FORTRA

Sechs Schritte Zur Best Practice in Der E-Mail-Sicherheit

Moderne Geschäftsprozesse sind auf E-Mails angewiesen. Stellen Sie sich vor, wie schwierig eine Zusammenarbeit mit Kollegen, Kunden und Geschäftspartners ohne E-Mails wäre. Die Forschungsgruppe Radicati prognostiziert, dass im Jahr 2020 täglich mehr als 306 Milliarden E-Mails gesendet und empfangen werden. Das reine Datenvolumen und die ständig zunehmenden Bedrohungen durch Email-basierte Cyberangriffe stellen IT-Teams vor große Herausforderungen. Alle Unternehmen, die E-Mail-Kommunikation nutzen, müssen:

- Die Gefahren durch Phishing-Attacken erkennen und beseitigen
- Das Spam-Aufkommen kontrollieren, ohne zu riskieren, echte Geschäfts-E-Mails zu beeinträchtigen
- Durch E-Mails übertragene Viren wie Ransomware und Malware verhindern
- Die Weitergabe vertraulicher Informationen durch Mitarbeiter verhindern
- Den fahrlässigen Datenverlust oder das Abgreifen von Daten verhindern, um spätere Geldbußen zu vermeiden.
- Die Verbreitung unangemessener Inhalte blockieren.

Mit der richtigen E-Mail-Security-Lösung können diese Risiken minimiert werden, ohne den Geschäftsbetrieb eines Unternehmens zu beeinträchtigen. Um dabei zu unterstützen, welche Anforderungen eine Lösung erfüllen sollte, haben wir einen sechsstufigen Leitfaden mit **bewährten Verfahren zur E-Mail-Sicherheit** zusammengestellt.

Schritt 1

Bestimmen Sie, Welche Daten Geschützt Werden Müssen

Seit Inkrafttreten der DSGVO (GDPR) wurden in Europa bereits zahlreiche Bußgelder für Datenschutzverstöße verhängt, darunter erhebliche Strafen für namhafte Unternehmen wie British Airways, Marriott Hotels und Google. Diese Bußgelder dienen Unternehmen als Warnung, ihren Datenschutz ernst zu nehmen. Regeln zur Verringerung des Risikos der Nichteinhaltung von Vorschriften (und des damit verbundenen Reputationsschadens) müssen definiert und umgesetzt werden. Der erste Prozessschritt ist die Festlegung der zu schützenden Daten. Das kann die folgenden und darüber hinausgehende Punkte umfassen:

- Persönliche identifizierbare Informationen (PII) über Mitarbeiter und Kunden (oder Patienten im Falle von Gesundheitseinrichtungen)
- Informationen wie Kunden-Bankdaten oder -Kreditkartendetails (PCI)
- Finanzinformationen des Unternehmens
- Produktdesigns und geistiges Eigentum
- Geheime oder vertrauliche Informationen

E-Mail-Sicherheitslösungen mit der Möglichkeit, automatisch in ein- und ausgehender Kommunikation sensible Daten identifizieren und unkenntlich machen zu können, ermöglichen die Zusammenarbeit zwischen Unternehmen ohne das Risiko der versehentlichen Preisgabe vertraulicher Informationen wie Kreditkartendetails. Mitarbeiter sind vor der versehentlichen Weitergabe von sensiblen Daten geschützt, gleiches gilt für die empfangenden Unternehmen. Encryption bietet einen weiteren Weg, sensible Daten zu schützen. Hier werden beispielsweise E-Mails mit PII- oder PCI-Daten automatisch verschlüsselt (siehe Schritt 5 für weitere Details).

Schritt 2

Machen Sie Sich Die Gefahren Bewusst

Ein Unternehmen muss die Bedrohungen, denen es ausgesetzt ist, eindeutig verstehen, bevor die erforderliche E-Mail Sicherheitsstrategie festgelegt werden kann. Wenn die Unternehmen wissen, was verhindert werden muss, können sie bei der Suche nach einer geeigneten E-Mail-Security-Lösung die richtigen Fragen stellen. Es handelt sich nicht um eine E-Mail-Sicherheitslösung, wenn sie nicht vor den folgenden Risiken schützt:

- Malware/Spyware/Ransomware
- Kompromittierung geschäftlicher E-Mails (Phishing)
- Sicherheitsverstöße (DSGVO, PCI, HIPPA etc.)
- Unerwünschte Datenerfassung
- Unnötige Dateitypen
- Hass-Mails und Pornografie

In der ersten Jahreshälfte 2019 wurden 4,1 Milliarden Datensätze im Rahmen von mehr als 3.800 Datenschutzverletzungen allgemein als kompromittiert gemeldet – **eine Zunahme von 54 %** im Vergleich zur ersten Jahreshälfte 2018 (Norton). **E-Mails** (in 70 % der gefährdeten Datensätze enthalten) und Passworte (in 60 % der gefährdeten Datensätze enthalten) hatten hieran den größten Anteil (Forbes).

