ivanti

Versteckte Bedrohungen 2023

Wie sich die Demografie der Belegschaft auf Ihre Sicherheitslage auswirkt

Teil der Ivanti-Reihe Cybersecurity Status Report

Demografie im Detail

Eine von oben auferlegte, standardisierte Unternehmenssicherheit ignoriert die speziellen Risiken, die u.a. mit Geographie, Alter, Geschlecht und Rolle einhergehen.

In diesem neuesten Bericht von Ivanti nehmen wir die Durchschnittswerte genauer unter die Lupe – von riskantem Mitarbeiterverhalten (die laschesten Mitarbeitenden sind nicht die, bei denen Sie es vermuten) bis hin zu Ungereimtheiten in der Sicherheitskultur.

Jeder dritte Mitarbeitende glaubt, dass sein Handeln keinen Einfluss auf die Unternehmenssicherheit hat.

Ivanti befragte 6.500 Führungskräfte, Cybersicherheitsexperten und Büroangestellte auf der ganzen Welt, um Folgendes herauszufinden:

- Die Einstellung der Mitarbeitenden zur Cybersicherheit und ihre wahrgenommene Rolle bei der Verteidigung von Unternehmen
- Diagnosen von Sicherheitsexperten zu den wichtigsten Herausforderungen und Schwachstellen
- Das technische Verhalten von Führungskräften und ihr Einsatz für die Cybersicherheitsstrategie

Inhalt:

01 **Generationen-Mythen:**
Sind jüngere Benutzer „besser” in Sachen Sicherheit?

02 **Auswirkungen von Vorfällen:**
Trends bei der Meldung von Vorfällen nach Dienstalter, Geschlecht und Region

03 **Regionale Schulung:**
Geografische Unterschiede bei der Schulung und im Sicherheitsverhalten

04 **Maßnahmen ergreifen:**
Wie Sie in Ihrer Sicherheitsstrategie demografische Merkmale der Endnutzer berücksichtigen können

ivanti

Methodik

Ivanti befragte im 4. Quartal 2022 über 6.500 Führungskräfte, Fachleute für Cybersicherheit und Büroangestellte, um die aktuellen Risiken zu verstehen und herauszufinden, wie sich Unternehmen auf noch unbekannte zukünftige Bedrohungen vorbereiten.

In diesem Bericht konzentrieren wir uns darauf, wie sich bestimmte demografische Merkmale von Endnutzern in Unternehmen auf deren persönliche Einstellungen und Verhaltensweisen auswirken – und wie diese Unterschiede fortgeschrittene Risiken darstellen können, die von Angreifern ausgenutzt werden können.

Demografische Daten der Um-frage

5.202
Büroangestellte
Büroangestellte ≤40 Jahre: 3.609
Büroangestellte>40 Jahre: 2.769

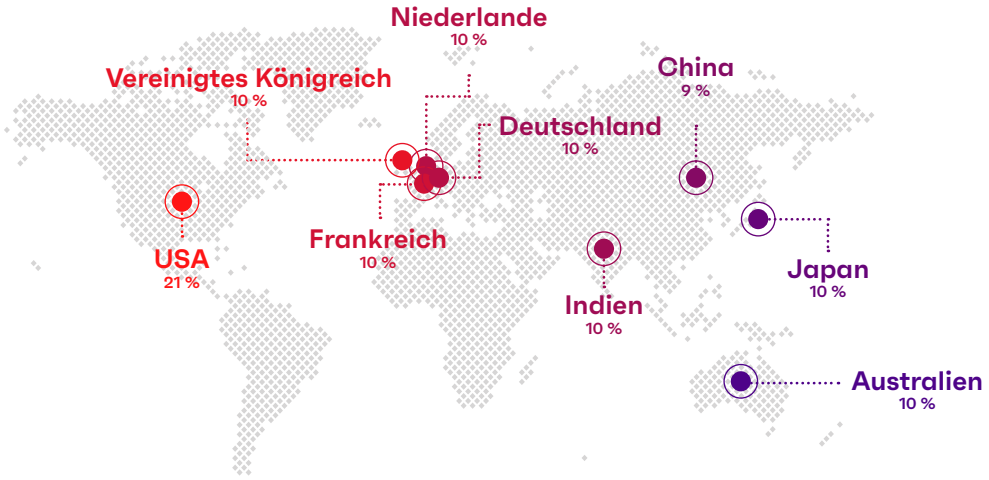
902
Sicherheitsfachkräfte

454
Führungspersonal

3.414
Weiblich

3,119
Männlich

27
Nicht-binär / möchte nicht antworten



01

Generationen-Mythen:

Sind jüngere Benutzer „besser” in Sachen Sicherheit?

ivanti

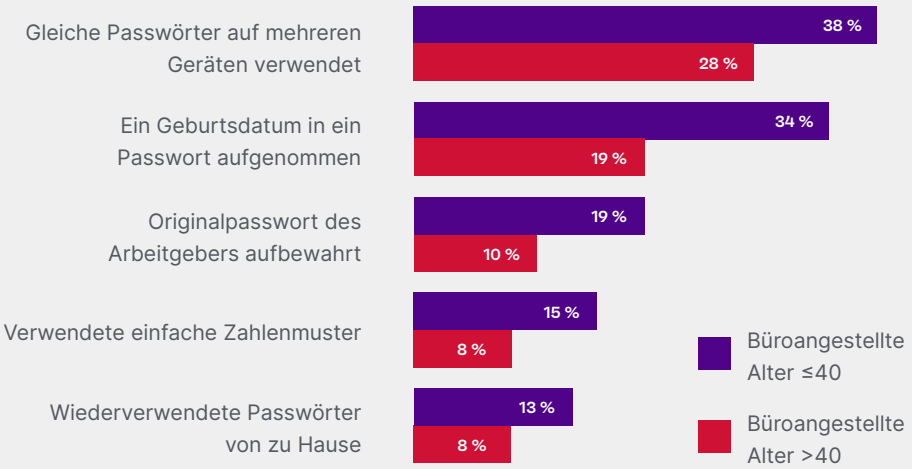
Das aktuelle Problem

Viele gehen davon aus, dass ältere Arbeitnehmer weniger technisch versiert sind – und daher eher zu riskantem Verhalten neigen. In Wirklichkeit ist das Gegenteil der Fall.

Bei jüngeren Berufstätigen (unter 40) ist die Wahrscheinlichkeit, dass sie wichtige Sicherheitsrichtlinien missachten, deutlich höher als bei der Generation X und älter. Das gilt für die Passworthygiene, das Anklicken von Phishing-Links und die gemeinsame Nutzung von Geräten mit Familie und Freunden.

Jüngere Büroangestellte haben eher unsichere Sicherheitsgewohnheiten

F: Wenn Sie bei der Arbeit aufgefordert werden, ein Login-Passwort zu erstellen, welche dieser Dinge haben Sie in den letzten zwei Jahren getan?



