Mit Empfehlung von

MetaCompliance®

Achtsamkeit bei Cybergefahren

für dummies®
A Wiley Brand

Die Sicherheitskultur der Mitarbeiter ändern

Mehr Sicherheitsbewusstsein schaffen

Dieses Playbook für Cybersicherheitskampagnen befolgen

Robert O'Brien

Geraldine Strawbridge

Sonderausgabe von MetaCompliance

Über MetaCompliance

MetaCompliance verfügt über mehr als 14 Jahre Erfahrung im Bereich der Sicherheitsschulung und Sensibilisierung von Mitarbeitern. Das Unternehmen arbeitet mit Kunden aus allen Branchen zusammen und hilft Unternehmen dabei, ihre Daten zu schützen, ihre Mitarbeiter zu schulen und Reputations- und Regulierungsrisiken zu bewältigen. In dieser Zeit haben die regulatorischen Herausforderungen für Unternehmen und die mit ihren digitalen Vermögenswerten verbundenen Bedrohungen ständig zugenommen.

MetaCompliance ist ein weltweit führendes Unternehmen, das den menschlichen Aspekt der Cybersicherheit und der Compliance in den Mittelpunkt stellt. Das Team von MetaCompliance arbeitet täglich mit Kunden aus dem öffentlichen und privaten Sektor zusammen, um auf Sicherheitsrisiken ausgerichtete Sensibilisierungskampagnen durchzuführen, die Mitarbeiter motivieren und Verhaltensänderungen bewirken.

Die grafisch ansprechende SaaS-Plattform bietet Kunden eine integrierte, mehrsprachige Funktionspalette, die simuliertes Phishing, eLearning für Cybersicherheit und Compliance, Richtlinienmanagement, Datenschutzmanagement und Incident Management umfasst. Durch einen „One-Stop-Shop" zur Verwaltung von Datenschutz und -sicherheit, Compliance und Cyberprojekten, der Mitarbeiter bei der Erfüllung ihrer Compliance-Aufgaben unterstützt, erhalten Unternehmen einen besseren regulatorischen Schutz.

Die von MetaCompliance entwickelte innovative Cloud-Architektur MyCompliance ist eine globale Enterprise-Lösung, die auf der Microsoft Azure Plattform bereitgestellt wird. MetaCompliance hat Niederlassungen in London (Großbritannien), Dublin (Irland) und Atlanta (Georgia) und einen ständig wachsenden Kundenstamm im öffentlichen und privaten Sektor.

Achtsamkeit bei Cybergefahren

für dummies®

Achtsamkeit bei Cybergefahren

Sonderausgabe von MetaCompliance

Robert O'Brien, Cybersicherheits- und Compliance-Experte
Geraldine Strawbridge, Redakteurin für Cybersicherheit

für dummies®

Achtsamkeit bei Cybergefahren für Dummies®, Sonderausgabe von MetaCompliance

Veröffentlicht von: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate

Chichester, West Sussex, www.wiley.com

Eingetragener Firmensitz

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, Großbritannien

Allgemeine Informationen zu unseren anderen Produkten und Dienstleistungen oder zur Erstellung eines individuellen *Für Dummies*-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von unserer Abteilung Business Development in den USA unter Tel. 877-409-4177, E-Mail: info@dummies.biz, oder auf www.wiley.com/go/custompub. Für Informationen zur Lizenzierung der *Für Dummies*-Marke für Produkte oder Dienstleistungen kontaktieren Sie bitte BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-29046-8 (pbk); ISBN 978-1-394-29047-5 (ebk); 978-1-394-29048-2 (ePub)

In Großbritannien gedruckt

10 9 8 7 6 5 4 3 2 1

Inhaltsverzeichnis

Einführung

In den letzten zehn Jahren hat sich die Cybersicherheitslandschaft dramatisch verändert. Nach Angaben von Cybersecurity Ventures verursachte Cyberkriminalität im Jahr 2021 weltweite Schäden in Höhe von 6 Billionen US-Dollar und ist damit profitabler als der internationale Drogenhandel. Unternehmen jeder Größe und in jeder Branche sind zu potenziellen Zielen für Cyberkriminelle geworden. Es gibt ständig neue Bedrohungen, sodass kein Unternehmen sich mehr voll und ganz auf seine Sicherheitsmechanismen verlassen kann.

Cyberkriminelle nehmen das schwächste Glied in der Abwehrkette eines Unternehmens ins Visier – und das sind nur allzu oft die Mitarbeiter. 90 Prozent aller Datenschutzverletzungen sind auf menschliches Versagen zurückzuführen. Unternehmen müssen daher ein Programm zur Sensibilisierung für Cybersicherheit einführen, damit alle Mitarbeiter die wichtige Rolle erkennen und übernehmen können, die sie beim Schutz sensibler Unternehmensdaten spielen.

Über dieses Buch

Cyber Security Awareness für Dummies, Sonderausgabe von MetaCompliance, besteht aus sechs Kapiteln, in denen die folgenden Themen behandelt werden: die moderne Cybersicherheitslandschaft (Kapitel 1), die Notwendigkeit von Sensibilisierungsprogrammen für die Cybersicherheit (Kapitel 2), Sensibilisierungskampagnen zur Förderung von Veränderungen 3), die Integration des Richtlinienmanagements in Sensibilisierungsprogramme (Kapitel 4), Methoden zur Entwicklung einer Best-Practice-Strategie zur Cyber-Sensibilisierung (Kapitel 5) und Best Practices zur Durchführung einer Sensibilisierungskampagne für Cybersicherheit (Kapitel 6).

Jedes Kapitel ist in sich geschlossen. Sie können deshalb einfach zu jedem beliebigen Thema springen, das Ihr Interesse weckt. Lesen Sie das Buch so, wie es Ihnen am liebsten ist (verkehrt herum oder rückwärts würden wir allerdings nicht empfehlen)!

Leichtfertige Annahmen

Beim Verfassen dieses Buches sind wir davon ausgegangen, dass Sie ein Cybersicherheits- oder IT-Experte sind, z. B. ein Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Information

Security Officer (CISO), Chief Privacy Officer (CPO), Datenschutzbeauftragter, IT-Direktor, IT-Leiter, Personalleiter, Schulungsleiter, Change Manager oder eine Führungskraft.

Wenn Sie sich in einer dieser Beschreibungen wiedererkennen, dann ist dieses Buch genau richtig für Sie! Wenn nicht, sollten Sie trotzdem weiterlesen, denn nach der Lektüre dieses Buches werden Sie auf jeden Fall ein geschärftes Bewusstsein für Cybersicherheit haben.

In diesem Buch verwendete Symbole

In diesem Buch verwenden wir gelegentlich einige spezielle Symbole, um Sie auf wichtige Informationen aufmerksam zu machen. Sie werden auf die folgenden Symbole stoßen:

Dieses Symbol macht auf wichtige Informationen aufmerksam, die Sie Ihrem nichtflüchtigen Speicher bzw. Ihren grauen Zellen anvertrauen sollten!

Wir hoffen, dass Sie diese nützlichen Informationen zu schätzen wissen.

Das Warnsymbol weist auf praktische Ratschläge hin, die Ihnen dabei helfen sollen, kostspielige und frustrierende Fehler zu vermeiden.

Zusätzliche Informationen

Auf diesen Seiten können wir natürlich nur eine Auswahl der wichtigsten Themen behandeln. Wenn Sie aber am Ende dieses Buches so beeindruckt sein sollten, dass Sie unbedingt noch mehr erfahren möchten, finden Sie weitere Informationen auf `www.metacompliance.com`.

IN DIESEM KAPITEL

- Die sich verändernde Bedrohungslandschaft
- Was motiviert Cyberkriminelle?
- Sicherheitsbewusstsein als integraler Bestandteil der digitalen Transformation
- Security Frameworks und Datenschutz
- Gesetzliche Compliance-Vorgaben

Kapitel 1
Die moderne Cyber-Sicherheitslandschaft

In diesem Kapitel erfahren Sie, warum ausgefeilte Cyberbedrohungen, ein höheres Maß an Governance, strengere Datenschutzvorschriften und die Notwendigkeit von „Security by Design" moderne Unternehmen dazu zwingen, ihr Bewusstsein für Cybersicherheit zu schärfen.

Gegen Personen gerichtete Cyberbedrohungen

Cyberkriminalität ist inzwischen zu einer der größten Bedrohungen für Unternehmen in aller Welt geworden. Die Angriffsvektoren ändern sich ständig, da Cyberkriminelle immer neue Wege finden und die unterschiedlichsten Taktiken nutzen, um sich Zugang zu wertvollen Unternehmensdaten zu verschaffen.

Um das Risiko einer Sicherheitsverletzung so weit wie möglich zu verringern, müssen Unternehmen die unterschiedlichen Arten von Cyberbedrohungen kennen, mit denen sie konfrontiert werden könnten:

- **Phishing:** *Phishing* ist eine Art von Social-Engineering-Angriff, bei dem Opfer dazu gebracht werden sollen, sensible Informationen

offenzulegen oder Malware zu installieren. Das Ziel der Angreifer ist es, vertrauenswürdig zu erscheinen. Sie verwenden E-Mail, soziale Medien, Telefonanrufe und Textnachrichten, um ihre Opfer zu einer bestimmten Handlung zu bewegen. Die Betroffenen werden zum Beispiel dazu gebracht, auf einen bösartigen Link zu klicken, einen Anhang herunterzuladen, eine gefälschte Website zu besuchen oder sensible Informationen preiszugeben.. Diese Informationen können dann verwendet werden, um auf persönliche Konten zuzugreifen oder Identitätsdiebstahl zu begehen.

- **Malware:** *Malware* ist eine Art von Schadsoftware, die darauf abzielt, ein Computersystem ohne das Wissen des Benutzers zu schädigen oder sich Zugang zu ihm zu verschaffen. Beispiele für Malware sind Viren, Würmer, Trojaner, Spyware, Adware und Ransomware. Malware wird gewöhnlich auf einem Computer installiert, wenn ein Benutzer einen Link anklickt, einen schädlichen Anhang herunterlädt oder ein bösartiges Softwareprogramm öffnet. Sobald die Malware installiert ist, kann sie sensible Daten stehlen, löschen oder verschlüsseln. Sie kann auch wichtige Computerfunktionen lahmlegen und das gesamte System unbrauchbar machen.
- **Insiderbedrohungen:** Eine Insiderbedrohung ist ein Sicherheitsvorfall, der seinen Ursprung im Unternehmen hat und nicht von außerhalb kommt. Die Bedrohung kann von einem derzeitigen oder ehemaligen Mitarbeiter, einem Auftragnehmer, einem Drittanbieter oder einem anderen Geschäftspartner ausgehen, der Zugang zu den Daten und Computersystemen des Unternehmens hat. Insiderangriffe können besonders gefährlich sein, denn im Gegensatz zu externen Akteuren, die versuchen, ein Netzwerk zu infiltrieren, haben Insider oftmals legitimen Zugriff auf die Computersysteme eines Unternehmens.
- **Lieferkettenangriffe:** Angriffe auf die Lieferkette, auch als Drittanbieter-Angriffe bezeichnet, sind Versuche, ein Unternehmen unter Ausnutzung von Schwachstellen im Lieferkettennetzwerk zu schädigen. *Lieferkettenangriffe können mit nur einer einzigen Kompromittierung das gesamte Netzwerk infiltrieren.* Diese Bedrohungen sind oft schwieriger zu erkennen als herkömmliche Malware-Angriffe.

WARNUNG

Die menschliche Natur ist eine Schwachstelle, die Cyberkriminelle nur allzu gut auszunutzen wissen.

Profile und Motive von Angreifern

In der Populärkultur werden Hacker oft als Gestalten mit Kapuze dargestellt, die in einer dunklen Kammer vor ihrem Computer hocken, oder als verärgerte Teenager, die die Welt in Ordnung bringen wollen. Eines der bekanntesten Beispiele aus Hollywood ist die fiktive Hackerin Lisbeth Salander, die Hauptfigur in Das Mädchen mit der Drachen-Tätowierung (Millennium-Trilogie) von Stieg Larsson. Als die Figur zum ersten Mal vorgestellt wird, setzt sie ihre Hackerkenntnisse im Auftrag einer privaten Sicherheitsfirma ein. Im Laufe der Handlung wird deutlich, dass sie von Rache motiviert ist. Dank ihrer Hackerfähigkeiten gelingt es ihr schließlich, einen gewagten Finanzbetrug gegen einen der Hauptbösewichte der Geschichte zu begehen. Dieses Beispiel verdeutlicht, dass Menschen, die sich mit Cyberkriminalität befassen, von vielen unterschiedlichen Motivationen getrieben werden.

Um mit Hackern richtig umgehen zu können, muss sich Ihr Unternehmen mit den Motivationen der Cyberkriminellen befassen. Hier einige der Gründe, warum Hacker in Aktion treten:

- **Finanzieller Gewinn:** Geld ist der größte Anreiz für verbrecherische Aktivitäten. Das gilt auch für die Cyberkriminalität, die nichts anderes ist als Diebstahl im digitalen Zeitalter – und noch dazu wesentlich einfacher in der Durchführung als herkömmliche Banküberfälle. Trotz der Aufsehen erregenden Hackerangriffe auf große Markennamen nehmen Angreifer zunehmend kleine und mittlere Unternehmen mit schwächeren Sicherheitspraktiken ins Visier. Tatsächlich ist es für einen Hacker weitaus lukrativer, mehrere kleinere Unternehmen anzugreifen als ein Fortune-100-Unternehmen, das Millionen in die Stärkung seiner technologischen Verteidigungsmaßnahmen investiert hat.
- **Spionage:** Hacker betreiben oft Cyberspionage, um an geheime Informationen, geistiges Eigentum oder Geschäftsgeheimnisse zu gelangen. Spionage stellt heute eine ernstzunehmende Bedrohung für alle Unternehmen dar, ganz gleich, ob es sich um nationalstaatlich gelenkte Angriffe oder Unternehmensspionage handelt.

  Die zunehmende Zahl von Sicherheitsverletzungen in zwei Bereichen macht deutlich, woran Hacker besonders interessiert sind: Informationen aus der Politik und aus der Produktion.

  Auch kritische Infrastrukturbereiche wie Verkehr, Wasserversorgung, Telekommunikation und Versorgungsdienste können das Ziel staatlich gestützter Angriffe werden. Malware in den Händen staatlicher Akteure dürfte für alle Unternehmen, außer vielleicht den größten Organisationen mit den besten Ressourcen, eine erhebliche

NICHT VERGESSEN

Herausforderung darstellen. Erstaunlicherweise sind es in erster Linie die Mitarbeiter, die diese Angriffsvektoren ermöglichen. Social Engineering und unzulängliche Sicherheitspraktiken sind die ersten Bereiche, die sich Cyberkriminelle zunutze machen. Deshalb ist es wichtig, dass Unternehmen ihre eigenen Mitarbeiter mobilisieren und ihnen dabei helfen, sich vor diesen Bedrohungen zu schützen. Ein Programm zur Mitarbeitersensibilisierung ist für den Schutz Ihres Unternehmens unerlässlich.

