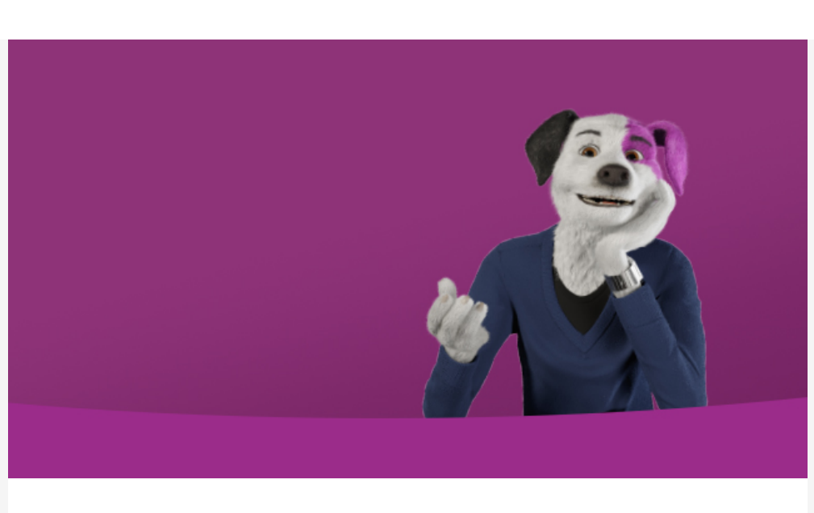
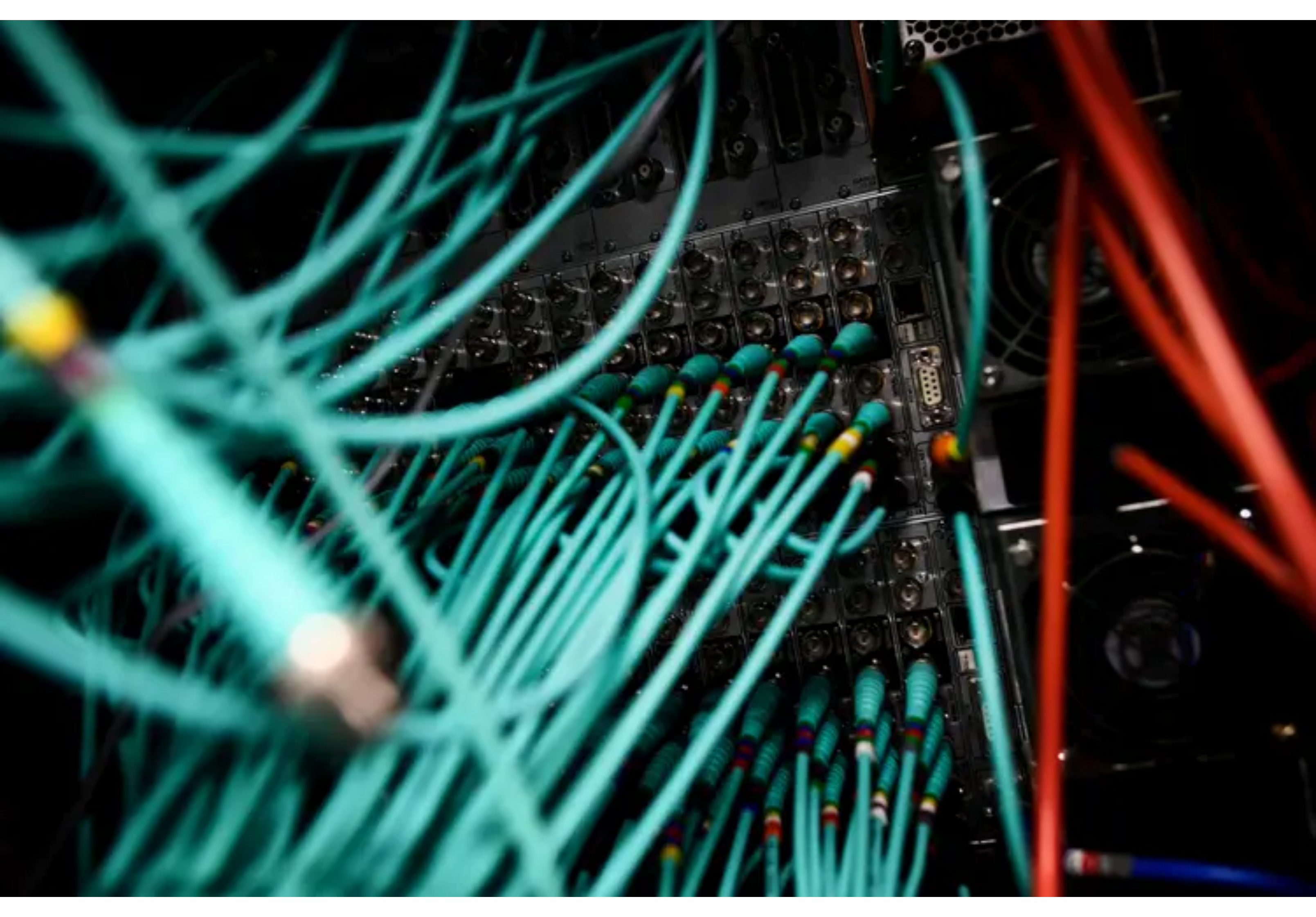
Neue Zürcher Zeitung



