Cyber Insights von Vodafone Business

3: SOCIAL ENGINEERING
Die vernachlässigte menschliche Komponente von Cyberkriminalität

Finden Sie mehr heraus

Together we can
vodafone
business

Contents

Einleitung

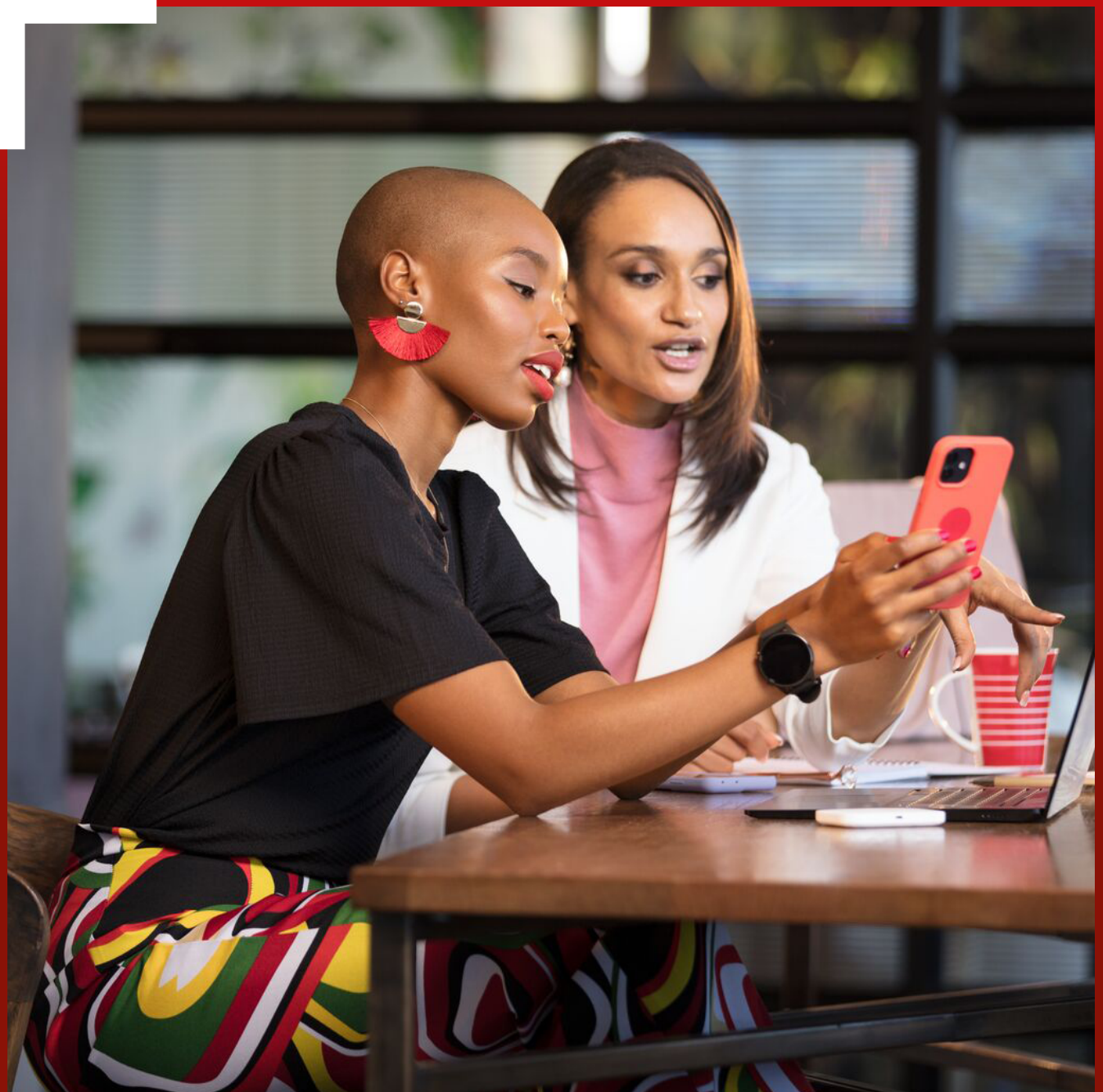
Erster Schwerpunkt:
Wie Social Engineering sich weiterentwickelt

Zweiter Schwerpunkt:
Wie Sie Ihr Unternehmen proaktiv schützen können

Dritter Schwerpunkt:
Wie Cyberkriminelle denken und handeln

Vierter Schwerpunkt:
Wie Vodafone helfen kann

Verweise



Einleitung

Social Engineering: Die vernachlässigte menschliche Komponente von Cyberkriminalität

In der neuesten Ausgabe unseres E-Books mit Hintergründen zu Cyber-Themen befassen wir uns mit Social Engineering, einer Form von Cyberkriminalität, die stark zunimmt.