	Büroangestellte Alter ≤40	Büroangestellte Alter >40
Hat – gezielt angesprochen – auf einen Phishing-Link geklickt	13 %	8 %
Hat Arbeitsgerät(e) mit Familie oder Freunden geteilt	34 %	19%

Warum das wichtig ist

Diese Versäumnisse, Nachlässigkeiten und Abkürzungen summieren sich bei jüngeren Mitarbeitenden zu deutlich gravierenderen Sicherheitslücken.

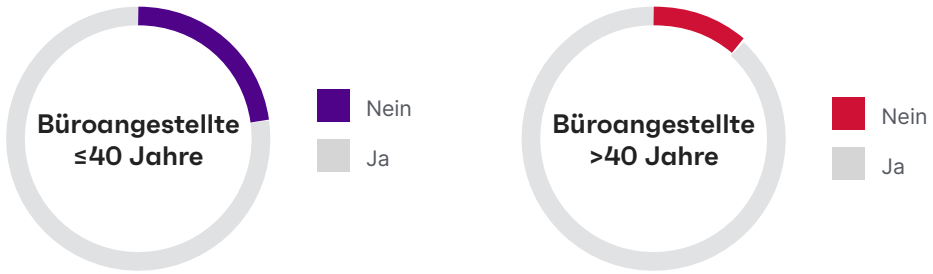
Stereotype über altersbedingtes technisches Wissen können Unternehmen in die Irre führen. Und das Problem hängt nicht nur mit der Cyber-Hygiene zusammen (z. B. Passwortgewohnheiten, gemeinsame Nutzung von Geräten). Die Studie zeigt, dass jüngere Berufstätige auch weniger bereit sind, Gefahren zu melden, wenn sie auf diese stoßen.

Von den Arbeitnehmern unter 40 Jahren gaben 23 % an, dass sie die letzte Phishing-E-Mail oder -Nachricht, die sie erhalten haben, nicht gemeldet haben, verglichen mit 12 % der über 40-Jährigen, die ebenfalls keine Meldung machten.

Der häufigste Grund für die Nichtmeldung?

„Mir war nicht bewusst, dass die Berichterstattung wichtig ist."

Büroangestellte, die ihre letzte Phishing-Nachricht NICHT an die Sicherheitsabteilung gemeldet haben



Stereotype über ältere Arbeitnehmer sind besonders heimtückisch, weil die meisten Arbeitnehmer im Tech-Bereich jünger sind und daher eher glauben, dass ihre älteren Kollegen keine Ahnung haben oder anfällig sind.

Eine Studie unter 2 250 Fachkräften im Vereinigten Königreich ergab beispielsweise, dass technische Angestellte ihre Kollegen als „gestrig" und „zu alt für ihren Job" ansehen, wenn sie 38 Jahre alt sind.[1]

(Dabei ist zu beachten, dass dies im Vergleich zu ihren Kollegen aus der Tech-Branche gilt, nicht zu den durchschnittlichen Arbeitnehmern, die eher weniger technikaffin sind).

Diese Ergebnisse unterstreichen, warum sich Unternehmen weniger auf das individuelle Urteilsvermögen ihrer Mitarbeitenden verlassen sollten. Sondern eher auf technische Maßnahmen, die das Befolgen von Regeln erleichtern.

Noch besser: Unternehmen sollten Automatisierungen in Betracht ziehen, die vollständig im Hintergrund ablaufen und von denen die Endbenutzer nicht einmal wissen, dass sie existieren.

„Die Annahme, dass jüngere Mitarbeitende sicherheitsbewusster und technisch versierter sind, ist überholt und sogar gefährlich. Unternehmen sollten diese Annahmen auf den Prüfstand stellen, indem sie interne Untersuchungen durchführen, die die Einstellung ihrer eigenen Mitarbeitenden zu Sicherheitsrisiken und ihre Rolle bei deren Bewältigung erfassen."

Daniel Spicer
Chief Security Officer bei Ivanti

02

Auswirkungen von Vorfällen:

Trends bei der Meldung von Vorfällen nach Dienstalter, Geschlecht und Region

ivanti

Das aktuelle Problem

Um die Sicherheit eines Unternehmens zu gewährleisten, müssen Informationen über Sicherheitsvorfälle oder -verletzungen nahezu in Echtzeit zur Verfügung stehen. Unsere Untersuchungen zeigen, dass einige Mitarbeitende weniger dazu tendieren, Gefahren zu melden.

Melden sich Ihre Mitarbeitenden schnell, wenn sie Sicherheitsbedenken haben? Die Untersuchungen von Ivanti zeigen, dass bestimmte Segmente Ihrer Belegschaft möglicherweise zögern, sich zu melden – ein Umstand, den Unternehmen bei der Entwicklung von Informations- und Schulungsprogrammen berücksichtigen sollten.

Dienstalter

Die größte Variable bei Meldungen von Vorfällen ist das Dienstalter. Zweiundsiebzig Prozent der von uns befragten Führungskräfte gaben an, dass sie sich mit einer Frage oder einem Anliegen an einen Cybersecurity-Mitarbeitende gewandt haben, verglichen mit nur 28 Prozent der Büroangestellten.

Geschlecht

Bei Frauen ist die Wahrscheinlichkeit, dass sie dasselbe tun, geringer als bei Männern. Achtundzwanzig Prozent haben sich mit einer Frage oder einem Anliegen an einen Cybersicherheitsmitarbeitenden gewandt, verglichen mit 36 Prozent der Männer.

Wussten Sie das schon?

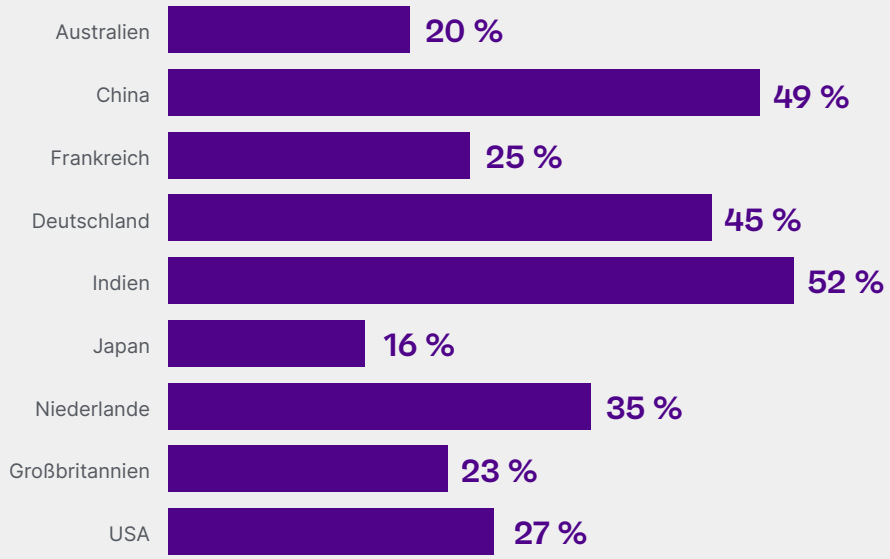
Führungskräfte geben doppelt so häufig als Büroangestellte an, dass sie Sicherheitsinteraktionen "unangenehm" oder "peinlich" empfinden.[2]

Diese häufigeren, aber negativen Sicherheitsinteraktionen können dazu führen, dass Führungskräfte verstärkt externen, nicht genehmigten technischen Support in Anspruch nehmen – Berichten zufolge viermal so häufig wie Büroangestellte.

