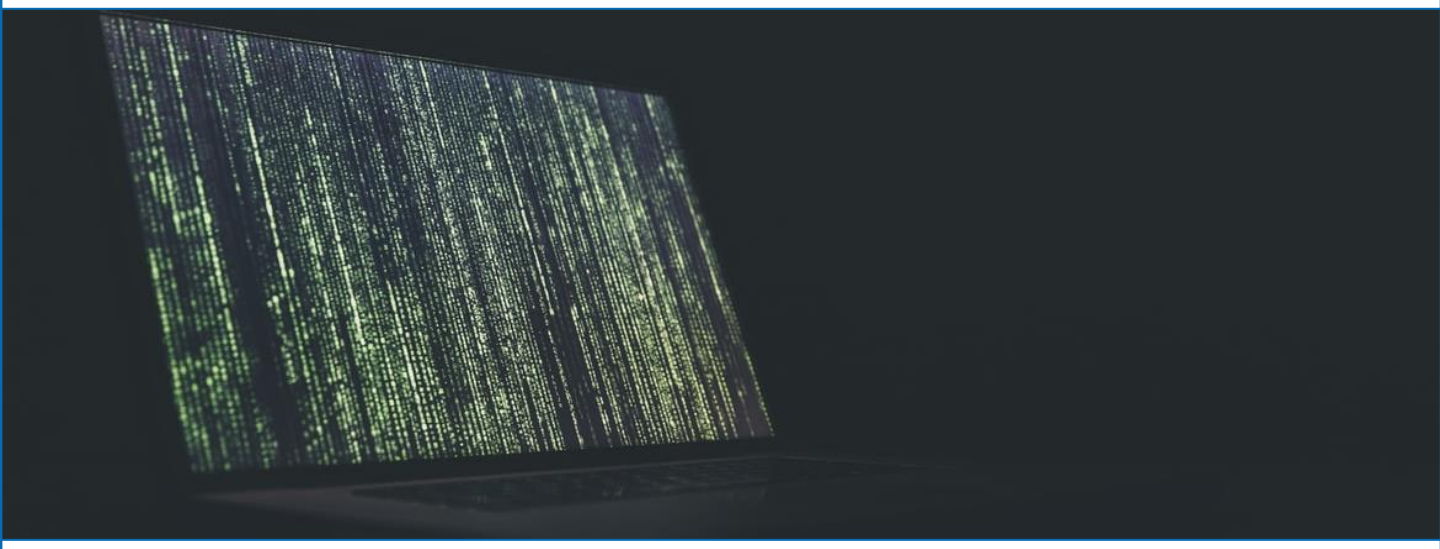
IV. QUARTAL, 2021

Allianz

CYBER-NEWSLETTER

Aktuelle Entwicklungen



Kritische Sicherheitslücke in log4j entdeckt

Eine Sicherheitslücke im breit eingesetzten log4j-Framework könnte einen Großteil der Server im Internet gefährden. Wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) mitteilte, könnte die kritische Schwachstelle Auswirkungen auf alle aus dem Internet erreichbaren Java-Anwendungen haben. Zahlreiche Hersteller, wie Cisco, Broadcom oder VMWare haben Nutzer bereits vor der Verwundbarkeit ihrer Produkte gewarnt und sie dringend dazu geraten, betroffene Systeme upzudaten.

log4j ist ein Framework zum Loggen von Anwendungsmeldungen in Java, das innerhalb vieler Open-Source- und kommerzieller Softwareprodukte eingesetzt wird. Vereinfacht formuliert kommt die Schwachstelle dann zustande, wenn log4j einen bestimmten Text interpretiert, um ein Ereignis zu protokollieren. In der Folge kontaktiert der Dienst daraufhin externe Server, nimmt von diesem Java-Code entgegen und führt ihn aus. Dies führt wiederum dazu, dass Schadsoftware auf die Systeme gelangen kann. Das BSI hat die log4j-Lücke mit der höchsten Warnstufe "4/Rot" eingestuft, auch weil sie bereits aktiv ausgenutzt wurde, z.B. für Krypto-miner und möglicherweise auch im Rahmen von Ransomware-Angriffen.

