Der komplette Leitfaden für Security Awareness Training

Inhalt

Einführung

Wie sich gezielte Angriffe auf Menschen im Jahr 2021 weiterentwickeln werden

Die Covid-19-Pandemie hat viele Sicherheitsherausforderungen mit sich gebracht. Unternehmen auf der ganzen Welt haben sich darauf eingestellt, von zu Hause aus zu arbeiten und sich sozial zu distanzieren, während sie sich gleichzeitig mit neuen Bedrohungen durch Cyberkriminelle auseinandersetzen, die Angst und Neugierde ausnutzen. Auch wenn sich die Unternehmen mit diesen Herausforderungen auseinandersetzen, sind die traditionellen Cyber-Bedrohungen so verbreitet wie eh und je und sorgen für eine zunehmend schwierige Bedrohungslandschaft.

Unter den großen Cyber-Bedrohungen bleibt Malware eine erhebliche Gefahr. Der WannaCry-Ausbruch von 2017, der Unternehmen weltweit bis zu 4 Milliarden US-Dollar gekostet hat, ist noch in aktueller Erinnerung, und täglich werden weitere neue Malware-Stämme entdeckt.

Auch das Phishing hat in den letzten Jahren einen Aufschwung erlebt, wobei viele neue Betrugsmaschen erfunden wurden, um ahnungslose Unternehmen auszunutzen. Allein eine Variante, der CEO-Fraud-E-Mail-Betrug, kostete britische Unternehmen im Jahr 2018 14,8 Mio. £.

Mitarbeiter, die von zu Hause aus arbeiten, befinden sich außerhalb der direkten Aufsicht von IT-Support-Teams und haben oft Schwierigkeiten, mit Cyber-Bedrohungen umzugehen und Unternehmensdaten angemessen zu schützen.

Das Versäumnis, Software und Betriebssysteme zu aktualisieren, das Versenden von Daten über unsichere Netzwerke und die zunehmende Abhängigkeit von E-Mails und Online-Nachrichten haben die Mitarbeiter viel anfälliger für Bedrohungen gemacht, die von Malware bis zu Phishing reichen.

Technische Lösungen wie Spam-Filter und Mobile-Device-Management-Systeme sind zwar wichtig für den Schutz von Endanwendern, aber angesichts der Anzahl von Bedrohungen und der Vielzahl von Systemen und Kommunikationswegen, über die Mitarbeiter ihre Arbeit verrichten, ist der eine verbindende Risikofaktor, der angegangen werden muss, um die Sicherheit grundlegend zu verbessern, die Rolle menschlichen Versagens.

Warum menschliches Versagen die Sicherheitsbedrohung Nr. 1 für Ihr Unternehmen ist

Fast alle erfolgreichen Cyberangriffe haben eine Variable gemeinsam: menschliches Versagen. Menschliches Versagen kann sich auf vielfältige Weise manifestieren: von der nicht rechtzeitigen Installation von Software-Sicherheitsupdates über schwache Passwörter bis hin zur Preisgabe sensibler Informationen an Phishing-E-Mails.

Auch wenn moderne Anti-Malware und Software zur Erkennung von Bedrohungen immer ausgefeilter geworden sind, wissen Cyber-Kriminelle, dass die Wirksamkeit technischer Sicherheitsmaßnahmen nur so weit geht, wie sie von Menschen richtig genutzt werden.

Wenn es einem Cyber-Kriminellen gelingt, das Passwort für ein Online-Firmenportal zu erraten oder einen Mitarbeiter durch Social Engineering dazu zu bringen, eine Zahlung auf ein vom Cyber-Kriminellen kontrolliertes Bankkonto vorzunehmen, können technische Lösungen dieses Eindringen nicht verhindern.

Im Jahr 2014 führte IBM eine Studie zu den Cyberverletzungen durch, die bei Tausenden ihrer Kunden in über 130 Ländern auftraten. Diese Studie war der umfassendste Blick auf die Ursachen von Cyberverletzungen, der zu diesem Zeitpunkt durchgeführt wurde, aber ihre Ergebnisse wurden seitdem durch ähnliche Studien bestätigt.

