Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: INTERNET-DIENSTLEISTER

E-Mail-Sicherheit

Handlungsempfehlungen für Internet-Service-Provider

Trotz diverser Vorhersagen, dass sich in Zukunft die Internetkommunikation immer stärker auf soziale Netzwerke verlagern wird, ist E-Mail derzeit immer noch das meistgenutzte Medium für die Übertragung von elektronischen Nachrichten. Hiermit verbunden ist jedoch leider auch die Tatsache, dass E-Mail nach wie vor einen der meistgenutzten Transportkanäle für die Verbreitung von Malware, wie Viren, Würmern und Trojanern, darstellt. Ein nicht minder großes Ärgernis ist das enorme Aufkommen an Spam-Nachrichten, welche nach wie vor den weitaus größten Anteil aller versendeten E-Mails umfassen. Die vorliegende Cyber-Sicherheitsempfehlung schlägt Internet-Service-Providern daher verschiedene Maßnahmen vor, mit denen sich einerseits das Malware- und Spam-Problem bei E-Mails in hohem Maße eindämmen lässt und die zum anderen der Absicherung des Zugangs der Kunden zu ihrem Postfach dienen.

1 Mindestanforderungen

Kein automatisiertes Verfahren liefert eine 100% sichere Erkennungsrate für Spam und Malware. Durch die Kombination verschiedener Maßnahmen (siehe hierzu auch [1]) lässt sich jedoch die Sensitivität von Filtersystemen bis nahe an den Optimalwert steigern. Welche Maßnahmen hierbei zu den besten Resultaten führen, hängt i. d. R. vom jeweiligen Geschäftsmodell eines Providers und der Zusammensetzung seines Kundenkreises ab. So ist es in manchen Fällen am effektivsten, verdächtige E-Mails bereits am äußeren Relay abzulehnen, während andere Provider ein mehrstufiges Filterverfahren bevorzugen. Dementsprechend wird erstere Strategie den Fokus eher auf Verfahren der E-Mail-Authentifizierung richten, während Letztere sich mehr an der Inhaltsanalyse orientiert.

Die vorliegende Sicherheitsempfehlung ist daher nicht so zu verstehen, dass *alle* im Folgenden beschriebenen Maßnahmen akribisch umzusetzen sind. Vielmehr sollten diese als Komponenten eines „Baukastens“ betrachtet werden, mit dessen Hilfe sich – individuell und auf das jeweilige Geschäftsmodell angepasst – eine wirkungsvolle Strategie gegen Spam und Malware erstellen lässt.

Während also einerseits bei der konkreten Umsetzung der Maßnahmen ein gewisser Gestaltungsspielraum besteht, ist es auf der anderen Seite jedoch unabdingbar, dass im Ergebnis das Ziel der E-Mail-Sicherheit gewährleistet ist. Welche Strategie daher auch immer im Einzelnen verfolgt wird, die folgenden Mindestanforderungen müssen durch diese erfüllt sein:

- Sowohl eingehende als auch ausgehende E-Mails sind auf Schadsoftware zu scannen. Unabhängig davon, wie bei einem positiven Ergebnis mit der einzelnen Mail verfahren wird (s.u.), muss soweit wie möglich sichergestellt werden, dass eine Infektion des Empfängers vermieden, bzw. eine möglicherweise schon vorliegende Infektion des Absenders von diesem erkannt und beseitigt wird.
- Durch eine geeignete Kombination von Maßnahmen, wie sie im Folgenden beschrieben werden, ist ein wirksamer Spamschutz zu implementieren. Zur rechtlichen Absicherung sollte dem Kunden die Möglichkeit gegeben werden, durch die Voreinstellungen seines Postfaches selbst zu bestimmen, wie mit automatisiert als Spam identifizierten Mails zu verfahren ist.
- Die E-Mail-Übertragung sollte durchgehend verschlüsselt erfolgen. Dabei muss es dem Kunden auch möglich sein, seine Mails selbst Ende-zu-Ende zu verschlüsseln.

2 Maßnahmen gegen Malware (Viren, Würmer, Trojaner)

Die Verbreitung von Schadsoftware via E-Mail ist Teil der übergreifenden Malware-Problematik im Internet. Hierzu sind bereits Handlungsempfehlungen [2] des BSI erschienen, die das Thema in seiner gesamten Breite abdecken und auf die an dieser Stelle ausdrücklich verwiesen sei. Die im Folgenden beschriebenen Maßnahmen sind dagegen in erster Linie auf den Aspekt der E-Mail-Sicherheit fokussiert.