- **Spaß:** Viele Hacker werden durch den Nervenkitzel und die Aufregung motiviert, die sie beim Eindringen in das Computersystem eines Unternehmens erleben. Beim diesjährigen Pwn2Own-Wettbewerb für ethisches Hacken gaben die Organisatoren den Teilnehmern zum Beispiel die Aufgabe, einen Tesla Model 3 zu hacken. Innerhalb eines Tages deckten zwei Hacker eine Sicherheitslücke auf, durch die sie in den internen Webbrowser des Fahrzeugs eindringen konnten. Das Duo kam jedoch nicht vor Gericht, sondern erhielt neben 375.000 Dollar Preisgeld einen Tesla Model 3, und vor allem die Anerkennung anderer Hacker – eine begehrte Währung in der Hacker-Community.
- **Hacktivismus:** Hacktivismus bezeichnet das Hacken eines Computersystems oder Netzwerks aus politischen oder sozialen Gründen. Es hat schon immer Menschen gegeben, die sich aktiv für eine Sache einsetzen, die der etablierten Ordnung zuwiderläuft. Das wird sich auch in Zukunft nicht ändern. Was sich jedoch geändert hat, ist die Allgegenwärtigkeit von Technologie.

  Technologie wird zunehmend als Waffe eingesetzt, um ideologische Ziele zu erreichen. Einer der Gründe dafür ist, dass Cyberangriffe viel billiger sind als direkte Militäraktionen.
- **Ressourcendiebstahl:** Die Ausnutzung öffentlicher Rechenressourcen für das Schürfen von Bitcoins ist zu einem einträglichen Geschäft geworden. Beim Bitcoin-Mining spielen Strom und Rechenleistung eine große Rolle, und Hacker nutzen jede Gelegenheit, sich diese Ressourcen anzueignen. Selbst multinationale Unternehmen wie Starbucks können ihnen zum Opfer fallen. Eine Starbucks-Filiale in Buenos Aires musste zum Beispiel vor kurzem feststellen, dass ihr WLAN gehackt worden war und von Betrügern genutzt wurde, um Bitcoin auf den Geräten ahnungsloser Kunden zu schürfen.
- **Andere Bedrohungen:** Zu dieser Kategorie gehören Insiderbedrohungen, unbeabsichtigte Datenlecks, Fehlkonfigurationen, Benutzerfehler und eine Reihe anderer Bedrohungen, die nichts mit Hackerangriffen durch Dritte zu tun haben. Die wahrscheinlichsten Methoden, die für Sicherheitsverletzungen genutzt werden, sind ungepatchte Software und Social Engineering. Diese Bedrohungen stellen für die meisten Unternehmen das größte Risiko dar.

Hier sind einige wichtige Fragen, die Sie in Ihrem Unternehmen stellen sollten: ***Was ist die beste Art, ein Sicherheitsmanagementsystem in meinem Unternehmen einzuführen, und welche Komponenten gehören dazu?***

Eine Antwort auf diese Frage bietet die Norm ISO/IEC: 27001, die einen Best-Practice-Ansatz für das Informationssicherheitsmanagement festlegt.

ISO/IEC 27001: Der globale Cybersicherheitsstandard

Der Schutz der Privatsphäre und der Datenschutz sind wichtige Initiativen für moderne Unternehmen. Maßnahmen, die darauf abzielen, die Bereitschaft der Belegschaft in diesen Bereichen zu erhöhen und aufrechtzuerhalten, stellen für jede Organisation ein erhebliches Unterfangen dar. Daher ist es wichtig, dass Mitarbeiter die nötige Zeit und angemessene Schulungen erhalten, um ihre mit dem Schutz der Privatsphäre verbundenen alltäglichen Verpflichtungen wirklich zu verstehen.

ISO/IEC 27001 ist nicht nur ein globaler Sicherheitsstandard, sondern auch die einzige Norm, die einer externen Prüfung unterzogen wird. Sie bietet Unternehmen die Möglichkeit, einen einheitlichen Ansatz zu verfolgen und nachzuweisen, dass sie sich an den Best Practices der Informationssicherheit orientieren. Viele Vorteile der ISO/IEC 27001 ergeben sich aus der Tatsache, dass das Zertifikat die Bereitschaft des Unternehmens für den Ernstfall demonstriert. Ein ISO/IEC 27001-Zertifikat ist ein Unternehmenswert, der ständig an Bedeutung gewinnt, da Kunden von ihrer Lieferkette ein hohes Maß an Sicherheit in Bezug auf Cyberrisiken erwarten.

Die Vorteile von ISO/IEC 27001

Da zur Erlangung der ISO/IEC 27001-Akkreditierung ein hohes Maß an Aufwand und Engagement seitens des Managements erforderlich ist, wird sichergestellt, dass das Unternehmen einen höheren Reifegrad in Bezug auf Cybersicherheit erreicht. Daneben gibt es jedoch noch weitere Vorteile:

- erhöhte Widerstandsfähigkeit des Unternehmens und Schutz vor Sicherheitsverletzungen
- größeres Kundenvertrauen
- erhöhte Zuverlässigkeit und Sicherheit von Kernsystemen und Informationsbeständen

- stärkere Konzentration auf Risiken und deren Auswirkungen auf das Geschäft

Um ISO/IEC 27001 zu erlangen, ist ein geeignetes System zur Mitarbeitersensibilisierung erforderlich. Speziell die Kapitel 7.2, 7.3 und 7.4 der ISO/IEC 27001 befassen sich mit dem Bewusstsein und dem Verständnis für das zu zertifizierende Informationssicherheitsmanagementsystem (ISMS). Allgemeine Cybersicherheitsschulungen reichen nicht immer aus, um die Anforderungen der Norm ISO/IEC 27001 zu erfüllen, zumal das ISMS jedes Unternehmens einzigartig ist, abhängig von den Risiken und Systemen, die seinen Tätigkeiten zugrundeliegen.

Mitarbeiter müssen mit der Funktionsweise der Sicherheitsprozesse in ihrem Unternehmen vertraut gemacht werden. Dazu ist in der Regel eine maßgeschneiderte Schulung über das ISMS des Unternehmens erforderlich. Eine auf Best Practice ausgerichtete Sensibilisierungskampagne umfasst die wichtigsten Cyberbedrohungen, von Phishing bis hin zu physischer Sicherheit, und unterstützt auch die Teilnahme an der ISO/IEC 27001-Initiative und ihr umfassendes Verständnis. Außerdem ist eine spezielle Schulung zum ISMS des Unternehmens erforderlich. Dabei kann es sich um eine einfache Veranstaltung wie ein unternehmensweites Webinar handeln, das einen Einblick in die Funktionsweise des Systems vermittelt.

TIPP

Wenn Ihr ISMS den Ausgangspunkt für Ihre Cyber-Sensibilisierungskampagne bildet, können Sie verhindern, dass sich die Benutzer überfordert fühlen: Sie müssen sich nur auf die konkreten Cyberbedrohungen konzentrieren , die für Ihr Unternehmen und Ihre Mitarbeiter tatsächlich relevant sind. Die von Ihrem ISMS vorgesehenen Maßnahmen können an die sich entwickelnde Bedrohungslandschaft angepasst werden. Das Wichtigste ist, dass Sie Ihre Mitarbeiter in diesen Prozess einbeziehen und sicherstellen, dass sie über alle Änderungen informiert werden.

Ein weiteres anerkanntes Rahmenwerk, das von Unternehmen auf der ganzen Welt zur Standardisierung von Prozessen, zur Risikominderung und zur Verbesserung ihrer Cybersicherheitsabläufe eingesetzt wird, ist das NIST Cyber Security Framework (siehe Seitenleiste).

NIST CYBER SECURITY FRAMEWORK

Das National Institute of Standards and Technology (NIST) hat das Cyber Security Framework (CSF) entwickelt, um Unternehmen einen Leitfaden zur Prävention, Erkennung und Reaktion auf Cybervorfälle an die Hand zu geben. Das international anerkannte Rahmenwerk fasst eine Reihe von

Best Practices, Standards und Empfehlungen zusammen, die Unternehmen bei der Verbesserung ihrer Cybersicherheitslage helfen sollen.

Das NIST CFS wurde ursprünglich zur Verbesserung von kritischen Infrastrukturdiensten entwickelt. Inzwischen wird es jedoch in den unterschiedlichsten Branchen eingesetzt und hilft vielen Unternehmen dabei, einen proaktiveren Risikomanagementansatz zu verfolgen.

Das Framework ist in drei Teile gegliedert:

- **Die Kernstruktur des Framework** enthält eine Reihe von Maßnahmen, mit denen bestimmte Ergebnisse im Bereich der Cybersicherheit erzielt werden können. Die Kernstruktur basiert auf fünf Funktionen:
  - **Identifizieren:** Entwicklung eines besseren Verständnisses für den Umgang mit Cybersicherheitsrisiken, denen die Systeme, Vermögenswerte, Daten und Fähigkeiten im Unternehmen ausgesetzt sind.
  - **Schützen:** Entwicklung und Umsetzung geeigneter Schutzmaßnahmen, um zu gewährleisten, dass kritische Infrastrukturdienste bereitgestellt werden.
  - **Erkennen:** Entwicklung und Umsetzung geeigneter Maßnahmen, um das Eintreten eines Cybersicherheitsereignisses zu erkennen.
  - **Reagieren:** Entwicklung und Umsetzung geeigneter Maßnahmen, um auf ein erkanntes Cybersicherheitsereignis reagieren zu können.
  - **Wiederherstellen:** Entwicklung und Umsetzung geeigneter Maßnahmen, um Pläne für die Widerstandsfähigkeit aufrechtzuerhalten und alle Fähigkeiten bzw. Dienste wiederherzustellen, die durch einen Cyber-Sicherheitsvorfall beeinträchtigt wurden.

Diese Funktionen sind in 22 Kategorien und 98 Unterkategorien eingeteilt.

- **Die Implementierungsstufen (Tiers)** geben einen Überblick darüber, wie Unternehmen Risiken wahrnehmen und welche Verfahren zur Minderung dieser Risiken eingesetzt werden können.
- **Das Profil** beschreibt die gewünschten Ergebnisse auf der Grundlage der Kategorien und Unterkategorien des Frameworks.

Sensibilisierung von Mitarbeitern bei digitalen Transformationsprojekten

Projekte zur digitalen Transformation sind spannende Initiativen. Sie bieten Unternehmen die Möglichkeit, sich neue Technologien zunutze zu machen und Produkte einzuführen, die zu Kostensenkungen und Ertragssteigerungen führen.

Digitale Transformationsprojekte basieren oft auf ehrgeizigen Strategien, die darauf abzielen, die Geschäftsabläufe eines Unternehmens mithilfe digitaler Technologien zu verbessern.

Sie sind wichtige Change-Management-Initiativen, die erhebliche Investitionen in die Mitarbeiterkommunikation erfordern. Diese Maßnahmen zielen darauf ab, die Unterstützung der Mitarbeiter zu gewinnen und sie zu motivieren. Oftmals wird bei diesen Initiativen jedoch ein wichtiges Risiko außer Acht gelassen: mangelnde Sorgfalt und Gewissenhaftigkeit im Bereich der IT-Sicherheit und Compliance. Sie sind jedoch unbedingt erforderlich, um ein Gleichgewicht zwischen einer Transformation um jeden Preis und angemessenen Kontrollen und Schutzmaßnahmen zu schaffen. Weitere Informationen über eine optimale Mitarbeiterkommunikation finden Sie in Kapitel3.

IN DIESEM KAPITEL

- **Risikoprofile**
- **Herausforderungen bei der Schaffung einer wachsameren Belegschaft**
- **Risikobewusstsein und Relevanz der Cybersicherheit**

Kapitel 2
Warum die Sensibilisierung für Cybersicherheit so wichtig ist

Nur wenige Leitfäden oder Handbücher enthalten konkrete Anleitungen zur Planung, Entwicklung und Umsetzung eines Cyber Security Awareness-Programms für Mitarbeiter. Dies liegt unter anderem daran, dass die IT-Sicherheitsbranche nach wie vor auf herkömmliche Technologien wie Firewalls und Anti-Malware-Lösungen fixiert ist. Diese technischen Schutzmechanismen vermitteln Unternehmen jedoch ein falsches Gefühl der Sicherheit und halten die Illusion aufrecht, dass der Perimeter effektiv verteidigt wird.

Trotz dieser hohen Investitionen in die Perimeter-Sicherheit gibt es nach wie vor ein gewisses Maß an „glaubhafter Abstreitbarkeit", dass diese Kontrollmechanismen durch die Handlungen eines einzelnen Mitarbeiters vollständig umgangen werden können.

Immer häufiger kommt es bei Blue-Chip-Unternehmen zu Daten-schutzverletzungen, und man ist sich weltweit darüber im Klaren, dass die Folgen dieser Vorfälle so schwerwiegend sind, dass sie

nicht mehr ignoriert werden können. Bei den meisten modernen Unternehmen befasst sich nun auch die Vorstandsetage verstärkt mit diesem Thema. Hinzu kommt, dass Aufsichtsbehörden zunehmend versuchen, mit Sanktionen und Geldstrafen die Einhaltung neuer Datenschutzvorschriften durchzusetzen. Diese und andere Makroeinflüsse machen eine grundlegende Änderung der Arbeitsweise von Mitarbeitern und ihrer Methoden zur Risikominderung erforderlich.

Eine Geschäftsleitung, die Cybersicherheitsrisiken als ernstzunehmende Geschäftsrisiken anerkennt, trägt wesentlich zum Reifeprozess eines Unternehmens bei. Der Erfolg eines Cyber Security Awareness-Projekts hängt in erster Linie davon ab, inwieweit die Geschäftsleitung des Unternehmens die Bedeutung von Cyberrisiken anerkennt und ob sie ihnen denselben Stellenwert einräumt und dieselben Ressourcen zuteilt wie Finanzrisiken. Kapitel 5 erklärt, warum es so wichtig ist, die Unterstützung der Geschäftsleitung für Ihre Kampagne zu gewinnen.

In diesem Kapitel wird ausführlich erläutert, wie Sie sicherstellen können, dass sich Ihr Unternehmen der Bedeutung des Themas Cybersicherheit bewusst ist.

