E-MAIL-ANGRIFFE ERFOLGREICH ABWEHREN

Einen hundertprozentigen Schutz vor Cyberangriffen via E-Mail gibt es nicht. Die Folgen von Trojanern, Ransomware, Phishing und Spam können gravierend sein: Datenverlust, Betriebsstörungen, enorme finanzielle Einbußen und oft auch Reputationsschäden. Um die geschäftliche Kommunikation abzusichern, brauchen IT-Verantwortliche einen langen Atem. VON MARTIN MATHLOUTHI

Die überwiegende Mehrheit der Unternehmen in Deutschland geht von einer weiteren Verschärfung der Bedrohungslage durch die zunehmende Digitalisierung aus, wie aus der jüngsten Cyber-Sicherheits-Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hervorgeht. Im vergangenen Jahr waren demnach ein Drittel der Umfrageteilnehmer Cyberangriffen ausgesetzt, hauptsächlich durch Malware, die via E-Mail eingeschleust wurde. Oft kommt es dadurch zu Ausfällen in der IT-Infrastruktur oder zum Verlust geschäftskritischer Daten. Die IT-Systeme wiederherzustellen sowie Reputationsschäden zu begrenzen, bindet weitere zeitliche und finanzielle Ressourcen, ebenso wie die Aufklärung solcher Vorfälle.

ADVANCED THREATS MACHEN ERWEITERTEN SCHUTZ NOTWENDIG

Heute überschreiten immer mehr Angriffsmethoden die Möglichkeiten konventioneller Abwehrmechanismen. Um solche Advanced Threats abzuwehren, genügen herkömmliche Schutzvorkehrungen wie Virenscanner, Spam- und Phishing-Filter nicht. Ein erhöhtes Sicherheitslevel gewähren Technologien wie Sandboxing und URL-Rewriting. Diese werden idealerweise mit innovativen Methoden zur Reaktion und Analyse kombiniert.

> **„Professionelle E-Mail Security Services aus der Cloud hingegen kombinieren notwendige Maßnahmen bedarfsgerecht, werden kontinuierlich aktualisiert."**

All diese Anforderungen mit selbstbetriebenen Systemen zu erfüllen, ist allerdings schwierig. Professionelle E-Mail Security Services aus der Cloud hingegen kombinieren notwendige Maßnahmen bedarfsgerecht, werden kontinuierlich aktualisiert und bieten somit eine sinnvolle Alternative.

TARGETED ATTACKS RECHTZEITIG ERKENNEN

Auch Social Engineering ist eine häufig genutzte Angriffsmethode. Sie setzt gezielt auf die Schwachstelle Mensch. In letzter Zeit gehäuft hat sich zum Beispiel „CEO-Fraud": Cyberkriminelle geben sich in täuschend echten E-Mails als Geschäftsführer eines Unternehmens aus und fordern potenziell autorisierte Personen auf, hohe Geldsummen zu überweisen. Die Kriminellen forschen dazu die richtigen Ansprechpartner im Unternehmen aus und setzen individuell angepasste, persönlich gestaltete E-Mails an diese ab.

Eine wichtige Maßnahme, um sich vor solchen Betrügereien zu schützen, ist die Sensibilisierung der Mitarbeiter. Oft sind solche E-Mails allerdings kaum als Betrugsversuch zu erkennen. Deshalb sollte eine E-Mail-Security-Lösung unbedingt Funktionen wie eine entsprechende Kennzeichnung verdächtiger E-Mails und Erkennungsmechanismen für CEO-Fraud beinhalten. Diese Technologien erkennen Fake-Adressen rechtzeitig und warnen die Empfänger und blockieren oder quarantinieren solche E-Mails.

