NEWS / PRESSEMITTEILUNG

Sicherheitsrisiko verschlüsselte PDF-Dateien? Erste Beurteilung und mögliche Alternativen

Bochumer Forschungsgruppe veröffentlicht eine Sicherheitslücke bei verschlüsselten PDF-Dateien. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) äußert sich in einer Vorinformation dazu. NoSpamProxy klärt auf, für wen welche Risiken tatsächlich bestehen und wer betroffen ist. Zudem werden Alternativen für Organisationen mit besonderen Sicherheitsanforderungen aufgezeigt.

Paderborn, 30. September 2019 – Net at Work GmbH, der Hersteller der modularen Secure-Mail-Gateway-Lösung NoSpamProxy aus Paderborn, erläutert eine aktuelle Sicherheitslücke bei verschlüsselten PDF-Dateien.

Viele Firmen nutzen verschlüsselte PDF-Dateien, um z.B. mit ihren Kunden DSGVO-konform zu kommunizieren, wenn diese nicht über Zertifikate oder Schlüssel verfügen, um bewährte und sichere Verschlüsselungsverfahren wie S/MIME oder PGP nutzen zu können. Unter bestimmten Bedingungen können Inhalte von verschlüsselten PDFs zugänglich gemacht werden. Ähnlich wie schon bei der vor einem Jahr unter dem Titel „Efail“ veröffentlichten Sicherheitslücke erfordert auch das nun beschriebene Angriffsszenario, dass der Angreifer die Mail mit der angehängten verschlüsselten PDF-Datei abfängt und die PDF-Datei durch eigenen Schadcode verändert. Nach Eingabe des Schlüssels durch den Empfänger wird der Inhalt dann über den ergänzten Code an den Angreifer übermittelt. Das bedeutet, dass der Angriff ohne Mitwirkung des Empfängers nicht funktioniert.

Wer ist betroffen?

Der Angriff richtet sich ausschließlich gegen Empfänger von verschlüsselten und passwortgeschützten PDF-Dateien auf deren Client. Firmen, die Mail-Gateways nutzen, um ausgehende Mails automatisch DSGVO-konform zu versenden, sind nicht betroffen.

Welche Maßnahmen werden empfohlen?

- Wo möglich, konsequente Nutzung und Erzwingung von Transportverschlüsselung durch TLS beim Mailversand (Force-TLS) – hierdurch wird der Empfänger zuverlässig vor Man-in-the-Middle-Attacken geschützt
- Umfassende Prüfung der Absenderreputation im empfangenden Mail-Sicherheitssystem
- Durch intelligentes Anhangsmanagement können verschlüsselte PDF-Dateien von nicht bekannten Absendern entweder abgelehnt oder in einer Quarantäne zur weiteren Prüfung zurückgehalten werden
- Wenn ein besonders hohes Schutzbedürfnis besteht: Umstellung auf alternative Verfahren über ein Webportal
- Falls AES mit 256 Bit in der PDF-Verschlüsselung genutzt wird, kann auf 128 Bit umgestellt werden, da das Angriffsmuster bei AESV2 (AES128-CBC) erschwert ist
- Endanwender, die über die vorgenannten Möglichkeiten nicht verfügen, sollten passwortgeschützte verschlüsselte PDF-Dateien nur dann öffnen, wenn sie von vertrauenswürdigen Absendern kommen, die die vorgenannten Maßnahmen zum Schutz der Empfänger umgesetzt haben

NEWS / PRESSEMITTEILUNG

- Endanwender sollten ihren PDF-Reader sofort auf die aktuellste Version umstellen. So ist der meistverwendete Adobe PDF-Reader in der aktuellen Version 2019.012.20040 vom 22.08.2019 bereits sicher vor dem berichteten Angriff

Bewertung des Angriffs-Szenarios

Nach Einschätzung des BSI und auch unserer Mail-Security-Experten ist die Wahrscheinlichkeit eines Angriffs sehr gering und eine breite Verwendung des Angriffsmusters kaum möglich. Ein Grund hierfür ist vor allem, dass der Angreifer Zugang zum PDF - also der Mail - haben muss, was in der Regel schwer umsetzbar ist (er müsste sich ja bei einem Provider auf dem Weg der Mail eingenistet oder das Gateway kompromittiert haben). In der Praxis werden die Angriffe mit Blick auf den Aufwand und die Hürden eher mit nachrichtendienstlichen Zielen erfolgen und nicht in Form von klassischer Cyberkriminalität. Zudem waren die Angriffe der Forschungsgruppe nur bei teilweise und auch nur bei deutlich veralteten Softwareversionen erfolgreich.

Wie geht es weiter?