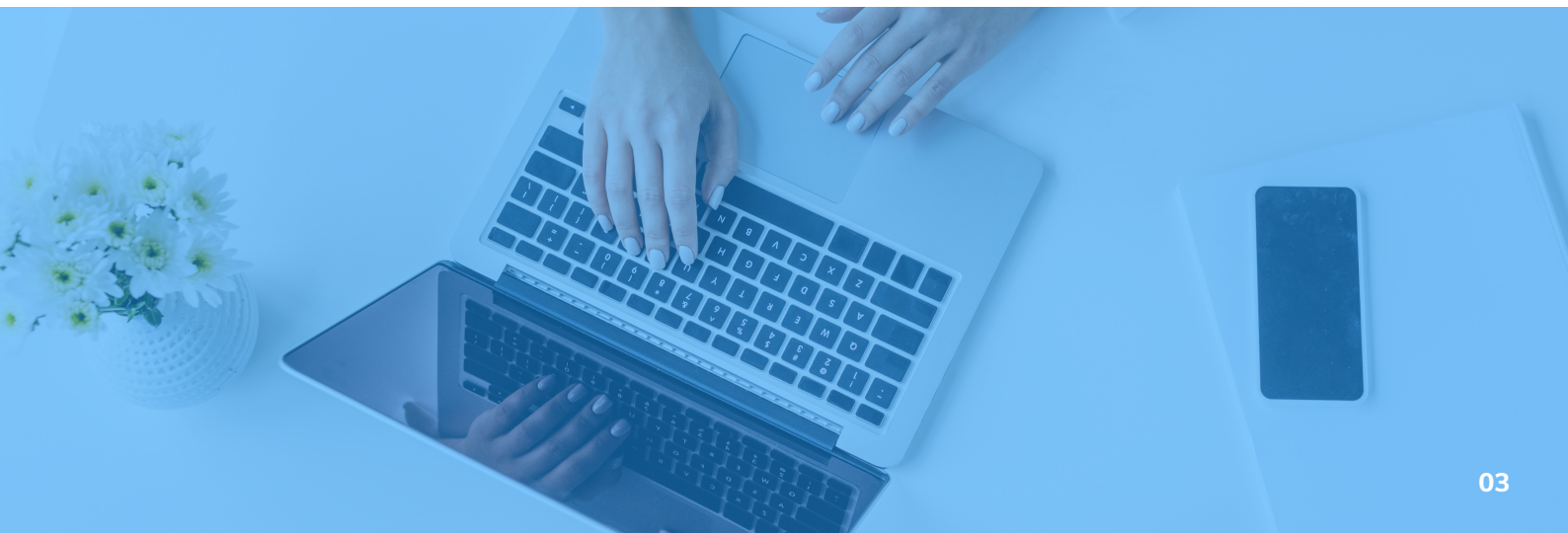
Eine der wichtigsten Erkenntnisse der IBM-Studie war, dass menschliches Versagen bei 95 % aller Sicherheitsverletzungen eine Hauptursache war.

Mit anderen Worten: Hätte menschliches Versagen keine Rolle gespielt, wären 19 der 20 in der Studie analysierten Sicherheitsverletzungen wahrscheinlich gar nicht erst passiert.

"Menschliches Versagen war ein Faktor, der zu 95 % aller Verstöße beitrug"

Da menschliches Versagen bei Cyberangriffen eine so große Rolle spielt, ist die Behebung dieses Problems der Schlüssel zur Verringerung der Wahrscheinlichkeit, dass Ihr Unternehmen erfolgreich angegriffen wird. Darüber hinaus können Sie Ihr Unternehmen vor einer weitaus größeren Bandbreite an Bedrohungen schützen, als dies mit einer einzelnen technischen Lösung möglich wäre - und Sie können Ihre Mitarbeiter dazu befähigen, aktiv nach neuen Bedrohungen Ausschau zu halten und diese zu melden.

Die Abschwächung menschlicher Fehler muss der Schlüssel für die Cybersicherheit von Unternehmen im Jahr 2021 sein - und im nächsten Abschnitt schauen wir uns an, wie man das am besten anstellt.



Wann liegt ein menschlicher Fehler vor?

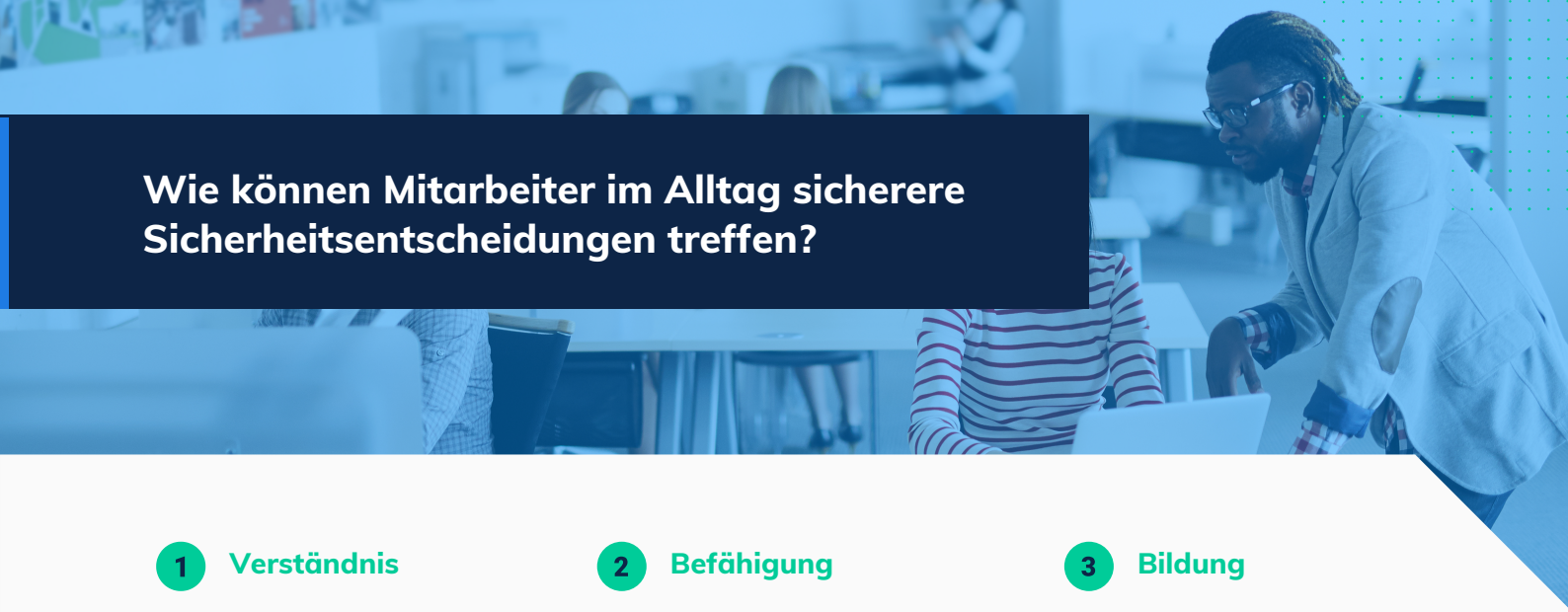
Damit sich menschliches Versagen manifestieren kann, müssen zwei Faktoren vorhanden sein: Gelegenheit und Entscheidung. Gelegenheit bedeutet, dass es eine Situation gibt, in der ein Mensch einen Fehler machen darf: z. B. die Überlassung von Software-Updates an Endbenutzer, anstatt Sicherheitsupdates mit Patch-Management durchzusetzen. Entscheidung ist die Handlung des Menschen: in diesem Fall die Untätigkeit bei der Installation von Sicherheitsupdates, wenn diese verfügbar sind.