IN DIESEM QUARTAL

Sicherheitslücke in log4j: Die Hintergründe

Zur Meldung des BSI gelangen Sie unter folgendem Link. Branchenexperten vergleichen die Schwachstelle in log4j mit vergangenen gravierenden Sicherheitslücken, wie Heartbleed oder Shellshock. Zurzeit häufen sich Meldungen zu potenziell betroffenen Produkten. Wie bei Heartbleed, handelt es sich bei der log4J-Lücke um eine Schwach-stelle innerhalb eines weit verbreiteten Open-Source-Dienstes, das seitens freiwilliger Entwicklern gepflegt wird.

Städte im Visier von Cyber-Kriminellen

Eine steigende Anzahl von kommunalen Behörden und Stadtverwaltungen ist während der letzten Monate Opfer von Cyber-Angriffen geworden. Für Cyber-kriminelle stellen sie ein attraktives und lukratives Ziel dar, da sie oft essenziell wichtige Dienste liefern und Opfer somit unter dringenden Handlungsbedarf stehen.

In Schwerin und dem angrenzenden Landkreis Ludwigslust-Parchim hat ein Verschlüsselungstrojaner weite Teile der öffentlichen Verwaltung lahmgelegt. Die Schadsoftware wurde auf den Systemen eines kommunalen Unternehmens entdeckt, das die IT-Dienste für den Landkreis sowie dessen Versorgungs-betriebe stellt. Als Folge fielen Bürgerdienste und der Betrieb der Verkehrsgesellschaft Ludwigslust-Parchim (VLP) aus. Sämtliche IT- Systeme mussten zudem heruntergefahren werden. Die Ruhrgebietsstadt Witten Hatten ebenfalls mit den Folgen eines Cyber-Angriffs zu kämpfen. Die Stadtverwaltung war danach weder telefonisch noch per E-Mail erreichbar. Termine in der Bürgerberatung mussten storniert werden und mehr als 1000 Computerarbeitsplätze waren nicht länger funktionsfähig.

Anfang Dezember hatten Kriminelle die Computersysteme der Stadtwerke Pirna angegriffen. Auch wenn die Versorgungssicherheit aufrecht-erhalten bleiben konnte, sahen sich die Stadtwerke dennoch gezwungen im Notbetrieb zu arbeiten. E-Mails konnten nicht beantwortet oder Abrechnungen erstellt werden.

Von Cyber-Angriffen betroffen waren auch die Stadt-verwaltungen Geisenheim und Anhalt-Bitterfeld. Letztere hatte für Schlagzeilen gesorgt, da als sie als Folge den deutschlandweit ersten Cyber-Katastrophenfall ausgerufen hatte.

Bedrohungslage bleibt angespannt bis kritisch

Auch in diesem Jahr hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinen Bericht zur aktuellen IT-Sicherheitslage in Deutschland veröf-fentlicht. Das ernüchternde Fazit: Die Lage in 2021 hat sich gegenüber zum Vorjahr nicht verbessert und ist als „angespannt bis kritisch“ zu betrachten.

Durch die enorme Zunahme der Arbeit im Homeoffice während der Pandemie haben sich neue Einfallstore in Unternehmen ergeben, die von Cyber-Kriminellen ausgenutzt werden. Das vergangene Jahr sah zudem einen rasanten Anstieg an Ransomware-Angriffen. Immer häufiger verschlüsseln Cyber-Kriminelle hierbei nicht nur die Daten von Unternehmen und Institutionen, sondern drohen auch mit der Veröffentlichung sensibler Daten, die sie im Verlauf des Angriff erbeuten konnten. Besorgniserregend sei laut BSI zudem der sprunghafte Anstieg neuer Malware-Varianten (+22%) sowie die Qualität und Verbreitung gravierenden Schwachstellen in IT-Produkten. So wurde eine Sicherheitslücke in MS Exchange auf etwa 98% aller geprüften Systemen festgestellt.