Beim **Social Engineering** geht es um die zwischenmenschliche Beeinflussung einer Person. Dabei versucht der Hacker das Vertrauen des Opfers zu gewinnen und ihn so zum Beispiel zur Preisgabe von vertraulichen Informationen oder zur Freigabe von Kreditkartendaten und Passwörtern zu bewegen. Social Engineering ist keine neue Methode. Seit Jahrhunderten versuchen Betrüger, ihre Opfer mit Charme und Tricks zur Preisgabe von Geld und Informationen zu bringen. Moderne Angreifer nutzen dieselben Techniken, allerdings online. Anstelle von persönlichen Gesprächen, Briefen und Anrufen erfolgt Social Engineering heute über Websites, E-Mails und soziale Medien.

Es ist das einzige Element eines Cyberangriffs, vor dem Sie keine noch so gute Firewall oder Antivirensoftware vollständig schützen kann. Einige dieser Angriffe sind leicht zu erkennen. Zum Beispiel eine fingierte E-Mail von Amazon, die einen eindeutig verdächtigen Link enthält. Oder eine Website, auf der elektronische Geräte zu Preisen angeboten werden, die zu gut sind, um wahr zu sein. Aber Social Engineering kann auch in sehr ausgeklügelten und schwer zu erkennenden Formen auftreten. Oft werden unsere Gefühle, unsere Ängste oder bestimmte Verhaltensroutinen ausgenutzt, über die wir nicht nachdenken.

In dieser Ausgabe befassen wir uns mit den verschiedenen Arten von Social Engineering und damit, was Sie tun können, um Ihr Unternehmen zu schützen. Diese Themen decken wir ab:

Erster Schwerpunkt: Wie Social Engineering sich weiterentwickelt

Zweiter Schwerpunkt: Wie Sie Ihr Unternehmen proaktiv schützen können

Dritter Schwerpunkt: Wie Cyberkriminelle denken und handeln

Vierter Schwerpunkt: Wie Vodafone helfen kann

Wichtige Kennzahl: KMU werden 350 % häufiger angegriffen als größere Unternehmen[1]

Unternehmen mit mehr als 2.000 Mitarbeitern müssen mit etwa fünf Social-Engineering-Angriffen pro E-Mail-Konto pro Jahr rechnen. Bei Unternehmen mit weniger als 100 Beschäftigten steigt diese Zahl auf beachtliche 17 an.[1]

Warum ist das so? Cyberkriminelle suchen sich immer die einfachsten Ziele. Es ist eher unwahrscheinlich, dass kleine und mittlere Unternehmen über eine unternehmensweite Cybersicherheit verfügen, zudem sind ihre Mitarbeiter seltener für das Thema Social Engineering sensibilisiert. Und wenn ein Angriff erfolgreich ist, haben KMU weitaus seltener hochqualifizierte Cybersicherheitsteams, um den Schaden zu begrenzen. Hier kommt Vodafone ins Spiel. Aber dazu später mehr.

Erster Schwerpunkt

Wie Social Engineering sich weiterentwickelt

Vielleicht glauben Sie, dass nur technisch unerfahrene Menschen auf einen fragwürdigen Link klicken oder auf einen Betrüger hereinfallen. Aber auch geschulte und technisch versierte Geschäftsleute sind schon durch Social Engineering hinters Licht geführt worden. Zu glauben, man selbst wäre für so einen Angriff zu intelligent und abgebrüht, ist Ausdruck von genau dem Gefühl falscher Sicherheit, das Cyberkriminellen in die Hände spielt.

COVID-19 hat einen Social-Engineering-Boom ausgelöst

Unsere Art zu arbeiten hat sich durch die Pandemie verändert. Fast alle Unternehmen setzen heute auf ein bestimmtes Maß an Home-Office. Und dabei nutzen Mitarbeiter oft ihre privaten Smartphones, Laptops, Tablets und Internetverbindungen. Das macht uns viel anfälliger für Social Engineering. Unsere Sicherheitssysteme sind stärker beansprucht, unsere Kommunikation ist unpersönlicher, und unser Arbeitsleben wird häufig mit Privatem vermischt.
Um diese Risiken zu bekämpfen, haben Unternehmen aller Größen ihre Cybersicherheit ausgebaut. Dies macht sie zwar weniger anfällig für rein digitale Angriffe, trägt aber gleichzeitig zur Zunahme von Social Engineering bei. Denn wenn alle ihre Sicherheitsinfrastruktur aufrüsten, werden am Ende die Mitarbeiter eines Unternehmens zum größten Schwachpunkt.

Schnelle Fakten: Zunahme von Social Engineering während der Pandemie

- Einem neuen Bericht über die Zukunft der Arbeit zufolge gaben 80 % der befragten Sicherheitsexperten an, dass sie seit der Umstellung auf Remote-Arbeit mehr Sicherheitsbedrohungen festgestellt haben. 62 % von ihnen gaben an, dass Phishing-Angriffe stärker zugenommen haben als jede andere Art von Bedrohung.[2]
- Als COVID-19 die Welt in den Lockdown versetzte, gab es zwischen dem 4. Quartal 2019 und dem 1. Quartal 2020 einen Anstieg von 87 % beim Phishing auf Mobilgeräten in Unternehmen.[3]
- Die weltweiten Kosten der Cyberkriminalität werden bis 2025 voraussichtlich 10,5 Billionen Euro jährlich erreichen.[4] Wäre die Cyberkriminalität ein Land, hätte es nach den USA und China die drittgrößte Wirtschaft.

