ALLGEIER secion

E-Mail-Sicherheit

Sechs bewährte Regeln für mehr E-Mail-Sicherheit

Das in Organisationen und Unternehmen nach wie vor meistverwendete Kommunikationsmittel ist noch immer die E-Mail. Es überrascht daher nicht, dass erfolgreiche Cyberangriffe zu über 90 Prozent mit einer vermeintlich harmlosen E-Mail beginnen. Die Schwachstelle ist dabei in fast allen Fällen ausnahmslos dieselbe: der Mensch.

Gefälschte Absender-Identitäten erhöhen dabei die Chancen, dass Malware-Anhänge geöffnet werden. Das perfide Spiel der CEO-Frauds ist so erfolgreich, weil sich die Angreifer bereits im Vorfeld genauestens und detailliert in die Gegebenheiten des Unternehmens einarbeiten. Mit den folgenden sechs Regeln schützen Sie sich effektiv vor der Bedrohung durch Ransomware, Phishing, virenverseuchte Attachments und Co.

Regel 1:
Plausibilitätscheck und richtige DKIM-Konfigurierung

Viele Angriffe über E-Mails können bereits vereitelt werden, indem der Adressat vor dem Öffnen einen **Plausibilitätscheck** durchführt. Überprüfen Sie zunächst, ob der Absender bekannt und der Betreff sinnvoll ist, sowie ob ein Anhang zu diesem Thema erwartet wird. **Offensichtliche Spam- und Phishing-E-Mails löschen** Sie am besten sofort – ohne sich deren Inhalt weiter anzusehen. Phishing-Mails erkennen Sie u. a. an Formulierungen, die Zeitdruck erzeugen sollen oder drastische Konsequenzen androhen. Sollten Sie doch einmal versehentlich eine echte Mail gelöscht haben, wird sich die bekannte Person sicherlich den Kontakt im Nachgang zu Ihnen suchen.

Aus technischer Sicht liegt eine der häufigsten E-Mail-Sicherheitslücken im Bereich der **Domain Keys Identified Mails (DKIM).** Diese sollten **unbedingt konfiguriert** werden. DKIM eine Methode zur E-Mail-Authentifizierung, bei der Absender überprüft und so Fälschungen erschwert werden. Bei korrekter Konfiguration wird beim Versand einer E-Mail wird die DKIM-Signatur dem Header hinzugefügt, die vom Empfänger mit dem öffentlichen Schlüssel aus der DNS-Zone verglichen wird.

Durch diese Kontrolle wird die Authentizität Ihrer E-Mails geprüft und garantiert die Integrität Ihrer Nachrichten.

Ursprünglich sollte das Verfahren Domain Keys Identified Mail nur die Spam-Flut eindämmen, doch da es gefälschte Absenderadressen entdeckt, verbessert es auch deutlich Ihren Schutz vor Phishing-Angriffen! Mit dem DKIM-Verfahren lassen sich folglich gefälschte Absenderadressen aufspüren. Sie sollten also DKIM auf Ihrem Mailgateway und Ihrem DNS-Server konfigurieren und nach Möglichkeit zudem **DMARC** (Domain-based Message Authentication, Reporting and Conformance) **aktivieren.** Damit können Sie festlegen, wie mit E-Mails verfahren werden soll, die als Gefahr identifiziert wurden.

Regel 2:
Grundlegende E-Mail-Schutzmaßnahmen

Schützen Sie E-Mail-Konten durch klassische Schutzmaßnahmen.

Dazu zählen:

- Immer eine verschlüsselte Verbindung (HTTPS) zum Postfach nutzen
- Auf die Darstellung und Erzeugung von HTML-Mails verzichten.
- Die Anzeige externer Inhalte, wie Bilder, deaktivieren.
- Ein starkes Passwort verwenden, damit Zugangsdaten nicht erraten werden.
- Zusätzlich Multifaktor-Authentifizierung (MFA) zum Standard machen.
- Berechtigungen für firmeneigene Mail-Postfächer aktuell halten und veraltete Konten deaktivieren.

