Cybercrime: Betrugsprävention im Zahlungsverkehr

Die Cyberkriminalität nimmt zu. Auch in den Finanzabteilungen wächst die Sorge. Der Einsatz moderner Technologie kann einen wichtigen Beitrag für besseren Schutz leisten.

Von Helmut Springer

Die Cyberkriminalität steigt. Je gezielter Hacker vorgehen, desto lauter wird die Forderung nach mehr Sicherheit. Insbesondere in der Finanzabteilung steigt die Anspannung, da es die Kriminellen oft auf Zahlungen und sensible Finanzdaten abgesehen haben. Auch Haftungsfragen spielen bei den Sorgen in der Finanzabteilung eine Rolle. Immer wieder müssen Finanzchefs, die ihre Pflichten verletzt haben, nach Betrugsfällen gehen. Aber auch Mitarbeiter, die tagein tagaus Zahlungen freigeben, sind besorgt: Würden sie einen Fake-President-Angriff rechtzeitig erkennen oder doch Millionen auf Konten von Betrügern überweisen? In letzter Zeit starten viele Unternehmen Initiativen, um die Sicherheit zu erhöhen. Dabei arbeiten Finanzabteilungen eng mit der IT-Abteilung und externen Sicherheitsexperten zusammen. Neben Sicherheitsprogrammen zählen auch Schulungen für Mitarbeiter für mehr Risikobewusstsein zu gängigen Instrumenten, um interne Prozesse transparenter und sicherer zu machen.

Transparente Cashflows

Auch Finanzabteilungen können einen wichtigen Beitrag zur Bekämpfung von Cyberkriminalität und Betrug leisten. Moderne Technologien helfen ihnen dabei. Finanzabteilungen, die unternehmensweite Kontostände und -bewegungen nicht kennen oder nur zeitverzögert bestimmen können, bemerken Cyberangriffe oft nicht oder erst dann, wenn es bereits zu spät ist. Treasury-Software hilft, weltweitBankkonten zu verwalten und Cashflows transparent zu machen. Zudem können Zahlungen zentral geplant, optimiert und abgewickelt werden. Somit kennt das Treasury alle Kontosalden und weiß, welche Zahlungen anstehen.

»In letzter Zeit starten viele Unternehmen Initiativen, um die Sicherheit zu erhöhen.«

Zahlungsverkehrssysteme werden nicht nur gehackt, um illegale Zahlungen zu tätigen, sondern auch, weil hier zahlreiche Informationen wie beispielsweise Kunden-, Lieferanten- und Mitarbeiterdaten zusammenfließen. Um es den Tätern möglichst schwer zu machen, ist es wichtig, strenge Autorisierungs- und Freigabeprozesse zu implementieren.

Auch hier können Treasury-Systeme helfen. Mit den Funktionalitäten im Zahlungsverkehr können Finanzverantwortliche einfach Benutzerprofile und -rollen, Zeichnungsberechtigungen, Freigabeprozesse, Autorisierungsstufen und Limite für Zahlungen konfigurieren. Zusätzlich helfen Überwachungssysteme wie Limit-Monitoring, Blacklists und Whitelists von Zahlungsempfängern, die Kontrolle weiter zu steigern. Schließlich können durch Warnmeldungen von integrierten Anti-Fraud-Radars Änderungen bei kritischen Daten, Manipulationen und Betrugsversuche rasch aufgedeckt werden. Viele Unternehmen arbeiten heute mit Sicherheitsexperten zusammen. Diese simulieren Cyberangriffe, um Sicherheitslücken in internen Prozessen und Systemen aufzudecken. Da Systemanbieter ihre Lösungen im Zahlungsverkehr laufend weiterentwickeln müssen, um aktuelle Sicherheitsstandards zu erfüllen, sind Finanzabteilungen, die aktuelle Software einsetzen und sie regelmäßig updaten, deutlich besser geschützt. Wer das Thema Sicherheit auslagern will, kann ein cloud-basiertes Treasury-System einsetzen. Dann kümmert sich der Systemanbieter um Hardware, Software und regelmäßige Updates.

Im Zahlungsverkehr ist Sicherheit ein zentrales Thema. Moderne Treasury-Software unterstützt Finanzabteilungen dabei, Sicherheitslücken durch Zentralisierung, Automatisierung und Kontrollmechanismen zu schließen und so Cyberattacken und auch interne Betrugsversuche zu verhindern. //

Helmut Springer
ist Vice President und Prokurist bei Reval in Graz.

helmut.springer@reval.com