Wir reichen im Folgenden unsere Serie zu Sicherheitslücken in den Webex-Instanzen der Bundeswehr, der Bundesregierung sowie deutscher Behörden ein. Kurz nachdem so genannten Taurus-Skandal, bei dem der russische Geheimdienst ein internes Meeting von führenden Bundeswehr-Generälen veröffentlicht hatte, fanden wir massive Sicherheitslücken in Webex. Unter anderem standen teils mit Geheimhaltungsstufe versehene Informationen von mehr als hunderttausend Video-Meetings der Bundeswehr im Netz. Auch den persönlichen Meetingraum unter anderem des deutschen Bundeskanzlers konnten wir besuchen - und im weiteren Verlauf die diverser Parteien und Behörden.

Nachdem weder Cisco noch die deutschen Behörden die dahinterliegende Webex-Sicherheitslücke ernst nahmen, gelang es unserer Autorin im zweiten Teil der Serie, sich teils unbemerkt in Meetings des SPD-Bundesvorstands einzuwählen. Im dritten Teil der Serie - nachdem die Verantwortlichen die Lücke weiterhin nicht ernst nahmen - konnten wir uns in interne Meetings von Behörden einwählen. Auch hunderttausende Meetings der niederländischen Regierung waren von dem Leak betroffen.

Die Serie zeigt, wie sehr Behörden und Politik selbst in Zeiten des Cyberwar IT-Sicherheit vernachlässigen und wie viele vertrauliche Meetings eine Journalistin uneingeladen besuchen muss, bis sich etwas bewegt.

Teil 1:

Jeder konnte sie finden

Recherchen von ZEIT ONLINE offenbaren eine Sicherheitslücke bei der Bundeswehr und der Bundesregierung: Wer wann zu einem Videocall einlud, ließ sich öffentlich einsehen.

Von Eva Wolfangel, Zeit Online 4.4.2024

Wer wissen will, was die Bundeswehr intern beschäftigt, konnte dies monatelang frei zugänglich im Internet nachlesen: Nach Recherchen von ZEIT ONLINE standen bis Freitagabend mehrere Tausend Links zu Videomeetings mit internen Informationen offen im Netz – darunter befanden sich viele als vertraulich eingestufte Treffen. Auch ver-

gangene Meetings wurden offenbar nicht gelöscht. Die Bundeswehr, die erst durch Nachfragen für diesen Artikel auf die Sicherheitslücke aufmerksam wurde, hat ihr Videokonferenzsystem nun vom Internet getrennt. Ob aufgrund der aktuellen Lücke vertrauliche Informationen an Unbefugte abgeflossen sind, konnte die Bundeswehr nicht ausschließen.

Die Schwachstelle hat ein Team aus IT-Sicherheitsexpertinnen und -experten des Vereins Netzbegrünung entdeckt. ZEIT ONLINE hat sie durch eigene Stichproben verifiziert.

Der Vorfall betrifft die eigene Webex-Instanz der Bundeswehr, die eigentlich als besonders sicher gilt und über die auch Gespräche mit Geheimhaltungsstufen geführt werden. Damit hält die Truppe nach eigenen Angaben 45.000 Meetings pro Monat ab, also im Schnitt mehr als 1.000 am Tag. Webex ist ein Videokonferenztool des US-Konzerns Cisco, es ist funktionsmäßig vergleichbar mit Zoom oder Teams. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Webex 2019 für den Einsatz von Behörden zugelassen und es entsprechend seinem Kriterienkatalog für Cloud-Computing zertifiziert.

Generell gibt es zwei Möglichkeiten, die Software zu nutzen: Unternehmen und Behörden können die öffentliche Cloud-Variante verwenden, dann werden die Videokonferenzen auf Servern von Cisco gehostet. Oder sie können eine private On-Premise-Variante wählen, dann setzen sie ihre eigene Webex-Instanz auf. Das bedeutet, dass die Informationen auf eigenen Servern liegen, was besonders für Behörden wichtig ist, damit zum Beispiel die Daten von Bürgerinnen und Bürgern nicht in anderen Ländern gespeichert werden, sondern hierzulande. Es ist aber natürlich auch in Fragen nationaler Sicherheit von Relevanz.

Die aktuelle Recherche offenbart mindestens zwei Schwachstellen der On-Premise-Lösung von Webex, die auch die Bundeswehr nutzt: Die Links zu Videomeetings der Bundeswehr ließen sich durch Hoch- oder Herunterzählen erraten. In der IT-Sicherheitsbranche wird empfohlen, Nummern in Webadressen randomisiert, also zufällig, zu verteilen, damit man sich nicht einfach von einem Meeting zum nächsten zählen kann. Das war bei Webex aber offenbar nicht der Fall.

So konnte man die Titel, den Zeitpunkt und die einladende Person wichtiger Meetings einsehen. Review Meilensteinplan Taurus und Finalisierung lautete etwa der Titel eines Webex-Meetings, das am 25. April morgens stattfand und sich offenbar mit dem Marschflugkörper Taurus beschäftigte. Ende Mai soll eine Verschlusssache diskutiert werden zum Thema "Digitales Gefechtsfeld" ("Verschlusssache – nur für den Dienstgebrauch") – und Ende April wurde offenbar einen ganzen Tag lang über den Lenkflugkörper Meteor gesprochen. Das älteste Meeting von insgesamt mehr als 6.000, die im Zuge dieser Recherche gefunden wurden, war eine Besprechung vom 2. November 2023. Allerdings waren noch deutlich mehr als die genannten 6.000 Meetings online.