Zu einer umfassenden Risikominderung gehört sowohl die Reduzierung der Fehleranfälligkeit als auch die Verbesserung der Entscheidungen der Endbenutzer. Es ist wichtig, in beiden Bereichen Maßnahmen zu ergreifen, um sicherzustellen, dass menschliches Versagen gründlich angegangen wird.

Beim Patching beispielsweise kann eine technische Maßnahme wie die Einführung eines Patch-Managements die Möglichkeit für menschliche Fehler in den meisten Fällen auf ein Minimum reduzieren - dennoch ist es wichtig, Situationen zu berücksichtigen, in denen die technischen Lösungen vorübergehend außer Kraft gesetzt sind oder wenn eine neue Situation wie eine BYOD-Richtlinie eingeführt wird, bei der die Benutzer ihre eigenen Geräte ohne Patch-Management verwenden dürfen.

In anderen Fällen, wie z. B. bei Phishing-E-Mails, haben technische Maßnahmen wie Spam-Filter und Software zur Erkennung von Sicherheitsverletzungen nur eine sehr begrenzte Wirkung, wenn es darum geht, die Möglichkeit von Fehlern bei einem gezielten Angriff zu reduzieren. In diesen Fällen besteht die einzige wirksame Möglichkeit, menschliches Versagen zu verringern, darin, den Endbenutzern beizubringen, wie sie bessere Entscheidungen treffen können.

"Zwei Faktoren müssen vorhanden sein, damit sich menschliches Versagen manifestieren kann: Gelegenheit und Entscheidung"



Wie können Mitarbeiter im Alltag sicherere Sicherheitsentscheidungen treffen?

1 Verständnis

Der Benutzer muss erkennen, dass er sich in einer Situation befindet, in der die Sicherheit potenziell auf dem Spiel steht. Ohne dies zu erkennen, merkt der Benutzer möglicherweise gar nicht, dass er durch seine Untätigkeit überhaupt eine Entscheidung trifft.

2 Befähigung

Der Benutzer muss wissen, was die richtige Vorgehensweise ist. Dies erfordert nicht unbedingt, dass er die Bedrohung vollständig versteht, sondern oft reicht es aus, die Situation einer Person in der IT- oder Sicherheitsabteilung zu melden, die sich darum kümmern kann.

3 Bildung

Der Benutzer muss wissen, warum Sicherheit wichtig ist, damit er versteht, wie wichtig es ist, Sicherheitsverfahren nicht zu ignorieren, und sich der möglichen Folgen eines Verstoßes bewusst ist.

4 Schmerzvermeidung beseitigen

Probleme wie schwache Passwortsicherheit und das Versäumnis, Software zu patchen, bestehen in Unternehmen auf der ganzen Welt, obwohl viele Computeranwender verstehen, warum diese Probleme für die Sicherheit kritisch sind. Der Grund dafür, dass trotz dieses Wissens keine Maßnahmen ergriffen werden, ist das, was wir als Schmerzvermeidung bezeichnen. Ein einzigartiges und starkes Passwort erfordert mehr Zeit, um es zu erstellen, und mehr Aufwand, um es sich zu merken, als ein kurzes, schwaches oder wiederverwendetes Passwort.

Obwohl ein Benutzer es besser weiß, ist dieser "Schmerz", der durch die Erstellung eines starken Passworts verursacht wird, oft stark genug, um den Benutzer gegen sein bestes Urteilsvermögen handeln zu lassen. Hinzu kommt, dass viele Benutzer zwar unter optimalen Umständen richtig handeln, aber geschäftige und dringende Arbeitssituationen sowie Stress können dazu führen, dass sich Sicherheitsmaßnahmen für Benutzer noch "schmerzhafter" anfühlen.

Endbenutzer müssen das Gefühl haben, dass der Schmerz, der durch die Befolgung von Best Practices im Bereich Sicherheit entsteht, geringer ist als die Befriedigung, die durch die Nichtbefolgung entsteht. Technische Maßnahmen wie Passwort-Manager sind dabei essenziell, da sie sicheres Handeln deutlich erleichtern: Wenn Mitarbeiter ihre eigenen Passwörter nicht erstellen oder sich merken müssen, haben sie keinen Grund, keine sicheren zu verwenden.

Gleichzeitig muss die Schwelle für die Durchführung der richtigen Aktion durch einen kulturellen Wandel gesenkt werden. Das bedeutet, die Sicherheit in den Vordergrund der Entscheidungsfindung zu stellen und sicherzustellen dass Benutzer nie das Gefühl haben, "Zeit zu verschwenden", wenn sie entsprechende Sicherheitsvorkehrungen treffen.

