NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Bezpečnostní standard pro videokonference

23.9.2020 Praha Vladimír JEŘÁBEK

Bezpečnostní standard pro videokonference

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

- Vojenské zpravodajství
- Bezpečnostní informační služba
- Úřad pro zahraniční styky a informace
- AFCEA – Pracovní skupina kybernetické bezpečnosti
- Armáda české republiky
- CISCO SYSTEMS (Czech Republic) s.r.o.
- MICROSOFT s.r.o.
- GESTO COMMUNICATIONS spol. s r.o.
- ATS – Telcom Praha, a.s.

NAKIT

Představení bezp. standardu pro VTC

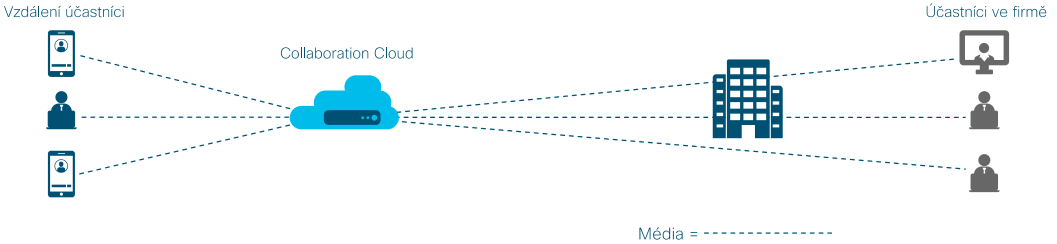
- Architektura / řešení videokonferencí
- Bezpečnostní principy
- Bezpečnostní opatření
- Bezpečnostní monitoring
- Funkční požadavky (včetně scénářů)
- Bezpečnost při vedení videokonference
  - uživatelé/účastnící
  - organizátoři
  - moderátoři

NAKIT

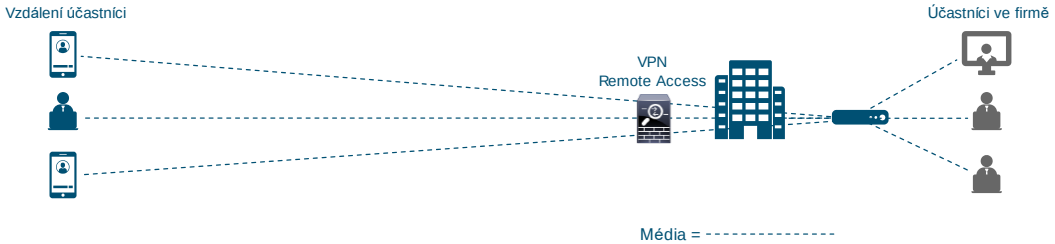
Architektura VTC

Bezpečnostní standard pro VTC

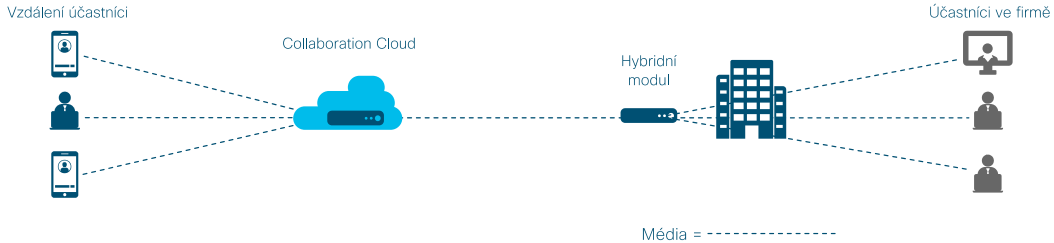
- **Cloudové řešení**



- **On-premise řešení**



- **Hybridní řešení**



NAKIT

Bezpečnostní principy VTC

Bezpečnostní úroveň videokonferenčního systému	Příklady	Popis hodnotících kritérií dané bezpečnostní úrovně z pohledu důvěrnosti komunikované informace
1	Provozní a organizační pokyny Poskytování školení a přednášek pro veřejnost	Komunikovaná informace je veřejně přístupná, je určena ke zveřejnění nebo jejím zveřejněním nemůže vzniknout organizaci ani nikomu jinému škoda.
2	Běžná pracovní komunikace Pracovní porady Individuální jednání s veřejností Úkony v rámci správního řízení nebo informace o něm	Komunikovaná informace není veřejně přístupná a její ochrana je vyžadována právními předpisy (především obecná povinnost mlčenlivosti podle zákoníku práce), smluvními ujednáními nebo jinými předpisy nad rámec předpisů upravujících ochranu osobnosti. Tato úroveň je minimální bezpečnostní úrovní pro videokonferenční systémy sloužící v organizaci pro běžné pracovní úkony.
3	Porady o zvlášť důležitých skutečnostech Obzvláště důležité neveřejné informace (strategická rozhodnutí, obchodní tajemství, bezpečnostní informace apod.)	Komunikovaná informace není veřejně přístupná a její ochrana je nejen vyžadována právními předpisy (především obecná povinnost mlčenlivosti podle zákoníku práce), smluvními ujednáními nebo jinými předpisy nad rámec předpisů upravujících ochranu osobnosti, ale vyžadují nadstandardní míru ochrany.