Persönlicher Meetingraum von Offizier Ingo Gerhartz auffindbar

Die zweite Schwachstelle: Auch persönliche Meetingräume waren leicht erratbar und nicht einmal durch ein Passwort oder ähnliche Sicherheitsmaßnahmen geschützt. Meetingräume sind Videokonferenzen, deren Links permanent bestehen und die häufig jederzeit abrufbar sind. Das heißt nicht, dass sie verwendet werden, aber sie sind eine einfache Möglichkeit, schnell ein digitales Meeting zu führen. Bevor die Bundeswehr die Möglichkeit sperrte, konnte man private Meetingräume mit einem Klick betreten, wie ein Versuch von ZEIT ONLINE zeigte. In diesem Fall war gerade niemand da.

Zudem waren auch die zugehörigen URLs besonders einfach zu kombinieren, weil sie alle nach dem gleichen Prinzip aufgebaut waren und direkt zu den persönlichen Räumen führten – wie zu jenem von Ingo Gerhartz, dem Chef der deutschen Luftwaffe, dessen Meetingraum ZEIT ONLINE ebenfalls im Zuge der Recherche fand. Mit simplen Zugangsdaten wie "Test" als Name konnte man dem Raum beitreten.

Gerhartz war ein Teilnehmer des von russischen Medien geleakten Taurus-Gesprächs. In einer Telegram-Gruppe hatte die Chefredakteurin des russischen Staatssenders RT Anfang März eine Audioaufnahme einer Webex-Konferenz von ranghohen Bundeswehroffizieren veröffentlicht. Diese diskutierten darin über den Einsatz von Taurus-Raketen – und erörterten unter anderem die Frage, ob die Marschflugkörper die von Russland gebaute Brücke zur völkerrechtswidrig annektierten ukrainischen Halbinsel Krim zerstören könnten.

Haben Webex-Sicherheitslücken zur Taurus-Affäre geführt?

Die aktuellen Vorfälle führen zur Frage, ob möglicherweise doch Sicherheitslücken in Webex zum Abhörskandal geführt haben könnten. Bislang hatte das Verteidigungsministerium eine nicht geschützte Telefonverbindung eines Bundeswehrgenerals in Singapur als Ursache angegeben. Demnach war das abgehörte Meeting eher ein Zufallsfund einer groß angelegten Überwachungsaktion von Spionen angesichts einer Messe, die zum gleichen Zeitpunkt in Singapur stattfand.

Wäre es theoretisch möglich, dass sich Spione unbemerkt in Webex-Meetings deutscher Behörden einschleichen, indem sie diese im Netz finden und das Passwort erraten? Es gab jedenfalls einmal eine alte Sicherheitslücke in Webex, mit der das möglich war: Wie IBM Ende 2020 entdeckte, konnten damals sogenannte Ghost-User Webex-Meetings beitreten. Die Eindringlinge blieben also unsichtbar.

Unsicherheit mit System?

Cisco verweist auf Nachfrage von ZEIT ONLINE auf das Statement des Verteidigungsministeriums im Taurus-Fall. Zudem sei die Sicherheitslücke von 2020 geschlossen, die unbemerkte Besuche ermöglicht hatte.

Auch die Bundeswehr schreibt, dass es "nach den derzeit hier vorliegenden Erkenntnissen" zum Taurus-Leak "keine inhaltlichen Zusammenhänge" gebe. Auf die Frage, ob man ausschließen könne, dass unter Ausnutzung der aktuellen Sicherheitslücken Informationen an Unbefugte gelangten, antwortet die Bundeswehr nur ausweichend, dass nur auf Metadaten, aber nicht auf Gesprächsinhalte hätte zugegriffen werden können. "Die Schwachstellen wurden unverzüglich geschlossen."

Ansonsten klingt in der Antwort der Bundeswehr durch: Es ist offenbar nicht einfach, Webex sicher zu machen. So werden die erwähnten persönlichen Meetingräume in der On-Premise-Lösung für die 248.000 Nutzerinnen und Nutzer der Bundeswehr automatisch "systemseitig bei Nutzer-Registrierung angelegt", schreibt die Bundeswehr. "Das ist ein firmenseitig implementiertes Feature des Produkts, welches jedoch jetzt als sofortige Sicherheitsmaßnahme mindestens bis zum Abschluss der weiteren Analyse und der Etablierung weiterer Schutzmechanismen gesperrt wurde." Das könnte man so

verstehen: Cisco mag die relativ leicht zugänglichen Meetingräume als eine hilfreiche Funktion empfinden, aber es ist unsicher.

Auch war es der Bundeswehr offenbar nach tagelangen Versuchen nicht möglich, vergangene Meetings einfach zu löschen, sodass man sich nun dafür entschieden hat, die Webex-Instanz komplett vom Internet zu trennen.

Dass bei der Bundeswehr keine automatischen Sicherheitssysteme ansprangen angesichts der vielen Zugriffe auf interne Meetings im Zuge der Recherche, ist erstaunlich. Auch und gerade vor dem Hintergrund, dass der russische Geheimdienst ja bereits öffentlich bewiesen hat, dass er Interesse an entsprechenden Gesprächen hat. Gerade in Bezug auf die Meetings, die für die Zukunft geplant und bis jetzt im Netz zu finden waren, hätten mögliche Angreifer viel Zeit gehabt, um Meetingpasswörter zu erraten.