Ein effektives Security Awareness Training adressiert nicht nur einen, sondern alle vier dieser Faktoren. Das bedeutet, Situationen zu identifizieren, in denen Daten oder Systeme kompromittiert werden könnten, Best Practices zu verstehen, zu wissen, was die potenziellen Folgen von Verstößen sind, und schließlich dabei zu helfen, einen Kulturwandel durchzusetzen, um eine Umgebung zu schaffen, in der Sicherheitsüberlegungen immer in die Entscheidungsfindung einfließen.

Sicherheitsbewusstsein zu Hause

Sicherheit für Mitarbeiter, die von zu Hause aus arbeiten

Die weltweite Reaktion auf die Covid-19-Pandemie hat viele Veränderungen an den Arbeitsplätzen verursacht. Die Veränderung, die sich am stärksten auf die Sicherheit ausgewirkt hat, war die Umstellung vieler Unternehmen darauf, dass die meisten oder alle Mitarbeiter innerhalb kurzer Zeit auf Heimarbeit umgestellt haben, was dazu geführt hat, dass viele Endbenutzer einem höheren Risiko ausgesetzt sind, Online-Bedrohungen zu erliegen.

Mitarbeiter, die es vor der Pandemie nicht gewohnt waren, von zu Hause aus zu arbeiten, entdeckten schnell einige der Probleme, die dies mit sich bringen würde: sich um Kinder und Haustiere kümmern zu müssen, mit schlechter Internetverbindung zurechtzukommen und all die anderen Störungen zu ertragen, die zu Hause auftreten können. Inmitten all dieser neuen Veränderungen in der Arbeitsumgebung stand die Sicherheit zu oft ganz unten auf der Prioritätenliste der Anwender.

Endbenutzer, die von zu Hause aus arbeiten, sind der Aufsicht der IT-Supportabteilung entzogen und haben möglicherweise mit einfachen technischen Problemen zu kämpfen. Darüber hinaus wurden wichtige Sicherheitsaufgaben wie die Aktualisierung von Software und Betriebssystemen, die Aktualisierung der Router-Firmware und die Sicherung des Netzwerks plötzlich in die Hände der Endbenutzer gelegt.

Es ist kein Wunder, dass Cyberkriminelle keine Sekunde damit verschwendet haben, die Umstände der Pandemie auszunutzen, um neue Formen von Betrug und Cyberkriminalität zu entwickeln.

Inmitten all dieser neuen Veränderungen in der Arbeitsumgebung stand die Sicherheit zu oft ganz unten auf der Prioritätenliste der Anwender.

Wie man die Sicherheit anspricht, wenn Endbenutzer zu Hause sind

Das IT Support-Team kann nicht bei jedem Endbenutzer zu Hause sein. Deshalb muss sichergestellt werden, dass die Endbenutzer nicht nur die richtigen Geräte haben, sondern sich auch ihrer individuellen Verantwortung bei der Aufrechterhaltung der Sicherheit bewusst sind. Endbenutzer müssen wissen, dass sie dafür verantwortlich sind, dass sie nur mit Geräten und Netzwerken auf Unternehmensinformationen und -netzwerke zugreifen, die aktuell und sicher sind.

Schulungen zum Sicherheitsbewusstsein sind der Schlüssel, um sicherzustellen, dass die Endbenutzer wissen, wie sie die Sicherheit aufrechterhalten können. Es ist am besten, das Training in kleine, verdauliche Komponenten aufzuteilen, da dies sicherstellt, dass die Benutzer nicht überfordert werden. Das Training sollte auch regelmäßig stattfinden - mindestens einmal im Monat - um sicherzustellen, dass das Gelernte behalten wird und dass die Benutzer die Sicherheit nicht vergessen, sobald das nächste Arbeitsprojekt die Prioritätenliste durcheinander bringt. Und schließlich ist es wichtig, die Endbenutzer zu testen.

Es sollte klargestellt werden, dass dies nicht dazu dient, Anwender zu beurteilen oder zu bestrafen, die mit ihrer Ausbildung Schwierigkeiten haben, sondern vielmehr dazu, wichtige Sicherheitslücken in der gesamten Belegschaft zu identifizieren und diese zu beheben, bevor sie von Cyber-Kriminellen ausgenutzt werden können.

"Sicherheitsbewusstse instraining ist der Schlüssel, um sicherzustellen, dass die Endbenutzer wissen, wie sie die Sicherheit aufrechterhalten können"

Old-School VS Modernes Training

Wie man das beste Format für Sicherheitsschulungen auswählt

Sicherheitsschulungen sind nicht alle gleich. Die Art und Weise, wie das Training durchgeführt, strukturiert und präsentiert wird, hat einen großen Einfluss auf die Effektivität bei der tatsächlichen Verbesserung der Sicherheitsergebnisse in Ihrem Unternehmen. In diesem Abschnitt werfen wir einen Blick darauf, was genau der beste Weg ist, um eine Sicherheitsschulung für Ihre Endbenutzer durchzuführen.

Früher bedeutete Sicherheitsschulung, dass die Endbenutzer einmal im Jahr an einer Sitzung teilnehmen mussten, die aus stundenlangen Vorträgen und Diashows bestand. Die Idee war, dass sich die Benutzer an das Gesehene und Gehörte erinnern würden - und im schlimmsten Fall konnte zumindest das Kästchen "Schulung der Benutzer" abgehakt werden. Aber wie weit hat es die Sicherheit tatsächlich verbessert? Es hat nicht funktioniert, und jeder hat es gehasst.

