NEWS / PRESSEMITTEILUNG

Prüfung der Senderreputation bietet weitgehende Sicherheit vor EFAIL

Neu entdeckte Sicherheitslücke EFAIL in OpenPGP und S/MIME ist bei der integrierten Nutzung von E-Mail-Verschlüsselung und Senderreputationsmanagement keine Bedrohung. NoSpamProxy-Kunden sind damit auf der sicheren Seite.

Paderborn, 15. Mai 2018 – Net at Work GmbH, der Hersteller der modularen Secure-Mail-Gateway-Lösung NoSpamProxy aus Paderborn, gibt heute Entwarnung im Zusammenhang mit der aktuell breit diskutierten Sicherheitslücke EFAIL.

Prüfung der Senderreputation bietet weitgehende Sicherheit vor EFAIL

Verschlüsselungstechnik OpenPGP und S/MIME betroffen

Unter dem Begriff EFAIL wurde vor wenigen Tagen eine Sicherheitslücke beschrieben, mit der unter bestimmten Umständen Bestandteile einer verschlüsselten E-Mail zugänglich gemacht werden können. Dazu muss der Angreifer zunächst in den Besitz der verschlüsselten E-Mail gelangen. Diese wird dann – vereinfacht gesagt – mit einem Schadcode modifiziert erneut an den Empfänger gesendet oder weitergeleitet. Beim automatischen Nachladen von Bildern kann dann der Schadcode ausgeführt werden, der den reinen Textinhalt der E-Mail ganz oder teilweise freigibt.

Betroffen sind hiervon E-Mail-Clients mit entsprechenden S/MIME- oder PGP-Plugins, die automatisch Inhalte nachladen und zudem nicht korrekt auf die Manipulation reagieren. Auch Gateway-basierte Lösungen können betroffen sein, wenn sie nicht intensiv die Möglichkeiten zur Bewertung der Senderreputation nutzen.

„OpenPGP und S/MIME sind an sich gute und sichere Komponenten zur E-Mail-Verschlüsselung, die durch Secure-Mail-Gateways wie NoSpamProxy mittlerweile auch sehr benutzerfreundlich und wartungsarm genutzt werden können“, sagt **Stefan Cink, E-Mail-Sicherheitsexperte bei Net at Work**. *„Umso wichtiger ist es, potentielle Gefahrenquellen gewissenhaft zu bewerten und zu schließen.*“

Schadenswahrscheinlichkeit richtig einschätzen

Zunächst einmal ist das Abgreifen der verschlüsselten Mails in Zeiten von Transportverschlüsselung wie TLS nicht einfach und erfordert ein hohes Maß an technischen Möglichkeiten, die typischen Hackern in der Regel nicht – sehr wohl aber Nachrichtendiensten – zur Verfügung stehen. Aber selbst, wenn dies gelingt, sind die Angreifer noch nicht am Ziel. Sie müssen die Mail erneut an den Empfänger versenden. Moderne Secure-Mail-Gateways wie NoSpamProxy nutzen hier intensiv die Möglichkeiten von SPF, DKIM und DMARC um zweifelhafte Mails zurückzuweisen.

Dabei ist es wichtig, dass das Gateway alle drei Elemente richtig kombiniert. Nur mit der gemeinsamen Auswertung von SPF-, DKIM- und DMARC-Informationen kann zweifelsfrei sichergestellt werden, dass eine Mail von dem Server kommt, von dem sie vorgibt zu kommen. Darüber hinaus kann die Manipulation der E-Mail anhand der DKIM Signatur entdeckt werden. Eine manipulierte Mail – auch verschlüsselt – wird als zweifelhaft erkannt werden und kann so zurückgewiesen werden, bevor sie Schaden anrichten kann. Über das DMARC-Reporting werden zudem die betroffenen Parteien informiert. Wird für den Versand von E-Mails auch die DANE-Information einbezogen, kann sichergestellt werden, dass sich kein Angreifer zwischen Sender und Empfänger einklinken kann, indem eine TLS-verschlüsselte Verbindung aufgebaut wird.

NEWS / PRESSEMITTEILUNG

Tipps zur individuellen Prüfung und Maßnahmen zur Vorsorge

Wer sich Sorgen macht, sollte folgende Punkte prüfen: Ist die eingesetzte Secure-Mail-Infrastruktur aktuell und nutzt sie die Senderreputation intensiv zur Abwehr zweifelhafter Mails? Sind die eigenen SPF-, DKIM- und DMARC-Records richtig eingerichtet? Wer hier passen muss, kann als Übergangslösung auf Plain-Text- statt HTML-Mails umstellen, auch wenn dies die Nutzer erheblich einschränken und so für erhebliche Irritationen sorgen wird. Damit wird diese Angriffsmöglichkeit zwar nicht vollständig verhindert, aber es wird für den Angreifer aufwendiger. Mittelfristig kommt man jedoch um eine moderne, integrierte Lösungen für Anti-Spam/Anti-Malware und Verschlüsselung nicht herum.

Entgegen der teilweise verbreiteten Panikmache, empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer aktuellen Pressemeldung, dass OpenPGP und S/MIME *„nach Einschätzung des BSI allerdings weiterhin sicher eingesetzt werden können, wenn sie korrekt implementiert und sicher konfiguriert werden.“* Allerdings erwarten die Experten, dass die Standards für OpenPGP und S/MIME angepasst werden müssen. Für letzteren ist mit dem S/MIME 4.0-Standard eine Lösung bereits absehbar, die mit der sogenannten "Authenticated Encryption" diese Angriffsform sicher abwehren kann.

