BEZPEČNOSTNÍ STANDARD PRO VIDEOKONFERENCE

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NAKIT

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

Verze 1.0, platná ke dni 17. července 2020

Na přípravě bezpečnostního standardu pro videokonference dále spolupracovali:

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.

Obsah

1 Úvod

1.1 Cíl dokumentu

Cílem tohoto dokumentu je uvést **základní požadavky na zajištění kybernetické bezpečnosti implementace a provozu videokonferencí** bez rozdílu toho, zda je systém videokonference začleněn do systému, jenž spadá pod zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále také jen „zákon o kybernetické bezpečnosti“) či nikoliv.

Informace a postupy uvedené v tomto dokumentu vychází ze zákona o kybernetické bezpečnosti, vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále také jen „vyhláška o kybernetické bezpečnosti“), mezinárodně uznávaných standardů a také z dobré praxe, která se problematiky kybernetické bezpečnosti týká.

Je nutné mít na paměti, že splněním tohoto standardu nedochází automaticky ke splnění požadavků zákona a vyhlášky o kybernetické bezpečnosti. Pokud organizace a její videokonferenční systém spadá pod regulaci zákona o kybernetické bezpečnosti, řídí se vždy především jeho požadavky.

Je důležité mít na paměti, že základním principem by měl být proces neustálého zlepšování. Nestačí totiž jednorázově zavést bezpečnostní opatření a následně spoléhat, že je tím tato problematika navždy vyřešena, ale je nutné proaktivně kontrolovat přiměřenost a aktuálnost všech zavedených opatření.

1.2 Rozsah dokumentu

Tento dokument se vztahuje pouze na komunikaci neutajovaných informací. Požadavky na informační systém pro komunikaci utajovaných informací a podmínky jeho bezpečného provozování stanoví zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a jeho prováděcí předpis, vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.

Tento dokument se také nezabývá problematikou souladu provozování videokonferenčního systému s požadavky Obecného nařízení o ochraně osobních údajů (známého pod zkratkou GDPR), avšak při přípravě a realizaci videokonference je třeba mít na paměti, že obrazová a hlasová data mohou mít povahu osobních údajů či osobních údajů zvláštního charakteru, a to zejména při záznamu videokonference a případném následném zpracování.

Tímto dokumentem jsou především upraveny základní funkce videokonferenčního systému jako přenos zvuku, obrazu, souborů a funkce chatu. Obdobně lze níže uvedená doporučení použít, pokud je to možné, i na další pokročilejší funkce videokonferenčních zařízení.

1.3 Použití dokumentu

Tento dokument je vytvořen jako standard, který je pro jakoukoliv organizaci dobrovolně aplikovatelný.

Pokud se organizace rozhodne tento standard přijmout a aplikovat, případně jí jeho přijetí bude uloženo nadřízenou organizací, **je potřeba pro dosažení shody s tímto standardem zajistit, že dojde ke správnému rozdělení videokonferenčních systémů do bezpečnostních úrovní podle komunikovaných informací a**

následně budou důsledně aplikována všechna bezpečnostní opatření nutná pro zabezpečení jednotlivých úrovní (kapitola 4 a 5), je tedy potřeba níže uvedené požadavky považovat za povinnosti s přihlédnutím na to, zda se jedná o přijetí a aplikaci tohoto standardu ve variantě Interní či Plné, viz níže.

V případě, že se organizace rozhodne neaplikovat tento standard na své videokonferenční systémy plně, tak jak je uvedeno v předchozím odstavci, je stále možné aplikovat jeho ustanovení pouze částečně, či užít uvedené požadavky podpůrně podle jiných potřeb organizace. Pak je však nutné se vyvarovat tvrzení, že jsou naplněny požadavky tohoto standardu.

Přijetí a aplikace tohoto standardu jsou možné ve dvou variantách:

1) **Interní** – V případě, že se organizace zaváže k přijetí standardu v této variantě, je nutné splňovat níže uvedené požadavky pro situace interního využívání videokonferenčního systému v organizaci. Z vyžadování těchto požadavků lze přiměřeně slevit v případech potřeby externí komunikace prostřednictvím videokonferenčního systému.
2) **Plná** – V případě, že se organizace zaváže k přijetí standardu v této variantě, je nutné splňovat níže uvedené požadavky jak pro situace interního využívání videokonferenčního systému v organizaci, tak v případech potřeby externí komunikace. Tato varianta vyžaduje, aby byl standard přijat a aplikován v rámci všech organizací, které budou prostřednictvím videokonferenčního systému komunikovat.

Využití tohoto standardu při videokonferencích mezi organizacemi může být realizováno v několika scénářích.

1) **Obě (všechny) organizace účastnící se videokonference aplikují tento standard.** V takovém případě mohou v rámci videokonference komunikovat informace nanejvýš takové bezpečnostní úrovně (podle níže uvedené kapitoly 4.1 Rozdělení videokonferenčních systémů do bezpečnostních úrovní), kterou mají jejich videokonferenční systémy společnou. Zároveň se některá bezpečnostní opatření, u kterých není v moci organizace zajistit jejich plnou aplikaci z důvodů na straně ostatních účastníků (např. opatření týkající se koncových stanic), aplikují přiměřeně.
2) **Pokud jedna z organizací účastnící se videokonference neaplikuje tento standard,** potom mohou být v rámci takové videokonference komunikovány informace maximálně druhé úrovně, a to za podmínky, že videokonferenci hostuje organizace využívající tento standard a tato organizace zároveň disponuje videokonferenčním systémem splňujícím podmínky alespoň druhé úrovně. V případě, že je nutné komunikovat informace nejvyšší úrovně, organizace účastnící se videokonference disponující systémem videokonference splňujícím podmínky nejvyšší úrovně využije videokonferenční systém nejvyšší úrovně, pozve účastníky z ostatních organizací a přiměřeně aplikuje bezpečnostní opatření nejvyšší úrovně (tj. organizátor videokonference musí disponovat videokonferenčním systémem nejvyšší úrovně a bezpečnostní opatření, u kterých není v jeho moci zajistit jejich plnou aplikaci z důvodů na straně ostatních účastníků, musí aplikovat přiměřeně).

1.4 Vztah dokumentu k zadávání veřejných zakázek a § 4 odst. 4 zákona o kybernetické bezpečnosti

Častou otázkou pro správce videokonferenčních systémů může být postavení tohoto standardu ve vztahu k zadávání veřejných zakázek stejně tak jako využití výjimky uvedené v § 4 odst. 4 zákona o kybernetické bezpečnosti.

Ustanovení § 4 odst. 4 zákona o kybernetické bezpečnosti hovoří o bezpečnostních opatřeních, která jsou v podrobnostech definována v § 5 zákona o kybernetické bezpečnosti a dále rozvedena vyhláškou o kybernetické bezpečnosti. Tzn. povinná osoba je povinna před výběrem dodavatele (potažmo před uzavřením smlouvy s ním) zvážit zavedení bezpečnostních opatření podle § 5 zákona o kybernetické bezpečnosti, resp. vyhlášky o kybernetické bezpečnosti, a požadavky vyplývající z těchto bezpečnostních opatření začlenit do smlouvy. Cokoli povinná osoba požaduje nad rámec požadavků vyplývajících z bezpečnostních opatření podle § 5 zákona o kybernetické bezpečnosti, resp. vyhlášky o kybernetické bezpečnosti (nejde jen o požadavky v oblasti kybernetické bezpečnosti, ale o všechny zbylé požadavky na předmět poptávaného plnění), požaduje mimo rámec § 4 odst. 4 zákona o kybernetické bezpečnosti a musí argumentaci ve prospěch svých požadavků založit na jiných ustanoveních (typicky jiných zákonů).

Standard není bezpečnostním opatřením, ani žádné z bezpečnostních opatření podle § 5 zákona o kybernetické bezpečnosti, resp. vyhlášky o kybernetické bezpečnosti, neprovádí. Jedná se o soubor doporučení především pro osoby spadající mimo působnost zákona o kybernetické bezpečnosti. Osoby spadající do působnosti zákona o kybernetické bezpečnosti jsou povinny provádět bezpečnostní opatření podle § 5 zákona o kybernetické bezpečnosti, resp. vyhlášky o kybernetické bezpečnosti. Ačkoli se standard může s některými oblastmi vyhlášky o kybernetické bezpečnosti překrývat, nenahrazuje je, nedoplňuje, de facto k nim nemá žádný formální vztah. Standard je tak z pohledu Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) především metodickým materiálem, kterým se osoby spadající do působnosti zákona o kybernetické bezpečnosti mohou při výběru bezpečnostních opatření, která budou v souladu s vyhláškou o kybernetické bezpečnosti zavádět, inspirovat, rozhodně však nelze tvrdit, že splněním „požadavků“ standardu dochází ke splnění požadavků vyplývajících z § 4 a 5 zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti.

Nelze vyloučit, že např. některý ústřední správní úřad (např. ministerstvo) stanoví povinné použití standardu pro své podřízené organizace. V takovém případě – pokud bude podřízená organizace současně povinnou osobou podle zákona o kybernetické bezpečnosti – bude nezbytné dodržet požadavky jak standardu (povinnost stanovená nadřízenou organizací), tak vyhlášky o kybernetické bezpečnosti (povinnost stanovená zákonem).

Co se týče zohlednění standardu v procesu zadávání veřejných zakázek v režimu zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „zákon o zadávání veřejných zakázek“), druhá věta § 4 odst. 4 zákona o kybernetické bezpečnosti se pro tento případ neuplatní, a to právě z důvodu, že standard není bezpečnostním opatřením, o kterém § 4 odst. 4 zákona o kybernetické bezpečnosti hovoří. Veškeré požadavky založené na standardu tak bude zadavatel povinen odůvodnit tak, aby dostál § 36 odst. 1 zákona o zadávání veřejných zakázek, tedy aby prokázal, že zadávací podmínky nejsou stanoveny tak, aby určitým

dodavatelům bezdůvodně přímo nebo nepřímo zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže. Výhodnější pozici by měli zadavatelé v případě, že by jejich nadřízená organizace stanovila povinné použití standardu (tzn. zadavatel by neměl na výběr, zda požadavky standardu aplikuje či nikoli, a nebylo by tedy možné hovořit o bezdůvodném omezování hospodářské soutěže). Bez stanovení povinného použití standardu se však jedná pouze o soubor doporučení, jejichž odůvodněnost musí v každém konkrétním případě zadavatel sám prokázat.

Co se týče použití výjimek podle § 29 zákona o zadávání veřejných zakázek, zadavatel je při jejich aplikaci vždy povinen prokázat, že splňuje všechny zákonné předpoklady pro jejich použití.

Podle § 29 písm. a) zákona o zadávání veřejných zakázek zadavatel není povinen zadat veřejnou zakázku v zadávacím řízení, pokud by provedení zadávacího řízení ohrozilo ochranu základních bezpečnostních zájmů České republiky a současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo. Standard nemá charakter zákonného ani podzákonného předpisu, z pohledu NÚKIB jde o pouhý soubor doporučení, jejichž nedodržení není sankcionováno. I pokud by nějaký centrální orgán stanovil povinnou aplikaci standardu pro své podřízené organizace, nesplnění této povinnosti by mělo spíše finanční a organizační důsledky. Standard bude nadto veřejný, tzn. každý si bude moci udělat jasnou představu o tom, jak vypadá zabezpečení videokonferencí ve veřejné sféře. Standard obecně nezavazuje osoby spadající do regulace zákona o kybernetické bezpečnosti, nebude mít tedy dopad na skutečně kritické systémy zajišťující základní bezpečnostní zájmy České republiky.

Podle § 29 písm. c) zákon o zadávání veřejných zakázek zadavatel není povinen zadat veřejnou zakázku v zadávacím řízení, jde-li o zadávání nebo plnění veřejné zakázky v rámci zvláštních bezpečnostních opatření stanovených jinými právními předpisy a současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo. Zvláštními bezpečnostními opatřeními je v oblasti kybernetické bezpečnosti nutno rozumět opatření podle § 11 zákona o kybernetické bezpečnosti, příp. opatření přijatá v souvislosti s vyhlášením stavu kybernetického nebezpečí podle § 21 zákona o kybernetické bezpečnosti. Toto ustanovení z principu míří na mimořádné situace (tj. na situace, které jsou vyhlašovány ve specifických případech a jsou neobvyklé), se kterými se zadavatel standardně v rámci své praxe nesetkává (na běžné bázi) a nemůže jim tak přizpůsobit svou činnost (a v návaznosti na to i zadávání veřejných zakázek). Standardní bezpečnostní opatření podle § 5 zákona o kybernetické bezpečnosti jsou pro aplikaci této výjimky málo „zvláštní“; jde o standardní požadavky, které jsou nerozlučně spjaty s činností povinné osoby a na jejichž zavedení má povinná osoba dostatek času (včetně výběru realizátorů bezpečnostních opatření v zadávacím řízení).

Pro obě výjimky pak platí, že současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo (srov. zejm. § 36 odst. 8, § 96 odst. 2 a § 218 odst. 3 zákona o zadávání veřejných zakázek).

1.5 Webové stránky NÚKIB

Webové stránky NÚKIB mohou rovněž sloužit jako zdroj informací o problematice kybernetické bezpečnosti.

Lze je nalézt pod tímto odkazem: https://www.nukib.cz/.

NÚKIB pravidelně vydává podpůrné materiály, které jsou primárně zaměřeny na potřeby povinných osob, ale lze z nich vycházet v rámci řešení jednotlivých oblastí kybernetické bezpečnosti. Tyto materiály jsou také dostupné na webových stránkách NÚKIB.

V neposlední řadě jsou důležitým zdrojem také informace o aktuálních hrozbách nebo doporučení vydávaná Vládním CERT, obojí dostupné taktéž na webových stránkách NÚKIB.

1.6 Kontakt

V případě dotazů se prosím obracejte na sekretariát odboru regulace NÚKIB:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

2 Související legislativa, standardy a normy

Při přípravě tohoto bezpečnostního standardu pro videokonference byly reflektovány jak legislativní normy, jako je zákon o kybernetické bezpečnosti, vyhláška o kybernetické bezpečnosti, tak některé z mezinárodně uznávaných norem, na kterých tento standard stojí.

Legislativa

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Vyhláška 82/2018 Sb., o kybernetické bezpečnosti
- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů)

Standardy/normy[1]

- ČSN ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO/IEC 27701 (PIMS)
- SOC 1 Type 2, SOC 2 Type 2
- TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0

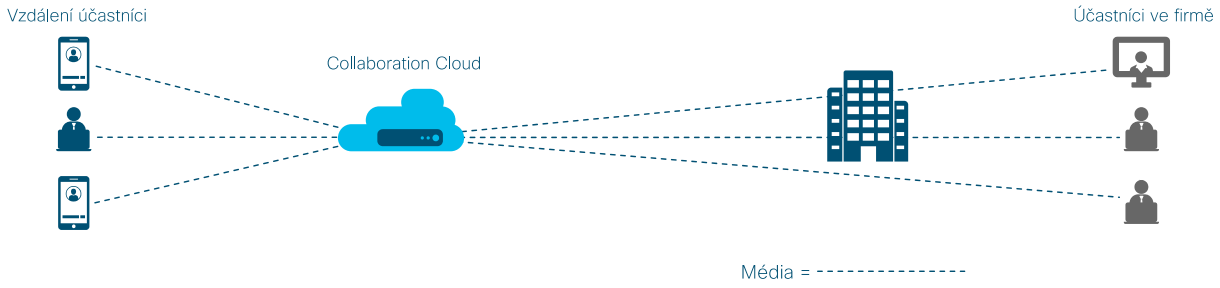
[1] V aktuálních verzích dle data vydání dokumentu.

