6 Gründe, warum Social Engineering in der Urlaubszeit erfolgreicher ist

Human-Engineering-Angriffe, Phishing-Versuche und die Nachahmung von Führungskräften sind in der Urlaubszeit erfolgreicher. Hier sind sechs Gründe weshalb:

1

Cyberkriminelle wissen, dass viele nicht im Büro sind.

Wenn also ein "kritischer" Anruf, eine E-Mail oder eine Sofortnachricht mit einer Aufgabe, die sofort erledigt werden muss, eintrifft, ist es weniger wahrscheinlich, dass die Angestellten deren Gültigkeit in Frage stellen. Dieselben Mitarbeiter stehen vielleicht sogar noch mehr unter Zeitdruck, weil ein Kollege im Urlaub ist, und sie wollen ihn nicht mit einem Anruf belästigen, um die Gültigkeit der Anfragen zu überprüfen.

2

Mitarbeiter nehmen auch ihre Arbeitsgeräte mit

Auch Arbeits-Laptops werden oft mit in den Urlaub genommen. Arbeitnehmer, die sich dringenden Projekten widmen oder vielleicht auch nur ihre E-Mails und Teams im Auge behalten wollen, während sie weg sind, nehmen wahrscheinlich ihre Arbeitsgeräte mit. Während diese Geräte die Sicherheitskontrollen am Flughafen, den Zoll und die Fahrt im Taxi vom Flughafen oder Bahnhof zum Hotel passieren, werden die Geräte und die darauf befindlichen Daten anfälliger für Diebstahl. Gestohlene Geräte können Bösewichten genau die Informationen liefern, die sie für einen erfolgreichen Social-Engineering-Angriff benötigen.

3

Cyberkriminelle nutzen Wifi-Spots aus

Die meisten Hotels und viele Flughäfen bieten Wi-Fi an, oft kostenlos, was es Bedrohungsakteuren sehr leicht macht, Daten zu exfiltrieren und Anmeldeinformationen zu stehlen. Sobald die Kriminellen im Besitz der benötigten Daten und Anmeldeinformationen sind, können sie sich als Teammitglieder ausgeben und kurzen Prozess machen.

4

IT-Fachleute sind im Urlaub

Auch wenn jeder für die **Cybersicherheit** verantwortlich ist, bleibt die Tatsache bestehen, dass kritische Systemaktualisierungen und die Behebung von Cyberverletzungen von IT-Experten durchgeführt werden. Doch was passiert, wenn diese Fachleute im Urlaub sind? Die Reaktionszeiten können sich verlängern, und es kann zu Verzögerungen bei wichtigen Aktualisierungen kommen. Auch wenn automatisierte Lösungen helfen können, können Lücken in den IT-Teams während der Urlaubszeit Social Engineers das nötige Zeitfenster verschaffen, um in einem Unternehmen Fuß zu fassen.

5

Mitarbeiter sind abgelenkt

Die größte Bedrohung während der Feiertage ist menschliches Versagen, insbesondere dann, wenn die Mitarbeiter abgelenkt oder in Eile sind. Für Cyberkriminelle ist es ein Leichtes, schnell das Vertrauen aufzubauen, das sie brauchen, um dann nach sensiblen Informationen oder, noch schlimmer, nach einer betrügerischen Transaktion zu fragen. Mitarbeiter können überfordert und abgelenkt genug sein, um kleine Fehler zu machen, die große Folgen haben können. Ein abgelenkter Mitarbeiter kann sehr leicht einen offensichtlichen Social-Engineering-Angriff übersehen.

6

Mitarbeiter, die online mitteilen, dass sie im Urlaub sind

Es ist so, als würde man mitteilen, dass das Haus nicht abgeschlossen ist: Cyberkriminelle können in manchen Fällen nur vermuten, dass ein Team unterbesetzt ist, wenn aber einzelne Mitarbeiter des Teams ihren Urlaub in sozialen Medien posten, können Cyberkriminelle die Gelegenheit für einen Angriff nutzen. Dies ist eine Form des Social Engineering, die als Pretexting bekannt ist.

Social Engineering ist ein wachsendes Problem im Bereich der Cybersicherheit, aber die Werkzeuge, um dieser Praxis entgegenzuwirken, sind vorhanden. Ganzheitliche E-Mail-Sicherheitsrichtlinien, gepaart mit einem starken Cybersecurity-Bewusstseinstraining, können Teams dabei helfen, auf dem Laufenden zu bleiben und ihre Verteidigung weiterzuentwickeln, um die neuesten Taktiken der Angreifer zu blockieren. Sehen Sie, wie Mimecast KI einsetzt, um Social Engineering zu vereiteln.