expertenReport

Quelle: experten.de / KI-generiert

Revolut-Datenleck: Wenn die Behörden-Mail selbst zum Sicherheitsrisiko wird

Dirk Stein

Ein Cyberangriff ohne Einbruch in die IT-Systeme: Beim Finanzdienstleister Revolut haben Angreifer offenbar einen besonders sensiblen Prozess ausgenutzt und das Unternehmen mit gefälschten Behördenanfragen zur Herausgabe vertraulicher Kundendaten bewegt. Nach Berichten der Financial Times wurden 680 Kunden über den Vorfall informiert. Betroffen sein können nicht nur persönliche Angaben, sondern auch Ausweisdokumente, Konto- und Transaktionsinformationen. Der Fall zeigt damit ein Sicherheitsproblem, das weit über Revolut hinausreicht. Denn Banken und Versicherer müssen nicht nur ihre eigenen Systeme gegen Angriffe schützen, sondern zunehmend auch die Identität und Berechtigung vermeintlich vertrauenswürdiger Kommunikationspartner überprüfen.

Authentischer Absender bedeutet nicht autorisierte Anfrage

Banken, Versicherer und andere Finanzunternehmen erhalten regelmäßig Auskunftsersuchen von Strafverfolgungs-, Aufsichts- oder anderen Behörden. Liegen die entsprechenden rechtlichen Voraussetzungen vor, müssen sie personenbezogene Daten übermitteln. Dafür existieren interne Prozesse, Zuständigkeiten und Prüfmechanismen. Gleichzeitig können gerade behördliche Anfragen unter Zeitdruck stehen, etwa wenn Ermittler Informationen kurzfristig benötigen.

Damit entsteht eine Konstellation, die für Social Engineering besonders interessant ist. Eine Nachricht kommt scheinbar von einer vertrauenswürdigen Institution, der Absender tritt mit entsprechender Autorität auf und fordert Informationen möglicherweise mit einer gewissen Dringlichkeit an. Stammt die Nachricht zusätzlich von einer tatsächlich zu einer Behörde gehörenden Domain, fallen wesentliche Warnsignale klassischer Phishing-Angriffe weg.

Der Revolut-Fall macht deshalb einen entscheidenden Unterschied sichtbar. Die technische Authentizität einer E-Mail beantwortet noch nicht die Frage, ob die Person hinter dieser Nachricht tatsächlich berechtigt ist, die verlangten Kundendaten anzufordern. Wird beispielsweise ein legitimes Behördenkonto kompromittiert, kann der Angreifer dessen Vertrauensstellung nutzen. Die Nachricht ist dann möglicherweise technisch „echt“, die Anfrage selbst aber dennoch betrügerisch.

Für das Risikomanagement von Finanzunternehmen bedeutet dies, dass die Kontrolle des Absenders allein nicht ausreicht. Je sensibler die angeforderten Informationen sind, desto wichtiger wird eine zweite, vom ursprünglichen Kommunikationsweg unabhängige Prüfung. Dazu können verifizierte Ansprechpartner, Rückrufe über bereits bekannte Kontaktdaten, gesicherte Behördenportale oder zusätzliche interne Freigaben gehören. Bei besonders umfangreichen Datensätzen bietet sich zudem ein Vier-Augen-Prinzip an. Entscheidend ist, dass ein kompromittiertes externes E-Mail-Konto nicht automatisch zur Eintrittskarte in den Datenbestand eines Finanzunternehmens wird.

Besonders sensible Kombination von Kundendaten

Revolut hatte zunächst lediglich von einer sehr begrenzten Zahl betroffener Kunden gesprochen. Nach Informationen der Financial Times wurden inzwischen 680 Kunden über den Vorfall informiert. Die absolute Zahl erscheint angesichts der Größe des Unternehmens zunächst überschaubar. Für die Risikobewertung ist allerdings weniger die Zahl der Datensätze entscheidend als deren Inhalt.

Medienberichten zufolge können Namen, Geburtsdaten, Telefonnummern und Wohnanschriften betroffen sein. Hinzu kommen je nach Kunde Kopien von Reisepässen oder Führerscheinen, Selfies aus Identifizierungsverfahren, IBANs sowie Informationen über Kontobewegungen und Transaktionen. Aus einzelnen personenbezogenen Angaben wird dadurch ein umfangreiches Identitäts- und Finanzprofil.

