4. JAHRESTAGUNG

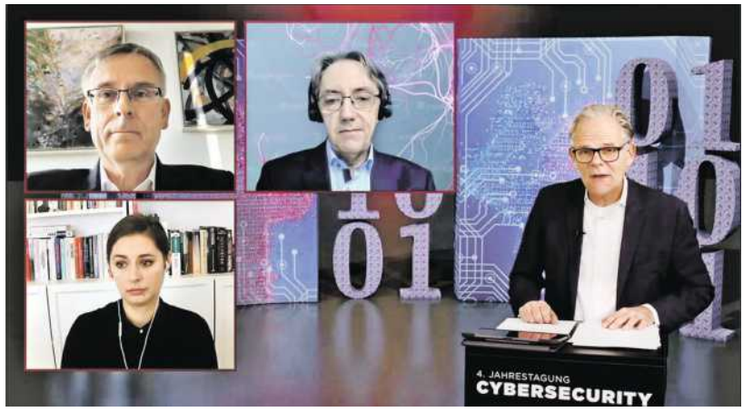
CYBERSECURITY

FORUM FÜR DATENSICHERHEIT, DATENSCHUTZ UND DATENETHIK

28. OKTOBER 2021 | VIRTUELL

#cyberffm

Craig Jones, Director Cybercrime bei Interpol (li.), referierte über die internationalen Aspekte des Kampfes gegen Cyberkriminalität.



Wie gut ist Deutschland im Kampf gegen Ransomware aufgestellt? Darüber diskutierten Andreas Könen, Abteilungsleiter Cyber- und Informationssicherheit im Bundesinnenministerium (links oben), Prof. Dr. Michael Waidner (Mitte), Leiter Fraunhofer Institut SIT, und die Publizistin Katharina Nocun (links unten).

Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), erläuterte die Gefahren für kritische Infrastrukturen.

»Wir haben Alarmstufe Rot«

Mobiles Arbeiten war der Trend schlechthin im Arbeitsleben 2020/21. Für Cyberkriminelle bedeutete das vor allem eines: viele Schwachstellen und Zugriffsmöglichkeiten. Was genau dahintersteckt und wie sich Angriffe verhindern lassen, war Kernthema der vierten Jahrestagung Cybersecurity am 28. Oktober 2021.

Egal, ob es um Angriffe durch Ransomware, also die erpresserische Verschlüsselung von Systemen, Viren oder einfach »nur« den »Diebstahl« von Betriebsgeheimnissen geht: Cyberattacken können jeden treffen, immer und überall – und es werden stetig mehr! Tatsächlich ist die Zahl der Angriffe in der Pandemie enorm gestiegen. Allein die Zahl der Phishing-Mails, mit denen Betrüger sich sensible Daten verschaffen oder bei Nutzern Schadsoftware einschleusen, ist laut der Europäischen Agentur für Cybersicherheit ENISA während der Corona-Krise um 600 Prozent gestiegen. Logisch, dass der Kampf gegen Cyberkriminalität auf internationaler Ebene erfolgen muss. Craig Jones, Director Cybercrime bei Interpol, berichtete daher von den Schwierigkeiten, mehr als 190 Länder dabei unter einen Hut zu bekommen.

Allgegenwärtig, aber oft vermeidbar

Doch wie sieht es in Deutschland aus? Für Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik, ist klar: »Es herrscht Alarmstufe Rot.« »Betroffen sind höchst unterschiedliche Betriebe und Institutionen, von Gerichten und Kliniken über Verwaltungen bis zu Universitäten« erklärte auch Andreas Könen, Abteilungsleiter Cyber- und Informationssicherheit im Bundesinnenministerium, »das ist eine echte Seuche, der wir uns entgegenstellen müssen«. Wie genau so ein Ransomware-Angriff aussehen kann, berichtete Maic Schillack, Erster Stadtrat der Stadt Neustadt am Rübenberge, die 2019 von einem Angriff betroffen war. Schätzungsweise 80 bis 90 Prozent der Angriffe könnten laut Michael Waidner, Leiter des Fraunhofer Instituts für Sichere Informationstechnologie, allerdings verhindert werden – zum Beispiel durch das Einspielen erforderlicher Updates und Sicherheitspatches sowie eine generelle Awareness für das Problem.