Die Bereitschaft der Benutzer, sich an die Sicherheitsabteilung zu wenden, ist von Land zu Land sehr unterschiedlich.

So hat sich beispielsweise fast die Hälfte der Büroangestellten in China mit einer Frage oder einem Anliegen an das Sicherheitsteam gewandt, während es in Australien nur 20 % sind.

Büroangestellte, die sich mit einer Frage oder einem Anliegen an den Sicherheitsdienst gewandt haben, nach Region



ivanti

Warum das wichtig ist

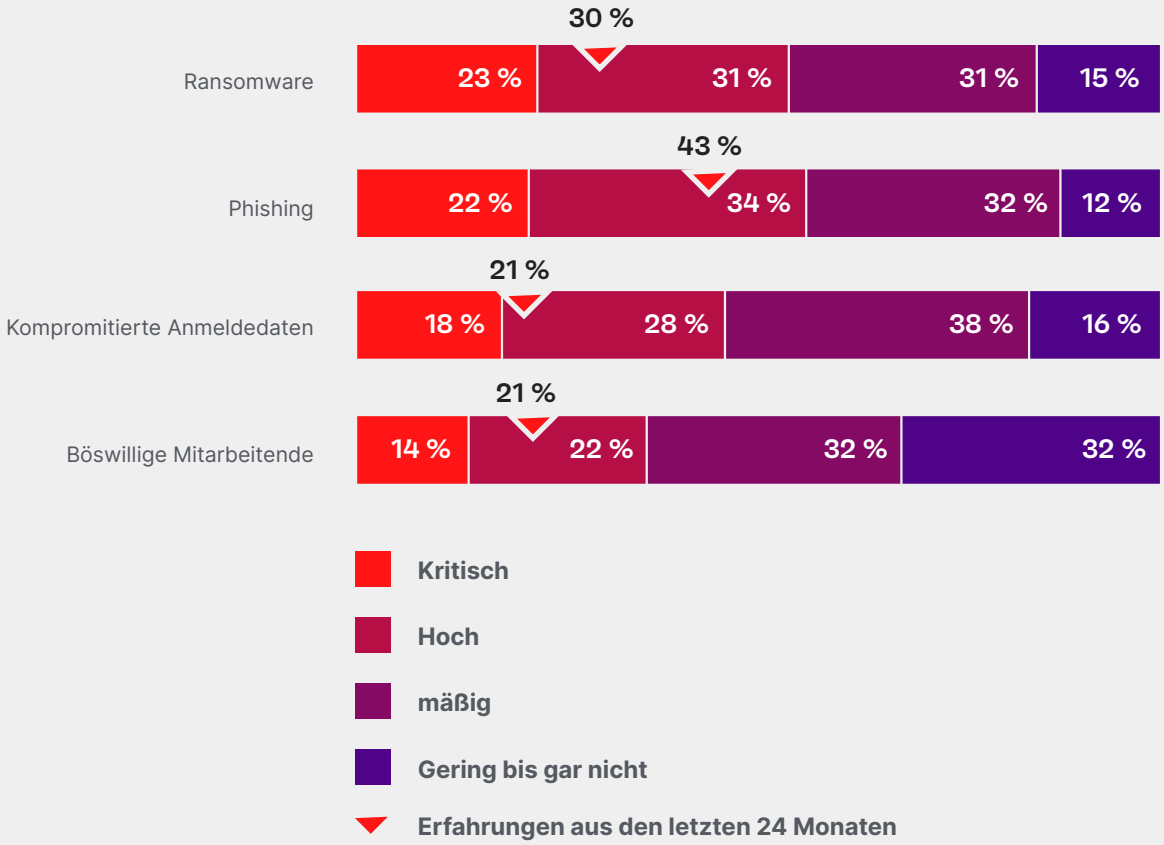
Ihre Sicherheitslage hängt von Tausenden von Mitarbeitenden ab und wie diese sich verteidigen. Verstehen diese Mitarbeitenden, dass sie wertvolle Mitglieder des erweiterten Sicherheitsteams sind?

Im Rahmen der großen Ivanti-Studie zur Sicherheitsbereitschaft wurden Sicherheitsexperten nach ihren größten branchenweiten Sicherheitslücken befragt. Ransomware und Phishing belegten die Plätze 1 und 2.

Und diese Bedrohungen werden von Jahr zu Jahr gefährlicher – vor allem dank der Fortschritte in der generativen KI, die das Erkennen von Phishing erschwert.

Die am besten bewerteten Sicherheitsbedrohungen und Schwachstellen bieten eine Chance zur Verteidigung für Mitarbeitende

F: Bitte bewerten Sie das für 2023 prognostizierte Bedrohungsniveau in Ihrer Branche für jede der folgenden …



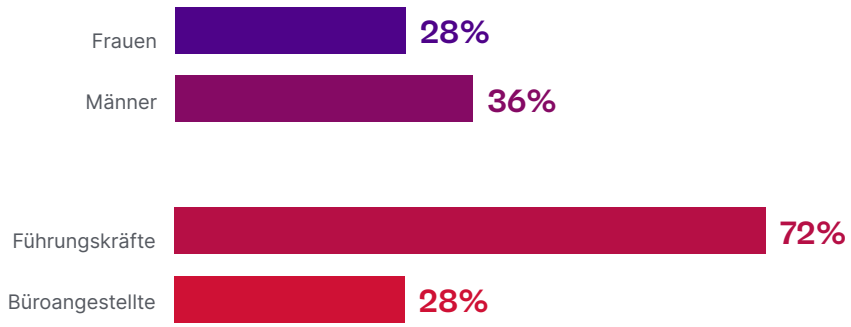
Diese beschleunigten Bedrohungen und erhöhten Risiken bedeuten, dass sich Ihre Mitarbeitenden wohl fühlen müssen, wenn sie sich an Ihr Sicherheitsteam wenden – selbst wenn der einzige „Beweis“, den sie für einen bevorstehenden Angriff haben, ein nagender Zweifel ist.

(Einige Beispiele: eine untypische Überweisungsanfrage, eine verdächtige Rechnungserinnerung oder ein unaufgeforderter Link zum Zurücksetzen des Passworts).

