchávat



• Videokonference

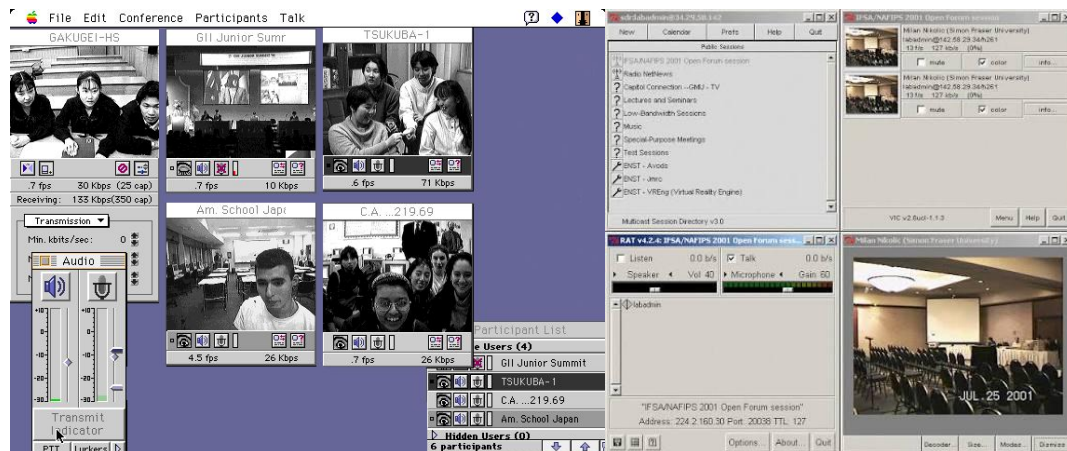
- 1992: Cu-SeeMe
- 1993: MBone Tools
- 1996: H.323 videokonference

• Bezpečnost?

- Nejprve žádná
- Videokonference byly spíše experiment a/nebo vyžadovaly výkonné a drahé vybavení

• Šifrování

- Prevence odposlechu
- Ve své době výpočetně velmi náročná úloha
- A taky neobratná – např., 3DES v MBone tools vyžadovalo ruční výměnu a zadávání klíčů



- Další vývoj
 - 00s: Videoconferencing stále spíše experiment
 - 10s: První rozšíření videokonferencí mezi běžné uživatele (Skype přidal podporu videa teprve v roce 2013)
- Softwarová bezpečnost
 - Skype samotný byl populární pro šíření virů
 - Později také snadný vektor pro šíření odkazů na malware
- Covid a po covidu
 - Videokonference najednou začali používat všichni
- A bezpečnost videokonferencí už je zásadní téma.



Meeting and risk
classification

Recommended
authentication measures

Unacceptable risk

Biometric
RBAC
ABAC
Deepfake prevention

High risk

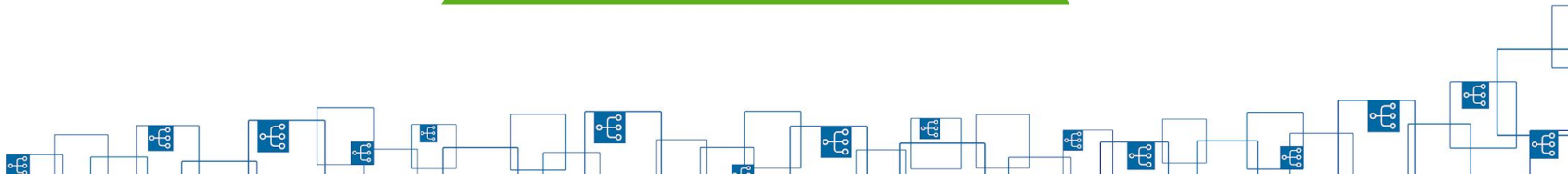
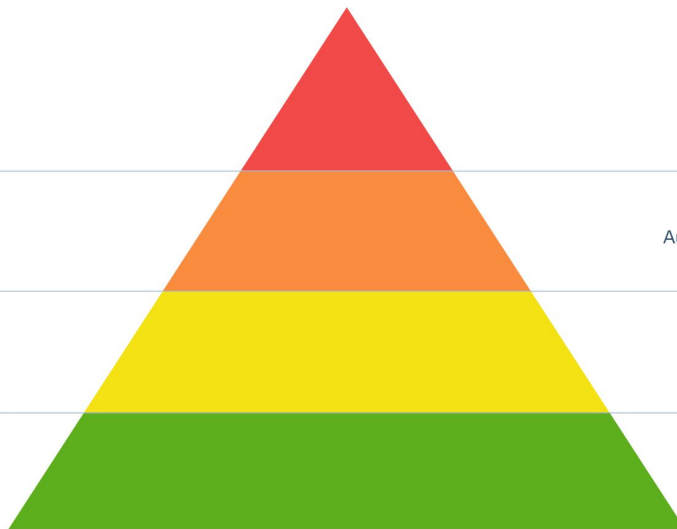
One-time meeting link
Authentication against IdP
2FA

