ANALÝZA VYBRANÝCH VIDEOKONFERENČNÝCH RIEŠENÍ

Autor: Analytické oddelenie

Vypracoval: Vládna jednotka CSIRT, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Vypracované dňa: 7.9.2020

Verzia: 1.0

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Obsah

Úvod

Hlavnou motiváciou pre túto analýzu je rastúci dopyt po softvérových riešeniach a službách umožňujúcich spoluprácu resp. audiovizuálnu komunikáciu dvoch a viacerých strán s prihliadnutím na zaistenie bezpečnosti, súkromia a použiteľnosť vybraného riešenia.

V analýze zvažujeme dva scenáre, pri ktorých môže vhodné videokonferečné riešenie pomôcť v spolupráci a komunikácii užívateľov na diaľku. V prvom scenári počítame so zamestnancami (účastníkmi) pracujúcimi formou teleworkingu (homeoffice) s obmedzeným prístupom k zamestnávateľom poskytnutej výpočtovej technike (PC, notebook, smartfón) a potrebou spolupracovať a komunikovať prostredníctvom komerčných alebo bezplatných služieb alebo softvérových riešení.
V druhom scenári sa snažíme nájsť vhodné riešenie v podobe softvéru alebo služby, ktorá by mohla pomôcť s výučbou na diaľku.

Upozornenie

Je vhodné upozorniť, že odporúčania a hodnotenia v tomto dokumente nemôžu byť vnímané ako definitívne, nakoľko softvér a služby tretích strán sa neustále vyvíjajú a menia. Týmto môže dôjsť k vzniku nových bezpečnostných zraniteľností týchto systémov, ako aj k zmene s nimi súvisiacich bezpečnostných rizík.

Analýza sa nezaoberá procesnou bezpečnosťou ani bezpečnosťou koncových zariadení užívateľov na ktorých má riešenie alebo služba prebiehať. Považujeme však za nutné spomenúť, že akokoľvek bezpečné videokonferenčné riešenie môže byť ľahko kompromitované, pokiaľ je kompromitovaná bezpečnosť koncového zariadenia užívateľa.

Metodika

Pri tvorbe predkladanej analýzy boli použité informácie z verejne dostupných - otvorených zdrojov s dobrou reputáciou a taktiež od odborníkov alebo autorít z oblasti informačnej a kybernetickej bezpečnosti. Počas analýzy sme netestovali jednotlivé softvérové riešenia a služby prakticky, t. j. neboli nasadzované a testované v našej infraštruktúre.

Hodnotiace kritériá

Hostiteľské prostredie

On-premise (hostovaný vo vlastnej infraštruktúre)

Tento spôsob inštalácie alebo hostovania softvéru znamená, že softvér beží lokálne v infraštruktúre organizácie alebo u konkrétnej osoby a nie vzdialene na výpočtových zariadeniach cloudového poskytovateľa alebo serverovej farmy.

Cloudový poskytovateľ

Cloudové hostovanie je spôsob, kedy organizácia alebo jednotlivec presúva výpočtové alebo úložné kapacity k poskytovateľovi služby, ktorý ponúka svoju infraštruktúru alebo výpočtové kapacity v rámci niektorého z úžitkových modelov (IaaS, PaaS, SaaS).
Pre porovnanie úžitkových modelov v cloudovom prostredí a on-premise uvádzame nasledovnú tabuľku. Tabuľka zobrazuje rozdielne kompetencie

On-premise	IaaS	PaaS	Saas
Aplikácie	Aplikácie	Aplikácie	Aplikácie
Dáta	Dáta	Dáta	Dáta
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualizácia	Virtualizácia	Virtualizácia	Virtualizácia
Servery	Servery	Servery	Servery
Úložiska	Úložiska	Úložiska	Úložiska
Siete	Siete	Siete	Siete

Vlastná réžia V správe poskytovateľa cloudovej služby

Dostupnosť bezplatnej verzie

Dostupnosť bezplatnej verzie softvéru alebo služby je ďalším z posudzovaných kritérií, nakoľko náklady spojené s obstaraním alebo prevádzkou môžu pre niektorých užívateľov predstavovať vstupnú bariéru.

Použiteľnosť podľa počtu účastníkov

Počet účastníkov, ktorí môžu súčasne používať videokonferenčný softvér, je ďalšie dôležité kritérium. Niektoré posudzované riešenia ponúkajú v tomto smere obmedzené možnosti (videohovory v móde *účastník – účastník*). Iné naopak širšie možnosti (*účastník – publikum*) o veľkosti viac ako 200 účastníkov.

