ivanti

Executive Security Spotlight 2023

Neue Untersuchung von Ivanti zeigt reale Risiken für die Chefetage

Teil von Ivantis Report-Serie zum Status der Cybersecurity

Cybersecurity-Bedrohungen für Führungskräfte abwehren

In der Regel wollen Unternehmen nicht glauben, dass mangelnde Unterstützung durch die Geschäftsleitung einer herausragenden Cybersicherheit im Weg steht. In unserem ersten Press-Reset-Bericht gaben nur 21 % der Führungskräfte und Sicherheitsexperten an, dass die mangelnde Unterstützung durch die Geschäftsleitung ein Hindernis für die Sicherheit darstellt. Das sind ganze 16 Prozentpunkte weniger als das am häufigsten genannte Hindernis, die Komplexität der Tech-Stacks (37 %).

Dennoch ist es wahrscheinlicher, dass Führungskräfte gefährliches Sicherheitsverhalten an den Tag legen, als es den Sicherheitsteams bisher bewusst war.

Sie geben fünfmal häufiger an dass sie sich absichtlich unbefugten Zugang zu sensiblen Kunden- oder Unternehmensdaten verschafft haben.

Mehr als eine von drei Führungskräften hat schon einmal auf einen Phishing-Link geklickt – viermal so häufig wie andere Büroangestellte.

Und es ist viermal wahrscheinlicher, dass sie ein Firmenpasswort an jemanden außerhalb des Unternehmens weitergeben.

Wie schützen Sie die Top-Führungskräfte – die am meisten gefährdete Mitarbeitergruppe –, wenn diese zwar sagen, dass sie die Vorgaben Ihres Unternehmens akzeptieren, aber häufig die Sicherheitsprotokolle umgehen? Eine neue Studie von Ivanti enthüllt die schwierige Wahrheit.

ivanti

Dieser Bericht zeigt:

Die beträchtliche Kluft zwischen den erklärten Prioritäten der Führungskräfte (z.B. der Kauf von Sicherheitsrichtlinien) und ihren Handlungen am Arbeitsplatz.

Wie die Sicherheitsgewohnheiten von Führungskräften ein wesentlich höheres Risiko zwischen den Führungskräften und den Teams, die für ihre Sicherheit verantwortlich sind - was dazu führen kann, dass die Führungskräfte externe IT-Unterstützung in Anspruch nehmen, anstatt interne Hilfe anzufordern.

Das derzeitige Misstrauen zwischen den Führungskräften und den Teams, die für ihre Sicherheit verantwortlich sind - was dazu führen kann, dass die Führungskräfte externe IT-Unterstützung in Anspruch nehmen, anstatt interne Hilfe anzufordern.

Praktische Wege zur Sicherung Ihres Unternehmens mit stillen, hinter den Kulissen stattfindenden Implementierungen – während Sie und Ihr Team das gegenseitige Vertrauen wiederherstellen, das notwendig ist, um die Zustimmung der Geschäftsleitung zu Ihrem Sicherheitsprogramm zu erhalten.

Sicherheitsverantwortliche wissen bereits, dass Personen mit hohen Befugnissen und hohem Zugang eine einzigartige Sicherheitsbedrohung darstellen. Vielmehr unterstreicht die neueste Studie von Ivanti das Ausmaß des Problems und legt nahe, dass diese Ausnahmen bei der Sicherheit von Führungskräften zu übergroßen organisatorischen Risiken führen.

„Es mag verlockend sein, Führungskräfte aufgrund ihrer geringen Anzahl von strengen Cybersicherheitsmaßnahmen auszunehmen, doch damit unterschätzt man die potenzielle Bedrohung, die sie darstellen.

„Jüngste Forschungsergebnisse zerstreuen jedoch solche Missverständnisse. Führungskräfte zeigen ein ganz bestimmtes Verhalten am Arbeitsplatz und genießen einen einzigartigen Zugang und Einfluss.

„Diese Untersuchung zeigt eindeutig, wie wichtig es ist, ihre Gewohnheiten und Verhaltensweisen anzusprechen und zu korrigieren.“

Giuliano Liguori,
CEO of Kenovy

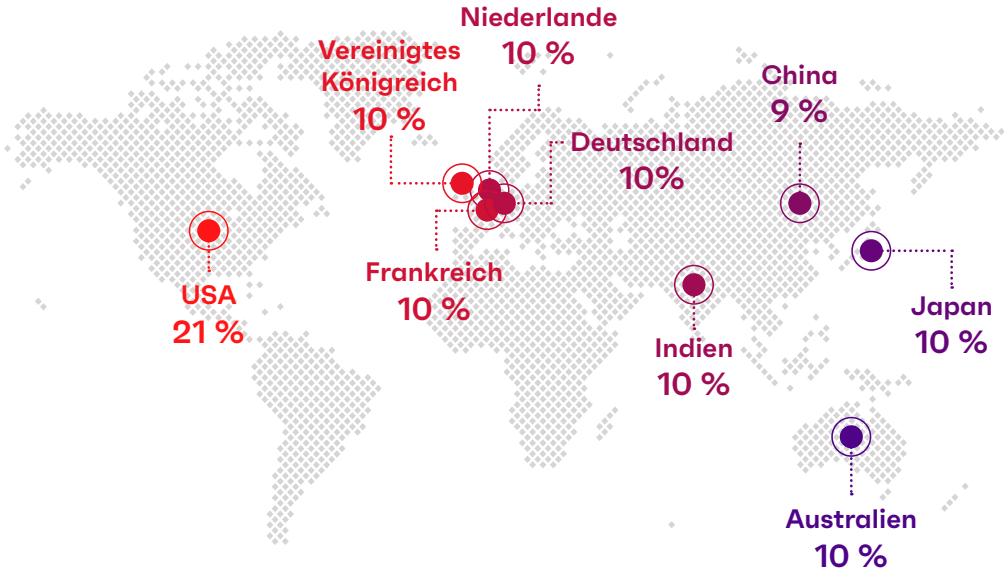
Inhalt:

ivanti

Methodologie

Ivanti befragte im 4. Quartal 2022 über 6.500 Führungskräfte, Cybersicherheitsexperten und Büroangestellte, um die heutigen Bedrohungen zu verstehen und herauszufinden, wie sich Unternehmen auf noch unbekannte zukünftige Bedrohungen vorbereiten.

In diesem Bericht konzentrieren wir uns auf Führungskräfte der C-Ebene – und auf die Einstellungen und Verhaltensweisen, die sie zu einer Gefahr für die Sicherheit machen.



Büroangestellte
5.202

Sicherheitsfachkräfte
902

Führungspersonal
454

01

Die Verhaltenslücke bei Führungskräften:

Der Unterschied zwischen dem, was Führungskräfte über Sicherheit sagen ... und dem, was sie tun

ivanti

Das aktuelle Problem

Es klafft eine große Lücke zwischen dem, was Führungskräfte sagen und dem, was sie tun.

Führungskräfte sagen, sie seien optimistisch, was die Cybersicherheit angeht; fast alle geben an, dass sie das Sicherheitsmandat ihrer Organisation unterstützen. Unsere Untersuchungen zeigen jedoch, dass zwischen dem, was Führungskräfte sagen, und dem, was sie in der Praxis tun, eine große Lücke klafft – wir nennen dies die Verhaltenslücke.