Erster Schwerpunkt

Wie Social Engineering sich weiterentwickelt

Social Engineering ist oft nur der Anfang eines Angriffs

Es ist leicht zu verstehen, warum Social Engineering eine beliebte Taktik ist: Es ist wesentlich billiger und einfacher als zu versuchen, fortschrittliche Sicherheitssysteme zu durchdringen. Außerdem können Cyberkriminelle denselben Trick bei beliebig vielen Menschen anwenden.

Oft genügt eine einzige Person, die auf den Trick hereinfällt, um die Sicherheitssysteme eines ganzen Unternehmens zu überwinden. Sobald sie in ein System eingedrungen sind, können Angreifer sensible Daten stehlen oder Schadsoftware auf dem Gerät des Opfers installieren (um nur ein paar Beispiele zu nennen). Oft weiß das Unternehmen nicht einmal, dass es einen sicherheitsrelevanten Vorfall gab.

Schnelle Fakten: Social Engineering in der heutigen Welt

- Phishing-Angriffe sind nach wie vor die Hauptursache für Zwischenfälle bei der Cybersicherheit. Sie machen 40 % aller Fälle aus, die dem ICO im ersten Halbjahr 2021 gemeldet wurden.[5]
- 98 % der Cyberangriffe basieren auf einer Form von Social Engineering.[6]
- Amazon ist mit 17,7 % der Phishing-E-Mails die am häufigsten in E-Mails imitierte Website.[6]
- 43 % der Cyberangriffe richten sich gegen kleine Unternehmen.[7]

Erster Schwerpunkt

Wie Social Engineering sich weiterentwickelt

Diese Angriffsmethoden sollten Sie kennen

Social Engineering kann verschiedene Formen annehmen. Hier sind einige der häufigsten Vorgehensweisen:

Phishing: Die Angriffe finden in der Regel über E-Mail statt. Cyberkriminelle versuchen dabei, in Massenkampagnen so viele Adressaten wie möglich zu erreichen. Das Ziel ist oft, vertrauliche Informationen zu stehlen oder Malware auf einem Gerät zu installieren. Dazu sollen die Opfer verleitet werden, auf einen Link zu klicken oder einen Anhang zu öffnen.

Smishing: Das SMS-Äquivalent zum Phishing, bei dem die Opfer von ihrem Handy aus auf bösartige Websites geleitet werden.

Vishing: Die Angriffe erfolgen per Telefonanruf. Der Anrufer gibt sich als Vertrauensperson aus, oft als Vertreter der Bank des Opfers oder einer Behörde. Der Cyberkriminelle verleitet das Opfer dann dazu, seine privaten Daten preiszugeben.

Spear-Phishing: Eine gezielte Form des Phishings, bei der Cyberkriminelle eine bestimmte Person, Gruppe oder ein Unternehmen ins Visier nehmen. Die Angreifer recherchieren ihr Ziel, damit sie die E-Mail, die SMS oder den Anruf so überzeugend wie möglich auf die jeweilige Person zuschneiden können.

Whaling: Eine noch gezieltere Form des Spear-Phishings. Whaling richtet sich an hochrangige Personen innerhalb einer Organisation, beispielsweise Vorstandsmitglieder. Ziel ist es in der Regel, eine Person dazu zu bringen, Geld zu überweisen oder wichtige Geschäftsdaten preiszugeben.

Business Email Compromise (BEC): Eine weitere Art von Phishing-Angriff. Hier erhält ein Mitarbeiter, der Finanztransaktionen genehmigen kann, eine E-Mail von Cyberkriminellen. Die E-Mail-Adresse das Absenders wurde dabei so manipuliert, dass sie aussieht, als käme sie aus dem eigenen Unternehmen. In der Regel wird in dieser E-Mail um die Überweisung eines Geldbetrags gebeten, oft für die Bezahlung eines Lieferanten oder etwas Vergleichbares.

Schnelle Fakten: Phishing ist die häufigste Bedrohung für KMU

Die Social-Engineering-Angriffe, von denen KMU betroffen sind, fallen in diese Kategorien:[8]

- 49 % sind Phishing-Angriffe
- 40 % sind Betrugsfälle
- 9 % sind Angriffe auf geschäftliche E-Mail-Konten

Zweiter Schwerpunkt

Wie Sie Ihr Unternehmen proaktiv schützen können

Wir sind bereits darauf eingegangen, dass weder Firewalls noch Virenschutzprogramme Sie vollständig vor Social Engineering-Angriffen schützen können. Das heißt aber nicht, dass Sie nichts tun können – ganz im Gegenteil.