2.1 Scan eingehender und ausgehender E-Mails

Sowohl die auf einem Mailserver des Providers eingehenden als auch die abgehenden E-Mails müssen mit einem Virenschutzprogramm gescannt werden. Sollte dabei Schadsoftware gefunden werden, ist sicherzustellen, dass diese nicht den Empfänger erreichen bzw. dessen Rechner infizieren kann. Dies lässt sich erreichen, indem z. B.:

- eingehende infizierte E-Mails bereits am Relay abgewiesen werden (Echtzeitfilterung),
- die E-Mail als Ganzes gelöscht wird,
- nur der infizierte Teil (z. B. ein gefährlicher Anhang) abgetrennt und gelöscht wird; der mit einer entsprechenden Kennung markierte Rest der E-Mail kann dann zugestellt werden oder
- die gesamte E-Mail in einen gesonderten Ordner verschoben wird.

2.2 Kundenbenachrichtigung

Gleichgültig, welche der o. g. Maßnahmen durchgeführt wurde, sollten bei eingehenden Nachrichten der Empfänger (bei ausgehenden entsprechend der Sender) darüber informiert werden, wie mit der E-Mail verfahren wurde. Das BSI empfiehlt darüber hinaus, den Kunden bereits im Rahmen des Vertragsabschlusses (z. B. über die AGB) auf diese Vorgehensweise hinzuweisen und sich sein Einverständnis damit bestätigen zu lassen (s. u.: „Vertragliche Regelungen mit den Kunden“).

2.3 Information und Bereitstellung von Anti-Virus-Produkten

Kunden sollten in geeigneter Form auf Anti-Virus-Produkte (AV-Produkte) aufmerksam gemacht werden. Dies kann durch Hinweise auf freie AV-Produkte (siehe z. B. BSI-Empfehlung „PCs unter Microsoft Windows für Privatanwender“) oder kommerzielle AV-Produkte – optional auch durch Bereitstellung als Bundle zusammen mit dem Internetanschluss – erfolgen.

3 Maßnahmen zur Abwehr von Spam und Phishing

Wie bereits erwähnt, lässt sich eine wirksame Spam-Abwehr nur durch eine Kombination verschiedener Maßnahmen realisieren. Dazu gehören zum einen verschiedene Methoden der E-Mail-Authentisierung, d. h. der Verifizierung, ob eine Nachricht tatsächlich von dem darin genannten Absender stammt bzw. ob die Quelle (d. h. der versendende E-Mail-Server) vertrauenswürdig ist. Die zweite Kategorie von Maßnahmen gegen Spam besteht aus verschiedenen Verfahren der Content-Filterung, durch die sich verdächtige E-Mails identifizieren lassen, um sie gegebenenfalls zurückzuweisen oder in einen Quarantäneordner zu verschieben. Alle diese Maßnahmen gegen Spam lassen sich natürlich auch zur Abwehr der Verbreitung von Schadsoftware durch E-Mail nutzen. Insofern besteht ein Überlapp zwischen dem vorigen Abschnitt und dem Folgenden.

3.1 E-Mail Authentifizierung

Bei der Prüfung, ob eine eingehende E-Mail als Spam zu klassifizieren ist, sollte – wenn möglich – in einer ersten Stufe der absendende Server authentifiziert werden. Hierzu stehen verschiedene Verfahren zur Verfügung, wie:

- DomainKeys Identified Mail (DKIM)
- Prüfen des (Reverse-)MX-Records
- Sender Policy Framework (SPF) und Sender ID
- Domain-based Message Authentication, Reporting and Conformance (DMARC)

Bei DKIM versieht der sendende E-Mail-Server oder -Client bestimmte Header-Informationen und den Body einer Nachricht mit einer elektronischen Signatur. Die Verifizierung erfolgt mittels des im Domain Name System (DNS) der sendenden Domäne hinterlegten öffentlichen Schlüssels. Neben der sicheren Authentifizierung besteht ein weiterer Vorteil der Methode darin, dass sich auch die Integrität der E-Mail überprüfen lässt. Allerdings ist das Verfahren wegen der erforderlichen Public-Key-Infrastruktur (PKI) recht aufwendig und bei umfangreichen Nachrichten ist die Integritätsprüfung auch ressourcenintensiv.