In IT-Sicherheitskreisen empfiehlt man, Sicherheit schon gleich bei der Konzipierung und bei der Verwendung von Software mitzudenken. Security by design beziehungsweise security by default heißt das in der Fachsprache. Auf Nachfrage bei der Bundeswehr, ob sich die beschriebenen Vorgänge mit diesem Konzept decken, heißt es: "Auch bei Verwendung von Commercial Of The Shelfs-Produkten, die nach den Prinzipien Security by Design/Default produziert wurden, kann nicht ausgeschlossen werden, dass im Nachgang zusätzliche Sicherheitsmaßnahmen getroffen werden müssen."

Max Pfeuffer aus dem Vorstand des Vereins Netzbegrünung warnt in diesem Zusammenhang vor proprietärer Software – also geschlossener Software, deren Quellcode nicht einsehbar ist, so wie im Fall von Webex. "Dort fehlt die Kontrolle darüber, ob der Code grundsätzlichen Sicherheitsanforderungen genügt", sagt Pfeuffer. Zudem sei es oft nicht einfach, entsprechende Lücken zu schließen. "Wenn man selbst keinen Zugriff auf den Code hat, ist das ein großes Problem."

Zwar sei es eine gute Maßnahme für den Schutz von Informationen, eine eigene Infrastruktur zu betreiben, wie es die Bundeswehr mit ihrer On-Premise-Lösung macht. "Es greift aber zu kurz, einfach nur eine Software auf eigenen Servern zu betreiben. Für einen sicheren und zuverlässigen Betrieb ist es notwendig, dass die betriebene Software verstanden und auch überprüft werden kann." Das sei nur mit sogenannten Open-Sour-

ce-Produkten gewährleistet, deren Code öffentlich verfügbar und von unabhängigen Sicherheitsexpertinnen überprüfbar ist.

Auch Bundesregierung betroffen

Cisco möchte zu den Sicherheitslücken auf Anfrage von ZEIT ONLINE nichts sagen: "Cisco ist Lösungslieferant und nicht Betreiber der von der Bundeswehr und anderen Behörden genutzten Webex-Instanzen", so lautet das schriftliche Statement, "zur Nutzung unserer sicheren Kommunikationslösung im Behördenumfeld können wir uns aus Sicherheitsgründen nicht äußern." Man empfehle allgemein, "sich an die Best Practices von Cisco für sichere Videokonferenzen zu halten".

Auch die Frage, ob sich die Vorgänge mit der Vorstellung von Cisco von security by design oder security by default decken, beantwortet der US-Konzern nicht.

Nicht nur die Bundeswehr ist von den Problemen betroffen. Auch der Bundestag und die Bundesregierung nutzen die Videokonferenzlösung Webex – und tappen offenbar in die gleiche Falle wie die Bundeswehr: Im Zuge der aktuellen Recherche wurden unter anderem auch die persönlichen digitalen Meetingräume von Kanzler Olaf Scholz, Wirtschaftsminister Robert Habeck und Finanzminister Christian Lindner gefunden und besucht. Manche davon wurden nach entsprechenden Hinweisen an das CERT-Bund, das IT-Sicherheitsnotfallteam, geschlossen. Die Meetingräume von Olaf Scholz und Robert Habeck waren am Samstag noch offen.

Teil 2:

SPD-Meetings, offen auch für Spione

Nicht nur die Bundeswehr, auch die SPD war von einer Lücke in der Konferenzsoftware Webex betroffen. Unsere Autorin konnte sich in Gespräche einwählen.

Von Eva Wolfangel, Zeit Online 14.5.2024

Es sind perfekte Bedingungen für die Spionin: Niemand bemerkt sie. "Ich glaube, wir sind heute nur zu zweit", sagt eine Teilnehmerin der Webex-Konferenz zu ihrem

Kollegen. Die beiden gehen ganz selbstverständlich davon aus, dass niemand zuhört. Aber sie liegen falsch. Eine Spionin belauscht das "Update Kabinettfrühstück" der Bundesgeschäftsführung der SPD unbemerkt. Eine dritte Person stößt hinzu, sie meldet sich mit "Hallo, hier ist Benny". Auch Benny hat keine Ahnung, dass jemand Fremdes zuhört.

Die Spionin ist die Autorin dieses Textes. Dass sie sich in die digitale Konferenz der SPD einschleichen konnte, bestätigt die Befürchtung, dass es möglich ist, unbemerkt an solchen Webex-Meetings teilzunehmen. Für die drei Teilnehmenden des Kabinettfrühstücks, darunter der SPD-Sprecher Benjamin Köster, kam die Stimme der Journalistin, als sie sich nach wenigen Minuten zu erkennen gab, wie aus dem Nichts. Es handelte sich um eine gravierende Schwachstelle in der digitalen Infrastruktur der Partei, die das betroffene System mittlerweile abgeschaltet hat.

Webex ist eine Software für Videokonferenzen und Telefonschalten des Konzerns Cisco, die von vielen Behörden, Unternehmen und anderen Insitutionen genutzt wird. Der Hersteller bewirbt das Programm als besonders sicher und geeignet für vertrauliche Gespräche. Umso schwerer wiegen die Sicherheitsprobleme, die Recherchen von ZEIT ONLINE nun erneut zeigen.

Anfang Mai hatte ZEIT ONLINE bereits eine Sicherheitslücke in der Webex-Lösung der Bundeswehr aufgedeckt, nach einem Hinweis des der Partei Die Grünen nahestenden Vereins Netzbegrünung. Tausende Links zu Webex-Meetings der Bundeswehr mit teils geheimen Informationen hatten offen im Netz gestanden, einfach auffindbar.