Ihr oberstes Ziel sollte der Aufbau einer Kultur der Cyber-Resilienz sein, die von wirklich allen Mitarbeitern gelebt wird. Betrüger haben dann Erfolg, wenn es keine geeigneten Sicherheitsmaßnahmen gibt und Mitarbeiter sich in falscher Sicherheit wiegen, sodass sie bei Gefahr keinen Verdacht schöpfen. So können Sie die Pläne von Angreifern an allen Fronten durchkreuzen:

Sorgen Sie dafür, dass Mitarbeiter wachsam sind

Social Engineering funktioniert am besten bei Menschen, die es nicht erwarten. Ihre Mitarbeiter müssen also die Bedrohung genau verstehen und immer einen klaren Kopf bewahren.

Schulen Sie alle Ihre Mitarbeiter zum Thema Cybersicherheit

Im Jahr 2021 führte CybSafe eine Umfrage unter 2.000 Personen durch, um ihre Gewohnheiten bei der Cybersicherheit zu ermitteln.[9] Bei einer Frage zu Schulungen stellten sie fest, dass

- 64 % der Teilnehmer angaben, keinen Zugang zu Schulungen zur Cybersicherheit haben;
- 10 % angaben, dass sie Zugang haben, ihn aber nicht nutzen;
- also **nur 26 % der Teilnehmer zum Thema Cybersicherheit geschult wurden.** Das ist eine erschreckend niedrige Zahl.

Für einen erfolgreichen Angriff reicht es aus, dass nur ein einziger Mitarbeiter auf den Betrug hereinfällt. Daher sollten Sie sicherstellen, dass alle Mitarbeiter gut geschult sind und aktuelle Bedrohungen verstehen. Sie sollten Mitarbeitern erklären, warum Cyberangriffe ein großes Risiko für Ihr Unternehmen darstellen.

Social Engineering kann für jeden zum Problem werden, unabhängig von der Position innerhalb des Unternehmens. Schulungen zur Cybersicherheit sind also für alle Mitarbeiter relevant. Sie sollten mehrmals im Jahr ein Trainingsprogramm durchführen, das regelmäßige Updates zu neuen Entwicklungen einschließt, um alle über aktuelle Gefahren auf dem Laufenden zu halten.

Stellen Sie sicher, dass Ihre Mitarbeiter wissen, wie raffiniert und gezielt Phishing sein kann

Sehen Sie sich diese beiden (fiktiven) E-Mail-Absender an:

1. Alasdair Cox [AlasdairCox@KingConsultants.com]
2. Alasdair Cox [AlasdairCox@KingConsuitants.com]

Stellen Sie sich vor, dass Alasdair Cox Ihr Chef ist und Sie es gewohnt sind, von seinem echten E-Mail-Konto (dem ersten) E-Mails zu erhalten, in denen es um Geld geht. Würde Ihnen etwas auffallen, wenn Sie eine E-Mail von dem gefälschten Konto (dem zweiten) bekämen, in der Sie aufgefordert werden, Geld zu überweisen?

So minimal können die Unterschiede sein. Betrüger können neue E-Mail-Adressen und Webadressen registrieren, die denjenigen sehr ähnlich sind, die sie imitieren wollen. Sie verkürzen auch URLs, um lange, komplexe Webseitenadressen in kurze Adressen umzuwandeln, die viel seriöser aussehen.

Um einem falschen Sicherheitsgefühl vorzubeugen, müssen Mitarbeiter im Detail verstehen, dass sie sehr wachsam sein müssen.

Zweiter Schwerpunkt

Wie Sie Ihr Unternehmen proaktiv schützen können

Führen Sie Phishing-Simulationen durch

Sie müssen wissen, wie effektiv Ihr Training ist, und Phishing-Simulationen sind eine gute Möglichkeit, es herauszufinden. Dazu senden Sie fingierte (aber sichere) E-Mails an Ihre Mitarbeiter, die bösartigen Phishing-E-Mails ähneln. Und dann sehen Sie, wie viele darauf hereinfallen. Die Ergebnisse geben Ihnen einen guten Anhaltspunkt dafür, wie sehr sie für das Thema sensibilisiert sind. Achten Sie aber darauf, dass Sie niemanden bestrafen. Wenn jemand den Test nicht besteht, sollten Sie versuchen zu verstehen, warum die Person bestimmte Anhaltspunkte nicht erkannt hat. Bieten Sie in diesen Fällen Hilfe an, damit es beim nächsten Mal besser gelingt.

