Phishing in Schulen

für Beginner

Herzlich willkommen! Dies ist das zweite E-Book in unserer Reihe „Cybersicherheit in Schulen“. In dieser Serie machen wir einen Streifzug durch die häufigsten Bedrohungen der Cybersicherheit, denen Schulen ausgesetzt sind. **Unser erstes Thema war Malware.**

So gern wir auch unsere Angeln und Köder herausholen würden, dies ist ein **Phishing-Trip** der anderen Art.

jamf

IN DIESEM E-BOOK GEHT ES UM:

Was ist Phishing?

„Phishing“ ist ein ziemlich alter Begriff, zumindest seit es das Internet gibt. Er kam bereits vor der Erfindung des Wi-Fi und der Einführung von Websites wie Google und Wikipedia auf. Wie beim guten alten Offline-Angeln werden beim Phishing Köder verwendet, um ahnungslose Menschen in eine Falle zu locken.

Phishing dient dazu, Daten wie Bankdaten, Anmeldeinformationen oder persönliche Informationen wie Geburtstag oder Sozialversicherungsnummer zu sammeln. Laut dem **IBM 2023 Cost of a Data Breach Report** ist dies die häufigste Methode des Erstangriffs und macht 16 % der Datenschutzverletzungen aus. Außerdem ist es sehr teuer: Diese Betrugsmache kostet Unternehmen durchschnittlich 4,76 Millionen Dollar.

In der Regel werden beim Phishing einige gängige Taktiken angewandt, um die Wahrscheinlichkeit zu erhöhen, dass die Opfer den Köder schlucken:

Dringlichkeit: Die Angreifer fordern oft sofortige Aufmerksamkeit und drohen mit dem Verlust eines Kontos, mit Strafen für Zahlungsverzug, mit dem Schaden für eine geliebte Person oder mit einer anderen Form von negativen Konsequenzen. Oder sie appellieren an die Freundlichkeit, indem sie behaupten, sie befänden sich in einer misslichen Lage und Sie könnten ihnen helfen.

Ähnlich aussehende URLs: Website-URLs können wie echte URLs aussehen, aber Sonderzeichen enthalten. Websites oder E-Mails können so verändert worden sein, dass sie vertraut aussehen, wie eine Bankwebsite oder eine E-Mail zum Zurücksetzen des Passworts.

Nachahmung: Hacker können sich als Personen ausgeben, die Sie kennen, indem sie deren E-Mail-Adresse, Telefonnummer oder sogar Stimme verwenden, um die Wahrscheinlichkeit zu erhöhen, dass Sie auf ihren Phishing -Versuch reagieren.

Angreifer nutzen diese Social-Engineering-Methoden aus dem einfachen Grund, dass sie oft keine großen technischen Kenntnisse erfordern. Es ist viel einfacher, jemanden auszutricksen, damit er dem Angreifer seine Kontodaten gibt, als alle Passwortkombinationen auszuprobieren, bis sie das richtige haben.

Social Engineering

Social Engineering ist eine Tricktechnik, die psychologische Manipulation einsetzt und menschliche Fehler oder Schwächen ausnutzt, um an private Informationen, Zugangsdaten oder Wertgegenstände zu gelangen. Dies wird manchmal als „Human Hacking“ bezeichnet.

Häufige Arten von Phishing-Angriffen

Phishing-Angriffe gibt es in verschiedenen Formen. Schauen wir uns nun einige von ihnen an.

E-MAIL-PHISHING

Die Angreifer senden eine E-Mail an eine große Gruppe von Personen. Diese E-Mail kann einen Anhang enthalten, in der sich Malware befindet, oder einen Link, der zu einer Website führt, die darauf abzielt, die Anmeldedaten zu stehlen.

SPEAR-PHISHING

Oft haben die Angreifer bestimmte Personen oder kleine Gruppen im Visier und kontaktieren diese per E-Mai. Diese E-Mails enthalten Inhalte, die der Zielperson bekannt sind. Schüler und Lehrer könnten beispielsweise eine E-Mail erhalten, die aussieht, als stamme sie von einer Software, die sie für die Schule verwenden, die aber Links zu einer bösartigen, ähnlich aussehenden Website enthält.

WHALING

Diese Angriffe konzentrieren sich auf prominente Personen, wie z. B. den CEO eines Unternehmens. Die Angreifer geben sich eventuell als Geschäftspartner aus und fordern Geld durch eine Überweisung. Oder sie geben sich als Hausmeister aus, um Informationen von einem Schulleiter zu erhalten.