Trotz Cyberangriffen: Russland, China und die USA können sich bei der Cybersicherheit überraschend einigen

Sechs Jahre lang ging in der Uno beim Thema Cybersicherheit nichts mehr. Die Fronten zwischen den Weltmächten waren verhärtet. Jetzt konnten sich erstmals alle Mitgliedstaaten auf Empfehlungen einigen – auch dank der Schweiz.

Lukas Mäder
28.03.2021, 14.39 Uhr



Angriffe auf IT-Systeme werden zu einer zunehmenden Bedrohung – die Schweiz engagiert sich deshalb für internationale Vereinbarungen.
Dylan Martinez / Reuters

Die Beziehungen zwischen den Cyber-Grossmächten USA, Russland und China sind schlecht. In den vergangenen Monaten wurden zwei spektakuläre Fälle von Cyberspionage bekannt, hinter denen höchstwahrscheinlich staatlich unterstützte Gruppierungen aus Russland beziehungsweise China stehen: der sogenannte Solarwinds-Angriff und die Exchange-Lücke. Die USA drohen mit Gegenmassnahmen.

Das sind keine guten Voraussetzungen für ein neues Übereinkommen im Bereich Cybersicherheit. Deshalb ist es umso überraschender, dass sich die Grossmächte jüngst im Rahmen der Uno zu einer Einigung durchringen konnten. Unter dem Vorsitz des Schweizer Diplomaten Jürg Lauber stimmten die 193 Uno-Mitgliedstaaten Mitte März Empfehlungen für mehr Cybersicherheit zu – einstimmig.

«In einer Zeit verstärkter Konflikte zwischen Russland, China und den USA ist die Einigung ein grosser Durchbruch», sagt Jovan Kurbalija von der Nichtregierungsorganisation Diplo-Foundation in Genf. Tatsächlich liegt die letzte gemeinsame Erklärung im Bereich Cybersicherheit bereits sechs Jahre zurück. Seither haben sich die Konflikte im Cyberraum verschärft; die drei Grossmächte treten zunehmend offensiv auf.

So ist Russland vermutlich verantwortlich für zwei Stromausfälle in der Ukraine, die durch Cyberangriffe herbeigeführt wurden, für das Eindringen in Server der Demokratischen Partei vor den amerikanischen Präsidentschaftswahlen 2016 oder für den Hackerangriff auf mehrere Ministerien der USA, der im letzten Dezember bekannt wurde.

China werden vor allem Spionageoperationen gegen Unternehmen oder Forschungseinrichtungen zugerechnet, auch im Gesundheitsbereich. Das Ziel: geistiges Eigentum oder Know-how in spezifischen Bereichen zu entwenden, etwa für den Aufbau einer Hochseemarine.

Russland hatte ein Interesse am Gelingen

Dass sich Russland, China und die USA nun trotzdem einigen konnten, liegt auch an der speziellen Vorgeschichte. Nachdem das Uno-Gremium, das früher über Sicherheit im Cyberraum beriet, sich nach 2015 nicht mehr einigen konnte, lancierte Russland einen neuen Prozess. Statt nur in einer ausgewählten Gruppe von Staaten sollten in einem neuen Gremium (OEWG) alle Uno-Mitgliedstaaten mitdiskutieren können. Russland erhoffte sich so mehr Einfluss.

Weil Russland diese Arbeitsgruppe lanciert hatte, wollte es unbedingt eine Einigung. Deshalb, so vermuten Beobachter, brachte es schliesslich kritische Staaten wie Iran, Venezuela oder Kuba zum Einlenken. Diese hatten noch bis zuletzt in markigen Worten Protest angemeldet. Jetzt kann Russland einen Erfolg für sich verbuchen. Gleichzeitig dürfte sich die neue Arbeitsgruppe als künftiges Gremium für das Thema Cybersicherheit innerhalb der Uno etabliert haben. Eine Fortsetzung seiner Arbeit ist bereits beschlossen.