Achten Sie darauf, dass Mitarbeiter nicht zu viel auf Social-Media-Websites wie LinkedIn preisgeben

Plattformen wie LinkedIn können eine nützliche Informationsquelle für Cyberkriminelle sein. Hier können Angreifer sich ein Bild von einer Person machen und ihre Social-Engineering-Aktionen auf sie abstimmen. Erklären Sie Mitarbeitern, dass sie sich nur mit Personen vernetzen sollten, die sie kennen. Außerdem sollten Sie nicht davon ausgehen, dass alle Profile seriös sind. Achten Sie auch darauf, dass Mitarbeiter keine sensiblen Geschäftsinformationen online stellen. Das passiert erstaunlich schnell: Oft ist es etwas Einfaches, wie Text in einem Notizbuch oder auf einem Bildschirm im Hintergrund eines Fotos.

Schnelle Fakten: Cyberkriminelle setzen in hohem Maße auf Phishing

- Jeden Monat werden 1,5 Millionen neue Phishing-Websites erstellt.[10]
- Bei fast einem Drittel aller Cyberangriffe ist Phishing das Mittel der Wahl.[11]

Zweiter Schwerpunkt

Wie Sie Ihr Unternehmen proaktiv schützen können

Machen Sie sich bewusst, worauf Sie achten müssen

Fast alle Social-Engineering-Angriffe setzen darauf, dass die Zielperson bestimmte Warnzeichen nicht erkennt oder einfach annimmt, dass eine Person auch wirklich die ist, die sie vorgibt zu sein. Wenn man also weiß, worauf man achten muss, und die Identität der Personen überprüft, ist man viel sicherer.

Seien Sie immer vorsichtig mit Links und Anhängen

Klicken Sie nicht auf Links in E-Mails, SMS oder Direktnachrichten von Absendern, die Sie nicht kennen. Klicken Sie nicht auf Links in Nachrichten von Organisationen, die Sie dazu auffordern, sich über den Link in Ihrem Konto anzumelden – auch wenn Sie der Organisation eigentlich vertrauen. Rufen Sie stattdessen selber die Website der Organisation auf. Selbst wenn Sie sicher sind, dass die Nachricht wirklich von Amazon, Ihrer Bank oder Ihrem Energieversorger stammt: Es ist immer besser, die E-Mail zu schließen und sich stattdessen über die Website des Unternehmens einzuloggen. Auf diese Weise können Sie sicher sein, dass es sich um die richtige Website handelt.

Schnelle Fakten:

- Im Jahr 2021 verloren Unternehmen weltweit durch Internetkriminalität schätzungsweise 1.797.945 Euro pro Minute.[12]
- Phishing ist die zweitteuerste Ursache für Datenschutzverletzungen. Eine durch Phishing verursachte Datenschutzverletzung kostet Unternehmen durchschnittlich 4,65 Millionen Euro.[13]
- Business Email Compromise (BEC) steht dabei an erster Stelle und kostet Unternehmen durchschnittlich 5 Millionen Euro pro Vorfall.[14]

Gewöhnen Sie sich an, Personen zu überprüfen, die Sie direkt kontaktieren

Jeder kann eine falsche Identität vorgeben. Seriöse Unternehmen wissen das und sollten daher nichts dagegen haben, wenn Sie sie um eine Verifizierung bitten. Wenn Sie eine seltsame Nachricht von einem Kollegen oder einem Bekannten erhalten, antworten Sie über einen anderen Kanal. So können Sie sichergehen, dass es sich wirklich um die Person handelt. Wenn ein Cyberkrimineller Zugang zur Mailbox des Absenders hat, ist es sinnlos, per E-Mail zu antworten – Sie würden nur den Betrüger erreichen. Stattdessen ist es am besten, zum Telefon zu greifen und die Person kurz anzurufen, um die Nachricht zu bestätigen.

Sie können einen Anrufer anhand von Informationen verifizieren, die nur diese Person kennt. Am besten ist es jedoch, wenn Sie sie unter einer sicheren Nummer zurückrufen. Wenn ein Anrufer angibt, Mitarbeiter eines seriösen Unternehmens zu sein, sollten Sie versuchen, seine Identität direkt bei dem Unternehmen zu überprüfen.

Vertrauen Sie auf Ihr Bauchgefühl: Oft stimmt tatsächlich etwas nicht, wenn Sie ein ungutes Gefühl haben

Wenn Sie aus heiterem Himmel ungewöhnliche Anfragen erhalten, sollten Sie sich einen Moment Zeit nehmen, um über die Situation nachzudenken und sie zu hinterfragen. Besonders dann, wenn Ihnen etwas merkwürdig vorkommt. Nehmen Sie dieses Beispiel: Im Jahr 2016 verlor die belgische Bank Crelan über 57 Millionen Euro durch einen Betrugsfall mittels Business Email Compromise.[15] Der Angreifer fälschte das E-Mail-Konto des CEO und forderte Mitarbeiter per E-Mail auf, Geld auf ein bestimmtes Konto zu überweisen. Ein gut geschulter und aufmerksamer Mitarbeiter hätte sich sicherlich gefragt: „Würde mich der CEO wirklich in einer E-Mail um eine Überweisung bitten?“.