Regel 3:
Halten Sie Betriebssystem, Virenschutz und andere Programme aktuell!

Es lohnt sich für den Fall vorzusorgen, dass doch mal ein Mitarbeiter unaufmerksam oder ein Mailsystem mangelhaft konfiguriert ist. So mancher Angriffsversuch lässt sich durch Sicherheitsfeatures des Betriebssystems oder der Anti-Virensoftware aufhalten. Seien Sie sich daher bewusst: **Ihr Rechner ist so sicher, wie Ihr letztes Sicherheitsupdate.**

Cyberkriminelle ersinnen jedoch immer weitere Angriffsstrategien und neue Malware. Zudem entdecken Programmentwickler Sicherheitslücken in ihrem Code häufig erst nach gezielten Nutzer-Hinweisen. Denken Sie an zielführendes und **regelmäßiges Patch-Management**, um Sicherheits-lücken rechtzeitig zu erkennen und – falls notwendig – schließen zu können. Neben dem Betriebssystem sollten insbesondere alle Anwendungen, die mit dem Internet kommunizieren, immer auf dem aktuellen Stand sein. Neuere Versionen einer Applikation besitzen oft mehr Sicherheitsfeatures und helfen so dabei kriminelle Angriffe abzuwehren. Softwareupdates können Ihre Mitarbeiterinnen bzw. IT-Fachkräfte zwar auch manuell herunterladen, dann sollten diese aber gesichert von der Herstellerseite stammen. Damit nicht wegen Urlaub oder Krankheit eine Update-Installation übersehen wird, haben sich Auto-Update-Mechanismen bewährt, die in den Optionen moderner Software aktiviert werden können.

Regel 4:
Achten Sie auf korrekte Serverkonfigurationen!

Mit den passenden **Servereinstellungen** können Sie die **Frequenz von Phishing-Angriffen** verringern. So sollten Sie das mögliche Validieren von Mail-Adressen über Ihren E-Mail-Gateway oder das IDP-System auf eine geringe Anzahl pro Tag limitieren und die IP-Adresse des Anfragenden danach blockieren lassen. Einige Kriminelle nutzen nämlich die Rückmeldung über vorhandene SMTP-User auf Unternehmensservern, um an persönliche Adressen zu gelangen.

Um **Spoofing (Identitätstäuschung)** mit dem Namen Ihres Unternehmens zu vermeiden, sollten Sie Ihren SPF-Record richtig konfigurieren. In einem Sender Policy Framework-Eintrag ist festgelegt, welche die gültigen Mailserver für den Versand Ihrer Domain sind. Dies sollten nur Server des Unternehmens sein, auch wenn es um Ihren Newsletter geht.

Um Log-in und andere persönliche Anmeldeinformationen zu verschlüsseln, setzen Sie bitte nicht auf selbst signierte Zertifikate, sondern nutzen **SSL-Zertifikate von externen Zertifizierungsstellen**. So kann die Identität Ihres Mailsystems von anderen Anwendern und Servern validiert werden. Viele Unternehmen sind vor allem wegen des Preisunterschieds versucht, selbst signierte Zertifikate anstelle der von einer vertrauenswürdigen Zertifizierungsstelle ausgestellten und überprüften Zertifikate zu verwenden. Selbst signierten Zertifikaten vertrauen viele empfangende Mailserver daher nicht und nutzen die TLS-Verschlüsselung folglich nicht bzw. geben eine Sicherheitswarnung an die Nutzer aus, wie z.B. beim Öffnen der Webseite des Mailsystems (OWA). Oft raten die Warnungen den Besuchern aus Sicherheitsgründen zum Seitenabbruch, was nicht sehr vertrauenswürdig wirkt. Potenzielle Kunden könnten vertrieben werden aufgrund der Befürchtung, dass die Website Anmeldeinformationen nicht korrekt sichert.

Zu guter Letzt: *Angreifer könnten den Webzugang unter einer anderen Seite hosten, die Anwender würden aber die gleiche Zertifikatswarnung erhalten.*

Regel 5:
Verschlüsseln Sie Ihre E-Mails!

