CYBERSICHERHEIT UND REQUEST-TO-PAY

Ein neuer Kanal zur Zahlungsaufforderung

Mit dem neuen europaweiten Standard Request-to-Pay (R2P) kann eine standardisierte Zahlungsaufforderung vom Zahlungsempfänger an den Zahler gesendet werden, beispielsweise auf dessen mobiles Endgerät. Eine solche Zahlungsaufforderung kann vom Zahler unmittelbar freigegeben oder abgelehnt werden, wobei hier eine starke Kundenauthentifizierung gewährleistet werden muss. Mit der Freigabe wird anschließend ohne weitere Eingaben direkt eine SEPA-Überweisung ausgelöst.

HERAUSFORDERUNG

Derzeit erhalten Ihre Kunden Zahlungsaufforderungen in erster Linie als Rechnung in Papierform oder per E-Mail. Wiederkehrende Zahlungen werden darüber hinaus meist per Lastschrift abgewickelt. Mit Request-to-Pay werden in naher Zukunft viele dieser Zahlungen direkt über die Bankeninfrastruktur bei Ihren Kunden angefragt. Das sorgt nicht nur für mehr Komfort und Kontrolle bei der Zahlungsauslösung, sondern stellt Banken auch vor ganz neue Herausforderungen im Bereich Cybersicherheit.

Betrugsversuche mit Zahlungsverkehrsbezug haben sowohl online als auch offline in den vergangenen Jahren stark zugenommen. Unter anderem durch Phishing, also den Versuch, Kunden zur Eingabe von PIN und TAN auf gefälschten Webseiten zu bewegen, oder durch Methoden, die Bankkunden direkt zur Auslösung von Zahlungen verleiten, sei es durch den Versand gefälschter Rechnungen (Spoofing) oder soziale Manipulationen (Social Engineering).

BEISPIEL 1

Ein Trickbetrüger setzt eine Mitarbeiterin der Buchhaltung telefonisch unter Druck, schnell eine Zahlung im Auftrag des Geschäftsführers durchzuführen („CEO-Fraud“). Durch Request-to-Pay kann der Betrüger die Hemmschwelle des Opfers zur Zahlung weiter senken.

Mit Request-to-Pay entsteht nun die neue Situation, dass Bankkunden prinzipiell von jedem Bankkonto innerhalb des SEPA-Raums eine Zahlungsaufforderung erhalten können. Da sie über die Bankeninfrastruktur zugestellt und im gesicherten Onlinebanking angezeigt wird, gilt sie grundsätzlich als vertrauenswürdiger als beispielsweise eine E-Mail. Dadurch steigt sowohl das Risiko für den Kunden, betrügerische Zahlungsaufforderungen ohne sorgfältige Prüfung freizugeben, als auch das Risiko für die Bank, hierdurch einen Reputationsschaden zu erleiden.

BEISPIEL 2

Ein Betrüger kauft im Darknet Listen geleakter Kontonummern und versendet per Request-to-Pay gefälschte Zahlungsaufforderungen, die auf den ersten Blick denen eines großen Rechnungsstellers ähneln und dadurch legitim wirken.

WIE WIR HELFEN KÖNNEN

Schritt 1

KONZEPTION

Wir überprüfen vorhandene Sicherheitsmaßnahmen und identifizieren Lücken.

Schritt 2

BERATUNG

Wir beraten Sie in einem persönlichen Gespräch und unterbreiten Ihnen Lösungsvorschläge, wie sie diese Lücken schließen.

Schritt 3

UMSETZUNG

Wir setzen verschiedenste Cybersicherheitsmaßnahmen um.

WARUM SYRACOM?

syracom verfügt über langjährige Erfahrung im Bereich Cybersicherheit und Banking. Mit einem umfassenden Partnernetzwerk bündelt das Beratungshaus optimal Experten und Know-how. syracom berät Sie dabei unabhängig bei der Lösungsfindung und versteht sich als ganzheitlicher Begleiter bei der Konzeption und Umsetzung. Sie profitieren von umfassendem Security-Wissen, das neben Social Engineering auch weitere essenzielle Bausteine zur Erhöhung der Informationssicherheit umfasst.

ÜBER SYRACOM

syracom ist ein unabhängiges Business- und IT-Beratungshaus. Mit fachlichem und technischem Know-how entwickeln wir zukunftsfähige Lösungen nach Maß und begleiten unsere Kunden auf dem Weg durch die digitale Transformation: *business efficiency engineering* – sicher, nachhaltig, effizient.

Das Beratungshaus wurde 1998 gegründet und ist Teil der Consileon-Gruppe.

Frank Hoffmann

Head of IT Security

syracom AG
Otto-von-Guericke-Ring 15
65205 Wiesbaden (Germany)
Fon: +49 6122 9176 0

frank.hoffmann@syracom.de
www.syracom.de