Wenige Wochen später folgt nun eine weitere alarmierende Entdeckung: Nicht nur die Bundeswehr scheint von dem Problem betroffen zu sein, sondern auch die SPD. Damit betrifft die Cisco-Lücke die zweite große deutsche Institution, deren vertrauliche Informationen bis zum Hinweis durch ZEIT ONLINE offen im Internet standen, und das nur wenige Wochen vor der Europawahl.

Gleichzeitig liefert die Recherche den Beleg, dass es unter Umständen sehr wohl möglich ist, sich über diese Lücke unbemerkt in Webex-Meetings eimzuschleichen. Das hatten das Verteidigiungsministerium und der Anbieter Cisco dementiert, nachdem Un-

bekannte ein vertrauliches Gespräch mehrerer Offiziere über den Marschflugkörper Taurus abghört hatten.

Das wirft eine sehr grundsätzliche Frage auf: Wenn es offenbar doch möglich ist, unbemerkt an Meetings teilzunehmen – wie kann dann ausgeschlossen werden, dass echte Spione an sensible Informationen gelangen?

Erst vor wenigen Wochen, als bekannt wurde, dass hinter einem Hackerangriff auf die SPD mutmaßlich der russische Geheimdienst steckt, hatte die Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik, Claudia Plattner, vor weiteren Fällen gewarnt. Sie hatte gefordert, mehr Ressourcen in IT-Sicherheit zu investieren und Systeme besser zu schützen.

Die Recherche offenbart: Webex hat Schwachstellen

Bereits 2020 gab es eine entsprechende Sicherheitslücke in Webex, die es erlaubte, einem Meeting als unsichtbarer "Ghost-User" beizuwohnen. ZEIT ONLINE hatte angesichts der aktuellen Probleme der Bundeswehr Cisco gefragt, ob der Konzern ausschließen könne, dass sich Angreifer unsichtbar in ein Meeting einschleichen: Ein Sprecher hatte daraufhin geäußert, dass die Lücke geschlossen sei. Aber offensichtlich gibt es weiterhin eine Möglichkeit, unbemerkt mitzuhören.

Es ist zwar noch immer unklar, wie der russische Geheimdienst im Februar das vertrauliche Taurus-Meeting der Bundeswehrgeneräle genau aufzeichnen konnte. Aber die aktuellen Recherchen von ZEIT ONLINE zeigen vor allem eines: Webex hat offenbar Schwachstellen, zumindest die von Cisco als besonders sicher angepriesene "sichere Kommunikationslösung im Behördenumfeld", wie Cisco das System nennt, das sowohl die Bundeswehr als auch die SPD nutzen.

Dabei handelt es sich um eine sogenannte On-Premise-Lösung, deren Instanzen von den Behörden selbst gehostet werden. Sie gelten als besonders sicher, weil keine Daten auf Servern von US-Firmen gespeichert werden. Auf diese Lösung verlassen sich auch Behörden in Deutschland – wohl ohne genau zu prüfen, wie sicher die Meetings tatsächlich sind. Anders lassen sich die aktuellen Vorfälle kaum erklären.

Nachdem das Webex-System der Bundeswehr sogar mit Geheimhaltungsstufen versehene Meetings ins Netz geleakt hatte, ist die SPD nun offenbar von der gleichen Sicherheitslücke betroffen: Hunderte Links zu Meetings der Partei standen zusammen mit Titel, Name der Gastgeberin beziehungsweise des Organisators und Datum offen im Netz. Die zugehörigen URLs ließen sich durch Hoch- und Herunterzählen erraten, sodass es einfach möglich war, einige aktuelle Meetings zu finden. Alle Links zu den Meetings der SPD waren dabei identisch, bis auf eine sechsstellige Ziffer. Wer diese systematisch änderte (plus oder minus eins und so weiter), konnte so gezielt alle vorhandenen Links mit den zugehörigen Meetinginformationen finden.

Da die so gefundenen Videokonferenzen zum Großteil nicht durch ein Passwort gesichert waren, musste die Spionin lediglich einen Namen und eine E-Mail-Adresse eingeben und den grünen Button klicken: "Dem Meeting beitreten." Dabei wird die angegebene E-Mail-Adresse nicht von Webex überprüft: Auch wer test@test.de eingibt, wird eingelassen.

Im Zuge dieser Recherche besuchte die Autorin am 8. Mai zwei Meetings der SPD: Das bereits erwähnte "Update Kabinettfrühstück" sowie eine Besprechung mehrerer Mitarbeiterinnen des Büros des SPD-Bundestagsabgeordneten Achim Post. Die Wahl fiel zufällig auf diese beiden Treffen.

Während bei der ersten Besprechung die drei anderen Teilnehmenden per Telefon zugeschaltet waren und so die Spionin nicht sehen konnten (die sich mit ihrem echten Namen angemeldet hatte und sich nach wenigen Minuten zu erkennen gab), fiel sie im letzteren Meeting nach wenigen Minuten auf: Auch hier waren nur drei Teilnehmerinnen anwesend, sie nutzten Webex aber nicht für eine Telefonkonferenz, sondern für eine Videobesprechung.

Der Name der Autorin ploppte also direkt auf den Bildschirmen auf. Die Frage einer Teilnehmerin "Wer ist Eva?" drängte sich also auf. Das ist bei größeren Meetings, bei denen gar nicht alle Teilnehmenden auf einen Bildschirm passen, vermutlich eher selten der Fall. Wer mit ausgeschalteter Kamera teilnimmt oder sich per Telefon einwählt, wird meist ganz hinten einsortiert.

