MEDIA ALERT / PRESSEMITTEILUNG

Internet-Betrugsmasche - aus LEONI-Fall lernen

Aktueller Betrugsfall mit gefälschten internen Mails macht Sicherheitslücken in gängigen Mail-Security-Lösungen deutlich. Schnelle Überprüfung der eigenen Infrastruktur bringt Sicherheit.

Paderborn, 17. August 2016 – Die Net at Work GmbH, Hersteller der modularen Secure-E-Mail-Gateway-Lösung NoSpamProxy aus Paderborn, empfiehlt Unternehmen und Organisationen aus dem € 40 Mio. Betrugsfall durch mangelnde Mail-Security bei LEONI zu lernen.

Am Freitag hat die LEONI AG aus Nürnberg bekannt gegeben, dass sie Opfer betrügerischer Handlungen unter Verwendung gefälschter Dokumente und Identitäten, sowie Nutzung elektronischer Kommunikationswege wurde. In deren Folge wurden Gelder des Unternehmens auf Zielkonten im Ausland transferiert. Die Ermittlungen der Kriminalpolizei laufen. Die Täter nutzten dabei eine Methode, die als „CEO-Fraud“ oder „Chefbetrug“ seit langem bekannt ist und immer häufiger angewendet wird. Nach Aussagen des Bundeskriminalamts sind in Deutschland seit 2013 rund 60 Betrugsfälle mit einem Gesamtschaden von 106 Millionen Euro bekannt geworden. Eine Meldepflicht gibt es aber nicht, so dass es auch eine Dunkelziffer geben dürfte. Das Volumen des aktuellen Schadens in Höhe von 40 Mio. Euro zeigt die Brisanz des Themas.

Kern des „CEO-Frauds“ oder des „Chefbetrugs“ sind gefälschte interne Mails, die vorgeben, von der Geschäftsführung oder anderen leitenden Mitarbeitern zu sein. Leider erkennt nach Recherchen von Net at Work die große Masse der am Markt erhältlichen Secure-Mail-Lösungen diese gefälschten Mails nicht als solche.. Net at Work erklärt anhand seines Secure-Mail-Gateways NoSpamProxy, wie dies geschehen kann:

Um gefälschte, angebliche interne E-Mails sicher von echten Mails des Chefs unterscheiden zu können, wendet NoSpamProxy ein 2-stufiges Sicherheitskonzept an. In der ersten Stufe wird eine Prüfung des Mail-Envelope durchgeführt. Neben anderen Merkmalen ist ein wesentlicher Punkt, die IP-Adresse des sendenden Mail-Servers zu prüfen. Wenn eine Mail aus der eigenen E-Mail-Domain empfangen wird, muss die IP Adresse mit einer der Adressen übereinstimmen, die im NoSpamProxy hinterlegt sind. Wurde die E-Mail von einer anderen IP-Adresse – d.h. einem nicht-autorisierten Mail-Server - gesendet, wird sie abgewiesen.

In der zweiten Stufe wird der Mail-Header geprüft: Das E-Mail Gateway weiß, dass eine zu prüfende Mail von extern gesendet wurde. Dann wird geprüft, ob die eigene Domain („meinunternehmen.de“) in der Absenderadresse vorkommt. Da eine interne Mail im Regelfall nicht von extern gesendet wird, kann die Mail ebenfalls rückgewiesen werden. Einfache Prüfungen könnte theoretisch auch jeder Anwender selbst durchführen. In der Praxis scheitert dies jedoch an der technischen Kompetenz der Mitarbeiter und auch am Zeitbedarf, unter hohem Arbeitsdruck zusätzliche Prüfungen und Rückversicherungen vorzunehmen.

Neben den genannten Verfahren nutzt NoSpamProxy weitere Merkmale zur Prüfung, die jedoch verständlicherweise geheim gehalten werden. Technisch ist es folglich kein Hexenwerk, Betrugsversuche nach der „Chef-Masche“ erfolgreich abzuwehren.

„Wir sind von der Häufigkeit und Höhe der Schäden, die durch diese Attacken verursacht werden, ebenfalls überrascht. Aber es bestätigt auch unseren innovativen Ansatz, komplexe neue Bedrohungen durch intelligent vernetzte Filter, Regeln und Prüfungen zu verhindern“, sagt **Uwe Ulbrich,** Geschäftsführer bei Net at Work. *„Die konsequente Bewertung der Senderreputation - und dazu gehört natürlich die Validierung des Absenders – sollte in keinem Secure-Mail-Gateway fehlen. Jedes Unternehmen sollte prüfen, ob die eingesetzte Mail-Security-Infrastruktur dies aktuell bereits leistet.“*

Als besonderen Service bietet Net at Work Unternehmen und anderen Organisationen, die ihre Mail-Security-Infrastruktur auf diese Lücke hin untersuchen wollen, fundierte Unterstützung an. Interessenten können sich gerne per Mail oder telefonisch unter anfragen@netatwork.de oder 05251-304-600 melden.

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

Interessenten können NoSpamProxy zudem mit telefonischer Unterstützung kostenlos testen:
https://www.nospamproxy.de/de/produkt/testversion

Keywords

LEONI, CEO-Fraud, Chefbetrug, Mail Security , Senderreputation, Secure E-Mail, Gateway, 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 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 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

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