E-BOOK

Mehr als nur Cybersicherheits-Schulungen

Der Aufbau einer nachhaltigen Sicherheitskultur – und warum sie wichtig ist

proofpoint.

Einführung

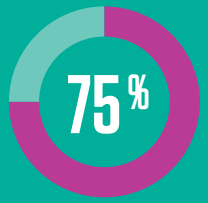
Mittlerweile wissen die meisten Verantwortlichen für Cybersicherheit, dass die größte Angriffsfläche ihres Unternehmens die Mitarbeiter sind. Remote- und Hybrid-Arbeitsplätze in Verbindung mit dem Wechsel zur Cloud machen die Bewältigung dieser Herausforderung noch schwieriger.

Laut dem „Verizon Data Breach Investigations Report 2021 (DBIR)“ ist an 85 % der Datenschutzverletzungen der Faktor Mensch beteiligt, wobei diese entweder durch Klicks auf schädliche Links in Phishing-E-Mails oder durch die Weitergabe von Anmeldedaten an Dritte ausgelöst werden.[1]

Laut einer aktuellen Proofpoint-Umfrage sind 75 % der CISOs in den USA und 58 % der CISOs weltweit der Meinung, dass menschliche Fehler ihre größte Sicherheitsschwachstelle darstellen.[2] Heute kann jeder zum Ziel eines Angriffs werden und die Sicherheit des Unternehmens gefährden.

Mit bester Absicht bieten viele Unternehmen ihren Anwendern jährlich ein oder zwei Stunden Schulungen zur Steigerung des Sicherheitsbewusstseins an. Dies ist jedoch zu wenig, um nachhaltige Verhaltensänderungen bewirken zu können. Zudem fördert es kein Sicherheitsdenken, mit dem die größte Angriffsfläche in eine wirksame Verteidigungslinie umgewandelt wird.

1 CISOMAG: „Verizon 2021 Data Breach Investigations Report: Cyberattacks Continue to Rise During Pandemic“ (Untersuchungsbericht zu Datenkompromittierungen: Cyberangriffe steigen während Pandemie weiter), Mai 2021.
2 Proofpoint: „Voice of the CISO 2021“, Mai 2021.



der Unternehmen weltweit verzeichneten 2020 einen Phishing-Angriff, gleichzeitig verliefen 74 % der Angriffe auf US-Unternehmen erfolgreich.[4]

verzeichneten Spearphishing-Angriffe. Gezielte BEC-Angriffe (Business Email Compromise) sind die zweithäufigste Social-Engineering-Form. Das Aufkommen von BEC-Angriffen war 2021 15 Mal höher als im Jahr davor.[5]

2,1 Mio.

1,6 Mio.

Google registrierte bis zum 17.01.2021 insgesamt 2.145.013 Phishing-Websites – 27 % mehr im Vergleich zu den am 19.01.2020 registrierten 1.690.000.[6]

Rund 95 % der Unternehmen sagen, dass sie ihren Anwendern Schulungen zur Sensibilisierung für Phishing bieten. Gleichzeitig geben 30 % an, dass sie nur einen Teil ihrer Anwender schulen.[3] Es verwundert daher nicht, dass Phishing-Betrug nach wie vor die Bedrohungsart ist, die am ehesten zu einer Datenschutzverletzung führt.

Was können wir besser machen? Die Antwort liegt im Aufbau einer systematischen, nachhaltigen und individuellen Sicherheitskultur, die sich durch das gesamte Unternehmen und alle digitalen Aktivitäten zieht.

Dazu sind gezielte Investitionen von Zeit, Energie und Ressourcen sowie unternehmensweite Unterstützung nötig. Das Ergebnis jedoch ist unbezahlbar, da eine robuste Sicherheitskultur die Sicherheit Ihres Unternehmens, die Einhaltung von Vorschriften und das Geschäftsergebnis verbessern kann. Richtig umgesetzt lässt sich damit sogar die Motivation und Produktivität der Mitarbeiter steigern.

3 Proofpoint: „State of the Phish 2021“, Januar 2021.
4 ebd.
5 Verizon: „2021 Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen 2021), Juli 2021.
6 Chuck Brooks (Forbes): „Alarming Cybersecurity Stats: What You Need to Know for 2021“ (Alarmierende Zahl zur Cybersicherheit: Das sollten Sie 2021 wissen), März 2021.

ABSCHNITT 1

Definieren einer Sicherheitskultur

Wir bei Proofpoint orientieren uns an der von den Forschern Keman Huang und Keri Pearlson (von der MIT Sloan School of Management) aufgestellten Definition einer unternehmensgerechten Cybersicherheitskultur. Ihnen zufolge besteht eine Sicherheitskultur aus „den Überzeugungen, Werten und Einstellungen, die die Anwender dazu bewegen, das Unternehmen vor Cyberangriffen zu schützen“.[7]

Mit anderen Worten: Alle Ihre Mitarbeiter sind beim Schutz der Daten, Systeme und Ressourcen des Unternehmens aktive Akteure.

7 Keman Huang and Keri Pearlson (MIT): „For What Technology Can’t Fix: Building a Model of Organizational Cybersecurity Culture“ (Technologie kann nicht alles beheben: Aufbau eines Modells einer Cybersicherheitskultur für Unternehmen), Januar 2019.

