Aktueller Kommentar von SentinelOne vom 27.11.2020

Cybersecurity im Wandel – Ein Ausblick auf 2021

Morgan Wright, Chief Security Advisor bei SentinelOne

Ein denkwürdiges Jahr neigt sich dem Ende zu und auch in der IT hat sich einiges getan. In Anbetracht zunehmender Bedrohungen aus dem Cyberraum stellt sich die Frage, wie die IT-Sicherheit auf diese Entwicklung reagieren wird. Die Pandemie lässt uns nicht los, sie ist und bleibt ein wichtiges Thema. Damit ist allerdings nicht nur die aktuelle Gesundheitskrise gemeint, sondern auch der Cyberbereich – die rasante **Verbreitung von Ransomware** <https://www.handelsblatt.com/technik/sicherheit-im-netz/digitale-erpressung-mit-ransomware-gefahr-fuer-unternehmen-durch-cyberkriminalitaet-nimmt-deutlich-zu/26115484.html?ticket=ST-3397065-oAecKS3b6Z1YeHseas03-ap2> rund um den Globus weist nämlich einige Parallelen zu einer menschlichen Vireninfektion auf.

Planbare IT-Sicherheit muss zur Chefsache werden

Eine wichtige Lektion aus dem Jahr 2020 ist, dass die meisten Unternehmen zwar einen generellen Business-Continuity-Plan haben, allerdings keinen solchen für den Umgang mit einer derart unberechenbaren Situation wie die, in der wir uns aktuell befinden. Nur die wenigsten Organisationen sind adäquat – oder gar gut – auf aktuelle Gefahren vorbereitet. Die Lücken in Sachen Betriebsplanung wurden in diesem Jahr sehr deutlich, als Unternehmen und Regierungen zum Anfang der Pandemie mit dem Versuch kämpften, quasi on-the-fly neue und ungetestete Konzepte zu entwickeln.

Im Jahr 2021 wird es nicht nur um die Widerstandsfähigkeit der Wirtschaft gehen, sondern zudem um die der Menschen. In den Chefetagen muss eine neue und modernere Art von Führungsstil herrschen, die Unternehmen und Teams dazu befähigt, in komplexen und dynamischen Situationen erfolgreich zu kommunizieren, und zusammenzuarbeiten. Für Unternehmen ist dies die Gelegenheit, sich von überholten und veralteten Sicherheitslösungen zu trennen und mutigere und effektivere KI-basierte Lösungen einzuführen.

Aller Wahrscheinlichkeit nach kommt es in der nahen Zukunft zu einem weiteren Anstieg der Angriffe auf das Gesundheitswesen und damit auch Krankenhäuser sowie auf Forschungs- und Entwicklungseinrichtungen, die sich mit COVID-Impfstoffen und -Therapien befassen. Die Vorgehensweise der Cyberkriminellen wird sich jedoch ändern. Es wird eine engere Zusammenarbeit zwischen Cyberkriminellen verschiedener Arten geben wie beispielsweise Hacker, die sich darauf spezialisieren in die Organisation einzudringen und Ransomware-Experten, welche die Daten des Opfers verschlüsseln und Lösegeldforderungen stellen. Zwei neue Hauptangriffsziele sind unter anderem Cloud-Speicher und Netzwerke im Bereich OT (Operational Technology). Schon in diesem Jahr konnten wir eine Anhäufung von Attacken auf OT-Systeme und -Maschinen (z.B. industrielle Steuerungssysteme) beobachten. Diese Entwicklung gibt Anlass zur Sorge und stellt eine große Bedrohung dar, insbesondere für Fabriken, Krankenhäuser und kritische Infrastrukturen.

Fazit

Die Vorfälle häufen sich, ausgelöst durch verschiedene Bedrohungen, von einfacher Malware bis hin zu gezielten Angriffen durch staatliche Akteure. Die schiere Anzahl von Attacken sowie deren Wirksamkeit haben gezeigt, dass es unzureichend ist, sich allein auf menschliches Eingreifen zu verlassen. Stattdessen muss ein größerer Fokus auf Prozesse und Lösungen gelegt werden, welche die Cybersicherheit zuverlässig

automatisieren und das Personal entlasten. Maschinengesteuerte (und dadurch blitzschnelle) Cyberangriffe erfordern automatisierten Schutz, der Viren und Malware keine Zeit bietet, das System zu infiltrieren.

Kontakt

Kafka Kommunikation GmbH & Co.
Lukas Reck
Dr. Bastian Hallbauer-Beutler
Kafka Kommunikation
089 74 74 70 580
sentinelone@kafka-kommunikation.de