Vor kurzem erschien auch das deutsch-französische Lagebild von BSI und dem französischen Pendant ANSSI zum Themenschwerpunkt Ransomware. Das BSI warnte zuletzt über eine Reihe besonders schwerwiegender Bedrohungen und Schwachstellen, darunter auch die kritische Sicherheitslücke in log4j (s. Titelseite).

.

Cyber-Angriffe auf kommunale Behörden

Die NDR-Sendung „Angriff auf Anhalt-Bitterfeld – Landkreis im Ausnahmezustand“ liefert interessante Hintergrund-informationen zu dem Cyber-Angriff, der für den ersten ausgerufenen Cyber-Katastrophenfall in Deutschland geführt hat. Mit dem Thema beschäftigte sich auch ein Hintergrundgespräch der Stiftung Neue Verantwortung, das unter folgendem Link in voller Länge zu finden ist.

Aufschwung und Wandel auf dem Cyber-Versicherungsmarkt

Immer mehr Unternehmen und öffentliche Behörden fallen Cyber-Angriffen zum Opfer. Die Tendenz zum Homeoffice und die damit einhergehenden Risiken haben die Lage noch weiter zugespitzt. Damit stehen Unternehmen und Behörden heute mehr denn je unter Druck, effektive Schutzmaßnahmen gegen die Folgen cyber-krimineller Handlungen einzuführen. Zu diesen zählen immer häufiger nicht allein technische Sicherheitslösungen, sondern auch Cyber-Versicherungen, die im Falle eines erfolgreichen Angriffs greifen. Schätzungen zufolge wird ihr Markt von rund sieben Milliarden Dollar (2020) bis auf 20 Milliarden Dollar im Jahr 2025 wachsen.

Doch mit der steigenden Nachfrage wächst auch der Druck auf die Versicherer. Diese sehen sich oft mit hohen Kosten konfrontiert, die im Falle von Cyber-Angriffen entstehen und die nur schwer zu kalkulieren sind. Vor allem kleinere Anbieter versuchen deshalb, den Markt für Cyber-Versicherungen wieder zu verlassen. Somit übersteigt die Nachfrage nach Cyber-Versicherungen heutzutage ihr Angebot. Hinzu kommen striktere Vertragsklauseln, die Versicherungsanbieter an Kunden stellen, um das steigende Risiko von Hackerangriffen besser handhaben zu können. In diesem Sinne haben Mitglieder der Lloyd's Market Association, einem der wichtigsten Branchenverbände, neue Standardklauseln für Cyber-Versicherungen beschlossen, die u.a. definieren, was unter einem Cyber-Angriff verstanden wird und welche Schäden nicht gedeckt werden. Dazu zählen beispielsweise Schäden durch Cyber-Angriffe, die im Rahmen von Auseinandersetzungen seitens von staatlichen Akteuren initiiert werden (sog. „Cyber-War-Klausel“).

Für interessierte Kunden wird der Zugang zum Markt für Cyber-Versicherungen schwieriger. Ein Ausweg aus diesem Engpass kann dadurch gelingen, dass Kunden gewisse Voraussetzungen gerecht werden, die ein Mindestmaß an Sicherheit gewährleisten können. Dazu zählen u.a. Mechanismen zur Multi-Faktor Authentifizierung (MFA), die Segmentierung von Netzwerken, oder die Einführung von Systemen zur Identifizierung und dem Management von Schwachstellen. Neben solchen technischen Maßnahmen, sollten auch organisatorische Maßnahmen implementiert werden. Hierunter zählen u.a. die Erstellung einschlägiger Sicherheitsdokumente (Strategien, Richtlinien und Policies), die Entwicklung eines Inventars relevanter IT-Systeme (Hardware und Software, inklusive Produktionsmaschinen) und die Einführung von Prozessen in den Bereichen des Business Continuity-, Notfalls- und Krisenmanagements. Eine essentielle Rolle spielen regelmäßige Schulungen und Awareness-Kampagnen für Mitarbeiter auf den Gebieten der Informations- und IT-Sicherheit sowie im Bereich des Datenschutzes. Von der Einführung der oben genannten Maßnahmen profitieren die Unternehmen langfristig, indem sie nicht allein für mehr Sicherheit und Resilienz sorgen, sondern auch einen fundamentalen Beitrag zur Compliance mit gesetzlichen Vorgaben auf nationaler und europäischer Ebene leisten.

