ivanti

Ein Bericht zum Stand der Cybersicherheit der Behörden

4 wichtige Wege, um im Jahr 2023 aktiv zu werden und den Wandel voranzutreiben

Teil von Ivantis Report-Serie zum Status der Cybersecurity

Der richtige Zeitpunkt? Jetzt

Die jüngsten Angriffe auf Krankenhausnetzwerke, globale Logistiksysteme und sogar demokratische Wahlen stellen eine grundlegende Bedrohung für die öffentliche Sicherheit und die Politik dar.

Aber wir befinden uns noch im Anfangsstadium.

Die rasanten Fortschritte bei der generativen KI und den „Deepfakes“ bedeuten, dass die Verbreitung von Ransomware noch glaubwürdiger wird – und damit noch gefährlicher.

ivanti

Die Regierungen auf der ganzen Welt sind aufmerksam geworden. Neue Vorgaben von US-Präsident Biden und Richtlinien der Europäischen Kommission machen deutlich, dass der Schutz kritischer Assets und Infrastrukturen vor Cyberangriffen weltweit dringlicher denn je ist.

Ivanti befragte über 800 Mitarbeitende von Behörden weltweit, um Folgendes zu verstehen:

- Verhalten und Einstellungen der Mitarbeitenden zur Cybersicherheit
- Die Auswirkungen flexibler und hybrider Arbeitsformen auf den öffentlichen Sektor
- Die Meinung von Cybersecurity-Experten zu neuen Bedrohungen und Sicherheitstechnologien

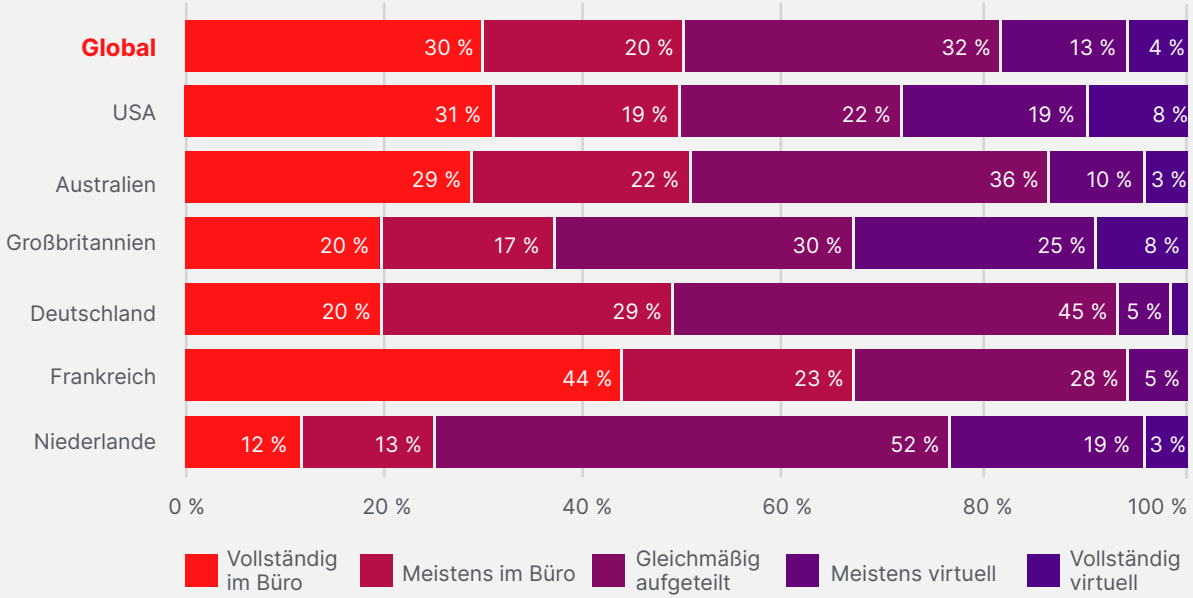
Warum die große Eile?