Obwohl ZEIT ONLINE nach dem Bundeswehrvorfall den Webex-Anbieter Cisco über die Sicherheitslücke informiert hatte, hat der Konzern offenbar weder etwas an der Systematik geändert, die dazu führt, dass sich die URLs durch hoch- beziehungsweise runterzählen erraten lassen, noch Behörden gewarnt, die von der gleichen Problematik betroffen sein könnten.

"Es gab keine Warnungen durch den Anbieter", bestätigt eine Sprecherin der SPD auf Anfrage. Man habe sich selbst geholfen und "umgehend nach der direkten Konfrontation durch Sie reagiert und das gesamte Konferenz-System abgeschaltet".

Nur jedes zehnte Meeting passwortgeschützt

Wieso hatten die meisten Meetings der SPD keinen Passwortschutz? "Wichtige und vertrauliche Gespräche werden bei uns persönlich oder in passwortgeschützten Meetings geführt", schreibt die SPD-Sprecherin. Insofern scheint die Partei sehr viele unwichtige Gespräche zu führen: Nur ungefähr jedes zehnte Meeting der zufälligen Stichprobe dieser Recherche war passwortgeschützt.

Die Default-Einstellung scheint bei der SPD zu sein, dass Webex-Meetings nicht geschützt werden – was ahnungslose Mitarbeitende in eine Falle tappen lässt. Die sechs unfreiwilligen SPD-Gesprächspartnerinnen der Autorin waren jedenfalls erstaunt, als sie erfuhren, dass ihr Meeting offen und ohne Passwortschutz im Internet steht. Wer ein sicheres Meeting abhalten will, muss das erstens wissen und sich zweitens aktiv darum kümmern, dass ein Passwort vergeben wird.

Wie viele Meetings betroffen seien und wie viele generell per Webex abgehalten würden, könne sie nicht beziffern, sagte die SPD-Sprecherin. Seit wann und wieso überhaupt Webex genutzt wird, wie viele Accounts die SPD betreibe und ob der SPD noch andere Videokonferenzlösungen zur Verfügung stehen, könne man "aus Gründen der IT-Sicherheit" nicht beantworten. Die von ZEIT ONLINE gefundenen Meetings deuten aber darauf hin, dass Webex zumindest breit genutzt wird – vom Büro des Generalsekretärs über die Jusos, das Finanzmanagement, das Wahlkampfteam Potsdam-Mittelmark über Landesverbände und deren Arbeitsgruppen, aber auch von Ortsgruppen wie der SPD Steglitz-Zehlendorf.

Anders als die SPD empfand die Bundeswehr Fragen nach der Zahl der Meetings und Accounts nicht als sicherheitskritisch: Die Bundeswehr hatte ZEIT ONLINE zuvor mitgeteilt, dass durchschnittlich 45.000 Meetings im Monat mit Webex abgehalten werden – also mehr als 1.500 pro Tag. Nachdem es über Tage auch mit der Hilfe von Cisco offenbar nicht einmal möglich war, vergangene Meetinglinks und Informationen zu löschen, hat die Bundeswehr ihre Instanz schließlich vom Internet getrennt. Die Webex-Lösung ist also nur noch intern aus dem eigenen Netzwerk der Armee erreichbar.

Kein Kommentar von Cisco

Das wirft viele drängende Fragen auf – nicht nur an die Bundeswehr und die SPD, sondern auch an Cisco. Etwa ob die Sicherheitsprobleme, die dazu führen, dass sich sensible Informationen offen im Netz finden lassen, der Vorstellung von Cisco in Bezug auf Security by Design und Security by Default entsprechen?

Das sind grundlegende Konzepte in der IT-Sicherheit, die beschreiben, dass ein System so gestaltet sein sollte, dass Sicherheit bereits im Designprozess berücksichtigt wird und die Grundeinstellungen sicher sind. Ein solches Design sollte nach gängigen Maßstäben verhindern, dass sich URLs durch Hoch- und Runterzählen erraten lassen, und Grundeinstellungen sollten einen Passwortschutz vorsehen. Beides scheint bei Webex aber nicht der Fall zu sein.

Cisco selbst möchte den aktuellen Vorfall nicht kommentieren. Auch Fragen nach den Verkaufszahlen, in Deutschland sowie global, beantwortet der US-Konzern nicht. Stattdessen meldet sich ein sogenannter Incident Manager – gemeint sind damit in der Regel Personen, die auf Sicherheitsvorfälle reagieren – aus den USA mit vielen Fragen (die ZEIT ONLINE nicht beantwortete): Wie ist es gelungen, die Meeting-IDs zu erraten? Waren diese Meetings aktiv, welche URLs hatten die beiden Meetings, die im Zuge der Recherche besucht wurden? Auch Screenshots und Aufzeichnungen werden gewünscht. Antworten auf die an Cisco gestellten Fragen gibt es hingegen keine.

Es lässt sich also kaum sagen, wie viele vertrauliche Informationen derzeit bereits im Internet stehen. Klar ist nur: Sicher ist die "sichere Kommunikationslösung im Behördenumfeld" nach gängigen Maßstäben jedenfalls nicht.

Meetingraum von Kanzler Scholz erreichbar

Andere Behörden nutzen Webex in der Cloud-Variante – sie hosten also ihre Instanzen nicht auf eigenen Servern. Dazu zählt die Bundesregierung. Auch die ist zumindest von einem Sicherheitsproblem betroffen: Für jeden Account legt Webex offenbar automatisch einen persönlichen Meetingraum an, und auch diese sind offen im Netz zu finden.

