Cisco WebEx bedste praksis for sikre møder til webstedsadministratorer og værter

Første gang udgivet: 15. marts 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

INDHOLD

Oversigt over WebEx-databeskyttelse

Cisco WebEx online løsninger hjælper globale medarbejdere og virtuelle teams med at holde møde og samarbejde i realtid, som hvis de arbejdede i det samme lokale. Virksomheder, institutioner og offentlige organer over hele verden, stoler på Cisco WebEx-løsninger til at forenkle deres forretningsprocesser og forbedre resultater for salg, markedsføring, undervisning, projektstyring og supportteams.

For alle disse organisationer og deres brugere, er databeskyttelse en grundlæggende bekymring. Online samarbejde skal tilbyde flere sikkerhedsniveauer, fra planlægning af møder til bekræftelse af deltagere til indholdsdeling.

Cisco WebEx er et sikkert miljø, men det kan dog konfigureres som et åbent sted til samarbejde. Forståelse af databeskyttelsesfunktionerne, som webstedsadministratorer og slutbrugere, kan tillade dig at skræddersy WebEx til din virksomheds behov.

For yderligere oplysninger, se WebEx hvidbog om sikkerhed.

Bedste praksis for administratorer

Effektiv databeskyttelse starter med WebEx-webstedsadministration, som tillader administratorer at administrere og håndhæve privatlivspolitikker for værts- og præsentationsværtsprivilegier. For eksempel kan en autoriseret administrator brugertilpasse sessionskonfigurationer til at deaktivere en præsentationsværts evne til at dele applikationer, eller til at overføre filer pr websted eller pr bruger.

Vi anbefaler at bruge følgende funktioner til beskyttelse af dine møder.

Gør alle møder til ikke-angivne

Selv mødetitler kan afsløre følsomme oplysninger. For eksempel et møde kaldet ”Diskussion af opkøb af virksomhed A” kan have finansielle indvirkninger, hvis det afsløres før tid. Oprettelse af ikke-angivne møder opretholder databeskyttelsen af følsomme oplysninger.

For angivne møder, vises mødeemnet og andre oplysninger på dit websted for autoriserede brugere, ligesom for uautoriserede brugere og gæster. Medmindre din organisation har et specifikt forretningsbehov for at vise mødetitler og oplysninger offentligt, bør alle møder markeres som ikke-angivne.

Procedure

Trin 1 Log ind på WebEx-websted administrationsværktøj.

Trin 2 Naviger til **Konfiguration > Fælles webstedsindstillinger > Valgmuligheder > Sikkerhedsindstillinger**.

Trin 3 Marker feltet for **Alle møder skal være ikke-angivne (MC, TC, og EC)**.

Kræv adgangskoder for alle møder, begivenheder og sessioner

Det mest effektive skridt til at styrke sikkerheden af alle dine møder, begivenheder og undervisningssessioner er at kræve en adgangskode. Adgangskoder beskytter mod uautoriseret deltagelse, fordi det kun er brugere med adgang til adgangskoden, der kan deltage. Ved at følge fremgangsmåden til at kræve adgangskoder sikrer man, at alle møder, begivenheder og undervisningssessioner oprettet af værter er sikre.

Vi anbefaler, at du bruger en meget stærk og usædvanlig adgangskode (stærk adgangskode). En stærk adgangskode bør indeholde en blanding af store og små bogstaver, numre og specialtegn (for eksempel, $Tu0psrOx!).

Bemærk Tilføjelse af adgangskoder til dine møder, begivenheder og undervisningssessioner påvirker ikke deltagelsesoplevelsen for autoriserede mødedeltagere. Deltagere kan let deltage ved at vælge URL-adressen i e-mailinvitationen eller fra WebEx-webstedet.

Procedure

Trin 1 Log ind på WebEx-websted administrationsværktøj.

Trin 2 Naviger til **Konfiguration > Fælles webstedsindstillinger > Valgmuligheder > Sikkerhedsindstillinger**.

Trin 3 Under afsnittet Meeting Center, marker **Alle møder skal have en adgangskode**.

Trin 4 Under afsnittet Event Center, marker **Alle begivenheder skal have en adgangskode**.

Trin 5 Under afsnittet Training Center, marker **Alle sessioner skal have en adgangskode**.

Trin 6 For at kræve stærke adgangskoder, marker **Kræv stærke adgangskoder for møder**.