BISLANG UNBEKANNTE ANGRIFFSMUSTER ENTDECKEN

Die Cyber-Sicherheits-Umfrage des BSI deckt auf, dass Angreifer allen Schutzmaßnahmen zum Trotz in die IT-Systeme der Unternehmen eindringen können. Das gelingt zum Beispiel, wenn die Angriffsmuster, etwa bestimmte Viren, noch nicht bekannt sind oder Malware eingeschleust wird, die nicht sofort aktiv ist. Dann können Virenscanner die Schadroutinen nicht erkennen und selbst Sandbox-Technologien manchmal keine ungewöhnlichen Aktionen feststellen. In der Folge werden potenziell schädliche E-Mails zugestellt.

Um Schaden zu vermeiden oder wenigstens zu begrenzen, eignen sich hier Mechanismen wie Post-delivery Protection. Diese greift dann, wenn neue Virenpattern bekannt werden – selbst wenn Malware via E-Mail bereits in die Unternehmensinfrastruktur gelangt ist. Besonders wirkungsvolle Technologien erzeugen bereits beim Eingang einer E-Mail im Rechenzentrum des EMail-Security-Anbieters einen digitalen Fingerabdruck aller Attachments sowie der enthaltenen URLs. Sobald bei einem späteren Empfänger in einem identischen Anhang Schadcode entdeckt oder eine URL als Phishing-Versuch identifiziert

DER AUTOR

MARTIN MATHLOUTHI

ist Product Line Manager für E-Mail Security bei Retarus.