WATERING-HOLE

Ein Watering-Hole-Angriff ähnelt dem Spear-Phishing, da beide Angriffe für ein bestimmtes Ziel entwickelt werden. Eine Watering-Hole beginnt jedoch im Allgemeinen nicht mit der Kontaktaufnahme zu einer Person. Stattdessen hacken sich die Angreifer in eine Website, die ihre Zielpersonen besuchen, und verändern sie so, dass sie deren Daten stehlen oder Malware installieren können.

DNS-SPOOFING

Wenn Sie eine Website-Adresse in Ihren Browser eingeben, übersetzt die DNS-Software (Domain Name System) diese Adresse in eine Reihe von Zahlen, die für die Website eindeutig sind. DNS-Spoofing trickst die DNS-Software aus, indem es die Nummern ändert. Das bedeutet, dass Sie, wenn Sie die richtige Adresse in Ihren Browser eingeben, von der nun kompromittierten DNS-Software auf die Website eines Angreifers geleitet werden, in der Hoffnung, dass Sie private Informationen eingeben.

SMISHING

Smishing ist eine Kombination aus „SMS“ und „Phishing“, d. h. es handelt sich um Phishing, das per Textnachricht durchgeführt wird. Dies kann schwierig zu erkennen sein, da Links in Textnachrichten oft gekürzt oder schwer zu erkennen sind.

Menschen benutzen ihre mobilen Geräte eher, wenn sie in Eile oder unterwegs sind, so dass sie sich weniger Zeit nehmen, den Link zu überprüfen.

VISHING

Vishing ist eine Kombination aus „Voice“ (Stimme) und „Phishing“, d. h. Phishing, bei dem die Stimme einer Person verwendet wird. Das kann die Stimme eines Fremden am Telefon sein, die es auf die Hilfsbereitschaft der Menschen abzielt. Dank der Fortschritte bei der künstlichen Intelligenz (KI) kann dies sogar die Stimme eines geliebten Menschen sein, der Sie dringend bittet, ihm Geld zu schicken.

In welchem Umfang sind Schulen von Phishing betroffen

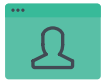
Der K12 Security Information eXchange (K12 SIX) bietet einen Leitfaden zur Cybersicherheit für Schulen an. In ihrer Incident Map listet K12 SIX die Cybersecurity-Vorfälle auf, denen Schulen in den Vereinigten Staaten zwischen 2016 und 2022 ausgesetzt waren. Hier sind einige Beispiele dafür, wie Schulen von Phishing betroffen sein können:

Es wurden E-Mails mit einem Phishing-Link an Lehrkräfte verschickt, die es den Angreifern ermöglichten, **die Gehaltszahlungen der Lehrkräfte umzuleiten**, was zu gestohlenen Gehaltsschecks im Wert von über 50.000 Dollar führte.

Ein Angreifer, der sich als Auftragnehmer des Verwaltungsbezirks ausgab, verleitete die Mitarbeiter*innen des Bezirks dazu, **2,9 Mio. USD auf ihr Konto zu überweisen**. Zum Glück wurde dies wieder rückgängig gemacht.

Ein Lehrer erhielt eine E-Mail eines **Angreifers, der sich als sein Kollege ausgab** und Geschenkkarten im Wert von 500 Dollar verlangte.

Die Angreifer gaben sich als Schulverwalter aus und schickten E-Mails an die Mitarbeiter*innen der Gehaltsabrechnung und/oder der Personalabteilung, **in denen sie Steuerinformationen der Angestellten anforderten**- einige Schulen fielen dieser Betrugsmasche zum Opfer.



Ein Schüler nutzte Spear-Phishing, indem er ein E-Mail-Konto eingerichtet hat, das sich als hochrangiges Mitglied der Verwaltung ausgab und Anmeldeinformationen von mehreren Lehrkräften anforderte. Der Schüler nutzte diese Informationen, um seine Noten aufzubessern und die der anderen Schüler zu verschlechtern.

Ein gängige Taktik bei diesen Angriffen sind E-Mails, die aussehen, als kämen sie von einer vertrauenswürdigen Quelle. Dabei kann es sich um E-Mails handeln, die von Angreifern mit kaum merklichen Unterschieden in der Schreibweise erstellt wurden, oder um die Kompromittierung von geschäftlichen E-Mails, bei der sich Angreifer Zugang zum eigentlichen E-Mail-Konto verschaffen.