Es sind nicht nur die neuen Angriffsmethoden und hochkarätigen Regierungsverordnungen. Die Art der Arbeit in den Behörden hat sich in nur wenigen Jahren dramatisch verändert – und das ohne jegliche Vorausplanung, die einer solch drastischen Veränderung normalerweise vorausgeht. Die hybride Arbeitsweise hat eine weitere Sicherheitslücke aufgetan.

Neue Realität

70 % der Mitarbeitenden im öffentlichen Dienst arbeiten zumindest zeitweise virtuell

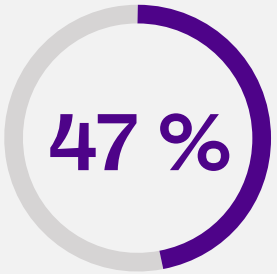
Q: Welche dieser Antworten beschreibt am besten die Art und Weise, wie Menschen mit Schreibtischjobs in Ihrer Organisation arbeiten?



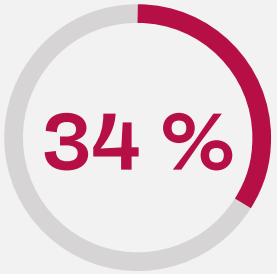
Die Summe der Länderergebnisse ergibt aufgrund von Rundungsfehlern möglicherweise nicht 100 %.

Neue Risiken

Eine Vielzahl von Geräten, Benutzern und Standorten erhöht die Komplexität und schafft neue Schwachstellen



der Sicherheitsexperten weltweit geben an, dass sie keinen umfassenden Einblick in alle Benutzer, Geräte, Anwendungen und Dienste in ihren Netzwerken haben.



der befragten Behördenmitarbeiter verwenden die gleichen oder ähnliche Passwörter für mehrere Geräte.

Inhalt:

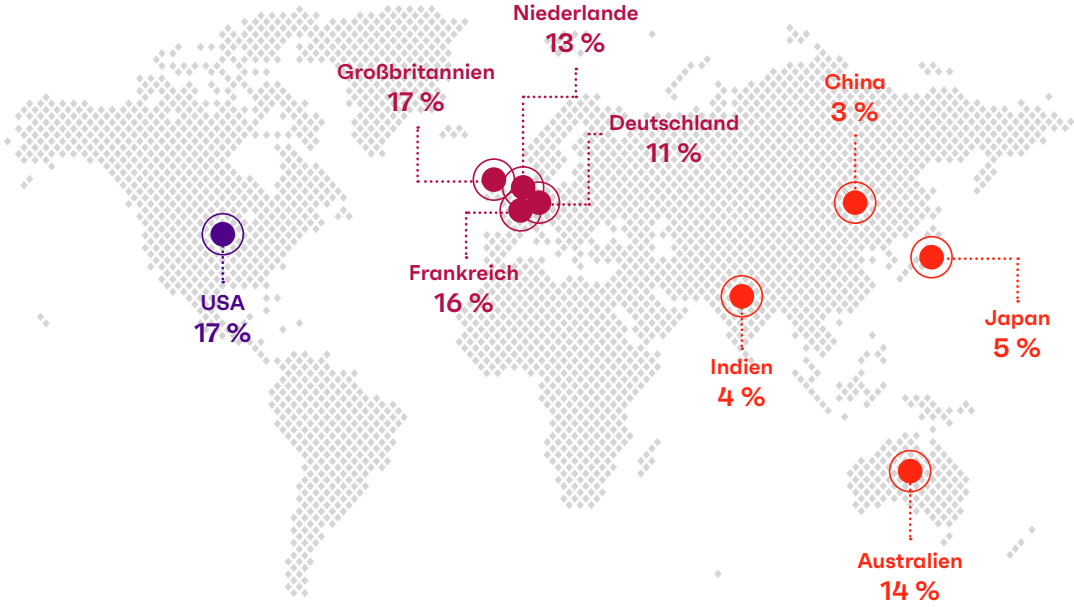
ivanti

Methodologie

Ivanti befragte im 4. Quartal 2022 mehr als 6.500 Führungskräfte, Cybersicherheitsexperten und Büroangestellte, um die heutigen Bedrohungen zu verstehen und herauszufinden, wie sich Unternehmen auf noch unbekannte zukünftige Bedrohungen vorbereiten, wie ursprünglich veröffentlicht in *„Reset drücken: Ein Bericht zum Stand der Cybersicherheit im Jahr 2023“.*