Das funktioniert nach immer dem gleichen Schema: Der Link endet stets mit dem Namen der Person. Die Links zu erraten, ist also ähnlich einfach wie das Hoch- oder Herunterzählen, man muss lediglich Namen durchprobieren. Auf diese Weise fand der Verein Netzbegrünung unter anderem die Meetingräume von Bundesfinanzminister Christian Lindner, Bundeswirtschaftsminister und Vizekanzler Robert Habeck und Kanzler Olaf Scholz. Während Lindner seinen nach einem Hinweis abschaltete, konnte ZEIT ONLINE jenen von Habeck und Scholz bis vor Kurzem noch erreichen. Erst nach einer erneuten Nachfrage beim Bundeskanzleramt und Wirtschaftsministerium wurden diese offline genommen.

Eine Sprecherin des Bundeswirtschaftsministeriums erklärte auf Anfrage, dass diese Räume "kein Sicherheitsrisiko" darstellten, weil sie nicht genutzt würden und ohnehin lediglich einem Warteraum entsprächen: Damit ist vermutlich gemeint, dass der Host Teilnehmer erst aktiv hereinlassen muss. Beim Besuch von ZEIT ONLINE wurde allerdings angezeigt, dass das Meeting beginne, sobald der Host beitrete. Ein Passwort war nicht nötig. Ähnlich äußerte sich eine Regierungssprecherin in Bezug auf den Raum von Scholz: Die Meetingräume der Videokonferenzlösungen des Bundeskanzleramtes seien "vergleichbar mit einer telefonischen Erreichbarkeit der vorgeschalteten Vermittlung des Bundeskanzleramtes". Eine "tatsächliche Teilnahme an Videokonferenzen oder Zugriff auf weitere Inhalte" sei so nicht möglich.

Dabei wird allerdings ein zentrales Problem übersehen: Zwar lässt sich so vielleicht nicht mal eben eine Besprechung von Kanzler Olaf Scholz unterwandern, aber die persönlichen Meetingräume zeigen eine Meeting-ID an – und diese kann eine entscheidende Information für Spione liefern. Denn genau über diesen Weg fand der Verein Netzbegrünung beispielsweise jeweils die ersten Links der Bundeswehr und der SPD. Wer die Links einmal hat, muss von dort aus dann nur noch hoch- und runterzählen.

Und kann zumindest im Fall der SPD dann auch ohne Passwort an zahlreichen Meetings teilnehmen.

Kann die SPD ausschließen, dass die Sicherheitslücke ausgenutzt wurde und dadurch Informationen an Unbefugte abgeflossen sind? Nein, das könne man "nicht mit absoluter Sicherheit ausschließen", sagte die Sprecherin. "In diesem Fall haben wir aber bis auf die Konfrontation durch Sie in den zwei Schalten am Mittwoch keine weiteren Hinweise darauf."

Allerdings kann man davon ausgehen, dass sich echte Spione nicht selbst zu erkennen geben würden.

Teil 3:

Mithören, wenn Beamte sprechen

Die Software Webex hat mehr Lücken, als der Betreiber Cisco behauptete. Wir fanden Tausende Videokonferenzen von Ministerien – und wählten uns in einige ein.

Von Eva Wolfangel, Zeit Online 5.6.2024

Kurz vor dem Ziel wirkt es so, als greife doch noch ein Sicherheitsmechanismus. "Geben Sie Ihre Teilnehmernummer ein", tönt eine automatische Ansage aus dem Telefon. Kommen wir doch nicht so leicht in das Videomeeting des Bundesamts für Migration und Flüchtlinge (Bamf) wie gedacht? Das Treffen ist ein sogenanntes Daily, ein täglicher Austausch "aller Teams", so steht es in der Beschreibung. Diese Beschreibung, den Namen des Gastgebers sowie die Zugangsdaten finden sich offen im Internet. Wir haben uns eingewählt, um zu testen, wie weit wir kommen.

Nur: Woher jetzt die geforderte Teilnehmernummer bekommen?

Die Software Webex macht es ungebetenen Gästen leicht. "Wenn Sie Ihre Teilnehmernummer nicht kennen, drücken Sie die Rautetaste", sagt eine sanfte Frauenstim-

me. Gesagt, getan – und schon sind wir in einem internen Meeting einer deutschen Behörde. Raute statt Passwort, wie einfach!

Ein Passwort, das man eingeben kann, aber auch nicht muss, wenn man es gerade nicht weiß. Das ist eher eine Kuriosität im Vergleich zum Ausmaß des Problems, das durch einen Fehler in der Videokonferenzsoftware Webex entstanden ist.

Hunderttausende Meetings offen im Netz

Links zu Hunderttausenden Meetings von Behörden und Unternehmen in Deutschland, den Niederlanden, Italien, Österreich, Frankreich, Schweiz, Irland und Dänemark wurden im Zuge dieser Recherche gefunden, an der auch der Verein Netzbegrünung beteiligt war, eine netzpolitische Organisation, die der Partei Die Grünen nahesteht. ZEIT ONLINE liegt eine Stichprobe von Tausenden Meetings vor. In zwei davon konnten wir uns problemlos einwählen. Potenziell wäre das bei vielen weiteren möglich gewesen.