Bezpečnostní opatření

4.3.1.4 Používat vícefaktorovou autentizaci

Používejte pro ověřování vícefaktorovou autentizaci (elektronický klíč, mobilní klíč, autentizační předmět apod.), zejména v případě ověřování privilegovaných účtů administrátorů.

Cíl opatření:

Jestliže jsou pro ověření uživatele použity mechanismy založené výhradně na sdílené znalosti (jméno, heslo, e-mail, PIN), nelze zabezpečit, aby toto sdílené tajemství (systém pro ověření a uživatel) nemohlo být použito, bez vědomí uživatele. Existuje zde množství hrozeb (odpozorování, odposlechnutí, úmyslné či neúmyslné zaznamenání, zveřejnění atp.), díky kterým lze tyto údaje zneužít. Naproti tomu je vícefaktorové ověření založeno na kombinaci alespoň dvou z následujících tří typů faktorů:

- *vlastnictví nějakého fyzického předmětu (karta, token, generátor náhodného kódu svázaný s konkrétním předmětem)*
- *znalosti (PIN, heslo atd.) nebo*
- *biometrie.*

dat

davatele

NAKIT

Další bezpečnostní doporučení

- Použít řízení kvality komunikace v síti (QoS)
- Pro externí připojení nepoužívat nezabezpečené veřejné sítě
- Videokonferenční systém neumožní nahrávání záznamů bez vědomí všech zúčastněných
- Řešení podporuje oddělený přenos zvuku, obrazu, souborů, textu (Chat).
- Data musí být vždy pod kontrolou vlastníka
- Implementovat DoS/DDoS ochranu
- Zajistit redundanci infrastruktury, load balancing
- Provádět testování infrastruktury proti výpadkům
- Provádět a vyhodnocovat penetrační testy, testy DoS/DDoS
- Požadavky na zabezpečení cloudových služeb se musí odvíjet podle úrovně poskytované služby (SaaS, Paas, IaaS)

Bezpečnostní monitoring

Opatření			
Bezpečnostní monitoring	**Úroveň 1**	**Úroveň 2**	**Úroveň 3**
Log management Minimální retence auditních záznamů	D 60 dní	A 12 měsíců	A 12 měsíců
SIEM	N	D	D
Vulnerability management	N	D	A
EDR	N	D	D
IDS/IPS	N	D	A
DLP	N	D	D
Antivirus	D	A	A
Firewall	A	A	A
Proxy	D	D	D
Netflow	N	D	A

NAKIT

Funkční požadavky

- Scénáře použití
- Technické vybavení
- Ochrana přenášených dat
- Ochrana uložených dat
- Řízení konference
- Autentizovaný i externí přístup
- Komunikační kanály
- Záznamy konferencí
- Interoperabilita
- Integrace
- Monitoring
- Reporting a audit

NAKIT

Bezpečnost při vedení videokonferencí

Bezpečnostní standard pro VTC

Účastníci v

Mode

jednotlivou schůzku

nologie

tné a přínosné

Videokonference bezpečně

Co je videokonference?

Videokonference (VTC) je živá video a audio konverzace (virtuální schůzka) prostřednictvím telefonu, tabletu nebo počítače mezi dvěma a více osobami, které se nacházejí na různých místech.

Videokonference jsou moderním komunikačním prostředkem využívaným nejen v krizových obdobích jako COVID-19 (kdy nabyly na důležitosti), ale používají se i pro běžnou komunikaci v soukromém a pracovním životě. Pokud jste na videokonferenci nováčkem, níže uvedené tipy Vám pomohou ji bezpečně používat. Pokud videokonference již používáte, ujistěte se, že tato základní bezpečnostní doporučení pro uživatele, organizátory a moderátory virtuálních schůzek znáte a používáte je.

ÚČASTNÍCI VIRTUÁLNÍCH SCHŮZEK

POUŽÍVEJTE JEN OFICIÁLNÍ APLIKACE DODAVATELŮ

Stahujte pouze oficiální aplikace dodavatelů z ověřených zdrojů, jako jsou Google

Děkuji

Q&A

Vladimír Jeřábek

E: vladimir.jerabek@nakit.cz
M: +420 602 496 219

W: www.nakit.cz

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.