Warum das jährliche "Tick-Box"-Training kläglich scheitert

Es gibt eine Reihe von Gründen, warum diese Art der jährlichen Vortragsschulung nicht effektiv ist.

Die erste davon ist, dass in einer jährlichen Trainingseinheit werden einfach zu viele Informationen auf einmal vorhanden sein, als dass ein Mitarbeiter sie verdauen und sich merken könnte.

Selbst wenn den Anwendern Lernmaterial mit auf den Weg gegeben wird oder sie gelegentlich daran erinnert werden, ist die Wahrscheinlichkeit groß, dass der meiste Stoff der Schulung durch ein Ohr hinein und durch das andere wieder hinaus geht - und in wenigen Augenblicken vergessen ist.

Vorträge und Diashows sind einfach keine ansprechenden Formate für Endbenutzer zum Lernen. Sie schaffen es nicht, das Interesse der Mitarbeiter auf die gleiche Weise zu wecken wie Videos und interaktive Inhalte, und sind zu oft mit unnötigen Informationen gefüllt, die nicht für jeden Endbenutzer relevant sind.

Folien, die bis zum Rand mit kleinem Text gefüllt sind, lassen jeden Mitarbeiter nach der Hälfte der Sitzung einschlafen.

Der letzte und wichtigste Grund, warum traditionelle Schulungen nicht effektiv sind, ist, dass sie das Lernen durch Wiederholung nicht nutzen. Wenn zwischen den Lerneinheiten ein Jahr liegt, erinnern sich die Anwender einfach nicht an das Gelernte - und das Bewusstsein für Sicherheitsthemen im Allgemeinen sinkt in den Tagen und Wochen nach der Schulung. Sicherheit kann nicht eine einmalige Sache sein, sondern muss das ganze Jahr über stattfinden, um effektiv zu sein.

Sicherheitsschulungen haben sich zunehmend auf Online-Software-as-a-Service-Lösungen verlagert. Cloud-basiertes Training bietet einige unmittelbare Vorteile gegenüber traditionellen Methoden, ist aber nicht unbedingt die ultimative Antwort auf Sicherheitsbewusstsein, es sei denn, es liefert in bestimmten Bereichen, die für eine wirkliche Verbesserung der Sicherheitsergebnisse wesentlich sind.

Wie man modernes Training wirklich effektiv macht

Material aufteilen

Es gibt eine begrenzte Menge an Informationen, die ein Mensch auf einmal aufnehmen kann. Um den Endbenutzer nicht zu überfordern, sollte die Schulung in Segmente unterteilt werden, die jeweils eine klare, einfache und leicht verdauliche Botschaft enthalten.

Kontinuierliches Lernen

Die Aufteilung des Lernmaterials ermöglicht es außerdem, das Lernen kontinuierlich zu gestalten, anstatt es als einmalige Sache zu betrachten, und ermöglicht es, die Kurse regelmäßig über das ganze Jahr hinweg zu verschicken - was dazu beiträgt, das Sicherheitsbewusstsein der Endbenutzer konstant im Auge zu behalten und das Behalten des Gelernten zu verbessern.

Relevantes Material

Wenn ein Endbenutzer Informationen erhält, die für ihn nicht relevant sind, wird er schnell das Interesse verlieren und weniger Aufmerksamkeit aufbringen. Das Lernmaterial muss nicht nur Jargon und Fachbegriffe vermeiden, sondern auch mit Blick auf reale Situationen erstellt werden, denen der Endbenutzer begegnen könnte.

Verankern Sie Sicherheit in Ihrer Kultur

Schulungen müssen Teil einer Unternehmenskultur sein, in der der Sicherheit stets die nötige Beachtung geschenkt wird und Benutzer werden ermutigt, Anliegen vorzubringen und Fragen zu stellen.

Praktische Hinweise

Es ist wichtig, dass die Mitarbeiter das Training mit konkreten Schritten im Kopf verlassen, die sie sofort in ihrer täglichen Arbeit anwenden können. Den Mitarbeitern die Möglichkeit zu geben, das Gelernte sofort zu testen, hilft auch dabei, das Gedächtnis aufzubauen - und kann mit Tools wie einer Phishing-Simulation erreicht werden.

Video und interaktive Inhalte

Videos und interaktive Inhalte eignen sich hervorragend, um Benutzer anzusprechen, die vielleicht eine andere Art von Lernerfahrung bevorzugen. Viele Menschen lernen, indem sie etwas tun, Fragen beantworten oder sich anderweitig beteiligen.

Messung der Auswirkungen

Es ist wichtig, dass die Benutzer nach den Trainingseinheiten getestet werden, was sie gelernt haben. Dies hilft Ihnen zu wissen, dass die Benutzer weggehen und etwas gelernt haben - aber es hilft auch dem Lernprozess der Benutzer, da sie die gerade gelernten Informationen aus ihrem eigenen Gedächtnis wieder abrufen können.

Aufbau einer sicherheitsbewussten Kultur

Wie man Sicherheit in die tägliche Mitarbeiterkultur einbettet

Schulungen zum Sicherheitsbewusstsein werden die Sicherheitsergebnisse nicht effektiv verbessern, wenn sie nicht von einem kulturellen Wandel begleitet werden. Umfassende Schulungen bringen den Endanwendern bei, wie sie Situationen erkennen können, in denen die Sicherheit gefährdet ist, und wie sie angemessen damit umgehen können - aber dieses Wissen wird nicht in die Praxis umgesetzt, wenn der Anwender nicht das Gefühl hat, dass Sicherheit in seiner Kultur einen hohen Stellenwert hat.