Die Nutzerakzeptanz von verschlüsselten PDFs ist im Vergleich zur Nutzung von Portallösungen – wie dem NoSpamProxy Webportal – deutlich höher. Dennoch sollten Organisationen mit besonderen Sicherheitsanforderungen die Möglichkeit in Betracht ziehen, auf die Bereitstellung über das Webportal umzustellen. Das kann durch eine einfache Konfigurationsänderung aktiviert werden. Um mögliche Akzeptanzprobleme zu minimieren, sollten die Nutzer entsprechend informiert werden. Für besonders sicherheitssensible Kunden wird NoSpamProxy kurzfristig eine angepasste Version bereitstellen, mit der diese Umstellung automatisch erfolgen kann.

Wenn Sie das Thema direkt mit uns diskutieren möchten, treffen Sie uns doch nächste Woche auf der it-sa. Sie können unter folgender URL einen Termin vereinbaren oder ein kostenloses Ticket für die it-sa anfordern: https://www.nospamproxy.de/de/it-sa-2019/

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

Hier finden Sie die Meldung der Universität Bochum:
https://news.rub.de/wissenschaft/2019-09-30-informationstechnik-sicherheitsluecken-pdf-verschluesselung

Zusammenfassung

Die berichtete Sicherheitslücke bei PDF-Dateien betrifft prinzipiell alle Anwender, die auf ihren Clients nicht die aktuellste Version der weit verbreiteten Adobe PDF-Reader-Software einsetzen. Angreifer müssen jedoch Mails mit solchen Anhängen zuvor abfangen (Man-in-the-Middle) und entsprechend modifizieren. Zudem muss der Angegriffene auch noch mitwirken. Ein massenhafter Angriff ist nicht zu befürchten. Firmen, die das Mail-Security-Gateway NoSpamProxy einsetzen, können auf andere Verschlüsselungsverfahren ausweichen.

Keywords

Sicherheitslücke, Verschlüsselte PDF-Dateien, PDFfail, Malware, Anhangsmanagement, Mail-Verschlüsselung

Über NoSpamProxy und Net at Work

Net at Work unterstützt als IT-Unternehmen seine Kunden mit Lösungen und Werkzeugen für die digitale Kommunikation und Zusammenarbeit. Der Geschäftsbereich Softwarehaus entwickelt und vermarktet mit NoSpamProxy ein innovatives Secure E-Mail-Gateway mit erstklassigen Funktionen für Anti-Spam, Anti-Malware und E-Mail-Verschlüsselung, dem weltweit mehr als 4.000 Kunden die Sicherheit ihrer E-Mail-Kommunikation anvertrauen. Die mehrfach ausgezeichnete

NEWS / PRESSEMITTEILUNG

Lösung – unter anderem Testsieger im unabhängigen techconsult Professional User Ranking – wird als Softwareprodukt und Cloud-Service angeboten. Mehr zum Produkt unter: www.nospamproxy.de

Im Servicegeschäft ist Net at Work als führender Microsoft-Partner mit acht Gold-Kompetenzen erste Wahl, wenn es um die Gestaltung des Arbeitsplatzes der Zukunft auf Basis von Microsoft-Technologien wie Office 365, SharePoint, Exchange, Skype for Business, Teams sowie Microsoft Azure als cloudbasierte Entwicklungsplattform geht. Dabei bietet das Unternehmen die ganze Bandbreite an Unterstützung: von punktueller Beratung über Gesamtverantwortung im Projekt bis hin zum Managed Service für die Kollaborationsinfrastruktur. Über die technische Konzeption und Umsetzung von Lösungen hinaus sorgt das Unternehmen mit praxiserprobtem Change Management dafür, dass das Potential neuer Technologien zur Verbesserung der Zusammenarbeit auch tatsächlich ausgeschöpft wird. Net at Work schafft Akzeptanz bei den Nutzern und sorgt für bessere, sichere und lebendige Kommunikation, mehr und effiziente Zusammenarbeit sowie letztlich für stärkere Agilität und Dynamik im Unternehmen.

Die Kunden von Net at Work finden sich deutschlandweit im gehobenen Mittelstand wie beispielsweise Diebold-Nixdorf, CLAAS, Miele, Lekkerland, SwissLife, Uni Rostock, Würzburger Versorgungs- und Verkehrsbetriebe und Westfalen Weser Energie.

Net at Work wurde 1995 gegründet und beschäftigt derzeit mehr als 100 Mitarbeiter in Paderborn und Berlin. Gründer und Gesellschafter des inhabergeführten Unternehmens sind Uwe Ulbrich als Geschäftsführer und Frank Carius, der mit www.msxfaq.de eine der renommiertesten Websites zu den Themen Office 365, Exchange und Skype for Business betreibt. 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