Risikoprofile

Was wäre, wenn Ihr Unternehmen einem Hackerangriff zum Opfer fallen würde? Wie hoch ist die Wahrscheinlichkeit, dass es dazu kommt, und was wären die Auswirkungen? Um die Antworten auf diese Fragen zu verstehen, müssen Sie das einzigartige Risikoprofil Ihres Unternehmens kennen. Der Grad der Gefährdung Ihres Unternehmens hängt davon ab, in welchem Maß es Cyberbedrohungen ausgesetzt ist. Ein Best-Practice-Ansatz zur Verringerung des Cybersicherheitsrisikos in Ihrem Unternehmen besteht darin, diese Schwachpunkte so gut wie möglich zu verstehen und entsprechende Abhilfepläne aufzustellen. Dies gilt besonders in Bezug auf Ihre Mitarbeiter und Lieferketten, da diese häufig von böswilligen Dritten als Angriffswege genutzt werden.

Die folgenden Abschnitte enthalten praktische Informationen, die Ihrem Unternehmen bei der Reduzierung dieses Risikos helfen sollen.

Eine Kampagne zur Stärkung des Risikobewusstseins

Es ist wichtig, sich mit dem Mitarbeiterverhalten in Bezug auf Cybersicherheits- und Datenschutzrisiken auseinanderzusetzen. Eine Sensibilisierungskampagne zielt darauf ab, die mit dem menschlichen Aspekt der Cybersicherheit verbundenen Risiken zu reduzieren.

Kampagnen, deren Ziel lediglich in einer möglichst schnellen Cyber Security-Schulung der Belegschaft besteht, sind jedoch nur begrenzt erfolgreich. Für eine dauerhafte Verhaltensänderung sind kontinuierliche Schulungen und erhebliche Anstrengungen seitens des Unternehmens erforderlich - und viel Zeit, denn Menschen neigen von Natur aus dazu, sich Veränderungen zu widersetzen.

Verstehen Ihre Mitarbeiter die Risiken?

Ihr Unternehmen hat mehrere Möglichkeiten, das Verständnis seiner Mitarbeiter für Sicherheitsrisiken schnell zu bewerten. Sie können zum Beispiel Folgendes tun:

- **Senden Sie allen Mitarbeitern eine simulierte Phishing-E-Mail, um zu sehen, wie viele auf den Betrug hereinfallen.** Achten Sie besonders auf die Benutzer, die der Aufforderung nachkommen, Anmeldedaten oder wichtige Informationen einzugeben. Diese Klickrate kann Ihnen als wichtiger Ausgangspunkt dienen.
- **Führen Sie eine schnelle Analyse der Vorfälle der letzten 12 Monate durch.** Gibt es ähnliche Vorfälle, die auf einen Trend oder eine Wiederholung hindeuten? Setzen Sie im Hinblick auf diese Risiken Prioritäten für Ihr Sensibilisierungsprogramm.

Diese Informationen helfen auch, Mitarbeitern zu erklären, warum Cyber-Security-Schulungen so wichtig sind. Zum Beispiel: Im vergangenen Jahr gingen in diesem Unternehmen 20 Laptops verloren. Bitte informieren Sie sich über Best Practices im Gerätemanagement, indem Sie das beigefügte eLearning absolvieren.

Bedarfsorientierte Schulungen

Cyber Security Awareness-Initiativen sind effektiver, wenn sie kontextbezogen und segmentiert sind. Es ist zum Beispiel nicht sinnvoll, alle Mitarbeiter im Umgang mit Laptops und Geräten zu schulen, wenn nur wenige von ihnen einen Laptop besitzen. Diese Art von Schulung wird nur von den Mitarbeitern benötigt, die mit einem solchen Gerät arbeiten. Eine generische Sicherheitsschulung für die gesamte Belegschaft ist kontraproduktiv. Wenn möglich, sollte Ihr Unternehmen die Sensibilisierungsschulung auf die spezifische Rolle und die Risiken des Einzelnen abstimmen.

Sensibilisierungskampagnen haben mehr Wirkung, wenn sie sich auf verständliche Risiken beziehen und wenn die Mitarbeiter die realen Konsequenzen erkennen können, die sich aus nachlässigen Cybersicherheitspraktiken ergeben.

TIPP

Organisieren Sie IT-Sicherheitsrisiken in Bezug auf bestimmte Nutzergruppen und technische Ressourcen. Letzteres bezieht sich auf die kritischen Geschäftssysteme des Unternehmens und die in diesen Systemen gespeicherten Daten. Bei Sensibilisierungskampagnen ist es wichtig, dass die richtigen Botschaften zur richtigen Zeit an die richtigen Personen gelangen. Berücksichtigen Sie auch, dass manche Nutzer und Daten in Sachen Risikominimierung eine größere Bedeutung haben als andere.

Die Finanzabteilung ist zum Beispiel eher dem Risiko eines Cyberangriffs ausgesetzt als ein Mitarbeiter der Kantine. Bei der Erstellung einer Sensibilisierungskampagne spielt das Konzept der Gewichtung eine wesentliche Rolle, da es Ihnen hilft, Mitarbeitern mit hohem Risiko besondere Beachtung zu schenken, anstatt sich pauschal an alle zu wenden.

Wer braucht mehr Schulung?

Es ist äußerst effektiv, sich Zeit für die Ausarbeitung konkreter Mitteilungen oder die Durchführung geeigneter Schulungen für diese Mitarbeitergruppen zu nehmen, vor allem, wenn dies in einer ihnen vertrauten Sprache erfolgt.

Die Bestimmung besonders gefährdeter Mitarbeitergruppen nimmt Zeit in Anspruch. Die drei wichtigsten Gruppen, die zusätzliche Risikoschulungen benötigen, sind:

- **die Finanzabteilung:** Diese Abteilung ist in der Regel den meisten Risiken ausgesetzt, da sie die Kontrolle über die Finanzen des Unternehmens hat.
- **technische Benutzer mit Privilegien:** Diese Benutzer werden oft von Angreifern ins Visier genommen, weil sie privilegierten Zugang zu sicheren Systemen haben und daher zur Eskalation eines Cyberangriffs ausgenutzt werden können.
- **leitende Angestellte des Unternehmens:** Führungskräfte werden zur Zielscheibe für Angreifer, weil sie über Befugnisse verfügen, die zur Eskalation eines Cyberangriffs genutzt werden können.

Vergessen Sie auch nicht Ihre gesamte Lieferkette und Ihr Partnernetzwerk. Sie sind ebenfalls ein bedeutender Teil Ihres Risikoprofils. In Kapitel 3 wird ausführlicher beschrieben, wie Sie „kritische Dritte“ identifizieren können, welche Risiken in einem modernen, agilen Unternehmen von ihnen ausgehen und wie Sie sie in Ihre Cybersicherheitsaktivitäten einbeziehen können.

Auch wie lange ein Mitarbeiter schon im Unternehmen ist, hat Einfluss darauf, wie leicht sich sein Verhalten ändern lässt. Neuen Nutzern fällt

es oft leichter, Richtlinien zu akzeptieren und neue Arbeitsmethoden zu erlernen, weil sie eine flexiblere Denkweise haben. Bei langjährigen Mitarbeitern kann das Erlernen neuer Methoden problematischer sein.

Bei der Erstellung eines Risikoprofils ist es außerdem wichtig, die Anzahl der in Ihrem Unternehmen verwendeten Sprachen zu ermitteln. Die Einbeziehung mehrerer Sprachen macht die Umsetzung des Sensibilisierungsprogramms nicht nur schwieriger, sondern erhöht auch die Anzahl der Bedrohungsvektoren für Ihr Unternehmen.

Ein Unternehmen, das in Brasilien tätig ist, muss sich zum Beispiel mit Phishing-E-Mails auf Portugiesisch und Englisch auseinandersetzen. Es ist wichtig, kulturelle und sprachliche Zielgruppen zu identifizieren, damit das Sensibilisierungsprogramm für sie relevant ist.

Priorisierung von Sicherheitsrisiken

In vielen Unternehmen wird Mitarbeitern nicht deutlich gemacht, dass die IT-Sicherheit ebenso wichtig ist wie die Bekämpfung finanzieller Risiken. Wenn Cybersicherheit nicht als notwendiger Aspekt des normalen Geschäftsbetriebs angesehen wird, entwickeln Benutzer mit der Zeit schlechte Gewohnheiten. Dies macht die Durchführung einer Sensibilisierungskampagne schwieriger. Die Kampagne muss Benutzer nicht nur in Sachen Sicherheit aufklären, sondern auch zur Überwindung schlechter Gewohnheiten beitragen, die sich im Laufe der Zeit entwickelt haben. Nur wenn Ihr Unternehmen konsequent vorgeht und die Botschaften seiner Kampagne ständig wiederholt, kann es seine Mitarbeiter für das Thema gewinnen.

Oft werden veraltete und schwer zu ändernde Systeme als Grund dafür angeführt, dass Verhaltensänderungen nicht notwendig sind. Haben Sie schon einmal den Spruch gehört: „Unser System funktioniert nun einmal so. Es hat keinen Sinn, etwas daran ändern zu wollen.“ Es ist nicht leicht, diese Denkweise zu überwinden.

Sicherheitsprobleme im Zusammenhang mit veralteten Systemen können bei der Betrachtung von Sicherheitsbedrohungen zu einem Gefühl der Hoffnungslosigkeit führen. Wenn zum Beispiel ein Zugangskontrollsystem auf einem veralteten Windows-Betriebssystem verwaltet wird, ist es verständlich, dass der Austausch aller elektronischen Schlösser im Unternehmen bei einem ansonsten einwandfrei funktionierenden System nicht unbedingt die beste Investition ist.

Derartige Altsysteme müssen jedoch so schnell wie möglich modernisiert werden. Mitarbeiter müssen wissen, dass das Unternehmen diese Herausforderungen erkannt hat und sie aktiv in Angriff nimmt. Dies sind zwar im Hintergrund stattfindende Maßnahmen, die nicht in den

Rahmen eines Sicherheitsprogramms für Mitarbeiter fallen, doch Fortschritte in diesen Bereichen sind für die Integrität einer auf Mitarbeiter gerichteten Sensibilisierungskampagne unerlässlich.

Mitarbeiter für Cybersicherheitsprogramme gewinnen

Cyber Security Awareness-Programme werden wahrscheinlich keine große Begeisterung auslösen, weder bei der Belegschaft noch beim Management.

NICHT VERGESSEN

Bei der Erstellung eines Schulungsprogramms für mehr Achtsamkeit im Umgang mit Cybergefahren ist zu beachten, dass die meisten Menschen, wenn überhaupt, gedanklich sehr wenig Zeit auf dieses Thema verwenden. Es ist schwer, Interesse für Cybersicherheit zu wecken. Ein Unternehmen hat jedoch die Aufgabe, für seine Mitarbeiter die Kommunikation zum Thema Sicherheit schmackhaft und wenn möglich sogar angenehm zu gestalten.

Die Beteiligung der Benutzer an Ihren Cybersicherheitsprogrammen ist eine der wichtigsten Kennzahlen für den Erfolg. Wenn Sie zum Beispiel eine Risikobewertung oder ein eLearning-Programm versenden und nur 50 Prozent Ihrer Mitarbeiter daran teilnehmen, haben Sie ein großes Problem. Ein wesentlicher Teil Ihrer Zielgruppe ist einfach nicht daran interessiert. Vor allem aber kann Ihr Unternehmen keine Compliance-Nachweise erbringen. Außerdem gehören die „Sorgenkinder" Ihres Cybersicherheitsprogramms wahrscheinlich zu den 50 % der Mitarbeiter, die nicht auf die Mitteilung reagiert haben.

Ihr Unternehmen hat drei Möglichkeiten:

- Das Management kann die Personen, die sich nicht beteiligt haben, einfach ignorieren und auf das Beste hoffen. Dieser Ansatz mag populär sein, doch letztlich ist er zum Scheitern verurteilt. Regulierungsbehörden erwarten Nachweise, die belegen, dass Sie sich um die Einbeziehung dieser Nutzer in das Sensibilisierungsprogramm bemüht haben.
- Das Management kann Benutzer an die Erfüllung ihrer Cyber Awarenes-Pflichten erinnern. Dies ist jedoch ein mühsamer und für das Management frustrierender Prozess, der die Informationssicherheit letztendlich weiter ins organisatorische Abseits drängt.

» Technologielösungen können Benutzer zur Beteiligung bewegen, sie verärgern, anspornen, mitreißen und schließlich dazu bringen, ihre Sicherheitsaufgaben zu erfüllen.

Letztendlich muss die Cyber-Sensibilisierungskampagne den Benutzer ansprechen, und dazu sind gute Medien, Grafiken und eLearning erforderlich. Wählen Sie deshalb die beste eLearning-Lösung, die Sie sich leisten können. Diese muss die wichtigsten Sprachen in Ihrem Unternehmen abdecken und den Benutzern die Möglichkeit geben, selbst die Sprache auszuwählen, in der sie die Inhalte verwenden möchten.

Risikomanagement und Relevanz

Fast alle Unternehmen sind heutzutage mit einem digitalen Transformationsprojekt beschäftigt. Sie erkunden neue Möglichkeiten zur Effizienz- und Umsatzsteigerung und machen sich neue Geschäftsmodelle zunutze, die sich durch Marktveränderungen und die Einführung von Technologien wie Cloud, Datenmanagement und Mobilfunk ergeben. Diese Projekte haben in jedem Unternehmen einen hohen Stellenwert und werden vom Vorstand und der Geschäftsleitung meist aufmerksam verfolgt und unterstützt.

Datenschutzgesetze wie die Datenschutz-Grundverordnung (GDPR) haben „Privacy by Design“ und „Security by Design“ in den Mittelpunkt neuer digitaler Initiativen gestellt. In einigen Regionen müssen Unternehmen eine Folgenabschätzung durchführen und die Auswirkungen neuer Systeme, Verfahren oder Geschäftsmodelle auf den Datenschutz bewerten. Datenschutz- und Informationssicherheitsexperten müssen sicherstellen, dass die für die digitale Transformation zuständigen Teams sich dieser Anforderungen bewusst sind und dass die neuen Systeme oder Ansätze geeignete Kontrollen und Kommunikationsmöglichkeiten für Mitarbeiter bieten.

NICHT VERGESSEN

Wenn die mit einem digitalen Transformationsprojekt zusammenhängende Kommunikation in Ihr jährliches Cyber Security Awareness-Projekt einbezogen wird, erhöht dies die Relevanz für das Unternehmen und trägt dazu bei, den Stellenwert der Sicherheit im Führungsteam zu erhöhen. Ein Vorsprung bei diesen neuen digitalen Projekten hilft Mitarbeitern außerdem dabei, die Informationssicherheit als förderlich und nicht als hemmend zu betrachten Letztes tritt unweigerlich ein, wenn Sicherheitskontrollen bei dieser Art von Initiativen zu spät eingeführt werden.