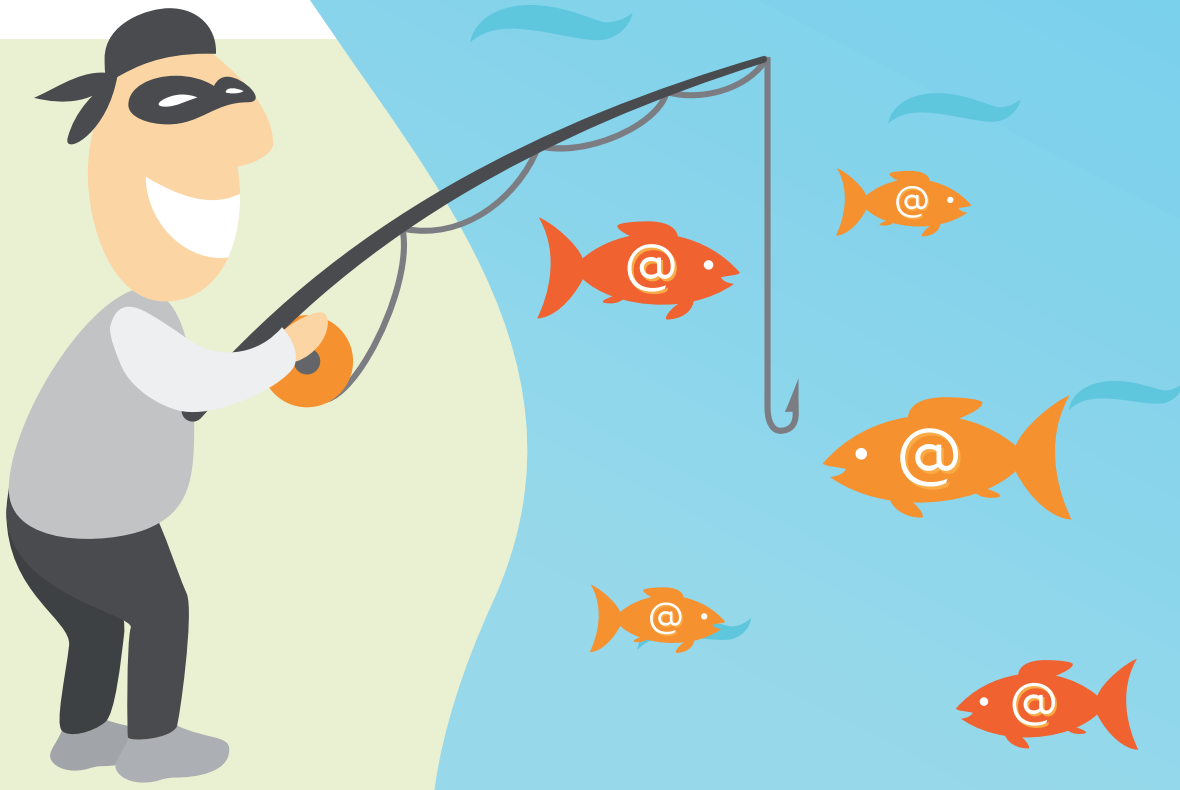

Bild: Dream Master/shutterstock.com

wird, werden unverzüglich alle bisherigen Empfänger sowie deren Administratoren informiert. In der Regel wird die Unternehmens-IT dabei so schnell alarmiert, dass infizierte E-Mails noch gar nicht geöffnet wurden und unmittelbar gelöscht werden können. Darüber hinaus lassen sich innovative Services mit der Cybersecurity-Systemlandschaft der Anwenderunternehmen integrieren, um notwendige Ereignisse für erweiterte forensische Analysen bereitzustellen, etwa über die Integration in SIEM-Tools zur Bereitstellung sicherheitsrelevanter Events.

FÜNF FAKTOREN FÜR MEHR E-MAIL-SICHERHEIT

01 Mitarbeiterschulung und E-Mail Policy

Ein wichtiger Faktor ist, Mitarbeiter für mögliche Gefahren zu sensibilisieren, etwa niemals unbekannte Anhänge oder Links zu öffnen und sich im Zweifelsfall auf einem anderen Kanal, zum Beispiel telefonisch, beim Absender rückzuversichern. Richtlinien für die E-Mail-Nutzung im Unternehmen vermitteln den Anwendern, was bei der E-Mail-Kommunikation zu beachten ist, und welche Maßnahmen gegebenenfalls technisch umgesetzt werden. Um optimal zu wirken, müssen E-Mail-Richtlinien verständlich, allen Anwendern bekannt, praktikabel, aktuell und flexibel anpassbar sein – an neue Anforderungen im Unternehmen und an neue Bedrohungen.

02 Advanced Threat Protection

Virenscanner, Spam-Filter sowie das Blockieren potenziell schädlicher E-Mail-Anhänge bieten einen guten Basisschutz. Um sich vor Advanced Threats abzusichern, genügt das aber nicht. Mechanismen wie Sandboxing, eine CEO-Fraud-Erkennung, ein erweiterter Phishing-Schutz via URL-Rewriting und Lösungen gegen „Zero Day Attacks" ergänzen den Basisschutz sinnvoll.

03 Post-delivery Protection

Immer wieder überwinden Angreifer auch die besten Schutzmaßnahmen. In solchen Fällen ist es wichtig, Malware schnell im Unternehmensnetz zu identifizieren, um einen Schadensfall zu verhindern oder zu begrenzen. Post-delivery-Protection-Lösungen wie zum Beispiel eine Patient Zero Detection sind hier besonders wirksam.

04 Vertrauliche Informationen schützen

Unverschlüsselte E-Mails sind eine leichte Beute für Datendiebe, ähnlich wie Postkarten auf dem Postweg. Mit der Verschlüsselung sowohl der Anbindung an den E-Mail-Security-Anbieter als auch vertraulicher E-Mails selbst lässt sich effektiv verhindern, dass Unberechtigte mitlesen. Eine Data Loss Prevention (DLP) stellt sicher, dass vertrauliche Daten wie Kunden-, Produktions- oder Konstruktionsdaten nicht ungewollt aus dem Unternehmensnetz gelangen.

05 Reputation und Integration

Authentifizierungsverfahren wie SPF, DKIM und DMARC tragen dazu bei, dass im Namen der authentifizierten Unternehmen keine Spam-Nachrichten oder Malware verschickt wird. Zusätzlich kann der Betrieb eines SIEM-Systems eine sinnvolle Lösung für ganzheitliche Überwachung und Reaktion auf sicherheitsrelevante Vorfälle sein. Professionelle EMail-Security-Anbieter bieten Schnittstellen zu diesen Systemen, so dass Informationen über erkannte Gefahren zentral und in Echtzeit zur Verfügung stehen.