Die Verhaltenslücke: Überzeugungen und Verhaltensweisen von Führungskräften

	Was Führungskräfte SAGEN:	Was Führungskräfte TUN:
Sicherheitskultur	96 % von Führungskräften erklären, dass sie das Cybersicherheits-Engagement ihres Unternehmens zumindest einigermaßen unterstützen oder es fördern.	**49 % von CXOs haben im letzten Jahr beantragt,** eine oder mehrere Sicherheitsmaßnahmen umgehen zu dürfen.
Schulungen	78 % sagen, dass ihre Unternehmen obligatorische Schulungen im Bereich Cybersicherheit anbieten.	**77 % verwenden leicht zu merkende Passwort-Hilfen,** wie z.B. Geburtsdaten oder Spitznamen. Außerdem ist die Wahrscheinlichkeit dreimal höher, dass Führungskräfte ihre Arbeitsgeräte mit unbefugten Nutzern wie Freunden, Familienmitgliedern und externen Freiberuflern teilen.
Phishing	88 % der Führungskräfte geben an, dass sie darauf vorbereitet sind, Gefahren wie Malware und Phishing zu erkennen und zu melden.	Von denjenigen, die auf Phishing hereingefallen sind, geben **35 % zu, auf den Link geklickt zu haben** — oder sogar Geld geschickt zu haben.

Sei es aus Zeitmangel, um die richtigen Prozesse zu durchlaufen, aus einem Gefühl der Sonderstellung („die Regeln können gar nicht für mich gelten“) oder aus anderen Gründen: Führungskräfte neigen einfach dazu, sich anders – sprich: riskanter – zu verhalten als andere Büroangestellte.

24 %

Führungskräfte, die angeben, dass sie das ursprüngliche Passwort für Arbeitsanwendungen, das sie bei der Einweisung erhalten haben, nie geändert haben.

14 %

Reguläre Büroangestellte, die das ursprüngliche Passwort ebenfalls nie geändert haben.

Warum das wichtig ist

Die Verhaltensweisen von Führungskräften sind alles andere als harmlos, sondern stellen eine ernsthafte Bedrohung dar

Die meisten erfahrenen Sicherheitsexperten wissen, dass es riskante Verhaltensweisen von Führungskräften gibt, aber sie schieben das Thema Cyberhygiene für Führungskräfte oft zugunsten anderer strategischer Prioritäten auf.

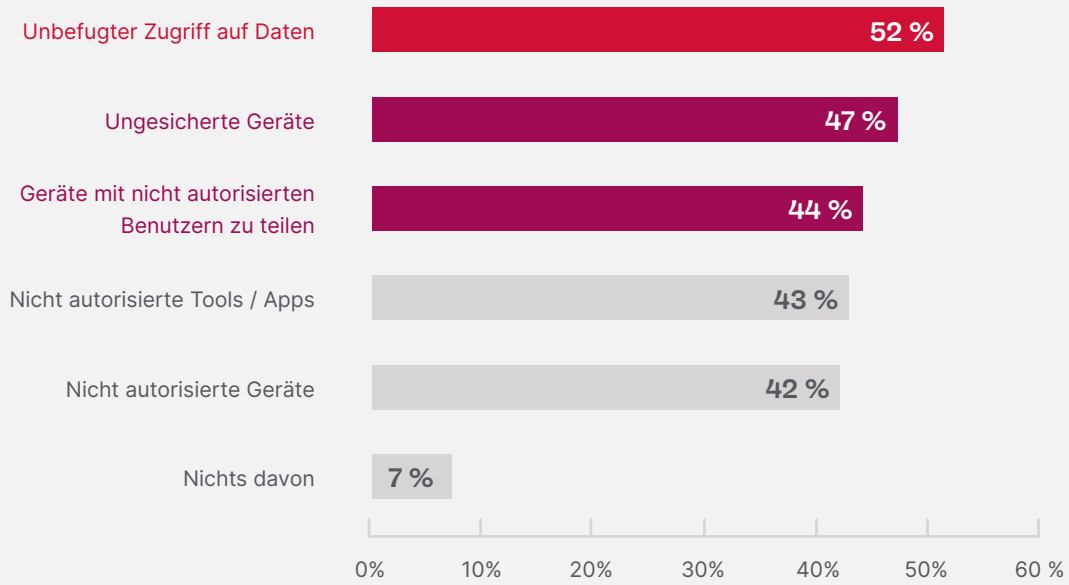
Sicherheitsverantwortliche müssen ihre begrenzte Zeit und Ressourcen so einsetzen, dass das Unternehmen vor den wahrscheinlichsten und gefährlichsten Risiken geschützt ist. Warum also, so die Logik, sollten Sicherheitsteams zusätzliche Zeit aufwenden, um Führungskräfte zu schützen, die sagen, dass sie sich für das Programm entschieden haben – und sogar das Budget für dieses Programm gesichert haben?

Die Untersuchungen von Ivanti bestätigen, dass die Sicherheit von Führungskräften nicht nur ein Problem ist, sondern dass es sich um ein systemisches Problem handelt, das die meisten Unternehmen betrifft.

Tatsächlich entsprechen dieselben Faktoren, die Sicherheitsprofis als hohes Sicherheitsrisiko für ihre Unternehmen angaben, direkt den selbst zugegebenen Gewohnheiten von Führungskräften.

Q: Frage: Was stellt ein hohes Sicherheitsrisiko für Ihr Unternehmen dar?

Anmerkung: Die befragten Sicherheitsfachleute konnten mehrere Optionen auswählen.



Eine von drei Führungskräften

1 von 3 Führungskräften gibt zu, auf nicht autorisierte Unternehmensdateien und -daten zugegriffen zu haben.

Bei Führungskräften ist die Wahrscheinlichkeit,

dass sie ihre Arbeitsgeräte mit Familie und Freunden teilen, dreimal höher als bei anderen Büroangestellten.

Machtdynamik spielt eine Rolle beim Sicherheitsverhalten von Führungskräften

Leider verschärft die ungleiche Machtdynamik zwischen Sicherheitsteams und Top-Managern das Problem.

Wie oft haben Sicherheitsexperten versucht, Best-Practice-Sicherheitsrichtlinien zu implementieren, und wurden dann mit offenen Beschwerden und Schatten-IT-Umgehungen von denselben Anwendern konfrontiert, die sie eigentlich schützen wollten.

Wie kann man von Sicherheitsteams erwarten, dass sie bessere Cyberhygiene und Sicherheitspraktiken von denselben Führungskräften durchsetzen, die ihre Budgets – und ihre Arbeitsplätze – in einem unsicheren Arbeitsmarkt genehmigen?

Aufgrund von begrenzter Bandbreite, Erschöpfung und Burnout geben Sicherheitsexperten oft dem Druck von Führungskräften nach.

ivanti

Warum Sicherheitsteams Schwierigkeiten haben, das Verhalten von Führungskräften zu verändern

Burnout

CISOs sind überlastet und ausgebrannt. 60 % der CISOs geben an, in den letzten zwölf Monaten ein Burnout erlebt zu haben, und 61 % sagen, dass die Erwartungen an CISOs/CSOs zu hoch sind.[1]

Kultur

Wenn der Chef (oder der Chef des Chefs) um einen Gefallen oder eine Umgehung der Vorschriften bittet, ist es den Mitarbeitern der Sicherheitsabteilung verständlicherweise unangenehm, zu widersprechen.