Schließlich ist bei einem aktiven Sicherheitsvorfall Schnelligkeit der wichtigste Faktor, wenn es darum geht, einen Angriff abzuwehren.

Wenn Arbeitgeber Stimmungsumfragen durchführen, um die Einstellung ihrer Mitarbeitenden zu verstehen, sollten sie die demografischen Muster und Sicherheitslücken genauer untersuchen.

Benutzer, die mit einem Sicherheitsmitarbeitenden in Kontakt getreten sind und Fragen oder Bedenken hatten



"Wir haben einige fortgeschrittene Phishing-Versuche erlebt, und die Mitarbeitende wussten überhaupt nicht, dass sie angegriffen wurden. Diese Art von Angriffen ist in den letzten zwei Jahren sehr viel raffinierter geworden - selbst unsere erfahrensten Mitarbeitenden fallen darauf herein."

— 2023 Press Reset-Umfrageteilnehmer[3]

03

Regionale Fortbildung:

Geografische Unterschiede in der Fortbildung und im Sicherheitsverhalten

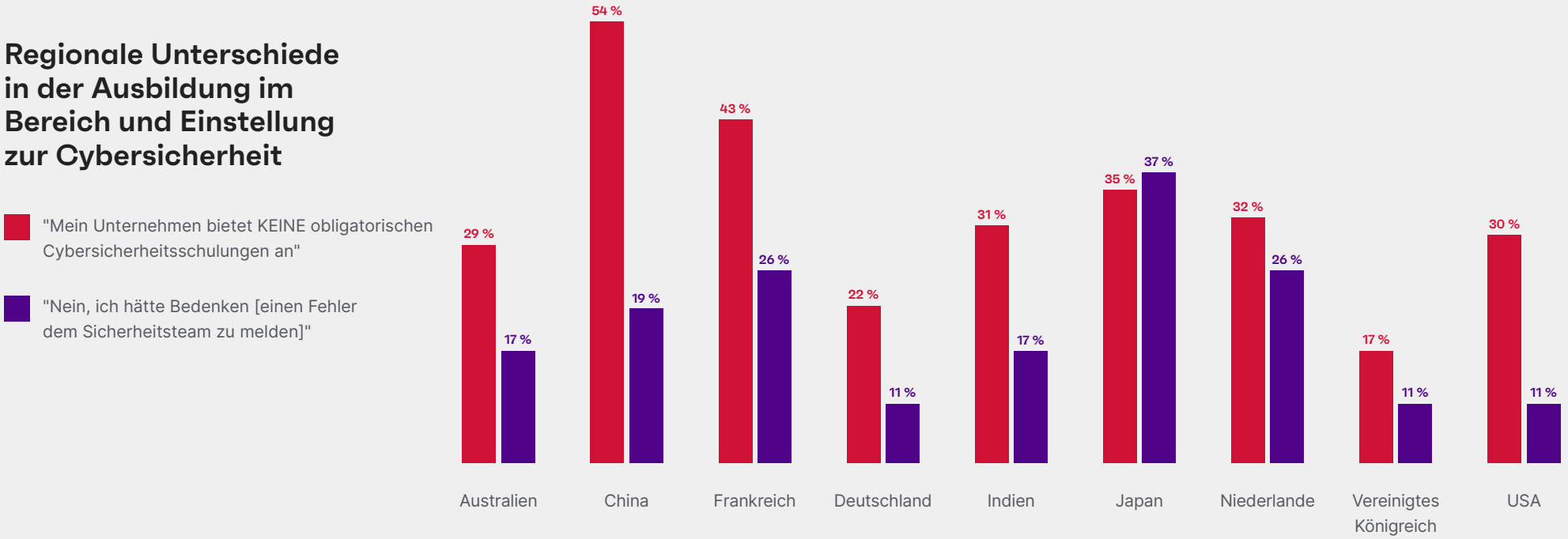
ivanti

Das aktuelle Problem

Kultur und Schulungsprogramme einer Organisation haben einen erheblichen Einfluss auf die Sicherheitsbereitschaft, aber unsere Untersuchungen zeigen, dass beides auf Länderebene unterschiedlich ausgeprägt ist.

Die Untersuchungen von Ivanti zeigen erhebliche Unterschiede in der Sicherheitskultur auf Länderebene – sowohl in Bezug auf die von der Organisation angebotene Schulung als auch auf die Einstellung der Führungskräfte und der Mitarbeitenden im Büro.

Regionale Unterschiede in der Ausbildung im Bereich und Einstellung zur Cybersicherheit



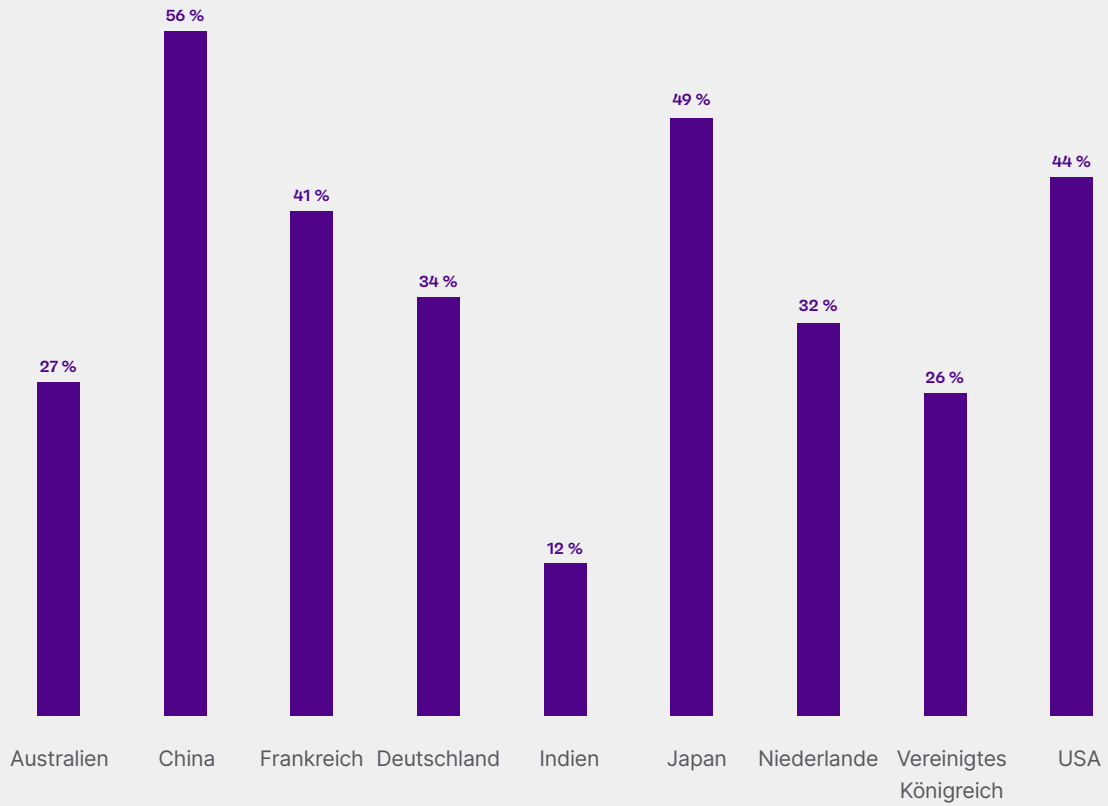
Warum das wichtig ist

Viele Unternehmen verfolgen einen Top-Down-Ansatz in Bezug auf Schulungen und Sicherheitskultur, aber die Studie zeigt, dass es entscheidend ist, die lokale Sicherheitskultur – und sogar die lokale Kultur – zu verstehen, um einen stimmigen Plan zu erstellen.

