VIDEOKOMMUNIKATION: EIN VIRUS KOMMT SELTEN ALLEIN

In Zeiten der Corona-Pandemie sind Videokonferenzen beliebt wie noch nie. Diesen Boom machen sich bedauerlicherweise auch Cyber-Kriminelle zunutze. Immer häufiger wird Schadsoftware verbreitet, auf diese Weise auf Nutzerdaten zugegriffen und Geld erpresst. Deutschlands oberste Internet-Sicherheitsbehörde, das Bundesamt für Sicherheit in der Informationstechnik (BSI), warnt vor gravierenden Sicherheitsgefahren und massiv steigenden Hackerangriffen in den nächsten Monaten. Warum sich Unternehmen schützen sollten und welche Maßnahmen einer Datenvernichtung effektiv vorbeugen, lesen Sie im folgenden Artikel.

Als würde Corona unser reales Leben nicht schon genug beeinträchtigen, drohen jetzt zusätzlich große Gefahren durch virtuelle Viren aus dem Internet. Die Zahl der Schadprogrammvarianten hat sich innerhalb eines Jahres laut Bundesamt für Sicherheit in der Informationstechnik (BSI) weltweit um 117 Millionen erhöht. Infolgedessen sei es allein in der DACH-Region im September 2020 zu durchschnittlich rund 7,1 Millionen Angriffen auf das Homeoffice gekommen. Dies entspricht einer Verfünffachung seit März 2020. „Die Bedrohungslage hat sich deutlich verschärft", sagt BSI-Präsident Arne Schönbohm.

Zunehmende Bedrohung

Aus einer von McAfee, Hersteller von Sicherheitssoft- und -hardware, veröffentlichten Studie geht hervor, dass Cyber-Angriffe die globale Wirtschaft 2019 über eine Billion Dollar (!) gekostet haben – ein Anstieg von über 50 Prozent gegenüber dem Vorjahr. Für Deutschland beziffert das Bundeskriminalamt (BKA) in diesem Zeitraum die Kosten auf rund 88 Millionen Euro (2018: 61 Millionen). Häufiges und immer attraktiveres Ziel sind laut BKA dabei Videokonferenzsysteme.

Meldungen wie diese „verdeutlichen die zunehmenden Bedrohungen in einer sich schnell digitalisierenden Welt", sagen Cyber-Sicherheitsexperten wie Professor Christoph Meinel vom renommierten Hasso-Plattner-Institut.

Vor Cyber-Kriminalität ist niemand gefeit. Leidvoll erfahren mussten das Hunderte von Behörden und Unternehmen in den USA. Hacker legten mithilfe von Schadsoftware deren Netzwerke lahm und erpressten Lösegeld. Betroffen davon waren nach Recherchen des „Handelsblatt" Organisationen wie das FBI und das Finanzministerium ebenso wie Microsoft, Intel, aber auch Siemens oder die Telekom. Zu den finanziellen Schäden kommen Unterbrechungen in den Betriebsabläufen, langfristige Produktivitätseinbußen und Reputationsschäden.

Modernste Security-Technologie contra Ransomware

Seit Pandemie-Ausbruch schickten viele Unternehmen ihre Mitarbeiter ins Homeoffice. Immer öfter findet dort die Kommunikation via Videokonferenz statt. Ein regelrechter Boom, den sich Cyber-Kriminelle zunutze machen wollen. „Geschickte Angriffe werden auf Mitarbeiter abzielen, die von zu Hause arbeiten", prognostiziert Kevin Mitnick, Sicherheitsspezialist bei KnowBe4, Anbieter der weltweit größten Plattform für Security Awareness Trainings und simuliertes Phishing.

© iStock

Ohne professionelle Sicherheitsvorkehrungen kann sich bestimmte Schadsoftware, sogenannte Ransomware (siehe Kasten „Ransomware in der Videokommunikation“), über Videokonferenzsysteme verbreiten und Endgeräte und Netzwerke infizieren. Mit verheerenden Folgen: Komplette Unternehmensdaten werden verschlüsselt und erst dann wieder entsperrt, wenn das geforderte Lösegeld bezahlt worden ist.

Zu ungewollter Prominenz hat es in der Vergangenheit die kostenfreie Videokommunikationslösung Zoom gebracht, bei der IT-Sicherheitsexperten immer wieder Sicherheitslücken entdecken konnten.

