NKSC prie KAM
Inovacijų ir mokymo skyrius
support@ims.nksc.lt

2020 – 11 – 11

TELEKONFERENCINIŲ PROGRAMINIŲ SPRENDIMŲ APŽVALGA IR REKOMENDACIJOS

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) stebi ir vertina telekonferencijų platformų kibernetinio saugumo bei asmens duomenų privatumo aspektus. Esant poreikiui, apie grėsmes saugumui bei rekomendacijas dėl nuotolinio darbo priemonių skelbiame NKSC interneto svetainėje.

NKSC atliko devynių rinkoje paplitusių telekonferencinių programinių sprendimų kibernetinio saugumo apžvalgą ir parengė rekomendacijas, leidžiančias saugiau naudoti produktų teikiamą funkcionalumą. Apžvalgoje nagrinėti devyni telekonferenciniai sprendimai: „Cisco WebEx Meetings“, „Google Meet“, „Microsoft Teams“, „BigBlueButton“, „Zoom“, „Jitsi Meet“, „Skype for Business“, „Slack“ ir „GoToMeeting“.

Nagrinėti sprendimai veikia Windows, iOS, macOS, Linux ir Android platformose. Svarbu tai, kad visuose produktuose yra įdiegta duomenų privatumą iš dalies užtikrinanti funkcija – audiovizualinio ryšio trakto ir tekstinių žinučių šifravimas. Tiesioginio šifravimo (*angl.* End-to-End Encryption, E2EE) funkcionalumas (skirtas užtikrinti, kad duomenys, siunčiami iš vieno įrenginio kitam, būtų apsaugoti visame duomenų perdavimo trakte) pilnai įdiegtas tik dalyje analizuotų sprendimų – „Cisco Webex Meetings“, „Microsoft Teams“ ir „Skype for Business“.

Verta pažymėti, kad nuo 2020 m. spalio antros pusės „Zoom“ sprendime E2EE funkcionalumas yra įdiegtas. Saugumo funkcija 30 dienų laikotarpyje veikia testavimo režimu[1] – šiuo periodu telekonferencijos organizatorius, kurdamas konferencinį pokalbį, turi savarankiškai ją aktyvuoti. „Jitsi Meet“ jį palaiko iš dalies, o „Google Meet“, „BigBlueButton“, „Slack“ ir „GoToMeeting“ produktuose šis saugumo išpildymas nėra naudojamas.

Telekonferenciniai sprendimai „BigBlueButton“ ir „Jitsi Meet“ gali būti realizuoti vartotojo valdomoje (administruojamoje) infrastruktūroje ir ryšio vykdymui (ar jo organizavimui) naudoti konkrečius, vartotojo nurodytus, serverius. Šis funkcionalumas, esant tam tikroms komercinėms sąlygoms, gali būti užtikrintas ir „GoToMeeting“ sprendime. Tai aktualu įmonėms ir korporacijoms dirbančioms tose šalyse, kur įstatymais reikalaujama jog asmens duomenys būtų saugomi tos šalies teritorijos serveriuose (Austrija, Suomija ir kt.).

Kiti nagrinėti sprendimai šios galimybės neturi, ryšio vykdymui (ar jo organizavimui) yra naudojama vartotojų nevaldoma, sprendimų kūrėjų administruojama infrastruktūra, dažniausiai naudojant debesų kompiuterijos sprendimus.

Lyginant vartotojo valdomus sprendimus su nevaldomomis sistemomis, galima teigti, kad sprendimų realizavimas korektiškai parengtoje, tinkamai administruojamoje ir stebimoje nuosavoje infrastruktūroje leidžia pasiekti geresnius perduodamų duomenų saugos rezultatus.

Detalesnė telekonferencinių programinių sprendimų apžvalga, nurodant palaikomas kibernetinio saugumo funkcijas, pateikta 1 lentelėje.

Siekiant užtikrinti didesnį telekonferenciniu ryšiu perduodamų duomenų saugumą, NKSC rekomenduoja:

1. Rezervuotai naudoti telekonferencijų platformas jautrių ir konfidencialių duomenų persiuntimui, visada įvertinti duomenų nutekėjimo riziką.
2. Reikia būti itin atidžiais naudojant telekonferencijų programinius sprendimus, realizuotus naršyklės pagalba pasiekiamais internetiniais portalais – egzistuoja telekonferencinių sprendimų

[1] Zoom informacija. *https://blog.zoom.us/zoom-rolling-out-end-to-end-encryption-offering/*

portalų klastotės, kuriose bandoma surinkti vartotojų duomenis arba priversti atsisiųsti kenkėjišką programinį kodą.