Ganz gleich, woher sie kommen, jeder neue Mitarbeitende bringt seine eigenen Sicherheitslücken in das Unternehmen ein, ob absichtlich oder nicht. Bei unzureichend geschulten Mitarbeitenden besteht die Gefahr, dass die Abwehrbereitschaft des gesamten Unternehmens beeinträchtigt wird.

Um dieses Risiko zu minimieren, müssen Unternehmen auf globaler und regionaler Ebene in solide Einführungs- und fortlaufende Sicherheitsschulungsprogramme investieren.

Büroangestellte: "Meine Handlungen haben KEINEN Einfluss auf die Fähigkeit meines Unternehmens, sich [vor Cyber-Bedrohungen] zu schützen."



Wie die lokale Kultur mit globalen Sicherheitsprogrammen zusammenwirkt

Die Kultur kann Einfluss darauf haben, wie Unternehmen ihre Assets und Mitarbeitenden schützen und wie sie auf einen Angriff reagieren.

Mögliche kulturelle Sicherheitsherausforderungen

Unbehagen der Mitarbeitenden bezüglich Schulungen auf globaler Ebene (z. B. mangelhafte Übersetzung von Schulungsmaterialien in die lokale Sprache und Kultur).

Unbehagen der Mitarbeitende bezüglich neuer Normen oder Regeln, die nicht auf lokaler Ebene "sozialisiert" wurden.

Eine Top-Down-Kultur in den lokalen Niederlassungen, die dem Einzelnen wenig Raum lässt, um Fehler oder Bedenken zu melden.

Unzureichende Sicherheitsunterstützung für lokale Niederlassungen: Mitarbeitende, die Fragen oder Bedenken haben, müssen sich beispielsweise an ein Mitglied des Sicherheitsteams in einem anderen Land wenden - und dabei sprachliche und kulturelle Barrieren überwinden.

"Diese länderspezifischen Unterschiede sind ein interessanter Weg, die Bereitschaft zu untersuchen.

"Es ist einfach - und üblich - für ein Sicherheitsteam, die Sicherheit danach zu beurteilen, was in ihrer größten oder nächstgelegendsten Niederlassung vor sich geht.

"Diese Untersuchung zeigt, wie wichtig es ist, detailliertere Daten zu erforschen und Sicherheitsverfahren an jedem Standort aufzudecken - sei es in der Firmenzentrale, in Forschungs- und Entwicklungseinrichtungen, in Außenstellen der Lieferkette oder in Produktionsstätten."

Daren Goeson
SVP, Produktmanagement bei Ivanti

04

Maßnahmen ergreifen:

Wie Sie in Ihrer Sicherheitsstrategie demografische Merkmale der Endnutzer berücksichtigen können

ivanti

Maßnahmen ergreifen

Hervorragende Leistungen auf breiter Ebene können über einzelne Risikofelder hinwegtäuschen.

Lassen Sie uns die Sicherheitsrisiken im Zusammenhang mit demografischen Merkmalen im Detail untersuchen. So können wir herausfinden, wie Sie die demografischen Risiken in Ihrem Unternehmen bewerten können und wie Sie Ihren Ansatz anpassen können, um die Probleme zu lösen.

5 Wege zur Beseitigung Ihrer versteckten Risiken

1. ### Befragen Sie Ihre Mitarbeitenden.

   Sehen Sie, wie die Sicherheitseinstellungen und das Verhalten Ihrer Benutzer im Vergleich zu diesen globalen Benchmarks aussehen.

2. ### Hinterfragen Sie Ihre Klischees.

   Untersuchen Sie die möglichen Annahmen und Vorurteile, die Ihr Sicherheitsteam selbst hat.

3. ### Lokalisieren Sie Ihr Material.

   Gehen Sie über die einfache Übersetzung hinaus, damit Ihre Schulungen und Richtlinien nicht auf regionale Fehlinterpretationen stoßen.

4. ### Gestalten Sie Ihr Backend neu.

   Eliminieren Sie die Beteiligung der Mitarbeitenden, wo immer Sie können, um die automatische Einhaltung der Vorschriften zu erhöhen.

5. ### Bauen Sie Ihre Kultur neu auf.

   Steigern Sie das Vertrauen der Mitarbeitenden in die Reaktionen Ihres Sicherheitsteams und erhöhen Sie so die allgemeine Unternehmenssicherheit.

Versteckte Risiken – Abhilfemaßnahme 1:

Befragen Sie Ihre Mitarbeitenden, um die einzigartigen demografischen Gewohnheiten Ihres Unternehmens zu ermitteln.

Nutzen Sie eine anonyme Umfrage, um Erkenntnisse über Ihren Mitarbeiterstamm zu gewinnen, und achten Sie dabei besonders auf mögliche demografische Unterschiede. (Gibt es unerwartete Ergebnisse? Antwortmuster, die Ihren ursprünglichen Annahmen widersprechen?)

Nutzen Sie die Ergebnisse, um Ihre Schulungs- und Aufklärungsbemühungen zu verstärken, indem Sie die Lösungen auf die Teile Ihrer Mitarbeiterschaft abstimmen, die zusätzliche Unterstützung benötigen.