Gerade diese Kombination erhöht das Missbrauchspotenzial erheblich. Mit authentischen persönlichen und finanziellen Informationen lassen sich beispielsweise Phishing-Nachrichten wesentlich glaubwürdiger gestalten. Ein vermeintlicher Bankmitarbeiter, der tatsächliche Kontodaten, frühere Transaktionen oder persönliche Angaben nennen kann, besitzt gegenüber dem Opfer einen erheblichen Vertrauensvorsprung. Auch Identitätsbetrug wird problematischer, wenn Kriminelle neben den Stammdaten gleichzeitig über Ausweisdokumente und Bilder aus Identifizierungsverfahren verfügen.

Für die Betroffenen besteht das Risiko deshalb nicht erst dann, wenn die Informationen öffentlich im Internet erscheinen. Bereits die Weitergabe an Kriminelle kann die Grundlage für weitere Angriffe bilden. Betroffene Kunden müssen entsprechend längerfristig mit gezielten Betrugsversuchen rechnen, bei denen die Täter genau jene Informationen einsetzen können, die ursprünglich zur Identifikation und Absicherung des Kunden dienen sollten.

Aus dem Datenleck wird ein Erpressungsfall

Zusätzliche Brisanz erhält der Vorfall durch Berichte über eine Erpressung. Nach Informationen der Financial Times sollen die mutmaßlichen Täter damit gedroht haben, die erlangten Informationen zu veröffentlichen, sollte Revolut kein Lösegeld zahlen. Damit nähert sich der Fall in seinen Folgen klassischen Data-Extortion-Angriffen an, obwohl der ursprüngliche Angriffsweg ein anderer gewesen sein soll.

Bei einem typischen Ransomware-Angriff verschaffen sich Kriminelle zunächst Zugang zur IT-Infrastruktur, kopieren Daten und verschlüsseln häufig zusätzlich Systeme. Anschließend versuchen sie, das Unternehmen mit der Drohung einer Veröffentlichung unter Druck zu setzen. Im Revolut-Fall mussten die Täter nach bisherigem Kenntnisstand hingegen keine Kundendatenbank selbst auslesen. Sie brachten das Unternehmen offenbar dazu, die gewünschten Informationen im Rahmen vermeintlicher Behördenanfragen bereitzustellen.

Für die Schadenswirkung macht dieser Unterschied nur bedingt einen Unterschied. Sobald vertrauliche Kundeninformationen in den Händen von Kriminellen liegen und als Druckmittel eingesetzt werden können, entstehen vergleichbare Herausforderungen: forensische Untersuchungen, Datenschutzmeldungen, Kundeninformationen, Rechtsberatung, Krisenkommunikation und möglicherweise regulatorische Konsequenzen.

Das britische Information Commissioner’s Office beschäftigt sich Medienberichten zufolge bereits mit dem Vorfall. Für die weitere Bewertung dürfte insbesondere relevant sein, welche Verfahren Revolut für Behördenanfragen vorgesehen hatte, wie die Legitimation der Anfragenden überprüft wurde und ob die vorgesehenen Kontrollen im konkreten Fall eingehalten wurden.

Cyberversicherer müssen über den klassischen Hackerangriff hinausdenken

Für die Versicherungswirtschaft ist der Fall aus einem weiteren Grund bemerkenswert. Cyberversicherungen werden häufig anhand klassischer Angriffsszenarien

diskutiert: Ein Angreifer dringt in ein Unternehmensnetzwerk ein, stiehlt Daten, verschlüsselt Systeme und fordert Lösegeld. Moderne Cyberrisiken lassen sich jedoch zunehmend schlechter in dieses einfache Schema einordnen.

Was gilt beispielsweise, wenn ein Unternehmen technisch überhaupt nicht kompromittiert wurde, ein Mitarbeiter aber aufgrund einer professionell manipulierten Behördenanfrage vertrauliche Informationen an einen unberechtigten Empfänger übermittelt? Der daraus entstehende Schaden kann erheblich sein, obwohl weder Schadsoftware installiert noch ein Sicherheitssystem technisch überwunden wurde.

Für Versicherer und Makler rücken damit die konkreten Bedingungen einer Cyberdeckung in den Mittelpunkt. Entscheidend kann sein, wie Datenschutzverletzungen, Social Engineering, Datenoffenlegung und Cybererpressung definiert sind und welche Ausschlüsse oder Obliegenheiten greifen. Ebenso relevant ist die Frage, welche organisatorischen Sicherheitsmaßnahmen Versicherer bei ihren Firmenkunden voraussetzen. Ein Unternehmen kann über moderne technische Schutzsysteme verfügen und trotzdem verwundbar bleiben, wenn für besonders sensible Datenherausgaben keine belastbaren Verifikations- und Freigabeprozesse bestehen.