Hintergründe: Cyber-Versicherungen im Wandel

Weitere Hintergrundinformationen zu den Klauseln bezüglich des Haftungsausschlusses im Falle kriegerischer Angriffe finden Sie unter dem folgenden Link. Über Risiken durch Cyber-Angriffe und die Stellung von Rückversicherern berichtet zuletzt der Spiegel. Das Thema Cyber-War wurde hingegen vor kurzem auch u.a. auf heise online thematisiert.

Zehn Staaten führen gemeinsame Cyber-Simulation durch

Das israelische Finanzministerium führte eine zehntägige Simulation eines großflächigen Cyber-Angriffs auf das globale Finanzsystem durch. Die Übung diente dazu, die Zusammenarbeit zwischen den Staaten gegen Cyber-Bedrohungen zu verstärken und wichtige Erkenntnisse zu sammeln die dazu beitragen können, die Schäden auf den Finanzmärkten im Falle eines Cyber-Angriffs zu minimieren.

An der Übung nahmen neben Israel auch die USA, Großbritannien, die Vereinigten Arabischen Emiraten, Deutschland, Italien, Österreich, Schweiz, die Niederlande und Thailand teil. Vertreter des Internationalen Währungsfonds und der Weltbank waren ebenfalls beteiligt.

In der Übung wurden mehrere Szenarien simuliert, darunter auch Angriffe, die auf die Manipulation von Transaktionen zielten und sich auf die globalen Devisen- und Anleihemärkte auswirkten. Zu den Szenarien gehörten darüber hinaus auch die Veröffentlichung sensibler Daten im Darknet oder die Verbreitung von Fake News, die dazu dienen sollen, das globale Finanzsystem zu destabilisieren.

Diese Cyber-Bedrohungen erwarten uns 2022

Das Jahr 2021 war von eine Reihe spektakulärer und gleichzeitig verheerender Cyber-Angriffe geprägt, darunter die ausgenutzten Sicherheitslücken in Produkten von SolarWinds und Kaseya oder der Ransomware-Angriff auf Colonial Pipeline. Auch für das nächste Jahr sind die Prognosen der Experten nicht rosig.

Ransomware-Angriffe werden auch in 2022 für Schlagzeilen sorgen, oft gepaart mit der Veröffentlichung sensibler Daten, die die Opfer dazu bringen sollen, Lösegelder zu zahlen. Immer häufiger werden solche Angriffe durch kriminelle Organisationen angeboten, die ihre Dienste auf dem Markt anbieten (*Cybercrime as a Service*).

Die allgemeine Verbesserung der Resilienz vieler Unternehmen führt immer häufiger dazu, dass Kriminelle versuchen diese über ihre Lieferkette anzugreifen. Im Falle solcher *Supply Chain Attacks* nutzen Angreifer z.B. Schwachstellen in der Software und Hardware im Produktionsumfeld aus, um ihre Ziel zu erreichen.

Weiterhin ist zu beobachten, dass immer häufiger auch staatliche Akteure eine zunehmende Rolle in der Entwicklung und dem Einsatz von Cyber-Angriffen spielen. Sie machen sich der destabilisierenden Wirkung von Angriffen auf kritische Infrastrukturen, beispielsweise im Finanz-, Gesundheits- oder Energiesektor zu Nutze, um ihre geopolitischen Ziele zu erreichen.

Webinar: „Cyber trends to watch in 2022"

Was sind die neuesten Cyber-Sicherheitstrends wie können Unternehmen im Angriffsfall richtig reagieren? Unseren Experten haben sich dazu im Rahmen des Webinars „Cyber trends to watch in 2022" ausgetauscht. Die Aufzeichnung in voller Länge finden Sie unter folgenden Link.