3. Naudoti tik pačias naujausias telekonferencinių programinių sprendimų versijas, kuriose yra ištaisyti žinomi pažeidžiamumai arba padidintas perduodamų duomenų šifravimas.
4. Neskelbti telekonferencinio pokalbio kanalų identifikacinio numerio (ID) viešai, pokalbių kambarius turėtų apsaugoti slaptažodžiais.
5. Esant galimybei, vartotojus į pokalbio kambarį rekomenduojama įtraukti per virtualų laukiamąjį (*angl.* Waiting-room), o ekranu dalintis (*angl.* Share-screen) leisti tik pokalbio organizatoriui. Ekrano dalinimosi metu paisyti „švaraus darbastalio“ etiketo.
6. Įvertinti turimų įrenginių saugumo charakteristikas – vartotojams jungiantis iš pažeistų sistemų, konferencijos programos saugumas įtakos neturės. Būtina išlikti budriems ir kritiškai vertinti gaunamas nuorodas ir siunčiamas rinkmenas (*žarg.* failus).
7. Paisyti bendrųjų kibernetinio saugumo rekomendacijų, pateiktų NKSC prie KAM internetiniame puslapyje: *https://www.nksc.lt/rekomendacijos.html*.

1 lentelė. Telekonferencinių programinių sprendimų apžvalga, nurodant palaikomas kibernetinio saugumo funkcijas

Eil. Nr.	Programinės įrangos pavadinimas	Dabartinė versija	Operacinių sistemų palaikymas	Komunikacijos protokolai	Šifravimo protokolai	Programinės įrangos turimi (deklaruojami) sertifikatai	Balso, vaizdo, teksto šifravimas ryšio trakte	E2EE šifravimo *(End-to-End Encryption)* funkcionalumas	Šalis	2020 m. registruotų saugumo spragų kiekis[2]	Pastabos
1	Cisco WebEx Meetings	Linux – naudojamas internetinis portalas, macOS – 40.11.4.15, Windows – 40.11.4.15, Android – 40.11.0, iOS – 40.11.0	Linux, macOS, Windows, Android, iOS	WebRTC, SIP, H.323, H.225 arba H.245	TLS 1.2, SRTP	ISO 27001, FedRAMP, Privacy Shield Framework [3]	Taip	Pagal nutylėjimą ši funkcija yra išjungta, tačiau galimas šios funkcijos aktyvavimas	JAV	17	E2EE funkcionalumo įvedimas leidžia ženkliai padidinti telekonferencijos saugumą. Telekonferencinis ryšys organizuojamas per Cisco serverius. Galimybės naudoti vartotojo valdomą serverį nėra.
2	Google Meet	Linux, macOS ir Windows platformoms naudojamas internetinis portalas – meet.google.com, Android – 2020.10.18.338 565675.Release, iOS – 49.0.0	Linux, macOS, Windows, Android, iOS	WebRTC	DTLS-SRTP	SOC 1/2/3, ISO 27001, ISO 27017, ISO 27018, FedRAMP Moderate ATO, HIPAA, HITRUST CSF, GDPR, Privacy Shield Framework, BSI C5, ENS High, MTCS Tier 3, OSPAR, CSA STAR [4]	Taip	Ne [5]	JAV	0	Telekonferencinis ryšys organizuojamas per Google serverius. Galimybės naudoti vartotojo valdomą serverį nėra.
3	Microsoft Teams	Linux – 1.3.00.25560,	Linux, macOS,	MNP24	MTLS-SRTP[6]	Nenustatyta	Taip	Pagal nutylėjimą naudojama	JAV	1	Telekonferencinis ryšys vykdomas per Microsoft

[2] JAV Nacionalinio standartų ir technologijų instituto (National Institute of Standards and Technology. U.S. Department of Commerce) informacija. *https://nvd.nist.gov/*
[3] Cisco Systems informacija. *https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf*
[4] Fourcast.io informacija. *https://www.fourcast.io/blog/security-privacy-in-google-meet-video-conferencing*
[5] Google dokumentacija. *https://support.google.com/a/answer/7582940?hl=en*
[6] Microsoft informacija. *https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide*

		macOS – 1.3.00.23764, Windows – 1.3.00.26064, Android – 1416/1.0.0.2020110302, iOS – 2.0.25	Windows, Android, iOS					konfigūracija sudaro technines sąlygas Microsoft atlikti turinio dešifravimą, tačiau yra galimybė Microsoft šifravimo raktus pakeisti savais raktais ir išvengti duomenų nutekėjimo rizikos			serverius. Galimybės naudoti vartotojo valdomą serverį nėra.
4	BigBlueButton	Linux, macOS ir Windows platformoms naudojamas internetinis portalas	Linux, macOS, Windows	WebRTC [7]	DTLS – SRTP	Nenustatyta	Taip	Ne	Kanada	17	Telekonferenciniam ryšiui naudojamas vartotojo valdomas serveris.
5	Zoom	Linux – 5.4.53391.1108 macOS – 5.4.2, Windows - 5.4.2 (58740.1105), Android – 5.4.2.524, iOS – 5.4.2	Linux (dalinai), macOS, Windows, Android, iOS	WebRTC data channels, Websockets[8], alternatyviai – SIP ir H.323 [9]	TLS 1.2, SRTP [10]	Soc 2, FedRAMP	Taip	Testavimo stadijoje	JAV	9	Zoom E2EE funkcionalumas šiuo metu yra testavimo stadijoje ir 2021 planuojama teikti paslaugą visiems Zoom vartotojams. Toronto universiteto (Kanada) tarpdisciplininė laboratorija „The Citizen Lab“ nustatė, kad Zoom aplikacija yra kuriama trijų, 700 darbuotojų turinčių Kinijos įmonių, esančiais vienodais „Ruanshi Software“ pavadinimais.