Wenn die Geschäftsleitung die Eignung eines digitalen Transformationsprojekts prüft, bewertet sie gemeinsam mit den potenziellen Vorteilen bereits unterschiedliche Geschäftsrisiken. Die Herausforderung besteht darin, das Projekt aus einer Risikoperspektive zu betrachten und sicherzustellen, dass Sicherheits- und Datenschutzrisiken dieselbe Bedeutung eingeräumt wird wie finanziellen und anderen geschäftlichen Risiken. Digitale Transformationsprojekte bieten die Möglichkeit, das Bewusstsein für Cybersicherheit im Rahmen einer viel größer angelegten Unternehmensinitiative zu vermitteln.

IN DIESEM KAPITEL

- Effektive Kommunikation
- Der Apathie entgegenwirken
- Mitarbeiter verbreiten die Botschaft
- Beziehungen zu Dritten

Kapitel 3
Sensibilisierungskampagnen zur Veränderung der Unternehmenskultur

Viele Unternehmen möchten sofort mit ihrem Programm zur Sensibilisierung für Cybersicherheit beginnen und eLearning und simulierte Phishing-E-Mails an Benutzer verschicken. Dieser Ansatz ist jedoch zum Scheitern verurteilt, wenn das Hauptziel – Verhaltensänderungen im Umgang mit Cyberrisiken zu bewirken – außer Acht gelassen wird. Sobald Sie das Konzept der Verhaltensänderung ins Spiel bringen, bewegen Sie sich im Bereich des Change-Managements. Wie jedes Unternehmen weiß, ist die Umsetzung von Change-Management-Programmen äußerst schwierig. Die besten Security-Awareness-Programme gehen an diese Aufgabe auf dieselbe Weise heran wie an andere Veränderungsprojekte im Unternehmen. Eine multidisziplinäre Gruppe wird zusammengestellt, zu der Projektmanager, interne Marketingexperten sowie HR- und IT-Fachkräfte gehören, um das im Unternehmen vorhandene Fachwissen in das Projekt einzubringen.

Dabei ist es keine Selbstverständlichkeit, dass auch wirklich Veränderungen erreicht werden. Der Prozess erfordert viel Zeit und ein hohes

Maß an Willenskraft und Anstrengung. Kein Wunder, dass das Management manchmal die Hände über dem Kopf zusammenschlägt und sich fragt, ob das Sensibilisierungsprojekt überhaupt notwendig ist und ob es jemals enden wird.

Diese Zweifel treten meist dann auf, wenn die Sensibilisierungskampagne mit anderen Kommunikationsinitiativen des Unternehmens zusammenfällt. Unter diesen Umständen kann es vorkommen, dass die Nutzerbasis protestiert. In der Planungsphase kann das Unternehmen diesen Spannungen entgegenwirken, indem es den Umfang und die Häufigkeit der Awareness-Kommunikation für einen begrenzten Zeitraum reduziert. Wichtig ist, dass das Programm nicht unterbrochen wird, da es sonst wahrscheinlich nie wieder in Gang kommt.

Dieses Kapitel enthält Empfehlungen zur Umsetzung einer erfolgreichen Sensibilisierungskampagne. Sie erfahren, wie Sie eine effektive Kommunikation einsetzen, Apathie überwinden, die Botschaft mithilfe von Mitarbeitern verbreiten und externe Auftragnehmer einbeziehen können.

Effektive Kommunikation

Ihre Sensibilisierungskampagne muss speziell auf die Bedürfnisse Ihres Unternehmens zugeschnitten sein. Damit die Kampagne Ihre Botschaft erfolgreich vermittelt, sollten Sie Folgendes tun:

- **Verwenden Sie Ihr Logo, um Ihrer Kampagne in den Köpfen Ihrer Nutzer einen hohen Wiedererkennungswert und Gewicht zu verleihen.** Da Ihre Mitarbeiter wahrscheinlich auch privat viel audiovisuellen Content konsumieren, sollten Sie sicherstellen, dass Ihre Schulungsinhalte als besonders wichtige und relevante Inhalte präsentiert werden. Allerdings ist jede Art von Cyber-Awareness besser als gar keine.
- **Passen Sie Ihre Botschaften an die Bedrohungen an, mit denen Ihre Mitarbeiter täglich konfrontiert werden.** Vermeiden Sie es, Schulungen nur zur Schau durchzuführen, um sagen zu können, dass Ihr Unternehmen ein Sensibilisierungsprogramm hat.

  Die meisten Mitarbeiter, die Cyberrisiken und deren persönliche und geschäftliche Folgen verstehen, werden positiv auf Ihre Kampagne reagieren und ihr Verhalten ändern. Nehmen Sie sich genug Zeit, um Ihre Botschaften richtig zu formulieren. Wenn das nicht zu Ihren Stärken oder denen Ihrer Teammitglieder gehört, dann

NICHT VERGESSEN

wenden Sie sich an Ihr Marketingteam. Sie können auch externe Hilfe in Anspruch nehmen.

TIPP

Ihre Nutzerpopulation kann nur eine begrenzte Informationsfülle zu diesem Thema verkraften. Fangen Sie daher klein an und bauen Sie Ihre Kampagne über einen Zeitraum von 12 Monaten auf. Wie viele eLearning-Kurse würden Sie selbst in einem Monat absolvieren wollen, auch wenn sie noch so kurz wären? Wenn Ihre Zielgruppe bisher noch keine derartige Schulung erhalten hat, sollten Sie in den ersten sechs Monaten ein eLearning pro Monat durchführen, damit die Mitarbeiter nicht überfordert werden.

NICHT VERGESSEN

Bevor Sie das Schulungspensum erhöhen, sollten Sie sich auch fragen, wie viele Cybersicherheitsrichtlinien, simulierte Phishing-Angriffe und Risikobewertungen Ihre Benutzer in den ersten sechs Monaten bewältigen können. Das alles summiert sich! Besprechen Sie mit dem Führungsteam, in welchem Maße die Nutzerbasis zur Konsumierung dieser Inhalte motiviert werden soll, damit die Sensibilisierungskampagne nicht vorzeitig endet. Erfahrungsgemäß gilt die Regel: Weniger ist mehr. Sie müssen Ihre Zielgruppe sozusagen mit auf Ihre Reise nehmen.

Bei vielen Sensibilisierungskampagnen werden die Nutzer nicht darüber informiert, warum Cybersicherheit für sie wichtig ist und warum das Informationssicherheitsmanagementsystem (ISMS) eine entscheidende Rolle bei der Abwehr von Cyberbedrohungen spielt. Machen Sie den Nutzern bei der Kommunikation dieser umfassenden Initiative klar, dass die Cybersicherheit in der heutigen digitalen Welt ein wichtiger Bestandteil des normalen Geschäftsbetriebs ist.

Der Apathie entgegenwirken

Normalerweise ist es nicht schwer, die Unterstützung der Geschäftsleitung für ein Projekt zur Förderung des Sicherheitsbewusstseins im Unternehmen zu gewinnen. Führungskräfte sind sich des Risikos von Geldbußen und Reputationsschäden nur allzu deutlich bewusst. Es kommt jedoch häufig vor, dass eine Kampagne gestartet wird und sechs Monate später durch die Trägheit des Unternehmens mit schlechten Ergebnissen endet. Bei Sensibilisierungsprojekten wird häufig versäumt, einen vorhersehbaren Kommunikationszyklus einzurichten und aufrechtzuerhalten.

Die meisten Mitarbeiter und Führungskräfte müssen gleich zu Beginn darüber informiert werden, dass die Sicherheitskampagne Teil einer langfristigen Strategie zur Verbesserung der Cyberabwehr im

Unternehmen ist. Es muss von Anfang an klar sein, dass es sich nicht um eine einmalige Initiative handelt. Deshalb ist es wichtig, wiederholbare Kommunikationsabläufe festzulegen. Regelmäßige Benachrichtigungen über Schlüsselbotschaften, Schulungen und Bewertungen sorgen dafür, dass sich alle Nutzer über die Bedeutung der Kampagne im Klaren sind. Integrieren Sie außerdem eine Feedback-Schleife in Ihre Kommunikation, damit die Geschäftsleitung frühzeitig über die Meinungen der Mitarbeiter informiert wird. Dieses Feedback kann vom Management genutzt werden, um die gesamte Sensibilisierungsinitiative im Laufe der Zeit zu verbessern und den zeitlichen Ablauf der aktuellen Kampagnen entsprechend anzupassen.

Da im Laufe des Jahres immer wieder aktive Cyberbedrohungen auftreten, ist es für das Management schwierig, die Aufmerksamkeit der Mitarbeiter das ganze Jahr über aufrechtzuerhalten. Cybersicherheit erfordert so viele Maßnahmen zur „Brandbekämpfung", dass kaum Zeit für die Ausarbeitung von Botschaften für das Sensibilisierungsprogramm übrigbleibt.

TIPP

Nehmen Sie sich zu Beginn des Jahres eine Woche Zeit, um die für die nächsten 12 Monate erforderlichen Sensibilisierungsmaßnahmen festzulegen (Richtlinien, Bewertungen, eLearning, simulierte Phishing-Angriffe, Blogs, Wettbewerbe, Veranstaltungen an Cyber-Sicherheitstagen). Legen Sie die Häufigkeit der Kommunikation nach eigenem Ermessen fest. Sichern Sie sich die Unterstützung der Geschäftsleitung, bevor Sie Ihren Plan in die Tat umsetzen. Gehen Sie nicht in kleinen Schritten vor, indem Sie zum Beispiel nur für die bevorstehenden drei Monate planen, da Sie sonst im Laufe des Jahres unweigerlich aus der Bahn geraten. Legen Sie stattdessen eine 12-monatige Kampagne fest und überprüfen Sie deren Fortschritte regelmäßig.

EINE DATENPANNE ALS KATALYSATOR FÜR VERÄNDERUNGEN NUTZEN

Ein gezielter Cyberangriff, der zu einer Verletzung der Datensicherheit führt, bringt gewöhnlich nichts Gutes mit sich. Auch im Lebenslauf eines Sicherheitsexperten sieht eine solche Erfahrung nicht besonders beeindruckend aus. Und trotzdem ist der Umgang mit einem größeren Cybervorfall ein wichtiges Ereignis, das zur Reifung von Führungskräften im Bereich des Informationssicherheitsmanagements beiträgt.

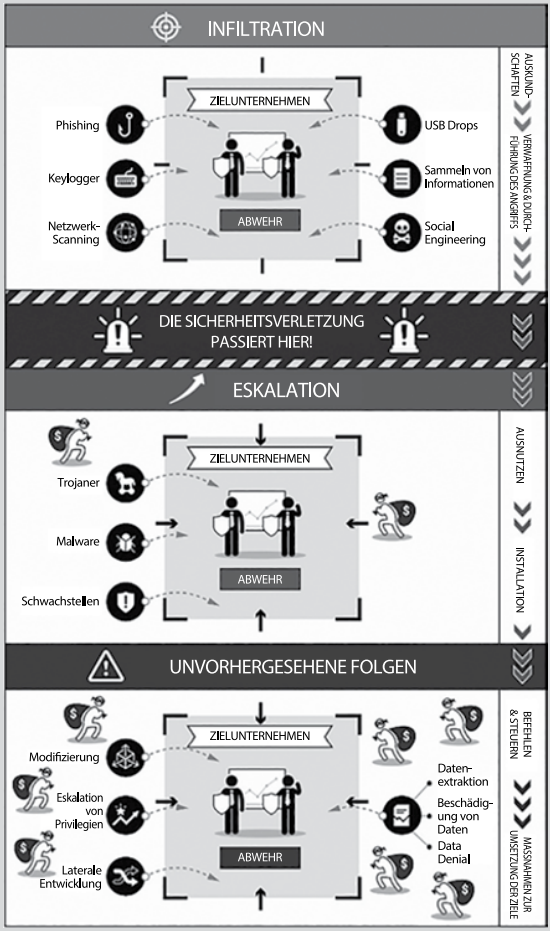
Ein Unternehmen, das eine Datenschutzverletzung (oder einen Beinahe-Vorfall) erlebt hat, verfügt über einen funktionierenden Incident-Response-Plan, während andere oft abwarten und nichts tun. Bei einem erfahrenen Managementteam kann man davon ausgehen, dass eine angemessene Notfallplanung stattgefunden hat.

Eine Datenschutzverletzung oder ein Beinahe-Vorfall hat also doch etwas Gutes an sich: Die Geschäftsleitung kann sich nicht mehr in Wunschdenken ergehen oder glaubwürdige Abstreitbarkeit einfordern. Sie muss in Aktion treten.

Zwar sind sich alle im Unternehmen der möglichen Bedrohungen bewusst und wissen, dass die Wahrscheinlichkeit eines Cyberangriffs hoch ist, doch Investitionen in Cyber Security Awareness sind nach wie vor unpopulär, und die Geschäftsleitung gibt sich gern mit einer Minimallösung zufrieden. Der Security-Branche kommt dabei eine gewisse Verantwortung zu, da sie die neueste Perimetertechnologie als Allheilmittel für alle Sicherheitsprobleme anpreist und dabei vergisst, dass die Person hinter der Firewall der einfachste Weg zur Umgehung der Schutzmaßnahmen ist.

Datenschutz-, Compliance- und IT-Sicherheitsexperten sollten sich jedoch davor hüten, das Management mit der Androhung von Bußgeldern zum Handeln zu bewegen. Besser ist es, die geschäftlichen Vorteile hervorzuheben, durch die sich Ihr Unternehmen von weniger sicherheits- und regelkonformen Organisationen abheben kann. Der sich daraus ergebende Wettbewerbsvorteil muss intern als Grund für Investitionen angeführt werden, speziell zur Veränderung der Mitarbeiterkultur.

Kurz nach einer Sicherheitsverletzung oder einem Beinahe-Vorfall, noch bevor das Ganze rationalisiert werden kann, hat das Management die einmalige Gelegenheit, das Führungsteam für das Anliegen der Informationssicherheit zu gewinnen und die erforderliche Unterstützung einzuholen. Diese Investitionen fließen meist in Arbeitskräfte und Lösungen, doch am wertvollsten ist letztendlich der zeitliche Einsatz dieser Gruppe. Die folgende Abbildung zeigt den typischen Zeitverlauf einer Datenschutzverletzung.



Cyber Security Champions

Allen Mitarbeitern muss klar sein, dass nicht nur die IT-Abteilung für die Bewusstseinsbildung im Bereich Informationssicherheit und Datenschutz verantwortlich ist. Vielmehr wollen Sie erreichen, dass sich *jeder* im Unternehmen für die digitale Sicherheit verantwortlich fühlt.

Eine Sensibilisierungskampagne braucht möglichst viele Mitstreiter. Sicher gibt es in Ihrem Unternehmen bereits Mitarbeiter, die in Sachen

Cybersicherheit besonders aktiv sind, über Vorfälle wie simulierte Phishing-Angriffe berichten und Feedback geben. Diese Mitarbeiter wissen genau, welche Schäden dem Unternehmen durch Cyberrisiken entstehen können. Arbeiten Sie mit diesen Nutzern zusammen. Nehmen Sie ihre Hilfe in Anspruch, um sicherzustellen, dass jeder seine Verantwortung versteht. Diese *Champions* sind gute Kommunikatoren. Sie sind sympathisch und können hervorragend mit Menschen umgehen. Sie sind wertvolle Helfer für Ihre Kampagne. Bitten Sie Ihre Kollegen in anderen Abteilungen, Ihnen bei der Suche nach möglichen Champions zu helfen.