Kryptografia

End-to-end šifrovanie (E2EE)

End-to-end šifrovanie (E2EE) znamená, že dáta šifrované odosielateľom na jeho zariadení môže dešifrovať jedine prijímateľ na svojom koncovom zariadení. V kombinácii s dostatočne silnou kryptografiou má takýto spôsob šifrovania zaistiť, že ak by došlo počas prenosu dát k ich zachyteniu útočníkom alebo prevádzkovateľom služby, nebude ich vedieť dešifrovať, a teda dostať sa k pôvodnej informácii.

Kvalita použitých kryptografických štandardov

Kvalita použitých kryptografických štandardov do veľkej miery rozhoduje o dôvernosti a integrite prenášaných dát. Z tohto dôvodu je odporúčané používať aktuálne, otvorené protokoly a algoritmy odporúčané bezpečnostnými autoritami ako NIST, IETF alebo ETSI.
Je vhodné vyhýbať sa neauditovaným proprietárnym kryptografickým primitívam a protokolom vytvoreným poskytovateľom nejakej služby alebo softvérového riešenia.

Dvojfaktorová autentifikácia (2FA)

Dvojfaktorová autentifikácia (2FA) slúži ako dodatočné overenie identity najčastejšie prostredníctvom princípu “niečo-čo-mám” vo forme SMS kódu, TOTP tokenu alebo hardvérového tokenu.
2FA predstavuje dodatočnú vrstvu zabezpečenia pri prihlásení v prípade, že útočník získa užívateľské heslo.

Dostupnosť zdrojového kódu

Otvorený zdrojový kód (open-source) poskytuje možnosť ľahšej auditovateľnosti kódu aplikácie, teda možnosť overiť si napr. deklarované kryptografické algoritmy a správnosť ich implementácie.
Je vhodné spomenúť, že samotná dostupnosť zdrojových kódov nezaručuje automaticky vyššiu bezpečnosť softvéru.

Súkromie

Zdieľanie užívateľských dát s tretími stranami

Platformy pre spoluprácu zo svojej podstaty častokrát musia zbierať základné informácie, aby mohli fungovať. Napriek tomu je žiadané, aby chránili citlivé údaje ako napríklad obsah hovorov alebo detaily jednotlivých kontaktov. Informácie zachytávajúce konverzácie by nemali byť zdieľané s tretími stranami. Toto sa vzťahuje aj na metadáta spájané s užívateľskými identitami, informáciami o zariadeniach, kolaboračných sedeniach a ďalšie informácie, ktoré by mohli vystaviť organizáciu bezpečnostnému riziku, resp. ohroziť súkromie jednotlivca.
Zdieľanie informácií s tretími stranami by malo byť jasne definované v pravidlách ochrany súkromia a osobných údajov.

Možnosť bezpečného odstránenia užívateľských dát

Je v záujme a taktiež právo používateľov mať možnosť zmazať nimi vytvorené dáta (správy, súbory) a taktiež trvalo vymazať ich účty u poskytovateľa služby, ktoré už neplánujú ďalej používať.

Ostatné

Do tejto kategórie sme zaradili nasledovné kritériá, ktoré nehodnotíme priamo, ale považujeme za potrebné ich spomenúť.

Zraniteľnosti a manažment zraniteľností

Každý softvér vytváraný človekom obsahuje chyby, a teda aj bezpečnostné chyby, ktoré predstavujú zraniteľnosti.

Rozhodli sme sa neposudzovať toto kritérium priamo, nakoľko ani názory odborníkov sa nezhodujú, či momentálne je alebo bude v budúcnosti určitá aplikácia bezpečná, ak obsahovala v minulosti zraniteľnosti.

Napovedať môžu v tomto smere skôr informácie o tom, ako autor alebo spoločnosť stojaca za vývojom softvéru alebo prevádzkou služby reaguje na prípadné objavené zraniteľnosti, ako je ochotná a ako rýchlo je schopná ich opraviť a tiež, či je ochotná podvoliť svoj produkt nestrannému auditu tretej strany. Prikláňame sa k všeobecnému názoru, že poskytovateľ služby alebo softvéru, ktorý dbá a zaujíma sa o bezpečnosť svojich produktov, bude reagovať na prípadné odhalené zraniteľnosti alebo úniky dát promptne a transparentne.

Platformy

Považujeme za potrebné upozorniť, že pri výbere videokonferenčného riešenia je vhodné zohľadniť aj platformy (operačný systém alebo aplikačné prostredie) účastníkov, na ktorých má softvér alebo služba fungovať. Z verejne dostupných informácií predpokladáme, že väčšinový podiel na operačných systémoch bude mať Microsoft Windows a na mobilných zariadeniach Android a iOS. Okrajovo zastúpené budú operačné systémy MacOS a GNU/Linux.

