DerTreasurer
NACHRICHTEN FÜR DIE FINANZABTEILUNG

Ausgabe 4 | 24. Februar 2022

Inhalt

Die Cybercrime-Welle rollt

Die massive Hacker-Attacke kam im Dezember 2021 etwas kryptisch daher: Es sei eine Schwachstelle namens „Log4Shell" in der beliebten Java-Protokollierungsbibliothek gefunden worden, warnten IT-Spezialisten. Experten rund um die Welt waren sich einig: Es handelte sich um eine der größten Sicherheitsbedrohungen für Unternehmen seit Jahren. Was können Treasurer tun, um sich für Cyber-Attacken zu wappnen?

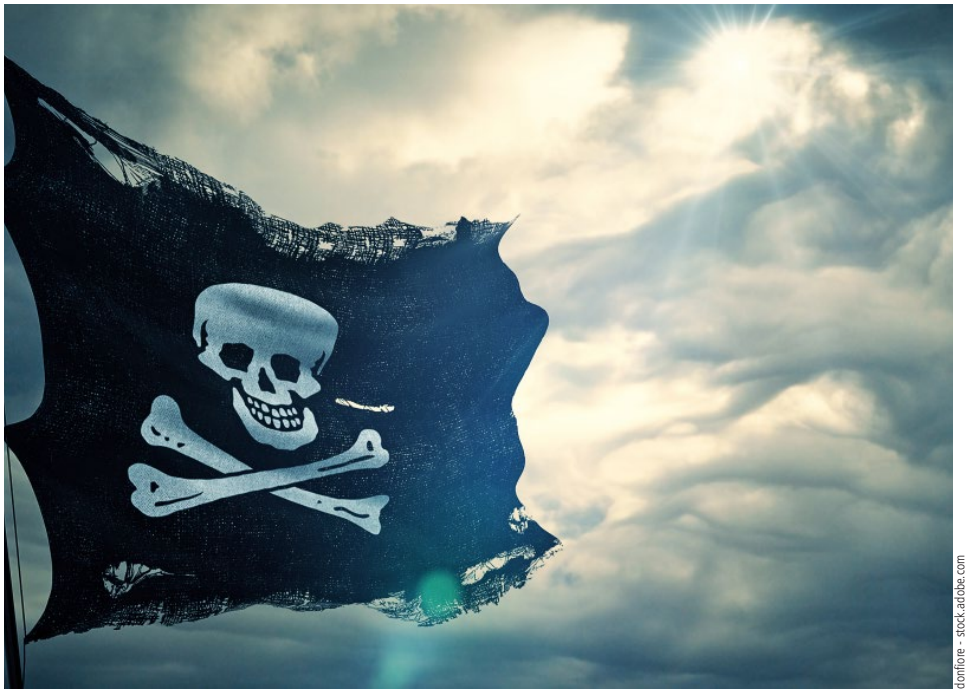
„Unter 100 Basispunkten möglich"
André Ofenloch, Factoringspezialist bei Gracher, spricht über die Eigenheiten und Vorteile des Finanzierungsinstruments.

Fitch steigt ins ESG-Rennen ein
Nach Moody's und S&P zieht Fitch am Markt für ESG-Ratings nach. Was die Ratingagentur vorhat, berichtet Gianluca Spinetti.

„Konnte keinen Mehrwert generieren"
Hufs Treasury-Chef Peter Helming über die Reise vom Excel-basierten Treasury hin zu einer zeitgemäßen Aufstellung des Autozulieferers

Die Cybercrimewelle rollt

Ransomware auf Rekordjagd / Treasury-Chefs verunsichert und besorgt



donfiore - stock.adobe.com

Hacker versuchen immer wieder, Unternehmen zu kapern und Beute zu machen. Immer öfter klappt es.

Die massive Hacker-Attacke kam im Dezember 2021 wie so oft für Laien etwas kryptisch daher: Es sei eine Schwachstelle namens „Log4Shell" in einer beliebten Java-Protokollierungsbibliothek gefunden worden, teilten IT-Spezialisten mit. Experten rund um die Welt waren sich einig: Es handelte sich um eine der größten Sicherheitsbedrohungen für Unternehmen seit Jahren. Hacker können die Schwachstelle leicht ausnutzen, der tatsächliche Schaden wird aber erst in den kommenden Monaten sichtbar.

Für Treasurer entstand durch „Log4Shell" ein typisches Problem. Sie kennen sich in den Untiefen der schwer verständlichen IT-Landschaft kaum aus, müssen ihre Abteilung aber auf Angriffe vorbereiten. „Log4Shell war ein Riesenthema bei uns", berichtet der Treasury-Chef eines Konzerns. „Wir wussten nicht, ob wir an allen Ecken sicher sind." Neben technischen Angriffen gibt es auch noch die vorwiegend auf Social Engineering basierenden Angriffsarten wie Fake President („CFO Fraud") oder Payment Diversion (Zahlungsumleitung). Mittlerweile gehen technische und soziale Attacken jedoch immer mehr Hand in Hand. Die Betrüger nutzen technische Lücken, um über sie wichtige Informationen abzugreifen. Diese nutzen sie später für einen Fake-President-Angriff oder eine Ransomware-Attacke. So auch bei „Log4Shell": Schnell kursierten Berichte, dass etwa chinesische Cyberkriminelle das Schlupfloch nutzten.

