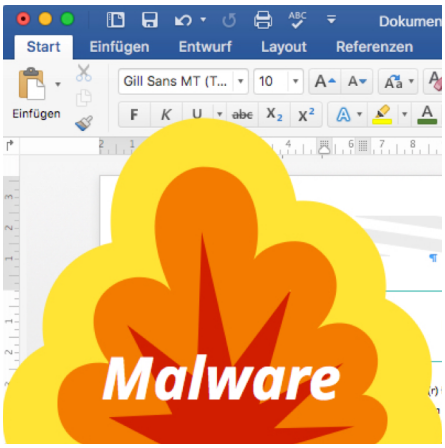
NEWS / PRESSEMITTEILUNG

DDE-Sicherheitslücke in Microsoft Office bereits Teil von E-Mail-Attacken

Sicherheitslücke durch Microsoft-Office-Dokumente in Mails ermöglicht Angreifern Zugriff auf Systeme. Bislang kein Patch von Microsoft angekündigt. Nur flexibles Content Disarming bietet Schutz.

Paderborn, 19. Oktober 2017 – Net at Work GmbH, der Hersteller der modularen Secure-Mail-Gateway-Lösung NoSpamProxy aus Paderborn, weist auf eine aktuell neue Bedrohungslage durch Mail-Anhänge hin.



Flexibles Content Disarming von NoSpamProxy verhindert aktuelle Malware-Attacken auf DDE-Sicherheitslücke

Nachdem Sicherheitsforscher in der vergangenen Woche eine schwerwiegende Sicherheitslücke in Microsoft Office entdeckt haben, wird diese bereits in konkreten E-Mail-Angriffen ausgenutzt. Durch speziell präparierte Dateien im Microsoft-Excel- oder Microsoft-Word-Format können Angreifer nach der Öffnung der Dateien seitens des Benutzers beliebigen Code auf dem System des Benutzers ausführen. Dadurch erhalten die Hacker Zugriff auf den Windows-Rechner.

Aktuell wird Zunahme derartiger Attacken registriert

Diese Lücke wird zunehmend in Mail-Attacken mit entsprechenden Anhängen ausgenutzt. Das renommierte SANS Institute hat bereits eine deutliche Zunahme an Attacken mit alten Malware-Bekannten wie Hancitor registriert. So wurde am Montag ein massiver Anstieg derartiger Angriffe beobachtet.

Die Sicherheitslücke tritt unter Verwendung von Dynamic Data Exchange (DDE) auf. Dieses Protokoll dient dem Austausch von Applikationen und wird unter anderem von Excel verwendet, um externe Informationen einzubinden. Nach einem erfolgreichen Angriff sind alle Daten auf den betroffenen Systemen gefährdet. Diese Sicherheitslücke wird durch die von Microsoft am 10.10.2017 veröffentlichten Patches noch nicht geschlossen. Daher müssen die eingesetzten E-Mail-Security-Lösungen verlässliche Sicherheit bieten.

Nur flexibles Content Disarming schafft Sicherheit

Mithilfe eines intelligenten Anhangsmanagements lassen sich derartige Angriffe durch sogenanntes Content Disarming sicher abwehren. Dabei wandelt das Secure-Mail-Gateway Anhänge im Word- und Excel-Format regelbasiert und automatisiert in unkritische PDF-Dateien um. So gelangt potenziell vorhandener Schadcode nicht in das Firmennetzwerk. Der Empfänger erhält dadurch einen garantiert ungefährlichen Anhang. Im PDF-Dokument findet sich eine Vorschaltseite, auf der individuelle Hinweise zum Grund der Konvertierung aufgeführt sind und – sofern gewünscht – auch ein Link zum Originaldokument, das sich in einer speziellen Quarantäne befindet.

Aktuelle Version 12.0 von NoSpamProxy steuert Content Disarming über die Reputation des Senders

In der aktuellen Version 12.0 von NoSpamProxy ist genau das möglich. NoSpamProxy kombiniert Content Disarming mit dem einzigartigen Level-of-Trust-Konzept und der Senderreputation. Im Falle einer akuten Bedrohungslage wie der aktuellen DDE-Lücke, können NoSpamProxy-Kunden einfach per Regel einstellen, dass

NEWS / PRESSEMITTEILUNG

Attachments von neuen oder unbekannten Sendern grundsätzlich über das Content Disarming laufen, während die Mails von Sendern mit höherer Reputation ungehindert passieren können. Erst diese feingliedrige Steuerbarkeit macht den Schutzmechanismus praxistauglich, da die normale Zusammenarbeit der Nutzer nicht gestört wird. Zudem senkt sie die Hemmschwelle für die IT, Content Disarming als wirksames Instrument einzusetzen, da die Beeinträchtigung der Nutzer auf ein Minimum reduziert wird.

„Content Disarming ist eine wirksame Maßnahme zum Schutz vor Malware-Anhängen in Mails. Erst wenn man dieses Instrument sehr zielgenau einsetzen kann, wird es praxistauglich. Dies ist ein weiterer Beleg dafür, dass ohne eine leistungsstarke und feingliedrige Bewertung der Senderreputation kaum noch ein praktikabler Schutz vor Malware und Spam gelingen kann“, sagt **Stefan Cink, E-Mail-Sicherheitsexperte bei Net at Work**.

Hintergrundinformationen zu dieser Sicherheitslücke erhalten Sie hier:
https://isc.sans.edu/forums/diary/Hancitor+malspam+uses+DDE+attack/22936/

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

Zusammenfassung

Eine neue Sicherheitslücke durch Microsoft-Office-Dokumente in Mails ermöglicht Angreifern Zugriff auf Systeme. Bislang wurde kein Patch von Microsoft dafür angekündigt, deshalb kann nur ein flexibles Content Disarming sicheren Schutz bieten.

Keywords

DDE, Sicherheitslücke, Hancitor, Senderreputation, Secure E-Mail, Gateway, Anti-Virus, Anti-Spam, Anti-Malware

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.

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 2.000 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 Wincor 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

NEWS / PRESSEMITTEILUNG

Pressekontakt

Herr Bernd Hoeck, Managing Partner, T +49 7721 9461 220, bernd.hoeck(at)bloodsugarmagic.com
bloodsugarmagic GmbH & Co. KG, Gerberstr. 63, D-78050 Villingen-Schwenningen, www.bloodsugarmagic.com