Cybersecurity im Unternehmen durch verbesserten Malware-Schutz bei E-Mails erhöhen

(Wien, 19.9.2018) Rund zwei Drittel des weltweiten E-Mail Aufkommens bestehen aus Spam-, Hoax- oder Phishing-Mails sowie elektronischen Nachrichten, die mit Malware gekoppelt ins Postfach trudeln. Ein unbedachter Klick auf einen scheinbar seriösen Link, ein vorschnelles Öffnen eines mit Schadprogrammen gespickten Dokuments und schon nimmt ein maliziöses Schicksal seinen Lauf. Der Faktor Mensch ist eine der größten Gefahrenquellen was IT-Sicherheit in Unternehmen betrifft. Mangelnde Schulung und Aufklärung über potentielle Risikoszenarien lassen Mitarbeiter immer wieder in die clever gelegten Fallen von Cyberkriminellen tappen. Und kosten Unternehmen ein Vermögen.

„Verbindliche IT-Richtlinien und Bewusstsein für die Gefahren bildende Workshops für Mitarbeiter sind ein wichtiger Schritt und sollten in keinem Unternehmen fehlen“, erklärt Marco Gschaider, CIO bei Iphos IT Solutions. „Gerade durch die EU-DSGVO sind ja auch auf gesetzlicher Ebene Regeln für eine starke IT-Sicherheit in Kraft getreten. Kommt es durch Fehlverhalten der Mitarbeiter im Umgang mit E-Mails zu Data Leaks ist oft nicht nur das Unternehmen betroffen und nimmt Schaden, auch die Personen, deren Daten auf der Unternehmenshardware gespeichert wurden, können durch solche Angriffe Schaden nehmen“, so Gschaider weiter. „Jeder Mitarbeiter sollte daher zumindest die Basics im Umgang mit E-Mails kennen.“

Potentielle Malware erkennen

„Da zurzeit im deutschsprachigen Raum wieder täuschend echt wirkende Fake-Bewerbungen mit inkludiertem Verschlüsselungstrojaner im Umlauf sind, gleich vorweg einer der wichtigsten Tipps: Niemals an Mails angehängte Dateien mit der Endung .exe anklicken. Diese implementieren in der Regel einen Schadcode auf den betroffenen Rechnern, im schlimmsten Fall verbreitet sich die so installierte Malware im Unternehmensnetzwerk weiter und bringt die gesamte IT-Infrastruktur zum Stillstand,“ warnt Gschaider.

„Überprüfen Sie, ob die in der Mail als Absendername und Mailadresse angegebenen Daten auch mit der tatsächlichen Absenderadresse übereinstimmen. Oft wird hier vorgegeben, dass Nachrichten von bekannten und vertrauenswürdigen Personen stammen, tatsächlich wurden diese allerdings von dubiosen Bots in Russland, China oder anderen bekannten Spam Nations in die Welt gesandt. Das gleiche gilt auch für Links in E-Mails. Kopiert man diese in den Browser – ohne sie auszuführen selbstverständlich – sieht man gleich, ob der Link tatsächlich zur eigenen Bank oder einer Website mit Malware oder Phishing-Intentionen geht“, so Gschaider weiter.

Gefahrenquelle Social Engineering

Nicht direkt mit Malware versehen sind E-Mails mit der Manipulationsabsicht, nichtsdestotrotz stellen diese ein hohes Gefahrenpotential dar. Social Engineering, wie diese Art der Manipulation genannt wird, soll Mitarbeiter durch das Vortäuschen, ebenfalls Mitarbeiter – oft höherer Hierarchieebene oder z.B. externe IT-Dienstleister – zu sein, zur Herausgabe vertraulicher interner Informationen, wie z.B. Login-Daten, bringen. „Nicht unter Druck setzen lassen, niemals vertrauliche Informationen per E-Mail weitergeben“, ist Marco Gschaiders Empfehlung zum Umgang mit Angriffsversuchen dieser Art.

Machine Learning im Kampf gegen Malware

Gschaider hat auch Tipps für den optimalen technischen Schutz vor über E-Mails verbreitete Malware parat: „Menschliches Versagen kann natürlich nie vollständig ausgeschlossen werden, deshalb sollten Unternehmen natürlich auch auf technologischer Ebene auf verbesserten Malware-Schutz für ihre E-Mail-Kommunikation setzen.“

Dank maschinellem Lernen bieten Endpoint Security Lösungen wie die des europäischen IT-Security Providers ESET auch bei Zero-Day-Angriffen – also bei Viren, Trojanern und Malware, die noch nicht bekannt ist – ein ausgesprochen gutes Schutzlevel. Gerade für den Business-Bereich wurde kürzlich mit der Lösung Dynamic Threat Defense durch cloudbasiertes Sandboxing eine verbesserte Möglichkeit, bislang unbekannte Bedrohungen zu erkennen und auszuschalten, geschaffen. Auf dem Mailserver des Unternehmens eingehende Mails von externen Quellen werden mit einer kleinen Verzögerung zugestellt. In diesem Zeitraum in einer Sandbox der reale Umgang von Usern mit der E-Mail imitiert, also Anhänge geöffnet, Links aktiviert, etc. Im Anschluss wird das dabei an den Tag gelegte Verhalten über neuronale Netzwerke analysiert und mit bereits bekannten Verhaltensmustern und Auffälligkeiten abgeglichen. Wird dabei ein potentiell schädliches Verhalten festgestellt, landet die Mail in Quarantäne, der Empfänger und die IT-Leitung werden informiert. Malware-freie Mails werden nach dem Check normal zugestellt.

Über Iphos IT Solutions

Iphos IT Solutions GmbH ist ein internationales Unternehmen, das Dienstleistungen in den Bereichen IT-Infrastruktur, Softwareentwicklung und Webentwicklung anbietet. 1998 in Wien gegründet betreibt Iphos IT Solutions einen weiteren Standort in Bulgarien (Sofia) und bietet seine Dienstleistungen im DACH-Raum sowie Bulgarien an. Ing. Christoph Wendl leitet gemeinsam mit Lyubomir Ivanov als Chief Executive Officer (CEO) das Unternehmen, das sich mit innovativen Lösungen den aktuellen Herausforderungen der IT stellt. Als ESET-Goldpartner konnte sich Iphos IT Solutions auch in der Implementierung komplexer IT-Security Lösungen einen Namen machen.

Rückfragehinweis für Medien:

Ing. Christoph Wendl
Geschäftsführer, Iphos IT Solutions GmbH
Arndtstraße 89/Top 22
1120 Wien
Tel.: +43 1 869 84 00
E-Mail: marketing@iphos.com
Web: https://www.iphos.com