Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

E-Mail-Security

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

E-Mail-Security – Was ist das?

Die E-Mail ist eine der am häufigsten verwendeten Kommunikationsmethoden in Unternehmen und Organisationen. Cyberkriminelle nutzen sie ebenfalls, um Unternehmen anzugreifen, sensible Daten zu stehlen oder zu beschädigen. Deshalb ist es wichtig geeignete Sicherheitsmaßnahmen zu ergreifen.
Der hier verwendete Begriff E-Mail-Security bezieht sich auf die Sicherheitsmaßnahmen, die getroffen werden können, um die **Vertraulichkeit, Integrität und Verfügbarkeit von E-Mails** zu gewährleisten. Es geht darum sicherzustellen, dass nur **autorisierte Personen** auf Nachrichten zugreifen können, diese **nicht manipuliert** werden und sie jederzeit **verfügbar** sind.

Wie kann ich meine E-Mails sichern?

Jeder E-Mail-Nutzer sollte über eine **eigene persönliche** E-Mailadresse verfügen. Auf dieses Postfach hat nur der Nutzer selbst standardmäßig Zugriff. Bei **Funktionspostfächern**, die von mehreren Nutzern verwendet werden, sollten **Regeln** erlassen werden, wie dieses Postfach zu verwalten ist.
Eine wichtige Möglichkeit, um sicherzustellen, dass nur autorisierte Personen auf E-Mail-Inhalte zugreifen können, besteht darin, sie zu verschlüsseln. Die **Verschlüsselung** sorgt dafür, dass die Nachrichten nur von Personen gelesen werden können, die über den richtigen Schlüssel verfügen. Eine weitere Möglichkeit besteht darin, sicherzustellen, dass E-Mails von einer vertrauenswürdigen Quelle stammen, beispielsweise durch die Verwendung **digitaler Signaturen**. Nützlich sind ebenfalls **Spam-Filter**, die unerwünschte oder betrügerische E-Mails herausfiltern und so die Wahrscheinlichkeit von Phishing-Angriffen oder anderen Arten von Betrug reduzieren.
Virenschutzprogramme tragen zudem dazu bei, Malware oder andere schädliche Programme zu erkennen und zu blockieren. Zudem sollte ein **Backup-System** implementiert werden, um sicherzustellen, dass wichtige E-Mails dauerhaft verfügbar und wiederherstellbar sind.
Nutzer sollten vor dem Senden prüfen, ob die **Empfänger korrekt** sind, um das Senden von vertraulichen Informationen an falsche Empfänger zu vermeiden. Diese Gefahr besteht besonders bei der Nutzung der **Funktion „Allen antworten"** und der **Auto-Vervollständigung** von Empfängern mit ähnlichen Namen.
Antwortet man auf alle Empfänger einer Mail, oder leitet eine Mail weiter, muss darauf geachtet werden, dass im weitergeleiteten **Mailverlauf** keine vertraulichen Informationen oder Anhänge sind, die nicht für den neuen Empfängerkreis relevant sind.
Für vertrauliche Informationen sollte ein Unternehmen generell überlegen, ob **Dateien** in einer Mail versendet werden oder über einen gesicherten Link aus einer Cloud abrufbar sind. E-Mail-Anhänge sollten generell auf **Viren** geprüft und Mails von verdächtigen Absendern gelöscht werden. Um das **Tracking in Mails** zu verhindern, sollte der automatisierte Download von Bildern ausgeschaltet sein. Der Mailversand sollte daher organisatorisch geregelt werden.

Cyber-Sicherheitsrat Deutschland e.V.

Technische Möglichkeiten

SPF, DKIM und DMARC sind drei wichtige Technologien, die zusammenarbeiten, um die Authentizität von E-Mails zu überprüfen und Nutzer vor Phishing-Angriffen zu schützen.

SPF (Sender Policy Framework) ist ein Protokoll zur Überprüfung der Absenderadressen. Hierbei wird eine Liste von **autorisierten IP-Adressen** erstellt, von denen aus E-Mails für eine bestimmte Domain gesendet werden können. Wenn eine Nachricht von einem unbekannten Server gesendet wird, wird diese als verdächtig eingestuft und möglicherweise blockiert oder in den Spam-Ordner verschoben.