Ohne eine solide Kultur, in der die Sicherheit an erster Stelle steht, beugen sich Mitarbeitende und Sicherheitsexperten oft einfach der Anfrage einer Autoritätsperson.

Nur-dieses-eine-Mal-Kultur

Die Argumentation *„nur dieses eine Mal“* oder „nur weil Sie es sind“ hat einen großen Reiz.

In diesem Moment kann es den Sicherheitsexperten peinlich sein, Regeln beim CEO durchzusetzen – vor allem, wenn früher Ausnahmen gewährt wurden.

„Nur dieses eine Mal“ ist fast nie nur ein einziges Mal, was das Risiko von Umgehungen durch Führungskräfte erhöht und einen Präzedenzfall schafft, der nur schwer wieder rückgängig gemacht werden kann.

02

Übergroße Risiken für Unternehmen durch Führungskräfte:

Die Auswirkungen der schlechten Sicherheitsgewohnheiten von Führungskräften auf ihre Cybersicherheit

ivanti

Das aktuelle Problem

Riskante Verhaltensweisen von Führungskräften haben übergroße Konsequenzen

Obwohl es nur wenige sind, verfügen Führungskräfte über ein außergewöhnliches Maß an automatischem Zugriff sowie über einige sicherheitsrelevante Verhaltensweisen, die ein weitaus größeres Sicherheitsrisiko für ihre Unternehmen darstellen als Büroangestellte.

Ungeschützte Verbindungen ersten Grades zu Führungskräften

45 % der Führungskräfte

lassen Familie und Freunde mindestens einmal im Monat ihre Arbeitsgeräte benutzen.

Fast eine von fünf

Führungskräften hat ihr Arbeitspasswort schon einmal mit jemandem außerhalb des Unternehmens geteilt.

Das ist dreimal so viel wie bei allen anderen Büroangestellten!

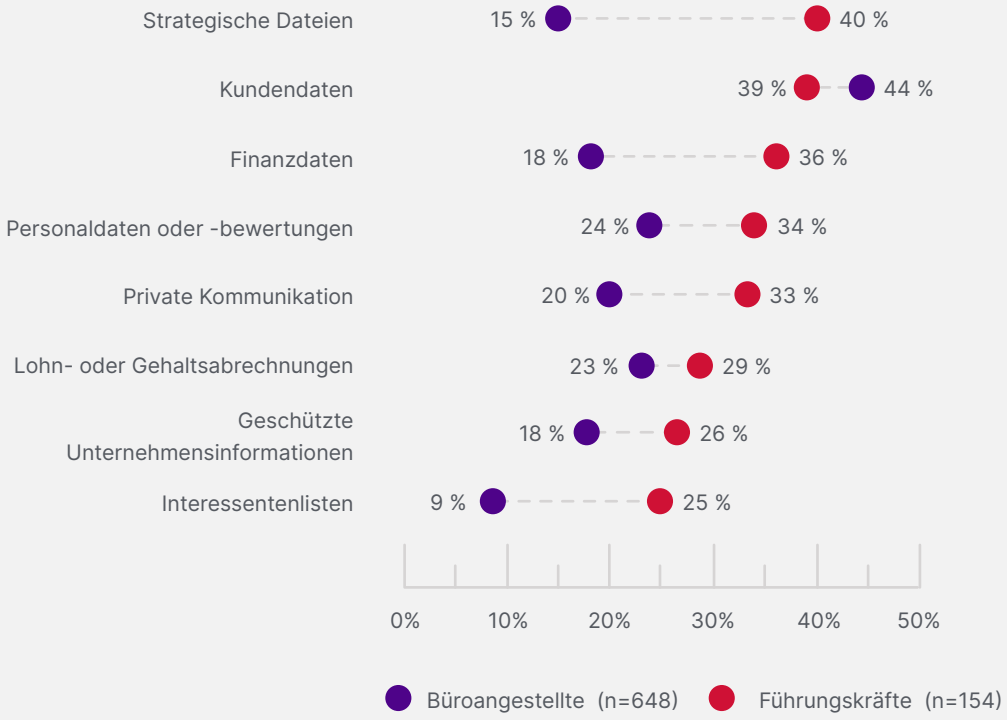
Diese Mitarbeiter ersten Grades sind weder in Sicherheitsfragen geschult noch investieren sie in die Sicherheit Ihres Unternehmens – selbst wenn sie die Geräte Ihres Unternehmens mit umfassendem Datei- und Netzwerkzugriff nutzen.

ivanti

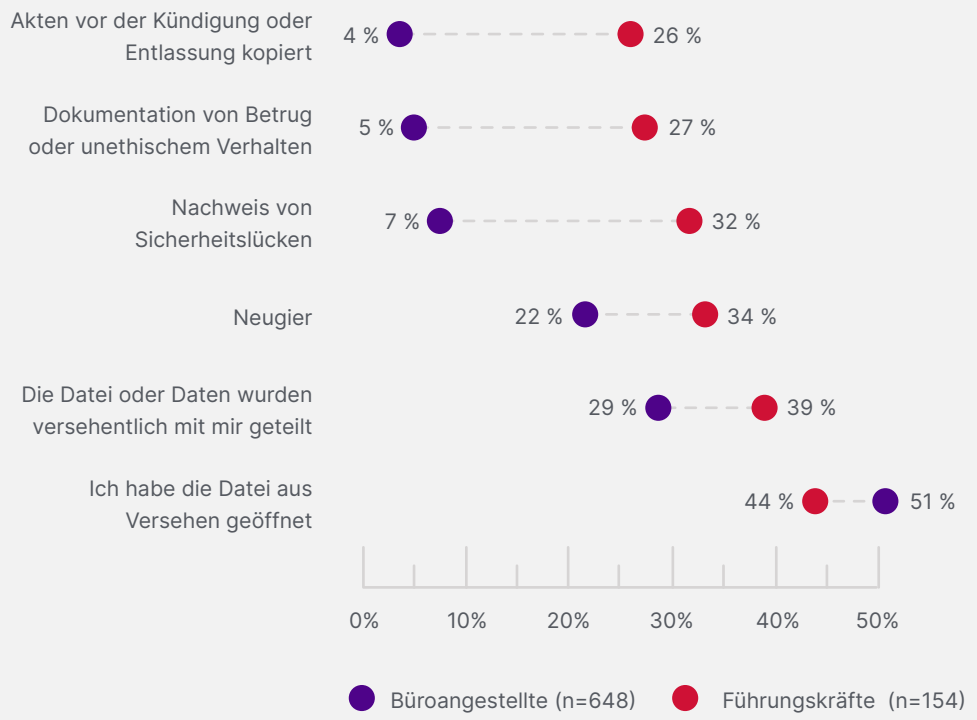
Unbefugter Zugriff durch Führungskräfte

Mehr als 1 von 3 Führungskräften (34 %) gibt zu, dass sie bei der Arbeit auf nicht autorisierte Informationen zugegriffen haben. Und fast 2 von 3 geben an, dass sie diese Dateien/Daten beim Zugriff auf sie hätten bearbeiten können.

