Umfassende E-Mail-Sicherheit im Gesundheitswesen

Betrügerische E-Mails werden vermehrt zur Gefahr, gerade im hektischen Berufsalltag im Healthcare-Sektor. Klassische E-Mail-Sicherheitslösungen erkennen solche Angriffe nicht immer zuverlässig. Auf Business E-Mail Compromise spezialisierte Lösungen und spezifische Anwenderschulungen schaffen ein Mehr an Sicherheit, schützen die Reputation und unterstützen den reibungslosen Betrieb.

Zahlreiche Analysen bestätigen es klar: Cyberangriffe via E-Mail machen den mit Abstand grössten Teil der Attacken aus. Dies haben das Gros der Unternehmen und Organisationen erkannt und schützen den E-Mail-Verkehr mithilfe eines E-Mail-Security-Gateways von Anbietern wie Proofpoint – so auch Universitätsspitäler in der Schweiz. Das Gateway blockiert Nachrichten zuverlässig, die mit Links zu bösartigen Websites oder Anhängen mit Schadcode aufwarten. Ein weiteres Sicherheitselement ist die Verschlüsselung und elektronische Signierung der E-Mails. Diese Aufgaben werden ebenfalls vom Gateway wahrgenommen oder durch einen spezialisierten Anbieter umgesetzt – im Schweizer Gesundheitswesen ist dies etwa das HIN-Netzwerk.

Betrug zunehmend relevant

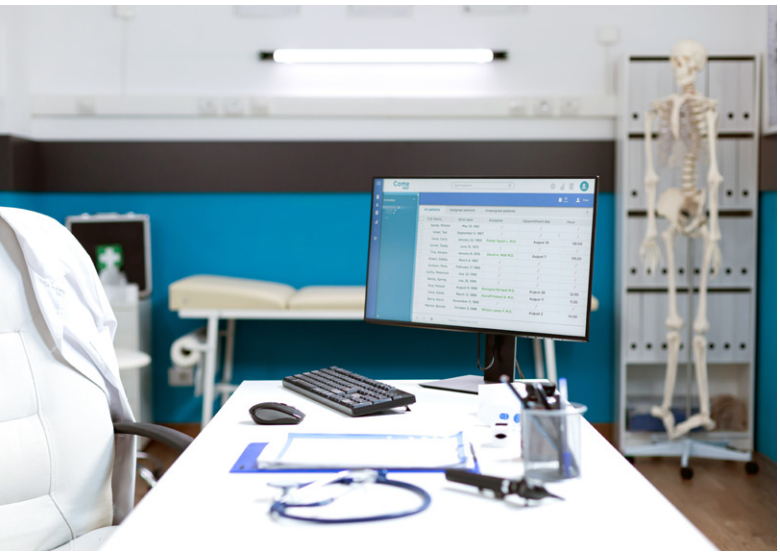
Unter den E-Mail-basierten Cyberbedrohungen sind klassische, breit gestreute Spammails sowie per Attachment verteilte Malware heute weniger relevant, weil sie von E-Mail-Security-Gateways gut unterbunden werden. Den Löwenanteil der E-Mail-Bedrohungen machen betrügerische Nachrichten aus. Dies zeigt etwa ein Blick auf die aktuellen Zahlen des Nationalen Zentrums für Cybersicherheit (NCSC): In Woche 14/2022 gingen zum Beispiel 329 Meldungen zu E-Mail-Betrug ein, während Spam mit 60 und Phishing mit 50 Meldungen massiv darunterlagen. Via E-Mail empfangene Schadsoftware wurde in dieser Woche nur zweimal gemeldet.

Betrügerische E-Mails, oft in dringlichem Ton abgefasst und vermeintlich von Vorgesetzten stammend, richten sich gezielt an bestimmte Mitarbeitende oder Abteilungen und sollen diese zum Beispiel zu illegitimen Geldüberweisungen oder zur Weitergabe von Daten an vermeintlich echte Lieferanten und andere Geschäftspartner verleiten. Die Angreifer gehen dabei in aller Regel dreist beziehungsweise clever vor. So ist es beispielsweise schon vorgekommen, dass eine Personalabteilung eine gefälschte, angeblich von einem eigenen Mitarbeiter stammende Nachricht mit der Information erhielt, sein Lohn sei künftig auf ein anderes Konto zu überweisen – das selbstverständlich nicht dem betroffenen Mitarbeitenden gehörte. Im IT-Jargon spricht man dabei von Business E-Mail Compromise (BEC) oder, falls es sich um gefälschte Mails aus der Führungsebene handelt, um CEO-Betrug.

Diese Art von Betrug hat auch im Healthcare-Sektor hohe Relevanz. In Spitälern, Arztpraxen und anderen Gesundheitsorganisationen sind zahlreiche Mitarbeitende tätig, die Informationen via E-Mail austauschen. Sie sind oft nicht spezifisch auf Cybersicherheit sensibilisiert oder haben im typischerweise hohen Arbeitsstress nicht die Zeit, Nachrichten genauer unter die Lupe zu nehmen. Stattdessen antworten sie reflexartig. Dabei sind oft höchst sensible Patientendaten involviert. Zudem kann eine an einen Betrüger bezahlte Lieferantenrechnung massive finanzielle Folgen haben.