Moderate risk

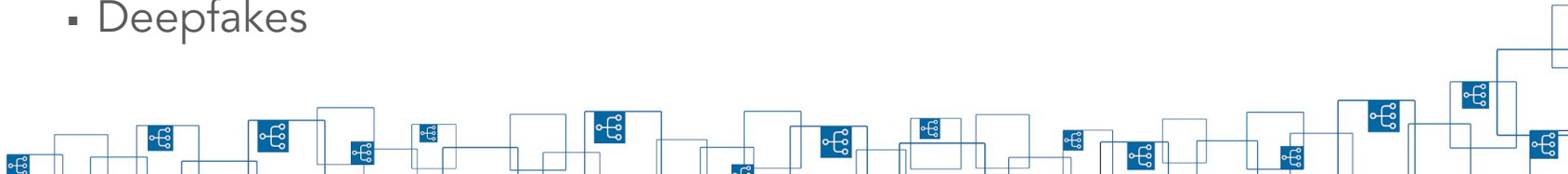
PIN codes
Personal VMRs

Low risk

Baseline security



- Jsou videokonference bezpečné
 - Videokonference jsou jen tak bezpečné, jak si je sami jako uživatelé zabezpečíme
- Zabezpečení videokonferencí
 - Zabezpečení meetingů/virtuálních videokonferenčních místností
 - Neautorizovaný přístup
 - Prevence nechtěného, rušivého chování účastníků videokonferencí
 - Triviální sociální inženýrství
 - Softwarová bezpečnost
 - Zabezpečení osobních údajů
 - Zabezpečení uživatelských dat
 - Deepfakes



- Nautorizovaný přístup, narušování videokonferencí
 - Zoombombing
 - Neomezuje se jen na Zoom – díky popularitě Zoomu vznikl termín
 - Obecný fenomén - komunity na Twitteru (#zoomcodes, #zoomraids) a Facebooku, podobně pro MS Teams např. na Instagramu (@microsoft_teams_raids)
 - "Zábava" pro děcka za Covidu
 - Ale je to reálný problém – např. infiltrace videokonference ruského Ministerstva obrany a obchodu Jevgenijem Volnovem (BTW: Kontur Talk/Jitsi Videobridge)
- Nevystavujte odkazy na videokonference (pokud je nezabezpečíte)
- RBAC – mějte pod kontrolou přístup účastníků do videokonference
 - Seznamte se s rolemi účastníků a s tím, co mohou účastníci vidět/slyšet/sdílet



- Přístup k videokonferencím
 - Historicky záměrně co nejjednodušší
 - Telefonní číslo (+420)95008xxxx, SIP URI videokonference@vc.cesnet.cz nebo URL <https://cesnet.zoom.us/xxxx>, <https://letsmeet.cesnet.cz/xxxx> atd.
 - Co očekáváte, že se stane, když vytočíte tel. č., zadáte SIP URI nebo URL v prohlížeči?
 - Okamžitě se připojíte k videokonferenci?
- Tradičně zejména “security by obscurity”
 - Tj., přístup k videokonferenci (tel. č., URI, URL) není veřejné (a pokud možno jej nelze uhodnout) - Špatně!
 - Videokonference v minulosti vyžadovaly drahé vybavení. Útočení na videokonference se nevyplácelo a nedávalo smysl jen pro zábavu.