TIPP

Das Management sollte ein Botschafterprogramm einführen, um sich die Unterstützung der engagiertesten und interessiertesten Mitarbeiter des Unternehmens zu sichern: Ihrer Champions. Ihr Botschafterprogramm braucht unternehmensweite Unterstützung und muss von der Führungsebene gefördert werden. Mit der Unterstützung der Geschäftsleitung können Sie Ihr Botschafterprogramm offiziell einführen und Ihren Mitarbeitern die gebührende Anerkennung zuteilwerden lassen.

Vielleicht haben Sie bereits Mitarbeiter, die sich an vorderster Front für Informationssicherheit und Datenschutz einsetzen. Diese Mitarbeiter sind im Sinne von ISO/IEC 27001 vielleicht zu Verantwortlichen für Informationswerte oder für Datenverarbeitungstätigkeiten ernannt worden. Möglicherweise haben sie auch schon eine einschlägige Schulung zum Thema Datenschutz oder Informationssicherheit absolviert.

Versuchen Sie, jeden Erfolg zu feiern. Bauen Sie Ihre Kampagne auf Positivität auf. Feiern Sie die erfolgreiche Rezertifizierung von ISO/IEC 27001 und alle anderen Errungenschaften auf diesem Gebiet.

TIPP

Wenn möglich sollte Ihr Cyber Security Champions-Programm über einen eigenen Kommunikationskanal in einem internen Messaging-Tool wie Microsoft Teams oder Slack verfügen, damit Sie regelmäßig Feedback über den Stand Ihres Sensibilisierungsprojekts erhalten. Dieser Kommunikationskanal kann zumindest dafür genutzt werden, um die Champions über alle Datenschutzverletzungen und Beinahe-Vorfälle zu informieren.

Die Einführung eines Cyber Security Champion-Programms ist ein zufriedenstellender Teil einer erfolgreichen Sensibilisierungskampagne, da es die Unterstützung für Ihre Veränderungsinitiative im gesamten Unternehmen „einbettet“. Es dient auch als Frühwarnsystem, wenn die Kampagne ins Stocken geraten sollte oder nicht die gewünschten Ergebnisse erzielt.

Durch ihre Handlungen und ihr Engagement können Champions demonstrieren, dass Sensibilisierungsprogramme das gesamte Unternehmen dazu veranlassen, diese Best Practices in den Geschäftsalltag zu integrieren.

Einbeziehung Dritter in Sensibilisierungsinitiativen

In den letzten 20 Jahren hatten die meisten Unternehmen Schwierigkeiten beim Management von Lieferanten- und Drittanbieter-Risiken, nicht zuletzt, weil viele von ihnen spezielle Aufgaben und nicht zum Kerngeschäft gehörende Tätigkeiten an vertrauenswürdige Partner ausgelagert hatten. Bei einigen modernen Unternehmen sind bis zu 50 % der Mitarbeiter keine Vollzeitbeschäftigten. Durch die Vergabe von Unteraufträgen entsteht eine besser skalierbare und agilere Organisation. Der Nachteil ist, dass dieser Ansatz auch Auswirkungen auf die Durchführung von Sensibilisierungskampagnen hat. In den folgenden Abschnitten wird erläutert, welche Unterauftragnehmer Sie in Ihren Sensibilisierungsplan einbeziehen sollten und mit welchen technologischen Herausforderungen sie möglicherweise rechnen müssen.

Wer soll einbezogen werden?

In welchem Umfang Unterauftragnehmer an Ihrem Sensibilisierungsprogramm teilnehmen sollten, hängt davon ab, wie stark sie in Ihr Unternehmen integriert sind. Drittanbieter, die mit Ihren Informationsbeständen, Datenverarbeitungstätigkeiten und Ihrem Netzwerk in Kontakt stehen, sollten zumindest bei der Planung Ihrer Sensibilisierungskampagne berücksichtigt werden. Gegebenenfalls sollte Ihr Unternehmen bestimmen, zu welchen Drittanbietern es besonders schwierige oder risikoreiche Beziehungen unterhält, um dann die notwendigen Kommunikationsmaßnahmen für jedes Segment festlegen zu können. Jeder, der auf Ihre internen Systeme zugreift, sollte zumindest Ihre Richtlinie zur akzeptablen Nutzung unterzeichnen. Auf dieser Grundlage können Sie dann weitere Anforderungen in Bezug auf Richtlinien und Schulungen aufstellen.

Fachberater und technische Experten vertrauenswürdiger Drittanbieter können zum Beispiel Zugang zu sensiblen Daten haben oder müssen auf wichtige Systeme zugreifen, besonders auf Datenbanken, die Finanz-, Personal- und Unternehmensdaten enthalten. Diese externen Mitarbeiter müssen über ihre Verpflichtungen beim Zugriff auf die digitalen Bestände Ihres Unternehmens unterrichtet werden.

Genau wie bei festangestellten Mitarbeitern muss das Management auch externe Auftragnehmer nach ihrem Risiko für das Unternehmen einstufen. Je größer das Risiko, desto mehr Kontrollen sind erforderlich. Einigen Sie sich mit Ihrem Unterauftragnehmer zum Zeitpunkt des Vertragsabschlusses über diese Kontrollmaßnahmen. Dabei kann es sich um eine Schulung oder eine Bescheinigung handeln, dass der Unterauftragnehmer Ihre Richtlinien gelesen und verstanden hat. Diese Voraussetzungen sollten in Ihre standardmäßigen Geschäftsbedingungen aufgenommen werden. Sie sind ein wichtiger Bestandteil Ihrer Beziehungen zu Lieferanten, die Zugang zu Ihren IT-Systemen haben.

Potenzielle technologische Herausforderungen

Manchmal muss ein Unternehmen große technologische Herausforderungen überwinden, um Dritte in seine Sensibilisierungsinitiative einzubeziehen. Es kann zum Beispiel vorkommen, dass Drittanbieter an entfernten Standorten nicht in der Lage sind, auf ein vor Ort installiertes Lernmanagementsystem (LMS) zuzugreifen, um das erforderliche eLearning zu absolvieren. Dasselbe Problem kann bei der Einhaltung wichtiger Richtlinien auftreten, die die Beziehung zwischen dem Unternehmen, dem Anbieter und dem Mitarbeiter regeln, der die jeweilige Dienstleistung erbringt. Früher wurde die Einbeziehung Dritter in derartige Sicherheitsinitiativen von Unternehmen oft vernachlässigt. Das Lieferantenmanagement und die mit der Zusammenarbeit mit Drittanbietern verbundenen Cyberrisiken bereiten dem IT-Management jedoch immer mehr Sorgen und stehen im Mittelpunkt mehrerer internationaler Datenschutzgesetze.

Schrittweise Sensibilisierung von Drittanbietern

Ein schrittweiser Ansatz zur Einbeziehung von Drittanbietern in Ihre Cyber-Awareness-Kampagnen ist die sinnvollste Methode, um die Beziehung zu ihnen zu optimieren. Zunächst benötigen Sie eine Lösung zur Verwaltung Ihrer wichtigsten Richtlinien und ein zuverlässiges Verfahren zur Einholung von Bescheinigungen – idealerweise eine elektronische Lösung zur Richtlinienverwaltung, die diesen Prozess automatisieren kann. Wenn es darum geht, unterzeichnete Dokumente in einem zentralen Ordner unterzubringen, ist Papier eine denkbar schlechte Lösung. Ermitteln Sie die Hauptrisiken jedes Unterauftragnehmers und bieten Sie dann entsprechende Schulungen an, möglichst über ein cloudbasiertes LMS, auf das der Unterauftragnehmer entweder aus der Ferne oder über Ihre Systeme zugreifen kann, bevor er zum Einsatzort kommt.

WARNUNG

Sie können auch in Erfahrung bringen, welche unerwünschten Verhaltensweisen Ihre Mitarbeiter in der Lieferantengemeinschaft an den Tag legen. Tailgaiting könnte zum Beispiel genauso gut durch einen Ihrer eigenen Mitarbeiter wie durch einen Unterauftragnehmer ermöglicht werden. Ihre interne Sensibilisierungskampagne deckt die physische Sicherheit durch Richtlinien und Schulungen ab. Stellen Sie sicher, dass auch der Unterauftragnehmer zu diesen Themen geschult wird.

Durch die Ausweitung Ihrer Sensibilisierungskampagne können Sie beurteilen, inwieweit ein Anbieter in seinem eigenen Umfeld entsprechende Schulungen durchführt und seine Mitarbeiterrichtlinien verwaltet. Diese Bewertung ist Teil der Due-Diligence-Prüfung des Anbieters, einem integralen Bestandteil des Onboarding-Prozesses in Ihrem Unternehmen. Viele Unternehmen senden ihren Lieferanten vor Vertragsabschluss eine Risikobewertung. Im Rahmen dieser Bewertung kann Ihr Unternehmen dem Anbieter Fragen zur allgemeinen Informationssicherheit wie Firewalls und Virenschutz stellen, um seine Bereitschaft zur Sensibilisierung für Cyberrisiken zu bewerten. Ein Anbieter, der keinen Nachweis über eine Richtlinien oder ein Schulungsprogramm zur Informationssicherheit erbringen kann, wird die Anforderungen Ihrer Sensibilisierungskampagne wohl kaum erfüllen.

IN DIESEM KAPITEL

- **Warum Richtlinien für eine Sensibilisierungskampagne wichtig sind**
- **Identifizierung von Risiken**
- **Richtlinienschulung für langjährige und neue Mitarbeiter**
- **Die Vorteile einer zentralisierten Technologiearchitektur**

Kapitel 4
Richtlinienmanagement in Ihr Sensibilisierungsprogramm integrieren

Unter einer Richtlinie versteht man eine Reihe von Regeln bzw. einen Plan, der das Verhalten in bestimmten Situationen vorschreibt und auf den sich eine Gruppe von Personen, ein Unternehmen, eine Organisation, eine Regierung oder eine politische Partei offiziell geeinigt hat.

Richtlinien legen also fest, was in bestimmten Situationen zu tun ist. Ihre Sensibilisierungskampagne braucht klare Richtlinien. Das Management hat festgelegt, was Mitarbeiter in bestimmten Situationen tun sollen. Richtlinien müssen den Mitarbeitern mitgeteilt werden. Wie kann man erwarten, dass sie das Richtige tun, wenn man ihnen nicht sagt, wie sie sich in bestimmten Situationen zu verhalten haben?

Dieses Kapitel erläutert, wie Richtlinien die Sensibilisierungskampagne für Cybersicherheit in Ihrem Unternehmen unterstützen.

Die Rolle von Richtlinien bei einer Kampagne

Die in einem Unternehmen festgelegten Richtlinien sind wie das Gesetzeswerk, mit dem eine Regierung die Gesellschaft verwaltet. Sie legen fest, wie das Unternehmen auf Cybersicherheitsbedrohungen reagiert (Richtlinien für soziale Medien, Passwortwortrichtlinien, Netzwerkrichtlinien usw.) und wie es gesetzliche Vorschriften einhält (Richtlinien für akzeptable Nutzung, Datenschutzrichtlinien, Verhaltenskodex usw.). Richtlinien sind ein wichtiger Bestandteil des Best-Practice-Prozesses für die Mitarbeiterkommunikation. Schulungsmaßnahmen und Richtlinien sind am effektivsten, wenn sie aufeinander abgestimmt sind. Bei getrennter Behandlung erhöht sich der Arbeitsaufwand und es gibt mehr Kommunikationsbedarf mit Mitarbeitern, was letztendlich zur Überlastung der Benutzer führt.

NICHT VERGESSEN

Betrachten Sie die Richtlinien als die Gesetze Ihres Unternehmens. Regierungen erlassen Gesetze nicht auf die Schnelle, und bei der Genehmigung von Gesetzen, politischen Maßnahmen und Mitteilungen mangelt es nie an einer strengen Kontrolle durch die Exekutive. Trotzdem wird das Richtlinienmanagement im Bereich der Informationssicherheit und des Datenschutzes in vielen Unternehmen von der Geschäftsleitung ignoriert.

Berücksichtigen Sie bei der Erstellung eines Sensibilisierungsprogramms alle wichtigen Elemente, die Sie den Mitarbeitern vermitteln müssen, darunter Richtlinien, eLearning, Risikobewertungen und simulierte Phishing-Angriffe. Um die Ziele der Sensibilisierungsstrategie zu erreichen, gilt es, das richtige Gleichgewicht zwischen diesen Elementen zu finden.

NICHT VERGESSEN

Wie bei allen Sensibilisierungsinitiativen steht auch hier der Mensch im Mittelpunkt. Stellen Sie sicher, dass alle Mitarbeiter hinter den Richtlinien stehen und akzeptieren, warum sie sich in bestimmten Situationen auf eine bestimmte Weise verhalten sollen. Diese Akzeptanz sorgt dafür, dass sich jeder einzelne Mitarbeiter persönlich verantwortlich fühlt, und trägt letztendlich zur Verhaltensänderung bei.

Richtlinien sind der dokumentierte Unternehmensstandard, an die sich alle Mitarbeiter halten müssen. Entscheidend ist, dass Ihre Mitarbeiter problemlos auf ein zentrales Richtlinienportal zugreifen können, das zur allgemeingültigen, verlässlichen Datenquelle des Unternehmens wird. Dieses Portal muss manipulationssicher sein, damit das Unternehmen im Falle einer gerichtlichen Anfechtung der Richtlinien über die nötige „Beweiskraft“ verfügt.

Außerdem müssen die Richtlinien einer strengen Revisionskontrolle unterzogen werden, damit alle im Laufe der Zeit vorgenommenen Anpassungen und Änderungen erfasst und anhand eines Prüfpfads nachvollzogen werden können. Richtlinien ändern sich ständig, um den Bedürfnissen des Unternehmens gerecht zu werden. Der im Unternehmen angewandte Change-Management-Prozess für Richtlinien sollte regelmäßig überprüft werden, um sicherzustellen, dass er weiterhin angemessen ist. Wichtig ist, dass Richtlinien den Mitarbeitern auf eine Weise vermittelt werden, die die Einhaltung von Cyber- und Rechtsvorschriften unterstützt. Diese Art der Kommunikation lässt sich am besten durch die Erstellung eines Kommunikationsplans für Richtlinien erreichen, wie in Abbildung 4-1 dargestellt.

