Cybersecurity-Awareness für Fortgeschrittene

Es vergeht kaum ein Monat, an dem nicht vor neuen Phishing-Attacken gewarnt wird. Und die Phishing-Methoden der Angreifer werden immer raffinierter. Dass immer mehr Mitarbeitende von unterwegs oder aus dem Homeoffice arbeiten und zum Teil zwischen Firmen- und Privatgeräten wechseln, spielt den Angreifern zusätzlich in die Hände.

VON MAX KELLER

Phishing ist die am meisten genutzte Angriffsmethode von Cyberkriminellen und weiteren Betrügern. Die Wahl dieses Initial Access Vectors (Angriffsvektor, der für den initialen Zugriff bzw. die initiale Kompromittierung eines Benutzerkontos, Computers oder IT-Systems genutzt wird) ist kein Zufall. Sie deutet unmissverständlich auf die schwächste Komponente in der Cybersecurity hin: den Menschen. Dass der menschliche Faktor den Grossteil erfolgreicher Cyberangriffe ausmacht, wird von zahlreichen Threat Intelligence Reports einschlägiger Cybersecurity-Anbieter untermauert. Je nach betrachteter Studie lassen sich 40 bis 70% der erfolgreichen Cyberangriffe auf das Phishing und damit die menschliche Schwachstelle zurückführen. Für Unternehmen ist es deshalb von besonderer Bedeutung, Mitarbeitende auf diese Bedrohung zu sensibilisieren.

Auf den Typ kommt es an

Phishing-Mails können in zwei Typen unterschieden werden: URL- bzw. Link-basierte Angriffe und Angriffe, die mittels Anhängen bzw. Attachments erfolgen. Bei der ersten Form geht es vor allem darum, Mitarbeitende auf eine täuschend ähnlich aussehende und vertrauenswürdig wirkende Website zu leiten, um dort die Credentials (Benutzernamen und Passwörter) mittels einer Login-Maske abzugreifen (Credential Harvesting). Bei der zweitgenannten Art wird der Phishing-Mail direkt ein Anhang beigefügt, welcher mit Schadprogrammen präpariert und oft mittels Makros ausgeführt wird. Da sich die E-Mail-Security der Unternehmen im Verlauf der letzten Jahre stetig verbessert hat (bessere Spam- und Phishing-Filter, Blocklisting bestimmter Dateitypen, standardmässige Blockierung der Makros durch Microsoft usw.), verlagerten die Cyberkriminellen ihren Fokus auf URL-basierte Angriffe. Dennoch zeigen die Ergebnisse von simulierten Phishing-Kampagnen, dass die Attachment-basierten Angriffe eine höhere Erfolgsquote (durchschnittlich 15%) als Credential-Harvesting-Angriffe (durchschnittlich 5%) haben, wenn eine entsprechende Phishing-Mail im Posteingang der Mitarbeitenden landet. So oder so sollten die Mitarbeitenden auf diese Angriffsarten aufmerksam gemacht werden. Dazu eignen sich virtuelle Trainings- bzw. Schulungssequenzen zu Themen rund um die Informationssicherheit sowie simulierte Phishing-Angriffe.

Herausforderungen bei der Sensibilisierung der Mitarbeitenden

Aufgrund der hohen Relevanz der Sensibilisierung von Mitarbeitenden haben sich zahlreiche Anbieter auf dem «Awareness-Markt» positioniert, die digitale Trainingssequenzen anbieten. Die Wahl eines passenden Anbieters ist dennoch nicht trivial. Schliesslich sollen die Trainingsinhalte möglichst nachhaltig in den Köpfen der Mitarbeitenden bleiben. Dazu werden meist didaktische und spielerische Methoden (Gamification) genutzt. Die Identifizierung des am besten geeigneten Anbieters bzw. der am besten geeigneten Trainingseinheiten stellt für Entscheidungsträger ohne pädagogisches Verständnis die erste, jedoch nicht die letzte Hürde dar.

Ist der Entscheid getroffen, gilt es, die Trainingseinheiten auszurollen und möglichst vollständig zu absolvieren. In der Vollständigkeit liegt die zweite Herausforderung, da sich einige Mitarbeitende der Wichtigkeit solcher Trainings nicht bewusst sind. Cybersecurity ist Chefsache. Deshalb müssen sich vor allem Führungskräfte zu der Durchführung von Sensibilisierungstrainings committen und dieses Commitment bei der Belegschaft einfordern. Doch auch danach ist der Erfolg einer Awareness-Kampagne eine Frage eines stetigen Nachfassens und Erinnerns der Mitarbeitenden. Da oft die Gefahr besteht, dass Schulungssequenzen «durchgeklickt» werden, empfiehlt sich immer ein anschliessender Test, um das Gelernte einerseits zu verinnerlichen und andererseits den Lernerfolg zu überprüfen. Die Redewendung «Steter Tropfen höhlt den Stein» gilt auch bei Awareness-Trainings.