Rôznorodosť platforiem je možné preklenúť softvérovým riešením alebo službou, ktorá bude fungovať z prostredia webového prehliadača, nakoľko tento komponent je prítomný na všetkých spomenutých platformách.

Tabuľka s hodnotiacimi kritériami

Služba	Hostiteľské prostredie	Dostupnosť bezplatnej verzie	Použiteľnosť podľa počtu účastníkov	End-to-end šifrovanie	Auditovateľná kryptografia	Dvojfaktorová autentifikácia (2FA)	Dostupnosť zdrojového kódu
Mattermost	cloud/on-prem	ÁNO	-	NIE	ÁNO	ÁNO [2]	ÁNO
Jitsi Meet	on-prem	ÁNO	75 [5]	ÁNO [4]	ÁNO	NIE	ÁNO
Signal	Cloud	ÁNO	2	ÁNO	ÁNO	ÁNO	ÁNO
Wickr	cloud/on-prem	ÁNO	30 [5], 50 [6]	ÁNO	ÁNO	ÁNO	ÁNO
Zoom	on-prem [4]	ÁNO	100 [5]	ÁNO [1, 4]	ÁNO	ÁNO [1]	NIE
Slack	Cloud	ÁNO	15 [5]	NIE	ÁNO	ÁNO	NIE
Cisco Webex	on-prem	ÁNO	100 [5]	ÁNO [1]	ÁNO	ÁNO [1,2]	NIE
GoToMeeting	Cloud	ÁNO	4 [5], 250 [6]	ÁNO [1]	ÁNO	NIE	NIE
Amazon Chime	Cloud	ÁNO	250 [6]	NIE	ÁNO	ÁNO	NIE
Microsoft Teams	Cloud	ÁNO	250 [6]	ÁNO [4]	ÁNO	ÁNO	NIE
Skype for Business	on-prem/cloud	ÁNO	50	ÁNO [4]	ÁNO	ÁNO	NIE
Google G Suite [7]	Cloud	ÁNO	25 [5], 250 [6]	NIE	ÁNO	ÁNO [1]	NIE
Pexip	on-prem/cloud	NIE	Limit záleží od HW vybavenia	NIE	ÁNO	NIE	NIE

---

[1] Nastaviteľné, [2] Neplatí pre bezplatnú verziu, [3] Detaily neboli zverejnené, [4] Čiastočne, [5] Bezplatná verzia, [6] Platená verzia, [7] Zahŕňa v sebe viacero produktov Google Meet, Google Hangouts

Služba	Zdieľanie užívateľských dát s tretími stranami	Odstránenie užívateľských dát	Riadenie prístupu do videokonferencie	Potreba registrácie účtu pre pripojenie do meetingu
Mattermost	NIE	Klient ÁNO Server NIE	ÁNO [4]	ANO
Jitsi Meet	NIE	Klient NIE [3] Server NIE [3]	ÁNO	NIE
Signal	ÁNO	Klient ÁNO Server ÁNO	ÁNO	ANO
Wickr	ÁNO	Klient ÁNO Server ÁNO	ÁNO	ANO
Zoom	ÁNO	Klient ÁNO Server NIE [3]	ÁNO	NIE
Slack	ÁNO [1]	Klient ÁNO [1] Server ÁNO [1]	ÁNO	ANO
Cisco Webex	ÁNO	Klient ÁNO Server NIE [3]	ÁNO [1]	NIE
GoToMeeting	ÁNO	Klient ÁNO Server NIE [3]	ÁNO [1]	NIE
Amazon Chime	NIE	Klient ÁNO Server ÁNO	ÁNO	NIE
Microsoft Teams	ÁNO	Klient ÁNO [1] Server ÁNO [1]	ÁNO	NIE
Skype for Business	ÁNO	Klient ÁNO [1] Server ÁNO [1]	ÁNO	NIE
Google G Suite	ÁNO	Klient ÁNO Server ÁNO [2]	ÁNO [1,4]	ANO [5], NIE [6]
Pexip	NIE	Klient ÁNO Server ÁNO	ÁNO	NIE

---

[1] Nastaviteľné, [2] Neplatí pre bezplatnú verziu, [3] Detaily neboli zverejnené, [4] Čiastočne, [5] Bezplatná verzia, [6] Platená verzia

Vyššie uvedená tabuľka porovnáva komerčné kolaboratívne riešenia so zadefinovanými hodnotiacimi kritériami. Údaje uvedené v tabuľke pochádzajú z oficiálnych publikácii spoločností a sú doplnené verejne dostupnými analýzami zaoberajúcimi sa videokonferenčnou problematikou.[1] Tabuľka by mala byť vnímaná ako jeden zo vstupov pri procese rozhodovania o vhodnom videokonferečnom riešení.