Statt der komplexen Authentisierung über eine elektronische Signatur, werten die anderen o. g. Verfahren E-Mail-Charakteristiken aus, welche stärker mit dem zugrunde liegenden SMTP-Protokoll verknüpft sind. So ist der MX-Record einer Domain ein Eintrag im DNS, der die Server (MTAs) umfasst, die für eine Domain die E-Mails entgegennehmen. Diesen MTAs sind im MX-Record Prioritäten zugeordnet, um beim Ausfall eines Servers eine Reihenfolge vorzugeben, wie dieser durch eine niedriger priorisierte Instanz zu ersetzen ist. Normalerweise wird eine E-Mail zunächst an den im MX-Record der Domain am höchsten priorisierten MTA gesendet. Versender von Spam hingegen verschicken diesen oft jedoch an den MTA mit der niedrigsten Priorität, in der Erwartung, dass die Spam-Filter nur auf den höchst priorisierten Servern laufen. Aus solchen Anomalien in der Adressierung von E-Mails lassen sich bereits erste Anhaltspunkte für Spam ableiten.

Wichtiger als der MX-Record selbst ist für die Bewertung des Spam-Potenzials einer Mail der reverse MX-Record. Dabei handelt es sich um den DNS-Eintrag des absendenden MTAs, in dem die IP-Adressen der Mail-Server aufgelistet sind, die zum Mail-Versand für die entsprechende Domain berechtigt sind.

Beim SPF-Verfahren wird die Absendeadresse im Envelope der Mail (MAIL FROM) mit den im reverse MX-Record der absendenden Domain als berechtigte Mail-Server aufgeführten IP-Adressen verglichen. In Erweiterung von SPF wird bei dem Verfahren „Sender-ID“ zusätzlich auch die Absendeadresse im Header mit ausgewertet.

Im Gegensatz zu DKIM und SPF ist DMARC kein weiteres Verfahren zur Prüfung der Identität des Absenders einer E-Mail, sondern definiert vielmehr eine Policy, wie mit der Nachricht auf Grundlage des Ergebnisses eines DKIM- und/oder SPF-Abgleiches zu verfahren ist. Eine solche Policy ist wichtig vor dem Hintergrund der Tatsache, dass die Authentifizierung oft zu keinem eindeutigen Ergebnis oder zu False Positives führt. Bei SPF passiert dies häufig, wenn die Mail weitergeleitet wurde und der weiterleitende Mail-Server das Sender Rewriting Scheme (SRS) nicht unterstützt. Bei DMARC veröffentlicht der Absender daher im DNS in Form eines Text-Files Regeln, wie vom Empfänger zu verfahren ist, wenn die DKIM- und/oder SPF-Authentisierung einer E-Mail fehlschlägt. Umgekehrt erhält der Sender vom Empfänger periodisch aggregierte Berichte über die Ergebnisse der DKIM- und SPF-Prüfungen der aus der Sender-Domain erhaltenen E-Mails und wie mit diesen auf Grundlage des DMARC-Records weiter verfahren wurde. Diese Informationen helfen der Sender-Domain, ihre DMARC-Policy weiter zu optimieren.

3.2 Spam-Filter

Die im letzten Abschnitt beschriebenen Maßnahmen dienten in erster Linie der Überprüfung, ob eine E-Mail tatsächlich von den im Envelope und Header genannten Absendeadressen stammt bzw. ob ein Mail-Server berechtigt ist, für eine Domain E-Mails zu versenden. Falls bei einer E-Mail sowohl die DKIM- als auch die SPF-Prüfung negativ ausfällt, spricht dies mit hoher Wahrscheinlichkeit dafür, dass es sich um Spam oder Phishing handelt. Wegen der zuvor bereits erwähnten relativ hohen False-Positive-Quote von SPF liefert in diesem Fall DKIM das verlässlichere Ergebnis.

Umgekehrt lässt ein übereinstimmend positives Resultat beider Prüfmethoden *nicht* zwingend darauf schließen, dass eine E-Mail frei von Spam oder Phishing ist. Z. B. durch die kurzfristige Anmeldung von „Wegwerf“-Domänen, die sich scheinbar regelkonform verhalten, lassen sich Authentisierungsverfahren in ihrer Wirksamkeit beeinträchtigen. DKIM und SPF müssen daher ergänzt werden durch Verfahren, die neben der Authentizität auch die Vertrauenswürdigkeit der Absender überprüfen. Als Grundlage für eine solche Prüfung eignen sich Maßnahmen wie:

- **Whitelisting**: E-Mails von bekannten vertrauenswürdigen MTAs werden immer akzeptiert.
- **Blacklisting**: E-Mails von bekannten nicht vertrauenswürdigen MTAs werden immer abgewiesen.
- **Frequenzanalyse**: Versendet ein Server plötzlich eine große Zahl von Nachrichten mit gleichartigen Eigenschaften (z. B. gleiche Größe) deutet dies auf Spam hin (Maßnahme: Blacklisting des Servers).
- **Greylisting**: E-Mails von unbekannten Servern werden zunächst abgewiesen und erst beim zweiten Zustellversuch akzeptiert (nutzt die Tatsache aus, dass Spam-Systeme i. d. R. keinen zweiten Zustellversuch unternehmen, wenn der Erste abgewiesen wurde;

allerdings verliert diese Methode zunehmend an Wirksamkeit, da Spammer sich darauf einrichten und auch wiederholt zustellen).