Diese Angriffe richten sich zwar in erster Linie gegen Lehrkräfte und Mitarbeiter*innen, doch auch die Daten von Studierenden sind betroffen. Phishing ist eine gängige Methode, mit der Angreifer Ransomware-Angriffe starten, die zu Datenschutzverletzungen führen, unter denen die Studierenden noch Jahre nach dem Angriff leiden. Angreifer können die Daten eines Schülers oder einer Schülerin nutzen, um Kredite aufzunehmen oder Kreditkarten zu beantragen, um nur zwei Beispiele zu nennen. Diese Studierenden, von denen viele noch sehr jung sind, beantragen erst viele Jahre nach dem Angriff ihre Kreditauskünfte, weil sie es zu dem Zeitpunkt nicht konnten oder nicht wussten, wie das geht.

PHISHING-PRÄVENTION

Es ist nicht so einfach, sich vor Phishing zu schützen. Schulen können zwar alle möglichen Schutzmaßnahmen ergreifen, aber es braucht nur eine Person, die einem Angreifer seine Anmeldeinformationen gibt.

Aber noch ist nicht alle Hoffnung verloren!

Lassen Sie uns ein paar Möglichkeiten besprechen, wie Schulen gegen die allgegenwärtige Bedrohung durch Phishing vorgehen können.

Benutzerschulung

Da Phishing häufig auf Social Engineering beruht, stellen Benutzer*innen, die Phishing-Angriffe erkennen und stoppen können, die erste Verteidigungslinie dar. Denn wenn Benutzer*innen niemals auf Phishing-Links klicken, bösartige Anhänge herunterladen oder den Aufforderungen der Angreifer nachkommen, sind die meisten Phishing-Angriffe nicht erfolgreich!

Tipp

Klären Sie Ihre Studierenden über Phishing-Angriffe auf!

Hier sind einige Themen, die Sie besprechen sollten:

Was Phishing ist

Phishing ist eine Art von Betrug, bei dem Angreifer vorgeben, jemand oder etwas zu sein, das sie nicht sind, um an private Informationen zu gelangen. Die Angreifer können sich als Freund*in, Familienmitglied, Mitarbeiter*in oder Autoritätsperson ausgeben. Oder sie geben sich als Ihre Bank oder ein Unternehmen, bei dem Sie ein Konto haben, wie Google, Apple oder Microsoft, oder eine andere Institution aus, das über Ihre Daten verfügen könnte. Phishing erfolgt in der Regel per E-Mail, kann aber auch über SMS, soziale Medien, Telefonanrufe oder persönlich erfolgen. Die Angreifer kontaktieren Sie vielleicht nicht einmal direkt, sondern **posten etwas in den sozialen Medien** über die Konten Ihrer Freunde.

Was Sie tun sollten, wenn Sie einen Phishing-Versuch vermuten

Wenn Sie eine verdächtige E-Mail erhalten, sollten Sie als Erstes **nichts anklicken**, d. h. keine Links und keine Anhänge. Wenn es sich um eine E-Mail von der Schule handelt, sollten Sie die E-Mail an Ihre IT-Abteilung senden und diese melden. An einigen Schulen gibt es eine Schaltfläche, mit der Sie dies ganz einfach tun können.

Wie Phishing aussieht

Ein Phishing-Angriff kann per E-Mail, Direktnachricht, SMS, Anruf, über eine Website oder persönlich erfolgen. Auch wenn keine zwei Angriffe genau gleich sind, gibt es doch einige Anzeichen, auf die man achten sollte:

- Eine Nachricht oder ein Anruf von jemandem, den Sie kennen, den Sie zu einer seltsamen Tages- oder Nachtzeit erhalten.
- Die Vermittlung eines Gefühls der Dringlichkeit, z. B. eine Zahlungsaufforderung oder dass ein Notfall vorliegt.
- E-Mail- oder Website-Adressen, die vertrauten Adressen **sehr** ähnlich sehen, aber leicht davon abweichen. Diese können Sonderzeichen enthalten oder andere Zeichen ersetzen, z. B. die "0" anstelle des "o". Beachten Sie, dass E-Mails auch völlig legitim sein können, aber dennoch ein Phishing-Angiff sind, wenn das Konto des Absenders von Angreifern gehackt wurde.
- Es ist zu schön, um wahr zu sein: Alles, was Sie tun müssen, ist, ihnen einige Informationen zu geben, und Sie erhalten einen Geschenkgutschein im Wert von 100 Dollar!
- Unerwartete Anfragen, z. B. wenn eine E-Mail, die aussieht, als käme sie von einem Freund, nach Ihrer Adresse, Ihrem Geburtsdatum oder anderen persönlichen Daten fragt.