[1] https://media.defense.gov/2020/Jun/03/2002310066/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-SHORT-20200602.PDF

Bližšie hodnotenie vybraných aplikácií a služieb

Mattermost

Mattermost[2] je komerčný softvér s otvoreným zdrojovým kódom určený na spoluprácu a komunikáciu medzi viacerými užívateľmi. Softvér však ponúka funkcionalitu videokonferencie len prostredníctvom integrácie so službami tretích strán (Zoom, CISCO Webex Cloud, BigBlueButton, Jitsi, Skype for Business a ďalšie), čím sa vyraďuje z užšieho okruhu analyzovaných videokonferenčných riešení. Mattermost je teda použiteľný najmä ako chatovacia platforma.

Napriek tomu ponúka 2FA, auditovateľnú kryptografiu, on-premise hostovanie a otvorený zdrojový kód (open-source). Neponúka však end-to-end šifrovanie, čo môže byť vnímané ako nedostatok, ak je kladený dôraz na zaručenie absolútnej dôvernosti prenášaných dát medzi odosielateľom a prijímateľom (v prípade chatových správ).

Zoom

Informácie vzťahujúce sa k Zoomu ako aj samotný softvér sú pomerne rozporuplné. Zoom bol na začiatku pandemickej krízy vďaka užívateľskej prívetivosti v komerčnom sektore a dokonca aj v rámci štátneho sektora viacerých krajín vnímaný ako prvá voľba.[3] S rastúcou popularitou sa začali objavovať problémy týkajúce sa súkromia, bezpečnosti a užívateľskej konfigurácie.[4]

Niektoré problémy týkajúce sa súkromia sa začiatkom roku 2020 zlepšili po tom, čo došlo k úprave licenčných podmienok. Avšak podľa viacerých zdrojov Zoom stále zbiera veľké množstvo užívateľských údajov.[5]

O bezpečnosti samotnej aplikácie sa začiatkom roku 2020 vyjadrovali odborníci nelichotivo, nakoľko vykazovala nedôsledné programátorské praktiky, ktoré mali za následok popri iných aj nasledovné problémy:

- škodlivá webstránka mala možnosť zapnúť bez povolenia webkameru užívateľa (klientska aplikácia pre MacOS),
- posielanie užívateľských dát Facebooku, aj keď užívateľ nemal Facebook účet (klientska aplikácia pre iPhone),
- Zoom mohol slúžiť ako prostriedok pri kompromitácii prihlasovacích údajov v systéme Windows, a to prostredníctvom chatovej funkcionality, v ktorej dochádzalo k odoslaniu NTLM hashov na adresu útočníka.[6]

[2] https://mattermost.com/
[3] https://www.bbc.com/news/technology-52126534
[4] https://www.cvedetails.com/vulnerability-list/vendor_id-2159/Zoom.html
[5] https://blogs.harvard.edu/doc/2020/03/30/zooms-new-privacy-policy/

Za zmienku stoja aj ďalšie problémy, ktoré sa týkali úniku užívateľských údajov, zlej kryptografie (v tomto prípade Zoom otvorene klamal) a veľmi pochybných praktík, kedy šifrovacie kľúče potrebné k zabezpečeniu hovoru boli účastníkom doručené prostredníctvom serverov nachádzajúcich sa v Číne. Napriek tomu, že všetci účastníci, rovnako ako klientska spoločnosť sídlili mimo územia Číny. Ďalší odborníci upozorňujú na fakt, že Zoom zamestnáva cca 700 programátorov prostredníctvom troch čínskych spoločností, čím sa vystavuje potenciálnemu tlaku zo strany tamojších štátnych orgánov napr. na úmyselné zavedenie bezpečnostnej chyby prostredníctvom ktorej by mohla byť ohrozená bezpečnosť aplikácie. [7]

Koncom prvého kvartálu roku 2020 po tlaku z viacerých strán zverejnila spoločnosť Zoom plán obsahujúci viacero krokov k zlepšeniu bezpečnosti ich produktu.[8]

Vyjadrenia viacerých expertov z oblasti kryptografie sa zhodujú v tom, že aplikácia sa stala po implementácii niektorých vylepšení bezpečnejšou, avšak stále existujú viaceré výhrady, napríklad týkajúce sa procesu generovania kryptografických kľúčov potrebných k zaisteniu bezpečnosti prenášaných dát. Popritom problém tzv. Zoombombingu v bezplatnej verzii aplikácie nebol stále vyriešený.