Display Name Spoofing, Doppelgänger-Domänen und Domain Spoofing

Cyberkriminelle bedienen sich bei ihren BEC-Aktivitäten unter anderem dreier Mechanismen:



- Beim **Display Name Spoofing** erscheint der Name des Absenders, die dem Empfänger angezeigt wird, als echt und bekannt, obwohl die Nachricht von einer anderen E-Mail-Adresse stammt.
- **Doppelgänger-Domänen** sind Domains, die fast genau gleich benannt sind wie die korrekte Domäne, mit ganz kleinen Unterschieden wie etwa einem zusätzlichen oder fehlenden Buchstaben – zum Beispiel abcc.ch statt abc.ch. Solche Differenzen übersieht man im hektischen Alltag rasch einmal.
- Beim **Domain Spoofing** nutzt der Angreifer die Domain des angegriffenen Unternehmens oder die Domäne eines Geschäftspartners – oft inklusive des Corporate Designs des vorgeblichen Absenders –, damit die versendeten betrügerischen E-Mails als legitim erscheinen.

Unabhängig vom genutzten Mechanismus und den Folgen sind BEC-Angriffe besonders gefährlich, weil sie vertraute Namen und Organisationen nutzen und dabei keine schädlichen Dateien oder betrügerischen Links verschickt werden. Der Text der Nachricht genügt, um beim angezielten Mitarbeitenden die gewünschte Reaktion auszulösen. Manche E-Mail-Security-Gateways können solche Betrugsfälle nur schwer entdecken.

Abwehrmassnahmen gegen E-Mail-Betrug

Ein Weg, betrügerische E-Mails zu identifizieren, ist die Authentifizierung der Absender-Domäne, die in der «Mail from:»-Adresse enthalten ist (die nicht der Domain entsprechen muss, die dem Empfänger angezeigt wird). Dabei werden nur Nachrichten, die von klar als vertrauenswürdig erkannten und in einer Whitelist erfassten Domains eintreffen, an die Empfänger weitergeleitet.

Bei der Authentifizierung kommen mehrere Verfahren zum Einsatz: Mit dem Sender Policy Framework (SPF) werden Domains anhand der IP-Adresse verifiziert, die Methode DKIM (Domain Keys Identified Mail) setzt auf digitale Signatur. Signiert werden dabei sowohl die «Mail from:»-Domain als auch die Nachricht selbst. Beide Verfahren haben ihre Vor- und Nachteile, was im Fall von SPF zu fälschlich als betrügerisch identifizierten Domains führen kann, zum Beispiel bei weitergeleiteten echten Mails. DKIM dagegen wird nicht von allen Mailservern unterstützt.

Das E-Mail-Authentifizierungsprotokoll DMARC (Domain-based Message Authentication, Reporting and Conformance) soll gewährleisten, dass die Absender-Domains vor betrügerischer Nutzung geschützt werden und Spoofing verunmöglicht wird. Dabei lässt sich auch festlegen, dass mindestens eine der Prüfungen – SPF oder DKIM – ergibt, dass die «Mail from:»-Domain derjenigen entspricht, die der Empfänger zu sehen bekommt.

Der beste Schutz ergibt sich, sowohl für die eigenen E-Mail-Nutzer als auch für Empfänger ausserhalb der Organisation, wenn alle drei Technologien kombiniert werden. Die oben stehende kurze Beschreibung lässt es jedoch schon vermuten: Die Einrichtung von SPF, DKIM und DMARC ist nicht ganz trivial. Proofpoint vereinfacht die DMARC-Implementierung mit seiner Lösung Email Fraud Defense (EFD) massgeblich – erstens durch einen geführten Schritt-für-Schritt-Workflow und zweitens durch die Unterstützung mit spezialisierten Experten, die das Projekt in jeder Phase des Rollouts begleiten. Dies beispielsweise beim Erfassen der legitimen E-Mail-Absender und Absender-Domains.

EFD schützt die Organisation und ihre Reputation vor Schäden durch E-Mail-Betrugsversuche und schafft Transparenz über Doppelgänger-Domänen und alle ausgehenden E-Mails. Dazu verifiziert EFD unter anderem alle Lieferanten, identifiziert von Dritten registrierte Doppelgänger-Domänen automatisch und stellt ein Tool zur Verfügung, um solche Domains rasch durch die Registrierungsstelle entfernen zu lassen.

Nutzer im Mittelpunkt

Die beste technische Abwehr bewahrt indes nicht davor, dass ungenügend geschulte Mitarbeitende in der Hitze des Gefechts auf Betrugs- und Phishing-E-Mails eingehen. Es ist deshalb für Organisationen jeder Branche und Grösse nachgerade Pflicht, alle Mitarbeitenden mit dem Optimum an Cybersicherheitswissen zu versorgen. Auch dafür bietet Proofpoint eine bewährte Lösung: Proofpoint Security Awareness Training bietet jedem Mitarbeitenden die passenden Schulungen und Simulationen, hilft bei der Identifizierung von Risiken und stellt sicher, dass die Anwender richtig reagieren, wenn sie mit einem ausgeklügelten Cyberangriff konfrontiert sind.