Achtung, Betrüger!

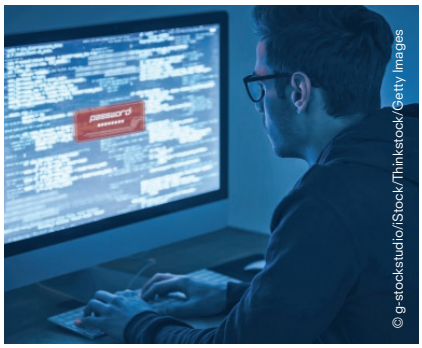
Unternehmen können jederzeit angegriffen werden – von innen und außen. Insbesondere der Zahlungsverkehr ist dabei das Ziel der Cyberkriminellen. Eine Systemlösung kann helfen, das Unternehmen zu schützen. Von Gregor Opgen-Rhein

In Zeiten gestiegener Cyberkriminalität ist Fraud-Prevention eine zentrale Aufgabe für jedes Unternehmen. Eines der beliebtesten Ziele der Angreifer ist der Zahlungsverkehr. Der Grund: die vielversprechenden Gewinnmargen. Dabei muss Angriffen von „innen" ebenso viel Aufmerksamkeit gewidmet werden wie den medienwirksamen Angriffen von „außen". Denn auch „unzufriedene" Mitarbeiter, die unbemerkt Unternehmenskonten eröffnen, Vollmachten ändern oder Konten schließen, können für erheblichen Schaden sorgen.

Unternehmen haben viele Möglichkeiten, sich vor Angriffen auf die Zahlungsprozesse zu schützen: Zur ersten Säule eines umfassenden Sicherheitskonzepts gehören technische Vorkehrungen wie die Verschlüsselung sämtlicher Datenströme und der Einsatz von Anti-Spyware-Programmen. Organisatorische Maßnahmen wie die Sensibilisierung der Mitarbeiter für CEO-Fraud-Versuche und die Einführung eines konsequenten Vieraugenprinzips bei der Zahlungserfassung und Stammdatenpflege bilden die zweite Säule.

Konten im Blick behalten

Die dritte Säule umfasst funktionale Optionen, etwa in der administrativen Kontoverwaltung. Im Fokus stehen dabei sowohl die eigenen Unternehmenskonten als auch die Kontoverbindungen der Geschäftspartner. Das höchste Sicherheitsniveau bei der Eröffnung und Schließung von



Ein Cyberangriff ist eine der größten Gefahren.

Konten sowie der Änderung von Vollmachten und Kontonummern kann dabei durch einen strukturierten, vordefinierten und mit verteilten organisatorischen Verantwortlichkeiten ausgestatteten Prozess erzielt werden.

Die Bankverbindung der Geschäftspartner unterliegt darüber hinaus weiteren, weitaus strengeren regulativen Anforderungen. Hier geht es vor dem Hintergrund der gesetzlichen Geldwäsche- und Sanktionsbestimmungen nicht nur darum, den Geschäftspartner einer Prüfung zu unterziehen. Auch die Bank des Geschäftspartners, respektive Zahlungsempfängers, könnte auf einer Liste stehen und muss ebenfalls permanent und nachweisbar einem Sanktionsscreening unterliegen.

Zugleich sollten Unternehmen die Zahlungsempfänger der operativen Zahlungsdateien auch gegen eine Positivliste prüfen, um so Zahlungen ausschließlich an interne, vorvalidierte Empfänger zu ermöglichen.

Eine weitere Maßnahme zur Schadensabwehr ist die Überwachung der Kontoauszüge: So könnte die Ursache für fehlende Auszüge oder Umsätze nicht nur auf technischen Fehlern in der Bereitstellung durch die Banken beruhen, sondern auch in der Verschleierung von auffälligen Abbuchungen. Systemlösungen sollten solche Auffälligkeiten aufdecken und somit wichtige Hinweise geben.

Durch die Kombination von technischen, organisatorischen und funktionalen Maßnahmen lassen sich operative Zahlungsprozesse und administrative Kontenverwaltungsprozesse inklusive sogenannter Denied Party Checks zu einem engmaschigen Netz der Fraud-Vermeidung knüpfen.

Eine Systemlösung für das elektronische Bank Account Management muss alle diese Features für das sogenannte Account-Lifecycle-Management unterstützen und bietet zugleich die Chance zur Zentralisierung, Standardisierung und Digitalisierung von sensiblen Prozessen. So kann sich ein Unternehmen vor Fraud-Angriffen schützen.

Gregor Opgen-Rhein
ist Key Account Manager bei Omikron Systemhaus in Köln.

gor@omikron.de