ZOOM UND DIE DATENSCHUTZFRAGE

20.04.2020

IG Metall
Bildungszentrum Sprockhövel

ZOOM UND DIE DATENSCHUTZFRAGE

Probleme und Antworten

- Warum Zoom?
- Die Sicherheitslücke
- Der Datenhandel
- Das Facebookleck
- Der Passworthandel
- Das Eye Tracking
- Das Zoom Bombing
- Die Unternehmensreaktionen
- DSGVO
- Tipps zur sicheren Kommunikation
- Neue Zoom Features
- Wie geht es weiter?
- Sonstiges

WARUM ZOOM?

Pro

- Es funktioniert einwandfrei, auch mit vielen Personen
- Die Nutzung ist intuitiv und leicht zu erlernen

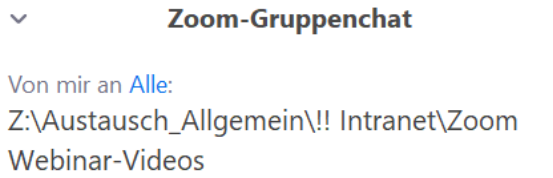
Kontra

- Es gibt Datenschutzbedenken
- In den letzten Wochen hat Zoom viel schlechte Presse bekommen
- Einige Unternehmen schränken die Nutzung von Zoom ein

DIE SICHERHEITSLÜCKE

Das Problem

- Links aus dem Windowsverzeichnis, die in den Zoom-Chat geschrieben wurden, haben versteckt Benutzername und Passwort von Windows übergeben



Die Antwort

- Zoom hat Stunden nach Bekanntwerden dieser Schwachstelle ein Update seines Programms bereitgestellt
- Dafür muss unter https://zoom.us/download die aktuelle Version des Client herunterladen werden
- Wenn Zoom bisher nur über euren Browser benutzt wurde, gibt es kein Problem
- Sicherheitshalber sollten trotzdem keine Informationen zur internen Verwendung oder Passwörter in den Chat geschrieben werden

DER DATENHANDEL

Das Problem

- Daten, die durch die Nutzung von Zoom entstehen, werden an Dritte weitergereicht oder verkauft

Die Antwort

- Die Daten sind nicht personenbezogen, sondern anonymisiert
- Es werden nur technische Daten weitergegeben: Zeitzone, die Geräteart (Smartphone oder Computer), Betriebssystem (z.B. Windows Version), Provider, Bildschirmgröße, Prozessorgeschwindigkeit, Größe der Festplatten, IP-Adresse (anonymisiert), MAC-Adresse, Kameratyp, Mikrofon oder Lautsprecher
- Mithilfe von Add-ons wie Lightbeam kann das sichtbar gemacht werden
- Das ist eine Herangehensweise, die im Internet üblich ist und die unter Datenschutzgesichtspunkten kein Problem darstellt

DAS FACEBOOKLECK

Das Problem

- Zoom hat bis vor kurzem anonymisierte Daten an Facebook weitergegeben
- Hauptsächlich bezog sich das auf Clients, die auf Apple-Computern heruntergeladen wurden

Die Antwort

- Das Problem liegt hier in Teilen bei Facebook, die sogenannte „Schattenprofile“ anlegen
- Diese Datenweitergabe wurde mit einem Update der Software beendet

DER PASSWORTHANDEL

Das Problem

- Zugangsdaten von Zoom werden in Foren des Darknets gehandelt
- Es ist offen, ob es sich um eine Sicherheitslücke bei Zoom handelt
- Es spricht vieles dafür, dass hier eher unsichere Passwörter durch das automatisierte Durchprobieren von Login-Daten geknackt wurden. Deshalb liegen die Passwörter auch im Klartext vor.