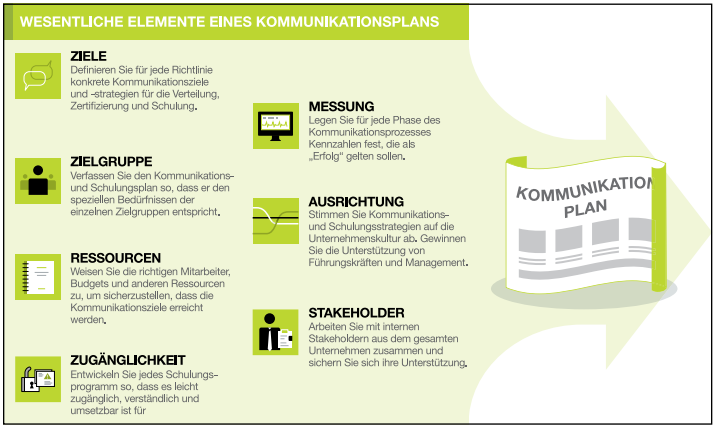


ABBILDUNG 4-1: Die wesentlichen Elemente eines Kommunikationsplans (Quelle: OCEG und GRC 20/20).

Richtlinienmanagement: Schulungen zur Erkennung von Risiken

Unternehmen stellen Richtlinien auf, um die in den Bereichen Compliance und Informationssicherheit identifizierten Risiken zu mindern. Richtlinien werden eingeführt, weil bestimmte Risiken so groß geworden sind, dass sie eine offizielle schriftliche Regelung erfordern. In einer Richtlinie werden auch die notwendigen Kontrollmaßnahmen zur Eindämmung des jeweiligen Risikos festgelegt. Eine Richtlinie ist jedoch nur ein Schritt im Sensibilisierungsprozess. Mitarbeiter müssen auch zum Inhalt von Richtlinien geschult werden.

Bei der Richtlinienschulung kann der Inhalt einer Richtlinie in verkürzter Form behandelt werden. Die zahlreichen mit der Risikominderung verbundenen Eventualitäten werden im Dokument selbst behandelt. Die Schulung sollte sich auf die wichtigsten Punkte der Richtlinie konzentrieren, die die Mitarbeiter kennen müssen. Es ist nicht nötig, den Inhalt des Dokument wortwörtlich wiederzugeben.

Richtlinien spielen bei der Veränderung der Unternehmenskultur eine wichtige Rolle. Wenn ein Mitarbeiter aufgefordert wird, eine Richtlinie zu bestätigen, sei es in elektronischer Form oder indem er ein Schriftstück unterzeichnet, bestätigt er damit auch, dass er sich der Bedeutung seines eigenen Handelns bewusst ist. Richtlinien helfen, die Bedeutung der Cybersicherheit am Arbeitsplatz zu erhöhen. Sie tragen dazu bei, dass Mitarbeiter in Bezug auf Unternehmensrisiken, -verfahren und -vorschriften persönlich Verantwortung übernehmen.

Die folgenden Abschnitte enthalten ausführliche Informationen zur Schulung bestehender und neuer Mitarbeiter.

Richtlinienschulung für Mitarbeiter

Richtlinien geben Mitarbeitern zwar eine Richtung vor, doch zu ihrer Umsetzung werden oft Schulungen benötigt. Der Umfang der erforderlichen Schulungsmaßnahmen steht in direktem Zusammenhang mit dem Risiko, auf das sich die Richtlinie bezieht, sowie dem ermittelten Risikoniveau. Für höhere Risiken gibt es Richtlinien, die eine umfangreichere Schulung erfordern, damit die Mitarbeiter die jeweiligen Kontrollmaßnahmen verstehen und anwenden können. Möglicherweise müssen Sie bei einem höheren Risikopotenzial auch einen hybriden Ansatz verwenden, der Richtlinienschulung, eLearning und Präsenzschulung miteinander kombiniert, damit die Richtlinie auch wirklich akzeptiert und verstanden wird. In Kapitel 5 wird dieser hybride Ansatz ausführlicher besprochen.

Es besteht ein klarer Zusammenhang zwischen dem in Richtlinien, Schulungen und Sensibilisierungsmaßnahmen investierten Zeit- und Energieaufwand und ihren tatsächlichen Auswirkungen auf das Unternehmen. Compliance-Maßnahmen, die durch die Unterstützung von Führungskräften besondere Resonanz bei den Mitarbeitern finden, führen in der Regel zu einer stärkeren Akzeptanz von Richtlinien und zu einem erfolgreicheren Abschluss von Schulungen und der damit verbundenen Prüfungen.

In Abbildung 4-2 sind wichtige Fragen aufgeführt, die Sie stellen sollten, wenn Sie Ihre Mitarbeiter in neue Richtlinien einweisen.

Warum Richtlinien für die Sensibilisierung neuer Mitarbeiter wichtig sind

Viele Unternehmen verlangen von neuen Mitarbeitern gleich in der ersten Woche, Richtlinien zu unterschreiben und täglich bis zu drei Stunden eLearning zu absolvieren. Damit helfen sie ihnen nicht, ihre Zeit effektiv zu nutzen. Mit einem Lernansatz dieser Art werden neue Mitarbeiter quasi gezwungen, aus einem Hochdruckschlauch zu trinken!

ABBILDUNG 4-2: Fragen (Quelle: OCEG and GRC 20/20).

In den ersten Wochen, wenn sich neue Mitarbeiter noch am Beginn ihre Lernkurve befinden, haben Unternehmen eine schwierige Aufgabe. Sie müssen einen Einarbeitungsplan erstellen, der für die Mitarbeiter angemessen ist. Wenn Sie jeden Tag zwei oder drei Stunden lang an Schulungen teilnehmen müssten, wären Sie sicher auch überfordert. Das Problem bei neuen Mitarbeitern besteht darin, dass sie gleich zu Beginn so viel lernen müssen. Berücksichtigen Sie bei Cybersicherheitsschulungen, dass Menschen nur zu einem gewissen Grad aufmerksam sein und lernen können.

NICHT VERGESSEN

Überlegen Sie genau, wie Sie neuen Mitarbeitern wichtige Richtlinien in Verbindung mit dem entsprechenden eLearning am besten vermitteln können. Begrenzen Sie das im ersten Monat zu absolvierende eLearning-Pensum. Im ersten Monat sind maximal drei Stunden pro Woche optimal. Diese Zeit ist für einen neuen Mitarbeiter ausreichend, um die wichtigsten Richtlinien und eLearning-Inhalte zu absolvieren, und hilft ihm, den Unternehmensansatz zu verstehen, ohne überfordert zu werden. Reduzieren Sie die Anzahl der Richtlinien und eLearnings nach dem ersten Monat, damit der Mitarbeiter in seiner neuen Rolle produktiv werden kann.

Eine zentralisierte Technologiearchitektur für Ihre Richtlinien

Richtlinienmanagement und eLearning sind inzwischen so kompliziert geworden, dass sie nicht mehr effektiv als manuelle Prozesse durchgeführt werden können. Ein zentralisiertes Richtlinienmanagementsystem kann dem Unternehmen dabei helfen, die sich ständig ändernden Anforderungen des Unternehmens, der gesetzlichen Vorschriften und des Geschäftsumfelds zu erfüllen.

Die Verwaltung des Richtlinien-Lebenszyklus mithilfe von Tabellenkalkulationen und File-Sharing-Systemen ist nicht nur schwierig, sondern deutet auch auf eine mangelnde Compliance-Reife im Unternehmen hin. Außerdem lässt sie einen Ad-hoc-Ansatz für das Sicherheits- und Compliance-Management erkennen.

In den folgenden Abschnitten erfahren Sie, wie ein zentralisiertes Richtlinienmanagementsystem Ihrem Unternehmen helfen kann und von wem das System genutzt wird.

Die Vorteile eines zentralisierten Systems

Hier sind einige der wichtigsten Vorteile eines zentralisierten Systems:

- **Es garantiert eine 100-prozentige Teilnahme.** Ein zentralisiertes Richtlinienmanagementsystems sorgt dafür, dass alle Mitarbeiter die erforderlichen Richtlinien erhalten, verstehen und bestätigen.
- **Es ermöglicht den Zugriff auf Schulungen und Richtlinien an einem Ort.** Die Möglichkeit, Schulungen mit den jeweiligen Richtlinien zu verknüpfen, kommt allen Mitarbeitern zugute.
- **Es entlastet das Management.** Durch die automatisierte Richtliniendurchsetzung kann die Richtlinienautomatisierung umfassende Kontrollmaßnahmen durch das Management überflüssig machen. Der Benutzer wird von der Technologie, nicht vom Management, benachrichtigt und daran erinnert, seine Verpflichtungen in Bezug auf Richtlinien und Schulungen zu erfüllen.
- **Alle Richtlinien und Schulungen befinden sich an einem Ort.** Der Hauptvorteil einer Technologielösung besteht darin, dass sie Ihnen eine einzige verlässliche Datenquelle für Ihre Compliance-Aktivitäten zur Verfügung stellt, besonders in Bezug auf Richtlinien, Schulungen und die Interaktion mit Ihren Mitarbeitern.

Abbildung 4-3 zeigt, wie zentralisierte Technologie Ihrem Unternehmen nutzen kann.

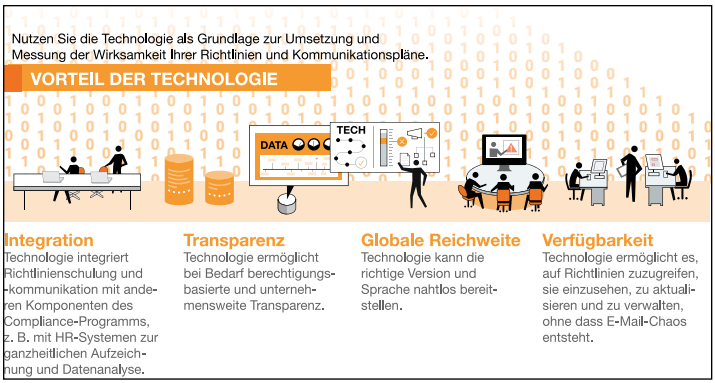


ABBILDUNG 4-3: Der Vorteil der Technologie (Quelle: OCEG and GRC 20/20).

Wer verwendet dieses System?

Diese Art von Richtlinienmanagementsystem wird hauptsächlich von drei Gruppen verwendet. Diese sind:

- **Administratoren, die das System einrichten und die Richtlinien und Schulungen verteilen:** Sie verfügen über eine eigene Verwaltungsschnittstelle zur Erstellung, gezielten Verbreitung und Verwaltung von Unternehmensrichtlinien.
- **Die Nutzer, die die Schulungen und Richtlinien verwenden:** Das System hilft ihnen, ihren Verpflichtungen nachzukommen, z. B. Richtlinien zu unterzeichnen, Schulungen zu absolvieren, ihre Interaktion mit den Inhalten selbst zu verwalten und auf diese Inhalte zuzugreifen, wenn sie ihr Wissen auffrischen müssen.
- **Das Management oder die Aufsicht über das System:** Das Management kann das System überprüfen, um sicherzustellen, dass die Mitarbeiter die erforderlichen Kommunikationskampagnen in Sachen Compliance durchführen. Prüfer und Aufsichtsbehörden können auf das System zugreifen, um sich davon zu überzeugen, dass das Unternehmen seiner Sorgfalts- und Aufsichtspflicht nachkommt.

IN DIESEM KAPITEL

- Die Unterstützung der Führungsetage gewinnen
- Eine Kampagne braucht einen Plan
- Eine Baseline für Ihre Strategie erstellen
- Wie sieht der Erfolg aus?
- Ein hybrider Ansatz

Kapitel 5
Entwicklung einer Best-Practice-Strategie für die Cyber-Sensibilisierung

Zur erfolgreichen Durchführung einer Cyber-Sensibilisierungskampagne benötigt Ihr Unternehmen einen klaren Aktionsplan. Dieses Kapitel enthält Empfehlungen für die Erstellung eines solchen Plans. Wichtig ist, dass die Führungskräfte Ihres Unternehmens dabei hinter Ihnen stehen. Wenn Ihr Plan fertig ist, müssen Sie messen können, ob er auch wirklich funktioniert. Gegebenenfalls sollte Ihr Unternehmen einen hybriden Ansatz in Betracht ziehen.

Die Unterstützung der Führungsetage gewinnen

Der Erfolg eines Sensibilisierungsprogramms hängt oft davon ab, ob es Unterstützung seitens der Führungsebene erhält. Ohne diese Unterstützung ist es schwierig, ausreichende Finanzmittel und Ressourcen zu erhalten, und ohne diese Mittel kann ein Sensibilisierungsprojekt nur begrenzt erfolgreich sein.

Cyber-Sensibilisierungsprogramme haben das Ziel, das Mitarbeiterverhalten zu ändern. Dabei spielt die menschliche Psychologie eine wichtige Rolle. Mit der Unterstützung des Führungsteams können Sie Hindernisse aus dem Weg räumen und sicherstellen, dass Entscheidungen schnell getroffen werden. Sie müssen von Anfang an wissen, welcher Ton an der Spitze vorherrscht. Welcher Ton wird zum Beispiel in Bezug auf schlechtes Verhalten bei der Cybersicherheit angeschlagen? Ist er eher locker oder herrscht Null-Toleranz? Wie oft muss ein Mitarbeiter bei einem simulierten Phishing-Test durchfallen, bevor disziplinarische Maßnahmen eingeleitet werden? Wenn kein bestimmter Ton gesetzt wird, kann jeder Manager und jeder Leiter im Unternehmen die Umsetzung der Sensibilisierungskampagne auf seine eigene Weise interpretieren.

Die Änderung des Mitarbeiterverhaltens beinhaltet ein psychologisches Element. Viele Mitarbeiter lassen sich zum Beispiel gern von ihren Führungskräften anleiten. Daher ist es sehr effektiv, eine Sensibilisierungskampagne mit einer Botschaft „von oben“ anzukündigen. Dies kann in Form einer E-Mail oder eines einfacher Videobotschaft erfolgen.


TIPP

Stellen Sie bei der Ausarbeitung Ihrer Sensibilisierungskampagne sicher, dass Sie die volle Unterstützung Ihres Führungsteams haben. Es ist sinnvoll, den Führungskräften ein paar spezielle Schulungsstunden anzubieten. Dies sollte in Form einer maßgeschneiderten Präsenzschulung erfolgen und durch eLearning für Führungskräfte ergänzt werden.

Einen Kampagnenplan aufstellen

Ein auf die Risikominderung ausgerichteter Planungsprozess ist der beste Ansatz für die Entwicklung einer geeigneten Cyber-Sensibilisierungskampagne. Achten Sie bei der Erstellung Ihres Plans darauf, dass er für den vorgesehenen Zeitraum (in der Regel zwölf Monate) geeignet ist und die wichtigsten Risiken enthält, denen das Unternehmen in diesem Zeitraum ausgesetzt ist. Seien Sie darauf vorbereitet, Ihre Risiken neu zu bewerten, da diese sich im Laufe der Zeit verändern können.