Trin 7 Marker og konfigurer de følgende felter:

- Kræv store og små bogstaver
- Minimum længde
- Minimum antal numerisk
- Minimum antal alfa
- Minimum antal specialtegn
- Tillad ikke, at nogle tegn gentages tre gange eller flere
- Tillad ikke brug af dynamisk websidetekst for mødeadgangskoder (webstedets navn, værtens navn, brugernavn, mødeemne)
- Tillad ikke mødeadgangskoder fra denne liste

Bed om mødeadgangskode, når der deltages fra telefon- eller videokonferencesystemer (WBS30)

Ud over at kræve adgangskoder når brugere deltager fra en mødeapplikation (for eksempel på Windows eller Mac), skal du også gennemtvinge krav om adgangskode for brugere, der deltager fra telefon- eller videokonferencesystemer. Denne funktion er tilgængelig på udgivelsen WBS30 og fremad. Når denne valgmulighed er valgt, genererer systemet automatisk en otte-cifret numerisk adgangskode for telefon- og videokonferencesystem mødedeltagere og tilføjer den til mødeinvitationen. Dette sikrer, at kun personer med en invitation kan deltage i mødet, når de bruger et telefon- eller videokonferencesystem.

Procedure

Trin 1 Log ind på WebEx-websted administrationsværktøj.

Trin 2 Naviger til **Konfiguration > Fælles webstedsindstillinger > Valgmuligheder > Sikkerhedsindstillinger**.

Trin 3 Under afsnittet Meeting Center, marker **Gennemtving krav om mødeadgangskode, når der deltages via telefon**.

Trin 4 Under afsnittet Event Center, marker **Gennemtving krav om begivenhedsadgangskode, når der deltages via telefon**.

Trin 5 Under afsnittet Training Center, marker **Gennemtving krav om adgangskode til undervisningssession, når der deltages via telefon**.

Trin 6 Under afsnittet Meeting Center, marker **Gennemtving krav om mødeadgangskode, når der deltages via videokonferencesystem**.

Kræv log ind, når der deltages i et møde, begivenhed eller undervisningssession (WBS30).

Vi anbefaler at du kræver, at alle brugere har en konto på dit WebEx-websted, hvis følsomme møder, begivenheder, eller undervisningssessioner skal afholdes der. Når den er aktiveret, bedes mødedeltagere, foruden værter, også om deres legitimation, når de forsøger at deltage i et møde, begivenhed eller undervisningssession.

For WBS30 og senere anbefaler vi, at du ud over at være logget ind på dit websted kræver, at mødedeltagere logger ind, når de ringer op fra en telefon. Dette forhindrer, at personer uden korrekt legitimation deltager i mødet eller undervisningssessionen.

Bemærk Deltagere, som deltager via Meeting Center- eller Training Center-applikationen skal bekræfte deres identitet, så de ikke bliver bedt om at godkende den igen, når de tilslutter til lyd. Således påvirker denne begrænsning kun brugere, som deltager via telefon.

Yderligere skal du overveje at begrænse videokonferencesystemer fra at ringe op til et møde, der kræver at mødedeltagere logger ind. Eftersom brugere ikke kan logge ind fra et videkonferencesystem, udgør tilladelse til deltagelse via konferencesystemer en risiko for, at uautoriserede brugere deltager i møder.

Procedure

Trin 1 Log ind på WebEx-websted administrationsværktøj.

Trin 2 Naviger til **Konfiguration > Fælles webstedsindstillinger > Valgmuligheder > Sikkerhedsindstillinger**.

Trin 3 For at kræve at alle brugere skal have en konto på dit WebEx-websted for at være vært for eller deltage i WebEx-møder, begivenheder eller undervisningssessioner, skal du markere **Kræv log ind før adgang til websted** (kun Meeting Center, Event Center, og Training Center).

Trin 4 For at kræve log ind når der deltages i et møde eller en undervisningssession via telefon, skal du markere **Kræv, at brugere har en konto, når du deltager via telefon** (kun Meeting Center og Training Center).

Når den er markeret og værter kræver log ind, skal mødedeltagere logge ind fra deres telefoner. Mødedeltagere skal have tilføjet et telefonnummer og en pinkode til deres profilindstillinger for at kunne gøre dette.

Trin 5 Når log ind er påkrævet for at deltage i et møde for at forhindre videokonferencesystemer i at deltage, skal du vælge **Blokeret** (kun Meeting Center).
Når blokeret er valgt, kan videokonferencesystem-brugere ikke starte eller deltage i møder, der kræver login. Dette omfatter personlige lokaler, når de er konfigureret til at kræve login.

Tillad ikke Deltag før værten

For alle møder skal du ikke aktivere muligheden for, at mødedeltagere kan deltage før værten, medmindre du har fuld forståelse for indvirkningen på sikkerheden og har brug for denne funktion.