Die hier gesammelten Erkenntnisse basieren auf den Antworten einer Teilmenge dieser Studie: Büroangestellte, die in Behörden rund um den Globus arbeiten (insgesamt 803), sowie Cybersecurity-Experten aus verschiedenen Branchen.

Befragte Mitarbeiter von Behörden (n=803)



01

Keine „Kultur der Verantwortlichkeit“

ivanti

Problem Today

Eine „Nicht mein Job“-Haltung gefährdet die Cybersicherheit der Behörden

Die Unzufriedenheit der Mitarbeitenden ist ein echtes Sicherheitsrisiko für Unternehmen. Laut der Partnership for Public Service liegen die Werte für Engagement und Zufriedenheit im öffentlichen Sektor 15 Punkte hinter denen der Mitarbeitenden in der Privatwirtschaft zurück.[1]

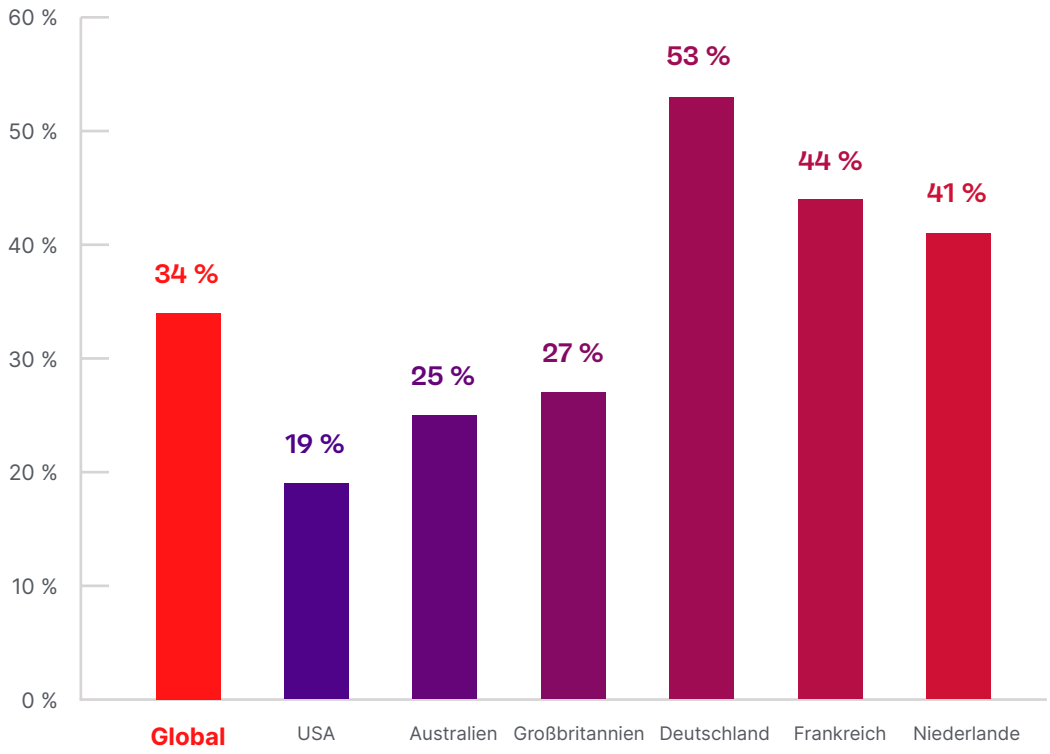
Und ein geringes Engagement bedeutet, dass sich die Mitarbeitenden nicht mit dem Wohlergehen des gesamten Unternehmens verbunden oder dafür verantwortlich fühlen.

