Videokonference bezpečně

Co je videokonference?

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

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

ÚČASTNÍCI VIRTUÁLNÍCH SCHŮZEK

POUŽÍVEJTE JEN OFICIÁLNÍ APLIKACE DODAVATELŮ
Stahujte pouze oficiální aplikace dodavatelů z ověřených zdrojů, jako jsou Google Play nebo Apple Store, případně systémy důvěryhodných poskytovatelů (Microsoft, Google, Cisco atd.). A pravidelně aktualizujte!

CHRAŇTE DŮVĚRNOST PŘÍSTUPOVÝCH ÚDAJŮ SCHŮZKY
Nesdílejte veřejně odkaz na schůzku, Vaše ID ani ID moderátora nebo PIN hosta.

MĚJTE KONTROLU NAD SDÍLENÝM OBSAHEM
Pokud je to možné, vyhněte se kliknutí na odkazy (nebo příjmu datových souborů), které jsou sdíleny v relačním chatu, zejména pokud neznáte osobu, která je sdílela.

SEZNAMTE SE S DOSTUPNÝMI FUNKCEMI
Seznamte se s jednotlivými funkcemi, které jsou pro Vás v rámci videokonference dostupné, a naučte se je používat.

POUŽÍVEJTE FUNKCI ZMĚNY NEBO ROZOSTŘENÍ POZADÍ
Zabráníte tak úniku citlivých informací.

VĚNUJTE POZORNOST ZABEZPEČENÍ UŽIVATELSKÝCH STANIC
Vybavte anitivirovým systémem všechna zařízení, ze kterých se připojujete. Operační systém i antivirový systém pravidelně aktualizujte.

NAPLÁNUJTE SCHŮZKY S JEDINEČNÝM IDENTIFIKÁTOREM (ID) PRO KAŽDOU JEDNOTLIVOU SCHŮZKU

Nepoužívejte permanentní videokonference, pokud jste nezablokovali přístup novým uživatelům nebo pokud nelze k videokonferenci přistupovat jen na základě pozvání.

ZNEJTE PŘESNÝ POČET UŽIVATELŮ

Vždy předem naplánujte společná setkání, ať už jde o audio nebo video obsah, s přesným počtem uživatelů. Ve chvíli, kdy všichni uživatelé vstoupí do videokonference (virtuální meeting room), uzavřete přístup novým uživatelům.

POSUZUJTE DŮVĚRNOST PROBÍRANÝCH TÉMAT A VHODNOST POUŽITÉ TECHNOLOGIE

Řiďte se schválenou interní politikou a buďte v souladu s nastavenou bezpečnostní úrovní videokonference (vizte dokument Bezpečnostní standard pro videokonference).

ZABEZPEČTE VAŠI VIRTUÁLNÍ SCHŮZKU

Zkontrolujte, zda je při zahájení schůzky povoleno šifrování.

PRO POZVÁNKY NA SCHŮZKY POUŽÍVEJTE NEJBEZPEČNĚJŠÍ PROSTŘEDKY

Pokud je to možné, zasílejte pozvánky na schůzky prostřednictvím jiných šifrovaných a ověřených služeb spolupráce. Nezveřejňujte pozvánky na schůzky na veřejně přístupných fórech nebo webech. Pokud musí být pozvánky zaslány otevřeným způsobem, zasílejte hesla nebo PIN jiným způsobem (např. e-mail a SMS nebo e-mail a telefonicky).

POUŽÍVEJTE HESLA NEBO KÓD PIN

Zajistěte, že všichni uživatelé, kteří mají přístup na schůzku, ke schůzce přistoupí pomocí hesla nebo PINu.

NAKONFIGURUJTE SCHŮZKU TAK, ABY VIZUÁLNÍ NEBO ZVUKOVÝ INDIKÁTOR VAROVAL PŘED VSTUPEM NEBO ODCHODEM NOVÉHO UŽIVATELE

Zajistěte, že moderátor a ideálně i ostatní uživatelé budou mít přesné a pravdivé informace o lidech, kteří jsou ke schůzce připojeni, a disponují jednoznačnými identifikátory těchto osob (například jméno nebo jiný spolehlivý způsob). To platí zejména u připojení využívajících pouze audio (zvuk).

ŘIĎTE PŘISTUPOVÁNÍ ÚČASTNÍKŮ KE SCHŮZCE

Zajistěte, aby uživatelé neměli přístup ke schůzce, dokud se moderátor nepřipojí, a aby po odchodu moderátora byla schůzka ukončena.

ZAJISTĚTĚ, ABY VŠECHNY SDÍLENÉ INFORMACE BYLY PRO UŽIVATELE NEZBYTNÉ A PŘÍNOSNÉ

Naplánujte si předem témata, která mají být probírána, a zvažte důsledky neplánovaného zveřejnění obsahu schůzky, abyste porozuměli možným rizikům.

BUĎTE OBEZŘETNÍ PŘI SDÍLENÍ OBRAZOVKY

Sdílejte pouze to, co je relevantní pro probíraná témata v rámci videokonference. Pokud je obsah citlivý, ujistěte se, že je vhodné tento obsah sdílet se všemi uživateli.

SEZNAMTE UŽIVATELE S DOSTUPNÝMI FUNKCEMI

Zajistěte, aby všichni uživatelé věděli, jak používat základní funkce videokonference, nebo zajistěte, aby vybrané funkce nebyly neznalým uživatelům k dispozici (například: sdílení obsahu apod.).

VĚNUJTE POZORNOST ZABEZPEČENÍ UŽIVATELSKÝCH STANIC

Vybavte zařízení, ze kterých se uživatelé připojují, softwarem pro ochranu před škodlivým kódem. Operační systém i software pro ochranu před škodlivým kódem pravidelně aktualizujte.

Role moderátora

Jako moderátor schůzky musíte být schopni řídit připojení uživatelů a musíte mít možnost vyloučit uživatele, ztlumit mikrofony nebo deaktivovat sdílený obsah či video.

MODERÁTOR SCHŮZKY ZAJIŠŤUJE ZÁZNAM (ZVUKU, VIDEA NEBO OBSAHU), POKUD MÁ BÝT ZAZNAMENÁN

Pokud zaznamenáváte zvuk, video nebo jiný obsah schůzky, všem uživatelům zobrazte vizuální a zvukový indikátor upozorňující na nahrávání. V případě použití cloudové služby se předem ujistěte, kde bude nahrávka uložena, kdo bude jejím vlastníkem a zda je možné její bezpečné smazání.

ZAJISTĚTE KOMFORTNÍ A NERUŠENÝ PRŮBĚH SCHŮZKY

Zajistěte, aby všichni uživatelé měli ztlumené mikrofony, pokud zrovna nehovoří. Tím se sníží počet rušivých elementů (echo, okolní ruchy apod.) a zároveň klesne riziko možného sdílení informací, které se schůzkou nesouvisí.

SNAŽTE SE ELIMINOVAT POTENCIÁLNÍ RIZIKA SDÍLENÍ OBSAHU SCHŮZKY S NEPOZVANÝMI OSOBAMI, A POKUD TO NENÍ MOŽNÉ, ALESPOŇ NA TATO RIZIKA UPOZORNĚTE

Pokud to vyžaduje charakter schůzky, doporučte účastníkům, aby se zdržovali jen v prostoru, kam nemají přístup jiné osoby.