Overvej at deaktivere valgmuligheden Deltag før værten for dit websted. Vi anbefaler at deaktivere disse valgmuligheder for angivne møder, da eksterne mødedeltagere kan have indflydelse på det planlagte møde til deres egne formål, uden værtens kendskab eller samtykke.

På samme måde skal du overveje ikke at tillade mødedeltagere at deltage i lyddelen før værten, hvis du tillader dem at deltage før værten. Hvis dit møde er angivet på dit websted eller ikke er beskyttet med adgangskode, kan uautoriserede brugere muligvis få adgang til og starte dyre opkald, uden værtens kendskab eller samtykke.

For personlige konferencemøder (PCN møder), anbefaler vi at deaktivere valgmuligheden deltag i lyd før værten. En vært vil først skulle indtaste WebEx adgangsnummer for lydbroen, og derefter indtaste værtsadgangskoden og værtspinkoden, før mødedeltagerne kan deltage i mødet.

Procedure

Trin 1 Log ind på WebEx-websted administrationsværktøj.

Trin 2 Naviger til **Konfiguration > Fælles webstedsindstillinger > Valgmuligheder > Sikkerhedsindstillinger**.

Trin 3 For at forhindre mødedeltagere i at deltage før værten, skal du fjerne markeringen af følgende bokse:

- **Tillad mødedeltagere eller paneldeltagere at deltage før værten** (MC, TC og EC)
- **Den første mødedeltager, der deltager, vil blive præsentationsvært** (kun MC)
- **Tillad mødedeltagere eller paneldeltagere at deltage i telekonference før værten** (MC, TC og EC)
- **Tillad mødedeltager at deltage i lyddelen af personlig konference før værten** (PCN møder)

Kontoadministration

Til administration af indstillinger for politik for alle brugere på dit websted, er følgende funktioner også tilgængelige i WebEx-webstedsadministration:

Værtskontoadministration

- Låse en konto ude, efter et antal forgæves forsøg på log ind, som du selv kan konfigurere

Oprettelse af konto

- Kræve, at nye brugere indtaster bogstaver eller tal fra et forvrænget billede, der vises på skærmen
- Kræve e-mailbekræftelse af nye konti
- Konfigurere regler for selvtilmelding af nye konti

Kontoadgangskoder

- Kræver specifikke regler for adgangskodeformat, længde og genbrug
- Mulighed for at ændre adgangskode med jævne mellemrum
- Forbyde adgangskoder, der let kan gættes (for eksempel ”adgangskode”)
- Indstil et minimum tidsinterval før ændring af adgangskode

Bedste praksis for værter

Som vært tager du den endelige beslutning med hensyn til sikkerhedsindstillinger for dit møde. Husk altid, at du kontrollerer næsten alle aspekter af mødet, inklusive hvor det begynder og slutter.

Følg bedste praksis for sikkerhed, når du planlægger mødet, og under og efter mødet, baseret på din virksomheds behov for at holde møder og oplysninger sikre.

Sådan bruges dit personlige lokale (WBS30)

Lås automatisk personligt lokale

Med WBS30 har du mulighed for at låse dit personlige lokale automatisk, efter dit møde starter. Dette kan gøres fra **Mit WebEx >Præferencer > Mit personlige lokale** på dit WebEx-websted. Vi anbefaler, at du låser dit lokale efter **0 minutter**. Dette er i bund og grund det samme som at låse dit lokale, så snart du deltager. Dette forhindrer alle mødedeltagere i din lobby fra at deltage automatisk i dit møde. I stedet vil du se en meddelelse i mødet, når mødedeltagere venter i lobbyen. Du kan derefter sortere og kun tillade autoriserede mødedeltagere at deltage i dit møde.

Bemærk Betragt URL-adressen for dit personlige lokale som en offentlig URL-adresse, og medmindre webstedsadministratoren har konfigureret personlige lokaler til kun at blive brugt af brugere, der er logget ind, kan enhver person vente på dig i din lobby. Kontroller altid navnene, før du accepterer mødedeltagere i dit lokale.

Personligt lokale-underretninger før et møde

Når brugere ankommer i lobbyen for dit personlige lokale, kan de sende dig en e-mailunderretning for at informere dig om, at de venter på, at et møde skal starte. Selv uautoriserede brugere, der opnår adgang til lobbyen for dit personlige lokale, kan sende underretninger.

Vi anbefaler, at du gennemser dine e-mailunderretninger, før du starter et møde, for at frasortere uautoriserede mødedeltagere. Hvis du ikke har låst dit personlige lokale automatisk ved nul minutter, vil alle mødedeltagere, der venter i lobbyen til dit personlige lokale, få adgang til mødet, når du tilgår det. Gennemse deltagerlisten, og udvis alle uautoriserede mødedeltagere.

