Welche Tendenzen zeichnen sich für die Cybersicherheit 2021 ab?

Cyber-Kriminelle scheinen von allen Seiten zu feuern

Welche Lehren in Sachen Cybersicherheit können aus dem Jahr 2020 gezogen werden? Welche Bedrohungen lauern im Jahr 2021? Stormshield zieht Bilanz und skizziert mögliche Bedrohungsszenarien für das aktuell laufende Jahr.

Wäre 2020 ein Film über Cybersicherheit gewesen, dann sicherlich ein Western, denn die Cyber-Kriminellen schienen von allen Seiten zu feuern: Das hinter uns liegende Jahr war besonders intensiv in Sachen Cybersicherheit. Ganz zu schweigen vom Sahnehäubchen der letzten Minute, dem «Sunburst»-Hackerangriff, dessen Raffinesse und Opferliste alarmierend ist. Wie könnte sich die Cyber-Bedrohungslandschaft also zukünftig entwickeln?

Trend 1: COVID-19 und Home-Office, ein perfektes Sprungbrett

Cyberangreifer agieren gerne «anlassbezogen». Der Coronavirus und die legitime Online-Suche nach Informationen sorgte 2020 für grösste Kreativität unter Kriminellen: Phishing-Kampagnen, Verbreitung von Schadsoftware, Vortäuschung offizieller Webseiten, explosionsartige Zunahme des Lieferbetrugs, der durch das Wachstum des E-Commerce angeheizt wurde.

iStock/metamorworks

Im Home-Office-Boom gab jedes vierte Unternehmen an, während des ersten Lockdowns Kompromisse in punkto Sicherheit eingegangen zu sein. Eine Zahl, die bis zur Hälfte aller Angestellten betreffen kann, die laut dem Tessian-Bericht «The State of Data Loss Report» zugeben, sich bei der Arbeit von zu Hause aus, Freiheiten in Bezug auf die Sicherheitsregeln einzuräumen. Das bekannte BYOD-Phänomen (Bring Your Own Device) wurde zu RYOOD (Retrieve Your Old Own Device) mit dem nicht zu vernachlässigenden Potenzial, die gesamte IT-Sicherheit von Unternehmen zu kompromittieren. Vorkommnisse wie das «Zoom-Bombing» entwickelten sich zum Trend und stellen dabei nur ein Beispiel von vielen dar.

Viele IT-Manager werden wahrscheinlich auch 2021 weiter leiden, denn ein gemischtes Arbeitsmodell (aus Präsenz und Home-Office) setzt sich in Organisationen nachhaltig durch, mit allen damit einhergehenden Risiken. Sofortige Massnahmen wären erforderlich: Alle Mitarbeiter müssten ausreichend zum Thema Cybersicherheit geschult werden, und die IT-Abteilung müsste eine regelmässige Verbindung sowohl mit Fern-Arbeitenden als auch mit Dienstleistern aufrechterhalten. Das reicht aber nicht. Sollten Unternehmen in Zukunft, die von ihren Mitarbeitenden auf dem eigenen Rechner installierte Software überwachen? Besteht die Notwendigkeit, eine verbindliche Cybersicherheitscharta zu erstellen, die die im Rahmen des Home-Office genutzten Tools regelt? Oder sollten Unternehmen allen Mitarbeitenden einen Firmen-Rechner oder -Laptop stellen, der den Sicherheits-Policies entspricht? Wie hoch ist der Preis dafür?

Trend 2: Bedrohungen durch künstliche Intelligenz

Im letzten Dezember vom europäischen Institute for Security Studies (ISS) veröffentlichten Dokument «Conflicts to come» stellen Experten 15 Kriegsszenarien für das Jahr 2030 vor. Der Begriff Künstliche Intelligenz kommt darin insgesamt 547 Mal vor. Laut einem Europol-Bericht über aktuelle und zukünftige Bedrohungen durch KI wird diese Technologie bereits eingesetzt, um Passwörter zu erraten, CAPTCHAs zu knacken und sogar Stimmen zu imitieren. Dabei spielen der Boom von Machine Learning Operations (MLOps) und die Industrialisierung von KI eine grosse Rolle. Forrester prognostiziert für 2021 ein Wachstum des Marktwertes für KI-Lösungen auf 37 Milliarden US Dollar bis zum Jahr 2025. Laut einer im Juli 2020 veröffentlichten Accenture-Studie unterschätzen Unternehmen jedoch die Risiken und planen nur langsam für die Absicherung dieser Technologien.