Auswertung von Phishing-Simulationen

Phishing-Simulationen haben sich ebenso als eine Möglichkeit zur Überprüfung des Lernerfolgs von Awareness-Trainings etabliert. Die präparierten Phishing-Mails können zahlreiche Erkennungsmerkmale (Absender, Absender-E-Mail, Betreffzeile, Rechtschreibfehler, persönliche Ansprache,

Autor

Max Keller leitet das Funk RiskLab beim Versicherungsbroker Funk Gruppe.

Phishing-Angriffe werden immer vielfältiger und raffinierter.

Gestaltung der URL bzw. des schadhaften Links usw.) enthalten, deren Anzahl zugleich auch den Schwierigkeitsgrad der Phishing-Simulation ausmacht. Die Wahl des Angriffsszenarios trägt ebenfalls zum Schwierigkeitsgrad der Simulation bei. So ist ein Szenario, welches auf die Kommunikationsplattform Zoom ausgerichtet ist, für die Unternehmen schwieriger abzuwehren, die tatsächlich mit dieser Anwendung arbeiten. Der Zeitpunkt des Versands einer simulierten Phishing-Mail ist ebenso entscheidend. Am Anfang und am Ende der Woche ist die Awareness am höchsten. Deshalb nutzen Cyberkriminelle oft den Dienstag oder Donnerstag zum Verschicken von Phishing-Mails, da hier der Stresslevel der Mitarbeitenden am höchsten respektive die Awareness am niedrigsten ist.

Nach der Durchführung der Phishing-Simulation geht es an deren Auswertung. Üblicherweise werden Kennzahlen wie die Klickrate auf den Link, die Öffnungsrate des Attachments oder die Anzahl offengelegter Credentials (Compromised Credentials Rate) angeschaut und für die Beurteilung des Erfolgs bzw. Misserfolgs einer Phishing-Simulation herangezogen. Diese sind jedoch nur eine Seite der Medaille. Die andere Seite macht die Reporting Rate aus. Diese impliziert die Anzahl der Mitarbeitenden, die das Phishing-Mail an die IT- oder Cybersecurity-Verantwortlichen meldeten. Mit einer Meldung einer Phishing-Mail oder einer erfolgreichen Kompromittierung eines Mitarbeitenden können in der Realität zeitnah proaktive Schritte (z.B. Blocklisting des Absenders, Deaktivierung eines Benutzerkontos oder Änderung eines Passworts) eingeleitet werden, um das Risiko eines Cyberangriffs einzudämmen. Ebenso empfiehlt es sich, einen genaueren Blick auf die Mitarbeitenden zu werfen, die auf die Phishing-Mail reingefallen sind. Denn die Kompromittierung eines Mitarbeitenden mit umfangreichen Zugriffsrechten (meist Führungskräfte) ist ernsthafter einzuschätzen als die eines Mitarbeitenden mit sehr eingeschränkten Zugriffsrechten.

Awareness und Fehlerkultur gehen Hand in Hand

Die Reporting Rate bzw. die Meldung eines erfolgreichen Phishing-Angriffs auf einen Mitarbeitenden ist für die Abwehr von Phishing-basierten Cyberangriffen von besonderer Bedeutung. Dafür sollte jedoch eine entsprechende Fehlerkultur im Unternehmen etabliert werden, die solche «Fehler» zulässt. Unsere Gesellschaft ist nun mal auf Effizienz getrimmt und das Klicken auf Links gehört zu unserem Berufsalltag. Die Abwehr der Phishing-Versuche wird künftig immer schwieriger werden, dafür sorgen neue KI-basierte Instrumente wie ChatGPT. Viel wichtiger sind unsere Reaktionen darauf.

Acht Sicherheitsmassnahmen

1. Nutzung von Phishing-resistenten Multi-Faktor-Authentifizierungs-(MFA-)Verfahren wie FIDO, QR-Codes oder physischen Token.
2. Implementierung von grundlegenden Zero-Trust-Richtlinien wie einer Step-up-Authentifizierung beim Starten vertraulicher Anwendungen, einer zwingenden Verwendung von MFA bei Profiländerungen oder einer Einrichtung automatischer Warnungen bei einem riskanten Benutzerverhalten.
3. Segmentierung des Netzwerks, um bei erfolgreichem Phishing die Bewegungsfreiheit des Angreifers innerhalb des Netzwerks einzuschränken und den Zugriff auf vertrauliche Ressourcen zu blockieren.
4. Sicherung der Endgeräte, die für Phishing und Malware anfällig sind, da der traditionelle Netzwerkperimeter im Cloud-Zeitalter als Verteidigungslinie ausgedient hat.
5. Überprüfung der BYOD-Richtlinien und der Vorgaben für die Mitarbeiter zur Nutzung von Endgeräten beim Zugriff auf Unternehmensanwendungen über das Internet.
6. Regelmässige Durchführung von «Phishing-Übungen» mit Live-Test-Szenarien und Red-Team-Trainings, wie im Artikel beschrieben.
7. Förderung einer engeren Zusammenarbeit zwischen den Fachabteilungen und der IT, um die Identity Governance und das Lifecycle-Management von Zugriffsberechtigungen zu verbessern.
8. Kontinuierliche Überprüfung von Zugangsberechtigungen und Durchführung von Penetrationstests sowie Optimierung ineffizienter Workflows und Prozesse.

(QUELLE: CYBERARK / RED.)