Mit Webex können Video- und Telefonkonferenzen abgehalten werden, ähnlich wie mit Programmen wie Zoom oder Microsoft Teams. Der Anbieter, das US-amerikanische Unternehmen Cisco, bewirbt die Software als besonders sicher. Genutzt wird sie von Institutionen und Unternehmen weltweit.

Vermutlich waren alle Webex-Kunden von der Lücke betroffen. Nach einer Nachfrage von ZEIT ONLINE hat Cisco die Lücke Ende Mai geschlossen.

Bis dahin war es möglich, die Internetadressen von Webex-Meetings auf einfache Weise zu erraten. Denn in diesen Adressen befand sich eine Ziffernfolge, die man nur herauf- oder herunterzählen musste, um auf die jeweils nächste zu kommen. So waren unter anderem Links und Zugangsdaten zu Tausenden Meetings auffindbar, darunter solche des Bundeskanzleramts, des Finanz-, Verkehrs- und Wirtschaftsministeriums, der Landeshauptstadt München, des Bundestags und des Bundesamts für Sicherheit in der Informationstechnik (BSI), das für die IT-Sicherheit des Bundes zuständig ist.

Cisco hat auf Nachfragen von ZEIT ONLINE nicht geantwortet, sondern stattdessen verlangt, weitere Details aus der Recherche preiszugeben. Viele der betroffenen

Bundesministerien und Behörden verweisen auf die Antwort des Bundesinnenministeriums (BMI). Dieses wiederum teilt mit, dass Cisco das BMI "über den grundsätzlichen Sachverhalt informiert" habe. Schwachstellen in Softwareprodukten allein seien "noch keine Grundlage für eine grundsätzliche Aussage über das IT-Sicherheitsniveau eines Produktes".

Bislang empfiehlt das BSI den Bundesbehörden die Software Webex ausdrücklich. Derzeit werde geprüft, ob es angesichts des aktuellen Vorfalls "Anlass zur Aktualisierung der vom BSI ausgesprochenen Empfehlungen" gebe.

Telefontermine zwischen Ministern

Durch die Lücken waren auch viele Meetings auffindbar, die in der Vergangenheit lagen. Beispielsweise stand im März ein "Telefonat mit BM Lindner" im Webex-Kalender von Wirtschaftsminister Robert Habeck, gemeint ist wohl Finanzminister Christian Lindner.

Das BSI sprach offenbar im Mai in Webex-Meetings über die Amtsleitung, tauschte sich mit Europol aus und will im Juli über "Spionage durch ausländische Nachrichtendienste: Akteure und Methoden" sprechen. Brisant, das gerade über Webex zu tun, wo doch mutmaßlich der russische Geheimdienst über eine entsprechende Leitung bereits Gespräche der Bundeswehr abgehört und veröffentlicht hat.

Auch die Landeshauptstadt München gehört laut dieser Recherche zu den betroffenen Großkunden von Cisco. In München sprach man unter anderem im April über einen "Penetrationstest Windows-Client" sowie die Änderung der Fußgängerführung, über die E-Akte und über Klima- und Datenschutz. Jeden Montag um 8.45 Uhr trifft sich die dortige Leiterin des IT-Referats Laura Dornheim mit ihren Mitarbeiterinnen. All das findet sich in den Daten.

Auch Meetings zahlreicher Unternehmen waren auffindbar, darunter ein italienischer Rüstungskonzern, ein deutsches Technologieunternehmen, ein Chemiekonzern, ein Chiphersteller und viele andere. In eine Konferenz der Krankenkassen Barmer wählten wir uns erfolgreich ein.

Ähnliche Lücke wie bei Bundeswehr und SPD

Vor einigen Wochen hat ZEIT ONLINE nach Hinweisen von Netzbegrünung bereits Links zu Hunderttausenden Meetings der Bundeswehr mit zahlreichen Informationen im Netz gefunden. Kurz darauf konnten wir durch die gleiche Sicherheitslücke unerkannt an einem digitalen Treffen der Bundesgeschäftsführung der SPD teilnehmen.

Die SPD und die Bundeswehr verwendeten eine Version von Webex, die auf eigenen Servern installiert und betrieben wird. Viele andere Kunden nutzen die Software als Cloudlösung, das heißt, sie wird auf den Servern von Webex betrieben. Im Mai teilte Cisco ZEIT ONLINE mit: "Unsere in der Cloud gehosteten Instanzen sind standardmäßig so konfiguriert, dass sie zufällig gewählte neun- bis elfstellige Meetingnummern für geplante Meetings verwenden. Diese Meetings sind standardmäßig so konfiguriert, dass sie nicht öffentlich aufgelistet sind, keine Informationen über das Meeting enthalten und passwortgeschützt sind."

Wie sich nun zeigte, stimmte das nicht. Auch in der Cloud-Version waren die Meetingnummern nicht zufällig generiert, sondern ließen sich durch Hoch- und Herunterzählen erraten. Anhand dieser Meeting-IDs ließen sich jede Menge Informationen im Netz finden, etwa die Anlässe, Zeiten und Teilnehmenden von Konferenzen.

Cisco beantwortete Nachfragen von ZEIT ONLINE dazu nicht mehr und verwies lediglich darauf, dass Sicherheit eine "top priority", eine hohe Priorität des Konzerns sei. Fragen könnten nur beantwortet werden, wenn die Redaktion weitere Informationen zum genauen Vorgehen zur Verfügung stellen würde. So detaillierte Rechercheergebnisse preiszugeben, widerspricht jedoch unseren journalistischen Standards.

