Secure E-Mail

Bei der Mehrheit aller E-Mails handelt es sich um SPAM-Mails oder Phishing-Mails. Rund 95% aller Cyberattacken resultieren aus einer erfolgreichen Phishing-Attacke. E-Mails sind einer der Hauptangriffsvektoren auf Unternehmen und dürfen deshalb im IT-Security-Umfeld nicht vernachlässigt werden.

Lösung

Mit Secure E-Mail kann verhindert werden, dass SPAM-/Phishing-Mails oder Mails mit Malware im Anhang beim End User im Postfach landen. Dazu bietet Netcloud E-Mail-Sicherheitslösungen von Microsoft und Cisco an, welche sich von den Grundfunktionen kaum unterscheiden.

1. MS Exchange Online Protection
Grundschutz vor simplen Attacken (Edge Protection, Sender Intelligence, Content Filtering). Bei Exchange Online immer inklusive; kann auch für On-Prem Exchange Server hinzugefügt werden.

2. MS Defender for M365 Plan 1
Zusätzlicher Schutz vor 0-Day-Malware, Phishing und Business E-Mail Compromise (User/Domain Impersonation), Safe Attachments und Safe Links, SIEM API Integration.

3. MS Defender for M365 Plan 2
Zusätzliche Reports (Threat Explorer und Trackers), reaktive Tools (Post-Breach Investigation, Hunting, Response & Automation) und Angriffssimulation.

4. Cisco Cloud Mailbox
Ergänzt den Grundschutz von Exchange Online Protection mit der Talos Intelligence (Spam, Malware, Phishing, 0-Hour-Auto-Purge) und hat eine übersichtliche Reporting-Oberfläche.

5. Cisco Secure E-Mail Gateway
On-Prem HW/VM Appliances für klassische E-Mail Security wie Antispam, Phishing (SPF, DKIM, DANE, etc.). Granulare Policies mit Message Filters, Domain Rewrite, DLP, Connection Filtering und Add Ons wie E-Mail Encryption oder Sandboxing.

6. Cisco Secure E-Mail Cloud Gateway
Analog Cisco Secure E-Mail Gateway; Appliances werden in der Cloud betrieben. Standardmässiges Management mit zentralem Logging und Policy-/End-User-Quarantänen.

Darum Security by Netcloud
Netcloud hat Expertise im Cloud-, Security- und Netzwerkumfeld sowie Erfahrung aus zahlreichen Secure-E-Mail-Implementierungen. Wir bieten die gesamte Lösung aus einer Hand an und decken von Beratung bis Betrieb alle Phasen ab.

Weitere Infos:

Cisco Secure E-Mail Übersicht

Microsoft Online Protection Übersicht

Edge Protection / Content Filtering	E-Mails werden nach IP-Adressen und Domänen mit Hilfe von DNS Blacklists, Reputationen und einem Rating vom Microsoft bzw. Cisco Talos gefiltert und vor Directory-Harvest-Angriffen geschützt, so dass die E-Mail-Server nicht ungewollt auf einer Antispam-Blacklist landen.
Sender Intelligence / Antispam	Mit Mechanismen wie SPF, DKIM, DMARC und ARC-Records können Spam- und Phishing-Mails erkannt und blockiert werden, indem sichergestellt wird, dass das Mail vom richtigen Senderserver und Absender kommt.
Message / Content Filtering	Nachrichten können auf deren Inhalt überprüft werden. Das Mail wird auf Viren und Malware überprüft, ungewünschte Attachments (z.B. Executables, Macros, etc.) können blockiert und die Mails können auf bestimmte Schlagwörter oder Links im Message Body überprüft werden. Der gesamte Inhalt eines Mails wird mit diesem Feature überprüft.
Sandboxing (AMP)	Bei Cisco Secure E-Mail (Cloud oder On-Prem) können zuvor definierte Attachments an die Sandbox geschickt werden. Diese Advanced Malware Protection (AMP) prüft die Dateien im Detail, indem der Hash mit bekannter Malware abgeglichen wird, aber auch indem die Datei ausgeführt und geprüft wird. Durch ein Rating wird dann dem Secure E-Mail Gateway mitgeteilt, ob das Mail mit dem Attachment blockiert oder zugestellt werden kann.

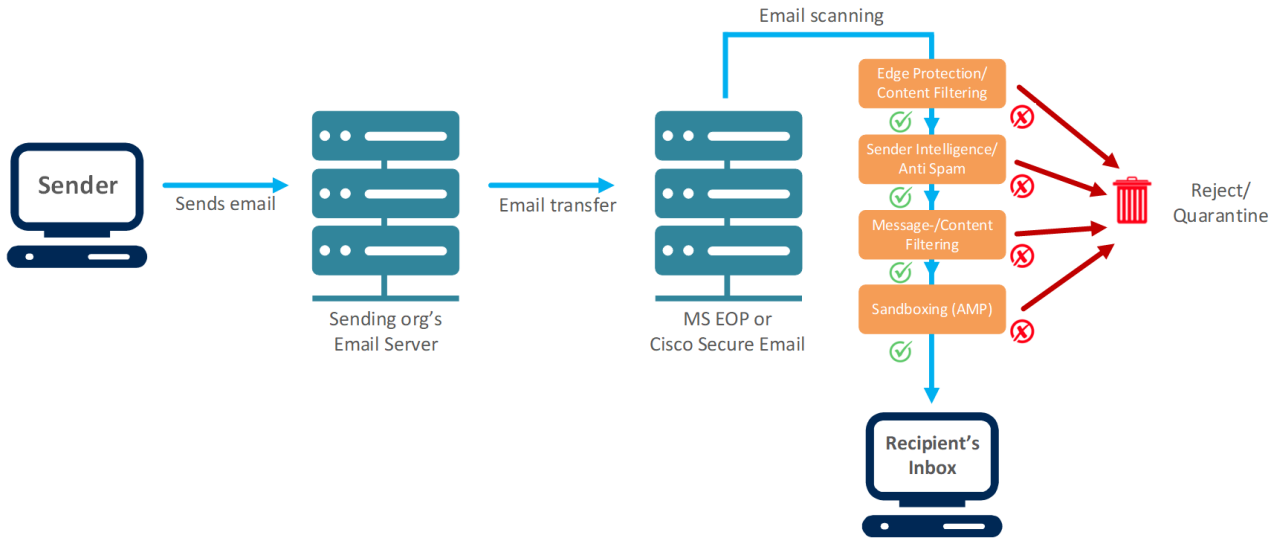

Abbildung 1: Secure-E-Mail-Prozess vom Versand bis zur Zustellung oder Quarantäne