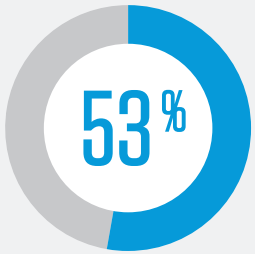
Für den Aufbau einer Sicherheitskultur sind Lösungen erforderlich, die bei den Mitarbeitern ein Umdenken beim Thema Sicherheit auslösen. Diese Sicherheitskultur sollte in die Unternehmenskultur eingebettet sein. Sie muss inspirieren – und zwar nachhaltig.

Faktoren einer Kultur

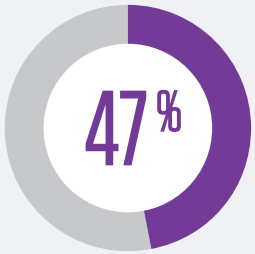
Eine Cybersicherheitskultur besteht aus drei sich überschneidenden Faktoren:

- **Die Verantwortung für die Cybersicherheit.** Die Mitarbeiter fühlen sich gemeinsam verantwortlich dafür, so zu handeln, dass Sicherheitszwischenfälle vermieden werden.
- **Das Wissen, warum Cybersicherheit wichtig ist.** Die Mitarbeiter sind davon überzeugt, dass Cyberbedrohungen ein erhebliches Risiko für den Erfolg des Unternehmens sind und persönliche Folgen für sie haben könnten.
- **Die Fähigkeit zu handeln.** Die Mitarbeiter fühlen sich durch ihr Cybersicherheitswissen gestärkt, verstehen die Sicherheitsrichtlinien und vertrauen darauf, dass das Unternehmen sie unterstützt, wenn sie unabsichtlich einen Fehler begehen.

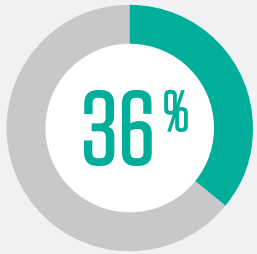
2021:



Nur etwas mehr als die Hälfte aller Anwender wusste, was Phishing ist



Nahezu die Hälfte aller Anwender glaubte, alle internen E-Mails seien sicher



Etwas mehr als ein Drittel der Anwender konnte Ransomware identifizieren

Quelle: Proofpoint: „State of the Phish 2022“, Januar 2022.

Eigenschaften einer starken Sicherheitskultur

Wie sieht eine Sicherheitskultur aus? Unternehmen sind so unterschiedlich wie ihre Mitarbeiter, zudem ist jede Branche Teil einer größeren Subkultur. Dennoch haben starke Sicherheitskulturen einige universelle Gemeinsamkeiten. Eine starke Sicherheitskultur hat folgende Merkmale:

- **Sie ist ganzheitlich und kontinuierlich.** Eine Sicherheitskultur darf nicht nur aus Schulungen und gelegentlichen Phishing-Simulationen bestehen. Das Ziel ist, die Moral zu heben und die Mitarbeiter dazu zu bewegen, sich für die Sicherheit im Unternehmen einzusetzen. Dies lässt sich auf vielen Wegen erreichen. Eine Sicherheitskultur fördert das Lernen und Sicherheitsbewusstsein durch relevante und maßgeschneiderte Inhalte sowie Updates zur sich verändernden Bedrohungslandschaft. Die Anwender erhalten E-Mails und andere Erinnerungen, die als Stütze dienen und ihnen bewusst machen, warum sie am Programm teilnehmen und wie es ihnen bei ihrer Arbeit – und im Privatleben – hilft. Zudem werden sie ermutigt, verdächtige digitale Ereignisse vorbehaltlos und entschlossen zu melden.
- **Sie hat positionsübergreifende Fürsprecher.** Die Unterstützung beginnt bei der Unternehmensführung und geht über die Abteilungsleiter bis hin zu den Endnutzern. Abgesehen von den Führungskräften können sich Fürsprecher unter anderem in der Sicherheits-, IT-, Personal-, Compliance- und Audit- sowie der Marketing- und Presse-Abteilung finden.[8]
- **Sie erzeugt Erwartungen und erhält sie aufrecht.** Dazu gehört die Entwicklung und Durchsetzung von Sicherheitsrichtlinien, die kulturelle Normen bestimmen.

