



## **Phishing: Eine ernstzunehmende Gefahr**

*Während früher nur Privatpersonen mit betrügerischen E-Mails zu kämpfen hatten, bereitet Phishing heute auch E-Mail-Administratoren Kopfzerbrechen, da zunehmend Unternehmen betroffen sind.*

### **INHALT**

<b>Den Feind verstehen</b>	<b>2</b>
<b>Drei Dinge, die Sie über Phishing wissen sollten</b>	<b>4</b>
<b>In vier Schritten zu einer effektiven Anti-Phishing-Lösung</b>	<b>7</b>
<b>Fazit</b>	<b>9</b>

Bei Phishing-Angriffen können Finanzdaten und persönliche Informationen sowie Identitätsdaten ausspioniert werden. Darüber hinaus verlieren die Betroffenen häufig das Vertrauen in E-Mail als Kommunikationsmedium. Phishing wird primär als Problem von Privatpersonen betrachtet, aber es kann genauso gut auch Unternehmen treffen – sei es durch den direkten Verlust von Informationen oder durch indirekte Produktivitätsverluste bei Mitarbeitern, die Phishing zum Opfer gefallen sind. Häufig ignorieren Unternehmen das Problem oder messen ihm nur eine geringe Bedeutung zu, da sie davon ausgehen, dass ein Spamfilter ausreicht, um Phishing-Mails aufzuspüren, oder weil sie glauben, dass ihre Mitarbeiter Phishing-Mails ohne weiteres erkennen können. Doch die Realität sieht anders aus. Dieses Whitepaper befasst sich mit den Herausforderungen, denen sich Unternehmen heute stellen müssen, um Phishing langfristig in den Griff zu bekommen. Außerdem wird eine Lösung vorgestellt, mit der Anti-Phishing-Maßnahmen in bestehende Prozesse integriert werden können.

## **Den Feind verstehen**

Von den vielen unterschiedlichen Arten von E-Mail-Bedrohungen bekommt Spam die meiste Aufmerksamkeit. Und das ist auch richtig so. Bei mehr als 90 Prozent aller E-Mails, die Unternehmen empfangen, handelt es sich um kommerzielle Spam-Mails. E-Mail-Bedrohungen sind äußerst vielfältig. Es können jederzeit neue Arten auftauchen und nur der Einfallsreichtum der Datendiebe setzt dabei den Möglichkeiten Grenzen. Und tatsächlich werden die gefährlichsten Bedrohungen nicht einfach per E-Mail-Nachricht übermittelt, sondern in Form raffinierter Phishing-Mails versteckt.

In der Vergangenheit waren vor allem Heimanwender unter Beschuss, doch angetrieben durch die Wirksamkeit ihrer Angriffe bei Privatpersonen richten die Phisher ihren Blick jetzt auch auf Unternehmen. Sie haben festgestellt, dass dieselben Methoden, die bei Privatpersonen verfangen, auch bei arglosen Unternehmensmitarbeitern funktionieren. Phishing-Mails, die sich an Mitarbeiter richten, kommen scheinbar von einer vertrauenswürdigen Quelle, z. B. von Vorgesetzten, von anderen Abteilungen im Unternehmen oder sogar von Geschäftspartnern. Die gefälschten Nachrichten sehen legitimen Firmen-E-Mails oft täuschend ähnlich, da sie in originalgetreuem Design gestaltet sind und firmentypische Inhalte und Links enthalten. Zudem werden die Angestellten zu Handlungen aufgefordert, die sinnvoll erscheinen, wie z. B. Firmeninformationen zu bestätigen.

Finanzdienstleister, Gesundheitsorganisationen und Versicherungsunternehmen, die sensible Daten verwalten, sind besonders häufig das Ziel von E-Mail-Angriffen. Gerade für diese Organisationen steht einiges auf dem Spiel, da sie verpflichtet sind, besonders strenge gesetzliche Datenschutz- und Sicherheitsrichtlinien einzuhalten. Doch kein Unternehmen ist vor E-Mail-Bedrohungen gefeit und jeder Angriff hat das Potenzial, verheerende Schäden anzurichten.

Durch Phishing-Angriffe verlieren Unternehmen nicht nur Zeit und Geld, sondern – was noch viel schlimmer ist – das Vertrauen ihrer Kunden und Partner. Eine einzige Phishing-Mail, bei der sich der Absender als ein Vertreter Ihres Unternehmens ausgibt, setzt Ihre Vertrauenswürdigkeit aufs Spiel. Was bislang eine Ihrer wertvollsten Geschäftsanwendungen war, kann so zu einer ernsthaften Bedrohung für Sie und Ihre Partner werden.

Betrügerische Mails stellen vor allem wachsende Unternehmen vor schwere Probleme. Die Auswirkungen können zwar für größere Unternehmen genauso verheerend sein, doch gerade

kleineren Unternehmen fehlen häufig die finanziellen und technischen Ressourcen, um sich effektiv zur Wehr zu setzen.

SonicWALL zeigt in diesem Whitepaper Möglichkeiten auf, wie sich wachsende Unternehmen, denen die zunehmenden Probleme durch Phishing Sorge bereitet, vor Gefahren wappnen können. Neben den drei Dingen, die Sie über Phishing wissen sollten (u. a. drei verbreitete Irrtümer) zeigt SonicWALL diesen Unternehmen, wie sie in vier Schritten effektiven Schutz vor Phishing gewährleisten können.

## **Drei Dinge, die Sie über Phishing wissen sollten**

Um Phishing erfolgreich zu bekämpfen, müssen Sie drei Dinge verstehen: Den Phisher, die Phishing-Mail und die Fakten.

### **Phishing: wenn Spammer richtig Schaden anrichten**

Viele Unternehmen behandeln Phishing-Mails genauso wie Spam. In gewisser Weise sind sich Phishing- und Spam-Mails tatsächlich ähnlich. Beide Varianten werden unaufgefordert versendet und fordern den Empfänger dazu auf, einen Kauf zu tätigen, Informationen preiszugeben o. Ä. Doch hier hören die Gemeinsamkeiten auch schon auf. Während Spammer Junk-Mails versenden, die meist schon auf den ersten Blick als Spam zu erkennen sind, geben sich Phisher als vertrauenswürdiger Partner oder Freund aus. Spammer legen alles daran, die Aufmerksamkeit des Empfängers zu gewinnen, während sich Phisher bemühen, nicht aufzufallen und sich als vertrauenswürdige Quelle zu tarnen. Dazu verwenden sie nicht nur Ihr E-Mail-System, sondern instrumentalisieren auch Ihre Mitarbeiter.

Weder Spam noch Phishing-Mails sind in Ihrem E-Mail-System willkommen, doch von Phishing-Mails geht bei weitem die größere Gefahr aus. Während Spam zwar lästig, aber harmlos ist, hört beim Phishing der Spaß auf. Wenn nur eine einzige Phishing-Mail ihr Ziel erreicht, könnten sowohl Ihr Firmennetzwerk und Ihre Unternehmensdaten als auch Ihre Mitarbeiter und Kunden zum Ziel der ausgeklügelten Angriffe aller möglichen Hacker und Cyber-Kriminellen im Internet werden. Selbst wenn die Sicherheitslücke sofort geschlossen wird, könnte Phishern oder ihren böswilligen Verbündeten genügend Zeit bleiben, um gesamte Datenbanken mit den Kreditkartennummern Ihrer Kunden „abzugrasen“ und Ihren Ruf nachhaltig zu schädigen

### **Die Phishing-Mail: Phishing, gefälschte Updates und Rechnungsbetrug**

Die drei gängigsten Arten betrügerischer E-Mails sind Phishing, gefälschte Updates und Rechnungsbetrug.

#### **Phishing**

Beim Phishing wird versucht, das Vertrauen von arglosen Mitarbeitern in bekannte Marken und vertraute Quellen auszunutzen. Genau wie im privaten Bereich kommen Phishing-Mails, die auf Unternehmen abzielen, ebenfalls von scheinbar vertrauenswürdigen Quellen, wie z. B. von Vorgesetzten, von der IT-Abteilung oder von einem Geschäftspartner. Der Empfänger wird darüber in Kenntnis gesetzt, dass bestimmte Informationen aktualisiert werden müssen, damit ein Konto aktiviert bleibt oder der Netzwerkzugriff weiterhin gewährleistet ist. Normalerweise enthalten die Mails einen Link zu einer „gespooften“ (d. h. gefälschten) Website. Folgt der Mitarbeiter den Anweisungen, stellt er dem Phisher unabsichtlich sensible Finanzdaten oder Netzwerkzugriffsinformationen zur Verfügung. Wurde das Firmennetzwerk erst einmal getroffen, bleibt Ihnen nur noch, die Sicherheitsausweise aller Mitarbeiter einzusammeln und neu auszustellen, alle Geräte nach Schadsoftware zu durchsuchen und sämtliche Kontoaktivitäten auf Spuren unberechtigter Aktivitäten zu überprüfen.

#### **Gefälschte Updates**

Auch gefälschte Updates stellen eine ernstzunehmende E-Mail-Bedrohung dar. Zu den gängigsten Arten von gefälschten Updates gehören Software-Updates. Dabei werden

fingierte E-Mails verschickt, in denen die Mitarbeiter darüber informiert werden, dass neue Softwareversionen verfügbar sind. Anschließend werden die Mitarbeiter auf gespoofte Websites geleitet, wo sie aufgefordert werden, Kontoinformationen zu bestätigen, damit sie das Update erhalten und die Schadsoftware herunterladen können. Nach dem Download kann die Malware ihre schädigende Wirkung auf verschiedene Arten entfalten. Sie kann Sicherheitsprotokolle umgehen, um an Unternehmensdaten zu gelangen, Festplatten so stark beschädigen, dass die Daten nicht wiederhergestellt werden können, E-Mail-Adressen für Massenmailings mit böswilliger Absicht erbeuten oder andere Benutzer über Chat-Sitzungen infizieren. Damit Mitarbeiter gefälschte Updates erkennen, sollten sie anhand klar definierter Richtlinien über die ordnungsgemäße Systemaktualisierung unterrichtet werden, so dass sie gefälschten E-Mails von vornherein nicht vertrauen.

### **Rechnungsbetrug**

Die Absender gefälschter Rechnungsmails machen es sich zunutze, dass weder Menschen noch Prozesse perfekt sind. Täglich werden in Buchhaltungsabteilungen auf der ganzen Welt legitime Zahlungen über viele Millionen Euro abgewickelt. Bei ausstehenden Zahlungen ist es üblich, dass Lieferanten Erinnerungsmails verschicken, worauf der verantwortliche Sachbearbeiter die Zahlung veranlasst. Um die Zahlung zu beschleunigen, kann es vorkommen, dass die Mitarbeiter der Buchhaltungsabteilung die Rechnung online mit der Firmenkreditkarte begleichen.

Mit fingierten Rechnungsmails, die den Nachrichten vertrauenswürdiger Lieferanten oder Partner zum Verwechseln ähnlich sehen, verschaffen sich Phisher Kreditkarteninformationen oder veranlassen unrechtmäßige Zahlungen. In seltenen Fällen gelingt es Phishern sogar, die elektronischen Fakturierungsprozesse zu manipulieren und alle Zahlungen an einen bestimmten Lieferanten an sich selbst umzuleiten.

### **Die Fakten: Anti-Spam- und Anti-Virus-Lösungen alleine reichen nicht aus, um Phishing in den Griff zu bekommen**

Unternehmen wissen nur zu gut, dass E-Mail-Bedrohungen wie Spam und Viren die Produktivität lahmlegen, Haftungsrisiken verursachen und IT-Kosten in die Höhe treiben können. Aus diesem Grund investieren sie viele Millionen Euro in Anti-Spam- und Anti-Virus-Lösungen.

- Irrglaube Nr. 1: Wie Spam-Mails lassen sich auch Phishing-Mails am besten mit einem Spam-Filter in den Griff bekommen.

Die Tatsachen: Phishing-Mails imitieren legitime Nachrichten. Als professionell formulierte Geschäftsmails aus scheinbar vertrauenswürdigen Quellen müssen Spam-Filter diese Art von Nachrichten durchlassen. Einige Phishing-Mails sind so gut getarnt, dass es ihren Absendern immer wieder gelingt, Spam-Filter damit auszutricksen. Auch wenn es naheliegend scheint, beide Varianten in einen Topf zu werfen, ist Phishing nicht gleich Spam. Phishing-Mails müssen speziell analysiert, identifiziert und behandelt werden, damit sie keinen Schaden in Ihrem Unternehmen anrichten können.

- Irrglaube Nr. 2: Eine URL-Blockade schützt vor Phishing-Mails.

Die Tatsachen: Bei einer URL-Blockade wird auf eine Liste bekannter Phishing-Websites zurückgegriffen. Links in E-Mails werden mit dieser Liste abgeglichen. Im Falle einer Übereinstimmung wird die Nachricht als Phishing-Mail behandelt. Diese Methode ist zwar gut, aber langsam. Phisher können in wenigen Stunden Angriffe starten und an die gewünschten Informationen kommen – oft bevor eine URL gemeldet, verifiziert und in die URL-Blockadeliste aufgenommen wurde. Daher muss eine Inhaltsanalyse durchgeführt werden, um potenzielle Phishing-Mails zu erkennen. Spamfilter können lernen, bei

welchen Mails es sich um Spam, also um offensichtlich unerwünschte E-Mails, handelt. Analog dazu benötigt man einen Phishingfilter, der raffinierte Angriffstechniken wie URL-Masking oder „gespoofte“ Absender in E-Mails erkennt, die auf den ersten Blick rechtmäßig erscheinen.

- Irrglaube Nr. 3: Wenn Phishing-Erkennungstechnologien versagen, können Phishing-Mails immer noch von den Mitarbeitern selbst erkannt werden.

Die Tatsachen: Sie können sich nicht darauf verlassen, dass Mitarbeiter Phishing-Mails auch wirklich von legitimen Nachrichten unterscheiden können. Untersuchungen von SonicWALL zufolge lagen Anwender in 22 % aller Fälle daneben, als sie angeben sollten, ob es sich bei einer verdächtigen E-Mail um eine legitime oder gefälschte Mail handelt. Außerdem lassen sich 10 % der Anwender von Phishing-Mails verführen, obwohl man ihnen vorher gesagt hatte, es handle sich um eine verdächtige Mail. Jeder zehnte Anwender öffnet eine Phishing-Mail, klickt auf einen der Links oder gibt Daten auf der gefälschten Website ein.

## **In vier Schritten zu einer effektiven Anti-Phishing-Lösung**

Eine effektive Anti-Phishing-Lösung kombiniert innovative Tools und Methoden, die speziell darauf ausgelegt sind, Phishing durch einen einheitlichen und präzisen Informationsfluss zu bekämpfen. SonicWALL empfiehlt die folgenden Schritte: Erkennung, Schutz, Integration und Information.

### **Erkennung: Setzen Sie spezielle Analyseverfahren ein, um fingierte Mails aufzuspüren.**

Spamfilter sind darauf ausgelegt, legitime E-Mails in Ihr Unternehmensnetzwerk hineinzulassen; sie sind jedoch nicht in der Lage, Phishing-Mails auszufiltern, die rechtmäßigen Nachrichten zum Verwechseln ähnlich sehen. Eine effektive Anti-Phishing-Lösung muss viele unterschiedliche Nachrichtenattribute (z. B. Absender, Format, Struktur und Inhalt) analysieren können, da diese Aufschluss über die Echtheit einer Nachricht geben.

### **Schutz: Entwickeln Sie spezielle Protokolle zur Eindämmung und zum Schutz vor Phishing-Mails.**

Phishing ist nicht gleich Spam. Daher sollten Phishing-Mails nicht zusammen mit Spam-Mails in Quarantänezonen aufbewahrt und in das Unternehmensnetzwerk gelassen werden. Denn dort können Mitarbeiter die Phishing-Mails aus der Quarantäne nehmen und die enthaltenen Anweisungen befolgen. Eine effektive Anti-Phishing-Lösung muss in der Lage sein, Phishing-Mails sofort von anderen Arten unerwünschter E-Mails zu isolieren. Außerdem sollte sie Ihrer IT-Abteilung die Möglichkeit geben, Phishing-Mails am Netzwerkrand zu neutralisieren, bevor sie eine Chance haben, ihren Empfänger zu erreichen. SonicWALL empfiehlt Unternehmen dringend, als Phishing-Mails identifizierte und isolierte Nachrichten ausschließlich von IT-Mitarbeitern prüfen und löschen zu lassen.

### **Integration: Binden Sie Ihre Anti-Phishing-Lösung in ein umfassendes E-Mail-Sicherheitssystem ein.**

Ihr Anti-Phishing-Konzept sollte keine Insellösung sein. Eine effektive Lösung muss mehrere Optionen bieten, die sich mit anderen Sicherheitsprozessen integrieren lassen. Möglicherweise erwartet Ihre Rechtsabteilung schriftlich dokumentierte Nachweise aller versuchter Phishing-Angriffe, während die Sicherheitsbeauftragten Ihres Unternehmens mit Warnmeldungen über neue Phishing-Arten informiert werden möchten. Darüber hinaus sollte Ihre Anti-Phishing-Lösung in ein größeres externes Netzwerk verschiedener Sicherheitspartner eingebunden sein, das regelmäßig Warnungen über neue Betrugsmethoden versendet, Ihre IT-Abteilung optimal mit Informationen versorgt und Ihnen die Möglichkeit gibt, neue Abwehrmechanismen rechtzeitig zu implementieren, bevor ein neuer Virenausbruch Ihr Netzwerk erreicht.

### **Information: Trainieren Sie Ihre Mitarbeiter, Phishing-Mails zu erkennen.**

Je besser Ihre Mitarbeiter darüber Bescheid wissen, wie Phishing-Mails funktionieren und was beim Empfang einer verdächtigen Mail zu tun ist, desto eher sind sie in der Lage, die richtigen Schritte einzuleiten, wenn Ihr Unternehmen von einem Phishing-Angriff getroffen wird. Eine effektive Anti-Phishing-Lösung benötigt spezielle Reporting-, Warn- und Feedback-Tools, die Administratoren über die aktuellen Trends auf dem Laufenden halten, so dass sie die erforderlichen Maßnahmen auf Netzwerkebene ergreifen und die Ergebnisse an andere interne und externe Sicherheitsstellen melden können. Diese Warnhinweise sollten relevante Informationen bereitstellen und das Bewusstsein gegenüber Sicherheitsbedrohungen schärfen.

Unter <http://www.sonicwall.com/phishing> bietet SonicWALL ein kostenloses Phishing-IQ-Quiz an. Dieses Quiz stellt lediglich einen Ausschnitt der Informationen dar, die Sie an Ihre Mitarbeiter weitergeben sollten, damit sie sicher mit Phishing-Mails umgehen. Je mehr Ihre Mitarbeiter wissen, desto besser sind sie vorbereitet.

## **Fazit**

Trickbetrug ist kein neues Phänomen. Immer schon mussten sich Geschäftsleute gegen betrügerische Angriffe zur Wehr setzen. Genauso wie Unternehmen ihre Geschäftspraktiken ständig weiterentwickeln, um mit den neuesten Entwicklungen Schritt zu halten, arbeiten auch Datendiebe an ihren Methoden und versuchen die Möglichkeiten auszunutzen, die ihnen moderne Technologien bieten. Wenn Sie Phishing jedoch als eigenständige und besonders raffinierte Form der E-Mail-Bedrohung betrachten und Lösungen einsetzen, die speziell auf Phishing zugeschnitten sind, können Sie sich und Ihre Firma trotzdem schützen.

Es gibt zwar auch spezialisierte Anwendungen, die Spam- und Viren-Angriffe abwehren. Sinnvoller ist es jedoch, eine Lösung einzusetzen, die Schutz vor Spam, Viren und Phishing kombiniert. Eine integrierte Lösung reduziert nicht nur den Verwaltungsaufwand und erhöht die Effizienz, sie erlaubt es Ihnen auch, die größten Gefahrenquellen aufzuspüren und entsprechend zu handeln. Entscheidend ist auch, dass alle Elemente einer effektiven Anti-Phishing-Lösung für Ihre Mitarbeiter transparent einsehbar sind und automatisch am Netzwerkrand ausgeführt werden.

©2008 SonicWALL ist eine eingetragene Marke von SonicWALL, Inc. Alle anderen hier erwähnten Produktnamen sind Eigentum der jeweiligen Inhaber. Änderung technischer Daten und Produktbeschreibungen ohne vorherige Ankündigung vorbehalten.