Die Forschungsdaten von Ivanti bestätigen dies: Ein großer Teil der Mitarbeiter von Behörden auf der ganzen Welt ist der Meinung, dass ihr Handeln keine Rolle spielt, wenn es um die Sicherheit geht.

IIn Großbritannien sagen 27 % der Mitarbeiter von Behörden, dass ihr Handeln keinen Einfluss auf die Fähigkeit ihrer Organisation hat, sich vor Cyberangriffen zu schützen; in Deutschland sind es sogar 53 %.

Glauben die Mitarbeitenden, dass ihr eigenes Handeln wichtig ist?

Q: Glauben Sie, dass Ihr Handeln die Fähigkeit Ihrer Organisation beeinflusst, sich vor Cyberangriffen zu schützen?



„Meine Handlungen haben keinen Einfluss auf die Fähigkeit meiner Organisation, sich vor Cyberangriffen zu schützen.“

Nicht alle Regierungsmitarbeiter melden verdächtige Aktivitäten

17 % fühlen sich nicht sicher, wenn sie einen Sicherheitsfehler, den sie bei der Arbeit gemacht haben, dem Cybersicherheitsteam melden.

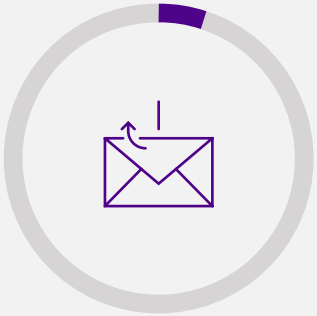
36 % haben eine Phishing-E-Mail, die sie bei der Arbeit erhalten haben, nicht gemeldet.

21 % sagen, dass es ihnen egal ist, ob ihre Organisation gehackt wird.

Behördenmitarbeiter werden gephisht – ein Auftakt zu Cyberangriffen

30 %

sagen, dass sie ein Ziel von Phishing waren



5 %

sind einem Phishing-Versuch zum Opfer gefallen – entweder durch Klicken auf einen Link oder durch Senden von Geld.

Warum das wichtig ist

AEin perfekter Cybersecurity-Sturm kommt auf jede Behördenorganisation zu

Mehrere, effektive Bedrohungsvektoren

Der öffentliche Sektor ist aufgrund der Größe und des Wertes des Ziels besonders anfällig für Angriffe. Im letzten Jahr haben sich Hacker von staatlich gesponserten persistenten Bedrohungen wie APT29 als formidable, sich schnell entwickelnde Gegner erwiesen.[2]

Sich schnell entwickelnde „synthetische“ digitale Inhalte

Generative KI hat Phishing-E-Mails „wie aus dem Bilderbuch“ ermöglicht – personalisiert auf die Sicherheitslücken jedes einzelnen Ziels.[3]

Noch alarmierender ist: Deepfakes stellen eine Bedrohung für die Glaubwürdigkeit des Journalismus und demokratischer Wahlen weltweit dar.[4]

Budgetbeschränkungen und organisatorische Silos schwächen die Sicherheitsbemühungen

Das US Government Accountability Office (GAO) sagt, dass 60 % seiner Empfehlungen zur Cybersicherheit in den letzten zehn Jahren nicht umgesetzt worden sind.[5]

Ein beträchtlicher Anteil an unmotivierten Mitarbeitern

Das durchschnittliche Engagement der US-Bundesangestellten liegt bei 64,5 von 100 Punkten – 14 Punkte unter dem des privaten Sektors.[6]

72 %

der Mitarbeiter der Regierung haben noch nie Kontakt mit dem Sicherheitsteam aufgenommen, um eine Frage zu stellen oder ein Anliegen vorzubringen.

ivanti

Handeln Sie

Machen Sie mit allen Mitarbeitenden Sicherheit zu einer gemeinsamen Verantwortung

Sicherheitsverantwortliche können die Mitarbeitenden nicht dazu zwingen, sich für Cybersicherheit zu interessieren, aber sie können die Einstellung der Mitarbeitenden mit der Zeit beeinflussen, indem sie in eine positive Sicherheitskultur investieren und diese pflegen.