Zweiter Schwerpunkt

Wie Sie Ihr Unternehmen proaktiv schützen können

Sorgen Sie für die richtigen Kontrollen

Die meisten Unternehmen verfügen über eine hochentwickelte Cybersicherheit. Doch oft sind es die kleinen, einfachen Sicherheitsmaßnahmen, die am meisten bewirken. Alle in Ihrem Unternehmen müssen diese Maßnahmen kennen und entsprechend handeln. Sie machen Ihr Unternehmen nicht nur schwerer angreifbar, sondern begrenzen auch den Schaden, wenn ein Angreifer doch einmal erfolgreich sein sollte.

Verwenden Sie verschiedene Passwörter

Es ist ein großes Risiko, dasselbe Passwort für mehrere Konten zu verwenden. Wenn es einem Angreifer gelingt, das Passwort für eines Ihrer Konten herauszufinden, probiert er es in der Regel auch bei anderen Accounts aus. Deshalb ist es wichtig, für jedes Konto ein anderes Passwort zu verwenden und die Passwörter regelmäßig zu ändern. Diese Passwörter sollten so komplex sein, dass sie schwer zu knacken sind. Anstelle von Wörtern, einprägsamen Daten und Namen sollten sie aus drei zufälligen Wörtern zusammengesetzt sein. Wenn sie dadurch schwer zu merken sind, sind Sie auf dem richtigen Weg. Verwenden Sie einen Passwort-Manager, um den Überblick über Ihre Anmeldedaten zu behalten. Auf diese Weise müssen Sie sich nicht alles merken.

Verwenden Sie Zwei-Faktor-Authentifizierung

Dadurch haben Sie nach der Eingabe Ihres Passworts eine zweite Kontrollinstanz bei der Kontoanmeldung. Es ist eine der einfachsten und effektivsten Methoden, um zu verhindern, dass sich fremden Person bei Ihren Konten anmelden. Selbst wenn ein Angreifer Ihren Benutzernamen und Ihr Kennwort kennt, kann er sich dank der Zwei-Faktor-Authentifizierung nicht anmelden, wenn die Anmeldung nicht per SMS, E-Mail, In-App-Aufforderungen, mit biometrischen Daten oder über einen USB-Stick bestätigt wird.

Schnelle Fakten: E-Mail ist der Hauptangriffspunkt, aber nicht der einzige

Für Social-Engineering-Angriffe über verschiedene Kanäle haben IT-Profis für das Jahr 2022 folgende prozentualen Zunahmen festgestellt:[16]

- Anrufe auf Videokonferenzplattformen (44 %)
- Über Mitarbeiterplattformen versandte Nachrichten (40 %)
- Über Cloud-basierte Plattformen freigegebene Dateien (40 %)
- Mobile Textnachrichten (36 %)

Halten Sie Ihre Antiviren- und Antimalware-Software auf dem neuesten Stand

Wenn Sie Antiviren- und Antimalware-Software regelmäßig aktualisieren, haben Sie immer die neuesten Signaturen – also aktuelle Informationen, mit denen die Antiviren-Software die neuesten Arten von Schadsoftware erkennen und bekämpfen kann. Sie sollten darauf achten, dass automatische Aktualisierungen aktiviert sind (diese Einstellung ist meistens leicht zu finden) und jeden Tag überprüfen, ob sie vollständig heruntergeladen wurden.

Aktualisieren Sie regelmäßig Ihre Software

Softwareentwickler überprüfen ihre Produkte ständig auf Sicherheitslücken. Wenn sie eine Schwachstelle finden, veröffentlichen sie in der Regel ein sogenanntes Patch, also ein Update, um Fehler zu beseitigen. Die meisten Geräte und Anwendungen installieren Updates automatisch. Es empfiehlt sich aber, die Updates im Auge zu behalten, falls sie aus irgendeinem Grund doch nicht automatisch installiert werden. Ihr Team sollte Aktualisierungen immer herunterladen, sobald es die Benachrichtigung erhält, dass welche verfügbar sind.

Dritter Schwerpunkt

Wie Cyberkriminelle denken und handeln

Cyberkriminelle setzen darauf, dass Sie sie unterschätzen. Sie wollen, dass man sie für einsame Wölfe hält – soziale Außenseiter, die einsam an einem Computer in einem heruntergekommenen Keller arbeiten. Und sie wollen, dass Sie ihre Methoden für leicht durchschaubar halten und glauben, dass nur naive oder technisch unbedarfte Menschen auf sie hereinfallen. Dies sind einige Aspekte, die Sie über die Denk- und Handlungsweise von Cyberkriminellen wissen sollten. Tun Sie ihnen nicht den Gefallen, sie zu unterschätzen.

Cyberkriminelle sind – genau wie Sie – Profis, die weltweit agieren

Einige sind Subunternehmer. Andere sind bei größeren Organisationen beschäftigt. Andere wiederum stehen auf der Gehaltsliste von Staaten, die für Cyberangriffe verantwortlich sind.

