NEWS / PRESSEMITTEILUNG

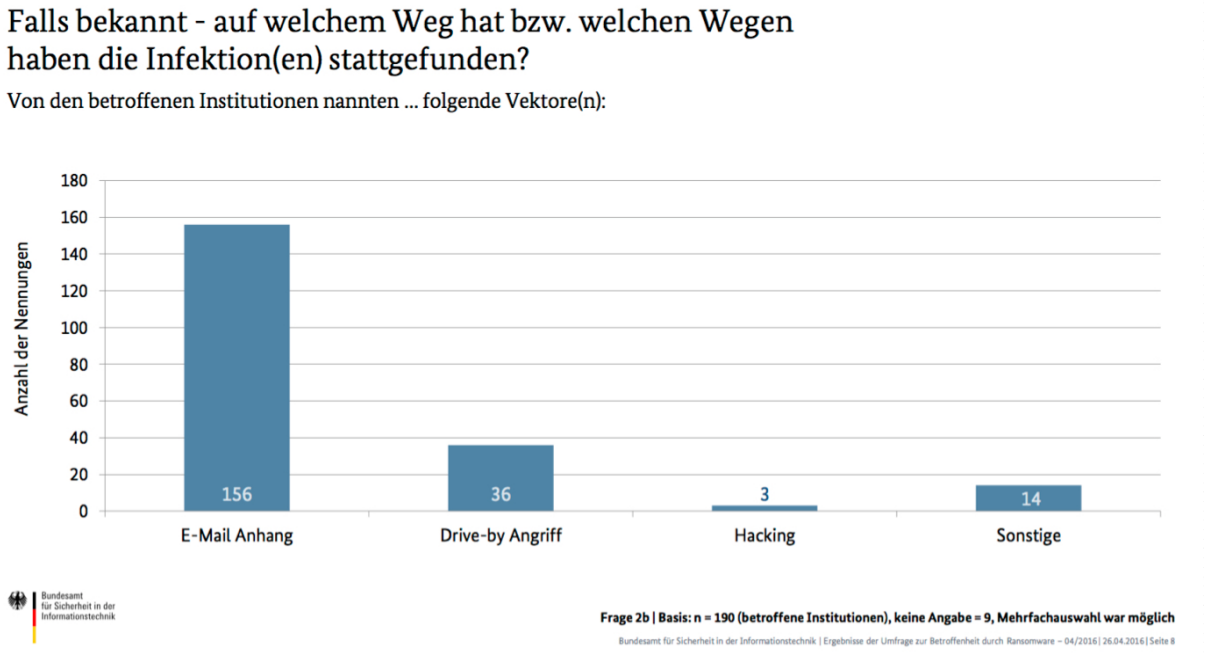
Bedrohung durch Ransomware stark gestiegen

E-Mail bleibt mit Abstand häufigstes Einfallstor für Malware im Unternehmen. Aktuelle Studie der Allianz für Cyber-Sicherheit macht wachsende Bedrohungslage deutlich. Integrierte Secure-E-Mail-Gateways bieten wirksameren Schutz.

Paderborn, 11. Mai 2016 – Die Net at Work GmbH, Hersteller der modularen Secure-E-Mail-Gateway-Lösung NoSpamProxy aus Paderborn, weist auf die anhaltend hohe Bedrohung durch Ransomware hin. Ein Drittel (32%) von rund 600 im April befragten Unternehmen war in den vergangenen sechs Monaten von Ransomware betroffen. Die Umfrage zur Betroffenheit der deutschen Wirtschaft durch Ransomware wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen der Allianz für Cyber-Sicherheit durchgeführt. Unabhängig von der eigenen Betroffenheit schätzen 60% der Befragten, dass sich die Bedrohungslage durch Ransomware für ihr Unternehmen oder ihre Institution verschärft hat.

E-Mail nach wie vor Einfallstor Nummer 1

Wie die Befragung deutlich macht, erfolgte die Infektion in drei von vier Fällen durch E-Mail-Anhänge, gefolgt von Drive-by-Angriffen mit 17% sowie, in 8% der Fälle, durch Hacking oder andere Mittel. Damit bleibt die unsichere E-Mail-Kommunikation ein besonders beliebtes Einfallstor für Schadsoftware ins Unternehmen. Die betroffenen Unternehmen berichten, dass neben dem Ausfall einzelner Arbeitsplätze teilweise auch große Teile der IT-Infrastruktur ausfielen oder präventiv abgeschaltet werden mussten. In rund 10% der Fälle kam es so zu erheblichen Ausfällen in der Produktion bzw. Dienstleistungserbringung und zum nicht wiederherstellbaren Verlust wichtiger Daten.



Die Unternehmen reagieren auf die wachsende Bedrohungslage mit einer verstärkten Sensibilisierung der Mitarbeiter für Ransomware, der Intensivierung von Anti-Spam-Maßnahmen und Filterung von Daten an Netzübergängen sowie mit der Aktualisierung der Anti-Virus-Lösungen auf Clients und Servern.