Angesichts der wachsenden Anzahl an Bedrohungen sowie der zunehmenden Komplexität von Geschäftsdiensten und des Zugriffs auf Daten und Systeme über mobile Geräte ist es unmöglich zu wissen, wo die nächste Bedrohung oder das nächste versehentliche Leck für Ihr Unternehmen auftauchen könnte.

Aus diesem Grund sollte es bei der Sicherheit nicht darum gehen, sicherzustellen, dass Ihre Endbenutzer starke Passwörter wählen oder andere spezifische Schritte befolgen - sondern vielmehr darum, sie zu befähigen, aktive Hüter Ihres Unternehmens, seiner Systeme, Geräte und Daten zu sein.

"Schulungen zum Sicherheitsbewusstsein werden die Sicherheitsergebnisse nicht effektiv verbessern, wenn sie nicht von einem kulturellen Wandel begleitet werden."

Wie man eine sicherheitsbewusste Kultur aufbaut

Unterstützung auf C-Level erhalten

Der kulturelle Wandel und die Werte des Unternehmens müssen von oben kommen. Die Geschäftsleitung spielt eine wichtige Rolle, wenn es darum geht, die Rolle der Sicherheit im Unternehmen zu betonen - aber es ist wichtig, dass sie die neue Kultur wachsen lässt, anstatt sie zu diktieren.

Das bedeutet, dass die Mitarbeiter ermutigt werden, eine aktive Rolle zu übernehmen, indem sie aufgefordert werden, Bedenken in Bezug auf ihre eigenen Rollen vorzubringen, und sie dazu veranlasst werden, Fragen zu stellen und sich mit Sicherheitsfragen zu beschäftigen. Auf diese Weise haben die Benutzer das Gefühl, in den Sicherheitsprozess eingebunden zu sein, und beginnen, aktiv über die Sicherheitsüberlegungen in ihren eigenen Rollen nachzudenken.

Zugriff mit geringsten Rechten

Während das Prinzip der geringsten Rechte oft als technische Maßnahme gesehen wird - die Beschränkung jedes Benutzers auf nur die Rechte, die er für seine spezifischen Aufgaben benötigt - sollte es auch direkt in die Unternehmenskultur eingebettet werden.

Das bedeutet, dass Benutzer dazu angehalten werden, aktiv zu melden, wenn sie Zugriff auf mehr Daten oder Systeme haben, als sie benötigen - was dazu beiträgt, die Möglichkeiten von Verstößen zu begrenzen.

Physische Sicherheit

In Bezug auf physische Maßnahmen können Gegenstände wie Poster hilfreich sein, um eine Sicherheitskultur aufzubauen, und auch hilfreiche Erinnerungen zu Themen wie der Passwortstärke enthalten.

Wesentliche Schulungsthemen für 2021

Was sind die wesentlichen Schulungsthemen für 2021?

Auch wenn jedes Unternehmen und jede Arbeitsstelle andere Anforderungen stellt, gibt es doch einige wesentliche Bereiche, die es wert sind, dass jeder einzelne Endbenutzer sie kennt.

Top-Themen für 2021:

1. Phishing-Techniken
2. Social Engineering
3. Sicherheit zu Hause
4. Sichere Internet- und E-Mail-Nutzung
5. Aus der Ferne arbeiten
6. Sicherheit für mobile Geräte
7. Passwort & Authentifizierung
8. Cloud-Sicherheit
9. Öffentliches Wi-Fi
10. Physische Sicherheit
11. Austauschbare MedienSecure
12. Nutzung sozialer Medien

#1. Phishing-Techniken

Phishing bleibt eine große Bedrohung. Einer der Gründe, warum Phishing bei Cyber-Kriminellen so beliebt ist, ist, dass es leicht angepasst werden kann, um jedes Ereignis oder jeden Umstand - wie z. B. die Covid-19-Pandemie - zu nutzen, um Benutzer mit neuen Betrügereien anzusprechen. Schablonenbasierte Betrügereien, die den Opfern Informationen anbieten, sind beliebter denn je - während Spear-Phishing-Angriffe, die auf einzelne Benutzer und Unternehmen abzielen, die gefährlichste Art bleiben.

Endbenutzer sind am empfänglichsten für Phishing-E-Mails, die ein Gefühl der Dringlichkeit vermitteln oder dem Benutzer etwas Wertvolles anbieten. Es ist wichtig, Endbenutzer darin zu schulen, dass sie zweimal überprüfen, ob sie dem Absender einer E-Mail vertrauen können, bevor sie auf Links klicken oder Informationen preisgeben. Auch wenn es für Benutzer unmöglich ist, jede Phishing-E-Mail abzufangen, sorgt das Sicherheitsbewusstsein in Kombination mit Spam-Filtern dafür, dass die potenzielle Reichweite von Phishing-E-Mails auf ein Minimum beschränkt wird.

#2. Social Engineering

Phishing ist nur eine von vielen Arten von Social-Engineering-Angriffen. Auch physische und telefonbasierte Social-Engineering-Angriffe werden von Kriminellen genutzt, um sich Zugang zu sicheren Räumlichkeiten und sensiblen Daten zu verschaffen.