Hvis du har låst dit personlige lokale automatisk og ser for mange e-mailunderretninger fra uautoriserede mødedeltagere, skal du overveje at slå disse underretninger fra. Gå til **Mit WebEx > Præferencer**, og sluk

for underretninger fra dit personlige lokale ved at fjerne fluebenet ved **Underret mig via e-mail, når nogen kommer ind i lobbyen til mit personlige lokale, under mit fravær**.

Personligt lokale-underretninger under et møde

Hvis du låser dit personlige lokale, kan du frasortere alle personer, der venter i din lobby. Efter du tilgår dit møde, underrettes du, når nye personer kommer ind i lobbyen, og du kan vælge, om du vil acceptere personen eller ej. Når flere mødedeltagere venter på dig i lobbyen til dit personlige lokale, kan du gennemse listen over navne, og enten give enkeltpersoner eller alle adgang til mødet.

Planlægning af mødet

Planlægning af ikke-angivne møder

For at øge mødets databeskyttelsesindstillinger, kan værter vælge ikke at angive mødet i mødekalenderen. For at gøre dette fjernes fluebenet fra denne valgmulighed for at hjælpe med at forebygge uautoriseret adgang til mødet og skjule oplysninger om mødet, såsom værten, emnet og starttidspunktet.

- Et ikke angivet møde vises ikke i mødekalenderen på siden Søg i møder eller på din side Mine møder.
- For at deltage i et ikke angivet møde skal mødedeltagerne opgive et unikt mødenummer.
- Ikke-angivne møder kræver, at værten informerer mødedeltagerne, enten ved at sende dem et link i en e-mailinvitation, eller værter kan indtaste mødenummeret ved at bruge siden Deltag i møder.

Bemærk Når et mødes angives, afsløres mødets titel og mødeoplysninger for offentligheden. Hvis et møde ikke er beskyttet med adgangskode, kan alle deltage.

Tip Vælg et sikkerhedsniveau baseret på mødets formål. Hvis du for eksempel planlægger et møde for at drøfte din virksomheds skovtur, behøver du sandsynligvis kun at opsætte en adgangskode for mødet. På den anden side, hvis du planlægger et møde, hvor du vil drøfte følsomme finansielle data, ønsker du muligvis ikke at angive mødet i mødekalenderen. Du kan også vælge at begrænse adgangen til mødet, når alle mødedeltagere deltager.

Vælg mødeemnet omhyggeligt

Et angivet møde eller en fremsendt e-mailinvitation kan, som minimum, afsløre mødetitler for et utilsigtet publikum. Mødetitler kan utilsigtet afsløre private oplysninger, så sørg for, at titler skrives med omtanke for at mindske afsløring af følsomme data, såsom virksomhedsnavne eller begivenheder.

Sikkert møde med stærk adgangskode

Brug af stærke adgangskoder til hver session er det vigtigste trin, som du kan tage for at beskytte dit møde. Selvom det er ualmindeligt, kan administratorer vælge at tillade oprettelsen af møder uden adgangskoder. I de fleste tilfælde anbefales det på det varmeste, at beskytte alle møder med en stærk adgangskode.

Det mest effektive skridt til at beskytte sikkerheden af dit møde er at oprette en meget stærk og usædvanlig adgangskode (stærk adgangskode). En stærk adgangskode bør indeholde en blanding af store og små bogstaver,

numre og specialtegn (for eksempel, $Tu0psrOx!). Adgangskoder beskytter mod uautoriseret deltagelse, fordi det kun er brugere med adgang til adgangskoden, der kan deltage i mødet.

Genbrug ikke adgangskoder til møder. Planlægning af møder med de samme adgangskoder svækker mødets beskyttelse betydeligt.

Bemærk Tilføjelse af adgangskoder til dine møder påvirker ikke mødedeltagelsesoplevelsen for autoriserede mødedeltagere. Deltagere kan let deltage i et møde ved at klikke på URL-adressen i mødeinvitationen sendt via e-mail, ved at bruge WebEx-mobilapplikationen eller andre kanaler, som Cisco Jabber.

Udeluk mødeadgangskoder fra invitationer

Hvis du inviterer mødedeltagere til et møde, vises mødeadgangskoden ikke i de e-mailinvitationer, mødedeltagerne modtager. Du skal levere adgangskoden til mødedeltagere på anden måde, såsom via telefonen.