Der Fall verdeutlicht damit zugleich eine Entwicklung im Cyber-Underwriting. Die Qualität eines Risikos lässt sich nicht ausschließlich anhand technischer Kriterien wie Multi-Faktor-Authentifizierung, Backup-Strategie, Endpoint Detection oder Patchmanagement beurteilen. Auch Geschäftsprozesse, Berechtigungskonzepte und die Behandlung außergewöhnlicher externer Anfragen können darüber entscheiden, ob ein Social-Engineering-Versuch erfolgreich ist.

DORA richtet den Blick auf die operationelle Widerstandsfähigkeit

Für europäische Finanzunternehmen passt der Vorfall zudem in die regulatorische Entwicklung der vergangenen Jahre. Mit dem Digital Operational Resilience Act (DORA) hat die Europäische Union die Anforderungen an die digitale operationelle Widerstandsfähigkeit des Finanzsektors deutlich ausgeweitet. Im Mittelpunkt steht nicht allein der Schutz einzelner Systeme, sondern ein umfassender Umgang mit Informations- und Kommunikationstechnologierisiken.

Der Revolut-Fall verdeutlicht, warum dieser breitere Ansatz notwendig ist. Technische Schutzmaßnahmen können verhindern, dass Angreifer unmittelbar in die Systeme eines Unternehmens eindringen. Sie verhindern jedoch nicht automatisch, dass legitime Geschäftsprozesse manipuliert werden. Wo Mitarbeiter aufgrund ihrer Funktion Daten herausgeben dürfen oder sogar müssen, wird die Gestaltung des Prozesses selbst zum Bestandteil der Informationssicherheit.

Das gilt insbesondere für die Kommunikation mit Institutionen, denen Unternehmen grundsätzlich vertrauen müssen. Behörden, Aufsichtsstellen, Rechtsanwälte oder externe Dienstleister können über legitime Kommunikationskanäle verfügen. Wird einer dieser Kanäle kompromittiert, verschiebt sich das Sicherheitsproblem vom technischen Zugang zur Frage der Berechtigung. Zero Trust darf deshalb nicht an der Unternehmensgrenze enden.

Das schwächste Glied muss nicht im eigenen Unternehmen sitzen

Über Jahre galt in der IT-Sicherheit der Grundsatz, dass ein Unternehmen nur so sicher ist wie sein schwächstes Glied. Der Revolut-Vorfall zeigt, dass dieses schwächste Glied inzwischen außerhalb der eigenen Organisation liegen kann. Banken und Versicherer kommunizieren mit einer Vielzahl externer Institutionen, Dienstleister und Behörden. Aus diesen Verbindungen entsteht ein Netzwerk gegenseitigen Vertrauens, das für Angreifer ebenso interessant sein kann wie die technische Infrastruktur eines einzelnen Unternehmens.

Für Kriminelle ist es schließlich nicht zwingend erforderlich, den am besten geschützten Teilnehmer eines solchen Netzwerks anzugreifen. Unter Umständen genügt es, einen Kommunikationspartner zu kompromittieren, dessen Identität bei anderen Organisationen besondere Rechte, beschleunigte Verfahren oder zumindest einen Vertrauensvorschuss auslöst.

Genau darin liegt die über Revolut hinausgehende Bedeutung des Falls. Unternehmen müssen nicht nur überprüfen, ob eine Nachricht technisch von dem Absender stammt, den sie vorgibt. Sie müssen bei sensiblen Vorgängen zusätzlich feststellen können, ob der konkrete Absender tatsächlich berechtigt ist, die verlangte Handlung auszulösen. Das ist weniger spektakulär als die Abwehr eines Hackerangriffs, kann für den Schutz vertraulicher Kundendaten aber ebenso entscheidend sein.

Für Banken und Versicherer entsteht daraus eine unbequeme Konsequenz: Selbst eine hervorragend abgesicherte eigene IT kann nicht verhindern, dass das Vertrauen in einen

externen Partner missbraucht wird. Informationssicherheit endet deshalb nicht mehr an der Firewall. Sie entscheidet sich zunehmend dort, wo Menschen, Prozesse und vermeintlich vertrauenswürdige Institutionen miteinander kommunizieren.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4951901/Revolut-Datenleck-Wenn-die-Behoerden-Mail-selbst-zum-Sicherheitsrisiko-wird/