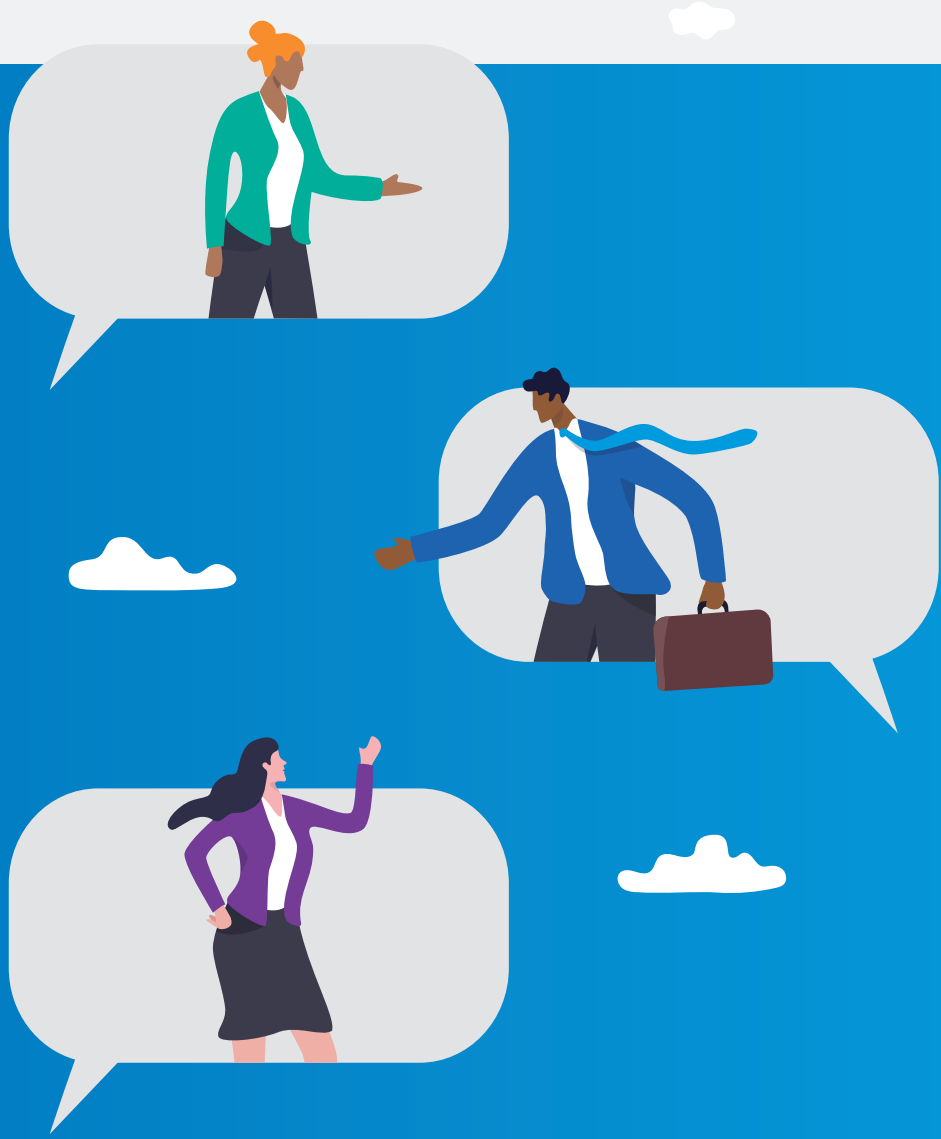
8 SANS Institute: „2021 Security Awareness Report: Managing Human Cyber Risk“ (Bericht zum Sicherheitsbewusstsein 2021: Verwaltung menschlicher Cyberrisiken), November 2021.

Schaffung einer sicheren und gerechten Kultur

Die Grundlage einer Sicherheitskultur bildet eine psychologisch sichere Umgebung. Sicherheitszwischenfälle können jedes Unternehmen herunterziehen, besonders wenn eine einzelne Person verantwortlich gemacht wird. In einigen Fällen empfinden Mitarbeiter Phishing-Simulationen als bestrafend und haben das Gefühl, versagt zu haben oder unfähig zu sein, wenn sie auf den Köder hereinfallen.

Sorgen Sie für eine Atmosphäre, in der die Mitarbeiter das Sicherheitsteam ohne Vorbehalte kontaktieren, wenn ihnen etwas Verdächtiges auffällt – und es ihnen nicht unangenehm ist, der Sicherheitsabteilung einen Fehltritt zu melden.

Zudem benötigen die Anwender die Gewissheit, dass sie sich wehren sollten, wenn sie darum gebeten werden, etwas zu tun, das ihrer Meinung nach ein Sicherheitsrisiko darstellt.



ABSCHNITT 2

Die Herausforderungen beim Aufbau einer Sicherheitskultur

Unternehmen geben Millionen für Sicherheitstools, Services und Personal aus. Doch selbst mit diesen Investitionen übersehen viele den größten Risikofaktor: den Menschen.

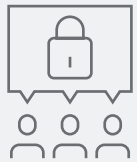
Der Faktor Mensch spielt beim Schutz des Unternehmens die größte Rolle – und ist ein Problem, das sich nur schwer bewältigen lässt. Aktivitäten zur Steigerung des Sicherheitsbewusstseins werden häufig als störend und ablenkend empfunden. Einige Mitarbeiter haben das Gefühl, dass sie dadurch von ihrer „richtigen“ Arbeit abgehalten werden. Viele stellen sich gegen die zusätzlichen Anforderungen wie das Melden von verdächtigen E-Mails oder die Schulungs-Webinare. Zudem können die technischen Fachkräfte und Mitarbeiter der Personalabteilung zurückhaltend auf den Aufbau einer Sicherheitskultur reagieren, da sie dafür nicht gerüstet sind.

Folgende Herausforderungen stellen sich:

Die Unternehmens-führung vom Konzept überzeugen

Die Rendite überzeugend quantifizieren

Die Anwender davon überzeugen, dass Schulungen und Sicherheitsbewusstsein etwas Positives sind und sie dabei mitmachen sollten



Das Anwender-verhalten ändern

Überwinden von Hindernissen

Nur wenige Sicherheitsverantwortliche würden den Wert von Sicherheitsbewusstsein anzweifeln. Der Aufbau einer starken Sicherheitskultur kann jedoch eine große Herausforderung darstellen. Im Folgenden führen wir einige mögliche Hindernisse an und erläutern, wie Sie diese überwinden können.