Niemand hat etwas zu verschenken. Wer kostenfreie Software, also auch Videokonferenzlösungen, nutzt, muss das wissen. Entsprechende Anbieter lassen sich ihre kostenlosen Programme selbstverständlich bezahlen. Sehr oft durch mäßige Programmierung und mangelnde Sicherheitsfunktionen, im schlimmsten Fall aber durch den Verkauf von Nutzerdaten.

Um größtmögliche Sicherheit in der Videokommunikation weitgehend auszuschließen und Daten ausreichend gegen Manipulation, Verlust und unberechtigte Kenntnisnahme durch Dritte zu schützen, bedarf es modernster Technologien und Kontrollmechanismen von Security-Experten. Dabei sollten insbesondere folgende Aspekte Berücksichtigung finden:

Vor Cyber-Kriminalität ist niemand gefeit.

Kontrollierte Benutzeranmeldung

Der Schutz des Anmeldevorgangs vor Hackern ist von grundlegender Bedeutung. Eine Sicherung kann ähnlich erfolgen wie beim Online-Banking-Zugang mit TLS. Über eine branchenübliche Public-Key-Infrastruktur stellt eine vertrauenswürdige Zertifizierungsstelle eines Drittanbieters ein digitales Zertifikat aus. Auf diese Weise können Endpunkte die Identität der Videolösung überprüfen und Unberechtigte daran hindern, die Kommunikation zu belauschen. Ist die TLS-Sicherheit aktiviert, wird prinzipiell ein verschlüsselter HTTPS-Kanal mit jedem Endpunkt eingerichtet, der versucht, auf das System zuzugreifen. Vor dem Übertragen von Anmeldeinformationen überprüft dieser Endpunkt oder Webbrowser das Zertifikat, ob es von einer vertrauenswürdigen Zertifizierungsstelle eines Drittanbieters ausgestellt wurde. Sobald das Zertifikat verifiziert

→ ist, werden Anmelde- und Kennwortinformationen sicher über denselben verschlüsselten HTTPS-Kanal an die Videolösung übertragen. Anmeldeinformationen sollten von den Clients prinzipiell nicht gespeichert werden.

Zugang zum virtuellen Besprechungsraum

Endpunkte sind auch in öffentlichen Netzwerken vor unbefugtem Zugriff über eine IP-Adresse zu schützen und dürfen von einem anderen Endpunkt aus keinesfalls direkt zugänglich sein. Der Anwender muss mithilfe der Vergabe einer PIN jederzeit die Möglichkeit haben, zu bestimmen, wer Zutritt zu seinem persönlichen virtuellen Besprechungsraum hat. Dazu gehört auch, nicht authentifizierte Benutzer, die an einer Besprechung teilnehmen möchten, als Gäste zu identifizieren, um die Vertraulichkeit bestimmter Themen berücksichtigen zu können. Apropos Vertraulichkeit: Den virtuellen Besprechungsraum sollte der Moderator sperren können, um zu verhindern, dass neue Teilnehmer beitreten. Ebenso sollten die Kommunikationsmöglichkeiten (Audio/Video) von Teilnehmern einzeln gesteuert werden können. Elegant ist eine Wartezimmerfunktion, die verhindert, dass sich die Teilnehmer sehen oder hören, bevor der Moderator den Besprechungsraum betritt.

Sichere Authentifizierung

Mitunter versuchen Hacker Zutritt zu einer Videokonferenz zu erhalten, indem sie die Identität einer scheinbar vertraulichen Komponente im Netzwerk übernehmen. Dem kann gegengesteuert werden, indem jeder Server im Netzwerk über eine eindeutige Kennung verfügt, die über eine sichere Verbindung an die Portalanwendung übermittelt wird und auf die sonst nicht zugegriffen werden kann. Wenn keine Konfiguration für die spezifische ID des Computers definiert ist, wird dieser daran gehindert, dem Netzwerk beizutreten – so lange, bis der Administrator die neue ID akzeptiert und die Komponente manuell konfiguriert.

Eindeutige Verschlüsselung

Werden innerhalb einer Videosystem-Architektur Informationen von Maschine zu Maschine übertragen (Signalisierung), müssen diese vor potenziellen Hackern geschützt werden. Eine Möglichkeit hierfür ist die AES-Verschlüsselung über TLS für die Endpunkt- und Serverkommunikation mit Zertifikatunterstützung. Für H.323-Endpunkte können Anrufe mit H.235-Verschlüsselung getätigt werden. SIP-Endpunkte können TLS/SRTP verwenden, um die Signalisierung und die Medien zu verschlüsseln. Für Medien sollten die von SRTP RFC-3711 festgelegten Standards Verwendung finden. Für jeden SRTP-Stream wird mithilfe

RANSOMWARE IN DER VIDEOKOMMUNIKATION

Unter Ransomware versteht man Schadprogramme, mit deren Hilfe Daten auf fremden Rechnern verschlüsselt werden. So wird den Inhabern der Zugriff auf diese Daten unmöglich gemacht. Um den für die Entschlüsselung notwendigen Schlüssel zu erhalten, soll das Opfer ein Lösegeld zahlen (meist in Bitcoins).