Der durchschnittliche finanzielle Schaden durch Cyberkriminelle für Privatpersonen und Unternehmen stieg im dritten Quartal 2019 auf mehr als 41.000 $, eine Zunahme von 13,1 % im Vergleich zum vorherigen Quartal. (Data Breach Today)

Schritt 3

Implementieren Sie Eine Solide und Nachhaltige E-Mail-Sicherheitsrichtlinie

Eine E-Mail-Sicherheitsrichtlinie sollte die Parameter definieren, innerhalb derer die Mitarbeiter Daten und E-Mails im Unternehmen nutzen können, sollten und müssen. Die Richtlinie sollte:

- **Gesehen werden** – Eine effektive Richtlinie muss bei ihrer Einführung gesehen werden. Informationen darüber sollten auch in Unternehmens-Newslettern, im Intranet usw. kommuniziert werden.
- **Deutlich sein** – Leicht verständlich mit wenig Interpretationsspielraum
- **Konsistent sein** – Anwendung auf den gesamten Messaging-Verkehr, einschließlich interner, eingehender und ausgehender E-Mails
- **Angemessen sein** – Unterschiedliche User, Abteilungen und Standorte verwenden E-Mails unterschiedlich (und haben dabei gemeinsame Grundsätze)
- **Regelmäßig überprüft werden** – Feedbacks aus allen Geschäftsbereichen widerspiegeln
- **Flexibel sein** – mit der Fähigkeit zur Weiterentwicklung bei geschäftlichen Veränderungen oder neuen Bedrohungen

Eine E-Mail-Sicherheitslösung, die einfach bereitzustellen, zu überwachen und zu verwalten ist, unterstützt dabei, die Richtlinie durchzusetzen, ohne dabei die IT-Abteilung oder E-Mail-Administratoren zu überlasten. Funktionen wie die Möglichkeit, alle Bedrohungen in einer einzelnen Benutzeroberfläche zu verwalten oder das Pflegen eigener Quarantänelisten durch einzelne Mitarbeiter verbessern die Effizienz der Lösung und bieten den IT-Teams letztlich mehr Zeit für andere Projekte.

Schritt
4

Schließen Sie Das Zero-Day-Fenster

Anti-Malware-Lösungen sind gut geeignet, bekannte Bedrohungen abzuwehren. Doch was geschieht, wenn ein neuer Virus versucht, in ein Netzwerk einzudringen, bevor die Sicherheitslücken identifiziert wurden?

Dieses „Zero-Day"-Fenster ist eine der eklatantesten Schwachstellen in den E-Mail-Strategien vieler Unternehmen. Und es gibt nur eine Möglichkeit, sich davor zu schützen: **Content-Filterung mit intelligenten Regeln.**

E-Mail-Sicherheitslösungen, die in der Lage sind, die Inhalte von Nachrichten und Anhängen zu filtern sowie zu analysieren, um die Eigenschaften schädlicher Inhalte zu bestimmen, sind hierbei von großem Wert. Selbst augenscheinlich harmlose Dateien, beispielsweise im Format Microsoft Word oder Adobe PDF, können schädliche Makros und Skripte enthalten. Eine solide Filter-Engine analysiert die Inhalte bis in das kleinste Detail. Wenn aktive Inhalte oder ausführbare Dateien erkannt werden, wendet die Lösung die jeweils implementierte Richtlinie an, um das Problem in Echtzeit zu lösen. Dies kann darin bestehen, die aktiven Inhalte zu entfernen (durch Structural Sanitization) und so die Kommunikation zu ermöglichen, oder sie zu blocken, zu löschen oder zu reporten –oder eine Kombination aus diesen Möglichkeiten anzuwenden. Ein ungehindertes Eindringen darf nicht gestattet werden.

Schritt
5

Verschlüsseln Sie Sensible Daten

Als letzte Verteidigungslinie zum Schutz der Mitarbeiter vor dem unbeabsichtigten Versenden wichtiger Informationen an nicht autorisierte Parteien sowie zur Sicherstellung der Einhaltung strenger Regularien sollten Unternehmen E-Mail-Nachrichten mit sensiblen Daten automatisch verschlüsseln. Viele E-Mail-Sicherheitslösungen bieten proprietäre Verschlüsselungsverfahren, deren Anwendung komplex und kostspielig ist. Andere Lösungen hingegen bieten eine Reihe benutzerfreundlicher, richtlinienbasierter Verschlüsselungsoptionen, einschließlich TLS, PKI-Techniken wie S/MIME oder PGP, per Web-Portal oder Passwort-geschützte Nachrichten.