Keine Einigung beim humanitären Völkerrecht erzielt

Weil die Fronten zwischen einzelnen Staaten verhärtet sind, stützt sich der neue Bericht inhaltlich weitgehend auf den letzten Beschluss von 2015. Nur gerade die wichtigsten Punkte konnten gerettet werden, sagt eine Person aus dem Umfeld der Schweizer Delegation.

Der Bericht hält fest, dass grundlegendes Völkerrecht auch im Cyberraum gilt. Er umfasst Empfehlungen für ein gutes Verhalten der Staaten, dazu gehört etwa der Schutz sogenannter kritischer Infrastrukturen. Doch das Anliegen der Schweiz und anderer Staaten, die Gültigkeit des humanitären Völkerrechts im Cyberraum zu bekräftigen, kam aufgrund des grossen Widerstands nicht durch.

«Viele Staaten haben die Gefährdung ihrer IT-Infrastruktur nicht oder zu wenig wahrgenommen»: Unter dem Vorsitz des Schweizers Jürg Lauber konnte sich die Uno-Arbeitsgruppe zu gemeinsamen Empfehlungen durchringen.
Salvatore Di Nolfi / Keystone

Dennoch besteht die Hoffnung, dass die jüngste Entwicklung dem Thema Cybersicherheit neuen Schub verleihen könnte. Das sagt etwa der Vorsitzende der Arbeitsgruppe, Jürg Lauber, auf Anfrage. Zum einen hofft er, dass der Dialog zwischen den Cyber-Grossmächten fortgesetzt wird, zum anderen, dass regionale Initiativen entstehen. Denn den Aufbau von Fähigkeiten und Kompetenzen («capacity building») auf regionaler Ebene hält der Bericht neu als Ziel fest.

Für Lauber ist eines der wichtigsten Ergebnisse der OEWG, dass das Bewusstsein für das Thema Cybersicherheit gewachsen ist. «Viele Staaten haben die Gefährdung ihrer IT-Infrastruktur nicht oder zu wenig wahrgenommen», sagt er. Jetzt gebe es ein gemeinsames Verständnis, dass die offene Fragen angegangen werden müssten.

Zu diesen Fragen gehört insbesondere die Zuordnung von Cyberangriffen («attribution») und die Verantwortlichkeit von Staaten («accountability»). «Das sind die zwei grossen Elefanten im Raum, die niemand ansprechen will», sagt Kurbalija von der Diplo-Foundation.

Wie bedeutend diese Fragen sind, zeigt sich bei Gegenmassnahmen, die die USA zurzeit bezüglich des Solarwinds-Hackerangriffs ergreifen könnten. Die USA gehen von einer russischen Urheberschaft aus. Doch worauf sich diese Attribution stützt, ist öffentlich nicht bekannt.

Um hier mehr Transparenz herzustellen, wäre zum Beispiel ein Netzwerk von unabhängigen IT-Laboren denkbar. Diese Möglichkeit schlagen etwa der Sicherheitsexperte Serge Droz und der ehemalige Schweizer Diplomat Daniel Stauffacher von der Schweizer Nichtregierungsorganisation ICT4Peace vor.

Demgemäss würden mehrere Institute getrennt voneinander die technischen Aspekte eines Cyberangriffs analysieren. Vergleichbar ist diese Aufgabe etwa mit jener des Labors Spiez, das als anerkanntes Prüflabor im Auftrag internationaler Organisationen chemische Kampfstoffe analysiert.

Die technischen Erkenntnisse würden publiziert, und die betroffenen Staaten könnten darauf basierend eine politische Attribution des Cyberangriffs vornehmen. Der Prozess wäre im Vergleich zu heute transparent und unabhängig, auch wenn die heikle Frage der staatlichen Verantwortlichkeiten damit noch nicht gelöst ist.

Mit einem neuen Uno-Gremium könnte aber zumindest das Verhalten der Staaten im Cyberraum thematisiert werden. Stauffacher von ICT4Peace schwebt eine gegenseitige Beurteilung der Staaten vor. So könnten etwa konkrete Cyberangriffe diskutiert werden, die gegen die international anerkannten Empfehlungen verstiessen, sagt Stauffacher. «Wie beim Menschenrechtsrat könnten die Mitglieder thematisieren, wenn ein Land zum Beispiel Cyberangriffe gegen medizinische Einrichtungen führt.»