„Das Beispiel EFAIL zeigt wieder einmal, dass die Zukunft der sicheren E-Mail-Kommunikation in zentral administrierten, integrierten Secure-Mail-Lösungen liegt. Nur mit der Kombination aller verfügbaren Sicherheitsmechanismen – wie hier der Senderreputation aus dem Spam- und Malwareschutz mit der Verschlüsselung – lassen sich die immer perfideren Angriffsmuster sicher und effizient abwehren, ohne die Nutzer einzuschränken“, zieht **Cink** als Lehre aus der aktuellen Diskussion.

Gateway-Lösungen erneut einfacher und damit sicher in der Administration

Auch wenn NoSpamProxy heute schon einen guten Schutz gegen diese Verwundbarkeit bietet, nutzt Net at Work dennoch die Gelegenheit, den Schutz in diesem Kontext weiter zu verbessern und wird kurzfristig ein Update für NoSpamProxy veröffentlichen, wenn die Analyse und Entscheidung über bestmögliche Gegenmaßnahmen abgeschlossen ist. Auch hier zeigen sich die Vorteile der Gateway-Technik: Während bei clientbasierten Lösungen sichergestellt werden muss, dass der bereitgestellte Fix auf allen Clients mit ihren potentiell unterschiedlichsten Softwareständen richtig installiert und ausgeführt wird, reicht bei zentral administrierten Secure-Mail-Gateways das Update an einer Stelle aus.

Weitere Informationen über die integrierte Mail-Security-Suite NoSpamProxy:
https://www.nospamproxy.de

Net at Work bietet einen detaillierten Ratgeber zur Einrichtung von DMARC & Co.:
https://www.nospamproxy.de/de/ratgeber-dmarc-dkim-spf-dane/

Zusammenfassung

Net at Work kommentiert die neu entdeckte Sicherheitslücke EFAIL in OpenPGP und S/MIME. Bei der integrierten Nutzung von E-Mail-Verschlüsselung und Senderreputationsmanagement ist sie keine Bedrohung. NoSpamProxy-Kunden sind damit auf der sicheren Seite.

Keywords

EFAIL, OpenPGP, S/MIME, E-Mail-Verschlüsselung, Senderreputation, DMARC, DKIM, SPF, Secure E-Mail, Gateway

Über Net at Work und NoSpamProxy

Die 1995 gegründete Net at Work GmbH ist Softwarehaus und Systemintegrator mit Sitz in Paderborn. Gründer und Gesellschafter des Unternehmens sind Geschäftsführer Uwe Ulbrich und Frank Carius, der mit www.msxfaq.de eine der renommiertesten Websites zu den Themen Exchange und Skype for Business betreibt.

NEWS / PRESSEMITTEILUNG

Als Softwarehaus entwickelt und vermarktet Net at Work mit NoSpamProxy eine integrierte Gateway-Lösung für Secure E-Mail. NoSpamProxy bietet sichere Anti-Malware-/Anti-Spam-Funktionen, eine automatisierte E-Mail-Verschlüsselung sowie einen praxistauglichen Large File Transfer auf einer technischen Plattform. So garantiert der modulare Ansatz von NoSpamProxy eine vertrauliche und rechtssichere E-Mail-Kommunikation. Die Experton Group sieht NoSpamProxy als Product Challenger für E-Mail- und Web-Kollaboration. Zu den mehr als 1.800 Unternehmen, die die Sicherheit ihrer Mail-Kommunikation NoSpamProxy anvertrauen, gehören u. a. DaimlerBKK, Deutscher Ärzte-Verlag, Hochland, Komatsu Mining, das Kommunale RZ Minden-Ravensberg/Lippe und SwissLife. Weitere Informationen zur E-Mail Security Suite NoSpamProxy finden Sie unter www.nospamproxy.de.

Im Servicegeschäft bietet Net at Work ein breites Lösungsportfolio rund um die IT-gestützte Kommunikation und die Zusammenarbeit im Unternehmen mit einem besonderen Schwerpunkt auf dem Portfolio von Microsoft. Als Microsoft Gold Partner für Messaging, Communications, Collaboration and Content, Cloud Productivity und Application Development gehört Net at Work zu den wichtigsten Systemintegratoren für Microsoft Exchange, SharePoint und Skype for Business. Das erfahrene Team von langjährigen IT-Experten verfügt über umfassendes Know-how bei der Umsetzung individueller Kundenanforderungen und berücksichtigt bei Projekten neben der Skalierbarkeit, Flexibilität und Sicherheit der Lösung auch die Einhaltung der definierten Zeit- und Budgetziele. Kunden finden somit bei allen Fragen kompetente Ansprechpartner, die ihnen helfen, modernste Technologien effizient und nahtlos in bewährte Geschäftsprozesse zu integrieren. Zu den Kunden im Servicegeschäft gehören u. a. Goldbeck, Miele, die Spiegel Gruppe, die Universität Duisburg-Essen sowie Diebold Nixdorf.

Weitere Informationen zum Unternehmen Net at Work und dem Serviceangebot finden Sie unter www.netatwork.de.

Unternehmenskontakt

Frau Aysel Nixdorf, Marketing & PR, T +49 5251 304627, aysel.nixdorf(at)netatwork.de
Net at Work GmbH, Am Hoppenhof 32 A, D-33104 Paderborn, www.netatwork.de

Pressekontakt

Team Net at Work, T +49 7721 9461 220, netatwork(at)bloodsugarmagic.com
bloodsugarmagic GmbH & Co. KG, Gerberstr. 63, D-78050 Villingen-Schwenningen, www.bloodsugarmagic.com