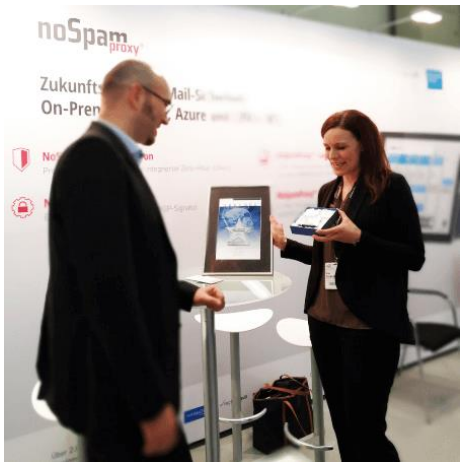
NEWS / PRESSEMITTEILUNG

Spear-Phishing und CEO-Fraud: In der Praxis versagen die meisten Mail-Security-Systeme

Mail-Security-Experten testen Schutz vor Spear-Phishing und CEO-Fraud in mehreren Live-Hackings auf der IT-Security-Conference. Unnötigerweise versagen die meisten Systeme.

Paderborn, 24. Oktober 2017 – Net at Work GmbH, der Hersteller der modularen Secure-Mail-Gateway-Lösung NoSpamProxy aus Paderborn, zieht ein ernüchterndes Resümee aus einer Folge von Live-Hacking-Workshops im Rahmen der diesjährigen IT-Security-Konferenzreihe der Vogel Business Akademie.

Die meisten getesteten Systeme versagten bei CEO-Fraud- oder Spear-Phishing-Attacken – obwohl solche Attacken mit wenig Aufwand und den richtigen Technologien vergleichsweise einfach abgewehrt werden könnten.



Svenja Mohn vom Vogel IT Verlag überreicht den Best Workshop Speaker Award an Stefan Cink von Net at Work

Live-Hacking-Workshops offenbaren Schwachstellen

In den Workshops zeigten die Mail-Security-Experten von Net at Work, wie einfach gängige Mail-Security-Systeme zu überlisten sind und welche Gegenmaßnahmen jedes Unternehmen treffen sollte. Dazu wurden in den Workshops – natürlich nicht schädliche – Angriffe auf die von Teilnehmern freiwillig bereitgestellten E-Mail-Adressen durchgeführt. Obwohl der angreifende Security-Experte von Net at Work keinerlei Kenntnis über die eingesetzten Mail-Security-Lösungen der Betroffenen hatte, waren die Angriffe in kurzer Zeit erfolgreich.

Nur mit einer E-Mail-Adresse und zwei oder drei weiteren Angaben, die jeder über XING oder andere Online-Quellen schnell recherchieren kann, haben die Experten von Net at Work eine täuschend echt aussehende Spear-Phishing-Mail erstellt, die für den Angegriffenen in seiner Mailbox so aussah, als sei diese von seiner Bank gekommen. Eine zweite Variante täuschte im klassischen CEO-Fraud-Muster vor, von einem Kollegen oder Vorgesetzten zu stammen. Innerhalb von Minuten drangen die Angriffe zu den Nutzern durch. Besonders auffällig war, dass alle cloudbasierten Security-Lösungen sofort beim ersten Versuch überwunden wurden.

Die Workshop-Teilnehmer waren von den frappierenden Erkenntnissen des Workshops und den wertvollen Praxistipps so begeistert, dass sie **Stefan Cink**, Produktmanager von NoSpamProxy, zum besten Workshop-Speaker im Bereich IT-Security der diesjährigen Veranstaltungsreihe gewählt haben.

BSI betont die Bedrohungslage und empfiehlt technische Verifizierung der Absenderadresse

Für Angreifer ist es heute – auch mittels der durch Social Media erzeugten Transparenz – sehr einfach, täuschend echt wirkende Mails zusammenzubauen. Vor dem Hintergrund der stetig wachsenden Bedrohungslage ist es unverständlich, warum dieser Sicherheitslücke nicht viel mehr Aufmerksamkeit gewidmet wird. Nicht umsonst weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf die akute Gefährdungslage durch CEO-Fraud hin. *„CEO Fraud ist ein einträgliches Geschäftsmodell für die organisierte Kriminalität, auf das wir als nationale Cyber-Sicherheitsbehörde schon seit Jahren hinweisen",* sagte **Arne Schönbohm**, Präsident des BSI in einer Pressemitteilung vom 10.7.2017.

Das BSI empfiehlt – neben diversen organisatorischen Maßnahmen – als technische Maßnahme explizit die gründliche Verifizierung der Absenderadresse. Dazu existieren bereits seit längerem die notwendigen technischen Grundlagen, die Net at Work in einem kostenlosen Praxisleitfaden zusammengefasst hat.

Net at Work gibt Praxistipps zur Nutzung von Senderreputation

Im Praxisleitfaden beschreiben die Entwickler von NoSpamProxy die verfügbaren Standards und geben praktische Hinweise zur Umsetzung, die unter anderem auch vom TeleTrusT-Verband unterstützt werden. Im Detail wird beschrieben, wie Verwaltungen, Organisationen und Unternehmen auch ohne teure Werkzeuge die relevanten Funktionen DMARC, DKIM, SPF und DANE zur besseren Absicherung des E-Mail-Verkehrs nutzen können und sich damit besser vor Spear-Phishing und CEO-Fraud schützen können.

Dazu ist es notwendig, dass die Mail-Security-Lösungen diese Informationen auch gewissenhaft auswerten, was leider – wie der Test gezeigt hat – bei vielen gängigen Produkten im Markt nicht erfolgt. NoSpamProxy von Net at Work geht sogar noch einige Schritte weiter und verwendet ein sehr umfangreiches Prüfsystem zur Senderreputation.

Den Praxisratgeber mit Schritt-für-Schritt-Anleitungen können Interessenten kostenlos unter folgendem Link anfordern: https://www.nospamproxy.de/de/ratgeber-dmarc-dkim-spf-dane

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

Zusammenfassung

Tests mit konkreten Installationen zeigen: Die meisten Mail-Security-Systeme versagen bei Spear-Phishing und CEO-Fraud. Dabei sind passende Maßnahmen nicht schwer. Ein kostenloser Praxisratgeber beschreibt die notwendigen Einstellungen.

Keywords

Mail-Security, CEO-Fraud, Spear-Phishing, Senderreputation, Secure E-Mail, Gateway, Anti-Virus, Anti-Spam, Anti-Malware, Large File Transfer, Mail-Verschlüsselung, Disclaimer

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