Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

SMTP Smuggling ermöglicht Social Engineering per E-Mail

Nr. 2023-292569-1022, Version 1.0, 22.12.2023

IT-Bedrohungslage*: 1 / Grau

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 18. Dezember veröffentlichte das Cybersicherheitsunternehmen SEC Consult Informationen zu einer neuen Angriffstechnik mittels "Simple Mail Transfer Protocol (SMTP) Smuggling". Beim SMTP Smuggling machen sich die Angreifenden zunutze, dass verschiedene SMTP-Implementierungen die Kennzeichnung des Endes einer E-Mail-Nachricht unterschiedlich interpretieren. Sie können so E-Mails versenden, die durch ein betroffenes E-Mail-System in mehrere E-Mails aufgespalten werden. Auf diesem Weg entstehen neue E-Mails, die gefälschte Absender nutzen (Spoofing), Authentifizierungsmechanismen, wie SPF, DKIM und DMARC umgehen oder Warnungen, wie z.B. eine Spam-Markierung in der Betreffzeile, nicht mehr tragen.

Durch die Ausnutzung von Unterschieden in der Interpretation einer Sequenz zwischen ausgehenden und eingehenden SMTP-Servern können Angreifende gefälschte E-Mails im Namen vertrauenswürdiger Domänen versenden. Dies ermöglicht wiederum verschiedenste Social Engineering- bzw. Phishing-Angriffe. Eine detaillierte technische Erklärung von SMTP Smuggling liefert der von SEC Consult veröffentlichte Blogartikel [SEC23].

Im Rahmen des Responsible Disclosure Prozesses des Unternehmens wurden durch SEC Consult identifizierte Großunternehmen (Microsoft, Cisco, GMX/Ionos) mit betroffenen IT-Produkten und IT-Services, vor der Veröffentlichung informiert, um ausreichend Zeit zur Behebung der Schwachstelle zu haben.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Microsoft und GMX haben daraufhin ihre Maildienste vor SMTP Smuggling abgesichert. Cisco hält laut SEC Consult das gefundene Problem in (on-prem / cloud-basiert) Cisco Secure Email (Cloud) Gateway für ein Feature und keine Schwachstelle. Das Problem in Cisco Secure Email Gateway ist das (standardmäßige) CR and LF Handling - dies erlaubt Nachrichten mit CR und LF Zeichen und konvertiert CR und LF Zeichen zu CRLF Zeichen. Dieses Verhalten erlaubt den Empfang von gefälschten Mails mit validem DMARC. [SEC23]

Bewertung

Die Schwachstelle besteht nicht in den zugrunde liegenden Standards, sondern in der oftmals unzureichenden Implementierung der selbigen. Der Angriff ist mit vergleichsweise geringem Aufwand durch eine striktere Interpretation der RFC5321 [RFC08a] und RFC5322 [RFC08b] sowie der Nutzung des BDAT-Kommandos, bei welchem der Sender die Datengröße explizit angibt, mitigierbar.

Maßnahmen

Das BSI empfiehlt, bereitgestellte Patches einzuspielen und sicherzustellen, dass genutzte IT-Systeme so konfiguriert sind, dass nur RFC-konforme Ende-Kennzeichnungen unterstützt werden.

Für das IT-Produkt (on-prem / cloud-basiert) Cisco Secure Email (Cloud) Gateway empfiehlt SEC Consult eine Anpassung der CR and LF Handling Konfiguration auf das Verhalten "Allow" (siehe [CISCO23]), um sich vor Angriffen mittels SMTP-Smuggling zu schützen [SEC23] [CISCO23].

Das BSI informiert bereits über das Warn- und Informationsdienstportal (WID) über bereitstehende Patches bzw. Mitigationsmaßnahmen für Systemanwendende [WID23]. So stellen bspw. die Entwickler von Postfix eine Anleitung für einen Workaround bereit [POST23].

Es ist davon auszugehen, dass auch Hersteller von bislang nicht genannten E-Mailinfrastruktur-Produkten in den kommenden Tagen Workarounds oder Patches veröffentlichen, die den hier beschriebenen Sachverhalt adressieren. IT-Sicherheitsverantwortliche sollten daher die Kommunikationskanäle der Unternehmen, deren Lösungen in der eigenen Institution zum Einsatz kommen, regelmäßig auf Neuigkeiten überprüfen. Bei produktspezifischen Fragen sollte der Kundenservice kontaktiert werden.

Links

[CISCO23] User Guide for AsyncOS 15.0 for Cisco Secure Email Gateway - GD (General Deployment):
https://www.cisco.com/c/en/us/td/docs/security/esa/esa15-0/user_guide/b_ESA_Admin_Guide_15-0/b_ESA_Admin_Guide_12_1_chapter_0100.html?bookSearch=true#task_1254814__table_985308C400C84CE3BC190BC8A3A95D86

[POST23] POSTFIX: SMTP Smuggling:
https://www.postfix.org/smtp-smuggling.html

[RFC08a] Network Working Group: Request for Comments 5321 - Simple Mail Transfer Protocol:
https://datatracker.ietf.org/doc/html/rfc5321

[RFC08b] Network Working Group: Request for Comments 5322 - Internet Message Format:
https://datatracker.ietf.org/doc/html/rfc5322

[SEC23] SEC Consult: SMTP Smuggling - Spoofing E-Mails Worldwide:
https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/

[WID23] [WID-SEC-2023-3206] SMTP Implementierungen: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen:
https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2023-3206

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

  TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
  Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.