Q: Frage: Auf welche Dateien haben Sie zugegriffen?



Q: Frage: Warum haben Sie auf nicht autorisierte Informationen zugegriffen?



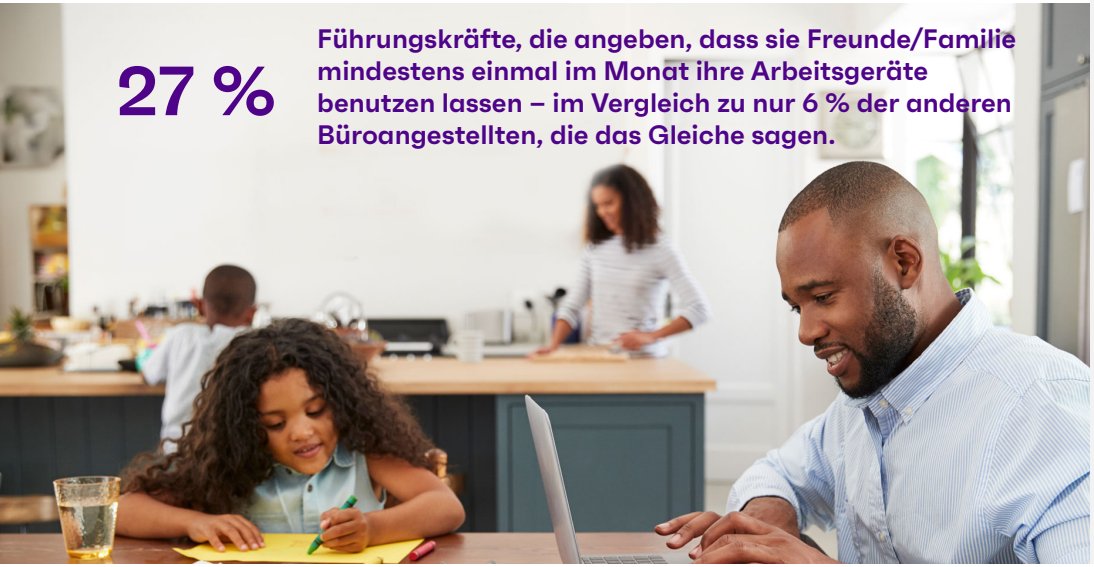
Anmerkung: Für jede Abbildung haben alle Befragten zuvor bestätigt, dass sie auf Dateien zugegriffen haben, die sie nicht für ihre Aufgaben benötigen.

Warum das wichtig ist

Sicherheitsausnahmen für Führungskräfte führen zu erhöhten Risiken

Viele Führungskräfte nehmen Abkürzungen, um Zeit oder Unannehmlichkeiten zu sparen. Die Untersuchungen von Ivanti zeigen jedoch, dass das Risiko systemischer ist als bisher angenommen.

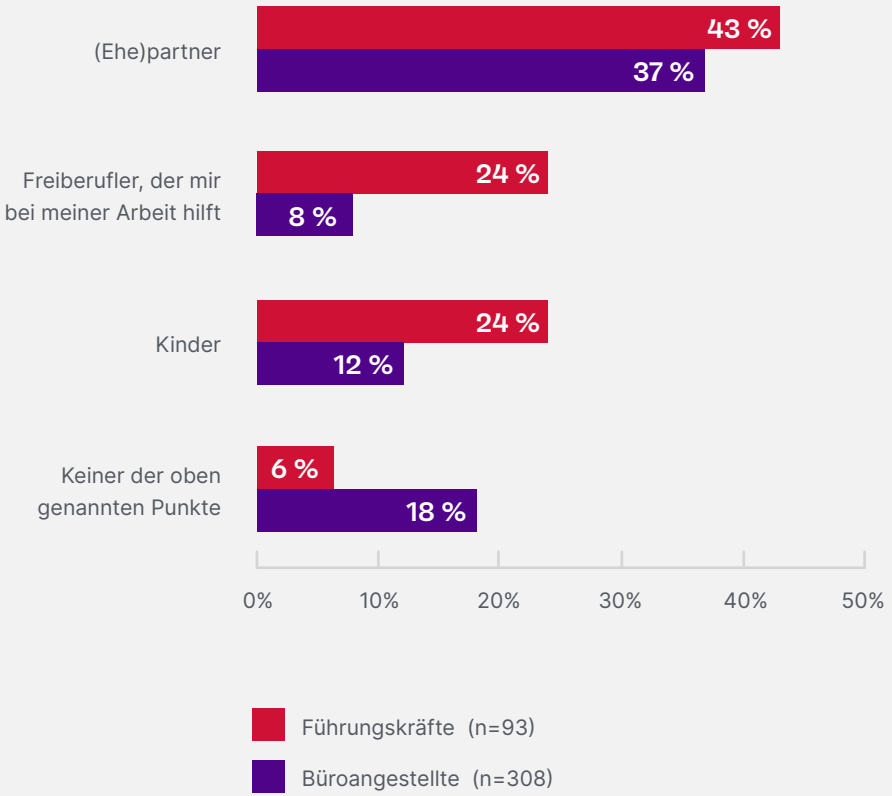
Führungskräfte glauben zu Recht, dass ihre Zeit kostbar und begrenzt ist. Die gemeinsame Nutzung von Passwörtern und Geräten mit Familienangehörigen, Kollegen und dem technischen Support von Drittanbietern kann zum Beispiel als risikoarme Zeitersparnis angesehen werden.