Hindernis Nr. 1: Kritische Stimmen in der Finanzabteilung und unter den operativen Führungskräften

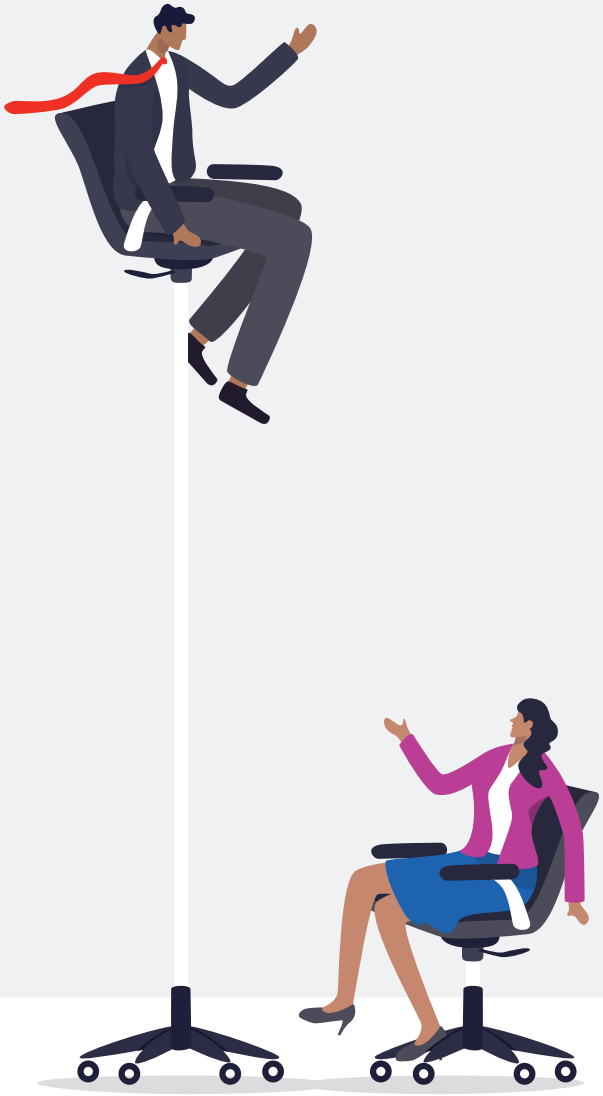
Ihre Finanzabteilung sperrt sich möglicherweise gegen die hohen Kosten für Programme zur Steigerung des Sicherheitsbewusstseins, besonders wenn das Unternehmen bereits in mehrere Sicherheitstools investiert hat. Gleichzeitig machen sich die operativen Führungskräfte Sorgen über geminderte Produktivität aufgrund der Schulungen. Zeitmangel und zu wenig Personal zur Durchführung des Programms sind zwei weitere wichtige Probleme, die die Verantwortlichen häufig vorbringen.[9]

So können Sie reagieren: Begründen Sie die Kosten und den Aufwand

Gehen Sie auf die finanziellen Vorteile ein. Um eine Sicherheitskultur wirtschaftlich zu rechtfertigen, können Sie beispielsweise die Kosten einer Kompromittierung anführen (durchschnittlich 4,24 Millionen US-Dollar[10]) und diese mit den Schulungskosten vergleichen. Gleichzeitig kann ein Gespräch mit der Abteilung für betriebliche Abläufe hilfreich sein, bei dem Sie die Gelegenheit haben, Ängste über belastende Pflichten für die Anwender auszuräumen. So wird beispielsweise die benötigte Schulungszeit durch Mikro-Lerneinheiten reduziert, während die Inhalte noch besser gefestigt werden. Zudem kann die Operations-Abteilung dabei helfen, die Umsetzung zu erleichtern.

Für Teams, die nur wenig Ressourcen entbehren können, schlägt Gartner den Einsatz eines verwalteten Schulungs-Services für die Durchführung und Aufrechterhaltung des Programms vor.[11] Die Service-Anbieter bieten in der Regel eine Plattform zur Steigerung des Sicherheitsbewusstseins mit speziellen Services wie geplante Phishing-Testkampagnen und weitere Schulungen als Abonnement an.

9 SANS Institute: „2021 Security Awareness Report: Managing Human Cyber Risk“ (Bericht zum Sicherheitsbewusstsein 2021: Verwaltung menschlicher Cyberrisiken), November 2021.
10 Ponemon Institute: „2021 Cost of a Data Breach Report“ (Kosten von Datenkompromittierungen 2021), August 2021.
11 Gartner: „Market Guide for Security Awareness Computer-Based Training“ (Market Guide zu computergestützten Schulungen zur Steigerung des Sicherheitsbewusstseins), September 2021.



Hindernis Nr. 2: Vorbehalte unter den Führungskräften

Ebenso wie die Finanzabteilung betrachtet häufig auch die Führungsetage Sicherheit als eine weitere Kostenstelle in der Bilanz. Möglicherweise sind die Führungskräfte der Meinung, dass das Unternehmen bereits Millionen für Tools und Technologien ausgegeben hat, und weitere Investitionen gut überlegt sein sollten.

So können Sie reagieren: Machen Sie deutlich, welche Kosten unbeseitigte Risiken haben

Das Bewusstsein der Führungskräfte lässt sich am besten mit Tabletop-Übungen schärfen, in denen Was-wäre-wenn-Szenarien für häufige Sicherheitszwischenfälle durchgespielt werden.

Zeigen Sie zum Beispiel den genauen Ablauf eines Ransomware-Angriffs und verdeutlichen Sie damit, wie leicht die Umgebung durch eine E-Mail mit Social Engineering infiziert werden kann. Erläutern Sie danach, wie die Ransomware Daten und Systeme blockieren und das Unternehmen praktisch lahmlegen würde.