Keine Scheu vor Outsourcing

Ein Grund, warum Deutschland in Sachen Netzsicherheit vergleichsweise schlecht dasteht, ist für Dr. Haya Shulman, Director Cybersecurity Analytics and Defences beim Fraunhofer Institut SIT: »In Sachen IT-Sicherheit kocht hier jeder sein eigenes Süppchen. Das geht so weit, dass jeder Lehrstuhl seinen eigenen Server aufsetzt.« Sie rät, »die Infrastruktur an professionelle Anbieter outzusourcen«, und dadurch von einer besseren und schnelleren Wartung zu profitieren.

Betroffen sind natürlich nicht nur große Unternehmen und Wissenschaftsbetriebe, sondern zunehmend auch kleine und mittlere Unternehmen. Michael Niemeier, Vize-Präsident im Bundesamt für Verfassungsschutz, riet daher eindringlich: »Der Mittelstand kann sein Maß an Sicherheit mit wenigen Instrumenten steigern – machen Sie Cybersecurity zur Chefsache!«

Drei Fragen an

Mohamed Ibbich, Director Solutions Engineering, BeyondTrust

Sie sind Experte für Zugriffsrechte: Welchen Fehler begehen Unternehmen in diesem Bereich besonders oft?

Wir sehen immer wieder, dass User Zugriffsberechtigungen auf Datenbanken und Server haben, die sie nicht benötigen. Oft wissen die Unternehmen gar nicht, wer welche Rechte hat und welche Dienste nutzt. Das ist eine echte Schwachstelle. Ein weiterer eklatanter Fehler ist es, überall dasselbe Passwort zu verwenden. Egal ob privat oder im Unternehmen. Einmal geknackt, tauchen diese Passwörter samt dazugehöriger Emailadresse im Internet auf. Dann ist es ein Leichtes, weitere Accounts zu kompromittieren. Besser ist, man hat eine zentrale Passwort-Ablage, die dann entsprechend gut mit einem Zwei-Faktor-Mechanismus und einem starken Passwort gesichert und verschlüsselt ist. Das ist der erste Schritt in die richtige Richtung.

Jeder weiß eigentlich, wie Phishing funktioniert – warum gelingt es Angreifern noch immer so oft, Daten abzugreifen?

Der Erfolg kommt quasi mit der Breite des Angebots: Durch die schiere Masse der Mails gelingt es hier und da, eine vermeintliche Verbindung zum User herzustellen, zum Beispiel weil das Thema der Mail zu einem aktuellen Arbeitsfokus passt. Und der Angreifer muss nur einmal richtigliegen, während Unternehmen immer zu 100 Prozent erfolgreich in der Abwehr sein müssen.

Was muss geschehen, um die Lage zu verbessern?

Von den technischen Lösungen ganz abgesehen, benötigen wir auch einen anderen Umgang mit dem Thema, mehr Austausch unter den Unternehmen und mehr Offenheit. Es ist kein Makel, wenn man angegriffen wurde; das kann jedem passieren. Im Grunde ist es nur eine Frage der Zeit, wann es passiert. Trotzdem ist es selten, dass Institutionen und Unternehmen darüber reden. Nur wenn wir offen mit diesen Angriffen umgehen, können wir langfristig möglichst viel über die potenziellen Angreifer herausfinden und reagieren.

Detaillierte Informationen zur 4. Jahrestagung Cybersecurity finden Sie unter **www.convent.de/cybersecurity**

Veranstalter: CONVENT | Ein Unternehmen der: DIE ZEIT VERLAGSGRUPPE | Premium-Partner: BeyondTrust | Partner: cisco, CROWDSTRIKE, Increase Your Skills, sure[secure] | Netzwerkpartner: ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit, DsiN Deutschland sicher im Netz, Fraunhofer SIT, GT:>_ | Medienpartner: GoingPublic Magazin, Unternehmer Edition