Auch die von der Sicherheitslücke betroffenen Behörden und Unternehmen scheinen teilweise nur lückenhaft von Cisco informiert worden zu sein. So zeigten Nachfragen von ZEIT ONLINE, dass nicht alle über das wahre Ausmaß der möglicherweise abgeflossenen Daten informiert worden waren.

Das Verkehrs- und Digitalministerium etwa schreibt, es sei von Cisco darüber informiert worden, nicht von der Lücke betroffen gewesen zu sein. Das stimmt aber nicht: Allein in der durchsuchten Stichprobe finden sich 16 Meetings, darunter ein Austausch zur Verwaltungsmodernisierung, ein Meeting zum Digitalgipfel, Referatsleiterrunden und persönliche Meetings von Mitarbeitenden.

Auch das National Cyber Security Centre der niederländischen Regierung erfuhr durch unsere Anfrage von der Lücke. Mehr als 10.000 Meetinglinks der Regierung waren auffindbar, mit Informationen und Daten mehrerer Minister.

Ob Angreifer die Schwachstelle ausgenutzt haben, ist unklar

Ob die Lücke von Angreifern ausgenutzt wurde, wird in vielen Fällen kaum noch aufzuklären sein. Das BSI jedenfalls schreibt, die dafür nötigen Logdaten würden nur "für einen begrenzten Zeitraum gespeichert". Zumindest in diesem Zeitraum liegen "keine Hinweise vor, dass die Schwachstelle von weiteren Angreifern ausgenutzt wurde". Für andere Zeiträume? Möglicherweise kann das niemand beantworten.

Zumindest potenziell kann eine solche Lücke ernste Folgen für die betroffenen Behörden und Unternehmen haben. Denn wie die Auswertung Tausender Screenshots zeigt, lässt sich schon über die Metadaten viel in Erfahrung bringen, was für Spione und Kriminelle interessant sein könnte: Wer bespricht sich mit wem? Worüber? Wann? Wie lange? Zwar ließe sich argumentieren, dass das noch nicht die am besten gehüteten Geheimnisse einer Institution sind. Aber eine Software, die als besonders sicher vermarktet wird, sollte diese Informationen schützen.

Noch schwerer wiegt, dass sich Angreifer möglicherweise unerkannt in Meetings einschleichen konnten. In unseren Tests beim Bamf und der Barmer Krankenkasse wurden wir zwar schnell bemerkt, weil den Teilnehmenden die unbekannte Telefonnummer im Videomeeting auffiel. Wenn aber Robert Habeck, wie es der Name seines Termins nahelegt, im März tatsächlich über eine mit Webex aufgesetzte Telefonschalte mit Christian Lindner gesprochen hat, dann wären unerwünschte Mithörer in diesem Gespräch wohl kaum zu erkennen gewesen. Denn wenn alle Teilnehmer einer Webex-Konferenz per Telefon zugeschaltet sind, können sie nicht sehen, wer alles da ist. Wie einfach es ist, sich dann unbemerkt zuzuschalten, das zeigte unsere Recherche bei der SPD.

"Dass europaweit Regierungen, Verwaltungen, Institutionen, Parteien und Unternehmen betroffen sind, verdeutlicht nicht nur den sorglosen Umgang mit kritischen Informationssystemen", kommentiert Ssaman Mardi, Geschäftsführer des Vereins Netzbe-

grünung die Recherche, "sondern auch die einseitige Abhängigkeit vom Standardprodukt eines Unternehmens, das seinen Programmiercode unter Verschluss hält."

Warum keine Open-Source-Lösungen?

Wieso entscheiden sich angesichts der bisher aufgedeckten Sicherheitslücken so viele Behörden dennoch für Webex? Nachfrage bei Laura Dornheim, die in der bayerischen Landeshauptstadt München für die IT zuständig ist. Auch ihre Webex-Meetings fand ZEIT ONLINE im Zuge der Recherche (diese waren allerdings mit einem Telefonpasswort gesichert, sodass dort kein Überraschungsbesuch möglich war).

Dornheim ist als Verfechterin von Open-Source-Lösungen bekannt. Dennoch hat sie kürzlich zur Vertragsverlängerung mit Cisco geraten. "Ich stehe immer noch zu public money, public code", sagt Dornheim ZEIT ONLINE. Damit ist gemeint, dass mit öffentlichen Mitteln quelloffene Software finanziert werden sollte. "Aber man muss immer mehrere Interessen abwägen. In der Verwaltung ist Nutzbarkeit ein großes Thema." Sie habe bisher keine Open-Source-Lösung gefunden, die die Bedürfnisse der Kommune mit ihren 43.000 Mitarbeitenden erfülle und intuitiv nutzbar sei.

Ändert sich das nach dem aktuellen Vorfall? Mit der Kommunikation zur aktuellen Sicherheitslücke seitens Cisco sei sie nicht besonders glücklich, sagt Dornheim. Aber noch sehe sie keine Alternative, zumal Cisco bisher viel für die Stadt getan habe. Eine eigene Open-Source-Lösung zu hosten, sei aufwendig und teuer: "Es ist leichter, etwas zu kaufen als die Menschen zu finden, die eine eigene Lösung betreuen können." Schließlich müsse diese rund um die Uhr verfügbar sein.

Aber immerhin, Dornheim verspricht: "Wir monitoren die Entwicklungen im Bereich Open Source sehr genau. Sobald es eine Lösung gibt, die unsere Anforderungen erfüllt und die wir mit vergleichbarem Aufwand betreiben können, werde ich einen Umstieg anstoßen."