WARNUNG

Bei der Erstellung eines Kommunikationsplans für ihr Sensibilisierungsprogramm verlassen sich Unternehmen häufig auf einen Informationssicherheitsexperten. Dieser sollte bei der Ausführung seiner Aufgabe mit internem Know-how zur Unternehmenskommunikation

unterstützt werden. Informationssicherheits- und Datenschutzexperten spielen in jedem Fall eine entscheidende Rolle für den Erfolg einer Cyber-Sensibilisierungskampagne. Ihr Wissen kann das Programm erheblich beeinflussen und bereichern. Risiken stehen im Mittelpunkt jeder Sensibilisierungskampagne. Mit der Unterstützung dieser Experten können die unterschiedlichen, zu behebenden Risiken identifiziert und nach Priorität eingestuft werden.

Möglicherweise muss sich jemand aus den Bereichen Projektmanagement oder Unternehmenskommunikation dem Team anschließen, um sicherzustellen, dass die Botschaft effektiv und effizient verbreitet wird. Das Team muss über unterschiedliche Fähigkeiten verfügen, um eine erfolgreiche Sensibilisierungskampagne zu erarbeiten.

Es kann verlockend sein, einfach ein paar simulierte Phishing-E-Mails zu verschicken und sich dann in dem Glauben zu wiegen, dass damit die Anforderungen an die Cyber-Sensibilisierung erfüllt sind. Diese Methode führt Mitarbeitern das Risiko des Social Engineering zwar sehr deutlich vor Augen, doch ein Sensibilisierungsprogramm muss alle Bedrohungen des Unternehmens berücksichtigen. Im Rahmen eines Sensibilisierungsprogramms müssen auch Abhilfemaßnahmen aufgezeichnet und Folgeaktivitäten dokumentiert werden. Diese Aufzeichnungen werden benötigt, um Compliance und Governance nachweisen zu können.

Die Erstellung eines Playbooks (siehe Abbildung 5-1) oder einer Maßnahmenkampagne für das bevorstehende Jahr ist für den Erfolg eines Cyber-Sensibilisierungsprojekts entscheidend. Dieser Prozess forciert die Identifizierung von Hauptrisiken. Das Unternehmen muss herausfinden, wie gut Mitarbeiter in der Lage sind, Compliance- und Sicherheitsmitteilungen zu verarbeiten. Das Management muss entscheiden, wie viele Mitteilungen welcher Art pro Woche, pro Monat und pro Jahr verschickt werden sollten. Es ist nicht immer einfach, die zu vermittelnden Risiken und die Überforderung der Benutzer gegeneinander abzuwägen. Das Team, das die Kampagne durchführt, darf bei der Umsetzung des Sicherheitsprogramms nicht zu übereifrig vorgehen.

Es braucht viel Zeit, um das Verhalten von Mitarbeitern zu ändern und ihre Widerstandsfähigkeit gegenüber Cybersicherheitsbedrohungen zu erhöhen.

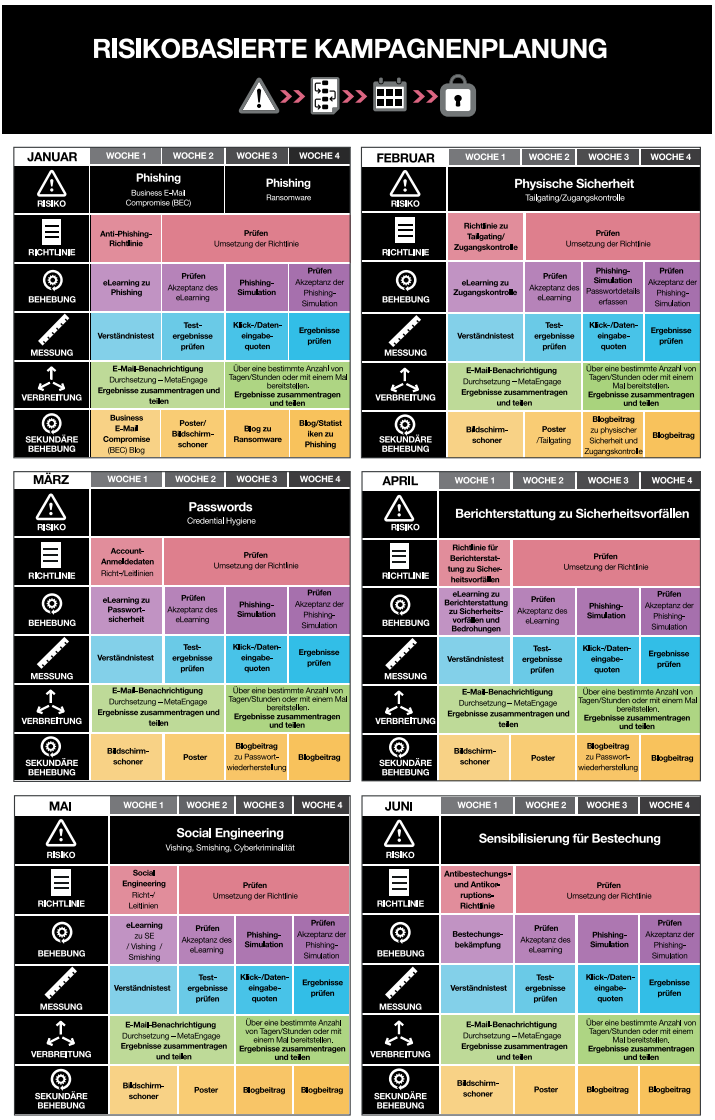


ABBILDUNG 5-1: Ein zwölfmonatiger Security Awareness Planer.

Erstellung einer Baseline

Leistungsindikatoren („Key Performance Indicators", KPIs) zeigen, ob ein Projekt erfolgreich ist oder nicht. Dies gilt auch für Ihr Cyber-Sensibilisierungsprogramm. Nutzen Sie die KPIs, die Sie ermittelt haben, um

eine Baseline zu erstellen. Anhand dieser Daten können Sie dann messen, welche Fortschritte erzielt worden sind.

Ihre Sensibilisierungsprogramme müssen sich an den Risiken orientieren, mit denen Ihr Unternehmen gegenwärtig konfrontiert ist. Die vor kurzem aufgezeichneten Vorfälle sind ein guter Ausgangspunkt und ein hervorragender Indikator für die Probleme und Risiken, die im Rahmen des Programms behoben werden müssen.

TIPP

Um herauszufinden, wie gut Ihre Nutzer über diese Risiken Bescheid wissen, eignet sich ein Online-Fragebogen/eine Online-Umfrage. Orientieren Sie sich bei den Fragestellungen an den Risiken, denen Ihr Unternehmen ausgesetzt ist. Die Umfrage sollte so kurz und prägnant wie möglich sein.

Die Ergebnisse der Umfrage fließen dann in jedes weitere Schulungsprogramm ein. Wenn die Umfrage zum Beispiel Wissenslücken in Bezug auf die physische Sicherheit aufzeigt, müssen Sie diese durch Schulungen oder die Vermittlung von Richtlinien schließen. Wir empfehlen, jeden Monat ein Hauptrisiko in Angriff zu nehmen. Durch die Umfrage wird also geprüft, was Ihre Mitarbeiter über mindestens zwölf Fragen/Risiken wissen.

NICHT VERGESSEN

Eine weitere Möglichkeit, um schnell eine Baseline zu erstellen, ist die Durchführung eines simulierten Phishing-Angriffs auf Mitarbeiter. Dadurch lässt sich feststellen, wie anfällig Ihr Unternehmen für betrügerische Phishing-E-Mails ist, und Sie erhalten einen Echtzeit-Überblick über den Anteil der Mitarbeiter, die einem tatsächlichen Angriff zum Opfer fallen würden. Noch besorgniserregender sind Nutzer, die ihre Anmeldedaten eingeben, wenn sie dazu aufgefordert werden.

Richtlinien sind ein wesentlicher Bestandteil des Sicherheitsbewusstseins von Mitarbeitern. Führen Sie zu Beginn eine Übung durch, um die wichtigsten Richtlinien zu bestimmen, an die sich die Mitarbeiter halten müssen. Denken Sie daran, dass es nur dann eine Richtlinie geben sollte, wenn sie sich auf ein Risiko bezieht. Deshalb sollte für jedes Ihrer Hauptrisiken eine Unternehmensrichtlinie vorhanden sein. Überprüfen Sie, wann Ihre Richtlinien zuletzt überarbeitet wurden und ob sie noch angemessen sind.

WARNUNG

Vermeiden Sie jedoch eine Massenüberprüfung der Unternehmensrichtlinien, da dies die Sensibilisierungskampagne ausbremsen kann. Es gilt als Best Practice, die jeweilige Richtlinie mindestens einen Monat vor der Behandlung des Risikos in Ihrem Sensibilisierungsplan zu klären.

Definition und Messung des Erfolgs

Nachdem eine Baseline vereinbart und dokumentiert wurde, müssen Sie Ihre KPIs monatlich verfolgen, um den Erfolg des Sensibilisierungsplans zu messen. Dabei sind unter anderem folgende Bereiche zu überprüfen:

- Prozentsatz der Nutzer, die sich an die wichtigsten Richtlinien halten
- Prozentsatz der Nutzer, die auf eine simulierte Phishing- Mail klicken
- Anzahl der Risikobewertungen von Lieferanten
- Anzahl der Datenverarbeitungsaktivitäten
- Anzahl der ausgefüllten Mitarbeiterbefragungen
- Anzahl der Sicherheitsvorfälle
- Anzahl der von Mitarbeitern gemeldeten Phishing-Fälle

Die letzten drei Kennzahlen sind wichtig, weil sie sich auf das Bewusstsein der Mitarbeiter für die wichtigsten Sicherheitsprobleme des Unternehmens beziehen. ***Hinweis:*** Die Zahl der gemeldeten Sicherheitsvorfälle kann zunehmen, nachdem die Mitarbeiter für unterschiedliche Risiken sensibilisiert worden sind.

Diese Kennzahlen bilden die Grundlage für die Berichterstattung an den Lenkungsausschuss für Informationsverwaltung (Information Governance Steering Committee) und tragen dazu bei, ihn über die Behebung von Risiken und den Fortschritt der Sensibilisierungskampagne zu informieren.

Ein hybrider Ansatz

Bei guten Marketingkampagnen kommen viele unterschiedliche Methoden zum Einsatz, um die Aufmerksamkeit der Kunden auf ein Produkt oder eine Dienstleistung zu lenken. Dabei wird eine Kombination aus digitalen Kanälen, E-Mail und sozialen Medien sowie traditionellen Methoden wie Werbeaktionen in Geschäften und Werbegeschenken genutzt. Bei Ihrem Sensibilisierungsprogramm können Sie ebenfalls einen hybriden Ansatz verfolgen, um die Aufmerksamkeit Ihrer Nutzer zu gewinnen und zu halten. Sobald Sie ihre Aufmerksamkeit gewonnen haben, müssen Sie versuchen, eine Verhaltensänderung herbeizuführen.

In den folgenden Abschnitten wird erläutert, wie Sie Storytelling und andere Methoden verwenden können, um Ihre Botschaft wirksam zu vermitteln.

Storytelling in das Programm einbauen

Beim Marketing und bei Sensibilisierungsprogrammen gibt es keine Standardlösung, die für alle geeignet ist. Im Bereich der Unternehmenskommunikation kämpfen mehrere interne Gruppen um die Aufmerksamkeit der Mitarbeiter. Ein gutes Sensibilisierungsprogramm trägt dieser Tatsache Rechnung. Das bedeutet, dass Sie mehrere Kommunikationskanäle nutzen müssen, um die Aufmerksamkeit Ihrer Zielgruppe auf sich zu ziehen, einschließlich physischer, digitaler und erzählerischer Mittel.

NICHT VERGESSEN

Menschen pflegen seit jeher die Tradition der mündlichen Überlieferung. Greifen Sie also auf diese Tradition zurück und erzählen Sie eine Geschichte oder verwenden Sie bei der Vermittlung Ihrer Botschaft ein Thema, mit dem sich Ihre Zielgruppe identifizieren kann. Ein gutes Thema für Ihre Mitarbeiter ist zum Beispiel folgendes Szenario: Lassen Sie sie in die Rolle eines Regierungsagenten schlüpfen, der versucht, die Pläne eines Bösewichts zu vereiteln. Wer identifiziert sich nicht gern mit Superhelden wie James Bond oder Wonder Woman?

Innovative Kommunikation

Physische Kommunikationsmethoden erfordern unterschiedliche kreative Ansätze. Hier sind einige Möglichkeiten, wie Sie die Botschaft Ihrer Kampagne verbreiten können:

- **Poster:** Die billigste und wirksamste Methode ist eine Plakatkampagne, die Ihre Schlüsselbotschaften und -themen hervorhebt. Sie können alle Arten von Postern verwenden, von digitalen Schildern am Empfang bis hin zu kleinen Plakaten in Aufzügen. Die Poster sollten auf die Risiken ausgerichtet sein, auf die Sie aufmerksam machen wollen, und alle vier bis sechs Wochen ausgetauscht werden, da die Botschaft sonst irgendwann nicht mehr wahrgenommen wird.
- **Digitale Methoden:** Digitale Methoden werden am häufigsten zur Kommunikation und Behebung von Risiken eingesetzt, die sich aus einer unzureichenden Mitarbeiterschulung ergeben. Einige Unternehmen verfügen über eigenständige eLearning-Systeme für simuliertes Phishing, Richtlinienmanagement oder Cybersicherheit, mit denen den Mitarbeitern wichtige Informationen vermittelt werden können.

AUTOMATISIERUNG DER KAMPAGNE

Automatisieren Sie Ihre gesamte zwölfmonatige Sensibilisierungskampagne, damit die wesentlichen Elemente zur richtigen Zeit an die richtige Zielgruppe übermittelt werden. Zu diesen Elementen sollte eine Kombination aus maßgeschneiderten eLearnings, wichtigen Richtlinien, einschlägigen Blogs, simulierten Phishing-E-Mails, Risikobewertungen und Umfragen gehören.

Ein automatisierter Security-Awareness-Ansatz ermöglicht die Aufzeichnung von Audit-Informationen, damit im Falle eines Verstoßes oder Audits alle gesetzlichen Vorschriften eingehalten werden.

IN DIESEM KAPITEL

- Die Spitze gibt den Ton an
- Ihre Zielgruppe ansprechen
- Vorbereitung auf eine Datenschutzverletzung
- Überprüfung Ihrer Sensibilisierungsinitiativen

Kapitel 6
Zehn Best Practices zur Durchführung einer Sensibilisierungskampagne für Cybersicherheit

Hier sind zehn Best Practices, die Ihnen dabei helfen sollen, eine möglichst effektive Sensibilisierungskampagne für Cybersicherheit in Ihrem Unternehmen durchzuführen.