For meget følsomme møder, skal mødeadgangskoden ikke inkluderes i e-mailinvitationen. Dette forhindrer uautoriseret adgang til mødeoplysninger, hvis e-mailinvitationen videresendes til en utilsigtet modtager.

Kræv, at mødedeltagere har en konto på dit websted

Når denne indstilling er aktiveret, skal alle mødedeltagere have en brugerkonto på dit websted for at kunne deltage i mødet. For oplysninger om, hvordan mødedeltagere kan få en brugerkonto, kan du forhøre dig med din administrator.

I Meeting Center avanceret planlægningsprogram, skal du markere **Kræv, at mødedeltagere har en konto på dette websted for at kunne deltage i dette møde.**

Brug indgangs- eller udgangstone eller annoncer navnefunktion

Brug af denne funktion forhindrer andre i at deltage i lyddelen af dit møde, uden at du ved det.

Denne funktion er aktiveret som standard for Meeting Center og Training Center. For at tilpasse indstillingerne, vælg **Lydkonferenceindstillinger > Indgangs- og udgangstone**.

Begræns tilgængelige funktioner

Begræns de tilgængelige funktioner, såsom chat og lyd, hvis du tillader mødedeltagere at deltage i møder før værten.

Anmod om, at invitationer ikke videresendes

Anmod dine besøgende om ikke at videresende invitationen, især for fortrolige møder.

Udpeg en alternativ vært

Udpeg en alternativ vært til at starte og kontrollere mødet. Dette holder møder mere sikre ved at udelukke muligheden for, at værtsrollen tildeles til en uventet eller uautoriseret mødedeltager, hvis du utilsigtet mister forbindelsen til mødet.

Bemærk Når mødedeltagere inviteres til et planlagt møde, kan du udpege en eller flere mødedeltagere som alternative værter for mødet. En alternativ vært kan starte mødet og fungere som vært. Derfor skal en alternativ vært have en brugerkonto på dit Meeting Center-websted.

Under mødet

Begræns adgangen til mødet

Lås mødet, når alle mødedeltagere deltager i mødet. Dette vil forhindre andre mødedeltagere i at deltage. Værter kan når som helst låse/låse op for mødet under en igangværende session. For at låse et møde, **Vælg møde > Begræns adgang**.

Tip Denne indstilling forhindrer alle i at oprette forbindelse til mødet, herunder deltagere der er blevet inviteret til mødet, men endnu ikke har oprettet forbindelse til det. For at låse et møde op, vælg **Møde > Genopret adgang**.

Bekræft identiteten af alle brugere i et opkald

Det er en sikker fremgangsmåde at redegøre for hver mødedeltager ved at bruge et rolleopkald. Bed brugere om at tænde for deres video, eller opgive deres navn for at bekræfte deres identitet.

Bemærk

- For at deltage i et møde via en telefon, skal en gæst blot kende et gyldigt WebEx-opkaldsnummer samt det ni-cifrede møde-id. Mødeadgangskoder forhindrer ikke mødedeltagere i at deltage fra lydkonferencedelen af WebEx.
- Hvis mødedeltagere uden en konto har tilladelse til at deltage i mødet, så kan uautoriserede brugere identificere sig selv med ethvert navn i dit møde.

Fjern en deltager fra mødet

Deltagere kan blive udvist når som helst under et møde.

Vælg navnet på den deltager, som du ønsker at fjerne, og vælg derefter **Deltager > Udvis**.

Del applikation, ikke skærm

Brug **Del > Applikation** i stedet for **Del > Skærm** til at dele specifikke applikationer og forhindre tilfældig afsløring af følsomme oplysninger på din skærm.

Efter mødet

Opsætte adgangskoder for optagelser

Den bedste måde at forhindre uautoriseret adgang til optagelser, er ikke at lave optagelser.

Hvis optagelser skal oprettes, kan du redigere mødeoptagelser og tilføje adgangskoder, før de deles, for at holde dem sikre. Optagelser beskyttet med adgangskoder kræver, at modtagere har adgangskoden, for at de kan se dem.

Slette optagelser

Slet optagelser, efter de ikke længere er relevante.

Personlige konferencer for værter

I afsnittet Mit WebEx-præferencer af dit WebEx-websted, skal du oprette en stærk lyd-pinkode og beskytte den.

Din pinkode er det sidste niveau af beskyttelse for forhindring af uautoriseret adgang til din personlige konferencekonto. Hvis en person opnår uautoriseret adgang til værtsadgangskoden til et personligt konferencemøde (PCN-møde), kan konferencen ikke startes uden lyd-pinkoden. Beskyt din lyd-pinkode, og del den ikke med andre.