Nicht-verschlüsselte Mails sind wie Postkarten, die im Klartext abgesendet, transportiert und empfangen werden. Dementsprechend können Kriminelle solche Mails bspw. leicht durch einen Man-in-the-Middle-Angriff mitlesen oder manipulieren. Seit der Verabschiedung der EU-Datenschutzgrundverordnung (EU-DSGVO) gehen Unternehmen hohe Risiken ein, wenn sie den E-Mail-Schutz vernachlässigen. Um dies zu verhindern, gibt es folgende grundlegende Verschlüsselungsmethoden:

- **TLS-Verschlüsselung:** der Mindeststandard für sichere E-Mail-Kommunikation, bei dem der Transport zwischen den Mailservern verschlüsselt wird.
- **Ende-zu-Ende-Verschlüsselung:** Mit Verfahren wie S/MIME oder OpenPGP wird die E-Mail von Client zu Client (end-to-end) verschlüsselt.
- **Symmetrische Verschlüsselung:** Der Sender verschlüsselt seine Nachricht mit einem geheimen Schlüssel, den der Empfänger erhalten muss, um die Nachricht lesen zu können. Es muss ein Weg gefunden werden, den gemeinsamen Schlüssel sicher an den Empfänger zu übermitteln.
- **Asymmetrische Verschlüsselung:** Es wird mit einem öffentlichen Schlüssel verschlüsselt, aber mit einem privaten Schlüssel entschlüsselt.

*Wir empfehlen **TLS als Mindeststandard für gesicherte E-Mail-Kommunikation** zu implementieren. Darüber hinaus setzen Sie **Ende-zu-Ende Verschlüsselung via S/MIME oder PGP** ein, damit E-Mail-Nachrichten bis zum Empfänger geschützt sind.*

Regel 6:
Mit digitaler Signatur den Sender verifizieren

Im Kontext von E-Mail-Sicherheit kommt man nicht an den Themen **E-Mail-Verschlüsselung und E-Mail-Signieren** vorbei. Beides sind wichtige Instrumente, um Schutzziele der Informationssicherheit umzusetzen. Man kann den Absender und die Integrität einer Nachricht auch überprüfen, ohne den Inhalt der Mail zu verschlüsseln (siehe Regel 5).

Dazu signiert man die Mail: Dabei wird eine Prüfsumme über die in der Nachricht enthaltenen Informationen gebildet. Die Prüfsumme wird mit dem privaten Schlüssel des Absenders verschlüsselt. Der Empfänger wiederum nutzt dessen öffentlichen Schlüssel, um die Prüfsumme zu dechiffrieren und zu verifizieren, dass die Nachricht vom echten Absender stammt.

Ist eine E-Mail zwar signiert wurde, aber nicht verschlüsselt, ist die Nachricht in Klartext zu lesen. Signieren dient zur Absender-Verifizierung und zur Beurteilung, ob eine Nachricht während der Übertragung verändert wurde.

Fazit

__E-Mails__ sind immer noch __eines der Haupteinfallstore für Malware__ und Ransomware-Angriffe! Phishing, virenverseuchte Attachments und auch Spam stellen konkrete Bedrohungen für Ihre IT-Sicherheit dar. Der Schlüssel zu einem hohen Sicherheitsniveau in der IT ist eine Sicherheitsstrategie, die alle potenziellen Gefahrenquellen berücksichtigt. Dazu gehören auch die eigenen Mitarbeitenden. Mit gezielten Social-Engineering-Trainings sowie Sicherheitslösungen wie einer geeigneten Lösung zur Angriffsfrüherkennung lässt sich das Niveau der IT-Sicherheit deutlich steigern.

ALLGEIER
secion

Allgeier secion, Zweig-
Niederlassung der
Allgeier CyRis GmbH

Tel.: 040 38 90 71 - 0
Fax: 040 38 90 71 - 299

info@secion.de
www.secion.de

Paul-Dessau-Str. 8
22761 Hamburg

Stand: September 2022