Sie verfügen über Marktplätze und Foren im Darknet. Sie analysieren ihre Einnahmeströme, Gewinne und Verluste genau. Es ist zwar ein illegaler Wirtschaftszweig, aber er funktioniert wie jeder andere Wirtschaftszweig auch. Wir haben dieses Thema eingehend in einer Ausgabe 1 unserer Reihe „Business Cyber Insights“ behandelt.

Ein Beispiel: Selbst Tech-Giganten können getäuscht werden

Zwischen 2013 und 2015 wurden sowohl Google als auch Facebook Opfer eines Rechnungsbetrugs, der sie am Ende 50 Millionen Euro kostete. Beide Unternehmen nutzten Produkte eines taiwanesischen Anbieters namens Quanta Computer. Ein Hacker gab sich als Quanta aus, schickte den beiden Unternehmen gefälschte Rechnungen und brachte sie zur Überweisung hoher Geldbeträge.[17]

Dritter Schwerpunkt

Wie Cyberkriminelle denken und handeln

Cyberkriminelle sind immer auf dem neuesten Stand der Technik

Cyberkriminelle sind technisch versiert und nutzen die neuesten Innovationen, sobald sie verfügbar sind, lange bevor die Technologie auf den Markt kommt. Das bedeutet, dass Betrüger Tools einsetzen, von denen Sie noch nie gehört haben und die Sie nicht kennen.

Deepfakes haben sich zum Beispiel sehr schnell weiterentwickelt. Dabei handelt es sich um gefälschte Videos, die digitalen Effekten in Filmen ähneln. Der Ersteller kann das Gesicht einer beliebigen Person in beliebiges Filmmaterial einbauen. Video und Ton sind inzwischen so realistisch, dass es fast unmöglich ist, zwischen einem Deepfake und einem echten Video zu unterscheiden.

Ein Beispiel: Audio Deepfakes können selbst die misstrauischsten Menschen überlisten

2019 erhielt der Vorstandsvorsitzende eines britischen Energieunternehmens einen Anruf. Den Anrufer hielt er für den Vorstandsvorsitzenden der Muttergesellschaft des Unternehmens. Er überwies wie angewiesen 243.000 Euro auf ein Bankkonto, von dem er annahm, es gehöre einem ungarischen Lieferanten. Es stellte sich heraus, dass der Anruf von einem Betrüger stammte, der mit Hilfe von künstlicher Intelligenz die Stimme des Chefs mit großer Genauigkeit nachahmte.[18] Da es sich um den Vorstandsvorsitzenden eines Energieunternehmens handelte, ist es sehr unwahrscheinlich, dass das Opfer technisch unbedarft oder unbeholfen war. Vermutlich wusste er schlicht nicht, dass es eine Technologie gibt, die die Stimme einer bestimmten Person so überzeugend nachahmen kann.

Cyberkriminelle wissen, wie sie uns mit sozialen und psychologischen Tricks manipulieren können

Auch wenn wir alle verschieden sind, reagieren wir in der Regel ähnlich auf Emotionen und soziale Signale. Betrüger wissen, dass sie das ausnutzen können, um unser Verhalten zu steuern. Das sind die häufigsten Tricks:

- **Angst:** Betrüger versuchen Opfer zur überzeugen, dass etwas Schreckliches passieren wird. Sie bauen darauf, dass wir überstürzt und mit weniger Vorsicht handeln, wenn uns eine Lösung angeboten wird.
- **Autorität:** Wenn wir glauben, dass eine Anfrage von jemandem in einer einflussreichen Position kommt, neigen wir dazu, sie weit weniger zu hinterfragen als sonst.
- **Gewöhnung:** Zuerst bitten Betrüger ihre Opfer um eine Kleinigkeit, die nicht verdächtig erscheint. Dann bitten sie um eine weitere Kleinigkeit und noch eine, bis wir uns daran gewöhnt haben, ihnen zu geben, was sie wollen.
- **Konsens:** Opfer sind weniger zögerlich, wenn man ihnen einredet, dass alle anderen das tun, worum es geht.
- **Knappheit:** Wenn etwas sehr gefragt und knapp ist, sind wir oft weniger vorsichtig, wenn wir es haben wollen.
- **Gegenseitigkeit:** Wenn jemand etwas Nettes für uns tut, fühlen wir uns verpflichtet, den Gefallen zu erwidern, wenn wir darum gebeten werden.
- **Zuneigung:** Betrüger, die erfolgreich eine Beziehung zu uns aufbauen und uns sympathisch sind, können auch unser Vertrauen gewinnen.

Vierter Schwerpunkt

Wie Vodafone helfen kann

Unsere Netze verbinden Millionen von Menschen, Haushalten und Unternehmen. Die Gewährleistung Ihrer Sicherheit auf höchstem Niveau ist ein zentraler Bestandteil unserer Unternehmensziele.