Was macht eine positive Sicherheitskultur aus?

Offen

Die Mitarbeitenden fühlen sich wohl dabei, dem Sicherheitsteam Fragen zu stellen

Integriert

Die Verantwortung für die Sicherheit wird geteilt; jeder Mitarbeitende hat eine Rolle zu spielen

Sicher

Mitarbeiter fühlen sich sicher, wenn sie Vorfälle oder Fehler melden

Iterativ

Die Schulungen sind häufig, iterativ und überzeugend

Strategisch

Sicherheit ist ein Asset – ein Schlüssel zum Erfolg des Unternehmens

Nächste Schritte

Prüfen, beteiligen und optimieren Sie die Erfahrungen Ihrer Mitarbeitenden für eine positive Sicherheitskultur

1

Prüfen

Befragen Sie die Mitarbeitenden, um Ihre Ausgangssituation zu definieren und die aktuellen Verhaltensweisen und Einstellungen zu dokumentieren. Die Ergebnisse werden Ihnen helfen, die spezifischen Schwächen Ihres Unternehmens zu identifizieren und einen praktischen Fahrplan für Veränderungen zu erstellen.

2

Beteiligen

Sprechen Sie mit der Unternehmensleitung, um deren Unterstützung und Zustimmung zu erhalten. Führungskräfte geben nicht nur den Ton an, sondern sie stellen auch eines Ihrer größten Risiken dar.

Lesen Sie mehr über das Risiko von Führungskräften für die Cybersicherheit auf Seite 19 („Whalephishing 101 in Behören“).

3

Optimieren

Ein Kulturwandel ist nie „einmalig“ und „fertig“. Es handelt sich um einen fortlaufenden Prozess, der es erfordert, wichtige Leistungskennzahlen zu überwachen, den Mitarbeitenden zuzuhören und bei Bedarf Kurskorrekturen vorzunehmen.

02

Passwort(nicht)verwaltung: Der „Ground Zero“ der Sicherheit

ivanti

Problem Today

Schlechte Cyber-Hygiene – einschließlich schlechter Passwortgewohnheiten – verfolgt Behörden

Sicherheitsexperten schlagen schon seit mehr als einem Jahrzehnt Alarm, wenn es um Passwortrisiken geht, aber die meisten Organisationen – einschließlich Behörden – gehen immer noch zu lasch mit der Passwortverwaltung um. Die Untersuchungen von Ivanti haben ein breites Spektrum an schlechten Angewohnheiten bei den von uns befragten Behördenvertretern aufgedeckt.

ivanti

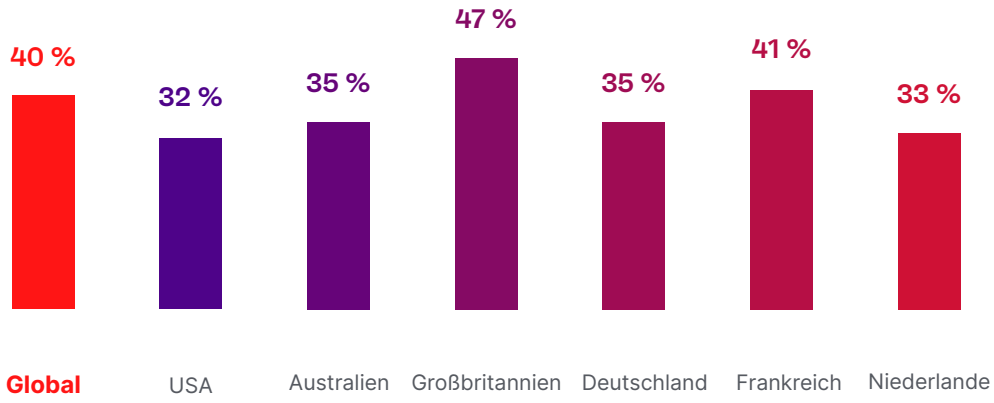
Missbräuche beim Zugang zu Behördenpasswörtern

der Mitarbeitende von Behörden geben zu, dass sie auf sensible Informationen zugegriffen haben, die sie für ihre Arbeit nicht benötigten.