Auch die Ukraine-Krise sorgt für Cyberangriffe. „Wir sehen Angriffe, um Unternehmen und Behörden in der Ukraine abzulenken oder Unternehmen der kritischen Infrastruktur abzuschalten", sagt Florian Oelmaier, Prokurist bei der Sicherheitsberatung Corporate Trust. Verfassungsschutzämter würden momentan Warnungen verschicken. Ohnehin spiele Russland, wo wichtige Ransomware-Gruppen mutmaßlich ihren Sitz haben, eine entscheidende Rolle. „Russland zeigt keinerlei Interesse an einer Verfolgung", sagt er. Dadurch hätten die Täter einen Rückzugsort.

Immer wieder Russland

Die Hacker haben ein fast ideales Umfeld, die Geschäfte florieren. „Momentan ist viel Ransomware im Umlauf", berichtet Oelmaier. „Wir wissen von Lösegeldern in zweistelliger Millionenhöhe, die allein in den vergangenen Wochen gezahlt wurden. Das Geschäftsmodell der Angreifer funktioniert." Die Zahlen unterstreichen den Eindruck von Sicherheitsexperte Oelmaier: Eine Studie von Chainalysis hat ergeben, dass 2021 mehr als 600 Millionen US-Dollar an bekannte Ransomware-Adressen in Kryptowährungen ausgezahlt wurden. Zum Vergleich: 2016 wurden gerade einmal 24 Millionen Dollar verzeichnet. Da viele Zahlungen erst später bekannt werden, sind die Schätzungen für 2021 noch sehr konservativ.

Immer wieder warnen Experten und auch Banken davor, Lösegeld an die Kriminellen zu zahlen. Doch die Realität sieht anders aus, weiß Berater Oelmaier: „Natürlich gibt es Gesetze gegen Terrorismusfinanzierung, speziell für Unternehmen, die eine Tochter in einer US-Jurisdiktion haben." Doch der wirtschaftliche Druck sei meistens zu groß, da mit jedem Tag ohne System Umsätze in Millionenhöhe verlorengehen. Hinzu kommt, dass Kriminelle neuerdings vermehrt auf eine Dreifacherpressung setzen. „Sie verschlüsseln Daten, klauen diese und drohen mit einer Veröffentlichung", sagt Oelmaier. Neu sei, dass Hacker mittlerweile auch mit einer nachgelagerten Distributed Denial of Service („DDoS") drohen, um die Systeme erneut lahmzulegen.

Eine Überweisung per Kryptowährung ist daher oft die einzige Möglichkeit, die IT-Systeme aus den Klauen der Angreifer zu lösen. „Wir arbeiten dafür mit einer Bank zusammen, die sehr schnell die nötige Menge an Bitcoins besorgen kann", sagt Berater Oelmaier.

Komplettschutz unmöglich

Doch was können Treasurer tun, um sich und ihre Abteilungen zu schützen? Die meisten setzen auf regelmäßige Schulungen ihrer Mitarbeiter, um die größten Einfallstore durch die Schwachstelle Mensch zu schließen. So sei zum Beispiel wichtig zu wissen, was dazu führen kann, dass Bankdaten verändert werden. In einigen Fällen sind die Weiterbildungen sogar verpflichtend, wie DerTreasurer erfahren hat. „Wichtige Unterlagen wie Bank- und Notfallkontakte müssen ausgedruckt in der Schublade liegen", mahnt ein weiterer Treasurer. „Denn wenn die Server ausfallen, kann man auf nichts mehr zugreifen."

Auch ein Vieraugenprinzip sollten Treasury-Abteilungen als Standard etablieren. Hier ist eine klare Kommunikation an die Mitarbeiter wichtig: „Bei uns gibt es keinen Prozess, dass der CFO oder CEO anruft und um eine Überweisung bittet", sagt noch ein weiterer Treasury-Chef. Mitarbeiter müssten immer kritisch und genau hinschauen. Sorge bereitet Treasury-Experten indes das deutlich gestiegene Niveau der Angriffe. Durch Deep Fakes können beispielsweise Stimmen und sogar Videos täuschend echt gefälscht werden. Für Mitarbeiter ist es fast unmöglich, Fälschung und Original zu unterscheiden. Ein Treasurer konstatiert deshalb: „Hundertprozentige Sicherheit gibt es nicht." *jae*

Die für Treasurer relevanten Angriffsarten

Angriffsart	Beschreibung
Fake President	Betrüger geben sich fälschlich als Chef aus, zweigen Gelder ab
Payment Diversion	Kriminelle ändern Bankdaten, leiten Zahlungen um
Goods Diversion	Kriminelle ändern Stammdaten, leiten Gütersendungen um
Ransomware	Hacker verschlüsseln Systeme mit Trojaner, fordern Lösegeld
Phishing	Basis vieler Attacken, Hacker erlangen Zutritt zu Systemen bspw. über infizierte E-Mails

Quelle: DerTreasurer