← Tweet

CRAACE Continuity/Rupture
@CRAACE1918_39

22 October, 6pm CET, don't miss this free lecture by
#Seminar and #CRAACE on Zoom:

[cesnet.zoom.us/j/98267536775?...](https://cesnet.zoom.us/j/98267536775?pwd=M0hUej...)

<https://cesnet.zoom.us/j/98267536775?pwd=M0hUej...>

**The Experience
of Miesian
Space**
on-line



Christopher Long

3:19 odp. · 16. 10. 2020 z místa Brno, Česká republika · Twitter for iPhone

3 Retweety 2 Tweety s citaci 2 Lajky

← Tweet

 **David Černý**
@higuys66935788

[cesnet.zoom.us/j/95932257945?...](https://cesnet.zoom.us/j/95932257945?pwd=M0hUej...) RAID THIS CLASS!
#zoomcodes #zoomraids



Join our Cloud HD Video Meeting

Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for vid...
cesnet.zoom.us

6:03 odp. · 8. 2. 2021 · Twitter Web App

 **BramoYT** @BramoYt · 50 m
Odpověď uživateli @higuys66935788
Imao
bro



1



- PIN/Hesla
 - Nezveřejňujte svá hesla!
- Zamykání meetingu
- Waiting room/Virtual lobby
 - Nestačí jen povolit. Je třeba je aktivně používat! Proč by měl mít Pius Čúrus přístup k Vašemu meetingu?
- Role Based Access Control
 - Sdílení obrazu a zvuku (funkce mute), sdílení obsahu atd.
 - Ve velkých veřejných meetinzích dnes dává smysl běžným účastníkům nepovolovat sdílení v podstatě žádného obsahu – což poněkud popírá smysl videokonferencí...
- V nejhorším případě odpojíme účastníka (a nedovolíme jim se znovu připojit) - neřeší to problém úplně ale částečně pomůže



