HELPDESK

Phishing-schutz fürs Unternehmen

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

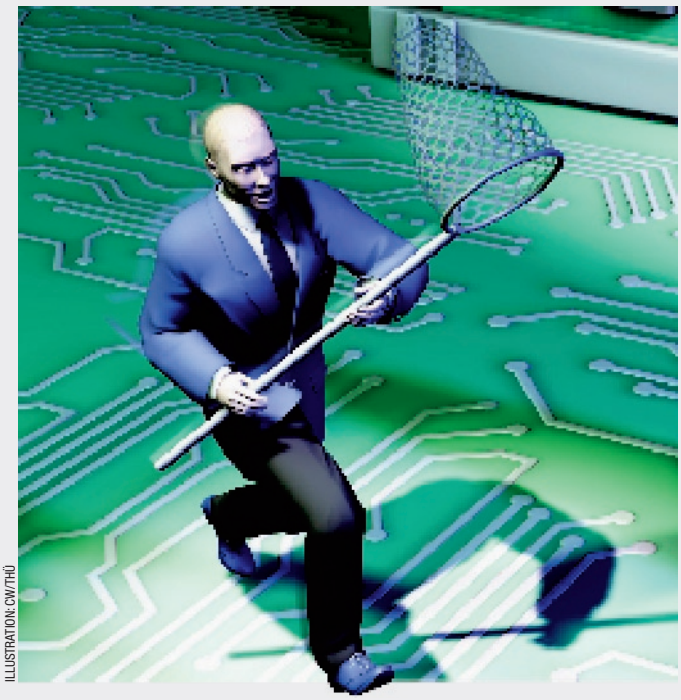

ILLUSTRATION: CW/THÜ

Frage: Laut den Prognosen von Marktforschungsunternehmen verlaufen zwischen 5 und 20 Prozent der Phishing-Attacken für die Betrüger erfolgreich. Wie kann sich ein Unternehmen wirkungsvoll vor Phishing schützen?

Eins vorweg, es gibt keinen absoluten Schutz vor Phishing. Eine gesunde Portion Misstrauen in Kombination mit geeigneten organisatorischen und technischen Massnahmen schützt aber vor allzu bösen Überraschungen. Folgende drei Massnahmen helfen gegen Phishing und dämmen als positiven Nebeneffekt die Spamflut ein.

1. Schutz vor unnötigem Informationsabfluss: Professionelle Spammer und Phishing-Betrüger durchforsten auf der Suche nach E-Mailadressen mit automatisierten Tools systematisch das Internet. Aus diesem Grund sollten generell nur generische, nicht aber persönliche E-Mailadressen kommuniziert werden – info@firma.ch statt peter.muster@firma.ch.

Die von manchen E-Mailsystemen generierten Mailheader enthalten in der Standardeinstellung diverse Informationen über das Mailsystem und allfällige Antiviren- und Antispam-Programme. An diese Informationen gelangen Betrüger mit einfachen Tricks. Das Senden einer E-Mail an nicht existierende E-Mailadressen der entsprechenden Domäne wird vom Mailserver mit einer Fehlermeldung via E-Mail beantwortet. Um dies zu verhindern, müssen die Mailheader-Einträge auf ein Minimum reduziert und «Banner Spoofing» (Fälschung der Einträge im Mailheader) eingerichtet werden.

«Guten Schutz bieten auf Zertifikatbasis signierte und/oder verschlüsselte E-Mails.»

Zwingend ist auch, die automatische Übermittlungsbestätigung auf dem Mailserver und die automatische Lesebestätigung auf dem Mailclient zu deaktivieren.

2. Schutz vor Phishing- und Spammails und deren Folgen: Manche Mailserver können so eingerichtet werden, dass der erste Sendeversuch generell abgebrochen, aber nicht verweigert wird und erst der zweite Versuch erfolgreich ist. Weil Spammer möglichst viele Mails in möglichst kurzer Zeit versenden möchten, verzichten sie oft auf einen erneuten Sendeversuch. Spamfilter erkennen und blockieren E-Mails von bekannten Spammern oder Phishing-Betrügern. Contentfilter erkennen und blockieren den Zugriff des Webbrowsers auf bekannte Phishing-Websites. Spam- und Contentfilter sind als Ergänzungssoftware oder als Appliance erhältlich. SPF (Sender Policy Framework) koppelt mittels DNS-Einträgen die Domänen mit zugehörigen Mailservern. Damit wird verhindert, dass Spammer oder Phishing-Betrüger unbemerkt Mail unter Vortäuschung einer anderen Absenderdomäne versenden – ausser Original-Mailserver wurde gehackt. Guten Schutz bieten auch auf Zertifikatsbasis signierte und/oder verschlüsselte E-Mails, weil der Absender einer E-Mail eindeutig identifiziert und eine Modifikation der E-Mail erkannt werden kann.

3. Schutz der Infrastruktur vor Missbrauch: Unzureichend geschützte Mail- und Webserver sind ein gefundenes Fressen für Betrüger. Deshalb sollten regelmässig Sicherheitspatches auf Servern und PCs eingespielt werden. Veröffentlichte Sicherheitspatches werden von interessierten Kreisen mittels Reverse Engineering analysiert, um offen zu legen, welche Sicherheitslücke mit dem entsprechenden Patch geschlossen wird. Nicht gepatchte Systeme weisen die Sicherheitslücke demnach weiterhin auf. Generell sollten Mailserver so konfiguriert werden, dass Mailrelaying nur für die E-Mailadressen des eigenen Betriebs möglich ist. Ein Missbrauch durch Spammer führt über kurz oder lang dazu, dass die Firmendomäne als Spamdomain registriert und von Antispamsystemen blockiert wird. Die Folge ist eine eingeschränkte Kommunikation. Ausserdem müssen betroffene Firmen einen Imageverlust und rechtliche Schritte geschädigter Dritter fürchten. ■

Der Autor
Christoph Baumgartner ist CEO und Senior Consultant bei OneConsult, Thalwil, www.oneconsult.ch

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch