5 Schritte um Ihren Office 365 Schutz zu verbessern

PROBLEMZUSAMMENFASSUNG

Eine umfassende Verteidigung ist von grundlegender Bedeutung, um Office 365-Benutzer vor ausgefeilten Phishing-Attacken zu schützen.

Microsoft Office 365 ist eine der weltweit führenden Softwareplattformen und hat 135 Millionen aktive Geschäftsbenutzer. Das Produkt wird in verschiedenen Paketen angeboten, einschließlich Produktivitäts-, Kooperations- und Kommunikationsanwendungen sowie Funktionen, um diese, die Plattform und die Benutzer zu schützen. Viele Organisationen setzen eine umfassende Verteidigungsstrategie ein, um Office 365-Benutzer vor ausgefeilten Phishing-Bedrohungen zu schützen.

Phishing ist derzeit die Top-Cybersicherheitsbedrohung

Phishing ist die wichtigste Quelle von Sicherheitsverletzungen – Die Zunahme des Phishing hat diese Bedrohung laut einer Umfrage von Osterman Research im Oktober 2018 zum wichtigsten Sicherheitsproblem unter IT-Managern gemacht. Phishing liegt dabei noch vor Ransomware. Die Sorgen um diese Bedrohungen basieren auf der Realität: In der gleichen Umfrage wurde Phishing auch als wichtigste Quelle von Sicherheitsverletzungen ermittelt. 54 % der Organisationen, die Office 365 als E-Mail-Plattform verwenden, melden, einem erfolgreichen Phishing-Angriff ausgesetzt gewesen zu sein. Und in der Regel nicht nur einem: die durchschnittliche Zahl erfolgreicher Phishing-Verletzungen, die pro Organisation für das Vorjahr gemeldet wurden, betrug 11,7.

IT-Manager beobachten wachsende Phishing-Volumina, die bei Benutzern ankommen – Phishing hat sich zu einem riesigen Problem entwickelt. Manche Sicherheitsinfrastruktur wird damit besser fertig als andere. Sowohl Branchenumfragen als auch kontrollierte E-Mail-Tests bestätigen, dass eine steigende Zahl von Phishing-E-Mails bestehende Sicherheitsvorkehrungen umgeht und Geschäftsbenutzer erreicht, und zwar unabhängig von der verwendeten E-Mail-Plattform. In der gleichen oben zitierten Umfrage sagten 45 % der IT-Manager und Sicherheitsadministratoren, dass die Anzahl der Phishing-E-Mails, die ihre Office 365-Benutzer erreichten, in den vergangenen 12 Monaten drastisch angestiegen sei. Sie schätzten den durchschnittlichen Anstieg mit 25 % ein, und mehr als die Hälfte meldete einen Anstieg beim zielgerichteten Spearphishing um 26 Prozent. Der zunehmende Erfolg von Phishing ist mit dem Anstieg der Aktivitäten der „Phishing-Industrie" verknüpft. Die eigene automatisierte Überwachung aktiver Phishing-URLs weltweit durch Cyren ergab einen drastischen Anstieg um 172 % in den 18 Monaten bis Ende 2017, auf insgesamt mehr als 10 Millionen aktive Phishing-URLs zu jedem beliebigen Zeitpunkt.

Realistische Tests zeigen eine „Fehlerquote" von 7,2 % – In realistischen Tests bestätigen die Ergebnisse der von Cyren durchgeführten E-Mail-Sicherheitsbeurteilungen das Ausmaß des Problems. Aggregierte Daten von Cyrens E-Mail-Sicherheitslücken-Analysetests bei verschiedenen Unternehmen mit unterschiedlichen bestehenden Sicherheitslösungen einschließlich Office 365 ergaben eine Fehlerquote von 7,2 %. Das bedeutet, dass 7,2 % aller an Benutzer gelieferten E-Mails entweder Spam oder Phishing waren oder Malware-Anhänge hatten. Bei der genaueren Untersuchung einer Stichprobe von 2,7 Millionen E-Mails identifizierten wir mehr als 7000 als Phishing-E-Mails. Mit zunehmender Geschwindigkeit und Fähigkeit der Phishing-Angriffe, Abwehrmaßnahmen zu umgehen, stellt eine ausreichend schnelle Entdeckung und Aktualisierung des Schutzes (in Sekunden oder Minuten, nicht in Stunden oder gar Tagen) eine große Herausforderung für herkömmliche E-Mail-Sicherheitsarchitekturen dar.

WAS SIE TUN KÖNNEN, UM OFFICE 365-E-MAIL-BENUTZER VOR PHISHING ZU SCHÜTZEN

1. **Automatisieren Sie E-Mail- und Websicherheits-Bedrohungs-Updates auf das kürzeste mögliche Zeitintervall.** Sie müssen sicherstellen, dass es keine zeitliche Verzögerung gibt, um sich vor neuen Bedrohungen zu schützen.
2. **Ergänzen Sie die native Office 365-E-Mail-Sicherheit mit cloudbasiertem E-Mail-Gateway-Schutz von einem Sicherheitsanbieter.** Cloudbasierte sichere E-Mail-Gateways bieten erweiterte Sicherheit wie Time-of-Click-URL-Analyse, Sandboxing und Schutz vor Phishing und Spear-phishing, darunter Business Email Compromise.
3. **Stellen Sie ein Websicherheits-Gateway bereit.** Ein wirksames Websicherheits-Gateway blockiert Verbindungen zu Phishing-Websites und Botnet-Command & Control-Servern.
4. **Verwenden Sie Multi-Faktor-Authentifizierung.** Die Wiederverwendung von Passwörtern macht Phishing für Kriminelle besonders attraktiv. Implementieren Sie Multi-Faktor-Authentifizierung unter Office 365, um Verletzungen der E-Mail-Account-Sicherheit zu verhindern.
5. **Schulen Sie Benutzer kontinuierlich.** Schulen Sie Benutzer zu Social Engineering-Tricks, die von Kriminellen eingesetzt werden, testen Sie die Benutzer und wiederholen Sie dies kontinuierlich.

CYREN

25 Mrd.
Sicherheitstransaktionen pro Tag

1,3 Mrd.
geschützte Benutzer

300 Mio.
abgewehrte Gefahren pro Tag

Websicherheit versagt ebenfalls – Wenn E-Mail-Sicherheit eine Phishing-E-Mail nicht blockiert und der Benutzer auf den darin enthaltenen Link klickt, können Sie ihn durch Blockieren der Verbindung mit der Phishing-URL trotzdem noch schützen. Cyren bietet ein kostenloses Web-Security-Test an, das die Effektivität der Websicherheit eines Benutzers beim Blockieren von Phishing-Websites evaluiert und andere Tests durchführt. Bis dato wurden mehr als 20.000 Diagnosen ausgeführt. Bei 62 % wurde ein grundlegender Phishing-URL-Test nicht bestanden, 75 % bestanden einen separaten Zero-Day-Phishing-Test nicht, bei dem geprüft wird, ob ein Benutzer auf eine Phishing-URL zugreifen darf, die in den vergangenen 24 Stunden neu ist. Dies erfolgt zum Teil, weil ein Großteil der Websicherheits-Infrastruktur auf eine Weise angelegt wurde, die der E-Mail-Sicherheit ähnelt und das gleiche „Anfälligkeitsfenster"-Problem aufweist: die Zeit zwischen der Erkennung einer Bedrohung und der Anwendung von Schutzaktualisierungen bleibt hinter der Geschwindigkeit moderner Bedrohungen zurück.

Unternehmen versuchen, Benutzer zu schulen, doch mangelt es an Beständigkeit – Bei der Umfrage von Osterman Research gaben 94 % der IT-Manager an, irgendwann für ihre Benutzer eine Schulung zum Thema Phishing durchgeführt zu haben. Dies zeigt, dass das Problem als solches erkannt und der Schutz davor als ein wesentlicher Bestandteil einer umfassenden Verteidigungsstrategie angesehen wird. Es ist aber Fakt, dass selbst hervorragend geschulte Benutzer oft Probleme haben, eine schlau entworfene Phishing-E-Mail-Nachricht zu erkennen, und ein bestimmter Anteil der Benutzer nimmt Schulungsinformationen nicht besonders gut auf. Darüber hinaus reicht eine einmalige Schulung nie aus. Studie um Studie belegt, dass eine kontinuierliche Schulung erforderlich ist. Nur 19 % der gleichen Befragten führten aber regelmäßige Vertiefungsschulungen durch.

> „Mit ausgefeilten Hacking-Mechanismen kann ein Eindringling auf schwach geschützte Transaktionen abzielen und dem Käufer z. B. eine E-Mail von einer Adresse senden, die fast mit der des Notarbüros identisch ist, mit einer plausiblen Betreffzeile, die auf eine „Überweisungsänderung" hinweist."
>
> **STAATLICHE US-WARNUNG VOR IMMOBILIEN-ÜBERWEISUNGSBETRUG, 10. APRIL 2018**

HÄUFIGE PHISHING-ATTACKEN UND DEREN AUSWIRKUNGEN

Office 365-Kunden müssen sich u. a. vor den folgenden häufigen Arten von Phishing schützen:

Anmeldeinformationen Phishing – E-Mail-Absender geben sich in der Regel als bekannte Marken, Social Media-Websites oder Online-Händler wie Apple, Amazon, Facebook und Microsoft aus. Die E-Mail enthält oft einen Link, der den Benutzer auf eine gefälschte Anmeldeseite weiterleitet, mit dem Ziel, seine Anmeldeinformationen zu stehlen. Diebstahl von Anmeldeinformationen ist vor allem deswegen ein Problem, weil Benutzer oft die gleichen Passwörter für private wie geschäftliche Accounts verwenden. Dadurch sind Arbeitgeber einem hohen Risiko ausgesetzt. Der Angreifer kann dann versuchen, mit den per Phishing angeeigneten Anmeldedaten auf Geschäftsanwendungen zuzugreifen, z. B. um sich bei Office 365 anzumelden und die Kontrolle über die E-Mail des Benutzers zu erhalten, um auf Salesforce.com zuzugreifen, um Kundeninformationen zu stehlen oder in Ihre Finanzsysteme einzudringen.

Finanz-Phishing – E-Mail-Absender geben sich dabei in der Regel als bekanntes Finanzinstitut aus und ermutigen den Empfänger, sein Geschäftskonto zu validieren oder warnen vor einer nicht autorisierten Transaktion. Wenn ein Benutzer auf den Link klickt, gelangt er zu einer gefälschten Website, auf der der Angreifer versucht, die Anmeldedaten zu stehlen. Damit bereitet er sich auf den Diebstahl von Finanzinformationen oder Mitteln vor. Das Ergebnis ähnelt dem obigen, außer dass der Angreifer sich jetzt direkt bei einem hochwertigen Vermögenswert wie dem Bankkonto des Unternehmens anmelden kann.

Spearphishing und Business Email Compromise (BEC) – Diese Arten von Phishing-E-Mails enthalten selten Links und sind in der Regel sehr zielgerichtet. Sie können vorgeben, z. B. von einer Führungskraft zu stammen, und zielen oft auf ein Mitglied des Finanzteams ab. Dabei wird dazu aufgerufen, einem angeblichen Geschäftspartner Mittel zu überweisen, oder es wird um Steuerinformationen von Mitarbeitern gebeten. Der Angreifer nutzt meist Verschleierungstechniken, damit die E-Mail wie eine Nachricht von der E-Mail-Adresse des jeweiligen vorgegebenen Absenders stammt. Wenn der Angreifer den E-Mail-Account des Absenders gehackt hat, kann er natürlich eine „echte" E-Mail senden. Das Ergebnis von BEC-Angriffen ist in der Regel ein finanzieller Verlust, auch wenn Prozesse implementiert sind, um Betrug dieser Art zu verhindern. Der E-Mail-Empfänger lässt die normalen Prozesse in diesem Fall vielleicht außer Acht, weil es dem Angreifer gelungen ist, eine besondere Dringlichkeit zu vermitteln.