Je vhodné spomenúť, že odborníci kritizujúci Zoom za vyššie uvedené nedostatky. Po posledných bezpečnostných zlepšeniach uvádzajú, že používajú Zoom ako štandardné videokonferenčné riešenie pre výuku na Harvardskej univerzite.[9]

Google (Meet, Hangouts)

Poskytovateľ služby Google ponúka viacero služieb, menovite Hangouts – bezplatnú verziu videokonferenčnej cloudovej služby pre každého užívateľa s Google účtom a Google Meet – platenú aj bezplatnú verziu videokonferenčnej cloudovej služby tvoriacu súčasť platených služieb G Suite. Služby sú proprietárne, teda neponúkajú k nahliadnutiu zdrojový kód softvéru, na ktorom sú postavené. Rozdiely medzi uvedenými službami sú v ponúkanej funkcionalite. Napríklad zdieľanie obrazovky, limit na počet účastníkov alebo možnosť zúčastniť sa videokonferencie ako hosť bez registrácie. Pri službe Google Meet je vyžadované od hostí, aby sa prihlásili do Google účtu pokiaľ organizátor videokonferencie používa osobný účet. Pokiaľ organizátor využíva platený balíček G Suite, tak hostia sa dokážu zúčastniť videkonferencie aj bez prihlásenia do Google účtu.

Google Meet aj Hangouts sú dostupné prostredníctvom webového prehliadača, čo predstavuje výhodu z hľadiska multiplatformovosti. Jedná sa o cloudové riešenie bez možnosti vlastného hostovania služby.

Z pohľadu bezpečnosti sú obe riešenia na takmer rovnako dobrej úrovni, avšak ani jedno nepodporuje end-to-end šifrovanie. Pri oboch riešeniach je potrebné brať do úvahy, že užívateľské dáta sú predmetom záujmu poskytovateľa služby – spoločnosti Google.

---

6 https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html
7 tamtiež
8 https://blog.zoom.us/zoom-hits-milestone-on-90-day-security-plan-releases-zoom-5-0/
9 https://www.schneier.com/blog/archives/2020/04/secure_internet.html

Jitsi Meet

Jitsi Meet je súčasťou väčšieho softvérového balíčka s názvom Jitsi, ktorý je kolekciou multiplatformového bezplatného, slobodného softvéru s otvoreným zdrojovým kódom (open-source) určeného na VoIP, videokonferencie a chatovú komunikáciu.

Klientska strana aplikácie Jitsi Meet je postavená na JavaScripte a WebRTC a funguje prostredníctvom natívnej aplikácie ale aj z prostredia webového prehliadača, čo umožňuje jej použitie naprieč rôznymi platformami. Softvér taktiež ponúka natívne aplikácie pre väčšinu bežných operačných systémov. Softvér je bezplatný a serverová časť môže byť nasadená vo vlastnej infraštruktúre (on-premise), alebo môžu byť použité servery tretej strany prevádzkované dobrovoľníkmi.[10]

Jitsi Meet ponúka dva spôsoby šifrovania komunikácie. Prvý je štandardný prostredníctvom protokolov DTLS-SRTP a druhý je dodatočný end-to-end[11]. Štandardné šifrovanie prostredníctvom DTLS-SRTP je využívané medzi dvoma účastníkmi (1:1) v peer-to-peer (P2P) móde bez použitia tzv. Jitsi Videobridge (JVB), kde môžeme de facto hovoriť o end-to-end šifrovaní. V prípade viacerých účastníkov, kde je potrebné použiť tzv. Jitsi Videobridge (JVB), ktorý slúži ako preposielací uzol (relay) pre videohovory, dochádza k dočasnému dešifrovaniu hovorov, takže nie je zachovaný end-to-end princíp. Pri on-premise nasadení toto nemusí predstavovať zásadný problém. Pokiaľ je však kladený dôraz na zachovanie dôvernosti, je vhodné použiť dodatočnú end-to-end funkcionalitu šifrovania. Tá je momentálne dostupná pre vybrané webové prehliadače. Jitsi platforma ponúka taktiež veľké množstvo bezpečnostných rozšírení a doplnkov.[12] Z pohľadu použiteľnosti viaceré zdroje informujú o limite približne 30 – 35 účastníkov, pri prekročení ktorého dochádza k zníženiu kvality videohovoru. Nakoľko sme však Jitsi Meet nemali nasadené v našej infraštruktúre, nevieme tieto tvrdenia overiť.

Zvažujúc vyššie uvedené skutočnosti je Jitsi Meet veľmi zaujímavou alternatívou k viacerým komerčným – plateným službám, pričom ponúka naviac niektoré pokročilejšie rozšírenia alebo doplnky.

Skype for Business

Skype for Business je komerčný proprietárny videokonferenčný softvér s dlhou históriou, čomu zodpovedajú aj pokročilé funkcionality a integrácia s ostatnými produktami spoločnosti Microsoft. Softvér je súčasťou cloudového riešenia Office 365, ale môže byť nasadený aj vo vlastnej infraštruktúre (on-premise). Neponúka end-to-end šifrovanie a pri cloudovej verzii je oprávnené predpokladať, že užívateľské dáta budú predmetom záujmu poskytovateľa služby.