Es ist wichtig, dass die Mitarbeiter über die verschiedenen Arten von Social-Engineering-Angriffen geschult sind - von denen über das Telefon bis hin zu persönlichen Bedrohungen - und wissen, wie sie mit jedem potenziellen Täter richtig umgehen.

#3. Sicherheit zu Hause

Das Arbeiten von zu Hause aus wurde im Jahr 2020 in den Vordergrund der Endbenutzersicherheit gerückt, da Unternehmen auf der ganzen Welt ihre Mitarbeiter dazu ermutigten, auf Remote-Arbeit umzusteigen. Die Geschwindigkeit dieser Umstellung bedeutete, dass viele Benutzer nicht mit den Tools und dem Wissen ausgestattet waren, um ihre Arbeit sicher ausführen zu können.

Es ist wichtig, alle Mitarbeiter, die von zu Hause aus arbeiten, zu schulen, wie sie sicherstellen können, dass die Daten und das Netzwerk des Unternehmens nicht durch Fernzugriff gefährdet werden. Die Aktualisierung von Software, der Schutz von WLAN-Netzwerken und die Verwendung von Sicherheitstools wie VPNs, um einen sicheren Zugriff zu gewährleisten, sind zu einem wesentlichen Bestandteil der Endbenutzerschulung geworden.

#4. Sichere Internet- und E-Mail-Nutzung

Im Jahr 2021 ist es ein seltener Mitarbeiter, der das Internet oder E-Mail bei der Arbeit nicht nutzt. Während die Pandemie dazu geführt hat, dass Unternehmen mehr denn je auf das Internet angewiesen sind, birgt die Nutzung des Internets auch Sicherheitsrisiken. Benutzer könnten versehentlich Malware installieren, Daten auslaufen lassen, Zugangsdaten für Phishing-E-Mails preisgeben oder auf einen der vielen anderen Angriffe hereinfallen, mit denen Cyberkriminelle es auf sie abgesehen haben.

In Schulungen sollten auch praktische Hinweise gegeben werden, wie z. B. die Information der Benutzer über den Unterschied zwischen cc- und bcc-Feldern und die Bedeutung des HTTPS-Verschlüsselungssymbols auf Websites.

#5. Aus der Ferne arbeiten

Im Jahr 2021 wird Remote-Arbeit beliebter denn je sein. Während die Pandemie der Heimarbeit in vielen Unternehmen eine Starthilfe gegeben hat, wird sie wahrscheinlich auch nach der Pandemie weitergehen. Die Mitarbeiter haben sich daran gewöhnt, von zu Hause aus zu arbeiten, und die Unternehmen erkennen die Vorteile.

Das Arbeiten aus der Ferne birgt auch Risiken. Laptops, Mobiltelefone, Tablets und andere Geräte können eine ernsthafte Sicherheitsbedrohung darstellen, wenn sie verloren gehen oder gestohlen werden. Wenn Mitarbeiter Unternehmensdaten auf ihren mobilen Geräten speichern oder darauf zugreifen, werden diese Daten alle angreifbar, wenn ein Gerät in die falschen Hände gerät. Bei der Schulung von Anwendern über sicheres Remote-Working sollte der Fokus darauf liegen, den Anwendern zu helfen, Punkte zu identifizieren, an denen Systeme oder Daten kompromittiert werden könnten - und die Schritte, die sie unternehmen können, um diese Risiken zu minimieren.

#6. Sicherheit für mobile Geräte

Die Nutzung mobiler Geräte in Unternehmen hat schnell zugenommen, und im Jahr 2021 wird dieser Trend voraussichtlich noch weiter verbreitet sein als bisher. Mobile Geräte wie Laptops, Mobiltelefone und Tablets ermöglichen es den Mitarbeitern, von zu Hause, in Cafés, auf Reisen oder an jedem beliebigen Ort zu arbeiten, was sowohl ihnen selbst als auch dem Unternehmen Flexibilität bietet. So praktisch mobile Geräte auch sind, sie bergen auch Risiken, über die die Benutzer aufgeklärt werden müssen.

#7. Passwörter & Authentifizierung

Passwörter bereiten Unternehmen, Mitarbeitern und Kunden nach wie vor große Kopfschmerzen. Menschen sind einfach nicht darauf ausgelegt, sich lange, komplexe Phrasen zu merken - schon gar nicht Dutzende von ihnen. Das bedeutet, dass Mitarbeiter ständig versucht sind, den einfachen Weg zu gehen und sie sich leicht zu merken - vor allem, wenn sie den Zugang zu Apps und Diensten mit ihren Kollegen teilen müssen.

Die meisten Endbenutzer wissen, warum Passwortsicherheit wichtig ist, und haben eine Vorstellung davon, was ein sicheres Passwort ausmacht. Der Fokus bei Schulungen rund um Passwörter und Authentifizierung sollte auf praktikablen Ratschlägen liegen, wie man die Passwortsicherheit aufrechterhalten kann, ohne den Endanwendern das Leben schwer zu machen. Das bedeutet, dass Sie die Verwendung von Passwortmanagern fördern (wenn Ihr Unternehmen dies zulässt), Mitarbeiter auffordern, die Zwei-Faktor-Authentifizierung für alle Dienste und Systeme mit Zugriff auf sensible Daten zu aktivieren, und Mitarbeitern beibringen, wie man ein Passwort erstellt, das sowohl angemessen komplex als auch leicht zu merken ist.