3 Architektura řešení

Videokonferenční systémy mohou být provozovány různými způsoby. Cílem této kapitoly je objasnit tři typy architektur a pro každou z nich definovat její výhody a nevýhody. Výběr architektury pak definuje případné technické nebo organizační požadavky, se kterými se organizace využívající zvolený videokonferenční systém musí vypořádat. Vybrané tři architektury pokrývají všechny majoritně používané videokonferenční systémy na trhu. Konkrétně jde o plně cloudová řešení, řešení plně on-premise (provozovaná vlastními prostředky a lidskými zdroji) nebo hybridní řešení, které kombinuje obě předchozí.

3.1 Cloudové řešení

Cloud do velké míry řeší kapacitní, výkonnostní problémy a potřeby flexibility. Jde o architekturu, ve které je služba provozována externím dodavatelem – dodavatelem veřejných cloudových služeb.



Obrázek č. 1 Cloudové řešení

S ohledem na bezpečnost má cloudové řešení následující výhody:

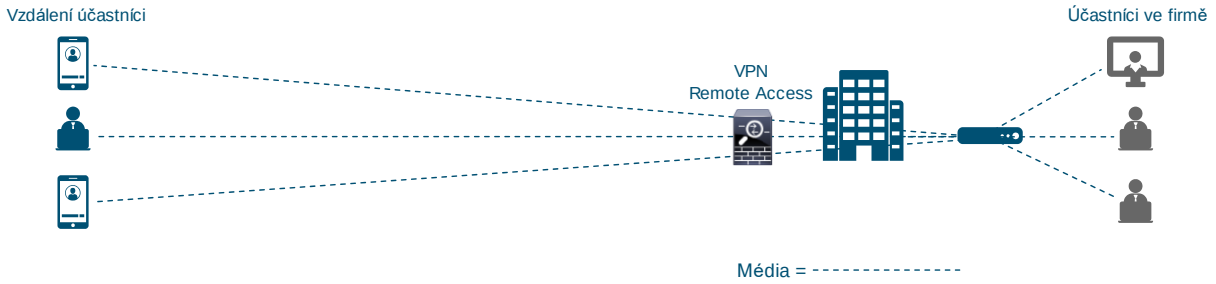
- Jednoduché ovládání a rychlá integrace nových služeb.
- Jednoduchá integrace různých koncových mobilních zařízení.
- Služby jsou pod trvalým dohledem a opravy a řešení bezpečnostních problémů se odehrávají mnohem rychleji než u on-premise řešení.
- Infrastruktura a propojení regionálních datových center cloudových dodavatelů je na vyšší úrovni (vybavenost, kapacita, bezpečnost atd.) než je tomu u lokálních datových center.
- Cloudové služby mají oproti on-premise řešení vyšší dostupnost odkudkoliv po světě díky propojenosti regionálních datových center a technologiím jako např. CDN apod.
- Cloudové služby dokáží poskytnout vyšší spolehlivost (SLA) za podstatně nižších finančních nákladů než on-premise řešení.
- Datová centra cloudových dodavatelů jsou certifikována a pravidelně auditována.

Nevýhodami cloudové architektury jsou:

- Složitější diagnostika – mezi klienty a službou leží různé sítě. Déle trvá, než se podaří zjistit, zda je problém v cloudové službě nebo po cestě. V některých případech lze řešit dedikovaným připojením mezi klientem a datovým centrem. Při komunikaci uživatelů připojených přes veřejný internet z mobilních zařízení je otázka kvality internetového připojení (ISP) identická pro všechny architektury a on-premis nebo hybridní varianta požadavek na kvalitu internetového připojení neeliminuje. Potřeba kvality a diagnostiky je u všech architektur identická.
- Záruky a podmínky provozu jsou dány jednotně pro všechny uživatele. U služeb veřejného cloudu je nelze individuálně uzpůsobit.
- Může existovat jazyková bariéra při komunikaci s technickou podporou. Závisí na úrovni technické podpory, jakou dodavatel videokonferenční služby nabízí.
- Vyšší požadavky na kapacitu připojení organizace do internetu z důvodu komunikace přes cloudové služby. Jestliže bude většina uživatelů konference ve vnitřní síti, on-premise nebo hybridní řešení snižuje nároky na připojení do internetu. V případě připojení uživatelů mimo vnitřní sítě není kapacita připojení organizace rozhodující.

3.2 On-premise řešení

On-premise architektura je optimalizována pro lokální uživatele. Vzdálení uživatelé se připojují formou bezpečného připojení – VPN nebo tzv. Edge prvku konferenčního systému.



Obrázek č. 2 On-premise řešení

Výhodami on-premise řešení jsou:

- Správa pod kontrolou organizace.
- Bezpečnostní politiky pod kontrolou organizace.

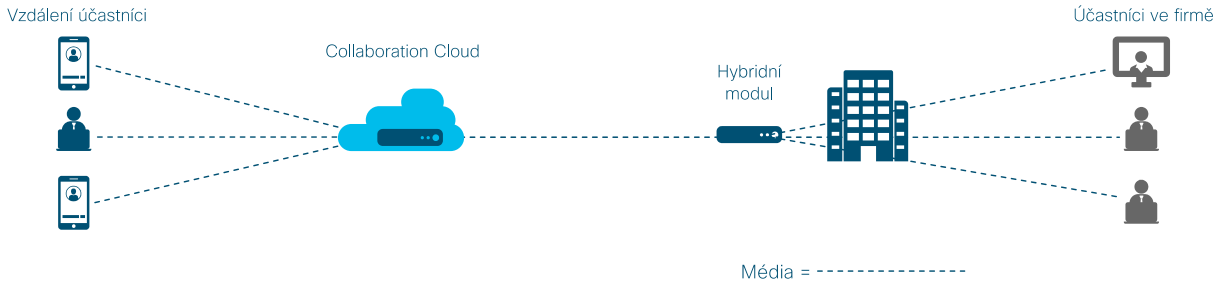
Nevýhody on-premise řešení jsou:

- Jestliže je více uživatelů mimo organizaci (práce z domova, uživatelé z jiných firem), objeví se problémy s kapacitou připojení. Úzkým místem je VPN koncentrátor nebo Edge prvek i kapacita přípojky do internetu. On-premise architektura také může mít problémy se škálováním – je připravena na odhadnutou kapacitu a může být problém pružně reagovat na zvýšený provoz.

- Složitá reakce na náhlé navýšení nároků na kapacitu. Vyžaduje rychlé investice a dodávky. Provozovatel musí být schopen pružně reagovat.
- Provoz a údržba řešení vyžaduje práci vysoce kvalifikovaných IT odborníků.
- Omezená rychlost rozvoje služeb, závislá na rychlosti upgradu na novou verzi.
- Zpravidla nižší odolnost proti DoS, DDoS a jiným kybernetickým útokům než u cloud řešení.
- Z pohledu souladu s bezpečnostními standardy je důležité, aby provozovatel zajistil soulad a získal požadované certifikace a ty pak s určenou periodou obnovoval. Z procesního i cenového pohledu jde o vysoce nákladné operace.
- Řada dodavatelů videokonferenčního řešení dnes minimalizuje investice do on-premis systémů, nebo tuto variantu vůbec neposkytuje.

3.3 Hybridní řešení

Hybridní architektura se snaží využít výhody obou výše uvedených řešení. Hybridní modul je součástí cloudu, který je vysunutý do firemní sítě. Lokální uživatelé tak využívají tento modul, vzdálení využívají cloud a mezi hybridním modulem a cloudem se vytvoří tzv. kaskáda, spojení s optimalizovaným přenosem, který šetří nároky na pásmo.



Obrázek č. 3 Hybridní řešení

Výhody hybridního řešení:

- Optimalizuje připojení do cloudu.
- Může sloužit jako „most“ pro propojení s cloudovým řešením, kdy videokonferenční služby jsou umístěny on-premise nebo online.
- Na firewallu lze nastavit přísnější pravidla, která umožní komunikaci do internetu pouze pro hybridní modul. Uživatelé mohou být zcela odděleni od internetu a komunikují přes hybridní modul.

Nevýhody hybridního řešení:

- Hybridní modul je spravován administrátory organizace, vyžaduje výpočetní zdroje v organizaci a je třeba věnovat pozornost nástrojům pro jeho správu a dohled, aby řešení nepředstavovalo zbytečnou zátěž pro administrátory.

- V některých případech může být toto řešení nákladnější, jelikož může vyžadovat investice do licencování obou prostředí, a to jak on-premise, tak v cloudu.
- Obecně vyžaduje více administrace a znalostí, protože pokrývá oblasti jak on-premise tak cloud technologií a technických prostředků. Tato komplexita je však vyvážena možností nejvyšší míry přizpůsobení.
- Z pohledu souladu s bezpečnostními standardy je identicky jako u on-premise řešení důležité, aby provozovatel zajistil soulad a získal požadovanou certifikaci. Je proto třeba věnovat pozornost způsobu aktualizací, zda se provádějí automaticky společně s rozvojem cloudového řešení nebo vyžadují zásah administrátora.

4 Bezpečnostní principy / požadavky

Tato kapitola je určena jako vodítko pro rozhodnutí o tom, zda je v organizaci možné realizovat služby videokonference, aniž by podstupovala neadekvátní rizika v oblasti kybernetické bezpečnosti a při ochraně dat.

Přestože se nutně nejedná o absolutní výčet bezpečnostních opatření a je možné zavádět i další opatření nad rámec níže uvedených, jsou pro tento standard uvedená bezpečnostní opatření dána jako potřebné minimum.

V případě, že organizace tato opatření odpovídající citlivosti sdělovaných informací není schopna naplnit, je potřeba snížit bezpečnostní úroveň videokonference změnou obsahu a citlivá data sdílet jiným bezpečným způsobem.

4.1 Rozdělení videokonferenčních systémů do bezpečnostních úrovní

V rámci použití videokonferenčních systémů je nutno nejdříve stanovit, jaké informace mohou být v rámci takového systému přenášeny (dále také „komunikovaná informace“).

S ohledem na závažnost dopadů způsobených možným narušením bezpečnosti komunikovaných informací je nutno komunikované informace rozdělit podle odpovídající bezpečnostní úrovně.

Kritérium pro komunikované informace je v tomto dokumentu dáno z pohledu jejich důvěrnosti, tzn. jejich bezpečnostní úroveň je dána tím, k jakému dopadu může v případě jejich vyzrazení dojít. Pokud je řešena škoda, ke které může vyzrazením takové informace dojít, nebo pokud je ochrana komunikované informace vyžadována právními předpisy, smluvními ujednáními nebo jinými předpisy, je nutno toto zohlednit nejen z pohledu organizace samotné, ale také obecně z pohledu ostatních subjektů.

S ohledem na to, že důvěrnost komunikované informace je ve většině případů hlavním a jediným kritériem, není hledisko dostupnosti nebo integrity komunikované informace v tomto dokumentu hodnotícím kritériem pro zařazení videokonferenčního systému do bezpečnostní úrovně. Ve výjimečných situacích, kdy hledisko integrity a dostupnosti převyšuje nad hlediskem důvěrnosti, je však vhodné přiměřeně povýšit výsledné hodnocení bezpečnostní úrovně nebo zavést další bezpečnostní opatření.

Z povahy věci jsou v rámci videokonferencí vždy zpracovávány osobní údaje (vždy alespoň jména uživatelů, audio záznam, video záznam). Hodnotící kritéria se tedy zaměřují na ochranu informací i z jiných pohledů, než je pouze rámec ochrany osobnosti, který bude přítomen již v nejnižší bezpečnostní úrovni; také z tohoto důvodu i nejnižší bezpečnostní úroveň obsahuje technická a organizační opatření k ochraně komunikované informace.

Kritérium ochrany komunikované informace, která je vyžadována právními předpisy, smluvními ujednáními nebo jinými předpisy, se odvíjí především od povinnosti zaměstnanců zachovávat mlčenlivost o skutečnostech, o nichž se dozvěděli při výkonu zaměstnání (obecně zákoník práce, správní řád, případně další speciální právní úprava) nebo od povinností, které zavazují organizaci z důvodu obsahu smluvních ujednání.

Pokud má organizace v plánu využívat videokonference jako běžný pracovní nástroj, je nutno využít videokonferenční systém alespoň úrovně 2.

V organizaci je tedy nutno si stanovit, jaké informace budou v rámci videokonferenčního systému přenášeny, a tyto srovnat s hodnotícími kritérii uvedenými v tabulce. V závislosti na zařazení komunikovaných informací do bezpečnostní úrovně musí videokonference splňovat níže definovaná bezpečnostní opatření.

Tabulka č. 1 Hodnocení bezpečnostní úrovně videokonferenčního systému podle důvěrnosti komunikované informace

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.

V rámci dané bezpečnostní úrovně videokonferenčního systému nesmí dojít k přenosu komunikované informace, která má být přenášena videokonferenčním systémem vyšší bezpečnostní úrovně.

Pro praktické využití se může jevit především jako nehospodárné zajistit pro celou organizaci videokonferenci úrovně 3, přičemž bude pravděpodobný model většinového využití úrovně 2 s doplněním videokonferencí úrovně 3.

S ohledem na to se může jevit jako vhodné rozdělit zaměstnance do skupin podle nejvyšší bezpečnostní úrovně komunikované informace, s jakou zaměstnanec může nakládat (např. řadový zaměstnanec úroveň 2, vedení organizace úroveň 3). V takové úrovni následně zaměstnanec využívá zvolenou videokonferenci. V takovém případě pak uživatel nemusí neustále zvažovat, zda danou informaci může prostřednictvím

videokonference dané bezpečnostní úrovně sdělovat, nebo zda musí použít videokonferenci vyšší bezpečnostní úrovně (nebo sdělit informaci až zcela mimo videokonferenční systém).

Pokud výše uvedené navržené řešení není vhodné, je nutno každého zaměstnance poučit o tom, jaké informace je možné v rámci videokonference dané bezpečnostní úrovně přenášet a dodržování takového pravidla po zaměstnancích vyžadovat.

Pokud organizace používá metodiku Traffic Light Protocol (TLP), je možné ji přiměřeně využít pro zařazení komunikovaných informací, označených podle této metodiky, do bezpečnostní úrovně.

Jako úroveň:

- TLP:WHITE, je označena taková informace, která může být dále poskytována a šířena bez omezení. Případná omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.
- TLP:GREEN je označena informace, která může být sdílena v rámci příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály. Příjemce při předání musí zajistit důvěrnost komunikace informace. Příjemce nesmí informaci poskytnout veřejně, může ji však při splnění a zajištění stejných podmínek ochrany předat dalším partnerským subjektům příjemce.
- TLP:AMBER je označena informace, která může být sdílena pouze v rámci organizace a s pracovníky příjemce, kteří je nezbytně potřebují k výkonu své funkce (need-to-know) a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným než výše uvedeným osobám, nesmí být informace poskytnuta, nebudou-li výslovně stanoveny další osoby, kterým ji lze poskytnout.
- TLP:RED je označena informace, která nemůže být použita jinou osobou než konkrétní osobou na straně příjemce, které byla informace poskytnuta, nebudou-li výslovně stanoveny další osoby, kterým lze tuto informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit po dohodě s původcem informace.

V uvedených případech odpovídá označení:

- TLP:WHITE a TLP:GREEN bezpečnostní úrovni 1
- TLP:AMBER bezpečnostní úrovni 2
- TLP:RED bezpečnostní úrovni 3

Je však potřeba mít na paměti, že použití této metodiky je pouze orientační a směrodatná jsou hodnotící kritéria obsažená ve výše uvedené tabulce: Tabulka č. 1 Hodnocení bezpečnostní úrovně videokonferenčního systému podle důvěrnosti komunikované informace.