1 von 3

sagen, dass sie glauben, dass ihre Passwörter an ihrem alten Arbeitsplatz noch funktionieren.

Prozentualer Anteil der Mitarbeitenden im öffentlichen Dienst, die länger als ein Jahr dasselbe Arbeitspasswort verwenden



Warum das wichtig ist

Das Spannungsfeld zwischen Sicherheit und Geselligkeit

Die so genannte „Schatten-IT“ und andere Umgehungslösungen sind der Feind sicherer Unternehmen. Wenn Mitarbeitende eine Sicherheitsmaßnahme als ineffizient oder lästig empfinden, werden sie einen Weg finden, sie zu umgehen, der definitiv nicht sicher ist.

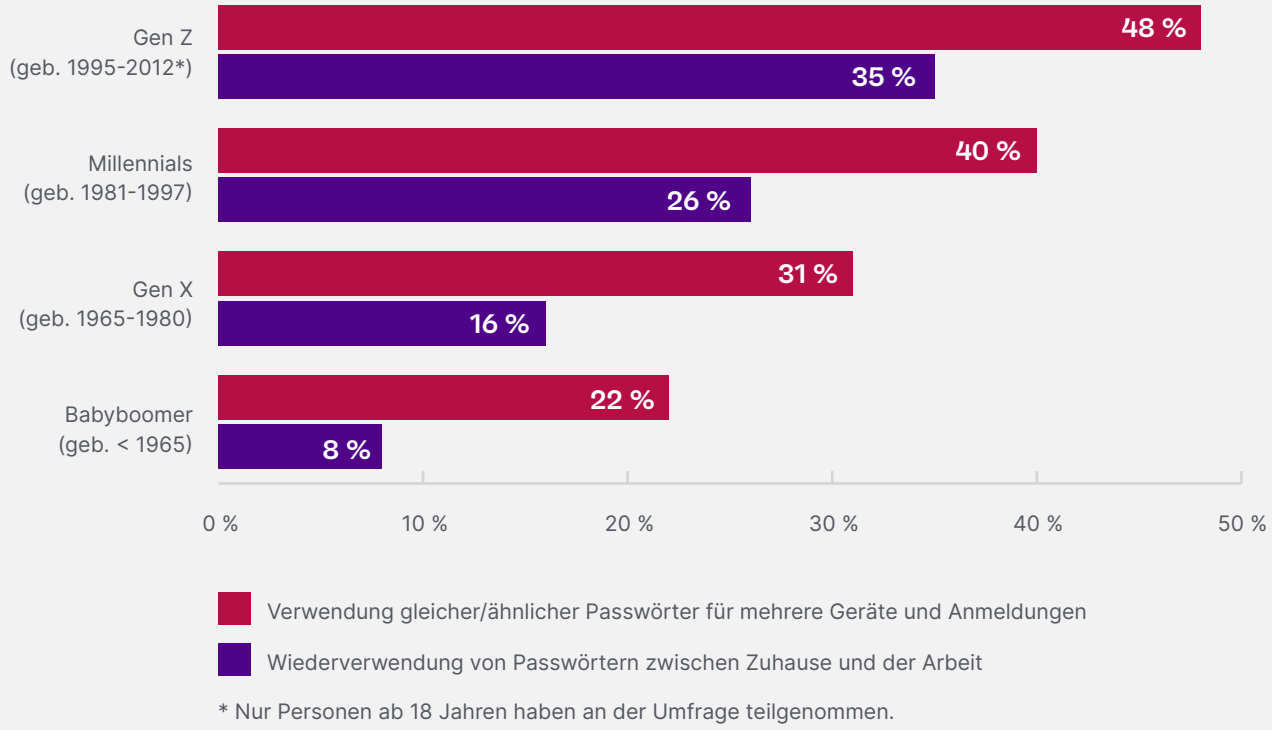
Passwörter sind der Ausgangspunkt für Sicherheitsumgehungen der Mitarbeitenden. Mitarbeitende in allen Branchen verwenden weiterhin Haftnotizen, Kosenamen, Geburtstage und den allgemein beliebten unknackbaren Code: „12345“.