Der Anfang: Die Führungsrolle des CEO

Cybersicherheit erhält endlich auch in den Vorstandsetagen die Aufmerksamkeit, die sie verdient. Da die Anzahl der Datenverstöße bei namhaften Unternehmen auch weiterhin ansteigt, wird mehr Wert auf den Umgang mit Cybergefahren gelegt, um die Wahrscheinlichkeit eines Angriffs zu reduzieren.

Für die Cybersicherheit ist jeder verantwortlich, aber resiliente Unternehmen benötigen einen CEO mit starker Führungsrolle. Ein engagierter CEO ergreift die richtigen Sicherheitsmaßnahmen, um die digitalen Werte des Unternehmens, seine Mitarbeiter und Kunden sowie den Ruf der Marke zu schützen. Wenn der CEO die Cybersicherheit ernst nimmt,

durchdringt diese Einstellung das gesamte Unternehmen und schafft eine Kultur der Achtsamkeit im Umgang mit Cybergefahren.

Kapitel 5 hilft Ihnen, die Unterstützung der Führungsebene zu erhalten.

Den Spielraum des eigenen Unternehmens kennen

Bei der Gestaltung eines effektiven Sicherheitsprogramms muss Ihr Unternehmen die Bedrohungslandschaft evaluieren und die Hauptrisiken ermitteln. Dadurch erhalten Sie ein besseres Verständnis für die tatsächlichen Bedrohungen, die sich auf die Sicherheit des Unternehmens auswirken können.

Gleich zu Beginn muss die Risikotoleranz definiert werden, um anschließend die Maßnahmen zu ergreifen, die den tatsächlich vorhandenen Bedrohungen entsprechen. Dadurch vermeiden Sie den Einsatz von Ressourcen für Bedrohungen, die wahrscheinlich nicht auftreten werden bzw. sich gar nicht oder kaum auf Ihr Unternehmen auswirken.

Sie müssen regelmäßig Risikobewertungen durchführen, um sicherzustellen, dass Ihr Cybersicherheitskonzept mit gesetzlichen Rahmenvorschriften, Informationssicherheitsnormen und Gesetzen wie der Datenschutz-Grundverordnung (GDPR) im Einklang steht.

Wenn Sie sich die Zeit für eine gründliche Analyse der Gefahren nehmen, können Sie leichter die Inhalte, Methoden und Zielgruppen Ihres Sensibilisierungsprogramms für Cybersicherheit festlegen.

Informations-Assets schützen

Für die Entwicklung einer umfassenden Cybersicherheitsstrategie und die wirksame Identifizierung von Risiken müssen Sie einen gründlichen Audit aller Informations-Assets Ihres Unternehmens durchführen.

Informations-Assets sind Daten, die einen Wert für Ihr Unternehmen haben. Dabei kann es sich um personenbezogene Daten (Personal Identifiable Information, PII), Finanzdaten, geistiges Eigentum oder andere Daten mit großer Bedeutung für Ihr Unternehmen handeln.

Sie müssen ermitteln, was die wertvollsten Informations-Assets sind, wo sie sich befinden und wer auf sie zugreifen kann. Jedes Asset sollte seinem Wert entsprechend klassifiziert werden (zum Beispiel als öffentlich, privat oder vertraulich). Das ist wichtig, um die Risiken zu erkennen und die Bereiche zu priorisieren, die geschützt werden müssen.

Wenn Sie diese Bereiche kennen, geht es als Nächstes darum, wie diese Informations-Assets potenziell kompromittiert werden können. Ob Sicherheitsverletzungen, Malware oder gar eine Insiderbedrohung – Sie haben eine gute Informationsgrundlage zur Verbesserung der Prozesse und reduzieren die Wahrscheinlichkeit, dass Cyberkriminelle Zugriff auf wichtige Systeme erhalten.

Auf risikobehaftete Gruppen konzentrieren

Bei einem effektiven Sensibilisierungsprogramm für Cybersicherheit kommt es darauf an, dass die richtigen Personen die richtigen Schulungen erhalten. Jeder kann einer Cyberbedrohung zum Opfer fallen. Manche Mitarbeiter haben jedoch ein höheres Bedrohungsprofil als andere. Die Personal- und die Finanzabteilung werden wegen ihres privilegierten Zugangs zu vertraulichen Daten zum Beispiel besonders oft angegriffen.

Auch der CEO, der CFO und andere Führungskräfte werden wegen ihrer umfassenden Zugriffsrechte für wertvolle Unternehmensdaten gern ins Visier genommen. Sie sind oft die Zielscheibe ausgeklügelter BEC-Betrügereien (Business Email Compromise). Bei dieser Art von Phishing-Angriffen geben sich Cyberkriminelle als hochrangige Führungskräfte aus, um Mitarbeiter, Kunden oder Lieferanten dazu zu bringen, Geld auf ein Fake-Konto zu überweisen oder vertrauliche Daten offenzulegen. Wenn jemand auf Führungsebene einem Betrug zum Opfer fällt, kann dies verheerende Folgen haben und die Sicherheit des gesamten Unternehmens untergraben.

In Kapitel 2 finden Sie weitere Informationen über die am meisten gefährdeten Gruppen und erfahren außerdem, wie Sie Schulungen auf sie zuschneiden können.

Schulungen mit gekonntem Storytelling ansprechend gestalten

Storytelling ist eine der wirksamsten Methoden, um Ihrer Sensibilisierungskampagne für Cybersicherheit Leben einzuhauchen. Machen Sie sich nichts vor: Cybersicherheit ist oft ein trockenes Thema. Es muss Ihnen aber gelingen, die Mitarbeiter zu motivieren, wenn sich das Verhalten in Ihrem Unternehmen verbessern soll. Die Botschaft ist zu wichtig, um in formellen Rundschreiben zu versanden.

Geschichten sind ein Grundbaustein des menschlichen Lernens. Sie erzeugen eine emotionale Reaktion, die das Erlernte besser im Gedächtnis verankert. Sie können Botschaften zur Cybersicherheit mit Leben erfüllen, um sie Menschen im Alltag näherbringen. Durch Geschichten mit Relevanz für die Endbenutzer erhöht sich die Wahrscheinlichkeit, dass diese sich die Informationen merken. Dadurch verbessert sich die allgemeine Sicherheitslage in Ihrem Unternehmen. In Kapitel 5 wird ausführlich erklärt, wie Sie Storytelling in Ihre Kampagne einbeziehen können.

Richtlinienmanagement auf den neuesten Stand bringen

Richtlinien sind wichtig, um das Verhalten für Personen, Prozesse, Beziehungen und Transaktionen in Ihrem Unternehmen in feste Bahnen zu lenken. Sie dienen als Grundgerüst für die Betriebsführung, zur Ermittlung von Risiken und für die Definition von Compliance. Das ist in der heutigen, zunehmend komplexen Landschaft behördlicher Vorschriften von großer Bedeutung.

Ein effektives Richtlinienmanagementsystem hat eine einheitliche Methode der Richtlinienerstellung, strukturiert die unternehmensinternen Verfahren und erleichtert die Nachverfolgung von Bescheinigungen und Mitarbeiterantworten. Dementsprechend können Sie damit interne Prozesse rationalisieren, die Einhaltung gesetzlicher Anforderungen dokumentieren und effektiv auf die Bereiche mit der größten Gefahr für die Datensicherheit abzielen.

Sofort mit den Vorbereitungen auf eine Datenschutzverletzung beginnen

Wenn Sie sich noch nicht auf eine Datenschutzverletzung vorbereitet haben, sollten Sie jetzt damit anfangen. Viele Milliarden vertrauliche Datensätze wurden bereits ausgespäht. IBM zufolge sind die durchschnittlichen Kosten einer Datenschutzverletzung weltweit auf schwindelerregende 3,92 Millionen USD gestiegen.

Es geht nicht mehr darum, „ob“ Ihr Unternehmen angegriffen wird, sondern „wann“. Sie müssen sich auf das Unvermeidliche vorbereiten und einen Plan entwickeln, damit bei einem Sicherheitsverstoß geeignete Maßnahmen getroffen werden.

Die Festlegung eines wirksamen Notfallplans hilft, die Mitarbeiter zu schulen und zu informieren, verbessert die Unternehmensstruktur, stärkt das Vertrauen der Kunden und Stakeholder und reduziert die potenziellen Schäden für die Finanzen oder den guten Ruf bei einer Datenschutzverletzung.


TIPP

Sie müssen den Notfallplan regelmäßig testen, um Schwachpunkte herauszufinden und sicherzustellen, dass alle im Team ihren Verantwortungsbereich bei der Vorbereitung und Reaktion auf Datenschutzverletzungen kennen.

Champions für die Cybersicherheit ernennen

Bei Cybersicherheit geht es nicht nur um Technologien. Ihre Mitarbeiter spielen eine wichtige Rolle beim Schutz des Unternehmens und der Ermittlung von Bedrohungen, die eine Sicherheitsgefahr darstellen könnten.

Champions für die Cybersicherheit zu ernennen, ist eine hervorragende Methode, selbständiges Handeln zu fördern und Ihren Mitarbeitern die nötigen Kompetenzen im Umgang mit Cyberangriffen zu vermitteln. Nach Angaben des National Cyber Security Centre stellte die Hälfte aller befragten Unternehmen nach einem Cyberangriff fest, dass die disruptivsten Bedrohungen direkt von den Mitarbeitern gemeldet und nicht automatisch von der Software erfasst wurden.

Champions für die Cybersicherheit müssen keine technischen Experten sein. Es geht um das menschliche Element Ihrer Sicherheitsstrategie und die Unterstützung durch Mitarbeiter, die sich für eine Stärkung der Achtsamkeit und die Umsetzung geeigneter Cybersicherheitsverfahren einsetzen.

Kapitel 3 enthält konkrete Tipps, wie Sie solche Champions in Ihrem Unternehmen identifizieren und einsetzen können.

Die Lieferkette berücksichtigen

Bei vielen Unternehmen ist die Lieferkette der Schwachpunkt der Cybersicherheit. Anstatt ein Unternehmen direkt anzugreifen, versuchen Cyberkriminelle oft, seine zentralen Netzwerke und Systeme über Lücken in den Prozessen und Systemen der Lieferkette zu kompromittieren.

Die Lieferketten sind ein wichtiger Teil des Geschäftsbetriebs, doch häufig handelt es sich um große und vielfältige Netzwerke in mehreren Ländern. Bei den Zulieferern ist die Cybersicherheit oft auf einem niedrigeren Niveau. Das bedeutet, dass Cyberkriminelle viele Schwachpunkte finden, die sie ausnutzen können.

Einige der größten Datenschutzverletzungen in der jüngeren Geschichte sind auf Lieferkettenangriffe zurückzuführen. Ein Paradebeispiel ist die Datenpanne, der die Kaufhauskette Target 2014 zum Opfer fiel und bei der die persönlichen Daten von über 70 Millionen Kunden abgegriffen wurden. Durch einen Phishing-Angriff auf einen der Dienstleistungsanbieter von Target konnten sich die Angreifer Zugang zu den POS-Kartenlesegeräten des Unternehmens verschaffen.

Jeder Zulieferer, der sich mit Ihrem Unternehmen vernetzt, ist ein potenzieller Risikofaktor. Daher kommt es darauf an, detaillierte Risikobewertungen für Drittfirmen durchzuführen, um möglichen Sicherheitsbedrohungen entgegenzuwirken. So können Sie leichter bestimmen, welche Sicherheitsmaßnahmen zum Schutz Ihrer Daten erforderlich sind.

Kapitel 3 zeigt, wie Sie Ihre Kampagne auf Drittanbieter ausweiten können.

Für angemessene Aufsicht und regelmäßige Prüfungen sorgen

Die Bedrohungslandschaft entwickelt sich ständig weiter. Ihr Sensibilisierungsprogramm für Cybersicherheit muss dies ebenfalls tun. Es ist wichtig, regelmäßig die Alarmbereitschaft der Mitarbeiter zu prüfen, um Schwachstellen zu identifizieren und herauszufinden, ob die aktuellen Richtlinien und Schulungen der Änderung bedürfen.

Um die Einhaltung behördlicher Vorschriften zu erleichtern, hat es sich bewährt, die Prüfungsergebnisse immer zu dokumentieren und Empfehlungen zur Risikominderung immer zu befolgen. Ohne solche regelmäßigen Prüfungen entspricht Ihr Sensibilisierungsprogramm für Cybersicherheit nicht der Bedrohungslandschaft und kann Ihr Unternehmen möglicherweise nicht vor Angriffen schützen.

Ihr erster Schritt in eine **cyber-sicherere Zukunft**

MetaCompliance bietet eine Reihe personalisierter Lösungen für Schulungen zur Sicherheitsbewusstseinsbildung. Von realistischen Phishing-Simulationen bis hin zum umfassenden Richtlinienmanagement – wir sind hier, um Ihr Team gegen moderne Cyber-Bedrohungen zu stärken und zu schulen.

Besuchen Sie **metacompliance.de**, um eine sicherere und cyber-bewusstere Belegschaft zu entwickein.

> MetaCompliance zeichnet sich durch seine vielfältigen Kursangebote, benutzerfreundliche Oberfläche und innovativen Funktionen aus.

> Unser Personal war voll in unser Programm zum Sichereitsbewusstsein eingebunden, mit Abschlussquoten von über 85%.

MetaCompliance®
Make it personal.

Eine Kultur mit erhöhtem Sicherheitsbewusstsein schaffen

Sicherheitsbedrohungen entwickeln sich ständig weiter und werden immer raffinierter. Herkömmliche technische Schutzmaßnahmen reichen nicht aus, um ein Unternehmen vor seiner größten Sicherheitslücke zu schützen: dem menschlichen Faktor. Die menschliche Natur ist eine Schwachstelle, die Cyberkriminelle nur allzu gut auszunutzen wissen. Das Buch *Achtsamkeit bei Cybergefahren für Dummies* schafft Abhilfe. Es ist Ihr Leitfaden für Strategien, Herausforderungen und bewährte Methoden zur Änderung des Benutzerverhaltens im Unternehmen, damit Cyber-Sicherheitsbedrohungen erkannt und bewältigt und wertvolle Informationen und Vermögenswerte effektiv geschützt werden.

Im Buch:

- Geschärftes Bewusstsein für Cybersicherheit im Unternehmen
- Erfüllung strenger gesetzlicher Anforderungen
- Erstellung relevanter und rollenspezifischer Schulungen, die Mitarbeiter ansprechen
- Integration des Richtlinienmanagements in Sensibilisierungsprogramme
- Unterstützung der Führungsebene für Sensibilisierungskampagnen

MetaCompliance®

Besuchen Sie Dummies.com®
um sich Videos und schrittweise Bildanleitungen anzusehen oder Produkte zu kaufen!

ISBN: 978-1-394-29046-8

für dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.