Content Filter

Leider kann die Aufklärung der Benutzer*innen nur bis zu einem gewissen Grad erfolgen. Menschen machen Fehler, und es bedarf nur eines erfolgreichen Versuchs, damit sich die Angreifer Zugang verschaffen können. Hier kann der Content Filter helfen.

Der Content Filter blockiert im Wesentlichen den Zugang zu bösartigen Websites. Wenn ein Benutzer zum Beispiel auf einen Phishing-Link in einer E-Mail klickt, erkennt ein Content Filter dies und verhindert den Zugriff auf den Link.

Ein Content Filter funktioniert auf verschiedene Weise. Eine Möglichkeit ist eine Zulassungs-/Blockierungsliste, in der IT-Administrator*innen ausdrücklich Websites aus einer Liste zulassen oder blockieren. Das funktioniert, aber die sicherste Implementierung bedeutet eine kurze Zulassungsliste, die einen Großteil des Internets blockiert. Diese Methode hindert die Schülerinnen und Schüler daran, frei zu forschen — schließlich ist dies die Version des Internets, zu der sie nach der Schule Zugang haben werden.

Eine bessere Methode ist der Content Filter mithilfe von künstlicher Intelligenz (KI) und maschinellem Lernen (ML). Anstatt das Internet auf eine Handvoll Websites zu beschränken, können KI und ML auf intelligente Weise feststellen, ob der Zugriff auf eine Website sicher ist, ohne dass ein IT-Administrator sie ausdrücklich zulassen oder sperren muss. Dies ermöglicht nicht nur den Zugang zu einem größeren Teil des Internets, sondern blockiert auch bedrohliche Websites, die noch nicht entdeckt wurden. Diese Methode gibt den Schüler*innen die Freiheit zu forschen — aber mit Vorgaben. **Auf diese Weise lernen die Schülerinnen und Schüler, wie sie sich auch nach dem Verlassen der Schule als sichere digitale Bürger verhalten können.**

Single Sign-On

Mit Single Sign-On (SSO) können sich Benutzer*innen anmelden, ohne sich ein Passwort für alle ihre Internetkonten merken zu müssen. Es kann sogar so eingerichtet werden, dass sich die Benutzer*innen mit ihrem Fingerabdruck anmelden können. Mit anderen Worten: Sie müssen sich nur Ihr SSO-Passwort merken, und Ihr SSO-Anbieter meldet sich für Sie bei den übrigen Konten an.

Dies hilft in mehrfacher Hinsicht, Phishing zu verhindern. SSO funktioniert nur für Websites und Konten, die es gespeichert hat. Wenn Sie auf einen Phishing-Link klicken, erkennt Ihr SSO-Anbieter die Website nicht und überträgt keine Ihrer Daten an die Angreifer. Da SSO die Verwendung eines Fingerabdrucks für die Anmeldung einer Person erforderlich machen kann, fungiert dies als zusätzlicher Authentifizierungsfaktor. Dadurch wird es für Angreifer noch schwieriger, sich Zugang zu Ihrem Konto zu verschaffen.

Geräteverwaltung

Die Geräteverwaltung ist ein notwendiger Bestandteil der Gerätesicherheit in einer Schule. Durch die Registrierung aller Geräte, die auf Schulressourcen zugreifen, in einer Mobile Device Management (MDM)-Lösung erhalten IT-Administrator*innen einen umfassenden Einblick in den Sicherheitsstatus eines Geräts.

Um so etwas wie Content Filter auf einem Gerät zu haben, muss es sich zunächst bei einer MDM-Lösung anmelden. MDM-Software gibt Administrator*innen die Möglichkeit, Geräte zu konfigurieren, z. B. durch Einschränkung bestimmter Einstellungen oder durch Hinzufügen von Software zum Content Filer.

Multi-Faktor-Authentifizierung

Die Multifaktor-Authentifizierung (MFA) ist eine gute Möglichkeit, die Wahrscheinlichkeit eines erfolgreichen Phishing-Angriffs zu verringern. MFA erfordert zwei dieser Authentifizierungsmethoden:

- **Etwas, das Sie kennen,** wie ein Passwort, eine PIN oder eine Sicherheitsfrage
- **Etwas, das Sie sind,** wie Ihr Fingerabdruck oder Ihr Gesicht
- **Etwas, das Sie haben,** wie ein anderes Gerät oder einen Sicherheitsschlüssel

Ein gängiges Beispiel ist die Eingabe Ihres Passworts (das Sie kennen) und der Empfang einer SMS mit einem sechsstelligen Code auf einem vertrauenswürdigen Gerät (das Sie haben).