Die bisher angeführten Verfahren gehen das Spam-Problem nur indirekt an, nämlich über eine Bewertung der Seriosität des Absenders. Eine direkte Prüfung auf Spam oder Phishing ist jedoch nur möglich, wenn auch die E-Mail selbst, d. h. deren Inhalt, automatisiert (und datenschutzkonform) auf gewisse charakteristische Merkmale hin untersucht wird. Hierzu stehen verschiedene Methoden der Content-Filterung zur Verfügung:

- **Prüfsummenvergleich**: Der Inhalt der Nachricht – bzw. charakteristische Textsequenzen - werden gehasht und mit bekannten Spam-Signaturen verglichen.
- **Heuristische Inhaltsanalyse**: Der Filter „lernt" Spam an Hand charakteristischer Merkmale (z. B. bestimmte Begriffe, Strukturen, Schreibweisen usw.) zu erkennen.
- **Statistische Inhaltsanalyse**: Der Filter erkennt Spam aufgrund der statistischen Verteilung gewisser Stichwörter (Tokens).
- **Provider-/User-Reports:** Filterung von Spam, der bereits von anderen Providern oder eigenen Usern als solcher erkannt und gemeldet wurde.

Ähnlich zu DMARC bei den Authentifizierungsverfahren, benötigt der E-Mail-Filter auch hinsichtlich der Prüfung der Vertrauenswürdigkeit des Absenders bzw. der Content-Analyse eine Policy, wie das Spam- oder Phishing-Risiko einzustufen und wie entsprechend mit einer E-Mail weiter zu verfahren ist.

Für die Bewertung des Spam-Risikos eignet sich ein Kriteriensystem, welches der E-Mail nach jedem Prüfschritt – je nach Ergebnis – eine gewisse Punktzahl zuordnet. Überschreitet die aufsummierte Gesamtpunktzahl am Ende einen gewissen Schwellenwert, so ist die E-Mail als Spam oder Phishing zu bewerten.

Hinsichtlich der weiteren Verfahrensweise bieten sich folgende Möglichkeiten an:

- Die E-Mail wird mit einer entsprechenden Kennzeichnung versehen (z. B. „Spam Verdacht") direkt an das Postfach des Kunden weitergeleitet.
- Die E-Mail wird im Postfach des Kunden in einem gesonderten Ordner für spamverdächtige Nachrichten abgelegt, aus dem der Kunde sie innerhalb einer bestimmten Frist entweder selbst entfernt oder in dem sie periodisch automatisiert gelöscht werden, um die Quota des Kunden nicht zu belasten.

Eine automatische Löschung Spam-verdächtiger E-Mails sollte wegen eventueller False Positives nicht erfolgen. Möglich ist es hingegen, im Rahmen des Blacklistings E-Mails von bekannten nicht vertrauenswürdigen MTAs abzuweisen, bevor sie den eigenen Mailserver fluten und ggf. dessen Verfügbarkeit beeinträchtigen.

3.3 Maßnahmen gegen Spam-Verbreitung durch Kunden

Um zu verhindern, dass die Rechner von Kunden – z. B. weil sie unwissentlich zum Teil eines Botnets geworden sind – unkontrolliert Spam oder Schadsoftware verbreiten, ist die Umsetzung folgender Maßnahmen zu empfehlen:

- Der Provider-MTA sollte von Clients oder von dynamischen IP-Adressen (d. h. also i. d. R. von Privatkunden) E-Mails nur nach vorheriger Authentifizierung – bevorzugt über Port 587 – annehmen. Falls Privatkunden über Port 25 Spam versenden, sollte dieser Port temporär gesperrt und der Kunde darüber informiert werden.

- Sollten Kunden, die einen eigenen MTA betreiben (typischerweise Geschäftskunden) Spam versenden, müssen diese darüber so schnell wie möglich informiert und aufgefordert werden, ihre Systeme umgehend zu reinigen.