NEWS / PRESSEMITTEILUNG

Auch verbreitete Anti-Malware-Lösungen teilweise wirkungslos

Da die Schadprogramme mit dem größten Schadensanteil jedoch Trojaner-Anhänge wie Locky, TeslaCrypt und CryptoWall waren, wirken die getroffenen Maßnahmen nur bedingt. Die Ransomware-Angriffe erfolgen mit einfachen, aber gut gemachten Spam E-Mails, die von vertrauenswürdigen Domains versendet werden, nicht auf Blacklists auftauchen und deren Absenderadressen oft nur einmalig für zwei bis drei Stunden verwendet werden.

Diese Form von Spam ist für gängige Spam-Filter nicht leicht zu unterbinden: Wortfilter finden keine Anhaltspunkte und insbesondere die Parameter des Mail-Headers bieten keinen Anlass zur Beanstandung. Die Trojaner in den Datei-Anlagen sind z.T. so alt, dass sie in den aktuellen Pattern-Files nicht mehr enthalten sind. Darüber hinaus sind die Prüfsummen der Anhänge grundsätzlich unterschiedlich, so dass die Suche nach bekannten Mustern nur stark eingeschränkt möglich ist. Klassische Ansätze zur Spam- und Gefahrenabwehr versagen somit.

Damit landen diese Mails mitsamt ihrem gefährlichen Inhalt in den Postfächern der Nutzer. Wenn dann die Betroffenen nicht richtig reagieren und die Endpoint-Security, die im Zweifel oft doch nicht aktuell genug ist, versagt, ist die Infektion im Netz.

„Dieser Angriffsform ist mit den bisherigen Lösungen selbst namhafter Security-Hersteller nur begrenzt Paroli zu bieten“, sagt **Uwe Ulbrich, Geschäftsführer bei Net at Work.** *„Durch die einzigartige Kombination mehrerer Sicherheitsmechanismen in einer integrierten Mail-Security-Lösung können wir mit unserem Produkt NoSpamProxy einen wesentlich besseren Schutz bieten.“*

Level of Trust erlaubt deutlich höheren Spamschutz

Als einziger Hersteller wertet Net at Work konsequent das Kommunikationsverhalten der Nutzer aus. NoSpamProxy lernt kontinuierlich, mit wem die Nutzer kommunizieren. Jedem einzelnen Kommunikationspartner wird ein Scoring zugewiesen, das einen sogenannten „Level of Trust“ darstellt. Dieser Level of Trust wird dann genutzt, um über Spam oder Nicht-Spam zu entscheiden. Auch mit Verdacht auf Spam werden E-Mail-Korrespondenten mit hohem Level of Trust nicht abgewiesen. So kann NoSpamProxy False Positives fast vollständig ausschließen und die Spamfilter können mit einem wesentlich höheren Schutzlevel gefahren werden, als bei herkömmlichen Lösungen.

Der zweite Baustein zum optimierten Schutz vor Anhang-Trojanern ist das Modul Large Files, mit dem Anhänge von Mails getrennt und über einen internen Webserver bereitgestellt werden können. Ursprünglich für den Empfang und Versand beliebig großer Dateien entwickelt, wird die Large-File-Transfer-Infrastruktur nun auch dafür genutzt, beim Maileingang kritische Mail-Anhänge gesondert zu behandeln. Nach einfach zu definierenden Regeln, werden die betroffenen Anhänge aus der Mail entfernt und durch einen Hinweis mit einem Downloadlink ersetzt. Doch was ist mit dieser Art der Zustellung gewonnen? Zunächst einmal Zeit – die Anhänge bleiben bis zum dedizierten Zugriff durch den User auf einem zentralen Server, der mit dem jeweils aktuellsten Stand der Anti-Virus-Software arbeitet. Da die Anti-Virus-Programme meist mit nur wenigen Stunden Verspätung reagieren, wird ein guter Teil der Attachements durch diesen zeitlichen Puffer mit aktualisierten Filtern getestet werden können. Als weiterer Gewinn ist die Sensibilisierung der Nutzer zu sehen: Wird ein Attachement aufgrund eines geringen Level-of-Trust-Wertes seines Senders von der Mail abgetrennt, kann man den Nutzer durch entsprechende Warnhinweise besonders sensibilisieren. Als Drittes ergibt sich die Möglichkeit, ausgewählte Anhänge durch die Administratoren prüfen zu lassen.

Integrierte Mail-Security-Lösungen sind die Zukunft

Die Studie der Allianz für Cyber-Sicherheit macht deutlich, dass es Zeit für einen Neuanfang in der Mail-Security ist. Die Fragmentierung von E-Mail-Sicherheitslösungen muss endlich überwunden werden. Eine Integration

von AntiSpam/AntiMalware-Funktionen mit einem sicheren Mechanismus zum Versand von Dateianhängen bietet mit Blick auf die aktuelle Problematik mit Trojaner-Anhängen deutlich mehr Sicherheit als Insellösungen. Die Kombination mit einer konsequenten Verschlüsselung von Mails schafft neben mehr Sicherheit zudem Kostenvorteile und Synergien im Betrieb.

Die vollständige Studie zur Mail-Security der Allianz für Cyber-Sicherheit finden Sie hier:
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ransomware-umfrage-2016-04.html#download=1

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

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

Keywords

Secure E-Mail, Gateway, Allianz für Cyber-Sicherheit, Studie, Anti-Virus, Anti-Spam, Anti-Malware, Ransomware, Large File Transfer, Mail-Verschlüsselung,

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