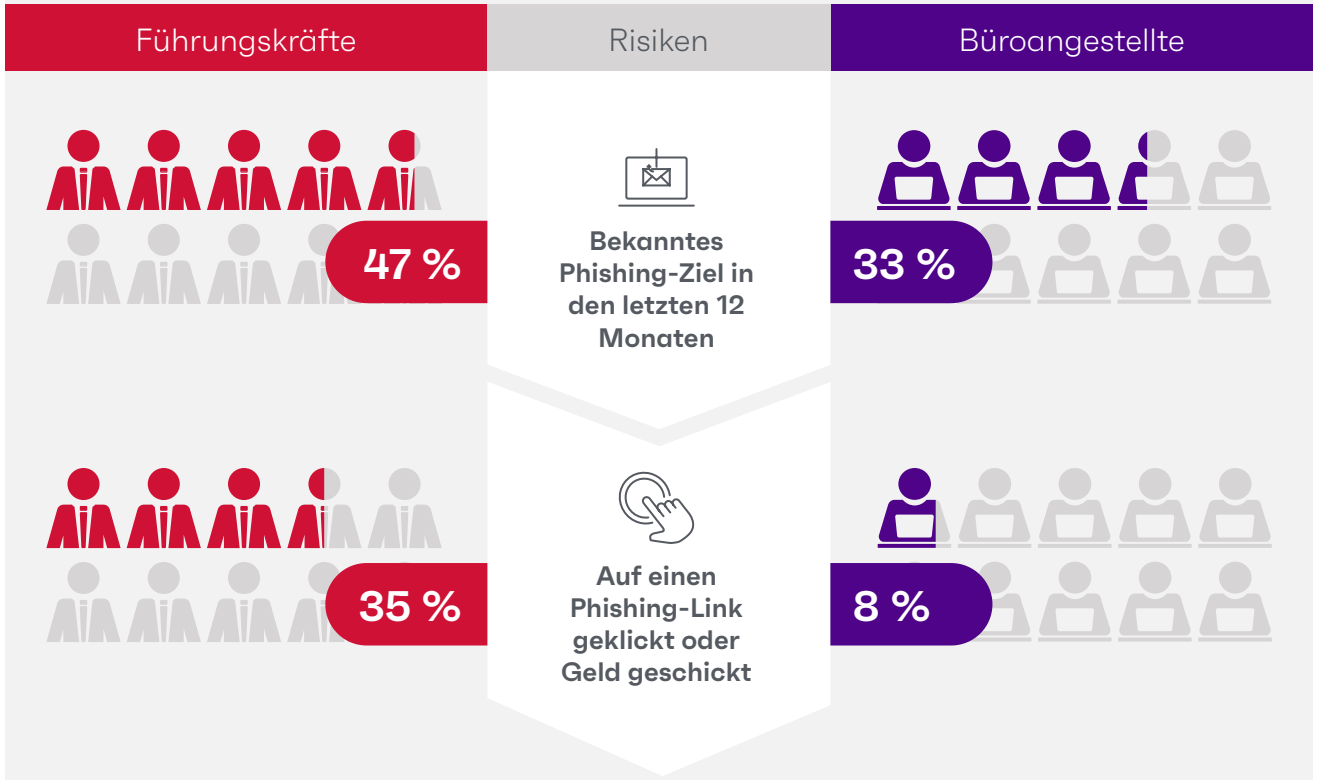
27 %

Führungskräfte, die angeben, dass sie Freunde/Familie mindestens einmal im Monat ihre Arbeitsgeräte benutzen lassen – im Vergleich zu nur 6 % der anderen Büroangestellten, die das Gleiche sagen.

Q: Frage: Mit wem haben Sie Ihr Passwort geteilt?



Führungskräfte haben ein höheres Phishing-Risiko als Büroangestellte



Diese höheren Raten sind möglicherweise auf einen Anstieg der auf Wale zugeschnittenen Spearphishing-Angriffe zurückzuführen. Für Angreifer lohnt sich der zusätzliche Zeitaufwand und die Mühe, Wale aufgrund ihres Zugangs und ihrer Privilegien ins Visier zu nehmen.

Bedrohungsakteure – ob finanziell motivierte Ransomware-Banden oder Advanced Persistent Threats (APTs) – haben es explizit auf hochrangige Führungskräfte abgesehen, da diese über beste Verbindungen zu wertvollen Datenquellen und vernetzten Anlagen verfügen und gleichzeitig weniger auf ihre Cyberhygienegewohnheiten achten.

Denn warum sollte man ein weites Netz für die Genehmigungen eines durchschnittlichen Büroangestellten auswerfen, wenn ein einziger „Wal“ außergewöhnlichen Zugang zu wertvolleren Werten gewährt?

„Es besteht eine 100%-ige Chance, dass Ihr Unternehmen im letzten Jahr Opfer eines Phishing-Angriffs geworden ist. Das ist die Nummer 1, wenn es darum geht, dass Bedrohungsakteure in Ihrem Netzwerk Fuß fassen.

„Wir müssen sicherstellen, dass wir das berücksichtigen und nicht einfach davon ausgehen, dass die Leute es ‚schon wissen‘ oder dass ein Phishing-Angriff sehr offensichtlich sein wird.

Daniel Spicer
Chief Security Officer bei Ivanti

Auswirkungen in der Praxis

Führungswechsel bietet ideale Phishing-Bedingungen

Im Jahr 2015 wurde Mattel Opfer eines öffentlichkeitswirksamen Spearphishing-Vorfalls, bei dem Cyberkriminelle mit Sitz in China 3 Millionen Dollar verloren.

Eine nachfolgende Fallstudie von Infosec2 stellte fest, dass Mattels Entscheidung, einen neuen CEO einzustellen, ein Szenario schuf, das für eine Ausnutzung reif war:

„Sie warteten auf den perfekten Moment, der kam, als Mattel beschloss, einen neuen CEO, Christopher Sinclair, zu ernennen, um Bryan Stockton im Januar 2015 zu ersetzen. Die Ankunft des neuen CEO bedeutete Veränderungen im höheren Management, die zu neuen Machtkämpfen in der Unternehmenshierarchie führen würden.

„Mit anderen Worten: Die Cyberkriminellen haben bei der Planung ihrer Walfang-E-Mails sogar die Büropolitik und die menschlichen Beziehungen bei Mattel berücksichtigt.“

Infosec Fallstudie[2]

ivanti

03

Reibung bei der Sicherheit:

Untersuchung des angespannten Verhältnisses von Führungskräften zu ihrem Sicherheitsteam

ivanti

Das aktuelle Problem

Die Sicherheitserfahrungen von Führungskräften verschlimmern schlechte Cyber-Hygiene

Die Studie von Ivanti zeigt, dass Führungskräfte 2,5 Mal häufiger als der durchschnittliche Angestellte auf die Sicherheitsabteilung zugehen – ein gutes Zeichen – aber sie sind auch deutlich häufiger bereit, ihre Interaktionen als *negativ* zu beschreiben.

Führungskräfte:

Geben zweimal häufiger an,

dass ihre früheren Interaktionen mit Sicherheitspersonal unangenehm waren.

Sind viermal häufiger bereit,

externen, nicht zugelassenen technischen Support in Anspruch zu nehmen.

33 %

Fühlen sich viermal häufiger unsicher, wenn sie Sicherheitsfehler wie das Klicken auf einen Phishing-Link melden. (Das ist mehr als eine von zehn Führungskräften!)

Sagen mit doppelt so hoher Wahrscheinlichkeit,

dass ihnen diese Interaktionen peinlich waren.

Sind fünfmal häufiger bereit,

ein Arbeitspasswort mit jemandem außerhalb des Unternehmens zu teilen.

Wie können Unternehmen die Kommunikationsbarrieren zwischen Führungskräften – denen es vielleicht unangenehm ist, Fehler zu melden – und den Sicherheitsteams, die sie schützen sollen, abbauen?

Es ist eindeutig, dass Datenschutzverletzungen zu den größten Sorgen von Führungskräften gehören. Für einen zuverlässigen Schutz müssen Führungskräfte jetzt die Fähigkeiten von KI bei der Echtzeit-Erkennung von Bedrohungen nutzen, um die Assets des Unternehmens zu stärken.

Ronald van Loon
CEO, Principal Analyst at Intelligent World

Anmerkung: Diese Statistik vergleicht Mitarbeitende der Führungsebene mit allen anderen Büroangestellten.

Warum das wichtig ist

Unternehmen brauchen ein robustes *Cybersecurity-Programm für Führungskräfte*

Die Workarounds der Führungskräfte führen zu schwerwiegenden Sicherheitslücken. Dahinter verbirgt sich jedoch eine Unternehmenskultur, die den Exzeptionalismus der Führungskräfte toleriert und Fehler bei der Berichterstattung weniger wahrscheinlich macht.