4.2 Bezpečnostní opatření – souhrn

Níže uvedená tabulka uvádí, jaká bezpečnostní opatření je nutné splňovat (resp. musí videokonferenční systém splňovat) v rámci jednotlivých bezpečnostních úrovní.

Bezpečnostní opatření se v konkrétní bezpečnostní úrovni (1, 2, 3) zavádějí podle následujícího označení:

N – Bezpečnostní opatření není vyžadováno

D – Bezpečnostní opatření je vhodné zavést (tj. nice to have)

A – Bezpečnostní opatření je nutné zavést (tj. must have)

Tabulka č. 2 Bezpečnostní opatření

Čísla kapitol a podkapitol	Opatření	Bezpečnostní úrovně		
4.3	**Bezpečnostní opatření**	**Úroveň 1**	**Úroveň 2**	**Úroveň 3**
4.3.1	**Autentizace**			
4.3.1.1	Používat centrální správu privilegovaných účtů (LDAP, MSAD apod.)	**D**	**A**	**A**
4.3.1.2	Používat centrální správu uživatelských účtů (LDAP, MSAD apod.)	**N**	**D**	**A**
4.3.1.3	Vynucovat ověřovací údaje a jejich komplexnost	**N**	**D**	**D**
4.3.1.4	Používat vícefaktorovou autentizaci	**N**	**D**	**A**
4.3.1.5	Využívat SSO autentizaci	**N**	**D**	**D**
4.3.1.6	Integrovat proces řízení účtů se stávajícím IdM	**N**	**D**	**D**
4.3.2	**Řízení přístupu a ochrana osobních údajů a zpracovávaných dat**			
4.3.2.1	Oddělit role (admin, poweruser, user …atd.)	**D**	**A**	**A**
4.3.2.2	Využívat možnost zapojení do konference pouze po schválení organizátora	**D**	**A**	**A**
4.3.2.3	Vypnout „auto-answer“ ve Virtuální konferenční místnosti	**A**	**A**	**A**
4.3.2.4	Nastavit oprávnění pro jednotlivé funkcionality videokonference na konkrétní role	**N**	**D**	**A**
4.3.2.5	Integrovat proces řízení rolí se stávajícím IdM	**N**	**D**	**D**
4.3.3	**Řízení systému videokonference**			
4.3.3.1	Zabezpečit napojení na další komunikační platformy (e-mail, kalendář atd.)	**N**	**D**	**A**
4.3.3.2	Implementovat antivir/ antimalware zabezpečení zařízení pro videokoference	**D**	**D**	**A**

Čísla kapitol a podkapitol	Opatření	Bezpečnostní úrovně		
4.3.3.3	Systém musí umožňovat řízení rolí	**N**	**D**	**A**
4.3.3.4	Používat podporovaný a aktualizovaný systém videokonference.	**D**	**A**	**A**
4.3.4	**Bezpečnost zařízení**			
4.3.4.1	Vynucovat bezpečnostní politiky na koncových zařízeních (MDM, Gpo atd.)	**N**	**D**	**A**
4.3.4.2	Provést hardening zařízení a serverů	**N**	**D**	**A**
4.3.4.3	Používat pouze bezpečná IoT zařízení (IP kamery apod.)	**N**	**A**	**A**
4.3.4.4	Používat pouze bezpečná klientská zařízení (stanice, mobilní zařízení) – „zařízení přidělená organizací anebo zařízení, na která byly aplikovány bezpečnostní politiky organizace a která byla schválena do provozu“	**N**	**D**	**A**
4.3.4.5	V případě použití IP telefonů nastavit a dodržovat hardening pro VoIP zařízení	**N**	**D**	**A**
4.3.5	**Bezpečnost komunikací**			
4.3.5.1	Implementovat zabezpečení komunikační infrastruktury (FW-NG /voice-aware firewall/, DMZ, IDS/IPS,)	**N**	**D**	**A**
4.3.5.2	V interní síti lze komunikovat pouze z autentizovaných a autorizovaných zařízení (802.1X, 802.1AE)	**N**	**D**	**D**
4.3.5.3	Implementovat patch management síťových prvků a komunikačních zařízení, používat pouze aktuální software (firmware)	**N**	**D**	**A**
4.3.5.4	Provést hardening síťových prvků a komunikačních zařízení (videokonferenčních serverů)	**N**	**D**	**A**
4.3.6	**Kryptografické prostředky**			
4.3.6.1	Využívat zabezpečení DNS (DNSSEC)	**N**	**D**	**D**
4.3.6.2	Používat zabezpečené protokoly (SIPS (a TLS) pro RTP a RCP, HTTPS), včetně možnosti nastavení kontroly proti MiM, call spoofing apod.	**D**	**A**	**A**
4.3.6.3	Implementace certifikovaného HW HSM	**N**	**N**	**A**
4.3.6.4	Použití bezpečných kryptografických prostředků dle doporučení NÚKIB	**N**	**D**	**A**
4.3.6.5	Šifrování musí být pod kontrolou společnosti po celou dobu přenosu videokonference	**N**	**D**	**A**
4.3.6.6	Využívat důvěryhodnou CA s online publikováním CRL a přímým napojením na HSM	**N**	**A**	**A**

Čísla kapitol a podkapitol	Opatření	Bezpečnostní úrovně		
0	**Bezpečnostní monitoring**			
4.3.7.1	Spravovat a vyhodnocovat bezpečnostní logy (monitorování v oblastech AAA, výměna šifrovacích klíčů, aplikace certifikátů apod.)	**N**	**D**	**A**
4.3.7.2	Vyhodnocovat aplikační logy (průběhy a sestavování hovorů, připojení uživatelů)	**N**	**D**	**A**
4.3.7.3	Napojit videokonferenční systém na log management	**N**	**N**	**A**
4.3.7.4	Napojit videokonferenční systém na SIEM	**N**	**N**	**D**
4.3.7.5	Videokonferenční systém neumožní nahrávání záznamů bez notifikace všech zúčastněných	**D**	**D**	**A**
4.3.7.6	Provádět auditing bezpečnostních nastavení	**D**	**A**	**A**
4.3.7.7	Napojení videokonferenčního systému na DLP řešení	**N**	**D**	**A**
4.3.8	**Cloud – služba videokonference prostřednictvím externího dodavatele**			
4.3.8.1	Zajistit požadavek na uložení dat v EU	**N**	**D**	**A**
4.3.8.2	Doložení certifikace ISO/IEC 27001 pro služby videokonferencí, případně auditní zprávy SOC II Type 2 nebo zajištění auditu na místě	**N**	**A**	**A**
4.3.8.3	Požadovat záruky bezpečné správy (dat, zařízení, software) v cloudu	**A**	**A**	**A**
4.3.8.4	Veškerá komunikace (pokud je to možné zajistit) musí probíhat přes důvěryhodné servery, důvěryhodného dodavatele služby videokonference	**N**	**D**	**D**
4.3.8.5	Na zprostředkujícím/ch zařízení/ch nesmí být trvale ukládána přenášená data	**N**	**A**	**A**

V následujících podkapitolách je uveden detailnější popis těchto bezpečnostních opatření.

4.3 Bezpečnostní opatření – detailní popis

4.3.1 Autentizace

4.3.1.1 Používat centrální správu privilegovaných účtů (LDAP, MS AD apod.)

Privilegované účty využívané pro autentizaci uživatele (administrátora, správce) během videokonference a pro správu videokonference jsou udržovány a spravovány prostřednictvím adresářového serveru, ke kterému je zprostředkován přístup prostřednictvím LDAP (Lightweight Directory Access Protocol), MS AD (Microsoft Active Directory) apod.

Cíl opatření:

Implementace centrální správy privilegovaných účtů snižuje riziko, že jsou vytvářeny neevidované účty, změny nejsou evidované, a pokud pomine důvod existence účtu, není tento účet zneplatněn a hrozí riziko zneužití, například bývalým zaměstnancem. Zároveň se u lokálních účtů zvyšuje riziko prolomení jejich důvěrnosti, zejména pak při nedostatečné kontrole a bezpečnostních nastaveních na zařízení.

4.3.1.2 Používat centrální správu uživatelských účtů (LDAP, MS AD apod.)

Uživatelské účty využívané pro autentizaci uživatele během videokonference a pro správu videokonference jsou udržovány a spravovány prostřednictvím adresářového serveru, ke kterému je zprostředkován přístup prostřednictvím LDAP (Lightweight Directory Access Protocol), MS AD (Microsoft Active Directory) apod.

Cíl opatření:

Implementace centrální správy uživatelských účtů snižuje riziko, že jsou vytvářeny neevidované účty, změny nejsou evidované a pokud pomine důvod existence účtu, není tento účet zneplatněn a hrozí riziko zneužití, například bývalým zaměstnancem. Zároveň se u lokálních účtů zvyšuje riziko prolomení jejich důvěrnosti, zejména pak při nedostatečné kontrole a bezpečnostních nastaveních na zařízení.

4.3.1.3 Vynucovat ověřovací údaje a jejich komplexnost

Pro ověření musí být vynucovány dostatečně komplexní ověřovací údaje, odolné proti útoku hrubou silou. Pro uživatelské účty platí následující pravidla:

- minimální délka hesla je 10 znaků,
- zákaz používaní stejného hesla (posledních 12 hesel),
- maximální doba platnosti hesla je 18 měsíců,
- zamčení účtu po 10 neplatných pokusech zadání hesla v řadě,
- jednorázové prvotní heslo, které musí být změněno po prvním přihlášení nebo zneplatněno po 24 hodinách.

Tato pravidla je nutné chápat jako minimální doporučení a jejich implementace může být přísnější.

Cíl opatření:

Nedostatečná komplexnost ověřovacích údajů (složitost hesla) může zapříčinit snadné prolomení tohoto údaje a následné zneužití účtu pro kompromitaci systému a napadení videokonference.

4.3.1.4 Používat vícefaktorovou autentizaci

Pro ověřování je nutné používat 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 vícefaktorové ověření je založeno na kombinaci alespoň dvou z následujících tří typů faktorů: 1) vlastnictví nějakého fyzického předmětu (karta, token, generátor náhodného kódu svázaný s konkrétním předmětem), 2) znalosti (PIN, heslo atd.) nebo 3) biometrie.

4.3.1.5 Využívat SSO autentizaci

Na zabezpečeném zařízení je využíváno k ověření SSO (Single Sign On). Ověření k systému je provedeno na základě důvěry k již jednou provedenému ověření uživatele, uživatelského účtu vůči centrálnímu IdM server (např. LDAP nebo MS AD).

Cíl opatření:

Tím, že není vyžadováno několikanásobné ověření identity opětovným přihlášením již jednou autentizovaného uživatele, se snižuje riziko kompromitace přihlašovacích údajů. Pokud je pro prvotní přihlášení používáno silné ověření vícefaktorovou autentizací, pak by následné ověření jiným způsobem pouze snižovalo důvěryhodnost tohoto ověření. Při správné implementaci SSO navíc nejsou systému předávány přihlašovací údaje uživatele a je tak sníženo riziko možného úniku těchto údajů.

4.3.1.6 Integrovat proces řízení účtů se stávajícím IdM

Pro správu účtů (vytváření, změny a rušení) je nastaven bezpečný proces obsahující evidenci a schvalovací postupy tak, aby bylo zabráněno vzniku nežádoucích oprávnění a aby veškeré činnosti týkající se správy účtů, byly evidované. Pro řízení těchto procesů je používán specializovaný systém IdM (Identity management).

Cíl opatření:

Použití nástroje pro řízení identit umožňuje systémovou správu oprávnění a pomáhá zamezit nahodilým chybám při zadávání, změnách či odebírání oprávnění. Pomáhá nastavit řízený proces a přehlednou evidenci s možností zjednodušit pravidelnou kontrolu. Napomáhá k efektivnímu využívání licencí a zamezuje nevyžádané eskalaci oprávnění. V neposlední řadě snižuje riziko zneužití neaktivních účtů, anebo zapomenutých privilegovaných účtů.

4.3.2 Řízení přístupu a ochrana osobních údajů a zpracovávaných dat

4.3.2.1 Oddělit role

Nastavení oprávnění pro správu a provoz videokonferenčního systému je realizováno prostřednictvím přidělených rolí. Oprávnění není přiřazeno napřímo k jednotlivým účtům. Role jsou oddělené tak, aby nebylo možné přiřazovat a zároveň využívat oprávnění pod jedním a týmž účtem.

Cíl opatření:

Zajištění oddělení rolí podle jim přidělených oprávnění snižuje riziko, že dojde ke kompromitaci privilegovaných účtů administrátorů a zároveň je chráněn videokonferenční systém před nahodilými, nechtěnými, změnami zabezpečení způsobenými méně zkušenými uživateli. Zjednoduší se i správa privilegovaných účtů.

4.3.2.2 Využívat možnost zapojení do konference pouze po schválení organizátora

Videokonferenční systém musí umožňovat, aby vstup uživatele do konference byl povolen pouze po schválení organizátorem (moderátorem) videokonference.

Cíl opatření:

Tím, že kromě přidělení rolí je přístup podmíněn ještě i schválením organizátora schůzky, je zajištěno, aby informace byly poskytované pouze oprávněným uživatelům k dané problematice. Není efektivní zřizovat role pro každou session zvlášť.

4.3.2.3 Vypnout „auto-answer" mód ve Virtuální konferenční místnosti u řešení, která toto podporují

Systém musí umožňovat vypnutí „auto-answer" módu. Tento mód bývá ve výchozím nastavení vypnut. Jedná se zejména o systémy VoIP a Polycom, kdy může být nastaveno automatické vyzvednutí „hovoru".

Cíl opatření:

Auto-answer mód může představovat riziko z hlediska nahodilého přístupu uživatele a zároveň může mít dopad na přetížení systému v případě mnohočetného připojení uživatelů.

4.3.2.4 Nastavit oprávnění pro jednotlivé funkcionality videokonference na konkrétní role

Systém pro videokonference umožňuje nastavení jednotlivých oprávnění prostřednictvím rolí. Oprávnění není nastaveno na jednotlivé konkrétní uživatele zvlášť.

Cíl opatření:

Tím, že jsou oprávnění svázána s rolí a nikoli pouze s konkrétním účtem uživatele, je zajištěno, že nedojde k nekonzistenci oprávnění v případě uživatelů s obdobnými potřebami či požadavky. Při rušení anebo změně potřeb je snazší editovat jednotlivé role než mnoho jednotlivých oprávnění u více účtů. Správa je přehlednější a méně náchylná k chybám.

4.3.2.5 Integrovat proces řízení rolí se stávajícím IdM

Pro přiřazení jednotlivých rolí ke konkrétním uživatelským účtům (vytváření, změny a rušení) je nastaven bezpečný proces, obsahující evidenci a schvalovací postupy tak, aby bylo zabráněno vzniku nežádoucích oprávnění a aby veškeré činnosti týkající se správy oprávnění byly evidovány. Pro řízení těchto procesů je využíván specializovaný systém IdM (Identity management).

Cíl opatření:

Tím, že je správa rolí prováděna prostřednictvím k tomu určeného informačního systému, je zajištěna jejich jednodušší správa a zároveň přehledné svázání rolí s účty po celou dobu jejich životního cyklu. IdM systém přispívá k efektivnímu využití licencí a možnosti kontroly přidělených oprávnění. Pomáhá zajistit transparentní schvalovací proces spojený s řízením rolí.

4.3.3 Řízení systému videokonference

4.3.3.1 Zabezpečit napojení na další komunikační platformy (e-mail, kalendář atd.)

Napojení dalších komunikačních platforem je řízeno tak, aby bylo zamezeno úniku dat jinými, neřízenými kanály mimo videokonferenční systém.