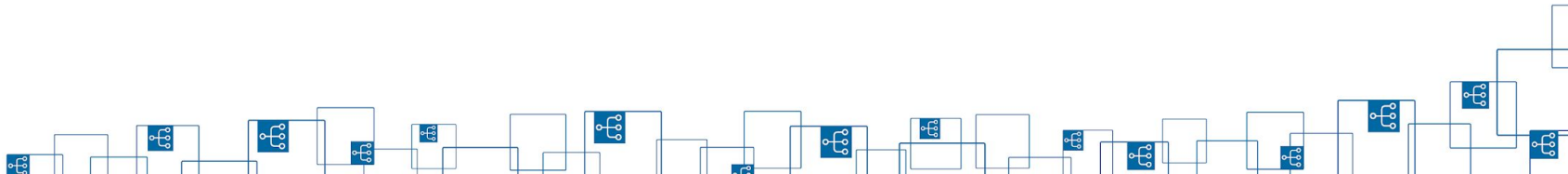
1	Participant	Device	IP Address	Location
40	WhatIsCunt	Windows	Public IP: 103.252.108.58 Local IP: 192.168.0.103	Ahmedabad (IN)
94	Lupu Stefan	Windows	Public IP: 109.101.147.233 Local IP: 192.168.1.11	Bacău (RO)
95	TaRon Gaines	Windows	Public IP: 69.14.244.238 Local IP: 192.168.5.134	Livonia (US)
142	Mark Joshua	Android	Public IP: 49.149.135.87 Local IP: 192.168.1.3	Lipa City (PH)
168	Кибер тролль анонимус да блять	Windows	Public IP: 188.69.195.168 Local IP: 192.168.8.104	Vilnius (LT)
203	snap-enrgeticmist	Android	Public IP: 73.54.96.217 Local IP: 10.0.0.9	Fort Myers (US)
225	Tomio Okamura SPD	iOS	Public IP: 1.143.56.170 Local IP: 0000:0000:0000:0000:0000:0000:2001:8004:2741:5ff9:fc44:be37:f20b:a1e2	Kew (AU)
356	Lupu Stefan	Windows	Public IP: 109.101.147.233 Local IP: 192.168.1.11	Bacău (RO)
390	JV	Web	Public IP: 3.127.251.113 Local IP: 10.0.9.230	Frankfurt am Main (DE)
393	Giosef	Android	Public IP: 85.74.249.98 Local IP: 192.168.1.10	Athens (GR)
397	Amálie Bulandrová	Web	Public IP: 3.127.251.113 Local IP: 10.0.9.230	Frankfurt am Main (DE)
405	Joe Mama	iOS	Public IP: 174.235.141.7 Local IP: 0.0.0.0,100.106.13.68	Destrehan (US)
424	misa	Web	Public IP: 3.127.251.113 Local IP: 10.0.9.230	Frankfurt am Main (DE)
440	deepen	Windows	Public IP: 108.44.195.241 Local IP: 192.168.1.154	Leesburg (US)
444	sasuke uchiha	Chrome OS	73.207.139.95	Atlanta (US)
454	kid	Chrome OS	108.45.165.82	Upper Marlboro (US)
459	Daisy Smith	Android	Public IP: 223.188.31.81 Local IP: 100.95.36.158	Kota (IN)
461	DERRICKA BULLOCK	Chrome OS	86.82.68.249	Nootdorp (NL)
488	UNMUTE ME INNOCENT	Windows	Public IP: 78.95.70.124 Local IP: 192.168.1.2	Riyadh (SA)
506	Lucus Mats	Windows	Public IP: 5.107.66.181 Local IP: 192.168.0.131	Sharjah (AE)
528	Bluh Booth	iOS	Public IP: 184.60.45.248 Local IP: 0.0.0.0,192.168.0.10	La Center (US)
566	Aniket Jaiswal	Android	Public IP: 157.40.39.18 Local IP: 25.98.63.184	Kolkata (IN)
567	Oneplus Gamerz	Android	Public IP: 203.192.213.171 Local IP: 192.168.0.100	Mumbai (IN)
666	John mcnuget	Windows	Public IP: 79.176.196.4 Local IP: 192.168.14.69	Tel Aviv (IL)
667	John mcnuget	iPAD	Public IP: 46.152.143.12 Local IP: 0.0.0.0,192.168.100.64	Riyadh (SA)
668	iphone	Windows	Public IP: 96.228.80.32 Local IP: 192.168.1.12	Lynchburg (US)
672	Jozlynn	Chrome OS	172.58.99.42	Houston (US)
673	Aniket Jaiswal	Android	Public IP: 157.40.39.18 Local IP: 25.98.63.184	Kolkata (IN)
685	Daisy Smith	Android	Public IP: 223.188.31.81 Local IP: 100.95.36.158	Kota (IN)
686	Student	Android	Public IP: 203.192.213.171 Local IP: 192.168.0.100	Mumbai (IN)
708	Aniket Jaiswal	Android	Public IP: 157.40.39.18 Local IP: 25.98.63.184	Kolkata (IN)
723	Bobby Hummer	iOS	Public IP: 172.58.172.42 Local IP: 0000:0000:0000:0000:0000:0000:2607:fb90:42e8:3d60:b1a0:6789:335c:40aa	Opa-locka (US)
725	Harry Gunawan	Android	Public IP: 223.188.121.129 Local IP: 100.95.36.158	Jaipur (IN)
763	emilly	Windows	Public IP: 102.160.242.175 Local IP: 192.168.8.103	(MU)
787	Antho	Windows	Public IP: 85.112.71.30 Local IP: 192.168.1.104	Beirut (LB)
793	DERRICKA BULLOCK	Chrome OS	86.82.68.249	Nootdorp (NL)
807	MrCan	Windows	Public IP: 88.230.199.11 Local IP: 192.168.1.43	Izmir (TR)
808	Ahmed hamood Habib	Windows	Public IP: 95.176.202.74 Local IP: 192.168.1.15	Straza (SI)
824	Bluh Booth	iOS	Public IP: 184.60.45.248 Local IP: 0.0.0.0,192.168.0.10	La Center (US)

- Je dobré znát účastníky videokonferencí!
- Pokud je neznáte, nebo je meeting veřejný, opravdu mějte pod kontrolou, jaká data mohou sdílet s ostatními
- I chat v meetingu může být problém, pokud není moderovaný
- Triviální vektor založený na sociálním inženýrství:
 - Hey, check out this cool link I have posted to the chat...
 - Hey, fix your mic audio. Use the script I have linked in the chat...
- A ještě později přidáme Deepfakes, aby byla větší zábava...