Beispielfragen für eine anonyme Studie zur Einstellung der Mitarbeitenden

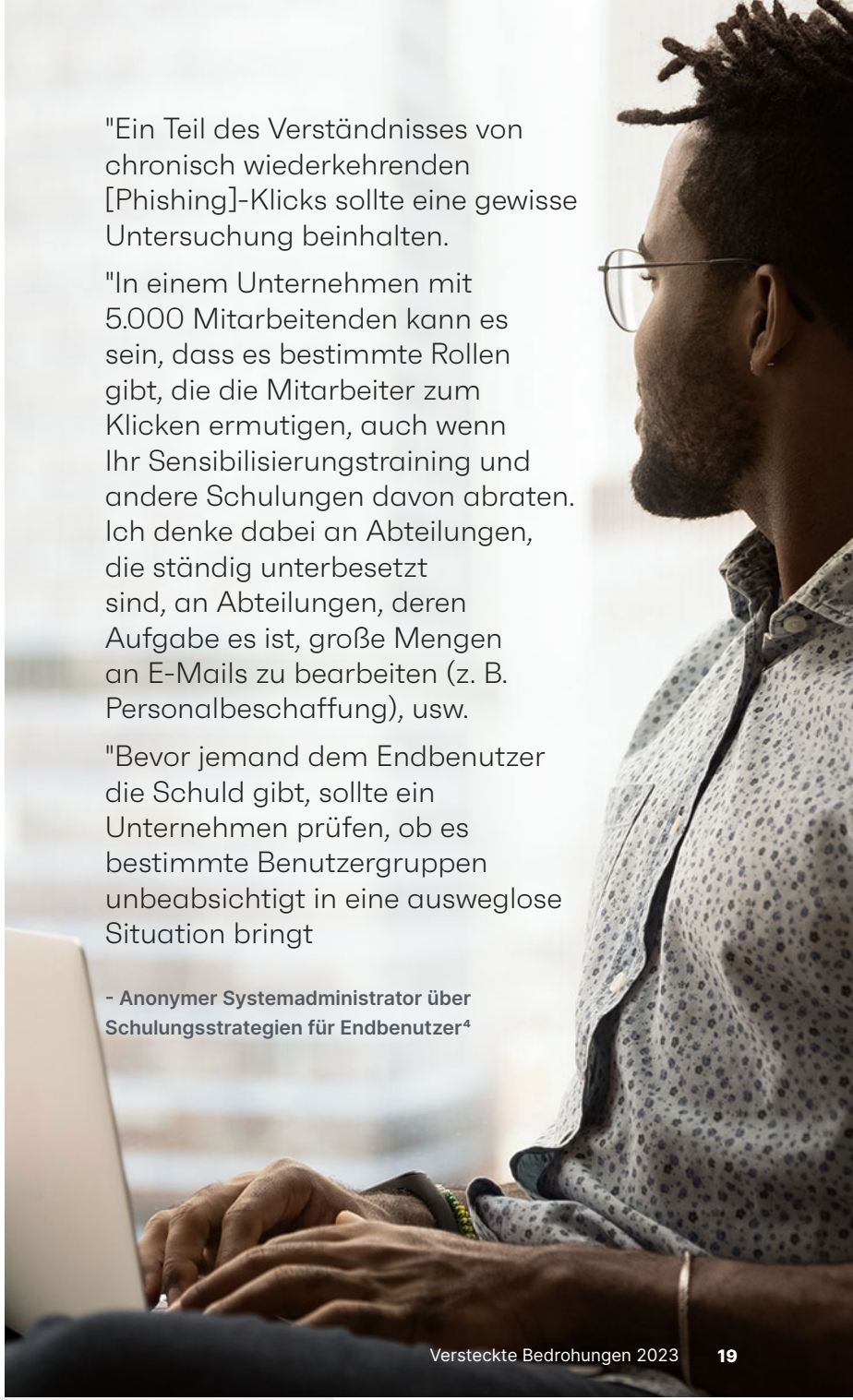
Können Sie einen Phishing-Versuch erkennen?

Wurden Ihnen Ressourcen und/oder Tools zur Verfügung gestellt, um einen Phishing-Versuch zu erkennen?

Fühlen Sie sich wohl, wenn Sie dem Sicherheitsteam eine Frage stellen?

"Nein, ich hätte Bedenken [einen Fehler dem Sicherheitsteam zu melden]"

Glauben Sie, dass Ihr Handeln Auswirkungen auf die Sicherheit des Unternehmens hat?



"Ein Teil des Verständnisses von chronisch wiederkehrenden [Phishing]-Klicks sollte eine gewisse Untersuchung beinhalten.

"In einem Unternehmen mit 5.000 Mitarbeitenden kann es sein, dass es bestimmte Rollen gibt, die die Mitarbeiter zum Klicken ermutigen, auch wenn Ihr Sensibilisierungstraining und andere Schulungen davon abraten. Ich denke dabei an Abteilungen, die ständig unterbesetzt sind, an Abteilungen, deren Aufgabe es ist, große Mengen an E-Mails zu bearbeiten (z. B. Personalbeschaffung), usw.

"Bevor jemand dem Endbenutzer die Schuld gibt, sollte ein Unternehmen prüfen, ob es bestimmte Benutzergruppen unbeabsichtigt in eine ausweglose Situation bringt

- Anonymer Systemadministrator über Schulungsstrategien für Endbenutzer[4]

Versteckte Risiken – Abhilfemaßnahme 2:

Hinterfragen Sie Stereotypen über die digitale Gewandtheit und Sicherheit der Benutzer.

Lassen Sie Ihr Sicherheitsteam eine anonyme Umfrage ausfüllen, die ihre Annahmen über verschiedene Mitarbeitergruppen untersucht. Vergleichen Sie diese Ergebnisse dann mit den Ergebnissen Ihrer allgemeinen Mitarbeiterbefragung, um Annahmen aufzudecken, die nicht nur unfair, sondern auch unwahr sind – und um herauszufinden, wie sich diese Stereotypen auf Ihre Sicherheitslage auswirken könnten.

3 von Menschen verursachte Schwachstellen, die Sicherheitsexperten betreffen

Zufriedenstellend

Ein spezifischer Entscheidungsfindungsprozess, der ein Minimum an praktikablem Ergebnis anstrebt, anstatt sich voll und ganz dem bestmöglichen Ergebnis zu widmen.[5]

Während die Fokussierung durch diesen Prozess ressourcenbeschränkten Teams helfen kann, kann das, was ein Team als "nicht wichtig genug" für die grundlegende Umsetzung aufgibt, beeinflusst werden oder sich gänzlich verschieben, wenn andere Perspektiven berücksichtigt werden.

Vernachlässigung der Wahrscheinlichkeit

Wie Menschen oft die Wahrscheinlichkeit des Eintretens eines Ereignisses nicht bedenken, wenn seine Auswirkungen groß sind - vor allem, wenn hohe Emotionen im Spiel sind.

Studien zeigen, dass Sicherheitsexperten oft eher dazu neigen, unwahrscheinlichen, aber sehr schädlichen Ereignissen Priorität einzuräumen und Abhilfe zu schaffen, selbst wenn kleinere Risiken - wie das Versäumnis eines Endanwenders, einen möglichen Sicherheitsvorfall zu melden - statistisch gesehen wahrscheinlicher sind.[6]

Selbstüberschätzung

Hochqualifizierte Personen neigen dazu, ihre Fähigkeiten zu überschätzen, was dazu führt, dass sie ihre Lösungen nicht mit Referenzen von Fachleuten vergleichen oder kein Feedback von Kollegen einholen.