Hier ist ein Szenario, bei dem die MFA helfen würde:

1. Sie erhalten eine E-Mail, die eine Einladung zu einem freigegebenen Google-Dokument enthält. (Sie merken nicht, dass es eine Phishing-E-Mail ist!)

2. Sie klicken auf den Link, der Sie zu einer Seite führt, die wie die Anmeldeseite von Google aussieht.

3. Sie geben Ihre Daten ein, aber Sie werden nie zu einem Dokument weitergeleitet.

4. Die Angreifer haben jetzt Ihre Daten! Später versuchen sie, sich bei Ihrem Konto anzumelden.

5. Sie erhalten eine MFA-Eingabeaufforderung, die Sie auffordert, die Anmeldeanfrage zu bestätigen.

6. Da die Anfrage von einem fremden Ort oder zu einer Zeit kommt, zu der Sie sich nicht anmelden wollen, lehnen Sie die Anfrage ab.

Die Angreifer können nicht auf Ihr Konto zugreifen.

Dies ist keine hypothetische **Art von Phishing-Betrug** , sondern eine, die immer wieder angewendet wird. In einem kollaborativen Bildungsumfeld können Menschen besonders leicht auf diesen Angriff hereinfallen, da diese Art von E-Mail bekannt ist oder erwartet wird.

IMPLEMENTIERUNG:

JAMF SCHOOL UND JAMF SAFE INTERNET

Wir haben bereits über eine Handvoll Möglichkeiten gesprochen, um sich vor Phishing zu schützen. Lassen Sie uns nun über die Implementierung sprechen.

Jamf School

Apropos Gerätemanagement - **Jamf School** bietet MDM speziell für Schulen an. Das Angebot:

- Gerätebestand, damit die Administrator*innen wissen, welche Geräte mit den Schulressourcen verbunden sind
- Transparenz über den Gerätestatus, damit eventuelle Probleme schnell behoben werden können
- Die Möglichkeit, Einschränkungen und Einstellungen für ein Gerät festzulegen, einschließlich eines erforderlichen Passcodes
- Kompatibilität mit SSO (mit zusätzlichem Identitätsanbieter)
- Eine einfache Möglichkeit für Lehrkräfte, die IT-Genehmigung für Apps anzufordern
- Und noch vieles mehr!

Die Verwaltungsfunktionen von Jamf School schaffen eine solide Grundlage für sichere Geräte, wobei Funktionen wie SSO und Gerätekonfiguration die Auswirkungen eines Phishing-Versuchs verringern.

Jamf Safe Internet

Jamf Safe Internet geht in Sachen Sicherheit noch einen Schritt weiter und ist mit Apple-, Chromebook- und Windows-Geräten kompatibel. Jamf Safe Internet ist vollständig anpassbar, sodass Sie ganz einfach Richtlinien für verschiedene Gerätegruppen auf der Grundlage ihres Standorts, ihres Typs oder anderer Attribute festlegen oder ändern können. Es funktioniert mit Geräten, unabhängig davon, ob sie sich im Warenkorb befinden, von der Schule zugewiesen werden oder ob es sich um ein eigenes Gerät des Schülers handelt.

Um sich gegen Bedrohungen wie Phishing zu schützen, bietet Jamf Safe Internet:

- **Leistungsstarker** , durch KI und ML unterstützter Content Filter: blockiert den Zugriff auf Phishing-Websites, noch bevor diese als bösartig erkannt werden
- **Blockierung von DNS- und Domainnamen** zum Schutz vor DNS-Spoofing
- **On-Device Content Filtering** auf dem iPad für die Filterung an jedem Ort
- **Netzwerkinterner Schutz** vor bösartigen Websites, bevor sie Geräte infizieren können
- **Google SafeSearch** und Google Safe Browsing verpflichtend, um zu verhindern, dass bösartige oder ungeeignete Websites in der Suche angezeigt werden

Die gesamte **Sicherheit ohne Überwachung:** Die Schülerinnen und Schüler können frei im Internet surfen und ihre Fähigkeiten als digitale Bürgerinnen und Bürger entwickeln, ohne dass ihre Privatsphäre verletzt wird.

jamf

Sehen Sie, wie Jamf ein Teil Ihrer Technologie-, Sicherheits- und Content-Filter-Lösung sein kann

Los geht's

www.jamf.com/de/