Mit Alarmübungen vermitteln Sie einen greifbaren Eindruck davon, was bei einem realen Angriff passieren kann. Dies hilft der Geschäftsleitung, Cyberrisiken zu bewerten und in einen Kontext zu stellen. Zudem wird damit auf eindrucksvolle Weise demonstriert, wie wichtig der Aufbau einer Sicherheitskultur ist.

Zeigen Sie außerdem, welche Anwender im Unternehmen aus welchem Grund am stärksten gefährdet sind, um die fundamentale Bedeutung der individuellen Resilienz zu unterstreichen. (Dies lässt sich sehr viel leichter mit einer modernen Sicherheitslösung bewerkstelligen, die die Risiken in Bezug auf Schwachstellen, Angriffe und Zugriffsrechte zu einem einfach verständlichen Anwenderrisikowert zusammenfassen kann.)

Ebenso sollten Sie zeigen, welchen Wettbewerbsvorteil eine Sicherheitskultur bietet. Eine wirksame Kultur sorgt für mehr Vertrauen und zeigt dem Markt, dass das Unternehmen sich um seine Kunden, Partner und Mitarbeiter kümmert.

Untermauern Sie Ihre Argumente mit wichtigen Kennzahlen, die Sie auf nichttechnische und positive Art und Weise in das Gespräch mit der Geschäftsleitung einfließen lassen.

78 %

der Unternehmen geben an, dass Schulungen zur Steigerung des Sicherheitsbewusstseins die Anfälligkeit verringern.[12]

Hindernis Nr. 3: Desinteresse und Widerstand bei den Anwendern

Veränderungen durchzusetzen ist immer schwierig. Noch schwieriger ist der Aufbau einer völlig neuen Sicherheitskultur. Möglicherweise fragen sich die Mitarbeiter, ob sie überwacht werden. Sie denken eventuell, Sicherheit sei nicht ihre Aufgabe oder sie sehen einfach keinen Nutzen darin.

Angesichts des Umstands, dass die Zeit der Mitarbeiter eine der wertvollsten Ressourcen eines Unternehmens ist, sorgen sich die Führungskräfte womöglich darum, dass die Sicherheitsprogramme die Anwender ablenken und die Produktivität verringern könnten.

So können Sie reagieren: Sprechen Sie Verstand und Gefühle an

Rücken Sie die Maßnahme auch hier wieder in ein positives Licht und erläutern Sie, warum Sicherheitsbewusstsein wichtig ist. Betonen Sie, dass bei den Schulungen und Festigungsmaßnahmen niemand bestraft werden soll. Stattdessen wird damit allen Beteiligten ermöglicht, zur Sicherheit sowie dem Erfolg des Unternehmens und aller Mitarbeiter beizutragen.

Zeigen Sie den Anwendern das eigene Risikoprofil (und eventuell den im letzten Abschnitt erwähnten Risikowert), um die Dinge auf eine persönlichere Ebene zu bringen.

Arbeiten Sie mit Schlagzeilen, also Szenarien aus dem wahren Leben, wo ein Mangel an Sicherheitsbewusstsein zu ernsthaften Bedrohungen und somit zu verringerter Produktivität sowie langwierigen Ausfällen geführt hat.

Viele der Sicherheitskompetenzen, die die Mitarbeiter am Arbeitsplatz lernen, können sie ebenso zu Hause und im alltäglichen Leben anwenden. Um die Akzeptanz zu erhöhen, kann es hilfreich sein, das Sicherheitsprogramm als eine persönliche Bereicherung darzustellen.

12 Proofpoint: „State of the Phish 2021“, Januar 2021.

Herausstellen der Vorteile einer Sicherheitskultur

Wenn Sie erläutern, wie eine Sicherheitskultur zu den geschäftlichen Zielen des Unternehmens beiträgt, sollten Sie sinnvolle und messbare Vorteile aufzählen. Hier sind einige Beispiele, die bei Führungskräften gut ankommen:

Verbesserte Agilität und Resilienz. Eine Sicherheitskultur spornt die Mitarbeiter dazu an, potenzielle Bedrohungen zu erkennen. Zudem ermöglicht sie dem Sicherheitsteam, schneller auf Bedrohungen zu reagieren und diese zu beheben. Agilität und Resilienz verbessern sich, wenn durch motivierte, regelmäßig geförderte und sich gegenseitig unterstützende Anwender ein Netzwerkeffekt entsteht. Die Vorteile wirken sich auf das gesamte Unternehmen aus.

Unternehmensweite Minimierung von Risiken. Wir leben in einer Zeit mit immer mehr Remote- und Hybrid-Arbeitsplätzen, in der Unternehmen zur Cloud wechseln und verstärkt private Geräte genutzt werden. Wenn es eine starke Sicherheitskultur gibt, können sich die Führungskräfte unbesorgt um andere Bereiche des Unternehmens kümmern.

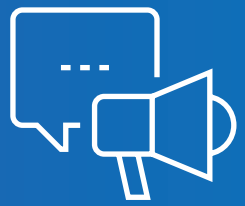
Unkomplizierte Compliance. Die Einhaltung von gesetzlichen Vorschriften, Branchenstandards und internen Sicherheitsrichtlinien wird einfacher, womit sich die Wahrscheinlichkeit von Strafen und Geldbußen verringert.