3.4 Spamtraps

Für einen ISP empfiehlt es sich, sog. Spamtraps zu betreiben, also spezielle E-Mail-Adressen, die nicht der normalen Kommunikation dienen, sondern ausschließlich dem Sammeln von Spam-Mails. Durch Auswertung dieser Fallen lassen sich zum einen die Blacklists bekannter Spam-MTAs aktualisieren und zum anderen die Content-Filter trainieren. Auch hier gilt: eigene Kunden sind zu benachrichtigen, falls sie als Absender von Spam identifiziert werden.

4 Vertraulichkeit des E-Mail-Verkehrs

Zur Gewährleistung der Vertraulichkeit des E-Mail-Verkehrs sollte möglichst weitgehend Verschlüsselung eingesetzt werden. Hierzu empfiehlt sich die Umsetzung folgender Maßnahmen:

- Sowohl auf Port 587 als auch auf Port 25 muss die Nutzung von STARTTLS möglich sein, damit sowohl die Übertragung der E-Mails an den Provider-MTA als auch – im Falle einer Authentifizierung (Port 587) – die Übermittlung der Credentials verschlüsselt erfolgen kann. Gleiches gilt für IMAP (STARTTLS) und POP 3 (STLS).
- Das für die verschlüsselte Annahme von E-Mails verwendete Zertifikat oder dessen Hashwert sollte – wie im RFC 6698 DNS-Based Authentication of Named Entities (DANE) beschrieben – per TLSA-Eintrag im DNS veröffentlicht und per DNSSEC signiert werden.
- Bei Nutzung von Web-Mail sollte sowohl die Anmeldung als auch die Sitzung selbst mit der jeweils aktuellen TLS-Version verschlüsselt sein.
- Die Zugangsdaten müssen auf dem Server *gesichert* (d. h. keinesfalls im Klartext) gespeichert werden. Hierzu ist ein entsprechend dem aktuellen Stand der Technik geeignetes Verfahren zu verwenden (z. B. rundenbasiertes Hashverfahren: PBKDF2).
- Für den Kunden sollte die Option bestehen, für seine E-Mails selbst eine Ende-zu-Ende-Verschlüsselung vorzunehmen. Da in diesem Fall eine Virenprüfung durch den Provider nicht möglich ist, sollten diese Mails beim Empfänger – soweit technisch möglich (z. B bei Web-Mail) – entsprechend gekennzeichnet werden, um ihn darauf aufmerksam zu machen, dass er für die Virenprüfung selbst verantwortlich ist.
- Die Übertragung der E-Mails zwischen den Provider-MTAs sollte verschlüsselt erfolgen. Dabei sollte insbesondere auch das Verfahren der Forward Secrecy genutzt werden.
- Der Kunde muss bei vom Provider zur Verfügung gestellten Mail-Clients (z. B. Web-Mailer) die Option haben, E-Mail-Tracking (z. B. das automatische Nachladen von Tracking-Pixeln) abzuschalten.

5 Vertragliche Regelungen mit den Kunden

Das BSI empfiehlt, vertraglich (zum Beispiel in den AGB) mit den Kunden zu vereinbaren, dass die Diensterbringung bei missbräuchlicher Nutzung eingeschränkt werden kann. Dies kann beispielsweise über eine sogenannte „Acceptable Use Policy“ geschehen, die Teil des Vertrags mit dem Kunden ist. Insbesondere sollte darin geregelt sein – bzw. der Kunde darauf hingewiesen werden – dass:

- ein automatischer Scan aus- und eingehender E-Mails auf Spam und Malware erfolgt,
- spezielle Verfahrensweisen für erkannte Malware- oder Spam-verseuchte E-Mails bestehen,
- bei Missbrauch des Internetanschlusses des Kunden zum Versand von Spam und Malware, dieser durch den Provider für den Versand von E-Mails gesperrt werden kann. Der Kunde wird über eine erfolgte Sperrung benachrichtigt und es wird ihm Gelegenheit gegeben, deren Aufhebung selbst zu veranlassen.

Die Maßnahmen zum Schutz vor Spam oder Malware sollten standardgemäß im Nutzerprofil voreingestellt sein. Allerdings sollte der Nutzer auch die Möglichkeit erhalten, diese (auf eigene Verantwortung) teilweise oder ganz zu deaktivieren.

6 Literatur

[1] Sicherer Betrieb von E-Mail-Servern (ISi-S): https://www.bsi.bund.de/dok/6620896

[2] Malware-Schutz: Handlungsempfehlungen für Internet-Service-Provider v1.0: https://www.allianz-fuer-cybersicherheit.de/dok/6621316