Cybercrime mit System abwehren

Hacker und Betrüger nehmen deutsche Unternehmen ins Visier. Viele Treasurer erhöhen deshalb ihre Anstrengungen, um ihre Finanzdaten zu schützen und die Workflows sicherer zu gestalten.

Von Helmut Springer

Der chinesisch-österreichische Luftfahrzulieferer FACC wurde mit der Betrugsmasche Fake President um 50 Millionen Euro erleichtert. Das ist leider kein Einzelfall. Viele Unternehmen werden zur Zielscheibe. Betrüger geben sich als Geschäftsführer aus und versuchen, bei einem Mitarbeiter in der Buchhaltung die Überweisung hoher Summen zu veranlassen. Den Fake-President-Trick gibt es als klassische Betrugsmasche und auch als lange geplantes Cybercrime, bei dem die Unternehmen virtuell ausgespäht werden.

„Cyberkriminalität macht vor niemandem Halt“, sagt ein Treasurer eines betroffenen Unternehmens, der anonym bleiben möchte. Auch hier versuchten Hacker mit einer gefälschten Geschäftsführer-E-Mail an die Buchhaltung auf die Unternehmenskasse zuzugreifen. Mit mehreren E-Mails und Telefonanrufen übten die Betrüger Druck aus. Da die für eine vermeintliche Auslandsakquise angeforderte Summe in das Überweisungsschema des Unternehmens fiel, schöpfte vorerst niemand Verdacht. Auch bei der Bank wäre die Zahlung unter dem Radar geblieben.

Erst als das mit zwei gefälschten Unterschriften versehene Formular für die Auslandsüberweisung nicht exakt der internen Vorlage entsprach, konnte der Fall von einer geistesgegenwärtigen Mitarbeiterin aufgedeckt werden. „Der Angriff war gezielt und von langer Hand geplant“, kommentiert der Finanzexperte.

Nach der abgewehrten Cyberattacke startete das deutsche Unternehmen eine Anti-Fraud-Initiative. In enger Zusammenarbeit mit der IT-Abteilung werden nun unternehmensweite Guidelines, Prozesse und IT-Systeme überprüft. Im Rahmen des Sicherheitsprojekts werden sämtliche Treasury-Prozesse durchleuchtet, um die sensiblen Finanzdaten noch besser zu schützen. Auf die Schnittstellen zwischen Abteilungen, Gesellschaften und Systemen wird dabei besonders geachtet, da diese die größten Sicherheitsrisiken bergen.

Der international tätige Konzern setzt im Treasury auf Transparenz: Die Finanzabteilung arbeitet seit Jahren mit einem integrierten Treasury-System. Hier werden sämtliche Cashflows zentral erfasst und gesteuert. Somit wissen die Finanzexperten jederzeit, wie viel Geld der Konzern bei welcher Bank hat und welche Zahlungen geplant sind.

» Transparente Finanzzahlen sind ein wichtiger Schritt zur Abwehr von Cyberattacken.«

Transparente Finanzzahlen sind ein wichtiger Schritt zur Abwehr von Cyberattacken, da fehlende Geldbeträge oder ungeplante Zahlungen schneller entdeckt werden können.

Software als Schutz

Aber auch Workflows können mit professioneller Treasury-Software gesteuert werden. Um den Zahlungsverkehr so sicher wie möglich zu machen, setzt das Treasury des Familienunternehmens auf ein System aus Berechtigungen, Unterschriftsregelungen, Zahlungsfreigaben, Audit-Trails, Sanktionslisten, White Lists und einem Anti-Fraud-Radar. Auch Schnittstellen zu Bank- und ERP-Systemen sind automatisiert.

Informierte Mitarbeiter

„Systemseitig haben wir eine hohe Sicherheit“, meint der Treasurer. Bleibt noch das operationelle Risiko. Der Konzern setzt auf Mitarbeiterschulungen, um Prozesse weiter zu verbessern. Da sich die Praktiken der Cyberkriminellen laufend ändern, sollen in Zukunft regemäßig Schulungen stattfinden, in denen aktuelle Betrugsfälle besprochen werden.

Viele Unternehmen starten mittlerweile Initiativen, um Sicherheitslücken zu schließen, die durch veraltete Technologien, ungeschultes Personal und unzureichende Kontrolle von Cashflows und Treasury-Prozessen entstehen. Einige investieren in neue Finanzsoftware und Awareness-Programme.

Doch der Treasurer des betroffenen Unternehmens sieht weiteren Verbesserungsbedarf: „Mittelfristig müssen Corporates, Banken und Systemanbieter enger zusammenarbeiten, um Fraud nachhaltig zu bekämpfen.“ //

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

helmut.springer@reval.com