Die Antwort

- Das Passwort bei Zoom ändern
- Allgemein sichere und verschiedene Passwörter benutzen (z.B. nicht 12345678, oder Vorname+Geburtsjahr)

DAS EYE TRACKING

Das Problem

- Das sogenannte Aufmerksamkeitstracking war bei Zoom Meetings und Webinaren möglich
- Es handelt sich hierbei um eine Funktion, die von einem Zoom-Administrator aktiv eingeschaltet werden musste
- Somit konnte nachvollzogen werden, ob TN an einem Meeting ihren Blick tatsächlich auf das Fenster richteten

Die Antwort

- Bei der IG Metall war das Tracking von Anfang an immer ausgestellt
- Diese Funktion ist mittlerweile von Zoom entfernt worden

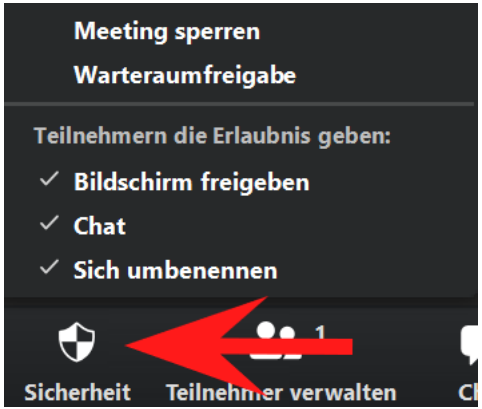
DAS ZOOM BOMBING

Das Problem

- Meetings bei Zoom wurden von Leuten infiltriert, die sich den Meeting-Link besorgt haben
- Um einer Zoom-Konferenz beizutreten, werden Internetadressen von Zoom erzeugt. Jede*r mit dem Link kann diesem Meeting beitreten.

Die Antwort

- Das kann verhindert werden, indem Meetings oder Webinare mit **Warteraum** eingerichtet werden. Dann muss jede*r beim Meetingbeitritt vom Host bestätigt werden
- Der Warteraum kann bei der Meeting-Planung unter erweiterte Einstellungen ausgewählt oder im Menu aktiviert werden
- Des Weiteren kann das Meeting gesperrt werden, wenn alle angemeldeten TN anwesend sind



DIE UNTERNEHMENSREAKTIONEN

Das Problem

- Verschiedene Unternehmen blockieren oder schränken die Nutzung von Zoom ein
- Damit reagieren sie auf vermeintliche und vorhandene Sicherheitslücken bei Zoom
- Eine wichtige Motivation ist dabei auch der Schutz der eigenen unternehmensspezifischen Videokonferenz-Anwendungen

Die Antwort

- Genaues Prüfen der Unternehmenspolitiken (im Zweifelsfall die entsprechenden E-Mails anfordern)
- Die meisten verbieten den Download des Zoom-Client. Die browserbasierte Nutzung wird dabei nicht eingeschränkt
- Die private Nutzung von Zoom wird dabei nicht beeinträchtigt
- Wenn man mit Kolleg*innen aus den entsprechenden UN kommunizieren möchte, kann man dann entsprechend auf deren Software umsteigen

DSGVO

Das Problem

- Die Datenschutzvereinbarung von Zoom weist einige Unklarheiten und Ungenauigkeiten auf
- Der Serverstandort war in Amerika.

Die Antwort

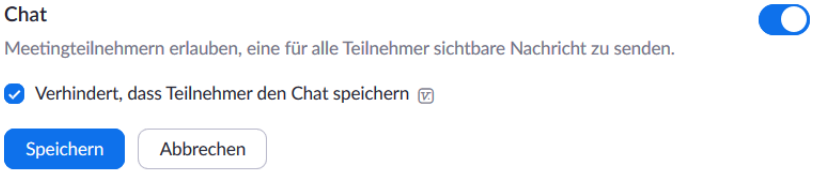
- Die IG Metall hat eine eigene Datennutzungsvereinbarung mit Zoom getroffen, die weitreichender ist als die allgemeine Datenschutzvereinbarung.
- Die Zuständigkeit der DSGVO klärt sich zwar nicht durch den Serverstandort. Denn die DSGVO ist zuständig für personenbezogene Daten, die im Raum der EU erhoben werden. D. h. die DSGVO war bereits zuständig als der Serverstandort noch in den USA war. Aber die Daten sind jetzt hier auf einem europäischen Server vor dem Zugriff durch amerikanische Behörden sicherer.