Sicherheitsteams müssen sich darauf konzentrieren, das Vertrauen und die Akzeptanz bei den Führungskräften wiederherzustellen, und zwar auf der Basis von Ehrlichkeit und freundschaftlicher Unterstützung – nicht von Verurteilung oder Herablassung.

Top-Führungskräfte

unterstützen eine Sicherheitskultur, indem sie die strategische Rolle der Cybersicherheit innerhalb des Unternehmens verstehen und sich sichtbar für ihre Bemühungen einsetzen.

Sicherheitsteams

Sicherheitsteams unterstützen eine Sicherheitskultur, indem sie einen offenen Kommunikationsstil pflegen, der darauf abzielt, Menschen, die Fehler machen, zu erziehen (anstatt zu bestrafen oder zu beschämen).

Die Minderung von Sicherheitsrisiken für Führungskräfte ist bei Entlassungen noch

Die Untersuchungen von Ivanti zeigen, dass die Deprovisionierung von Anmeldedaten in allen Bereichen ein Problem darstellt. Sicherheitsexperten berichten, dass die Anleitung zur Deprovisionierung in einem Drittel der Fälle ignoriert wird – ein erstaunliches Eingeständnis angesichts der damit verbundenen Risiken.

Und 26 % aller befragten Führungskräfte geben an, dass sie noch brauchbare Passwörter von einem früheren Job haben – etwas, das *wir Zombie-Anmeldedaten* nennen.

Das Risiko, das von Zombie-Anmeldedaten ausgeht, ist in Zeiten von Entlassungen sogar noch höher – wenn Mitarbeiter eher dazu neigen, Daten mitzunehmen oder einen Groll gegen einen ehemaligen Arbeitgeber hegen.

Jeff Pollard, ein Forrester-Analyst, unterstützt diese Schlussfolgerung: „Wir wissen, dass Entlassungen oder Arbeitsplatzverluste Insider-Risiken vorhersagen und damit die Wahrscheinlichkeit von Sicherheitsvorfällen erhöhen. Wir haben im Laufe der Jahre gesehen, dass dies geschehen ist.“[3]

„Früher war es schwer [einen Insider-Job auszuführen], heute ist es einfach. In der Vergangenheit konnten Sie mitnehmen, was Sie in Ihrer Aktentasche tragen konnten. Heute können Sie ganze Terabytes mitnehmen.“

Pete Nicoletti
Field CISO for the Americas bei Check Point Software[3]

26 %

der befragten Führungskräfte geben an, dass sie noch über funktionierende Passwörter aus einem früheren Job verfügen

04

Maßnahmen ergreifen:

Die Verhaltenslücke bei Führungskräften in Ihrem Unternehmen schließen

ivanti

Maßnahmen ergreifen

Beleuchten Sie das Problem kompromisslos

Die Studie von Ivanti bestätigt, was viele von uns schon seit langem wissen: Führungskräfte stellen eine einzigartige und erhebliche Bedrohung für die Sicherheit eines Unternehmens dar. Jetzt, wo wir die Daten haben, ist es an der Zeit, das Problem anzugehen.

1. ### Führen Sie Audits

   durch, um die aktuellen Lücken im Verhalten Ihrer Führungskräfte zu bewerten.

2. ### Beseitigen Sie zuerst die einfachsten und am wenigsten auffälligen Risiken

   und vermeiden Sie direkte Konflikte mit der Unternehmensführung, wenn dies nicht notwendig ist.

3. ### Spielerische Tabletop-Übungen

   können Führungskräfte dazu zwingen, die Zusammenhänge zwischen grundlegender Cyber-Hygiene und den Auswirkungen eines zukünftigen Einbruchs auf ihre Abteilungen selbst zu erkennen.

4. ### Erwägen Sie die Einführung eines „White Glove"-Sicherheitsprogramms für Führungskräfte.

   Auch wenn es im Vergleich zu Ihren Büroangestellten vergleichsweise wenige sind, könnte die persönliche Betreuung dieser Interessengruppe den größten Nutzen für Ihre begrenzten Ressourcen bringen.

„Sie müssen eine Kultur aufbauen – ich sage das, als ob es einfach wäre, aber es ist wahr – in der Sie die Führung herausfordern und einen Prozess aufbauen können, in dem jeder verantwortlich ist.

AJ Nash
Vice President und Distinguished Fellow of Intelligence bei ZeroFox

20 %

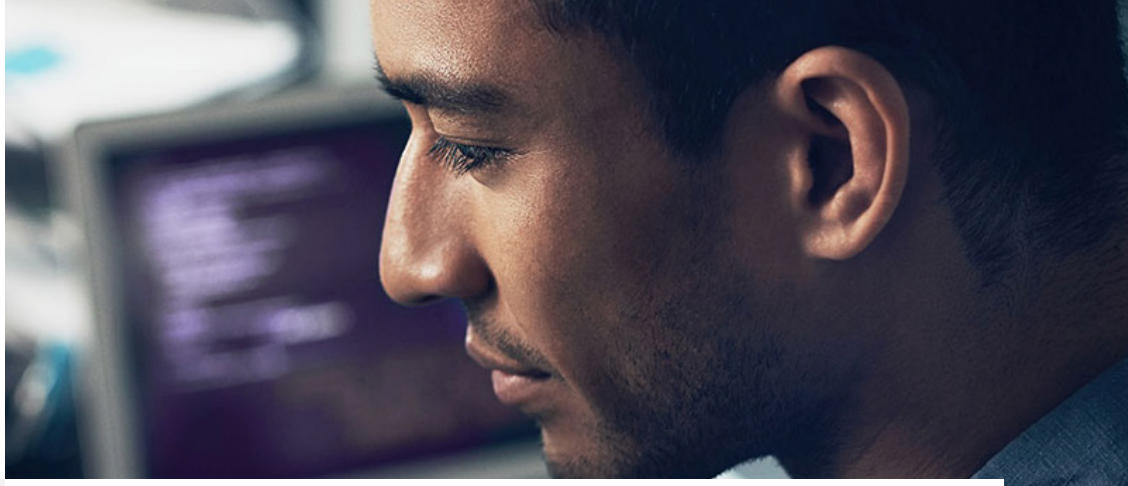
der weltweiten Datenschutzverletzungen können mit Insider-Angriffen in Verbindung gebracht werden.

Wussten Sie das?

Bei Führungskräften ist die Wahrscheinlichkeit, dass sie Dateien kopieren, bevor sie kündigen oder gekündigt werden, 6,5 Mal höher als bei anderen Wissensarbeitern.

1 Ein Audit durchführen

Um sich über das Verhalten von Führungskräften und Mitarbeitern in Ihrem Unternehmen zu informieren, sollten Sie ein Audit in Betracht ziehen. Dabei geht es nicht darum, zu bestrafen oder zu beschämen, sondern sicherzustellen, dass die Sicherheitsrichtlinien für alle Mitarbeiter gelten, unabhängig von ihrer Position.



Internes Audit

Machen Sie eine Bestandsaufnahme der Interaktionen Ihres Sicherheitsteams mit Führungskräften (ab der Ebene des Geschäftsführers) in den letzten 12 Monaten und suchen Sie nach Mustern von Fehlkommunikation und riskantem Verhalten – sowohl bei den Führungskräften als auch bei den Mitgliedern des Sicherheitsteams.