Eine Studie über Sicherheitsexperten ergab, dass je mehr Allgemeinbildung ein Sicherheitsexperte vorweisen konnte, desto anfälliger war er für Entscheidungsfehler - weil er glaubte, die richtige Antwort bereits zu kennen![7]

Versteckte Risiken – Abhilfemaßnahme 3:

Verstehen Sie, wie Ihre globale Sicherheitskultur übersetzt und lokalisiert wird.

Bei einem abteilungsübergreifenden Programm wie Ihren Sicherheitsschulungen und -richtlinien reicht es nicht aus, die Materialien in die richtige Sprache zu übersetzen. Sie müssen Ihr Sicherheitsmaterial „lokalisieren", damit die Kernaussage alle potenziell verwirrenden kulturellen Hürden überwindet.

Beraten Sie sich also proaktiv mit Ihren lokalen und regionalen Teams und bitten Sie sie vor der Übersetzung um ihre Meinung und Zustimmung zu den neuen Materialien.

Und denken Sie daran: Lokale Führungskräfte können mächtige Botschafter sein! Sie können Ihre Sicherheitsbotschaft auf natürliche Weise weitergeben, so dass andere regionale Mitarbeitende sie verstehen, ihr vertrauen und ihr folgen.

Lokalisierungsprüfungen für Sicherheitsprogramme und Kommunikation

Farbe

Chinesische Nutzer sehen rot markierte Einträge möglicherweise als Glücksfall und positiv an - und erkennen nicht sofort, dass das westliche Home Office "Stopp" bedeutet xxx Grün kann negative Reaktionen bei indonesischen und südamerikanischen Konsumenten auslösen, die Grün mit Untreue bzw. Tod assoziieren.[8]

Sport

In einer Studie über englisch/arabisch/arabisch-englisches Material wurde festgestellt, dass die Basisübersetzungen in 37 % der Fälle "unangemessene" Ersetzungen für Sport-Idiome enthielten.[9] Andere Studien über Sport-Idiom-Übersetzungen haben ähnliche Schwierigkeiten für Polnisch[10], Persisch/Farsi[11] und praktisch jede andere Sprache festgestellt.

Symbole

In vielen englischsprachigen Ländern symbolisiert ein Häkchen eine "richtige" oder "vollständige" Antwort. In Schweden und Japan hingegen markiert ein Häkchen eine falsche Antwort, während ein "R" oder "O" eine richtige Antwort kennzeichnet.[12] Sogar die Bedeutung von Emoji ändert sich je nach Generation[13] und Region[14]!

Versteckte Risiken – Abhilfemaßnahme 4:

Entwerfen Sie Ihr technisches Stack so, dass er möglichst wenig Unstimmigkeiten und Inkonsistenzen bei den Benutzern verursacht.

Anstatt sich darauf zu verlassen, dass einzelne Benutzer die Sicherheitsprotokolle einhalten, sollten Sie eine stärkere Back-End-Automatisierung aufbauen, die den Endbenutzern verborgen bleibt – Eingriffe, die die Einhaltung der Vorschriften reibungslos machen.

3 gängige Sicherheitsupgrades, die die Probleme für Endbenutzer verringern

Just-in-time-Sicherheitsupdates

Die meisten Mitarbeitenden fahren ihre Computer nur ungern herunter und starten sie für Updates neu. Daher neigen sie dazu, den Prozess auf unbestimmte Zeit zu verschieben - oder vergessen, ihn neu zu beginnen!

Verwenden Sie stattdessen ein System, das automatisch einen Neustart innerhalb eines bestimmten Zeitrahmens erzwingt, dem Benutzer aber die Möglichkeit gibt, diesen Neustart außerhalb seiner Arbeitszeit zu planen, um so zeitnahe und dennoch bequeme Updates zu ermöglichen.

Moderne Passwortrichtlinien

Kürzlich haben viele globale Cybersecurity-Frameworks die ältere Empfehlung, Passwörter zu wechseln, wenn es keine Beweise dafür gibt, dass ein Benutzer keine Geheimnisse preisgibt, stillschweigend gestrichen.15 Anstatt die Sicherheit zu erhöhen, fördern die Richtlinien zum Ablauf von Passwörtern eher eine schlechte Passworthygiene, da die Benutzer damit zu kämpfen haben, sich Passwörter auszudenken - und zu merken! - neue Passphrasen oder PINs.[16]

Erwägen Sie stattdessen den Einsatz von Passwortmanagern, Single-Sign-On-Richtlinien oder passwortlosen Technologien - ohne Benutzerspeicher oder Notizzettel.

Stille Richtlinien zur akzeptablen Nutzung (AUP) - mit integrierter Durchsetzung

Auch wenn Ihre Mitarbeitenden bei der Einarbeitung einen Überblick über die AUP Ihres Unternehmens erhalten, sind Richtlinien ohne Durchsetzung das Papier nicht wert, auf dem sie gedruckt sind.

Konfigurieren Sie Ihre gesamte digitale Infrastruktur für bestimmte Benutzerprofile und Zugriffsberechtigungen - mit einer einfachen Möglichkeit für Benutzer, erweiterten Zugriff zu beantragen, wenn die grundlegenden Berechtigungen für ihre spezielle Arbeitsbelastung nicht ausreichen.[3]

Versteckte Risiken – Abhilfe 5:

Proaktiver Aufbau einer offenen und einladenden Sicherheitskultur.

Die Ergebnisse dieses Hidden Threats-Berichts unterstreichen die Notwendigkeit einer kooperativen und positiven Sicherheitskultur in jedem Unternehmen. Letztlich sollten die Mitarbeitenden nicht verunsichert sein, ob sie sich an Sicherheitsexperten zu wenden sollten – egal wie klein die Frage oder wie dumm der Fehler auch sein mag.

Nur in einer Sicherheitskultur, die nicht auf Bestrafung setzt, können die Sicherheitsteams genügend Zusammenarbeit von den Benutzern erwarten, um das gesamte Unternehmen angemessen zu schützen.

"Wiederholte Clicker [bei Sicherheitstrainingstests] sind nicht wirklich ein Problem. Oder besser gesagt, sie sind ein relativ vorhersehbares Problem.

Wenn man weiß, dass es jemandem Betrugsversuche nur schwer erkennen kann, braucht er Unterstützung in Form von Leitplanken – keine Repressionen oder noch unwirksamere Schulungen."

- Anonymer Systemadministrator über Sicherheitstrainingslösungen[17]

4 Grundpfeiler einer starken Sicherheitskultur

Offen

Die Mitarbeitenden haben keine Bedenken, wenn sie einen Vorfall melden, und werden für ihre Ehrlichkeit und Transparenz belohnt. Sie fühlen sich wohl, wenn sie sich an das Sicherheitsteam wenden, egal wie trivial ihre Frage ist.

