Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Misure per un impiego sicuro delle soluzioni di audio e videoconferenza

Nell'ambito della crisi del coronavirus, in Svizzera e nel mondo intero la popolazione sta vivendo una situazione che ha completamente sconvolto il modo di essere abituale. Da un giorno all'altro non è più stato possibile incontrare parenti e conoscenti né scambiare informazioni con i colleghi o tenere riunioni in ufficio. Per rimanere in contatto, cittadini e imprese sono quindi stati costretti a impiegare rapidamente soluzioni di audio e videoconferenza. La fretta di spostare nel mondo virtuale riunioni di lavoro, comunicazioni di bambini o nonni e feste non deve però farci dimenticare l'importanza di garantire la sicurezza delle informazioni e di evitare violazioni della privacy durante le videoconferenze. Questa scheda informativa si rivolge a tutti i gruppi di utenti, sia in ambito privato che professionale.

L'IFPDT raccomanda pertanto, come primo passo, misure immediate per garantire che la soluzione attualmente in uso possa essere utilizzata nel modo più sicuro possibile, quantomeno temporaneamente durante una situazione straordinaria. A posteriori o durante l'uso, l'impiego di questi servizi e prodotti deve essere sottoposto a una nuova valutazione nell'ambito di un'analisi dei rischi conforme ai criteri dettati dalla normativa in materia di protezione dei dati; se del caso va valutato e impiegato un prodotto maggiormente adatto alle esigenze. A tale scopo, la presente scheda informativa contiene i punti da osservare durante la preparazione e la successiva introduzione di una soluzione di audio e videoconferenza conforme alle norme sulla protezione dei dati.

Misure per l'impiego di una soluzione di audio e videoconferenza

Non comunicare pubblicamente il numero della riunione (NR)
Per NR si intende il numero univoco attribuito a una determinata riunione. Anche se potrebbe apparire una soluzione pratica, i NR non devono essere pubblicati in Internet né sulle reti sociali; in questo caso infatti, usando tali numeri, potrebbero connettersi anche persone indesiderate.

Utilizzare NR a impiego unico e bloccare le riunioni
Non utilizzate lo stesso NR per conversazioni diverse e badate di bloccare la riunione in corso non appena si sono connessi tutti i partecipanti. In tal modo chi deve partecipare a una riunione successiva non ha la possibilità di ascoltare quella in corso.

Organizzare per quanto possibile riunioni protette da password
Impostando una password si garantisce che si connettano soltanto le persone autorizzate. Si raccomanda, se possibile, di non comunicare NR e password nella stessa e-mail.

Prestare sempre attenzione ai partecipanti
Verificate periodicamente chi partecipa alle riunioni. Se appaiono persone sconosciute, intimate loro di confermare la loro identità.

Avvisare sempre se è prevista una registrazione della riunione
I partecipanti devono essere previamente ed esplicitamente informati in caso di registrazione della riunione (suono, video, ecc.). Devono avere la possibilità, senza subire pregiudizi, di pronunciarsi contro la registrazione ed eventualmente di lasciare il meeting.

Attenzione al phishing
Se ricevete un link per una videoconferenza tramite e-mail o reti sociali, si raccomanda prima della connessione di contattare il mittente al fine di verificarne l'identità. Non aprite mai link e allegati provenienti da mittenti sconosciuti o sospetti.

Coprite la telecamera, se non utilizzata, e controllate l'ambiente inquadrato
Si raccomanda di coprire la telecamera, se non utilizzata, per impedire di essere osservati a vostra insaputa. Prima di una videoconferenza, verificate le informazioni visibili nell'inquadratura (p. es. iscrizioni su una lavagna o documenti confidenziali). Potete anche utilizzare p. es. strumenti video che permettono di rendere sfuocato lo sfondo.

Presentazioni sullo schermo / condivisione dello schermo
Presentate unicamente informazioni rilevanti per la riunione. Chiudete quanto non è necessario mostrare. Se possibile, presentate soltanto il programma in questione e non il desktop. È possibile impostare un desktop alternativo, privo di documenti o link.

Controllate le direttive in materia di protezione dei dati dell'offerente
Alcuni offerenti trasmettono dati personali a terzi o mettono a disposizione di terzi metadati come la durata e l'ubicazione della riunione nonché l'identificazione e il numero dei partecipanti. Se l'offerente della vostra attuale soluzione di audio e video conferenza condivide le vostre informazioni personali con terzi, deve renderlo noto nelle sue direttive in materia di protezione dei dati. Vi raccomandiamo pertanto di consultare tali direttive e, se necessario, di avvalervi del vostro diritto all'informazione.

Osservate i seguenti punti per la valutazione, la pianificazione e la preparazione di una soluzione di audio e videoconferenza:

Informarsi sulla reputazione dell'offerente
Cercate in Internet indizi sulla soddisfazione degli utenti, su funzioni interessanti o su

notori problemi di sicurezza. In caso di dubbi, scegliete un offerente già affermato sul mercato.