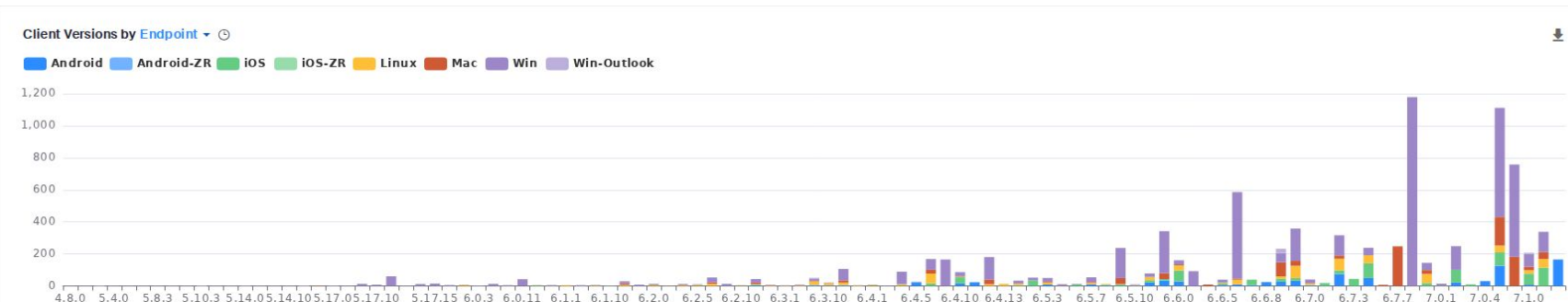


- SW bezpečnost

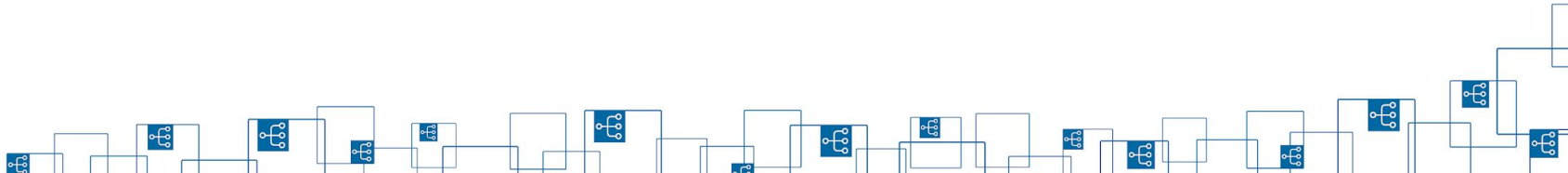
- Obvyklá pohádka...
- SW z oficiálních zdrojů lze považovat za bezpečný
- Stále ale může obsahovat vážné zranitelnosti!
- Udržujte svůj SW. Updatujte pravidelně ručně nebo lépe automaticky
- Používejte SW zodpovědně
 - Nestahujte videokonferenční SW z pochybných zdrojů
 - Dávejte pozor na podpisy instalačních balíčků
 - Na mobilních platformách používejte jen Google Play/App Store



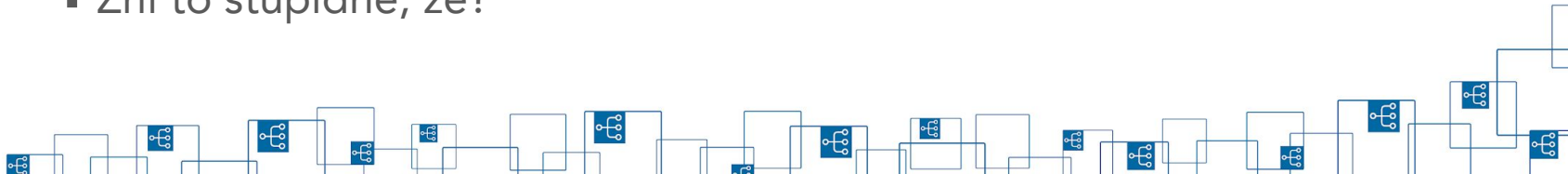
- Client Versions by Endpoint  
- Android Android-ZR iOS iOS-ZR Linux Mac Win Win-Outlook
- 
- | Endpoint | Android | Android-ZR | iOS | iOS-ZR | Linux | Mac | Win | Win-Outlook |
|----------|---------|------------|-----|--------|-------|-----|-----|-------------|
| 4.8.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.4.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.8.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.10.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.14.05 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.14.05 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.17.05 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.17.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.17.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.17.15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.0.11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.1.1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.1.1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.1.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.2.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.2.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.2.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.3.1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.3.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.4.1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.4.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.4.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.4.13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.5.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.5.7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.5.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.6.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.6.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.6.8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.7.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.7.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6.7.7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7.0.1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7.0.4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7.1.0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |



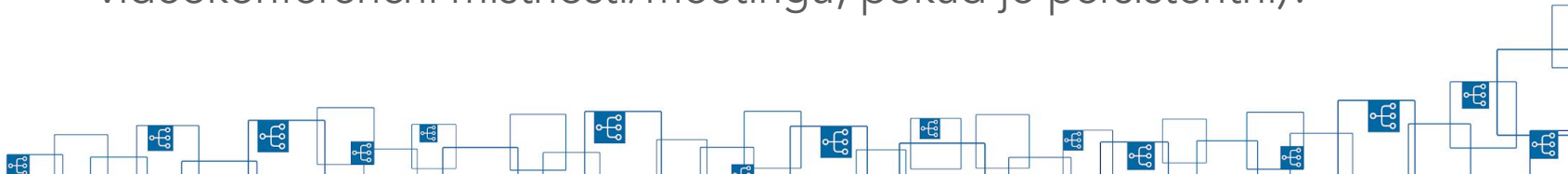
- Zranitelnost Wormable v MS Teams
 - Vcelku tradiční Cross-site-scripting (XSS) exploit
 - Útočník dokáže zneužít XSS zranitelnost, aby získal autorizační tokeny z SSO v MS Teams
 - Útočník jen pošle nebo edituje existující zprávu v chatu, do které vloží kód v JS, který stáhne a spustí škodlivý kód



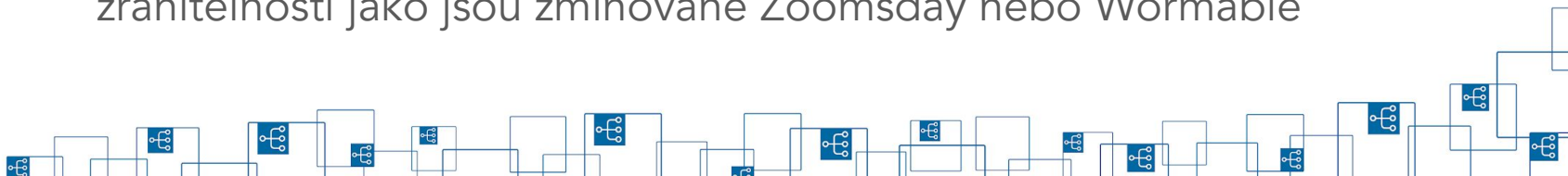
- Zajištěná poskytovatelem služby
 - CESNET, Zoom Communications, Microsoft, Cisco atd.
 - On-premise vs. cloudové služby
- Co mít na zřeteli v kontextu bezpečnosti osobních dat?
 - GDPR compliance
 - Jaká osobní data uvolňuji a zpřístupňuji VC službě?
 - Kam zadávám uživatelské jméno/heslo při přihlašování?
 - Neposílejte nikomu svá uživatelská jména a hesla mailem ani nijak jinak, ani když potřebujete technickou podporu!
 - Zní to stupidně, že?



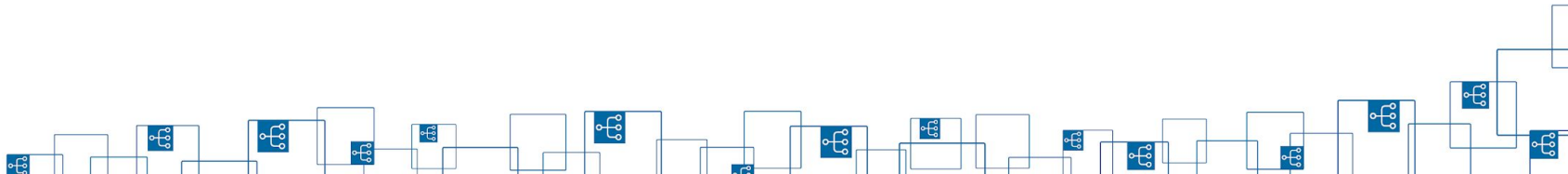
- Jaká data sdílím ve videokonferenci/meetingu?
- Mají být sdílená data persistentně uložena?
- Pokud ano, tak kde (on-premise vs. cloud)
- A jak?
 - Permanentně nebo po omezenou dobu?
 - Jsou šifrovaná?
 - Jsou zálohovaná?
 - Kdo může k datům přistupovat (ne jen v cloudu ale i ve videokonferenční místnosti/meetingu, pokud je persistentní)?