TIPPS ZUR SICHEREN KOMMUNIKATION

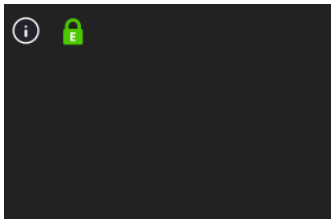
- Zoom Videokonferenzen sind über einen Link im Internet erreichbar. Kommunikation sollte dementsprechend geschützt werden
- Es gibt einige Einstellungen, die beachtet werden sollten. Alle Einstellungen finden sich unter https://zoom.us/profile/setting :
  - Einbetten des Kennworts in den Meeting-Link für die Teilnahme mit einem Klick ausstellen. Damit muss ein, am besten separat, verschicktes Passwort eingegeben werden.
  - Die Dateiübertragung ausstellen, um zu verhindern, dass sensible Daten per Zoom verschickt werden
  - Entfernten Teilnehmern den erneuten Beitritt erlauben, deaktivieren
  - Keine Zugangsdaten und interne Links per Zoom Chat posten

NEUE ZOOM FEATURES

- Wie in den einzelnen Folien schon angesprochen, hat Zoom in den letzten Wochen viele zusätzliche Sicherheitsfeatures eingebaut
  - Über den Button „Sicherheit“ kann sowohl der Warteraum aktiviert als auch der weitere Zutritt zu Meetings gesperrt werden



- Das Speichern der Chatinhalte durch TN kann in den Einstellungen verhindert werden
- Die Meeting-ID, die vorher in der Ecke links oben sichtbar war, ist jetzt verborgen



WIE GEHT'S WEITER?

- Als Videokonferenz-Anwendung ist Zoom aus guten Gründen Marktführer. Diese Qualität, mit vielen Personen zugänglich zu kommunizieren, ist mit keinem anderen Tool zu erreichen
- Zoom hat bei allen wesentlichen Kritikpunkten nachgesteuert
- Die Nutzung von Zoom ist mit einem aktualisierten Client oder über den Browser, aus datenschutzrechtlicher Sicht, nicht bedenklich
- Datenschutz, IT und der GBR sind bei der Frage der Zoom-Nutzung eingebunden
- **Aber:** Wenn weitere Unternehmen die Verwendung von Zoom einschränken, wird es notwendig sein, Alternativen wie WebEx Cisco in Betracht zu ziehen
- Von unserer Seite werden wir die Gesamtsituation (Medien, Datenschutz, Unternehmensreaktionen, Mitgliederrückmeldungen) weiterhin aufmerksam Beobachtung

SONSTIGES

Kontakt bei weiteren Fragen

- Sok-Yong Lee (sok-yong.lee@igmetall.de | 0160-5331253)
- Guido Brombach (guido.brombach@igmetall.de | 0175-5808753)
- Gesine Walnsch (gesine.walnsch@igmetall.de | 0160-5331714)
- Stefan Marx (stefan.marx@igmetall.de | 0160-90768071)

Interessante Links

- https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook
- https://www.heise.de/security/meldung/Zugangsdaten-fuer-hunderttausende-Zoom-Accounts-zum-Kauf-im-Darknet-entdeckt-4701838.html
- https://www.heise.de/mac-and-i/meldung/Zoom-auf-dem-Mac-Sicherheitsluecken-erlauben-Lauschen-und-Root-4695129.html
- https://gist.github.com/GEWStudisFAU/af7583739e06ee14848d5753b5947b0e?fbclid=IwAR1-7DrUO7dTtZri7KQkDvR80ZCxBiA9-B_blHV-xVqhWqnLh_O5YDbhVuM