Datenblatt

Phishing Kampagne

Phishing gehört heute zu den Top-Cyberrisiken in Unternehmen. E-Mais sind aus unserem Geschäftsleben und Privatbereich nicht mehr wegzudenken. Daher nutzen immer mehr Kriminelle sogenannte Phishing-Mails, um an sensible Daten zu kommen oder durch betrügerische Mails Geld zu erschwindeln. Häufig genügt schon der Klick eines einzelnen Mitarbeiters, um als gesamtes Unternehmen Opfer eines Phishing-Angriffs zu werden.
Ohne sensibilisiertes und geschultes Personal ist ein wirksamer Schutz gegen diese Form von Cyber-angriffen unmöglich. Simulierte Phishing-Angriffe sind eine wirksame Maßnahme, um das Bewusstsein Ihrer Mitarbeiter zu erhöhen oder den Erfolg erfolgter Trainingsmaßnahmen zu überprüfen.

Das secobit Phishing Paket

Beim secobit Phishing-Angriff handelt es sich um einen geplanten, simulierten Angriff per E-Mail, den wir in Ihrem Auftrag und in enger Absprache mit Ihnen durchführen. Im Rahmen des Angriffs wird weder Schadsoftware heruntergeladen noch werden vertrauliche Daten ausgelesen oder missbraucht. Stattdessen messen wir, wie viele der adressierten Mitarbeiter den Angriff nicht als solchen erkennen und den Link in der von uns präparierten Phishing E-Mail anklicken und eventuell auch Daten auf der Web-Seite eingeben.

Leistungen im Überblick

Folgende Leistungen sind Bestandteil des Basis-Pakets:

- Bereitstellung von Informationen und Templates zur technischen, organisatorischen und kommunikativen Unterstützung der Awareness-Kampagne innerhalb Ihres Unternehmens
- Bereitstellung von Templates und Textvorschlägen für die Phishing E-Mail und die Zielseite, die sich hinter dem angebotenen Link befindet
- Abstimmung des Vorgehens sowie der Inhalte der Phishing Awareness-Kampagne
- Initialisierung der Zielseite sowie des Zählmechanismus
- Einmaliges oder wiederholtes Versenden von Phishing E-Mails an eine durch Sie definierte Nutzergruppe
- Protokollierung der Zugriffe auf die Zielseite im definierten Auswertungszeitraum sowie Analyse der gesammelten Daten
- Informationsmail an das Opfer mit Link zum Online Phishing-Training (einstellbar)
- Abschließender Bericht über die Anzahl der Zielseitenbesuche unterschiedlicher Mitarbeiter

Darüber hinaus haben Sie die Möglichkeit, optionale Leistungen unserer Berater in Anspruch zu nehmen, wie die begleitende Beratung und Koordination des Phishing-Angriffs oder die Konzeption eines entsprechenden Security Awareness Programms für Ihre Mitarbeiter.

Unser Vorgehensmodell

Vorbereitung

In einem Vorbereitungsmeeting legen wir mit Ihnen den Umfang der Phishing-Kampagne fest. Wir stimmen mit Ihnen gemeinsam den Versandtermin der Phishing E-Mail, Inhalt der E-Mail und der Zielseite, die Absender-Adresse, die konkrete Zielgruppe, den Auswertungszeitraum und das

abschließende Reporting auf Basis unseres Standards ab. Weiterhin haben Sie in dieser Phase die Möglichkeit, Ihre interne Organisation und IT auf das Vorhaben vorzubereiten.
Ergebnis dieser Phase ist ein dokumentiertes Vorgehen inklusive der gemeinsam abgestimmten Inhalte. Sie geben dies final frei.

Durchführung

Wir empfehlen, die Phishing-Kampagne vorher mit der Arbeitsnehmervertretung abzustimmen und den Mitarbeitern per Email anzukündigen. Nach Ihrer expliziten Freigabe starten wir die Kampagne auf unserer Phishing Plattform, stellen die abgestimmte Zielseite online und richten den Zählmechanismus für Ihre Zielseite ein. Die versendeten Phishing E-Mails enthalten dazu einen Link zur Zielseite. Wir können sowohl den Besuch der Zielseite als auch die Eingabe von Daten auf der Zielseite auswerten.

Auswertung

Nach einem vorher bestimmten Zeitraum wird die Kampagne gestoppt, die Daten werden ausgewertet, in einem übersichtlichen Bericht zusammengefasst und Ihnen zur Verfügung gestellt.

Bericht

Der Abschlussbericht beinhaltet die folgenden Punkte:

- Beauftragungsdatum, Versandtermin und Auswertungszeitraum
- Absender-Adresse
- Phishing E-Mail (Texte und finaler Snapshot)
- Zielseite (Texte und finaler Snapshot)
- Anzahl der versendeten E-Mails
- Gesamtzahl der Zielseitenbesuche und der Eingaben auf dieser Seite
- Anzahl der Besuche von verschiedenen Mitarbeitern

Projektabschluss

In einer Abschlussbesprechung gemeinsam mit Ihrem Projektleiter, Berater oder dem Verantwortlichen wird die Phishing-Kampagne ausgewertet, offene Fragen des Abschlussberichtes erörtert und Empfehlungen fixiert.

Ihre Beistellungsleistung

- Teilnahme der Verantwortlichen am Vorbereitungsgespräch und innerbetriebliche Abstimmung.
- Mitarbeit bei der Definition und Erstellung einer E-Mail-Vorlage.
- Teilnahme der Verantwortlichen an der Abschlusspräsentation.

Wer profitiert von diesem Service?

- Sie als Geschäftsführer oder Sicherheitsverantwortlicher
- Ihr Unternehmen durch gezielte Verbesserung in auffälligen Bereichen
- Ihre Mitarbeiter durch Schutz der Unternehmenswerte und ihres Arbeitsplatzes

---

Bestellung

Secobit GmbH
Warndtstraße 28
86161 Augsburg
Telefon: +49 821 5675041
Email: awareness @secobit.de

Weitere Information

unter https://secobit.de/phishing

Leistungserbringung

Sofern nicht schriftlich anders vereinbart gelten für die Leistungserbringung die „Allg. Geschäftsbedingungen der secobit GmbH“.