Wettbewerbsvorteil. Wenn Kunden und Partner den Eindruck haben, dass Ihr Unternehmen mehr Sicherheit bietet, werden sie sich für Sie anstatt für Ihre Mitbewerber entscheiden. Sicherheit sollte als Grundwert kommuniziert werden.

Merkmale einer starken Sicherheitskultur

Bei einer starken Sicherheitskultur haben die Mitarbeiter gelernt, kritisch zu hinterfragen und überlegt zu handeln. Sie verfügen über die Tools, Ressourcen und das Wissen, um selbst Antworten finden zu können. Zudem werden sie dazu ermutigt, kontinuierlich Fragen zu stellen.

Eine Sicherheitskultur wird durch Handlungen, Einstellungen und Überzeugungen bestimmt. Folgende Verhaltens- und Denkweisen zählen zu den Merkmalen einer ausgeprägten Kultur:



Verdächtiges sofort melden

Erst überlegen, dann klicken

Auch bei der Arbeit zu Hause an die Sicherheit denken

Diskret mit privaten Informationen umgehen

Informationen werden als wichtige Ressource angesehen

ABSCHNITT 3

Die Umsetzung: Drei Schritte zum Aufbau einer Sicherheitskultur

Sie sind also von den Vorteilen einer starken Sicherheitskultur überzeugt und Ihr Unternehmen ist zur Umsetzung bereit. Wo fangen Sie an?

Motivation ist der Schlüssel zur Entwicklung einer starken Sicherheitskultur und besteht aus drei wichtigen Bestandteilen. Der erste ist **Autonomie**. Das bedeutet individuell gestaltetes und selbstbestimmtes Lernen für jeden Anwender. Der zweite ist die **Entwicklung von Kompetenz**. Das heißt, den Anwendern die Tools und Zeit zu geben, die sie benötigen, um sich weiterzuentwickeln und Cybersicherheitswissen und Fähigkeiten anzueignen bzw. zu erlernen. Der letzte Bestandteil ist der **Sinn und Zweck**. Die Anwender sollen das Gefühl bekommen, dass sie Teil einer umfassenden Mission sind.

Der Aufbau einer nachhaltigen Sicherheitskultur kann mit drei Schritten unterstützt werden. Dieser fortlaufende Prozess gliedert sich wie folgt:

1. Bewertung der Anwenderschwachstellen
2. Änderung des Anwenderverhaltens
3. Bewertung und Beobachtung des Fortschritts

Schritt 1: Bewerten der Bereitschaft und Risiken der Anwender

Jedes Unternehmen hat seine individuellen Risiken und Sicherheitsprioritäten.

Stellen Sie sich folgende Fragen:

- Wer wird angegriffen?
- Welchen Arten von Angriffen sind Ihre Anwender ausgesetzt?
- Wie minimieren Sie das Risiko, falls die Angreifer doch durchkommen?

Anhand dieser und anderer Fragen können Sie ermitteln, wo Ihre Schwachstellen liegen. Mit dieser Übung können Sie sich auf die dringendsten Bereiche konzentrieren, die eine Gefahr darstellen oder eine Kompromittierung verursachen könnten.

Diesen Schritt sollten Sie regelmäßig wiederholen, um Ihren Ansatz neu zu bewerten und auszurichten.

So bewerten Sie das Anwenderrisiko

Gehen Sie ins Detail und berücksichtigen Sie unbedingt die weiteren Umstände, indem Sie sich die Unternehmensdemographie und das Verhalten Ihrer Mitarbeiter anschauen. Kontextbezogene Kennzahlen sind unerlässlich, denn die einzelnen Gruppen im Unternehmen verhalten sich unterschiedlich.

Häufig begehen Unternehmen den Fehler, nur das zu messen, was sich am einfachsten messen lässt. Die Zahl der fehlgeschlagenen Phishing-Versuche allein gibt Ihnen keinen Überblick über Ihre Sicherheit oder das Sicherheitsbewusstsein Ihrer Mitarbeiter. Andere Kennzahlen zur Sicherheit sind beispielsweise die durchschnittliche Zeit zur Erkennung bzw. Behebung von Bedrohungen. Es gibt jedoch Angriffe, die sich erst spät bemerkbar machen. Daher sind diese Kennzahlen nicht in jedem Fall hilfreich.

Sinnvolle Kennzahlen

Dies sind einige der besten Möglichkeiten zur Bewertung des Anwenderrisikos:

- Finden Sie heraus, welche Ihrer Anwender (einschließlich Dritter wie Partner, Anbieter und Auftragnehmer) am häufigsten angegriffen werden und ordnen Sie sie nach Position und wie häufig sie auf Links in E-Mails klicken. Bei Proofpoint nennen wir diese Anwender Ihre Very Attacked People™ (VAPs).
- Identifizieren Sie anfällige Anwender. Behalten Sie die Reaktionen auf Phishing-Simulationen im Blick, die aktuelle reale Bedrohungen widerspiegeln. Hinweis: Simulierte Phishing-Angriffe sind eine Möglichkeit, anfällige Anwender zu erkennen. Allerdings sollten Sie noch weitere Kennzahlen einbeziehen. So können beispielsweise Anwender, die schlecht abschneiden oder keine Schulungsübungen absolvieren, ein Hinweis auf Schwachstellen sein. Diese Kennzahlen sollten Sie daher ebenfalls im Blick behalten.
- Finden Sie heraus, was Ihre Mitarbeiter tun, wenn ihnen niemand über die Schulter schaut. Verwenden sie aktiv Kennwort-Manager? Melden sie eingehende Phishing-E-Mails an das Unternehmen? Geben sie Unternehmensinformationen an externe Konten weiter?