Prüfen Sie zum Beispiel eine Stichprobe von Anrufaufzeichnungen und archivierten Ticketnachrichten. Überprüfen Sie diese und achten Sie auf Hinweise zum Tonfall und zur Wortwahl beider Parteien.

Hat der Austausch Folgendes ausgelöst:

- Scham wegen eines dummen Fehlers?
- Angst vor den Folgen eines Versehens?
- Entfremdung oder Frust einer der beiden Parteien?

Externes Audit

Erwägen Sie auch die Beauftragung eines externen Auditors für eine Risikobewertung der Geschäftsführung.

When a company is considering changing executive privileges or imposing greater controls on top management, it's always a good idea to get an outside perspective.

Ein externer Auditor kann eine unparteiische Risikobewertung der Geschäftsleitung vornehmen und – falls nötig – dem Führungsteam und dem Vorstand schlechte Nachrichten überbringen.

Auswirkungen in der Praxis

Interne Richtlinie rettet Schule vor 100.000-Dollar-Phishing-Betrug[4]

Dr. Jan McGee, die Direktorin einer Charterschule in Florida, stellte einen Scheck in Höhe von 100.000 Dollar aus, nachdem sie monatelang mit einer Person korrespondiert hatte, die sie für den Milliardär Elon Musk oder seinen Vertreter hielt.

Dr. McGee hatte nur die Befugnis, einen Scheck in Höhe von bis zu 50.000 Dollar aus Schulgeldern ohne Genehmigung des Vorstands auszustellen. Glücklicherweise gelang es dem Geschäftsleiter der Schule, Brent Appy, den Scheck zu stornieren, bevor die Betrüger ihn einlösen konnten.

„Ich bin eine sehr smarte Frau. Gebildet. Und trotzdem bin ich auf einen Betrug hereingefallen.

„Grooming ist, wenn man mit jemandem redet und ihm glaubt und er einen dazu bringt, ihm zu vertrauen, dass alles wirklich echt ist, und ich bin darauf hereingefallen.“

Dr. Jan McGee
Ex-Direktorin einer Privatschule in Florida

ivanti

2 Beheben Sie zuerst die einfachsten und am wenigsten auffälligen Risiken für die Geschäftsführung.

Nach Abschluss des Audits und einem besseren Verständnis Ihrer Sicherheitslücken ist es an der Zeit, einen Aktionsplan zu erstellen – und zwar auf eine Weise, die nicht zu aufdringlich ist

Ermitteln Sie auf der Grundlage der Lückenprüfungen Ihrer Führungskräfte die am häufigsten auftretenden Sicherheitsverletzungen oder -risiken in Ihrem Unternehmen und setzen Sie diese als erstes in den Vordergrund.

Einige der einfachsten Dinge könnten sein:

Erstellung und Aktualisierung Ihrer Richtlinien zur Datensensitivität und -klassifizierung: Wer darf worauf zugreifen, unter welchen Umständen und für wie lange – und warum sind bestimmte Berechtigungen nicht erlaubt. Machen Sie transparent und für jeden ersichtlich, was erlaubt ist und was nicht, und *warum*.

Dokumentation und Implementierung von Standardverfahren zur Zugriffsgenehmigung und -erfüllung, um zu gewährleisten, dass die Richtlinien zur Zugriffskontrolle auf alle Mitarbeiter angewendet werden und dass alle Aktivitäten vollständig dokumentiert und überprüfbar sind. (Wenn Ihr Audit den Zugriff oder die Netzwerkaktivität nicht bestätigen konnte, dann ist es an der Zeit, dafür zu sorgen, dass es das kann!)

Aktualisierung der internen Kommunikationsstrategien zur Einführung von Richtlinien zur akzeptablen Nutzung (AUPs) und zur Datensensibilität bei der Einarbeitung jedes Mitarbeitenden sowie regelmäßige Erinnerungen. Sie können sich nicht darauf verlassen, dass ein einziges „offizielles“ Richtliniendokument im Intranet Ihres Unternehmens alle internen Stakeholder aufklärt – vor allem nicht die vielbeschäftigten Führungskräfte!

Betrachten Sie die aktuelle digitale Erfahrung Ihrer Mitarbeitenden (DEX). Bestrafende oder hemmende Sicherheitsmaßnahmen, die den regulären Arbeitsablauf von Führungskräften beeinträchtigen, verstärken das Gefühl des Misstrauens. Entscheiden Sie sich stattdessen für Sicherheitstools, die unauffällig im Hintergrund arbeiten und den Führungskräften Sicherheit bieten, ohne dass sie übermäßig viele Fragen stellen oder sich über häufige Sperrungen beschweren müssen.

3 Machen Sie Tabletop-Übungen für Führungskräfte zum Spiel.

Gamifizierte Sicherheitstrainings, die sich explizit an nicht-technische Führungskräfte richten, können eine größere Akzeptanz bei den Führungskräften erreichen, da diese Trainings den Teilnehmern helfen, die Auswirkungen von Sicherheitsverletzungen auf Abteilungsebene selbst zu erkennen – gemeinsam mit der IT-Sicherheitsabteilung, um sie in die richtige Richtung zu lenken.

Fangen Sie doch einfach klein an mit „Finde den Phish“.

Sie können Ihre nächste Vorstandssitzung mit einer einfachen Runde „Finde den Phish“ beginnen, bei der Sie Ihrem Team Beispiel-Phishing-Nachrichten zeigen und die Gruppe fragen, welche echt und welche gefälscht war.

Sie benötigen zwei Folien und weniger als drei Minuten für dieses einfache und interaktive Spiel, das echte Cyberattacken zeigt.

Gamifizierte Sicherheitstrainings-Tipps für Führungskräfte

Halten Sie es kurz

Versuchen Sie es mit kürzeren und häufigeren von Menschen geleiteten Sitzungen – persönlich oder remote – anstelle von halb- oder ganztägigen Workshops. Nehmen Sie sich zu Beginn der regelmäßigen Führungstreffen fünf Minuten Zeit für ein kurzes Sicherheitsspiel oder eine Session!

Zufall hinzufügen

Verteilen Sie die Bedrohungen und Szenarien nach dem Zufallsprinzip. Das kann so einfach sein wie ein 20-seitiger Würfel, um ein Risiko aus einer nummerierten Liste auszuwählen, oder so komplex wie ein Generator, der die realistischsten Risiken für Ihr spezifisches Unternehmen, Ihre Region oder Branche gewichtet.

Seien Sie kreativ

Ermutigen Sie Ihre Führungskräfte zu kreativen Lösungen, um einen Angriff abzuwehren oder die Risiken der vorgestellten Szenarien auszunutzen. Verzetteln Sie sich nicht, indem Sie erklären, warum eine Idee unrealistisch, unpraktisch oder ungenau ist.

Im selben Team spielen

Nennen Sie niemals aktuelle oder ehemalige Mitarbeitende als Risiko oder Bedrohung, auch nicht in vorgetäuschten Übungen! Sorgen Sie dafür, dass sowohl die Führungskräfte als auch die Mitglieder des Sicherheitsteams an einem Strang ziehen, so dass alle entweder gemeinsam erfolgreich sind oder gemeinsam scheitern.