Cíl opatření:

Opatření zabezpečí, aby nedošlo k úniku informací prostřednictvím přidružených služeb, které nejsou součástí řízení videokonference.

4.3.3.2 Implementovat antivir/antimalware zabezpečení zařízení pro videokonference

Všechna zařízení, je-li to technicky realizovatelné, jak na straně serverové, tak na straně koncových stanic, mají implementovanou ochranu proti škodlivému kódu. Tato ochrana je pravidelně aktualizována a kontrolována.

Cíl opatření:

Vzhledem k množství škodlivého kódu (malware[2]) vyskytujícího se v kybernetickém prostředí je tato ochrana základním, avšak ne jediným a samostatně dostačujícím prvkem zabezpečení kybernetické bezpečnosti. Zabraňuje infekci zařízení známým škodlivým kódem a následnému ohrožení bezpečnosti dat. Jde hlavně o infekci v důsledku přenosu souborů obsahujících tento škodlivý kód.

4.3.3.3 Systém musí umožňovat řízení rolí

Videokonferenční systém umožňuje řízení oprávnění prostřednictvím rolí a jejich správu pomocí externího identity managementu (IdM).

Cíl opatření:

Oddělením rolí pro administraci a řízení konference, aktivního a pasivního uživatele, je efektivně zabezpečen videokonferenční systém, a to i v případě většího počtu uživatelů, bez nutnosti individuálních nastavení na konkrétního uživatele. Napojení na IdM minimalizuje riziko nechtěného přidělení oprávnění. V případě kompromitace uživatelského účtu není ohrožen celý videokonferenční systém, ale pouze data v rozsahu dané role přidělené účtu.

4.3.3.4 Používat podporovaný a aktualizovaný systém videokonference

Videokonferenční systém musí být provozován pouze v podporované, aktualizované a schválené verzi. Nesmí obsahovat neošetřené známé kritické zranitelnosti. Stejně tak všechna zařízení využívaná pro videokonference musí mít pravidelně aktualizovaný software i firmware tak, aby videokonference byla provozována pouze na bezpečné verzi systému. Toto se týká také jednotlivých softwarových knihoven a IoT zařízení, jako jsou IP kamery a další sofistikovaná zařízení. Anebo je nutné snížit riziko jiným způsobem

[2] Petr JIRÁSEK, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* 3., doplněné a upravené vydání. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

(vypnutím služby, izolací prostředí atd.). Proces řízení aktualizací si stanoví organizace, a to včetně způsobu, četnosti kontrol a časových rámců.

Cíl opatření:

Pokud systém není náležitě aktualizovaný se všemi bezpečnostními opravami, hrozí neúměrné riziko jeho kompromitace a následný únik dat. Vzhledem k tomu, že jde zpravidla o videokonferenční systém, komunikující prostřednictvím nezabezpečeného prostředí internetu, je riziko, že v případě kompromitace videokonferenčního systému může (v případě že to umožní architektura a další okolnosti), dojít až ke kompromitaci celého prostředí organizace. A tím k daleko rozsáhlejším škodám než pouze na datech v rámci videokonference.

4.3.4 Bezpečnost zařízení

4.3.4.1 Vynucovat bezpečnostní politiky na koncových zařízeních (MDM, GPO atd.)

Koncová zařízení pro videokonference mají nastavené a vynucované politiky tak, aby bylo znemožněno, anebo alespoň znesnadněno, neautorizované použití prostředků zařízení či jeho kompromitace.

Cíl opatření:

Vynucením bezpečnostních politik na koncových zařízeních organizace lze snížit riziko, že dojde k jejich napadení a zneužití k dalším škodlivým činnostem, ať už vůči internímu systému organizace anebo i k útoku proti jiné organizaci, což může vést k nechtěné publicitě a reputačním škodám.

4.3.4.2 Provést hardening zařízení a serverů

Pro všechny severy a koncové stanice je určeno a schváleno bezpečné nastavení (hardening), včetně schválených výjimek. Bezpečné nastavení vychází z doporučení výrobců či dodavatelů a je v souladu s obecnými standardy (např. CIS Benchmarks[3]).

Cíl opatření:

Vynucení bezpečnostních politik na serverech a koncových zařízeních sníží riziko náhodné, nechtěné změny v konfiguraci, která umožní kompromitaci systému. Tomu musí předcházet analýza a schválení tzv. bezpečné konfigurace, která je pak organizací kontrolována a vynucována.

4.3.4.3 Používat pouze bezpečná IoT zařízení (IP kamery apod.)

Pro videokonferenční systém jsou používána pouze taková IoT zařízení, u nichž není známá neošetřená kritická zranitelnost a od výrobce je garantovaná podpora.

Cíl opatření:

Významným rizikem posledních let se jeví různé útoky prováděné prostřednictvím tzv. internetu věcí (IoT). Jedná se zejména o technologická zařízení, která však obsahují řídící kód, jsou napojena na internet, a přesto

[3] https://www.cisecurity.org/cis-benchmarks/ obsahuje více než 140 bezpečných konfigurací pro různé technologické skupiny, vytvořených skupinou bezpečnostních expertů.

obsahují neošetřené chyby. Jsou chráněna pouze minimálními prvky zabezpečení. Prostřednictvím těchto zařízení, což jsou například internetové kamery, pak dochází k útokům na třetí strany anebo ke zneužití například obrazových dat snímaných zranitelnou internetovou kamerou.

4.3.4.4 Používat pouze bezpečná klientská zařízení (stanice, mobilní zařízení) – „jen pracovních – přidělených zařízení“

Pro zprostředkování videokonference jsou použita pouze ta koncová zařízení, která jsou schválena organizací. Nelze používat zařízení (veřejná koncová zařízení, BYOD – zařízení ve vlastnictví uživatele), která nemůže mít organizace pod svoji plnou kontrolou, anebo která nejsou pod kontrolou organizace prostřednictvím MDM.

Cíl opatření:

U neschválených, neřízených zařízení není možné zajistit bezpečnost videokonferencí. Organizace neumožňuje používání jí neschválených koncových zařízení a komunikačních stanic. Toto schválení zabezpečí, že pravidla týkající se zařízení pro videokonferenci, budou aplikovatelná.

4.3.4.5 V případě použití IP telefonů nastavit a dodržovat politiky pro VoIP zařízení (hardening)

V případě použití VoIP zařízení musí být nastaveny a dodržovány politiky stejně jako u ostatních zařízení, včetně specifických bezpečnostních doporučení (hardening) pro tato zařízení.

Cíl opatření:

Tím, že je provedeno bezpečné nastavení i na specifických zařízeních připojených do videokonference, sníží organizace riziko napadení jak videokonferenčního systému, tak i další infrastruktury organizace.

4.3.5 Bezpečnost komunikací

4.3.5.1 Implementovat zabezpečení komunikační infrastruktury (FW-NG, DMZ, IDS/IPS atd.)

Interní infrastruktura obsahuje bezpečnostní prvky, vycházející z vlastní analýzy rizik a způsobu realizace videokonference, jako jsou: FW-NG (voice-aware firewall), DMZ, IDS/IPS atd.

Cíl opatření:

Nedostatečným zavedením bezpečnostních prvků při návrhu a realizaci infrastruktury se organizace vystavuje riziku, že nebude možné zjistit případné hrozby, infrastruktura bude náchylná k realizaci těchto hrozeb a nebudou existovat ani technické prostředky, jak se hrozbám bránit. Toto může mít dopad, kromě jiného i na bezpečnost videokonferenčního systému.

4.3.5.2 V interní síti lze komunikovat pouze z autentizovaných a autorizovaných zařízení

Zařízení pro videokonference v interní síti jsou vždy autentizovaná a autorizovaná. Do interních sítí určených pro videokonferenční systém není umožněno připojit jiná než schválené zařízení.

Cíl opatření:

Tím, že by nebyla komunikační sít chráněna před připojením neautorizovaných a neschválených zařízení, se vystavujete riziku, kdy muže být videokonferenční systém organizace napaden umožněním přímého fyzického přístupu.

4.3.5.3 Implementovat patch management síťových prvků a komunikačních zařízení, používat pouze aktuální software (firmware)

Všechna síťová zařízení využívaná pro videokonference musí mít pravidelně aktualizovaný software i firmware tak, aby videokonference byla provozována pouze na bezpečné infrastruktuře. Proces řízení si stanoví organizace. Včetně způsobu, četnosti kontrol a časových rámců.

Cíl opatření:

Pokud jednotlivé síťové prvky systému nejsou náležitě aktualizovány, se všemi bezpečnostními opravami, hrozí neúměrné riziko jejich kompromitace a následného úniku dat. V případě kompromitace jednotlivých prvků infrastruktury, může v případě, že to umožní architektura a další okolnosti, dojít až ke kompromitaci celého prostředí organizace a tím pádem k daleko rozsáhlejším škodám než pouze na datech v rámci videokonference.

4.3.5.4 Provést hardening síťových prvků a zařízení

Všechny sítové prvky a zařízení, která to umožňují, musí být nastavena v bezpečné konfiguraci, tzv. hardening, vycházející z doporučení výrobců, či dodavatelů, anebo podle obecně uznávaných standardů (např. CIS Benchmarks).

Cíl opatření:

Nastavení bezpečnostních politik (hardening) na síťových prvcích organizace se sníží riziko napadení. Tomu musí předcházet analýza a schválení tzv. bezpečné konfigurace, která je pak kontrolována a vynucována. Organizace tím zamezí možnému zneužití chyb v nastavení a také zranitelností v rámci nepotřebných, nepoužívaných služeb, které však mohou být zneužité pro napadení.

4.3.6 Kryptografické prostředky

4.3.6.1 Využívat zabezpečení DNS (DNSSEC)

Pro překlad adres během komunikace v rámci videokonference jsou využívány zabezpečené DNS servery podporující technologii DNSSEC. Taktéž všechny použité domény jsou zabezpečeny touto technologií.

Cíl opatření:

Využitím zabezpečených DNS serverů lze předejít riziku přesměrování komunikace na podvržený videokomunikační server a útoku typu MiTM (Man-in-the-middle).

4.3.6.2 Používat zabezpečené protokoly, včetně možnosti nastavení kontroly proti MiM, call spoofing apod.

Pro přenos dat během videokonference musí být používány výhradně bezpečné a zabezpečené protokoly, odolné proti útokům MiM, Call spoofing atd. Šifrování musí být realizováno mezi koncovými zařízeními bez

přerušení a bez možnosti přístupu k obsahu přenášených dat ze strany zprostředkujících zařízení. Ujistěte se, že řešení je realizováno dle těchto požadavků.

Mezi tyto protokoly patří zejména:

- HTTPS s využitím HSTS a TLSv1.2 a novější
- SIPS s využitím TLSv1.2 a novější
- SRTP v souladu s požadavky RFC 3711[4], 5124 a 6904
- DTLS verze 1.2 a vyšší

Cíl opatření:

Zavedením těchto protokolů, respektive vyloučením nezabezpečených protokolů, anebo vyloučením použití slabých šifer, výrazně snižujete riziko napadení komunikace v rámci videokonference, které může vést ke ztrátě zabezpečení přenášených dat. V případně použití nezabezpečených protokolů používajících slabé šifry hrozí napadení a kompromitace nejen komunikace v rámci videokonference.

4.3.6.3 Implementace certifikovaného HW HSM

V případě, že videokonference je realizovaná prostřednictvím serverů umístěných v nedůvěryhodném prostředí či v cloudovém prostředí dodavatele služby, je v závislosti kritičnosti přenášených informací nezbytné pro zabezpečení dat ukládaných v datovém úložišti dodavatele využít HSM umístěný u dodavatele. Pokud ten neumožňuje využití bezpečného cloudové HSM řešení, a kritičnost komunikace v rámci videokonference tomu odpovídá, je třeba zabezpečit veškerou komunikaci prostřednictvím hardwarového modulu pro šifrování (HW HSM) na bezpečnostním perimetru organizace. Veškerá komunikace v rámci videokonference pak musí probíhat prostřednictvím tohoto šifrovacího zařízení.

Doporučené certifikace:

- FIPS 140-2 level 2 a vyšší
- FIPS 140-3 level 2 a vyšší
- Common Criteria minimálně EAL4 a vyšší

Cíl opatření:

Aby byla zajištěna důvěrnost přenášených dat, musí být šifrování realizováno tak, aby organizace měla celý proces pod vlastní kontrolou. K šifrování se využívají hardwarové šifrovací moduly (včetně virtuálních HSM), které však je třeba také chránit. Což je možné nejlépe realizovat, pokud jsou umístěny v perimetru organizace. V případě umístění HSM mimo perimetr organizace, musí být zajištěna bezpečná správa šifrovacích klíčů. Šifrovací klíče a jejich správa, musí být plně pod kontrolou organizace.

---

[4] RFC 3711 – The Secure Real-time Transport Protocol (SRTP)
RFC 5124 – Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF)
RFC 6904 – Encryption of Header Extensions in the Secure Real-time Transport Protocol (SRTP)

4.3.6.4 Použití kryptografických prostředků dle doporučení NÚKIB

Pro šifrování videokonference musí být vždy použity výhradně odolné šifrovací algoritmy a klíče s dostatečnou délkou, dle použitého algoritmu. Pro určení bezpečnostních parametrů se primárně řídí organizace aktuálním doporučením NÚKIB v oblasti kryptografických prostředků. Doporučení lze nalézt na webových stránkách NÚKIB.

Cíl opatření:

Protože každý kryptografický algoritmus má svoji životnost a po nějaké době je prolomen, ať už hrubou silou anebo nalezením chyby v algoritmu, je třeba používat takové šifrovací klíče a algoritmy u nichž není taková hrozba známa. Proto jsou vydávána nejen upozornění na tyto hrozby, ale také doporučení. Jedním ze zdrojů je i doporučení NÚKIB.

4.3.6.5 Šifrování musí být pod kontrolou organizace po celou dobu přenosu videokonference

Řešení videokonference musí být navrženo a realizováno tak, aby po celou dobu přenosu přes nedůvěryhodné prostředí (internet, dodavatel) byla zajištěna kontinuita zabezpečení (šifrování). Šifrování nesmí být ve správě dodavatele, ale organizace. Šifrování je realizováno na koncové stanici, či pomocí HSM on premise, anebo HSM na straně dodavatele v případě ukládání sdílených dat. Správa klíčů pro šifrování videokonference (v aplikaci anebo HSM) musí být vždy výhradně v režii organizace (uživatele služby). A to, i pokud je využíván HSM dodavatele služby videokonference. Systém pro správu klíčů musí umožnit organizaci řídit životní cyklus klíčů. Vyměnit šifrovací klíče, nebo je zneplatnit. V případě, že by byl videokonferenční systém využíván pro přenos citlivých dat, je doporučeno systém správy klíčů integrovat s Hardware Security Modulem (HSM).

Cíl opatření:

Pokud by bylo šifrování komunikace po cestě přenosu přerušeno, dešifrováno (například dodavatelem služby) a následně opět šifrováno, hrozí, že jednak nebude organizace schopna potvrdit konzistentnost komunikace a podle toho, kde k dešifrování dojde, je zde i riziko kompromitace vlastních přenášených dat v rámci videokonference. Slabým místem každého šifrování je nakládání (generování, ukládání, rušení) s šifrovacími klíči a certifikáty a zabezpečení jejich důvěrnosti. Pokud nemá organizace tento proces pod svojí kontrolou, hrozí riziko jejich zneužití.