Cybersicherheit auf höchstem Niveau erschwinglicher machen

Der Aufbau von Resilienz gegen Cyber-Attacken kostet Geld. Dazu brauchen Sie eine Infrastruktur auf dem neuesten Stand und Fachkenntnisse, die bis vor kurzem nur für die größten globalen Konzerne bezahlbar waren.

Da wir mit einigen der besten Cybersicherheitspartnern zusammenarbeiten – Accenture, Lookout, und Microsoft – können wir Unternehmen jeder Größe einen erschwinglichen Zugang zu marktführendem Know-how im Bereich Cybersicherheit anbieten. Wir helfen Ihnen, Ihre wichtigsten Ressourcen zu schützen: Ihre Mitarbeiter, Standorte, Objekte und Daten. So können Sie sich darauf konzentrieren, Ihr Unternehmen voranzubringen.

Um mehr zu erfahren, sprechen Sie mit Ihrem Kundenbetreuer oder besuchen Sie Vodafone Security: IT-Sicherheitslösungen für Unternehmen

Aufbau von Resilienz gegen Cyber-Attacken

Wir bieten Cybersicherheitsdienste, damit Ihr Unternehmen vor Bedrohungen wie Social Engineering geschützt ist.

Machen Sie Ihre Mitarbeiter weniger anfällig für Social Engineering. Wir helfen Ihnen, die menschlichen Elemente von Cyberangriffen mit Schulungen zum Sicherheitsbewusstsein, Bewertungen der Sicherheitskultur und bedarfsorientierter Beratung zu verstehen und sich vor Ihnen zu schützen.

Sorgen Sie dafür, dass Mitarbeiter wachsam sind und verfolgen Sie ihre Fortschritte. Unsere vertrauenswürdigen Partner versenden harmlose E-Mails, die typische Phishing-Angriffe imitieren sollen. So können Sie nachvollziehen, wie resilient Ihre Mitarbeiter sind und wer zusätzliche Schulungen benötigt.

Finden Sie Ihre Cybersicherheits-Schwachstellen und beheben Sie sie. Wir können eine vollständige Prüfung Ihrer Sicherheitsmaßnahmen durchführen und genau aufzeigen, wie hoch (oder niedrig) Ihr Risiko ist. Wir betrachten nicht nur Ihre IT-Systeme, sondern auch das Verhalten und die Kultur der Mitarbeiter. Wenn wir Schwachstellen finden, zeigen wir Ihnen genau, was Sie dagegen tun können.

Sorgen Sie für die richtigen Kontroll- und Schutzmaßnahmen. Profitieren Sie von einer Software-Suite, die alles enthält, was Sie für den Schutz Ihrer PCs, Macs, Server und von mobilen Geräten brauchen.

Holen Sie sich den bestmöglichen Schutz für Ihre mobilen Geräte. [Lookout Mobile Security] Unser Online-Dashboard bietet Ihnen einen vollständigen Überblick über alle potenziellen Bedrohungen für mobile Geräte. Es zeigt alle Phishing-, Malware- und Hacking-Versuche an, außerdem alltägliche Sicherheitsprobleme, wie veraltete Software und unsichere Geräteeinstellungen.

Suchen Sie Rat bei Experten für Cybersicherheit, wenn Sie ihn brauchen. [BR&FS] Wenn der schlimmste Fall eintritt und ein Angriff Ihre Schutzmaßnahmen überwindet, helfen wir Ihnen, schnell zu reagieren und den Schaden zu minimieren. Unsere Teams für digitale Forensik und Incident Response stehen telefonisch bereit, um Ihr Unternehmen zu schützen.

Verweise

1. SMBs Are 350% More Likely to Experience Social Engineering Attacks Via Phishing | Knowbe4
2. The new future of work: research from Microsoft into the pandemic's impact on work practices | Microsoft
3. COVID-19 emergence leads to 37% jump in mobile phishing attacks in 2020 | TechRepublic
4. Cybercrime to cost the world $10.5 trillion annually by 2025 | Cybercrime Magazine
5. ICO data analysis: human error to blame for 8 in 10 data breaches in 2021 | Financial IT
6. 21 social engineering statistics – 2022 | Firewall Times
7. 9th annual cost of cybercrime report | Accenture
8. Micro-businesses are underestimating social engineering | Hutsix
9. The annual cyber security attitudes and behaviours report 2021 | CybSafe
10. 2022 Cyber Security Statistics: The ultimate list of stats, data & trends | PurpleSec
11. What is phishing, and how do I prevent attacks? | Verizon
12. Cybercrime costs organizations nearly $1.79 million per minute | Infosecurity Magazine
13. Cost of a data breach 2022 | IBM
14. Consumers pay the price as data breach costs reach all-time high | IBM
15. Belgian bank Crelan loses €70 million to BEC scammers | Help Net Security
16. Cloud phishing: new tricks and the crown jewel | HackerNoon
17. Facebook and Google were victims of $100M payment scam | Fortune
18. A voice deepfake was used to scam a CEO out of $243,000 | Fortune

Together we can

vodafone business