DKIM (DomainKeys Identified Mail) ist eine Methode zur Authentifizierung von E-Mails. Hierbei wird eine **digitale Signatur** angehängt, die vom Absender stammt und die Echtheit der Mail bestätigt. Wenn die Nachricht vom Empfänger empfangen wird, wird die Signatur mit einem öffentlichen Schlüssel des Absenders überprüft. Wenn die Signatur gültig ist, wird die Authentizität der Nachricht bestätigt und diese zugestellt. Wenn die Signatur ungültig ist, wird die E-Mail abgelehnt.

DMARC (Domain-based Message Authentication, Reporting & Conformance) ist ein Protokoll, das auf SPF und DKIM aufbaut und zusätzliche Funktionen bietet. Mit DMARC kann ein Domain-Inhaber eine **Richtlinie festlegen**, die bestimmt, wie Empfänger mit einer E-Mail verfahren sollen, die von einer anderen Domain stammt. Wenn eine Nachricht von einer Domain gesendet wird, die eine DMARC-Richtlinie hat, wird der Empfänger die Richtlinie überprüfen und entsprechend handeln. Zusammen bieten SPF, DKIM und DMARC eine **zusätzliche Schutzschicht** indem sie die Authentizität und Zuverlässigkeit von Nachrichten überprüfen.

Welche Chancen gibt es?

Maßnahmen zur Stärkung der E-Mail-Sicherheit helfen Unternehmen, ihre vertraulichen Informationen und Daten zu schützen. Durch den **Schutz von Daten** können Unternehmen **Vertrauen** bei Kunden und Partnern aufbauen und sich **vor Haftungsansprüchen schützen**.

Entsprechende Sicherheitsmaßnahmen können zudem dazu beitragen, das **Risiko von Cyberangriffen** wie Phishing-Angriffen oder Malware-Infektionen zu reduzieren. Dies kann dabei helfen den Betrieb des Unternehmens aufrechtzuerhalten und **Ausfallzeiten zu minimieren**.

Viele Branchen und Regierungen haben darüber hinaus spezifische Vorschriften und Anforderungen in Bezug auf die Sicherheit von Daten. Die Implementierung von E-Mail-Sicherheitsmaßnahmen kann dazu beitragen, diese Anforderungen zu erfüllen und Geldstrafen oder anderen **rechtlichen Konsequenzen vorzubeugen**.

Nicht zuletzt reduzieren effektive Sicherheitsmaßnahmen die Anzahl unerwünschter Nachrichten und dadurch auch den **Arbeitsaufwand** von Mitarbeiterinnen und Mitarbeitern.

Cyber-Sicherheitsrat Deutschland e.V.

Welche Risiken gibt es?

Die Planung und Umsetzung von Sicherheitsmaßnahmen für E-Mails kann mit **Kosten** verbunden sein. Unternehmen müssen möglicherweise in Hard- und Software oder externe Dienstleistungen investieren, um ihren Nachrichtenverkehr zu schützen.
Spam-Filter und andere Sicherheitsmaßnahmen können manchmal auch legitime E-Mails **fälschlicherweise blockieren** oder in den Spam-Ordner verschieben. Unternehmen sollten daher sicherstellen, dass ihre Sicherheitsmaßnahmen so konfiguriert sind, dass falsch-positive Ergebnisse minimiert werden.

Wem nutzen die Maßnahmen?

E-Mail-Sicherheitsmaßnahmen sind besonders wichtig für Unternehmen und Organisationen, die **sensible Daten** wie Finanzinformationen, geistiges Eigentum oder persönliche Informationen von Kunden und Mitarbeitern verwalten. Durch die Implementierung geeigneter Schutzvorkehrungen können diese Daten vor Cyberangriffen wie Phishing, Malware oder Datendiebstahl geschützt werden. Einzelpersonen können auch von Sicherheitsmaßnahmen profitieren, indem sie sich vor **Spam, Betrug oder Identitätsdiebstahl** schützen.

Fazit

Insgesamt ist E-Mail-Security ein wichtiger Aspekt der Cybersicherheit für Unternehmen und Organisationen. Die Implementierung von geeigneten Maßnahmen wie SPF, DKIM und DMARC kann dazu beitragen, die **Vertraulichkeit, Integrität und Verfügbarkeit von Nachrichten zu gewährleisten** und Unternehmen vor Cyberangriffen zu schützen.

Cyber-Sicherheitsrat Deutschland e.V.