[10] https://meet.jit.si/
[11] https://jitsi.org/blog/e2ee/
[12] https://en.wikipedia.org/wiki/Jitsi#Jitsi_Meet

Od roku 2019 už Skype for Business nie je súčasťou produktového portfólia pre niektorých zákazníkov spoločnosti Microsoft a koniec celkovej podpory pre produkt je plánovaný na Júl 2021.[13] [14] Nástupcom sa stal Microsoft Teams.

Microsoft Teams

MS Teams je komerčný proprietárny softvér, ktorý ponúka nie len možnosť videohovorov ale aj ďalšie funkcie a možnosti spolupráce medzi užívateľmi (chat, zdieľanie obrazovky, spolupráca na dokumentoch). Softvér sa vyznačuje dobrou integráciou s ostatnými produktami spoločnosti Microsoft.

MS Teams je dostupný buď bezplatne, alebo ako platená verzia v rámci balíka Microsoft Office 365 (MS O365) ako cloudová služba SaaS.[15] Bezplatná verzia MS Teams poskytuje možnosť videohovorov prostredníctvom serverov Microsoftu pre 50 účastníkov, pri platených verziách môže byť počet účastníkov vyšší. V oboch prípadoch je možná účasť na videokonferencii aj bez nutnosti registrácie (hosťovský účet).[16] Pri využívaní bezplatnej verzie je citeľná snaha poskytovateľa služby presvedčiť užívateľa k predplateniu služieb MS O365.[17]

Softvér ponúka klientsku aplikáciu pre viaceré platformy (Windows, GNU/Linux, MacOS, Android, iOS) a taktiež možnosť pripojiť sa prostredníctvom webového prehliadača. Dostupná je aj možnosť používať viacfaktorovú autentifikáciu (2FA).

Používa štandardné šifrovanie prostredníctvom protokolov TLS, mTLS a SRTP, ale neponúka možnosť end-to-end šifrovania, čo ho diskvalifikuje v scenároch, kde si užívatelia potrebujú vymieňať citlivé informácie. MS Teams podobne ako konkurenčný softvér zaznamenala v posledných rokoch niekoľko vážnych zraniteľnosti, ktoré boli v rámci manažmentu zraniteľností v krátkom období opravené.

MS Teams predstavuje dobre použiteľné riešenie na komunikáciu a spoluprácu v organizáciách, avšak je potrebné zvážiť vyššie popísané nedostatky softvéru/služby. Platená verzia je dobre škálovateľná a bezplatná verzia môže poskytnúť dostatočne multiplatformové riešenie pre obmedzený počet účastníkov. Softvér disponuje dobrou bezpečnosťou[18], avšak neposkytuje možnosť end-to-end šifrovania, čo v kombinácii s cloudovým prostredím, kde šifrovacie kľúče sú manažované poskytovateľom služby, prípadne hybridným nasadením, vytvára priestor pre zber užívateľských dát poskytovateľom služby. Microsoft už v minulosti vyvolal niekoľkokrát pochybnosti o súkromí užívateľských dát.[19]

---

[13] https://docs.microsoft.com/en-us/office365/servicedescriptions/skype-for-business-online-service-description/skype-for-business-online-service-description

[14] https://docs.microsoft.com/en-us/skypeforbusiness/legal-and-regulatory/end-of-integration-with-3rd-party-providers

[15] https://www.microsoft.com/en-us/microsoft-365/microsoft-teams/compare-microsoft-teams-options

[16] https://answers.microsoft.com/en-us/msoffice/forum/all/microsoft-team-free-version-group-call-limit/11c54ae6-e55a-4b2c-89e0-75620a21e950

[17] https://www.theverge.com/2018/7/12/17563710/microsoft-teams-free-version-slack-competitor

[18] https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide

[19] https://www.forbes.com/sites/daveywinder/2019/08/28/microsoft-confirms-windows-10-privacy-investigation-with-a-4-billion-sting/

Technická podpora spoločnosti Microsoft nás počas prípravy tejto analýzy informovala, že spoločnosť pracuje na koncepte, kedy by mala mať organizácia možnosť použiť vlastné šifrovacie kľúče, čo by mohlo zvýšiť dôvernosť prenášaných dát.