So tun, als ob

Stellen Sie vorgefertigte Sicherheitstrainingsboxen mit verschiedenen Szenarien, Materialien, Requisiten, Werkzeugen oder sogar Spielzeugbausteinen zusammen, um die Trainingsübungen zu erleichtern und gleichzeitig einzigartige und kreative Möglichkeiten zu bieten, sich zu beteiligen.

Brettspiele umrüsten

Kaufen Sie ein gebrauchtes Brettspiel wie „Spiel des Lebens“ oder das „Leiterspiel" für ein leicht nachrüstbares Sicherheitsspiel in einem Pappkarton.

Preise vergeben

Belohnen Sie die besten und kreativsten Teilnehmer mit kleinen Firmengeschenken!

Komplexe Fachsprache vermeiden

Vermeiden Sie Sicherheitsjargon und Akronyme sowie auch versteckte Bemerkungen über die aktuellen Sicherheitsgewohnheiten von Führungskräften.

Verwenden Sie Fallstudien aus der Praxis, um die Zusammenhänge zu verdeutlichen.

Sicherheitsverantwortliche sollten außerdem anhand von Fallbeispielen aus einer ähnlichen Branche, einer Führungsposition oder einem Risikoprofil aufzeigen, wie sich bösartige Angriffe auf das persönliche Leben und die Karriere auswirken. Denken Sie daran, sowohl gute *als auch* schlechte Reaktionen zu finden!

Beispiel-Fallstudie: Levitas Capital

Der Vorfall:

Im Jahr 2020 klickte ein Gründer von Levitas Capital auf einen gefälschten Zoom-Link, der Malware im Netzwerk des Unternehmens installierte. Die Angreifer stahlen 800.000 Dollar, bevor der Betrug entdeckt wurde.

Was schiefgelaufen ist:

Kurz gesagt? Die normalen Kanäle zur Genehmigung von Finanztransfers brachen zusammen; die Angreifer erlangten die Kontrolle über das E-Mail-System des Unternehmens und gaben sich gegenüber einem Drittverwalter zweimal als Mitbegründer eines Fonds aus.

Was danach geschah:

Der größte Kunde von Levitas verlor das Vertrauen und verließ den Fonds. Zwei Monate nach dem Vorfall wurde der Fonds geschlossen – eine sehr öffentliche Niederlage für die beiden Gründer des Fonds, Michael Brookes und Michael Fagan.

„Es gab so viele Warnsignale, die hätten erkannt werden müssen."

Michael Fagan
Mitgründer von Levitas Capital

4 Erwägen Sie die Einführung eines „White Glove Security Service“ für Führungskräfte.

Aufgrund ihres höheren Bekanntheitsgrades und ihres Zugangs verdienen hochrangige Führungskräfte die individuelle Aufmerksamkeit von Sicherheitsteams: ein „White Glove Secruity Service“, sozusagen.

In Anbetracht der Tatsache, dass Führungskräfte doppelt so häufig angeben, dass ihre Interaktionen mit der Sicherheitsbehörde unangenehm sind – und viermal so häufig externe technische Unterstützung in Anspruch nehmen – besteht das Ziel eines solchen Programms darin, Vertrauen aufzubauen und die Hürden für die Meldung von Sicherheitsfehlern oder -fragen zu senken.

Berücksichtigen Sie bei der Erstellung Ihres „White Glove“-Sicherheitsprogramms:

Zuweisung eines einzigen Kontakts – und zwar *nicht* Ihr oberster Sicherheitsverantwortlicher! – für hochrangige Führungskräfte. Dies hilft, Vertrauen aufzubauen und gleichzeitig die Kommunikation zu konsolidieren und zu standardisieren.

Durchsetzung von Deprovisioning-Richtlinien durch Automatisierung, einschließlich manueller Offboarding-Prüfungen zur Vermeidung von Zombie-Anmeldedaten.

Überarbeitung des Onboarding für Mitarbeitende auf Führungsebene, einschließlich benutzerdefinierter Zugriffsberechtigungen und Einrichtung eines persönlichen Passwortmanagers. Die Führungskräfte selbst haben vielleicht keine Zeit, die Schritt-für-Schritt-Anleitung für die richtige Konfiguration zu befolgen, aber Ihr Unternehmen kann es sich nicht leisten, dass seine Führungskräfte auf diese grundlegenden Leitplanken verzichten.

Entwicklung eines persönlichen Sicherheitstrainings, bei dem es sich nicht um eine allgemeine Präsentation handelt, die Führungskräfte einfach übergehen können. Verwenden Sie frühere Tabletop-Übungen und wählen Sie Fallstudien aus, die sich auf Vorfälle konzentrieren, die der Abteilung oder der Rolle der neuen Führungskraft ähnlich sind.

Unabhängig von den ergriffenen Maßnahmen sollte sich Ihr Team darauf konzentrieren, eine positive – nicht strafende – Sicherheitskultur zu schaffen und durch überzeugende Aufklärungsarbeit und kooperative Einblicke eine höhere Compliance der Führungskräfte zu erreichen.

Wie die in diesem Bericht zitierten Fallstudien beweisen: menschliche Fehler passieren. Sie werden Ihrer Organisation passieren. Sie sind unvermeidlich und lassen sich nie ganz ausschließen.

Aber nur Unternehmen mit einer echten Beteiligung der Geschäftsleitung werden in der Lage sein, die Systeme und das Vertrauen wiederherzustellen und über die Sicherheitsverletzung hinaus zu navigieren.

Greifen Sie auf die Forschungsergebnisse und Berichte von Ivanti zum Thema Cybersicherheit zu!

References

1. Proofpoint. (2022, May). 2022 Voice of the CISO: Global Insights Into CISO Challenges, Expectations and Priorities. From Proofpoint: https://go.proofpoint.com/en-voice-of-the-ciso-2022.html

2. Yip, K. N. (2016, May 21). Whaling Case Study: Mattel's $3 Million Phishing Adventure. From Infosec: https://resources.infosecinstitute.com/topic/whaling-case-study/

3. Pratt, M. K. (2023, February 28). Economic pressures are increasing cybersecurity risks; a recession would amp them up more. From CSO Online: https://www.csoonline.com/article/3689008/economic-pressures-are-increasing-cybersecurity-risks-a-recession-would-amp-them-up-more.html

4. Metz, C. (2023, March 29). Florida principal resigns after sending $100K to scammer posing as Elon Musk. From CBS News Miami: https://www.cbsnews.com/miami/news/florida-principal-resigns-after-sending-100k-to-scammer-posing-as-elon-musk/

5. Garzón, G., & Garzón, F. (2020, June 30). Cybersecurity Incident Response: Tabletop Exercises Using the Lego Serious Play Method. From ISACA: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/cybersecurity-incident-response

6. SecureWorld News Team. (2020, November 23). Hedge Fund Closes Down After Cyber Attack. From SecureWorld: https://www.secureworld.io/industry-news/hedge-fund-closes-after-bec-cyber-attac

Executive Security Spotlight 2023

Neue Untersuchung von Ivanti zeigt reale Risiken für die Chefetage

Teil von Ivantis Report-Serie zum Status der Cybersecurity

ivanti

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