Unternehmen, die den Zugriff auf Unternehmensdaten auch nach dem Verlassen des Unternehmens kontrollieren wollen, sollten eine E-Mail-Sicherheitslösung mit eDRM-Funktionalität (Enterprise Digital Rights) einsetzen. eDRM definiert, welche Aktionen (wie Bearbeiten, Drucken, Kopieren) der Empfänger mit den erhaltenen Daten durchführen und wie lange er darauf zugreifen kann. Dies wird häufig in Branchen wie Bankwesen, Finanzdienstleistungen, Fertigung, Pharmazie und Recht eingesetzt, wo regelmäßig sensitive Informationen ausgetauscht werden.

Schritt 6

Überwachen Sie Das Verhalten und Die Performance Ihres Datenverkehrs

Die Redensart „Sie können nicht sichern, was Sie nicht sehen“ ist für die E-Mail-Sicherheit von besonderer Bedeutung, daher ist das Reporting ein so wichtiger Bestandteil des Prozesses. Wenn E-Mail-Verhaltens- und Performance-Probleme hervorgehoben werden, können schnelle Maßnahmen ergriffen werden. Mitarbeiter, die große Mengen an E-Mails versenden oder empfangen, können überwacht werden, ebenso der Typ und die Größe der versendeten Dateien. Diese Informationen können sich bei der Identifizierung von Problembereichen als ausgesprochen wertvoll erweisen und dem Unternehmen die Möglichkeit bieten, bei Bedarf die Richtlinie nachzubessern und Ressourcen umzuverteilen. Beschränkungen in Bezug auf die Anzahl von Anhängen oder Dateien einer bestimmten Größenordnung schützen darüber hinaus Speicher- und Bandbreitenressourcen. Erarbeiten Sie eine Richtlinie, um große Dateien entweder herauszufiltern oder für eine spätere Zustellung zwischenzuspeichern.

E-Mail-Sicherheitslösungen, die detaillierte Prüfketten bieten, unterstützen die IT-Teams bei der Untersuchung potenzieller Verstöße. Lösungen mit einer Exportfunktion für SIEM-Systeme ermöglichen Unternehmen eine 360-Grad-Betrachtung ihres ein- und ausgehenden Datenflusses.

Zusammenfassung

Diese Schritte fassen ein einfaches Konzept für bewährte Praktiken in der E-Mail-Sicherheit zusammen. Während sich die Technologien zur Abwehr von Bedrohungen und Datenverlust verändert haben, gelten dennoch die gleichen Grundsätze: definieren Sie eine klare Richtlinie zur E-Mail-Sicherheit und setzen Sie diese mit der richtigen Technologie um.

Warum Clearswift?
Seit mehr als 25 Jahren unterstützt Clearswift Unternehmen dabei, ihre Daten zu schützen und zu sichern. Mit prämierten Adaptive-Redaction-Technologien bieten die E-Mail- und Web_Security-Lösungen Unternehmen absoluten Schutz vor Cyberbedrohungen und Datenverlust, ohne die Zusammenarbeit im Tagesgeschäft zu beeinträchtigen.

www.clearswift.de

Nächste Schritte

Die sichere E-Mail von Clearswift Gateway-Angebote:

- Integrierter Malware- und Spam-Schutz
- Zero-Day Erkennung von aktivem Code
- Adaptive Data Loss Prevention, einschließlich Data Redaction, Document und Structural Sanitization
- Automatisierte Verschlüsselung

Kontaktieren Sie uns für Hilfe bei der Definition Ihrer E-Mail Sicherheitspolitik oder um mehr zu erfahren über unserem sicheren E-Mail-Gateway

LEARN MORE

FORTRA

Über Fortra

Fortra ist ein Cybersicherheits-Unternehmen wie kein zweites. Wir erschaffen eine einfachere und solidere Zukunft für unsere Kunden. Unsere bewährten Experten und unsere breite Palette integrierter und skalierbarer Lösungen bringen Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Bei Ihrer Reise zu mehr Cybersicherheit sind wir Ihr Wegbereiter und Ihr unermüdlicher Verbündeter auf jeder Etappe. Erfahren Sie mehr auf fortra.com/de.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

fta-csw-gd-1022-r1-79d