Üblicherweise werden solche Schadprogramme großflächig und wahllos per E-Mail versandt. Sofern diese Mails nicht vorab durch Sicherheitsmaßnahmen wie beispielsweise Spamfilter oder allgemeine Virenscanner eliminiert werden, besteht die Gefahr, dass Empfänger die E-Mails und auch die zugehörigen schadhaften Anhänge öffnen. Dann beginnt die automatische Verschlüsselung aller Daten. Zusätzlich kann sich die Schadsoftware über das interne Netzwerk verbreiten.

© Enghouse Interactive

Mit fatalen Folgen. Eine derartige Datenverschlüsselung kann die Verfügbarkeit von Dienstleistungen und Produktionskapazitäten tagelang behindern, im schlimmsten Fall sogar unmöglich machen. Zusätzlich leidet die Reputation des Unternehmens stark durch mediale Negativ-Schlagzeilen.

Per E-Mail verschickte Ransomware enthält meist angebliche Informationen unterschiedlichster Art, mit denen die Empfänger zum Öffnen verleitet werden sollen. Unter anderem sind das gefälschte Spendenaufrufe, medizinische Maßnahmen und Angebote in Sachen Corona, Finanzberatungen. Dabei bedienen sich die Hacker oftmals gefälschter Websites, die vom Original kaum zu unterscheiden sind. Besonders raffinierte Ransomware basiert mittlerweile auf künstlicher Intelligenz und wird zum Beispiel durch Gesichts- und Spracherkennung während einer Videokonferenz aktiviert.

eines Kryptokerns (FIPS 140-2-zertifiziert) ein eindeutiger Hauptschlüssel generiert. Dieser Hauptschlüssel wird über eine sichere TLS-Verbindung ausgetauscht. Gemäß dem SRTP-RFC wird ein Sitzungsschlüssel von beiden Seiten regelmäßig aktualisiert, sodass ein Angreifer keine großen Mengen an Chiffretext von einem einzelnen Schlüssel sammeln kann. Zudem sollten Videolösungen die Möglichkeit bieten, einen verschlüsselten Speicher für aufgezeichnete Videos zu unterstützen.

Geschützte Datenbanken

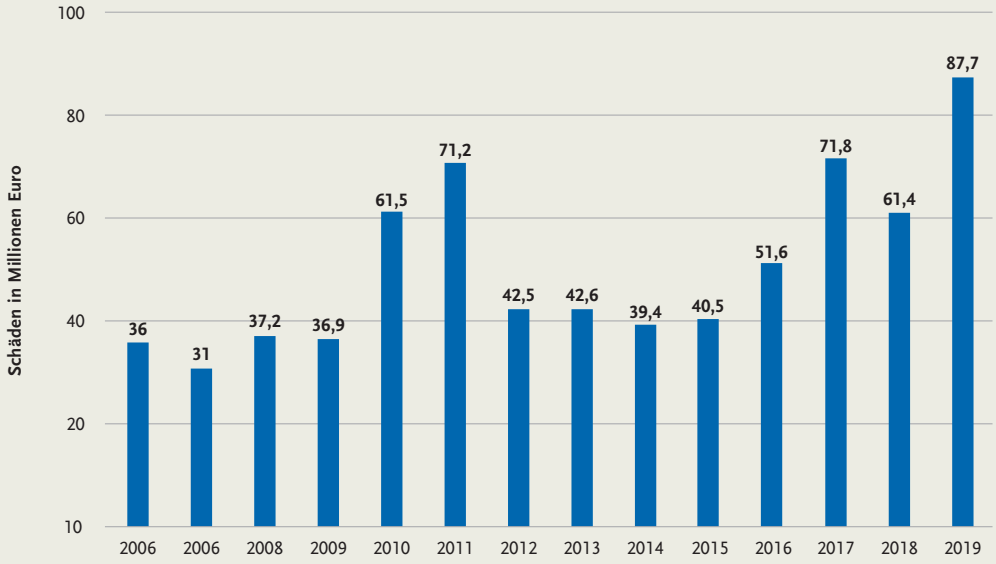
Eine externe Datenbank für die Benutzerkontenverwaltung, LDAP, SAML und Active Directory (AD) sollte vom Videosystem unterstützt werden – ohne dabei Kennwörter zu speichern. Sinnvoll sind Kennwortrichtlinien über die LDAP-Integration in das Unternehmensverzeichnissystem – zum Beispiel AD, Oracle, Novell usw. Für Anwender, die mit SAML authentifiziert werden, fungiert die Videolösung als Dienstanbieter und kann Benutzer über externe SAML 2.0-Identitätsanbieter authentifizieren, ohne Anmeldeinformationen zu speichern oder verfügbar zu machen. Für Benutzer, die LDAP/SAML/AD nicht verwenden, werden Kennwortinformationen immer mit PBKDF2 in der Datenbank „zerhackt". Dadurch wird sichergestellt, dass Kennwörter auch bei einer Sicherheitsverletzung nicht angezeigt werden können.