Empfohlene Aktivitäten

Folgende Dinge können Sie tun, um den Aufbau einer Sicherheitskultur zu fördern:

- **Monatliche Kurzinformationen zu relevanten Angriffen und Schulungen zu aktuellen Bedrohungen**
- **Wöchentliche Bedrohungswarnungen mit technischen Informationen, die die Anwender über Slack- oder Teams-Kanäle und Wiki-Seiten erhalten**
- **Würdigung hervorragender Leistungen über motivierende Programme, die auf Ihre Unternehmenskultur zugeschnitten sind (z. B. Ranglisten oder Preise für die Meldung realer Phishing-Versuche) – dies ist besonders am Anfang wichtig**
- **Unterstützung durch Mitarbeiter aus der Marketing- und Presseabteilung, um die Sicherheitskultur auf überzeugende und ansprechende Art und Weise bekannt zu machen (über Poster, E-Mails, in Newslettern des Unternehmens und von Abteilungen sowie internen Blog-Artikeln)**

Schritt 2: Ändern von Verhalten durch bedrohungsbezogene Inhalte und festigende Schulungen

Der Aufbau einer Sicherheitskultur ist ein fortlaufender Prozess und kein einmaliges Ereignis. Wählen Sie einen ganzheitlichen Ansatz.

Wenden Sie sich dazu regelmäßig über verschiedene Kommunikationskanäle an Ihre Mitarbeiter, zum Beispiel in regelmäßigen Newslettern, über interne Blog-Artikel und durch aktuelle Informationen über die neuesten Bedrohungen und Angriffsvektoren.

Zudem sollten Sie den Anwendern ansprechende Inhalte bieten, die die Anforderungen der Marke und Kultur unterstützen. Beziehen Sie die aktuelle Bedrohungslandschaft in die Schulungen ein, um sie für die Anwender relevanter zu machen. Entwickeln Sie abwechslungsreiche und ansprechende Lerninhalte: animierte Videos, Comedy-Einlagen oder etwas Einfaches wie ein Quiz. Sorgen Sie für eine bunte Mischung an Inhalten und gestalten Sie sie individuell. Jeder ist unterschiedlich und reagiert bzw. lernt anders.

Denken Sie daran, immer wieder auf positive Art und Weise auf die Bedeutung von Sicherheit hinzuweisen. Versetzen Sie sich in die Lage Ihrer Mitarbeiter und berücksichtigen Sie die Unternehmensdemografie. Ihre Mitarbeiter haben vielfältige Interessen.

Der Aufbau einer Sicherheitskultur hängt wesentlich vom Gefühl der Mitverantwortung der Anwender ab. Entwickeln Sie ein überzeugendes, unverwechselbares internes Branding für Ihr Sicherheitsprogramm.

Schritt 3: Bewerten und Beobachten des Fortschritts

Geben Sie Kennzahlen weiter, die den Fortschritt, die kontinuierliche Verbesserung und die Rendite zeigen. Diese quantifizierbaren Bewertungen bestätigen Ihre Investition und zeigen der Geschäftsleitung sowie dem gesamten Unternehmen, wie wertvoll eine Sicherheitskultur ist.

Lassen Sie niemals eine gute Krise ungenutzt verstreichen. Zeigen Sie nach einem Angriff, wie durch eine starke Sicherheitskultur der Zeit- und Arbeitsaufwand sowie die Finanzmittel zur Behebung verringert oder der Angriff völlig vermieden werden konnte.

Der Fortschritt lässt sich anhand der folgenden Kennzahlen messen:

- Suchen Sie sich acht bis zehn der größten Sicherheitsprobleme heraus, auf die Sie sich konzentrieren, und ermitteln Sie, welches Risiko sie darstellen.
- Messen Sie die Zeit für Updates. Schaffen Sie es, dass alle das Programm schnell durchlaufen? Was machen Sie mit Nachzüglern und wie finden Sie sie? (Warum brauchen sie so lange? Fehlt ihnen die Motivation oder liegt es an etwas anderem?) Wie schnell können Ihre Mitarbeiter die Schulung absolvieren?
- Heben Sie die Aktivitäten zur gezielten Förderung der Sicherheitskultur hervor. (Beispiel: Wie häufig informieren Führungskräfte ihr Team über die neuesten Bedrohungen?)

Woran lässt sich Erfolg erkennen?

Es gibt viele Möglichkeiten, das Sicherheitsbewusstsein in Ihrem Unternehmen zu messen und einzuschätzen, wie sich die Sicherheitskultur auf das Anwenderverhalten ausgewirkt hat.

Klickraten für die am meisten gefährdeten Anwender

Anfällige Anwender sind Mitarbeiter, die eher auf Phishing und andere Bedrohungen hereinfallen. Wenn Sie Vorlagen für Phishing-Simulationen verwenden, die auf die verschiedenen Positionen im Unternehmen zugeschnitten sind, erhalten Sie einen Überblick darüber, wer schädliche Nachrichten meidet und wer darauf hereinfällt.