Controllare le direttive in materia di protezione dei dati dell'offerente
Anche in questa fase, verificate le direttive in materia di protezione dei dati dell'offerente, in particolare per quanto concerne la trasmissione di dati personali. Nel caso di una soluzione di videoconferenza che ha sede al di fuori della Svizzera o dell'UE, oppure se al momento dell'utilizzo di tale soluzione i dati sono trasferiti in cosiddetti «Paesi terzi», occorre chiarire se il Paese o l'offerente in questione offre un livello di protezione adeguato (certificazioni di protezione della sfera privata nel caso delle aziende statunitensi) o se il fornitore fornisce comunque garanzie adeguate (conclusione di clausole standard di protezione dei dati).

Gestione dei metadati da parte dell'offerente
In linea di principio, dovete assicurarvi che l'offerente non raccolga metadati, non li elabori per propri scopi e non li trasmetta a terzi. Oltre alla durata, al luogo, all'identificazione e al numero dei partecipanti alla riunione come già menzionato sopra, i metadati includono anche gli indirizzi e-mail di altri contatti della rubrica nonché il modello di cellulare e il browser utilizzato.

Cifratura dei dati
I dati devono essere protetti nello stato in cui si trovano e anche durante la trasmissione. Requisito minimo: trasmissione cifrata; requisito ottimale: cifratura end-to-end.

Sicurezza fisica
Controllate dove si trovano i centri dati dell'offerente e verificate se soddisfano i vostri requisiti di sicurezza. Soprattutto per le soluzioni con archiviazione centralizzata dei dati, assicuratevi che tutti i centri di calcolo siano sicuri, controllati regolarmente e protetti da intrusioni fisiche 24 ore su 24. L'ubicazione dei server in Svizzera o nell'UE rappresenta un vantaggio.

Elementi di sicurezza e di controllo
Alcuni servizi di videoconferenza offrono funzioni avanzate per individuare i ripetuti errori di login. Questo può aiutare a rilevare e fermare i tentativi di intrusione, come ad esempio la digitazione ripetuta di NR. L'arrivo e la partenza di un partecipante devono essere resi riconoscibili agli altri partecipanti attraverso segnalazioni diverse. È auspicabile avere la possibilità di constatare individualmente il numero di partecipanti o di identificarli tutti. Le funzioni di delega consentono di delegare il monitoraggio e il controllo della riunione nonché di moderare le riunioni.

Modificare le impostazioni in materia di protezione dei dati
Stabilite come standard la protezione dei dati all'interno dello strumento per evitare l'eventuale trattamento non autorizzato dei dati. Fornite agli utenti all'interno della vostra organizzazione istruzioni su come implementare impostazioni rispettose della protezione dei dati.

Punti importanti da considerare quando si introduce una soluzione di audio e video conferenza:

È necessaria la registrazione rispettivamente l'iscrizione?
L'uso senza previa registrazione rispettivamente iscrizione può essere pratico, soprattutto per le soluzioni basate su browser senza installazione di programmi. L'identificazione dei partecipanti è in tal caso tuttavia molto limitata e una simile soluzione non dovrebbe pertanto essere utilizzata per la comunicazione interna dell'azienda.

Impedire l'accesso indesiderato alle app
Molte applicazioni – soprattutto su dispositivi mobili – accedono a dati personali senza che questo sia assolutamente necessario. In primo luogo occorre scegliere impostazioni di protezione dei dati volte a evitare un'eventuale elaborazione non autorizzata dei dati. In secondo luogo, le autorizzazioni delle app devono essere configurate in dettaglio (limitazione dei diritti alle funzioni necessarie al funzionamento della soluzione), documentate e monitorate.

Regolamento di utilizzazione all'interno dell'azienda
Se non viene emanato un regolamento di utilizzazione, vi è incertezza circa il diritto all'uso privato della soluzione di audio e videoconferenza. Senza limitazioni o divieti espliciti, il dipendente può presumere che l'uso privato sia consentito, nel rispetto della proporzionalità, e che non venga effettuata alcuna sorveglianza.

Informazioni sulla sorveglianza e la registrazione all'interno dell'azienda
A differenza del regolamento di utilizzazione, la cui emanazione non è obbligatoria, il datore di lavoro ha l'obbligo di comunicare in modo trasparente qualsiasi attività di sorveglianza e di registrazione all'interno della soluzione di audio e videoconferenza, in quanto potrebbe rappresentare un'intrusione nella sfera privata del dipendente (principio di buona fede, art. 4 cpv. 2 LPD).

Berna, aprile 2020

Per ulteriori informazioni

Lista di prodotti per la collaborazione digitale (Digitale Zusammenarbeit), aprile 2020, Incaricato della protezione dei dati del Cantone di Zurigo