Iterativ

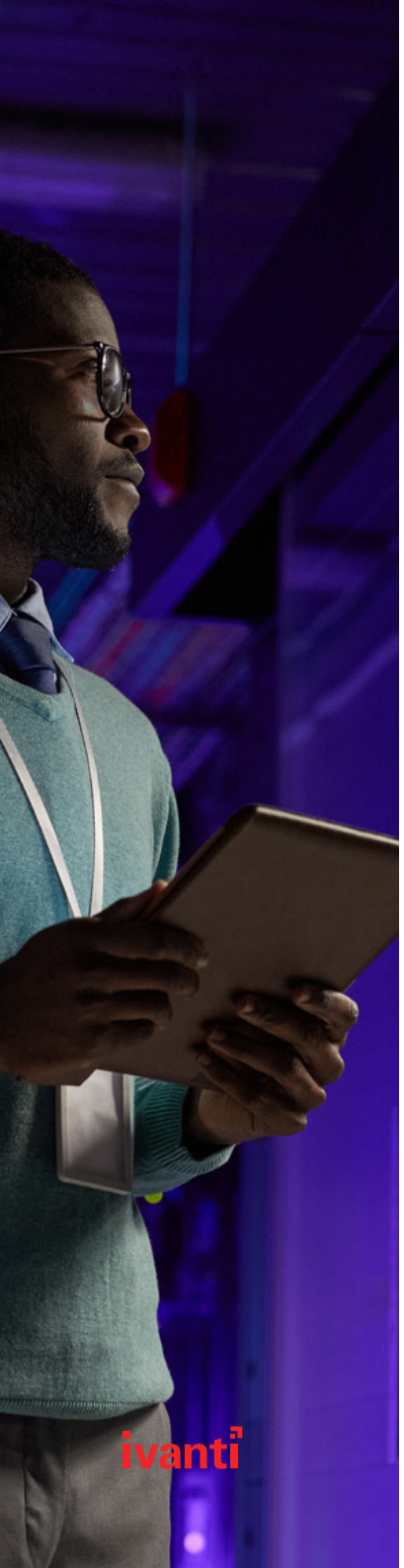
Das Unternehmen bietet häufige, sich wiederholende Schulungen an, die für die Mitarbeitenden attraktiv sind - von formellen Schulungsworkshops und regelmäßigen unternehmensweiten Mitteilungen bis hin zu spielerischen Sicherheitswettbewerben mit realen Sicherheitsszenarien.

Gut konzipiert

Das Verhalten der Mitarbeitenden wird durch technologiegestützte Verhaltensinterventionen geschärft. Diese Technologien sollten so gut konzipiert sein, dass sie Schatten-IT-Umgehungen und die allgemeine Nichteinhaltung von Vorschriften erheblich reduzieren.

Integrierte Funktionen

Die Verantwortung für die Unternehmenssicherheit wird von allen geteilt, und Ihre Mitarbeitenden sind daran interessiert, die Sicherheit des Unternehmens zu gewährleisten.



Referenzen

1. Sevilla, C. (2022, May 23). Everyday ageism in the tech industry. From CWJobs: https://www.cwjobs.co.uk/advice/ageism-in-tech
2. Ivanti. (2023, August 29). 2023 Executive Security Spotlight: New research from Ivanti shows real risks facing the C-suite. From Ivanti: https://www.ivanti.com/resources/v/doc/ivi/2773/17cca519291d
3. Ivanti. (2023, December 12). Press Reset: A 2023 Cybersecurity Status Report. From Ivanti: https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
4. u/CyberAndFolkloreGuy. (2023, January 19). Security Awareness: How to properly address colleagues who repeated fail Phishing tests? From Reddit: https://www.reddit.com/r/cybersecurity/comments/10g4688/comment/j55k4cn/
5. Frankenfield, J. (2022, August 23). Satisficing: Definition, How the Strategy Works, and an Example. From Investopedia: https://www.investopedia.com/terms/s/satisficing.asp
6. De Wit, J. J., Pieters, W., & Van Gelder, P. H. (2022). Individual Preferences In Security Risk Decision Making: An Exploratory Study Under Security Professionals. WIT Transactions on The Built Environment, 187-199. doi:10.2495/SAFE210161
7. De Wit, J., Pieters, W., Jansen, S., & van Gelder, P. (2021). Biases in Security Risk Management: Do Security Professionals Follow Prospect Theory in Their Decisions? Journal of Integrated Security and Safety Science, 1(1), 34-57. doi:https://doi.org/10.18757/jisss.2021.1.5700
8. Eriksen Translations. (2020, February 3). How Translating Colors Across Cultures Can Help You Make a Positive Impact. From Erksen Translations: https://eriksen.com/marketing/color_culture/
9. Nasser, L., & Al-Aazzawi, K. (2022). Context Impact in Translating Sport Idiomatic Expressions from English into Arabic with Regard to Types of Idioms. Adab Al-Rafidayn Journal, 1-26. doi:10.33899/radab.2021.170415
10. Mazurkiewicz, M. (2014). Sports Vocabulary and Idioms – Some Observations About the Specificty of English-Polish and Polish-English Translation. Cultures and Literatures in Translation, 140-153. From https://www.academia.edu/40425597/Sports_Vocabulary_and_Idioms_Some_Observations_about_the_Specificity_of_English_Polish_and_Polish_English_Translation
11. Suzani, S. M. (2007). Sports Idioms and Duality of Meaning in Translation. Iranian Journal of Translation Studies. From https://journal.translationstudies.ir/ts/article/view/126

12. Grove, L. (1989). Signs of the times: graphics for international audiences. International Professional Communication Conference 'Communicating to the World', 137-141. doi:10.1109/IPCC.1989.102119

13. Brants, W., Sharif, B., & Serebrenik, A. (2019). Assessing the Meaning of Emojis for Emotional Awareness - A Pilot Study. Companion Proceedings of The 2019 World Wide Web Conference, 419–423. doi:https://dl.acm.org/doi/abs/10.1145/3308560.3316550

14. Gao, B., & VanderLaan, D. P. (2020). Cultural Influences on Perceptions of Emotions Depicted in Emojis. Cyberpsychology, Behavior, and Social Networking, 567-570. doi:https://doi.org/10.1089/cyber.2020.0024

15. National Institute of Standards and Technology (NIST). (2020, March 03). NIST Special Publication 800-63B. From https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

16. WIlson, K. R.-H. (2020, March 9). The Debate Around Password Rotation Policies. From SANS Institute: https://www.sans.org/blog/the-debate-around-password-rotation-policies/

17. u/securebxdesign. (2023, April). What does your policy/training look like for people who fail phishing campaigns? From Reddit: https://www.reddit.com/r/cybersecurity/comments/13csxs0/comment/jjk37bo/

2023 Versteckte Bedrohungen

Wie sich die Demographie der Beschäftigen auf Ihre Sicherheitslage auswirkt

Teil der Ivanti-Reihe Cybersecurity Status Report

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com