#8. Cloud-Sicherheit

In den letzten Jahren haben sich Geschäftsdienste und -daten zunehmend in die Cloud verlagert. Im Jahr 2021 erreicht dieser Trend seinen Höhepunkt. Viele Geschäftsvorgänge werden dann vollständig über webbasierte Tools und Dienste abgewickelt. Während die Cloud Unternehmen eine große Flexibilität bietet, ist es wichtig, dass die Benutzer wissen, wie sie diese sicher nutzen und darauf zugreifen können.

Starke Passwörter und Authentifizierung sowie E-Mail-Sicherheit werden besonders wichtig, wenn Ihr Unternehmen Cloud-Dienste nutzt.

Ein bösartiger Akteur, der die Passwörter eines Mitarbeiters errät, könnte von überall auf der Welt auf Ihre sensiblen Daten zugreifen. Deshalb ist es wichtig, dass die Mitarbeiter überdie notwendigen Maßnahmen zur Sicherung von Cloud-Accounts geschult werden. Die Multi-Faktor-Authentifizierung ist besonders für alle Dienste und Apps, die sensible Geschäftsdaten enthalten, ein Muss.

#9. Öffentliches Wi-Fi

Da Benutzer zunehmend von unterwegs arbeiten, ist es wahrscheinlich, dass sie sich mit Geschäftsdiensten, Netzwerken oder Daten von öffentlichen WLAN-Zugangspunkten aus verbinden. Öffentliches WLAN ist für die mobile Arbeit sehr praktisch, birgt aber auch Sicherheitsrisiken.

Es ist wichtig, den Endbenutzern beizubringen, dass ihre Daten in öffentlichen Wi-Fi-Netzwerken potenziell abgefangen werden können. Wenn Sie Ihren Endbenutzern erlauben, über öffentliche WLAN-Netzwerke auf Unternehmensdaten oder -dienste zuzugreifen, sollten Sie sie mit Software für virtuelle private Netzwerke ausstatten und sie darin schulen, diese auf sichere Weise zu nutzen.

#10. Physische Sicherheit

Auch wenn die Bedrohungen für die Cybersicherheit zunehmen, darf die physische Sicherheit nicht außer Acht gelassen werden. Es nützt nichts, Daten mit starken Passwörtern und Multi-Faktor-Authentifizierung zu schützen, wenn eine unbefugte Person einfach ins Büro gehen und eine Papierkopie eines sensiblen Dokuments direkt aus dem Druckerschacht nehmen kann.

Bei der Schulung von Endbenutzern im Bereich der physischen Sicherheit ist es wichtig, dass der Schwerpunkt auf die Identifizierung und Abschwächung von Bedrohungen gelegt wird, die für die täglichen Aktivitäten der einzelnen Endbenutzer relevant sind. Wenn Ihr Unternehmen in einem Büro angesiedelt ist, wird jeder Mitarbeiter durch die Bürotür gehen - daher ist Tailgating ein Beispiel für eine Sicherheitsbedrohung, die für alle Mitarbeiter relevant ist. Endbenutzer sollten darin geschult werden, aktiv darüber nachzudenken, welche Bereiche und Dokumente sicher sind, und dafür zu sorgen, dass sie immer sicher verschlossen sind oder einen Account haben, wenn sie nicht benutzt werden.

#11. Austauschbare Medien

Auch wenn File-Sharing und Online-Collaboration-Dienste im Internet immer beliebter werden, sind Wechselmedien in Unternehmen immer noch weit verbreitet. So nützlich Wechseldatenträger auch sind, sie bergen viele Risiken: Sie können leicht verloren gehen oder gestohlen werden, was zu einer Kompromittierung von Daten führen kann, oder sie können durch Geräte mit Malware ersetzt werden. Ein weit verbreiteter Betrug besteht darin, ein mit einem Virus infiziertes USB-Laufwerk auf dem Parkplatz eines Büros liegen zu lassen, das darauf wartet, von einem ahnungslosen Mitarbeiter abgeholt und in den Firmencomputer eingesteckt zu werden. Darüber hinaus ist vielen Anwendern nicht bewusst, dass nicht nur Speichergeräte ein Risiko darstellen können: Auch einfache USB- oder Ladekabel könnten von einem Cyberkriminellen modifiziert werden, um Malware zu enthalten.

Die Aufklärung der Endbenutzer über die sichere Verwendung von Wechseldatenträgern läuft auf die Verantwortlichkeit hinaus. Den Anwendern sollte klar gemacht werden, dass sie die Verantwortung für die Geräte übernehmen müssen, die sich unter ihrer Kontrolle befinden - und dass sie keine unkontrollierten Geräte an irgendeinen Computer anschließen, sondern diese dem IT-Team oder dem Sicherheitspersonal melden sollten.

#12. Sichere Nutzung sozialer Medien

Mitarbeiter - und Unternehmen - verbringen einen immer größeren Teil ihres Tages in sozialen Medien. Es muss jedoch sichergestellt werden, dass die Sicherheit des Unternehmens nicht durch eine unvorsichtige Nutzung von sozialen Netzwerken gefährdet wird.

Der Schwerpunkt der Social-Media-Schulungen sollte darauf liegen, den Benutzern bewusst zu machen, dass das, was sie teilen, für jeden im Internet verfügbar sein könnte - und dass selbst kleine Details aus dem Büro für Angreifer entscheidend sein könnten. Zum Beispiel könnte ein unschuldiges Selfie aus dem Büro ein Whiteboard im Hintergrund mit sensiblen Geschäftsinformationen oder sogar Kundendaten zeigen.