Resilienzfaktor

Der Resilienzfaktor wird anhand der Phishing-Meldungsrate für Simulationen geteilt durch die Phishing-Klicks errechnet. Es sollte ein Resilienzfaktor von 14 angestrebt werden, was sich folgendermaßen ausdrückt:

- Eine Meldungsrate von mindestens 70 % für Phishing-Simulationen
- Eine Klickrate von unter 5 %
- Eine Zuverlässigkeitsquote für gemeldete E-Mails (Sind die von Anwendern gemeldeten E-Mails tatsächlich schädlich?)

Branchen-Benchmarks

In Dashboards für Führungskräfte sehen Sie, wie Sie verglichen mit Ihren Mitbewerbern in wichtigen Bereichen Ihres Programms zur Sensibilisierung für Sicherheit abschneiden. Dadurch lässt sich genau feststellen, wo noch Raum für Verbesserung besteht. So können Sie beispielsweise sehen, ob Ihre Anwender harmlose Nachrichten als schädlich melden und wo Sie damit im Vergleich zu anderen Unternehmen stehen.

Weitere Kennzahlen

Dies sind weitere von Menschen beeinflusste, sicherheitsrelevante Ergebnisse, die Sie bei der Bewertung des Erfolgs Ihrer Sicherheitskultur berücksichtigen können:

- Erfolgreiche Phishing-Zwischenfälle
- Klickrate bei bekannt schädlichen Inhalten
- Kompromittierung von Anmeldedaten
- Insider-Zwischenfälle
- Computerseitige Behebung von Ransomware-Zwischenfällen

Acht Schritte zum Aufbau einer Sicherheitskultur[13]

Innerhalb eines Jahres hat Jason Cox von Elevate Textiles, einem weltweit tätigen Textilhersteller, eine umfassende Sicherheitskultur aufgebaut.

Dies sind seine „acht einfachen Regeln für Sicherheitsbewusstsein“:

1. Akzeptieren Sie, dass Ihre Mitarbeiter der Teil Ihres Unternehmens ist, der am meisten angegriffen wird.
2. Beziehen Sie die Geschäftsleitung mit ein, da sie für die Durchsetzung von Veränderungen entscheidend sein und die Unterstützung unter den Verantwortlichen sichern kann.

3. Sammeln Sie Daten zur Unterstützung Ihres Programms und nutzen Sie dabei Tools wie Cybersicherheitsbewertungen, Umfragen und Protokolle für gemeldete Infektionen.
4. Nehmen Sie Verantwortliche, die die Gründe für das Programm kennen, in die Pflicht: Sichern Sie sich die Unterstützung der jeweiligen Abteilungsleiter, denn sie wissen, was ihre Mitarbeiter benötigen und welche Daten geschützt werden müssen.
5. Zuerst umfassend schulen, dann regelmäßig üben. Suchen Sie sich einen Monat aus, in dem sie anfangen (der Oktober ist zum Beispiel in den USA der National Security Awareness Month), und schulen Sie Ihre Anwender intensiv zu wichtigen Themen. Führen Sie danach regelmäßig Festigungsmaßnahmen durch und geben Sie Updates heraus. Der Aufbau einer Sicherheitskultur ist ein fortlaufender Prozess.
6. Bringen Sie die Dinge auf eine persönliche Ebene. Wie wirkt sich Informationssicherheit bei den Mitarbeitern am Arbeitsplatz und zu Hause aus? Erzählen Sie persönliche Geschichten. Gestalten Sie das Programm kurzweilig und ansprechend.
7. Belohnen Sie richtiges Verhalten mit Gutscheinen und anderen positiven Anreizen.
8. Umfrage wiederholen, Ergebnisse dokumentieren, regelmäßig wiederholen. Starten Sie nach einem Jahr eine neue Umfrage. Führen Sie erneut Phishing-Tests durch. Behalten Sie die Zahl der Sicherheitstickets im Auge. Und bleiben Sie im Austausch mit der Geschäftsleitung, die die Verantwortung für die Risiken und die Haftung trägt und wissen muss, welchen Nutzen das Programm bringt.

13 Nach einer Präsentation auf der Proofpoint Wisdom-Konferenz 2021 (https://www.proofpoint.com/us/wisdom-2021-demand-content-library).

Fazit

Der Aufbau einer starken nachhaltigen Sicherheitskultur wirkt sich auf alle Ihre Anwender positiv aus – von der Geschäftsleitung über die Abteilungsleiter bis hin zu den Endnutzern.

Doch es gibt keine universelle Vorlage für eine Sicherheitskultur. Jedes Unternehmen hat einen eigenen Charakter und individuelle Anforderungen. Einige dieser Unterschiede hängen vom Unternehmen ab, andere wiederum von der Branche. Zudem wird jede Kultur durch eine ganze Reihe an internen und externen Faktoren bestimmt.

Durch den Aufbau eines langfristigen Programms, das von allen Beteiligten getragen wird, kann Sicherheitsbewusstsein zu den festen Grundwerten Ihres Unternehmens werden. Eine echte Sicherheitskultur besteht nicht aus einmaligen Schulungen. Sie ist geprägt von einer inneren Einstellung, die sich auf die alltäglichen Aktivitäten im Unternehmen und im privaten Bereich auswirkt.

Weitere Informationen dazu, wie Proofpoint Sie dabei unterstützen kann, eine für Ihre Unternehmenskultur maßgeschneiderte Sicherheitskultur zu entwickeln, finden Sie unter https://www.proofpoint.com/de/products/security-awareness-training.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0504-003-01-01 04/22