4.3.6.6 Využívat důvěryhodnou CA s online publikováním CRL a přímým napojením na HSM

Pro generování certifikátů a klíčů musí být používány výhradně důvěryhodné certifikační autority. Důvěryhodnou certifikační autoritou (CA) se rozumí buď CA pod kontrolou organizace, kvalifikovaná CA dle EIDAS anebo CA, jež je uvedena v seznamu certifikačních autorit výrobce (např. v operačním systému Microsoft a či v seznamu od společnosti Mozilla[5]). Certifikační autorita musí využívat tzv. Certificate Transparency dle RFC 6962.

Cíl opatření:

[5] Dostupné zde: https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport

Pokud by hrozilo, že je certifikát (CA) a následně i šifrovací klíč kompromitován, a toto by nebylo možné online ověřit, hrozí riziko, že dojde k ohrožení důvěrnosti komunikace, aniž by to byla organizace schopna zjistit.

4.3.7 Bezpečnostní monitoring

4.3.7.1 Spravovat a vyhodnocovat bezpečnostní logy (monitorování v oblastech AAA, výměna šifrovacích klíčů, aplikace certifikátů apod.)

Řešení pro realizaci videokonference musí umožňovat sběr bezpečnostních auditních záznamů (logů) v požadované míře, vycházející z požadavků legislativy a best practice. Jde zejména o oblasti autentizace, autorizace, accounting, správu klíčů a certifikační služby. Kritické operace (mnohočetné pokusy o přihlášení apod.) musí být monitorovány a oznamovány.

Cíl opatření:

Aby bylo možné předcházet různým typům hrozeb a také odhalit jejich zneužití, je třeba mít dostatečné informace o činnostech a fungování celého videokonferenčního systému. Proto je nutné zajistit dostatečné zaznamenávání událostí na systému a jejich konsolidaci pro potřeby vyhodnocování.

4.3.7.2 Vyhodnocovat aplikační logy (průběhy a sestavování hovorů, připojení uživatelů)

Řešení pro realizaci videokonference musí umožňovat sběr aplikačních logů o činnostech správců a uživatelů. Záznamy musí být organizaci k dispozici v požadované míře vycházející z požadavků bezpečnosti. Musí odrážet historii, jak bylo nakládáno s chráněnými údaji během realizace videokonference.

Cíl opatření:

Sníží se hrozba neoprávněného nakládání s údaji. Je možné dohledat, kdo a kdy provedl jakou operaci, jako je například změna nastavení přístupu ke službě apod.

4.3.7.3 Napojit videokonferenční systém na log management

Řešení pro realizaci videokonference musí umožňovat sběr auditních záznamů a jejich export pro potřeby vyhodnocování a archivace. Během celého procesu nakládání s auditními záznamy musí být zabezpečeny proti nechtěné či úmyslné změně či vymazání. Například pro potřeby forenzního vyšetřování. Toto je zajištěno nastavením procesu zpracování auditních záznamů s použitím specializovaných nástrojů.

Cíl opatření:

Vzhledem k obecně velkému množství událostí na systému a také různému způsobu jejich sběru, je velice těžko realizovatelná jejich konsolidace a ochrana bez specializovaného systému. Tento systém, tzv. Log management, také pomáhá s jejich efektivní komprimací, šetření prostoru pro jejich ukládání, a chrání je před úmyslným, či neúmyslným, zničením anebo změnou.

4.3.7.4 Napojit videokonferenční systém na SIEM

Auditní záznamy pořízené při realizaci videokonference musí být vyhodnocovány prostřednictvím SIEM.

Cíl opatření:

Protože množství auditních záznamů, logů, a jejich provázanost je obvykle nad možnosti ručního vyhodnocování, je nutné používat na tuto činnost nástroj pro jejich automatické vyhodnocování, SIEM. V něm jsou zpravidla předdefinovány známé sledy událostí anebo jejich typů, které značí možné napadení anebo chyby systému.

4.3.7.5 Videokonferenční systém neumožní nahrávání záznamů bez notifikace všech zúčastněných

Auditní záznamy musí obsahovat také údaje související s ochranou osobních údajů dle GDPR (údaje o záznamech atd.) Tam, kde je to třeba, je dotčený uživatel neprodleně informován o zpracování svých osobních údajů (nahrávání hlasu či videa) a to prokazatelně a neprodleně. Zároveň musí být umožněno s takovou činností vyjádřit jeho souhlas, či zrušení tohoto zpracování.

Cíl opatření:

V souvislosti se zákonnou povinností ochrany osobních údajů (GDPR, zákon č. 110/2019 Sb.) existuje riziko, že bez možnosti řádného auditu a notifikace nebude možné splnit povinnosti získávat a evidovat souhlas se zpracováním osobních údajů při používání videokonference. Navíc se v případě videokonferencí může jednat o nakládání s osobními údaji zvláštního charakteru (hlas, podoba). Tento požadavek umožňuje dodržení uvedených zákonných nařízení.

4.3.7.6 Provádět audit bezpečnostních nastavení

Součástí provozování videokonferenčního systému v organizaci musí být i audit bezpečnostních nastavení či postupů a jejich dodržování. Audit je prováděn v pravidelných intervalech a při změnách, které mohou mít negativní dopad na zabezpečení systému. Při stanovení četnosti výkonu auditu je třeba zvážit povahu a rozsah rizik a dopady spojené s provozem videokonferenčního systému. Audit je možné provádět vlastními zdroji, kdy osoba vykonávající audit musí být pro tuto činnost vyškolena a je nutné, aby byla zajištěna její nezávislost. V případě auditu s využitím třetí strany, je potřeba interně určit osobu, která bude dohlížet na jeho průběh. Výsledky auditu slouží k průběžnému vyhodnocování bezpečnosti informací a pro plánování zlepšení.

Cíl opatření:

Součástí auditních záznamů musí být monitorování změn v bezpečnostních nastaveních, jež by mohly způsobit ohrožení systému. Pokud organizace nezná aktuální stav nastavení a dodržení souladu se schválenými politikami, vystavuje se riziku napadení systému či ztráty dat.

4.3.7.7 Napojení videokonferenčního systému na DLP řešení

Při přenosu textových informací či souborů, obsahujících chráněné informace používejte systém pro ochranu dat DLP.

Cíl opatření:

Protože se v rámci videokonference mohou přenášet dokumenty, a i různá nestrukturovaná data, včetně osobních údajů a dalších chráněných informací, hrozí riziko jejich nechtěného anebo úmyslného zveřejnění,

anebo jiné porušení jejich důvěrnosti. Systém DLP může tomuto porušení pomoct zabránit a řídit jejich pohyb v rámci organizace a při odesílání mimo organizaci.

4.3.8 Cloud – služba videokonference prostřednictvím externího dodavatele

4.3.8.1 Zajistit požadavek na uložení dat v EU

V případě použití řešení videokonference, využívajícího cloudová řešení pro přenos dat, je nutné, aby uložení zákaznických dat bylo v rámci jurisdikce EU. Toto se týká zejména případů, kdy nelze zaručit, že data jsou bezpečně chráněna šifrováním v režii organizace a nejsou ukládána v cloudovém prostředí v průběhu přenosu, a to ani dočasně.

Pokud by mělo dojít k předání dat, a to jak komunikovaných informací, tak s nimi spojených metadat, do zemí mimo EU, potom musí být splněny následující podmínky:

- musí být splněny podmínky GDPR pro předávání osobních údajů, zejm. články 44 až 49 GDPR,
- k takovému předání musí dojít pouze v nezbytně nutném případu, v nezbytně nutném rozsahu a na nezbytně nutnou dobu,
- v případě předání komunikovaných informací nebo metadat musí být organizace informována, kam jsou tato data předávána, na jakou dobu, z jakého důvodu a v jakém rozsahu.

Organizace musí zohlednit i rizika, pokud je uživatel videokonference mimo EU.

Cíl opatření:

Protože je Česká republika součástí Evropské Unie a jejího právního prostředí, je více než vhodné využívat cloudové služby spadající pod tuto legislativu. Tímto si organizace zajistí právní jistotu v případě řešení problémů s poskytováním cloudových služeb videokonference.

4.3.8.2 Doložení certifikace ISO/IEC 27001 pro služby videokonferencí

Protože organizace nemá možnost přímo ovlivnit bezpečnost dodavatele cloudového řešení anebo jím poskytovaných služeb, je třeba doložit úroveň bezpečnosti dodavatelem. K tomu nejlépe slouží potvrzené doložení souladu. Proto musí organizace vyžadovat, aby byl dodavatel držitelem certifikátu, dokládajícího soulad se standardem pro řízení ISMS, ISO/IEC 27001. A to konkrétně pro daný videokonferenční systém. Certifikát musí být aktuálně platný.

V případě, že dodavatel nemá certifikaci ISO/IEC 27001, a bezpečnostní úroveň videokonference tomu odpovídá, musí organizace při využívání služeb cloudu pro videokonference požadovat po dodavateli předložit vhodný ekvivalent (například auditní zprávu SOC II Type 2 nebo jinak zajistit provedení auditu na místě).

Cíl opatření:

Vzhledem k tomu, že většinou není reálné, aby organizace mohla provádět sama dostatečné posouzení stavu řízení bezpečnosti u dodavatele cloudových služeb, je nutné zajistit potřebnou důvěru jiným způsobem.

Jednou z možností je platná certifikace vydaná akreditovanou certifikační společností v působnosti EU. Nicméně, i tak je třeba ověřit rozsah certifikovaných služeb.

4.3.8.3 Další možností, jak ověřit bezpečnost poskytovaných cloudových služeb v rámci videokonference je doložení auditní zprávy dle SOC II Type 2, týkající se dodavatele těchto služeb případně zajištění auditu na místě jiným způsobem. Požadovat záruky bezpečné správy (dat, zařízení, software) v cloudu

V případě, že není dodavatel cloud řešení držitelem certifikátu ISO/IEC 27001 nebo ekvivalentu (např. auditní zprávy SOC II Type 2), požadujte smluvně jiné záruky bezpečné správy systému. Službu lze používat pouze tehdy, pokud existují záruky odpovídající bezpečnostní úrovni videokonference a souvisejícím rizikům. Službu videokonference nelze používat bez odpovídajících bezpečnostních záruk.

Cíl opatření:

Pokud by nebyl dodavatel služby schopen dodat žádné z výše uvedených standardizovaných potvrzení úrovně bezpečnosti videokonference, pak je nutno, v závislosti na kritičnosti dat přenášených v rámci videokonference, zvážit jiný způsob záruky. Vždy je však třeba usilovat o smluvní zajištění možného auditu bezpečnosti u dodavatele v místě poskytování služby. Organizace takto může snížit rizika vyplývající z nedostatků v řízení bezpečnosti u dodavatele a zajistit i soulad s požadavky zákona na bezpečnost při řízení dodavatelů.

4.3.8.4 Veškerá komunikace (pokud je to možné) musí probíhat přes důvěryhodné servery, důvěryhodného dodavatele služby videokonference.

V rámci řešení, kdy nemá organizace pod kontrolou všechny komponenty, jejichž prostřednictvím je videokonference realizována, musí ověřit, že komunikace v rámci videokonference je realizována výhradně prostřednictvím důvěryhodných serverů důvěryhodného dodavatele.

Cíl opatření:

V případě, že se při realizaci videokonference jedná o data hodnocená vyšším stupněm rizika, je třeba, aby organizace požadovala realizaci spojení výhradně prostřednictvím důvěryhodných zařízení dodavatele cloudové služby. Tím bude minimalizováno riziko sofistikovaného porušení důvěrnosti komunikace.

4.3.8.5 Na zprostředkujícím/ch zařízení/ch nesmí být trvale ukládána přenášená data.

Přenášená data nesmí být na zařízeních zprostředkujících přenos trvale ukládána. Při dočasném uložení musí být zajištěna jejich dostatečná ochrana a toto musí být pouze na omezenou jasně definovanou dobu.

Cíl opatření:

Pokud by byla přenášená data trvale ukládána v prostředí dodavatele, hrozí, že při ukončení služby zůstanou neřízena a bude možné jejich zneužití například s použitím hrubé síly i v případě, že jsou chráněna šifrováním.

4.4 Další bezpečnostní doporučení

V této kapitole jsou uvedena doporučení, která nemíří na zabezpečení důvěrnosti videokonference, ale jež je třeba vzít v úvahu při návrhu řešení, a to zejména k pokrytí rizik spojených s integrací do stávající infrastruktury organizace, jako je například dostupnost videokonference a ostatních systémů na sdílené infrastruktuře.

Tabulka č. 3 Další bezpečnostní doporučení

Čísla kapitol a podkapitol	Doporučení
4.4	**Další bezpečnostní doporučení**
4.4.1	Použít řízení kvality komunikace v síti (QoS) pro nastavení kapacit pro videokonference
4.4.2	Pro externí připojení na videokonferenci nepoužívat nezabezpečené veřejné sítě (WiFi hotspots)
4.4.3	Zajistit, že videokonferenční systém neumožní nahrávání záznamů bez vědomí všech zúčastněných
4.4.4	Ověřit, že řešení podporuje oddělený přenos zvuku, obrazu, souborů, textu (Chat).
4.4.5	Data musí být vždy pod kontrolou vlastníka
4.4.6	Provést oddělení komunikace videokonferencí od ostatní datové komunikace (pro videokonference, VoIP – Polycom apod.)
4.4.7	Implementovat DoS/DDoS ochranu
4.4.8	Zajistit redundanci infrastruktury, load balancing
4.4.9	Provádět testování infrastruktury proti výpadkům
4.4.10	Provádět a vyhodnocovat penetrační testy, testy DoS/DDoS
4.4.11	Požadavky na zabezpečení cloudových služeb se musí odvíjet podle úrovně poskytované služby (SaaS, Paas, IaaS)
4.4.12	Vyžadovat od dodavatele cloudových služeb minimálně stejnou úroveň zabezpečení, jako při realizaci videokonference vlastními prostředky společnosti.
4.4.13	Požadovat stejnou úroveň zabezpečení u všech subdodavatelů, jejichž činnost může mít vliv na kvalitu a bezpečnost poskytované videokonference.

4.4.1 Použít řízení kvality komunikace v síti (QoS) pro nastavení kapacit pro videokonference

V případě, že videokonference je realizovaná na sdílené síti s jiným typem služby, a komunikační toky nejsou oddělené, je nutné v komunikaci vynucovat řízení přenosových kapacit, určených pro službu videokonference (technologický parametr QoS).

Cíl opatření:

Jestliže není možné z nějakých důvodů, technických či organizačních, zajistit oddělení provozu videokonference od ostatního provozu sítě, pak je třeba definovat a nastavit řízení kvality přenosu a kapacit dle jednotlivých typů protokolů a přenášených dat. Zabráníte tím jak problémům videokonference, tak hlavně ohrožení ostatního sdíleného datového provozu, který je závislý na latenci anebo propustnosti.

4.4.2 Pro externí připojení na videokonference nepoužívat nezabezpečené veřejné sítě (Wi-Fi hotspots)

Pro realizaci videokonference nepoužívat veřejné anebo nezabezpečené sítě. Tyto přístupové sítě lze využívat pouze v případě realizace videokonference prostřednictvím bezpečně spravovaného koncového zařízení s využitím šifrování na koncovém zařízení či na ustavené VPN do důvěryhodného prostředí interní sítě.

Cíl opatření:

Tím, že se vyvarujete používání nezabezpečených veřejných sítí, snižujete riziko nejen napadení vlastní komunikace v rámci videokonference, ale i koncového zařízení, z kterého je videokonference realizována. Pokud se tomuto vyhnout nedá, pak je nutné komunikovat prostřednictvím VPN prostřednictvím zabezpečeného zařízení.