Nachdem im August 2020 künstliche Intelligenz in einem Militärflugzeug der US Air Force eingesetzt wurde und autonome Fahrzeuge zunehmend auf KI setzen, sind für 2021 gehackte Fahrzeuge auf der Strasse und Flugobjekte in der Luft denkbar. Hier stellen die Wahrung der Datenintegrität und die Absicherung des Datenflusses zentrale Anliegen dar: Die Manipulation von Befehlen, die Kaperung von autonomen Fahrzeugen, Drohnen oder via KI gesteuerter Militärflugzeuge sind ein möglicher Ausgangspunkt für Katastrophenszenarien, genauso wie Attacken auf – mittels KI gesteuerte – Stromerzeugungsanlagen beziehungsweise vernetzte Smart Cities.

Trend 3: 5G und IoT in der Industrie, ein zweischneidiges Schwert

Höhere Datenaustauschgeschwindigkeit und Leistung, Echtzeitfunktionen sowie drahtlose Konnektivität zur Vermeidung der Risiken von drahtgebundenen Lösungen sind Argumente, die 5G zur möglichen Grundlage der tatsächlichen vierten industriellen Revolution machen. Jedoch verheissen der dezentrale Aufbau von 5G-Netzwerken und die absehbar explosionsartige Zunahme verbundener Objekte, die nicht unbedingt nach den Prinzipien der Security-by-Design konzipiert wurden, eine deutliche Erweiterung der Angriffsfläche. Dahingegen mangelt es noch an einem durchgängig greifenden Sicherheitskonzept. Dazu ist anzumerken, dass Europa im Dezember 2020 ein Audit mit dem Ziel gestartet hat, zu prüfen, ob die derzeit in mehreren Ländern eingesetzte 5G-Cybersicherheit tatsächlich dem erwarteten Niveau entspricht, denn bereits heute sind Attacken an Fertigungsanlagen denkbar, die die ersten 5G-Pilotverbindungen in Betrieb nehmen. Die drei grossen klassischen Bedrohungen (Industriespionage, Manipulation oder Stillstand der Produktion) stehen nach wie vor im Vordergrund.

Trend 4: Eine Geopolitik, die Cyberattacken ausgeliefert ist

Ob die falsche Zählung von elektronisch übermittelten Wahlzetteln durch Fehler der dafür eingesetzten KI (Beispiel Brasilien), gezielte Angriffe auf nationale, strategische Ziele (Beispiel israelische Wasserindustrie), die Bekennung von Cyberattacken durch Gruppen, die staatlichen Strukturen nahestehen oder die Verbreitung von Deep-Fakes zur Einflussnahme bei wichtigen geopolitischen Fragen: Wenn selbst die Financial Times manches Szenario mit «Cyber winter is coming» beschreibt, ist die Lage mehr als nur besorgniserregend. Zu befürchten ist die Entstehung einer neuen Art von Cyber-Terrorismus, die aus einer möglichen Konvergenz zwischen Hackern und Milizen entspringen könnte. Ob Staaten dabei mitmischen, spielt hier allerdings vorerst eine sekundäre Rolle, viel wichtiger sind die Folgen: Ein mögliches Worst-Case-Szenario könnte die Durchführung eines physischen Attentats in Verbindung mit einem Cyberangriff sein, wodurch beispielsweise die Rettungsdienste blockiert oder der Zugang zur medizinischen Versorgung der Opfer verzögert oder sogar verhindert werden könnte. «