Ohne professionelle Sicherheitsvorkehrungen kann sich bestimmte Schadsoftware, sogenannte Ransomware, über Videokonferenzsysteme verbreiten und Endgeräte und Netzwerke infizieren.

Management von Sicherheitslücken

Professionelle Videokonferenzlösungen zeichnen sich dadurch aus, dass deren Anbieter über einen multidisziplinären Sicherheitsrat verfügen. Dieser überwacht regelmäßig die neuesten Sicherheitslücken für die in der Videolösung verwendeten Softwareelemente von Drittanbietern und prüft, ob Sicherheitsupdates erforderlich sind. Das Expertenteam führt außerdem regelmäßig Code-Überprüfungen durch, um potenzielle Sicherheitslücken zu identifizieren. Dabei können branchenführende Sicherheits-Scan-Tools wie Nessus von Tenable, Nexpose von Rapid 7 und eine Vielzahl von Open-Source-OWASP-Tools zum Einsatz kommen. Wird eine potenzielle Sicherheitslücke identifiziert, bewertet der Sicherheitsrat sofort deren Auswirkungen.

SCHÄDEN DURCH CYBERKRIMINALITÄT IN DEUTSCHLAND VON 2006 BIS 2019 (IN MILLIONEN EURO)



Quelle: Bundeskriminalamt, © Statista 2020

„VIDYOCONNECT“: SICHERE LÖSUNG FÜR MEETINGS UND TEAM-KOLLABORATION

„VidyoConnect“ wird auf Servern in der Europäischen Union gehostet und verfügt über sehr umfassende Sicherheitsrichtlinien. Folgende Funktionen kontrollieren die korrekte Kommunikation und schützen private Informationen vor unberechtigtem Zugriff und Cyberkriminalität:

Keine Weitergabe von Benutzerdaten an Dritte

- Auf dem Client werden keine Anmeldeinformationen gespeichert.
- Verschlüsselte Token-Technologie für Sitzungssicherheit.
- Passwort-Hashing in der Datenbank.

End-to-End-Sicherheit

- Verwendung von TLS-, SRTP-RFC-, H.235- und AES-128-Bit-Verschlüsselung für Signalisierung und Medien.
- Für jeden SRTP-Stream wird mithilfe eines Kryptokerns (FIPS 140-2-zertifiziert) ein eindeutiger Hauptschlüssel generiert.
- Verschlüsselter Speicher für aufgezeichnete Videos.

Lokale Bereitstellung (optional)

- Im Gegensatz zu vielen Mitbewerbern unterstützt „VidyoConnect“ eine echte lokale Bereitstellung (On-Prem).
- On-Prem-Bereitstellungen bieten ultimative Privatsphäre und Sicherheit für Nutzer, die die vollständige Kontrolle über ihre Videokommunikation benötigen (z. B. Regierungen).
- „VidyoConnect“ unterhält eine staatliche Richtlinie zur Informationssicherheit, die den Umgang mit Vertraulichkeit, Integrität und Verfügbarkeit von Informationen regelt.

Authentifizierung – Sicherheit für Kommunen

- Eindeutige Kennung für jeden Server im Netzwerk, die über eine sichere Verbindung an die Portalanwendung übermittelt wird.