4.4.3 Zajistit, že videokonferenční systém neumožní nahrávání záznamů bez vědomí všech zúčastněných

Je nutné zabezpečit, aby případné zaznamenávání videokonference bylo vždy v souladu s požadavky na ochranu osobních údajů. Všichni dotčení uživatelé musí být předem o této činnosti informováni, musí být zabezpečen jejich souhlas a musí být o této činnosti informováni po celou dobu záznamu. Mají možnost vyjádřit jednoznačný souhlas či nesouhlas s touto činností.

Cíl opatření:

V souladu s požadavky legislativy v oblasti ochrany osobních údajů, budete schopni prokázat souhlas jednotlivých uživatelů se zpracováním jejich osobních údajů. Snížíte riziko nahodilého zpracovávání a následného zneužití těchto záznamů proti zájmům organizace a jednotlivých uživatelů.

4.4.4 Ověřit, že řešení podporuje oddělený přenos zvuku, obrazu, souborů, textu (Chat).

Musí být umožněno oddělené řízení využití jednotlivých typů komunikace (obraz, zvuk, data).

Cíl opatření:

Oddělené řízení a provoz jednotlivých typů komunikace zajistí, aby v případě problémů byly zajištěny alespoň minimální prostředky pro komunikaci, a umožní vymezit, jaký typ dat je možné během videokonference sdílet.

4.4.5 Data musí být vždy pod kontrolou vlastníka

Ověřte, že data (včetně hlasových a obrazových), jsou po celou dobu přenosu pod výhradní kontrolou organizace, respektive správce dat. Že k datům nemá přístup třetí strana, mimo vlastníka a dodavatele cloudové služby. Data jsou šifrována na koncových zařízeních, či na perimetru a řešení není sdíleno vícero

subjekty, aniž by bylo zajištěno oddělení správy a přenos dat. Ujistěte se, že není možné, aby třetí strana získala přístup k vašim datům anebo řízení provozu videokonference.

Cíl opatření:

Vzhledem k tomu, že cloudová řešení jsou často sdílena s více subjekty, a i přes certifikace a ubezpečení dodavatele, je zde stále riziko neoprávněného zásahu do systému v cloudu třetí stranou. Je třeba mít zajištěnu kontrolu nad přenášenými daty, dle kategorií a typů, po celou dobu přenosu mimo prostředí organizace.

4.4.6 Provést oddělení komunikace videokonferencí od ostatní datové komunikace (pro videokonference, VoIP apod.)

Oddělte komunikační toky videokonference, pokud to lze realizovat, od ostatní datové komunikace prostřednictvím virtuálních oddělených sítí, vyhrazených pro videokonference. Ve specifických případech je třeba oddělit tyto sítě fyzicky. V některých případech je implementováno již přímo v řešení dodavatele.

Cíl opatření:

Jednotlivé typy komunikací mají obvykle různé požadavky na kvalitu a dostupnost. Tím, že oddělíte komunikaci v rámci videokonference od ostatní komunikace, snížíte možnost kompromitace způsobenou chybou v zabezpečení jiného systému než videokonference a zároveň získáte kontrolu nad kvalitou videokonference bez nutnosti řízení jednotlivých toků dat ve společné přenosové síti (QoS, QoE).

4.4.7 Implementovat DoS/DDoS ochranu

Pokud je videokonference realizována přes veřejnou síť internet, pak je nutné na perimetru zajistit ochranu před útoky typu DOS/DDoS.

Cíl opatření:

Útoky typu DoS/DDoS jsou běžnou součástí internetového provozu a směřují k zahlcení služeb organizace a jejich nedostupnost, včetně videokonference. Je proto třeba realizovat sofistikovaná opatření ke zmírnění dopadů takového útoku včetně DDoS útoku na anebo prostřednictvím videokonference.

4.4.8 Zajistit redundanci infrastruktury, load balancing

Komunikační infrastruktura pro videokonference musí být navržena a realizována tak, aby zajišťovala požadovanou odolnost proti výpadku. Z toho důvodu je vyžadována přiměřená redundance síťových zařízení také load balancing.

Cíl opatření:

Tím, že organizace navrhne a realizuje takovou infrastrukturu, která bude odolná proti výpadku, zajistí nejen dostupnost služby videokonference, ale i ochranu kapacit a lidských zdrojů v případě častého odstraňování závad na komunikaci v rámci videokonference.

4.4.9 Provádět testování infrastruktury proti výpadkům

Aby bylo možné zaručit požadavek na dostupnost systémů (nejenom videokonference), je třeba provádět pravidelné testování. V případě využití služeb dodavatele, je třeba se ujistit, že je takto testováno i prostředí dodavatele.

Cíl opatření:

Nebude-li prováděno testování dostupnosti, hrozí, že nebude zajištěna dostatečná odezva a dojde k porušení dostupnosti videokonference anebo ovlivněných systémů.

4.4.10 Provádět a vyhodnocovat penetrační testy a testy DoS/DDoS

Aby bylo možné zajistit funkčnost videokonference, je třeba provádět testování proti známým hrozbám (včetně DoS/DDoS) a monitoring sítě. Je třeba se ujistit, že ochranu proti útokům včetně DoS/DDoS řeší i dodavatel služby, a to i testováním odolnosti.

Cíl opatření:

DoS/DDoS útoky mohou vést k nedostupnosti služby videokonference anebo, pokud budou vedeny prostřednictvím služby videokonference, mohou mít dopad na ostatní služby organizace. Bez tohoto testování a monitoringu mohou být opatření proti DoS/DDoS neúčinná, anebo naopak předimenzovaná, což vede k neefektivnosti těchto opatření.

4.4.11 Požadavky na zabezpečení cloudových služeb se musí odvíjet podle úrovně poskytované služby (SaaS, Paas, IaaS[6])

Bezpečnostní požadavky musí reflektovat úroveň poskytované služby. Je třeba rozlišit hranice služby a tomu přizpůsobit bezpečnostní požadavky na dodavatele a na bezpečnost systému videokonference v kompetenci organizace.

Cíl opatření:

Jde o to, aby se požadavky odvíjely od úrovně a rozsahu poskytované služby. V případě, že by poskytované služby byly širší, než jen zprostředkování videokonference (například pronájem celého tenantu), je třeba vztáhnout interní bezpečnostní požadavky na celé prostředí. A zároveň, pokud je využívána pouze služba, je třeba získat potvrzení, že dodavatel služby má dostatečně řízenou bezpečnost celého cloud řešení. Požadovaná úroveň bezpečnostních požadavků se odvíjí od bezpečnostní úrovně videokonference.

4.4.12 Vyžadovat od dodavatele cloudových služeb minimálně stejnou úroveň zabezpečení jako při realizaci videokonference vlastními prostředky společnosti.

V případě, že dodavatel cloudového řešení či služeb nemá certifikaci ISO/IEC 27001, je nutné smluvně vyžadovat minimálně stejnou úroveň řízení systému řízení bezpečnosti informací (ISMS), jakou má

[6] Petr JIRÁSEK, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. 3., doplněné a upravené vydání. vyd. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

objednatel služby, respektive uživatel videokonference. Toto musí být smluvně vymahatelné a ověřitelné místním šetřením objednatele.

Cíl opatření:

Jestliže dodavatel služby videokonference není schopen doložit soulad s obecně uznávanými standardy, jako je skupina norem ISO/IEC 27000, pak je třeba vyžadovat, aby prokázal, že jeho úroveň řízení bezpečnosti není nižší než požadovaná úroveň v organizaci. Jinak hrozí nesoulad s požadavky legislativy a také ohrožení důvěrnosti videokonference.

4.4.13 Požadovat stejnou úroveň zabezpečení u všech subdodavatelů, jejichž činnost může mít vliv na kvalitu a bezpečnost poskytované videokonference.

Stejnou úroveň zabezpečení jako je vyžadována u dodavatele služby musí dodavatel vyžadovat od všech subdodavatelů, jejichž činnost může mít vliv na kvalitu a bezpečnost poskytované videokonference. Takovou záruku je nutné požadovat po dodavateli videokonference.

Cíl opatření:

Jestliže by některý ze subdodavatelů dodavatele služby videokonference mohl mít vliv na bezpečnost poskytované služby a při tom nebyl v souladu s požadavky organizace na dodavatele, pak hrozí, že k porušení bezpečnosti může dojít v důsledku neošetřené hrozby na straně subdodavatele, avšak důsledky půjdou na vrub organizace.

5 Bezpečnostní monitoring

Bezpečnostní monitoring pro vzdálené videokonference je nutné chápat v moderním slova smyslu – v dnešní době totiž nejde pouze o video a zvuk, ale také o spolupráci nad dokumenty, sdílení obrazovky, a to často na různých zařízeních.

Je tedy nutné monitorovat nejenom služby videokonferencí, ale i další služby a koncová zařízení.

Základní architektury bezpečnostního monitoringu pro videokonference:

- On-premise
- Hybrid
- Plně cloudová

V prostředí organizací státní správy a samosprávy se lze setkat s plně cloudovým prostředním neintegrovaným na interní identitu jen velmi výjimečně, převažují architektury hybridní a on-premise. Jako ideální se opakovaně ukazují hybridní architektury, kdy je část služeb a dat /uživatelů umístěna za perimetrem, část je umístěna a komunikuje v cloudovém prostředí. Velmi důležité je využívání pokročilého monitoringu s možností korelací k dalším událostem.

Pro dohled je určující povaha konference a sdílených dat (citlivost dat a informací) více než architektura řešení.

Procesní požadavky na monitoring:

- Seznam USE-CASE/korelačních pravidel s „knowledge base“
- Evidence kybernetických incidentů
- Klasifikace informací
- Klasifikace incidentů

Předpokládá se, že požadavky na bezpečnostní monitoring lze realizovat ve stávajícím prostředí zákazníka nebo externě.

5.1 Rozdělení monitoringu podle bezpečnostní úrovně

Tabulka č. 4 Rozdělení monitoringu podle bezpečnostní úrovně

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**

5.1.1 SIEM

SIEM (Security Information and Event Management) je specializované řešení pro varování před útoky nebo kybernetickými incidenty, které umožňuje sbírat, korelovat a analyzovat události ze všech možných vrstev IT infrastruktury a mnoha zařízení.

Doporučené zdroje logů pro SIEM:

- Proxy
- Antivirus
- Produkty z kategorie EDR/MDR
- IDS/IPS
- Firewall
- Logy z koncových zařízení (endpoint, server)

SIEM řešení musí splňovat minimální požadavky na následující funkcionality:

- Vyhodnocování událostí/flow a vznik varování v reálném čase podle vytvořených pravidel
- Reporting
- Notifikace

5.1.2 Log management

Log management je doporučen již od nízké bezpečnostní úrovně.

5.1.3 Vulnerability management

Nástroj k vyhodnocování zranitelností v prostředí a sloužící mimo jiné jako vstup pro patch management.

5.1.4 EDR

Pokročilý bezpečnostní nástroj nabízející detekci a reakci na koncových bodech využitím velkého množství dalších funkcionalit (threat hunting, threat intelligence atd.)

5.1.5 IDS/IPS

Detekční (IDS), případně obranný nástroj (IPS), který monitoruje síťový provoz a snaží se v něm odhalit podezřelé aktivity.

5.1.6 DLP

Nástroj k detekci a/nebo ochraně proti záměrnému nebo náhodnému odcizení dat.

5.1.7 Antivirus

Řešení k zastavení běžných hrozeb na koncových bodech s centrální správou.

5.1.8 Firewall

Síťové zařízení k zabezpečení provozu mezi sítěmi s různým účelem a/nebo zabezpečením.

5.1.9 Proxy

Server sloužící jako prostředník v komunikaci klientů vůči cílovým serverům. Může plnit větší množství funkcionalit (cache, filtrace komunikace, …)

5.1.10 Netflow

Účelem sběru je monitorování síťového provozu a poskytnutí detailního pohledu na provoz v reálném čase.

6 Funkční požadavky

Tyto požadavky vymezují rozsah služby a její použitelnost. Cílem je definovat rovnováhu mezi bezpečností a použitelností služby. Základem bezpečnosti služeb je nezpochybnitelné ověření uživatele a řízení jeho přístupových práv. Ověření identity je klíčovým bezpečnostním parametrem u řešení poskytovaných ve veřejných cloudových službách. Požadavky na jeho komplexitu jsou dány požadovanou bezpečnostní úrovní a požadavky na správu a ochranu identit.

Jako základní funkční požadavky definujeme:

- **Interoperabilita** – multiplatformní řešení založené na otevřených průmyslových standardech
- **Autentizovaný i externí přístup** – prokázání identity uživatelů vázáno na pravidla a na technická opatření; řízení přístupu a rolí postavených na identitě uživatele. Možnost řízení přístupu externích uživatelů
- **Komunikační kanály** – základní a volitelné způsoby komunikace (hlas, video, konverzace, sdílení obsahu)
- **Záznamy konferencí** – možnost záznamu a zpětného přehrávání video a hlasové konference
- **Scénáře použití** – základní uživatelské scénáře (1-1 komunikace, týmové konference, vysílání událostí,…)
- **Technické vybavení** – požadavky na technické vybavení uživatelů
- **Ochrana přenášených dat** – architektura systému a ochranných prostředků
- **Ochrana uložených dat** – architektura systému, DLP proti nežádoucímu zveřejnění informací uživatelem
- **Řízení konference** – zajištění bezpečného a bezproblémového průběhu video a audio konferencí a komunikace v konverzačních kanálech
- **Integrace** – propojení digitálních komunikačních kanálů a standardních hlasových služeb
- **Monitoring** – on-line dohled nad průběhem konference
- **Reporting a audit** – historické reporty včetně uživatelské a administrátorské aktivity

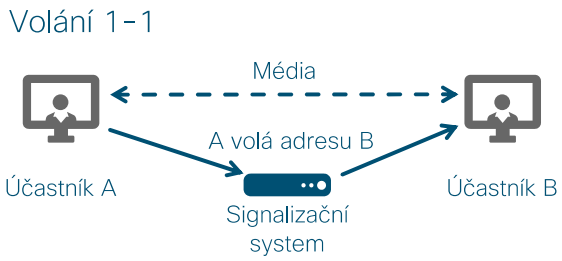
6.1 Scénáře použití

Scénáře použití ukazují typické způsoby navázání videokonference. Důležité je si uvědomit, že uživatelé nemusí mít k dispozici vybavení pro vedení plnohodnotné videokonference. Řešení musí počítat s těmito různými koncovými zařízeními, které se mohou připojit do videokonference:

- Videokonferenční jednotka (osobní nebo konferenční místnost)
- Aplikace na PC nebo mobilním zařízení
- Webový prohlížeč

- Telefonní přístroj připojený k interní telefonní ústředně nebo k veřejné telefonní síti

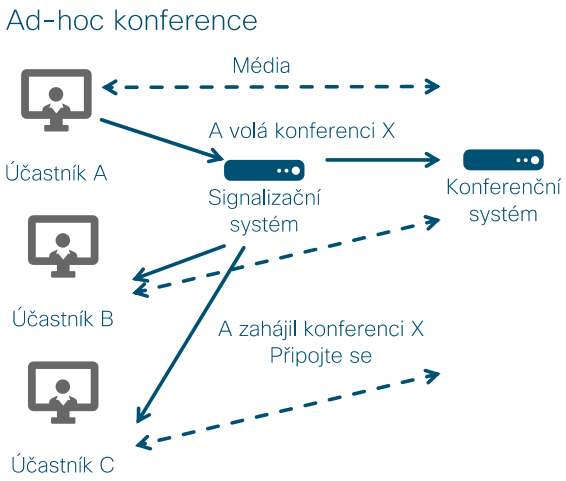
6.1.1 Volání 1-1 – přímé spojení mezi dvěma klienty



Obrázek č. 4 Volání 1-1

Spojení se naváže tak, že volající zadá adresu volaného a hovor se mezi nimi spojí přímo. Adresou je typicky telefonní číslo, SIP nebo H.323 URI. V případě URI je vhodné používat u uživatelů jejich e-mail adresy, u video zařízení srozumitelné pojmenování, které v doménové části identifikuje volanou organizaci, uživatelskou lokalitu a jednací místnost.