Cisco Webex

Webex od spoločnosti Cisco je komerčné proprietárne videokonferenčné riešenie s možnosťou použitia aj bezplatnej verzie. Serverová časť produktu beží v infraštruktúre poskytovateľa služby, jedná sa teda o cloudovú službu. Nasadenie serverovej časti on-premise už nie je možné, nakoľko Cisco Webex Meetings Server oznámil end-of-life, teda koniec predaja a podpory produktu, ktorý mohol byť nasadený vo vlastnej infraštruktúre.[20]

Z informácií pojednávajúcich o bezpečnosti produktu a modelovaní rizík zverejnených výrobcom vyplýva, že spoločnosť má seriózny záujem na bezpečnosti produktu.[21] Softvér používa štandardné auditovateľné kryptografické algoritmy a protokoly, pri ktorých momentálne nie sú verejne známe žiadne bezpečnostné zraniteľnosti. Z bezpečnostného hľadiska nás zaujali nasledovné informácie deklarované spoločnosťou.

Pri tzv. encryption-at-rest, teda šifrovaní dát uložených na pamäťových médiách v infraštruktúre poskytovateľa služby, disponuje šifrovacími kľúčmi prevádzkovateľ služby – spoločnosť Cisco, ktorá tvrdí, že ich spravuje pre svojich zákazníkov. Jedná sa v tomto prípade o užívateľské dáta a dáta súvisiace s videokonferenciami, avšak možnosť uchovávať tieto dáta je voliteľná. Pri použití verejnej telefónnej siete v prípade audiohovoru dochádza k dešifrovaniu dát na serveroch poskytovateľa služby (Webex) za účelom prevodu dát a ich prípadného nahrávania.

Pri videohovoroch s použitím end-to-end šifrovania sa zdieľaný symetrický kľuč generuje na koncovom zariadení hostiteľa (osoba vytvárajúca meeting) a následne sa za použitia asymetrickej kryptografie distribuuje medzi ďalších účastníkov videokonferencie. Tento proces si kladie za cieľ zaručiť dôvernosť prenášaných dát tak, aby prístup k prenášanej informácii mal iba koncový klient (účastník).

Je vhodné zdôrazniť, že end-to-end šifrovanie nie je možné použiť pri viacerých príležitostiach a taktiež je nekompatibilné s viacerými funkcionalitami: [22]

- použitie fyzických meetingových zariadení (dedikované webkamery s mikrofónom),
- Cisco Webex Meetings webová aplikácia (klientsky softvér),
- klientsky softvér pre systémy GNU/Linux,
- pripojenie sa do meetingu ešte pred hostiteľom a
- ďalšie..[23]

[20] https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meetings-server/datasheet-c78-717754.html
[21] https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf
[22] tamtiež
[23] tamtiež

Z uvedeného je asi najdôležitejší fakt, že princíp E2EE nie je kompatibilný s webovou aplikáciou Webex. Táto skutočnosť v kombinácii s využívaním cloudovej infraštruktúry Cisco diskvalifikuje použitie Webexu v prípadoch, kedy sa užívatelia snažia o využitie multiplatformovosti a zároveň o zachovanie absolútnej dôvernosti prenášaných dát.

Napriek tomuto nedostatku sa Webex teší vysokej popularite a býva častokrát vnímaný ako alternatíva k Zoom-u. Okrem videokonferencie ponúka aj chat, plánovanie, kreslenie a zdieľanie obrazovky, čo zvyšuje jeho použiteľnosť pre bežného používateľa v podnikovom prostredí. Veľmi dobré ohlasy sú aj na spoľahlivosť samotného produktu.[24] Produkt Webex má v rámci manažmentu zraniteľností vlastnú Bug Bounty iniciatívu, čo dáva priestor na nahlasovanie bezpečnostných chýb nájdených dobrovoľníkmi.[25]

Zhrnutie

Analýza priblížila schopnosti a vlastnosti vybraných videokonferenčných riešení. Väčšina analyzovaných služieb je vhodná na bežnú prácu, ako výučby študentov z domu alebo pracovné porady kolegov, na ktorých nebudú komunikovane citlivé informácie a kde bezpodmienečné zachovanie ich dôvernosti, ako aj niektorých časti súkromia nebudú vnímané ako determinujúci faktor.

V prvom teoretickom scenári sme sa zaoberali situáciou, kedy pracovníci niektorej z organizácií budú pracovať z prostredia domova a budú musieť komunikovať a vymieňať si informácie. V tomto prípade môže nastať situácia, kedy si účastníci videokonferencie budú potrebovať vymeniť aj informácie citlivej povahy.

Pre tento scenár odporúčame výber videokonferenčného riešenia spĺňajúceho nasledovne kritéria:

- end-to-end šifrovanie (E2EE) - zaručuje zachovanie dôvernosti dát medzi účastníkmi,
- viacfaktorová autentifikácia (2FA) - zaručuje dodatočnú formu zabezpečenia pri prihlasovaní,
- možnosť lokálneho hostingu (on-premise) - možnosť mať pod kontrolou infraštruktúru, na ktorej beží serverová časť softvéru a taktiež metadáta vznikajúce pri prevádzke služby.