Management von Schwachstellen und potenziellen Bedrohungen

- Der sogenannte „VidyoConnect“-Sicherheitsrat tritt regelmäßig zusammen, um die Sicherheitsrichtlinien und -prozesse zu überprüfen und zu aktualisieren sowie potenzielle Bedrohungen und Probleme zu überprüfen.
- Verfügbarkeit von Prüfungsberichten in den Rechenzentren gemäß SOC 2-Richtlinien.
- Das QA-Team verwendet branchenführende Sicherheits-Scan-Tools wie Nessus von Tenable, Nexpose von Rapid 7 und eine Vielzahl von Open-Source-OWASP-Tools.
- „VidyoConnect“ verwendet das Dienstprogramm Qualys SSL Labs von Drittanbietern, um zu qualifizieren, dass seine serverbasierten Lösungen das hohe Sicherheitsniveau erfüllen.

Datenbanksicherheit

- Keine Kennwortspeicherung in externen Datenbanken für die Benutzerkontenverwaltung – stattdessen Kennwortrichtlinien über die LDAP-Integration in das Verzeichnissystem.
- Kennwörter werden auch bei einer Sicherheitsverletzung nicht angezeigt.
- „VidyoConnect“ authentifiziert Benutzer, ohne Anmeldeinformationen zu speichern oder verfügbar zu machen.

Anwender haben einen Anspruch auf branchenübliche und bewährte Technologien, damit die Kommunikation und private Informationen gesichert sind.

Physische Sicherheitsmaßnahmen

Videolösungen müssen in sicheren Rechenzentren gehostet sein, die auf den neuesten NIST-Standards basieren und in denen SOC 2-Prüfungsberichte verfügbar sind. Zusätzlich ist es angemessen, wenn Anbieter von Videokonferenzlösungen externe Beratungs- und Prüfungsunternehmen mit der Vorbereitung der Bewertung gemäß den SOC 2-Richtlinien beauftragen. Darüber hinaus ist es nur im Sinne potenzieller Kunden, Lösungen von akkreditierten Testunternehmen bewerten zu lassen.

„VidyoConnect“: Durchgängige Verschlüsselung

Enghouse Interactive unterstützt Organisationen und Unternehmen auf der ganzen Welt dabei, vertrauliche Informationen, die während einer Videokonferenz ausgetauscht werden, vor jeglichen unbefugten Zugriffen zu schützen. Mit „VidyoConnect“ bietet Enghouse eine Videokommunikationslösung, die als sicher und hoch zuverlässig gilt und daher weltweit in vielen Ministerien und Branchen im Einsatz ist. Laut dem Marktforschungsunternehmen Grand View Research ist „VidyoConnect“ einer der weltweiten großen Player im Videomarkt. Große Finanzinstitute und Versicherer, Medienkonzerne, Krankenhäuser, Behörden wie das amerikanische Verteidigungsministerium setzen auf die Software. In Indien kommunizieren rund 90 Prozent aller Justizbeamten per Video, beispielsweise bei der Befragung von Zeugen aus weit entfernten Orten. Zudem nutzen das Innenministerium und das Militär die Software für Bildungs- und Schulungszwecke. Aus Sicherheitsgründen werden alle Videos auf einem Regierungsserver gespeichert, zugriffssicher von außen, und können von niemand anderem abgerufen werden. Die Lösung selbst wird im regierungseigenen Rechenzentrum gehostet und ist durchgehend verschlüsselt.

„VidyoConnect“ wird auf Servern in der Europäischen Union gehostet und verfügt über sehr umfassende Sicherheitsrichtlinien (siehe Kasten „VidyoConnect“: Sichere Lösung für Meetings und Team-Kollaboration).

Fazit

Die Sicherung der Kundenkommunikation und privater Informationen beim Einsatz von Videokonferenz- und Kollaboration-Tools, ohne deren Wert und Leistungsfähigkeit zu beeinträchtigen, muss Priorität haben. Lösungsanbieter haben die vornehme Aufgabe, permanent visuelle Überwachung sowie Maßnahmen zur Bewältigung aufkommender Sicherheitsbedrohungen zu bieten. Denn Anwender haben einen Anspruch auf branchenübliche und bewährte Technologien, damit die Kommunikation und private Informationen gesichert sind.

Wie sichere Videokommunikation in der Praxis funktioniert, können Interessenten unverbindlich testen. „VidyoConnect“ ist mit wenig technischem Aufwand einsatzbereit. Kostenfreie Testlizenzen dieser Videokommunikationslösung von Enghouse Interactive erhalten Interessenten für drei Monate mit anschließend 50 Prozent Rabatt auf die Softwarelizenz für ein Jahr.

AUTOR: DÖRTHE RECKHAUS
MARKETING MANAGER ENGHOUSE INTERACTIVE

www.enghouseinteractive.de