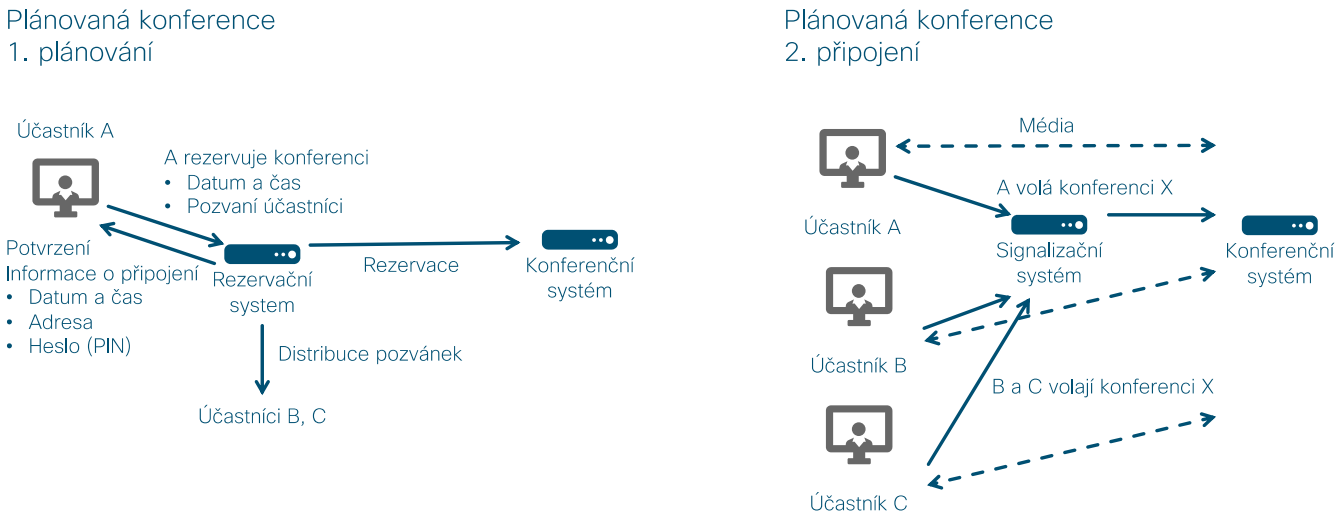
6.1.2 Ad-hoc konference – spojení konference bez předchozí pozvánky



Obrázek č. 5 Ad-hoc konference

Ad-hoc konference obvykle vzniká z dvoucestného hovoru přidáním dalšího uživatele, tj. zadáním jeho adresy na koncovém zařízení nebo v aplikaci. Přidávaný uživatel dostane indikaci příchozího hovoru. Po jeho vyzvednutí se stane členem konference. Ostatní uživatelé vidí, že byl připojen.

6.1.3 Plánovaná konference – vytvoření pozvánky a spojení do konference



Obrázek č. 6 Plánovaná konference

Plánování konference spočívá v přípravě konferenčních zdrojů (rezervace konferenční adresy, kapacity na konferenčním systému) a v rozeslání pozvánek. Pozvánky je nutné posílat bezpečnou cestou, protože obsahují citlivé informace o konferenci (adresu, heslo/PIN, seznam uživatelů). Plánování konferencí je doporučeno realizovat tak, aby bylo pro uživatele komfortní a srozumitelné:

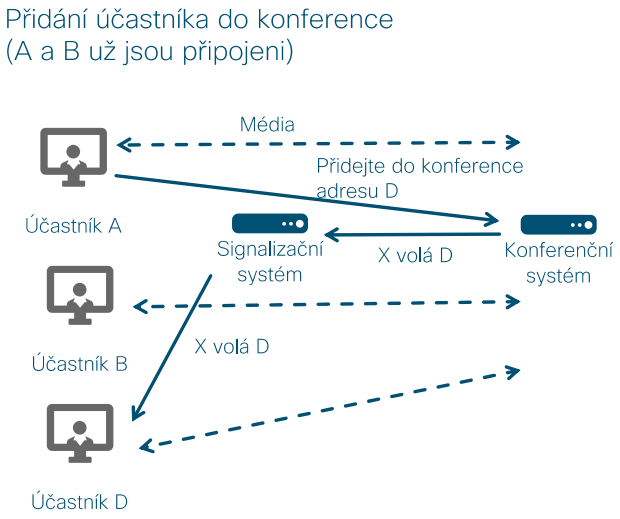
- Pozvánky se automaticky propíšou do kalendáře uživatelů
- Konferenční aplikace vyzve uživatele při zahájení schůzky, aby se připojil
- Videokonferenční zařízení jsou rezervována včetně zasedací místnosti, ve které jsou umístěna (integrace s jejím kalendářem)

Další možné funkce:

- Na videokonferenčním zařízení se zobrazí seznam schůzek a u aktivních dále tyto informace:
    - Tlačítko pro rychlé připojení (není nutné vytáčet ručně adresu konference)
    - Seznam uživatelů, kteří už jsou v konferenci

Spojení do konference proběhne podle typu vybavení uživatelů – zadáním adresy, kliknutím na odkaz, vytočením tel. čísla. Efektivní a bezpečné vedení konferencí vyžaduje odpovídající nástroje v konferenčním systému, viz Řízení konferencí.

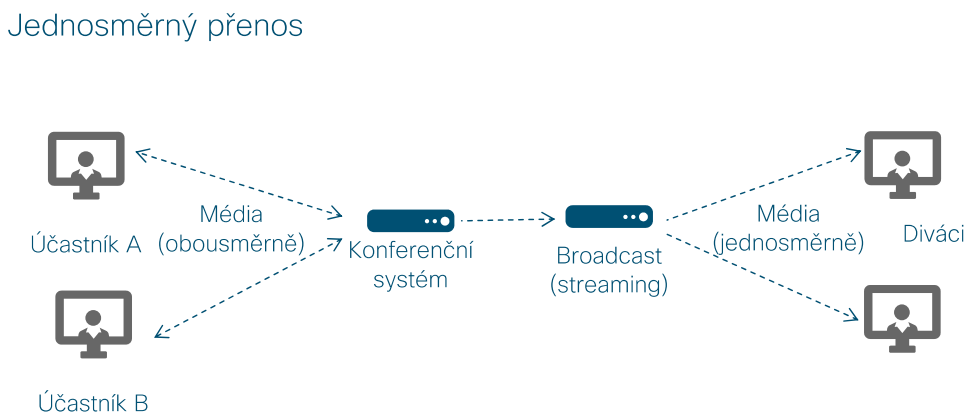
6.1.4 Přidání uživatele do probíhající konference – zřízení spojení na nového uživatele



Obrázek č. 7 Přidání uživatele do probíhající konference

Přizvání uživatele do probíhající konference má stejný průběh jako scénář Ad-hoc konference – spojení konference bez předchozí pozvánky.

6.1.5 Jednosměrný přenos (broadcast)



Obrázek č. 8 Jednosměrný přenos

Ve scénářích, kde je informace předávána jednosměrně většímu počtu uživatelů, jako jsou školení, konference nebo jiné události, je doporučeno využít možností jednosměrného přenosu videa a hlasu formou broadcast technologií. Případná zpětná vazba může být integrována formou textové komunikace. Typické funkce broadcast videokonferenčních systémů jsou následující:

- Produkce vysílaní události
- Streamingová platforma s podporou CDN
- Záznam obsahu přenosu pro pozdější zpětné přehrání
- Podpora příjmu konference v prohlížeči a tlustém klientovi na všech typech koncových zařízení

6.2 Řízení konferencí

Efektivní a bezpečné řízení konferencí zahrnuje tyto funkce:

- Ochrana přístupu do konference
  - Ověřený uživatel
  - Heslo/PIN
  - Čekárna pro uživatele, kdy správce nebo jiní uživatelé konference kontrolují a povolují vstup
  - Omezení přístupu pouze na pozvané uživatele
- Indikátor, zda jde o uživatele organizace nebo se jedná o externího hosta
- Vypnutí mikrofonu (Mute) správcem konference individuálním uživatelům nebo celé audienci
- Odstranění uživatele z konference
- Signalizace v průběhu konference
  - Nový příspěvek v textové konverzaci (chat)
  - Hlášení se o slovo
- Řízení obrazu
  - Automatické přepnutí na mluvčího
  - Hlavní obrazový kanál trvale zaměřen na důležitou osobu (např. přednášejícího)
  - Rozmazání pozadí nastavitelné uživatelem – cílem je ochrana soukromí uživatele

Další možné funkce:

- Přesun uživatele do čekárny (lobby), tj. mimo konferenci
- Automatické nebo manuální uzamčení konference, které znemožní přímý vstup do konference
- Rozložení obrazu nastavitelné uživatelem
  - Největší obraz pro mluvčího, ostatní uživatelé v malých oknech – cílem je zaměření na mluvčího
  - Všichni uživatelé ve stejné velikosti – cílem je viditelnost všech nebo alespoň většiny uživatelů, např. kvůli identifikaci nebo hlasování

6.3 Zařízení uživatele

Zařízením uživatele rozumíme všechna zařízení, která uživatel používá pro připojení do videokonference. Každý uživatel je schopen, a pro splnění zejména termínového úkolu i ochoten, použít jakékoliv zařízení kdekoliv.

Skupiny zařízení, které by uživatel mohl k takové komunikaci využít, by mohly uživateli postačit k rychlé úvaze a přijetí rizika, které by mohlo vlastní nezabezpečené nebo zcela cizí zařízení představovat.

6.4 Lokalita

Pokud uživatel bude chtít komunikovat citlivé informace, měl by znát i definici termínu „Citlivá informace“. I když se nejednalo, nejedná a pravděpodobně nebude jednat o zákonný termín, měl by to být termín s kompromisním výkladem využívaný komunitně na základě.

Uživatel může své zařízení používat v jakékoliv lokalitě. Je proto nutné, aby si uživatel uvědomil rizika spojená s možných odposlechem nebo odezíráním nepovolanou třetí stranou.

Lokality by také mohly být rozdělené do několika skupin, aby uživatel rámcově tušil, která lokalita je pro sdělované citlivé informace v takové komunikaci méně nebo více vhodná.

6.5 Uživatelé

Uživatele videokonferenčních systémů můžeme rozdělit do třech skupin. Zaměstnanci organizace vlastnící VTC systém (on-premise nebo cloud), externí uživatelé z organizací s federovanou identitou a tzv. hosté. Hosté jsou externí jednotlivci, kteří získávají přístup ke spolupráci ve videokonferenčním prostředí kmenové organizace. V závislosti na konkrétní implementaci videokonferenčního systému a licenčních podmínkách, mohou mít hosté přístup pouze k omezené sadě funkcí videokonference.

6.6 Hlas

Komunikace při konferenčních hovorech musí podporovat hlasové služby postavené na standardech Voice over IP (VoIP) včetně podpory komunikace mezi koncovými klientskými zařízeními. Dále je nutné umožnit připojení klientů z prostředí telekomunikačních sítí – pevných linek a mobilní sítě – propojením videokonferenčního řešení na PSTN síť.

Doporučené funkce pro službu hlasové komunikace:

- Hlasové služby (VoIP)
- Propojení hlasových služeb do veřejné telefonní sítě (PSTN)

Možné další služby:

- Integrace a náhrada PBX
- Možnost ovládání zvukových periferií v probíhajícím hovoru
- Možnost připojení telefonních přístrojů a dalších audio periferií

6.7 Video

Video konverzace mohou probíhat ve dvou formátech. V prvním se video sdíleno mezi uživatele (1:1 nebo skupinová konverzace), v druhém je pak video přenášeno pouze od přenášejících k posluchačům. Jednosměrná videokonference je určena pro větší události s vysokým počtem uživatelů a bez nutnosti tyto uživatele aktivně zapojovat do vysílání video konverzací.

Doporučené funkce pro službu video komunikace:

- Obousměrné video ve schůzkách
- Jednostranné video u vysílaných událostí (streaming video k posluchačům)
- Zobrazení několik video streamů souběžně
- Možnost ovládání video periferií v probíhajícím videohovoru
- Možnosti respektu soukromí uživatele
    - Rozmazaní pozadí
    - Nahrazení pozadí obrázkem

6.8 Textová komunikace (Chat)

Textová komunikace může být typu tzv. instantní, kdy se stejně jako u videokonferencí komunikuje přímo mezi uživatele, kteří jsou v danou chvíli přítomni nebo typu store&forward, kdy se zprávy ukládají v konverzační skupině anebo dvoucestném konverzačním vlákně, a kde jsou dostupné účastkům po jejich připojení. Textová konverzace musí být dostupná pouze uživatelům konverzace případě členům skupinové konverzace. Oprávněná osoba však může další uživatele do konverzace připojit a zpřístupnit komunikační kanál a případnou historii v daném kanále.

Doporučené funkce pro službu textové komunikace:

- Textová komunikace během online meetingu/callu
- Dvoucestná textová komunikace
- Skupinová textová komunikace
- Perzistentní textová komunikace (zachování historie chatu)
- Možnost pozměnění textu po odeslání
- Datum a čas odeslané zprávy v textu
- Indikace přečtení zprávy druhou stranou
- Archivace/Retence a eDiscovery textových zpráv
- Ochrana obsahu zpráv před unikem citlivých informací – DLP (Data Loss Prevention)
- Moderované Q&A v rámci schůzky nebo přímého přenosu

V případě, že videokonferenční systém těmito funkcemi nedisponuje, doporučujeme chat zcela zakázat a pro videokonferenční hovory nepoužívat.

Další možné funkce:

- Možnosti Rich textu/HTML formátů obsahu zpráv
- Vkládání dalších elementů do zpráv (obrázky, emoji, Giphy atd.)

6.9 Sdílení informací

Během konferenčního hovoru lze uživatelům sdílet od prezentujících následující typy informací

- Prezentace
- Soubory (dokumenty)
- Obrazovka prezentujících
- Zápisy spojené s probíhajícím meetingem nebo opakujícími se meetingy
- Whiteboard – tabule pro volné kreslení/psaní poznámek

Pokud je povoleno, uživatelé mají možnosti převzít kontrolu nad sdílenou prezentací, případně sdílet obrazovku ze svých koncových zařízení.

Dokumenty uložené na sdílených úložištích je povoleno autorizovaným uživatelům konference souběžně editovat a spolupracovat v reálném čase na jejich obsahu.

6.10 Ukládání dat a informací

Veškerá data a informace, které vznikají během konferenčních hovorů a konverzací musí být transparentně ukládána a jsou plně ve vlastnictví organizace. Organizace musí být schopna řídit a omezit ukládání dat z videokonference ve zvolených geografických regionech, primárně Evropské unii (EU) a Evropském hospodářském prostoru (EHS).

Ukládaná data a informace jsou členěny do následujících kategorií:

- Záznamy konferenčních hovorů
- Hlasový záznamník (Voicemail)
- Pozvánky v kalendářích
- Kontakty
- Soubory
- Chat/Zprávy
- Obrázky
- Telemetrie/logy

Přístup k uloženým datům musí být řízen na základě oprávnění (role based security) vázaných na ověřenou identitu uživatele.