Doplnkovými kritériami môžu byť užívateľská prívetivosť a multiplatformovosť, preferujúc možnosť pripojiť sa do videokonferencie prostredníctvom webového prehliadača.

Pri organizáciách, ktoré disponujú vlastnou IT infraštruktúrou a dostatočne zdatným personálom v oblasti prevádzky ako aj informačnej bezpečnosti, pripadajú do úvahy on-premise riešenia, teda softvér hostovaný vo vlastnej infraštruktúre. Pre tento prípad si vieme predstaviť použitie nasledovného softvéru.

[24] https://www.nytimes.com/wirecutter/reviews/best-video-conferencing-service/
[25] https://hackerone.com/webex

- Jitsi Meet.

V opačnom prípade, kedy organizácia nemá dostatočné hardvérové prostriedky a/alebo dostatočne odborný IT personál, odporúčame prikloniť sa k niektorému z nižšie uvedených poskytovateľov cloudových služieb.

- Cisco Webex - využívajúc natívnu aplikáciu pre MS Windows s end-to-end šifrovaním,
- Zoom – využívajúc end-to-end šifrovanie.

Spomedzi analyzovaných riešení veľmi dobre obstála aj aplikácia Signal, ktorú vnímame ako etalón bezpečnej komunikácie a súkromia. Je to multiplatformová aplikácia s otvoreným zdrojovým kódom a end-to-end šifrovaním, využívajúca cloudovú infraštruktúru spoločnosti Signal. Nevýhodou je, že z pohľadu videokonferencií ponúka Signal rozhovory len v režime 1:1, čo ho diskvalifikuje pre bežné použitie v oboch scenároch. Pokiaľ však chceme docieliť dôvernosť videohovoru medzi dvoma účastníkmi, je Signal rozhodne dobré riešenie.

Pre teoretický scenár, v ktorom by vzdelávacie inštitúcie mohli použiť niektoré z videokonferenčných riešení na diaľkovú výučbu si dokážeme predstaviť riešenie s nasledujúcimi vlastnosťami:

- Bezplatné riešenie – odstránenie vstupnej bariéry vo forme obstarávacích nákladov.
- Hostované v cloude – vyriešia sa tým starosti s vlastnou infraštruktúrou (potrebný hardware, nasadzovanie, administrácia) a personálom.
- Multiplaformovosť – možnosť zúčastniť sa videokonferencie prostredníctvom webového prehliadača, aby bolo možné pripojiť sa z akéhokoľvek zariadenia, resp. operačného systému.
- Riadenie prístupu do videokonferencie – správca udalosti má mať možnosť riadiť prístup do videokonferencie.

Doplnkovými kritériami môže byť rozsah zbierania užívateľských dát a nakladanie s nimi, ako aj užívateľská prívetivosť, keďže užívatelia pravdepodobne nebudú vysoko technicky zdatní. Samotná bezpečnosť väčšiny posudzovaných videokonferenčných riešení je pre vyššie uvedený účel dostačujúca.

Konkrétne riešenia spĺňajúce vyššie uvedené požiadavky:

- Jitsi Meet (využívajúc serverovú infraštruktúru spoločnosti 8×8 [26]),
- Cisco Webex,
- Zoom,
- Microsoft Teams.

[26] https://meet.jit.si/

Pri službách od spoločností Google alebo Amazon vnímame potrebu registrácie u týchto spoločností ako určitú vstupnú bariéru.

Za spomenutie stojí aj skutočnosť, že niektoré prestížne zahraničné univerzity (Harvard) sa rozhodli používať Zoom ako štandardný prostriedok na vzdialenú výučbu. Jeho používanie povolilo aj mesto New York pre svoje školy po tom, ako došlo k oprave bezpečnostných chýb, ktoré boli objavené začiatkom roku. [27] [28]

Dodatočné zdroje

https://blog.mozilla.org/blog/2020/04/28/which-video-call-apps-can-you-trust/

https://freedom.press/training/blog/videoconferencing-tools/

https://www.schneier.com/blog/archives/2020/04/secure_internet.html

https://www.securemessagingapps.com/

https://www.securemessagingapps.com/about/

https://videoconferencing.guide/

https://blogs.harvard.edu/doc/2020/03/30/zooms-new-privacy-policy/

https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

[27] https://www.schneier.com/blog/archives/2020/04/secure_internet.html

[28] https://www.washingtonpost.com/education/2020/05/10/nyc-schools-lift-ban-zoom-even-hackers-hit-other-educational-online-events-with-horrendous-material/