[7] BigBlueButton informacija. *https://docs.bigbluebutton.org/*
[8] Webrtchacks informacija. *https://webrtchacks.com/zoom-avoids-using-webrtc/*
[9] Zoom informacija. *https://support.zoom.us/hc/en-us/articles/201362723-Encryption-for-Meetings*
[10] Zoom dokumentacija. *https://zoom.us/docs/doc/Zoom%20Encryption%20Whitepaper.pdf*

											Ankstesnėse Zoom versijose[11] buvo aptiktos kritinės saugumo spragos ir netiesiogiai JAV federalinės prekybos komisijos[12] iškeltas klausimas dėl saugumo garantijų pastūmėjo gamintoją parengti šifravimo metodą, ištaisantį aptiktas saugumo spragas[13]. Zoom įsipareigojo atlikti nepriklausomą vystomų sprendimų analizę. Telekonferencinis ryšys vykdomas per Zoom serverius. Galimybės naudoti vartotojo valdomą serverį nėra.
6	Jitsi Meet	Linux – 2.0.5142, macOS – 2.10.5550, Windows – 2.10.5550, Android – 20.4.2, iOS – 20.4.2	Linux, macOS, Windows, Android, iOS	WebRTC, XMPP	DTLS-SRTP	Nenustatyta	Taip	Iš dalies palaikomas	JAV	2	Tiesioginė komunikacija yra šifruojama „End-to-End“ principu. Konferenciniai skambučiai yra dešifruojami serveryje ir kiekvienas vaizdo traktas yra peršifruojamas atskirai kiekvienam vaizdo konferencijos dalyviui. Telekonferencinis ryšys vykdomas per Jitsi Meet serverius.

[11] Talosintelligence.com informacija. https://blog.talosintelligence.com/2020/06/vuln-spotlight-zoom-code-execution-june-2020.html
[12] Arstechnica.com informacija. https://arstechnica.com/tech-policy/2020/11/zoom-lied-to-users-about-end-to-end-encryption-for-years-ftc-says/
[13] Wired.com informacija. https://www.wired.com/story/how-to-enable-zoom-encryption/

											Yra galimybė naudoti vartotojo valdomą serverį.
7	Skype for Business	macOS – 16.29.39, Windows – 16.0.13426.20120, Android – 6.27.0.18, iOS – 6.27.0	macOS, Windows, Android, iOS	SIP, Uždaras vaizdo siuntimo protokolas	MTLS-SRTP	Nenustatyta	Taip	Pagal nutylėjimą naudojama konfigūracija sudaro technines sąlygas Microsoft atlikti turinio dešifravimą, tačiau yra galimybė Microsoft šifravimo raktus pakeisti savais raktais ir išvengti duomenų nutekėjimo rizikos	JAV	3	Telekonferencinis ryšys vykdomas per Microsoft serverius. Galimybės naudoti vartotojo valdomą serverį nėra.
8	Slack	Linux – 4.11.1, macOS – 4.10.3, Windows – 4.11.0, Android – 20.10.20.0, iOS – 20.11.10	Linux, macOS, Windows, Android, iOS	WebRTC, TURN, STUN	TLS 1.2, DTLS-SRTP	ISO 27001, ISO 27017, ISO 27018, SOC 2, SOC 3	Taip	Ne	JAV	0	Telekonferencinis ryšys vykdomas per Slack serverius. Galimybės naudoti vartotojo valdomą serverį nėra.
9	GoToMeeting	Linux – naudojamas internetinis portalas, macOS – 10.14.0, Windows – 10.14.0.18962, Android – 4.6.0.7, iOS – 7.12.0	Linux, macOS, Windows, Android, iOS	WebRTC, AVTP	TLS 1.2, SRTP	CCPA, SOC2 Type II + BSI C5, TRUSTe Verified Privacy	Taip	Ne	JAV	0	Konferenciniai skambučiai yra dešifruojami serveryje ir kiekvienas vaizdo traktas yra peršifruojamas atskirai kiekvienam vaizdo konferencijos dalyviui. Komerciniai klientai turi galimybę telekonferenciniam ryšiui naudoti jų pačių valdomus serverius.