6.11 Nahrávání konferencí

Nahrávání telekonferencí obsahuje záznam audio a video obsahu a dále pak sdílených obrazovek během konferenčního hovoru. Záznamy jsou uloženy do centrálního úložiště, odkud mohou být bezpečně řízeným způsobem sdíleny.

Možnost zapnutí záznamu musí být konfigurovaná a jeho pořízení mohou realizovat pouze autorizovaní uživatelé. Informace o zapnutém záznamu musí být dostupná všem uživatelům. Pokud existuje organizační politika pro pořizování záznamů, uživatelé musí dát explicitní souhlas s dodržením specifikované politiky před započetím záznamu.

6.12 Ukládání dat/informací

Podobně jako u textové komunikace lze soubory jen přenést nebo je vystavit k vyzvednutí.

Řízení přístupu k datům.

6.13 Videokonferenční zařízení

H.323/SIP videokonference se skládají z různých kombinací zařízení pro přenos obrazu, zvuku a dat a komunikují spolu buď na přímo 1:1, nebo v režimu vícebodového připojení pomocí jednotky MCU

Cloudové videokonferenční systémy jsou napojeny na cloudové služby, které zajišťují veškerá spojení mezi videokonferenčními systémy.

Videokonferenční systém je složen z:

- **Osobních zařízení** – náhlavní soupravy, stolní telefon, osobní hlasitý telefon, mobilní telefon, tablet a další.
- **Sdílených zařízení** – kamera, displej, videokonferenční PC (kodek), hlasitý telefon, interaktivní tabule a další.

Tyto jednotlivé prvky se připojují kabelem/bezdrátově do portů videokonferenčního PC, který je napojen do počítačové sítě. Tyto PC jsou dnes jednoúčelové se zaměřením k přenosu obrazu a zvuku a jsou takto také certifikované z hlediska bezpečnosti. Pokud u nových typů videokonferencí je hlasitý telefon připojen přímo k síti platí pro něj stejná bezpečnostní pravidla jako pro videokonferenční PC, nebo telefony. Zasedací místnosti se dnes budují spíše malé, nebo střední a ostatní uživatelé jsou napojeni z osobních zařízení z míst, kde se nacházejí.

- **MCU** – zařízení pro vícebodová videokonferenční spojení. Jedná se o zařízení, které je buď realizováno dedikovaným hardwarem, nebo softwarem na virtuální platformě. V současné době cloudových videokonferencí může MCU sloužit jako GW do cloudové služby a vytvářet tzv. hybridní spojení prostředí onPrem a cloudu.
- Videokonference typu **„All in One“** mají periferie integrované spolu s displejem a umožňují nejenom přenos obrazu a zvuku, ale také standardní práci s integrovaným počítačem. Systémy jsou propojeny s počítačovou sítí a umožňují komunikaci se s mobilními zařízeními standardními protokoly.
- Videokonference typu **„Bar“**, kde jsou audio periferie s kamerou a případně s počítačem integrovány do bloku, který se propojí s displejem kabelem. Tyto systémy opět umožňují určitou formu komunikace s mobilními prostředky a jsou napojeny do počítačové sítě.

S posilováním telekomunikačních linek se stále více prosazuje komunikace z místa, kde se uživatel právě nachází a komunikačním prostředkem, který má k dispozici, např. z mobilu, tabletu a tabletu. HD kvalita

obrazu je odvislá od kvality spojení. Pokud bude kvalita spojení dobrá, na mobilech a tabletech budou dány aplikace pro tato zařízení a ve videokonferenčních místnostech pro více uživatelů bude Full HD (případně nový standard 4K – 3840x2160 pixelů), pak bude kvalita zobrazení vysoká. Pokud kvalita spojení bude špatná, Full HD bude degradovat na nižší kvality zobrazení, aby byl obraz i nadále sledovatelný.

6.14 Řízení kvality služeb

Kvalita služby (QoS) má vliv především na efektivitu videokonference. Výpadky zpomalují komunikaci nebo mohou vést k nedorozuměním. Z bezpečnostního hlediska je kvalita služby důležitý nástroj pro zajištění spolehlivosti a dostupnosti. Ochranu proti některým typům útoků lze provést právě pomocí nastavení QoS, kdy je potenciálně nebezpečný provoz klasifikován do QoS třídy s nízkou prioritou (scavenger) a neovlivní tak samotnou konferenci.

Zajištění QoS je vhodné realizovat podle doporučení pro DiffServ (differentiated services), RFC4594[7] a navazujících. Nastavení DiffServ je důležité i z pohledu interoperability (kapitola 8).

Způsob konfigurace a monitorování QoS v síťovém prostředí organizací nebo jejich připojení na cloudové služby je nad rámec tohoto dokumentu.

[7] Dostupné zde: https://tools.ietf.org/html/rfc4594

7 Integrace

Cílem integrací je usnadnit uživatelům práci s videokonferencemi a sdílet bezpečnostní funkce stávajících systémů.

7.1 Plánování

Videokonferenční řešení má obvykle svůj rezervační systém, jehož cílem je plánování kapacity a usnadnění připojení do konference (např. tlačítko rychlé volby, URI adresa nebo http odkaz). Pro uživatele je podstatné propojení s jejich kalendářem. Integrační služby zajistí:

- Rozeslání pozvánek e-mailem se všemi potřebnými údaji pro připojení ke konferenci
- Rezervaci zdrojů (zasedacích místností), ve kterých jsou umístěny HW videokonference.
- Usnadnění přístupu z HW videokonference:
    - Ovládací prvky videokonference zobrazí seznam naplánovaných schůzek (pokud zařízení umožňuje). Z bezpečnostních důvodů lze skrýt detaily navazujících schůzek.
    - Ovládací prvky videokonference umožní rychlé připojení do schůzky

7.2 Úložiště

Jak bylo uvedeno v kapitole 6.10, v souvislosti s videokonferencemi vzniká množství dat, která je třeba uložit. Organizace mohou mít vlastní zabezpečené úložné systémy, je tedy vhodné řešení postavit tak, aby byla využita existující úložiště a nebudovala se zbytečně nová. Zde opět hovoříme o využití jak on-premise tak cloudových úložišť. Je důležité upozornit, že zejména u archivace nahrávek je třeba plánovat navýšení kapacity úložných systémů. Lze očekávat ukládání těchto typů dat:

- Uživatelský typ dat:
    - Nahrávky konferencí
    - Sdílené soubory
- Auditní typ dat:
    - Metadata o konferencích
    - Textová komunikace

U uživatelských dat je podstatná ochrana přístupu a logování aktivity. Auditním datům je věnována kapitola 5.1.1 SIEM.

7.3 Externí aplikace

Konferenční aplikace nabízejí následující typy rozšíření:

- Plug-in do existujících aplikací (např. MS Outlook, webový prohlížeč)
- Plug-in nebo add-on do konferenční aplikace

V prvním případě je třeba zajistit, aby plug-in vyhověl stávající aplikační politice, tj. zda nepředstavuje bezpečnostní riziko a zda se bez něj lze obejít a konferenční systém i tak nabídne plnou funkčnost.

Druhý případ znamená, že management nástroje konferenčního systému musí umožnit nastavení politik, které omezí nebo zcela zakážou instalaci add-ons uživatelem. A dále, že administrátor bude mít k dispozici nástroje, kterými uživateli nastaví jednotné prostředí včetně add-ons.

V obou případech je pak nutné, aby měl administrátor k dispozici nástroje pro vzdálenou aktualizaci plug-inů.

7.4 API

Aplikační rozhraní nabízejí možnosti integrace nad rámec hotových aplikací nebo plug-inů. Lze tak např. postavit plánovací systém s rozšířenými funkcemi nebo navázat konferenční systém na existující pracovní postupy. API ale nabízí uživatelské i administrátorské funkce a je tedy třeba věnovat pozornost jeho zabezpečení. Podstatnými bezpečnostními parametry API jsou:

- Použití zabezpečených protokolů s odpovídající úrovní kryptografie
- Konfigurovatelná bezpečnost politikami videokonferenčních systémů
- Moderní metody autentizace a autorizace, které umožní:
    - Stanovit rozsah dostupných služeb pro konkrétní aplikaci
    - Neukládat v aplikaci uživatelská jména a hesla pro přístup k API
    - Při úniku autentizačních informaci zablokovat aplikaci přístup
- Logování API komunikace

8 Interoperabilita

Videokonference jsou otevřeným komunikačním systémem. Doporučujeme v co nejvyšší míře využívat stávající vybavení splňující současné standardy. Pro jeho efektivní použití je nutné definovat parametry, které zaručí interoperabilitu a zpětnou kompatibilitu. Videokonferenční zařízení mohou představovat významnou investici, u které musí být garantována dlouhodobá udržitelnost. Doporučujeme, aby konferenční systém nabízel kompatibilitu s vybavením, které bude provozováno po dobu 5 let.

Interoperabilita bývá k dispozici buď přímo v koncových zařízeních a aplikacích nebo v komunikačních platformách (na straně aplikačních severů nebo cloudové služby). K proprietárním systémům pak často existují řešení (gateway) třetích stran, která mohou zajistit potřebnou interoperabilitu a propojit systémy více dodavatelů, které nejsou přímo propojitelné.

Interoperabilita se řeší jak na úrovni signalizačních a přenosových protokolů (interworking), tak i v kódování hlasu, videa a sdílení obrazovky (transcoding).

8.1 Standardní protokoly

Tak jako se překotně vyvíjí všechny videokonferenční platformy, prudký rozvoj je i v oblasti používaných protokolů. Při výběru videokonferenční platformy je nutné průběžně sledovat aktuální standardy a volit takovou platformu, která je postavena nejen na standardech zpětně kompatibilních, ale balancovat tento požadavek se standardy nadcházejícími. U kryptografie se například řídit doporučenými algoritmy publikovanými na stránkách NÚKIB. Následující kapitoly uvádějí přehled standardů poplatných době vzniku dokumentu.

Z otevřených protokolů doporučujeme vyžadovat kompatibilitu se SIP (Session Initiation Protocol, RFC 3261 a navazující) protokolem. Jedná se o všeobecně respektovaný standard, u kterého je od počátku jeho vzniku kladen důraz na vzájemné testování interoperability jeho implementací (SIP bakeoffs). V proprietárních řešeních je SIP používán jako protokol, který zajistí interoperabilitu s jinými systémy.

V rámci realizace videokonferenčního řešení doporučujeme provést praktické testy interoperability, které prokážou kompatibilitu s existujícími systémy.

8.1.1 Hlasové kodeky

Kódování hlasu prochází trvalým vývojem. U koncových zařízení je důležitá podpora nejen nejnovějších algoritmů, které zajistí kvalitní poslech a odolnost proti výpadkům, ale i dlouhodobě osvědčených kodeků, jako je např. G.711. Zařízení musí být schopna se domluvit na optimálním kódování hlasu.

U všech zařízení doporučujeme, aby podporovaly minimálně kodeky G.711 a G.722.

8.1.2 Video kodeky

I kódování obrazu prochází vývojem. Důraz je kladen nejen na odolnost proti ztrátám, ale i na efektivitu přenosu, aby bylo možné spojit video hovor přes mobilní data nebo běžnou přípojku do internetu.

U všech výrobků doporučujeme, aby zařízení podporovala základní kodeky H.263 a H.264.

8.1.3 Signalizace

Vedle protokolu SIP se stále ještě používá protokol H.323, zejména v HW videokonferencích. Pro interoperabilitu s H.323 je tedy vhodném mít k dispozici modul, který umožní propojit SIP a H.323 tak, aby jedna strana mohla k připojení do konference použít SIP a druhá H.323.

WebRTC/RTCWeb – implementace audio/video přenosu přímo ve webovém prohlížeči. Aktuálně k dispozici ve všech moderních prohlížečích jak v počítači, tak v mobilních zařízeních.

8.1.4 Transport

RTP/SRTP + RTCP/SRTCP – Realtime protocol nad UDP, otevřená a šifrovaná varianta

8.1.5 Značkování QoS (DiffServ)

V případě, že se bude v síťovém prostředí využívat prioritizace provozu podle DiffServ (kapitola 6.14), je nutné do interoperability zahrnout i jednotné značení provozu tak, aby všechny systémy v konferenci používaly stejné třídy a nebylo nutné měnit nastavení sítě.

Doporučení na shodu s kapitolou 4.3.6.

9 Zkratky a pojmosloví

Zkratka/pojem	Význam
ČR	Česká republika
DLP	**Data Loss Prevention** – vynucuje nápravu pomocí výstrah, šifrování a dalších ochranných opatření, aby koncovým uživatelům zabránila v náhodném nebo zlomyslném sdílení dat, která by mohla ohrozit organizaci.
DNS	Domain Name System (Systém doménových jmen)
Dodavatel	Dodavatelem je zároveň i poskytovatel cloudových služeb
DoS, DDoS	Denial of service, Distributed denial of service – jde o typ útoku na informační systém, kdy jsou systém či služba zahlceny velkým množstvím požadavků, často s chybnými anebo podvrženými parametry. A to buď z jednoho místa (DOS), anebo s využitím mnoha kompromitovaných zdrojů (DDoS).
E2E encryption	šifrování obsahu pomocí klíčů, které si vygenerují sami uživatelé komunikace a vymění si je mezi sebou bezpečnou cestou. Komunikace je tak zabezpečena po celé přenosové trase. Příkladem jsou protokoly Signal nebo MLS (IETF)
EDR	Endpoint detection and response
EU	Evropská unie
GDPR	(General Data Protection Regulation) Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
H.323	skupina ITU-T protokolů pro navázání komunikace typu hlas, video, sdílení obsahu. Předchůdce SIP.
Hardening	Pod pojmem hardening se rozumí proces zabezpečení zařízení či systému, prostřednictvím definované konfigurace (politik) tak, aby byla minimalizována možná rizika v důsledku existujících zranitelnosti.
IdM	Identity management
IDS/IPS	Intrusion Detection System/Intrusion Prevention System – systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity. IPS dokáže na základě těchto aktivit reagovat a komunikaci například zablokovat či odklonit.
IP adresa	Číslo (označení) které jednoznačně identifikuje síťové rozhraní v počítačové síti
IT	Informační technologie
NAKIT	Národní agentura pro komunikační a informační technologie
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
QoE	Quality of Experience – způsob hodnocení kvality poskytovaných služeb na základě spokojenosti zákazníků.
QoS	Quality of Service. Jedná se o technologický parametr, který umožňuje řídit různou šíři pásma k využívání pro komunikaci zařízení a aplikací v rámci sítě a přidělovat jim rozdílnou důležitost.

RTCP/SRTCP	protokol pro zpětnou vazbu o přenose, stejně jako RTP/SRTP používá UDP, koncová zařízení vysílají RTCP zpět ke zdroji přenosu.
RTP	**Real Time Protocol** – specifikuje zapouzdření přenosu v reálném čase (hlas, video, doplňující informace) pomocí UDP
SIEM	Security Information and Event Management (Management bezpečnostních informací a událostí)
SIP	**Session Initiation Protocol** – rodina otevřených standardů IETF pro navázání komunikace typu hlas, video, sdílení obsahu, textové zprávy
SIP URI	adresa koncového zařízení v SIP prostředí. Princip je stejný jako u e-mailu – pravá strana za @ určuje doménu, levá strana konkrétní lokální adresu (uživatele).
SRTP	šifrovaný RTP přenos
VMR	Virtual Meeting Room – Virtuální jednací místnost
VPN	Virtual Private Network (Virtuální privátní síť)

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
17.07.2020	1.0	NÚKIB, NAKIT, BIS, VZ, UZSI, AČR, AFCEA Microsoft, Cisco, Gesto Communications, ATS – Telcom Praha	Vytvoření dokumentu