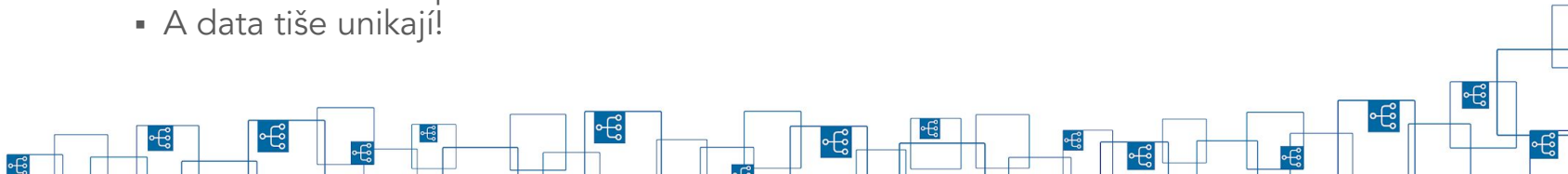
- “Svatá kráva” videokonferencí
- Je to vůbec vždy možné?
 - Point-to-point videokonference
 - Multipoint videokonference - videokonferenční “mixer” a “server-side” zpracování audia, videa a sdílených dat
 - Cloudové záznamy meetingů
- Chceme vždy end-to-end šifrování?
 - End-to-end šifrování např. znemožňuje server side mitigaci zranitelností jako jsou zmiňované Zoomsday nebo Wormable



- Videokonferenční nástroje dnes typicky varují, pokud jsou vaše data zaznamenávána a nebo zpracovávána (včetně zpracování AI)
- Je těžké (až nemožné) kontrolovat, co se stane s vašimi daty ve chvíli, kdy se dostanou až ke koncovým VC klientům dalších účastníků
 - Jakmile koncový účastník přijme audio/video/sdílená data, může s nimi nakládat libovolně (nahrávat, zpracovávat, přeposílat), aniž by o tom kdokoliv věděl



- AI nástroje jsou samozřejmě populární
 - Přepisy a souhrny meetingů, (živé) titulkování a/nebo překlady, asistované psaní, agentic retrieval
- Built-in ve VC nástroji nebo dostupné skrz API
- Ne všechny AI nástroje musí být dostupné ve VC nástroji, platformě, nebo s dostupnými licencemi
- Tady se přímo nabízí nástroje třetích stran
 - Klidně zdarma – platíte svými daty!
 - Mohou používat API VC nástrojů/platform (třeba Zoomu)
 - Ale také se mohou připojovat jako běžní účastníci meetingu!
 - Pak nemáte nad zpracováním Vašich dat žádnou kontrolu
 - A data tiše unikají!



- Přesně zacílený útok
- Bez kompletní autentizace a attribute based access control máme jen statickou kontrolu identity – jméno, profilový obrázek atd. a to všechno poskytnuté účastníkem/útočníkem
 - Jak poznáte, že účastník není deepfake – audio vs. video?
- BlueNoroff Deepfake Zoom Scam Vector
 - Spear phishing email s požadavkem na meeting se zaměstnancem, útočník posílá odkaz na Calendly s časem meetingu
 - Odkaz na meeting se v Calendly tvářil jako Google Meet event, ale URL přesměřovalo zaměstnance na podvzřenou Zoomovou doménu
 - Zoom meetingu se účastnilo několik podvržených členů managementu
 - Ti zaměstnanci nutili nainstalovat “rozšíření Zoomu” sdílené přes Telegram





KEEP CALM IT'S NOT ROCKET SCIENCE

#PROPOJUJEME VĚDU