Die Uno könnte ein permanentes Gremium schaffen

Ob sich die Uno in den nächsten Jahren tatsächlich auf solche weitgehenden Instrumente einigen wird, ist fraglich. Doch möglicherweise nimmt sich künftig ein neues Gremium der Uno dauerhaft des Themas Cybersicherheit an. Diese Idee ist Teil eines Aktionsprogramms, das Frankreich und Ägypten eingebracht hatten. Inzwischen findet der Vorschlag bei rund 50 Mitgliedstaaten Unterstützung, inklusive der Schweiz.

Daraus könnte eine Art Leitfaden entstehen, wie die geltenden völkerrechtlichen Bestimmungen konkret im Cyberraum umgesetzt werden sollen. Dieser Punkt ist entscheidend, wie viele Beobachter sagen. Neue rechtliche Cyber-Bestimmungen braucht es kaum.

Doch die Prozesse innerhalb der Uno sind langsam, und eine Einigung ist unsicher. Deshalb gibt es auch Stimmen, die stärker auf andere internationale Organisationen setzen, die näher an der Privatwirtschaft und der Zivilgesellschaft sind. Gerade IT-Unternehmen müssen in die Diskussion darüber, wie die Cybersicherheit auf der Welt erhöht wird, einbezogen werden.

Die Schweiz könnte dabei eine wichtige Rolle spielen. Was sie als neutraler Akteur mit einem integrativen Ansatz erreichen kann, hat Lauber nun im Rahmen der Arbeitsgruppe gezeigt. Diese Fortschritte sind auch im Interesse der Schweiz. Cyberangriffe sind heute eine Bedrohung für die lokale Infrastruktur, selbst wenn sie sich eigentlich gegen Ziele im Ausland richten – die internationalen Abhängigkeiten sind so gross, dass es leicht zu Folgeschäden weltweit kommen kann.

Deshalb ist in der Schweiz der Wille vorhanden, eine wichtige Rolle zu spielen. Sie engagiert sich nicht nur im Rahmen der Uno, sondern zum Beispiel auch in einer Arbeitsgruppe der OECD für mehr Cybersicherheit. Bereits 2018 hat das Aussendepartement den Geneva Dialogue lanciert, an dem Unternehmen wie Cisco, Huawei, Kaspersky oder Microsoft beteiligt sind. Der Vorteil dieser Initiative: Es geht um handfeste Fragen wie die nach der Sicherheit von digitalen Produkten und Diensten. Und die Cyber-Grossmächte Russland, China und die USA können den Prozess nicht blockieren.

NZZ-Live-Veranstaltung: Wem gehören unsere Daten?
Die Corona-Pandemie hat nicht nur die Digitalisierung beschleunigt, sondern auch die Debatte um die Verwendung unserer Daten. Wie kommen wir in den Besitz unserer Daten? Und wie können wir sie für die Verbesserung des Gemeinwohls nutzen? Gemeinsam mit Expertinnen und Experten sprechen wir über unseren Datenschatz und darüber, wie wir das Maximale herausholen können.
Dienstag, 13. April 2021, 18.30 Uhr, Online-Veranstaltung
Tickets und weitere Informationen finden Sie hier

Mehr zum Thema

Was beim Cyberangriff auf Microsofts Software für Hacker aus China spricht

Der amerikanische Konzern hat den riesigen Angriff auf die E-Mail-Software Exchange Server einer staatlich gestützten Hackergruppe aus China zugeschrieben. Den Vorwurf erhärten weitere Firmen für Cybersicherheit.

Matthias Sander, Taipeh 18.03.2021

Hintertüre bei Microsoft Exchange: Nach den chinesischen Cyberspionen dringen jetzt die Kriminellen ein

Eine Hintertüre im populären E-Mail-Server von Microsoft beschäftigt IT-Verantwortliche weltweit. Inzwischen ist von Hunderttausenden betroffenen Geräten die Rede. Das zieht Cyberspione und Kriminelle an.

Lukas Mäder 10.03.2021

Firmenchefs zum Solarwinds-Hack angehört – langfristige Folgen seien noch nicht absehbar

Vor dem Geheimdienstausschuss des Senats haben am Dienstag die Chefs der in den Cyberangriff involvierten Firmen ausgesagt – und warnend darauf hingewiesen, dass die Angreifer eine verbreitete Schwachstelle in der Lieferkette für Software ausgenutzt hatten.

Marie-Astrid Langer, San Francisco 24.02.2021