Behörden brauchen Sicherheitslösungen, die so bequem – so mühelos – sind, dass die Mitarbeitenden nicht nach Wegen suchen, um die sogenannte Lösung zu umgehen.

Der Mythos der „Digital Natives“

Glauben Sie, dass Ihre jüngeren Mitarbeitenden mehr über Passwortsicherheit wissen? Die Daten bestätigen das nicht.

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



* Nur Personen ab 18 Jahren haben an der Umfrage teilgenommen.

Maßnahmen ergreifen

Investieren Sie für mehr Sicherheit in die digitale Personalerfahrung (Digital Employee Experience – DEX)

Sicherheitsteams sollten neue Richtlinien oder Technologien durch die Brille der digitalen Personalerfahrung (DEX) bewerten und sich fragen: „Wird die Erfahrung für die Nutzer aus Bequemlichkeitsgründen zu Workarounds oder anderem unangemessenen Verhalten führen – und wenn ja, ist es dieses Risiko wert?“

Nächste Schritte

Implementierung benutzerfreundlicher Erfahrungen bei gleichzeitiger Gewährleistung der Sicherheit

1 Konzentrieren Sie sich auf hochgradig gefährliche Workarounds

- Mitarbeitende umgehen die Sicherheit zugunsten der Bequemlichkeit
- Hochrangige Führungskräfte fordern Ausnahmen von den Sicherheitsvorschriften

2 Priorisieren Sie DEX-fokussierte Technologie

- Schaffen Sie nutzerzentrierte Erfahrungen (weniger Reibungspunkte = höhere Konformität)
- Beseitigen Sie wenn möglich menschliche Eingriffe
- Machen Sie Ausnahmeregelungen unmöglich

Auswirkungen in der Praxis

Zero Trust Architektur (ZTA) Implementierungen und DEX-Überlegungen

Unabhängig davon, ob Sie eine Zwei-Faktor-Authentifizierung, Token oder biometrische Daten verwenden, sollten Organisationen und Behörden einem Modell mit möglichst wenig Privilegien für alle Mitarbeitenden den Vorzug geben und sich zu einer Zero Trust-Architektur (ZTA) verpflichten.

Im Rahmen von ZTA arbeiten Sicherheits- und IT-Lösungen zusammen, um die Sicherheitslage und die Einhaltung von Vorschriften kontinuierlich zu überprüfen, indem sie jedem Mitarbeitenden nur so viel Zugang wie nötig gewähren.

Neben anderen Sicherheitsvorteilen gewährleistet dieser eingeschränkte Zugang die Sicherheit einer Agentur und ermöglicht gleichzeitig eine flexible

Denn wenn ein Mitarbeiter auf einen Phishing-Angriff hereinfällt, kann der Angreifer nur auf die begrenzten Optionen zugreifen, die dem Mitarbeiter zur Verfügung stehen.

ZTA kann sich jedoch als zu schwerfällig für den täglichen Betrieb (für die Mitarbeitenden) und die Wartung (für das IT-Personal) erweisen, was die Verwendung von Schatten-IT fördert und jeden Vorteil von ZTA zunichte macht.

Daher sollten Behörden, die eine ZTA in Erwägung ziehen, folgende Hebel ansetzen:

- Strategische Automatisierung für Benachrichtigungen über unbekannte Geräte, Warnungen über verdächtiges Verhalten und Zeitüberschreitungen beim Zugriff auf Benutzerprivilegien.
- IT-Playbooks und Entscheidungsbäume für Genehmigungsanträge und allgemeine Abfragen.
- Intuitive, leicht zugängliche Anweisungen für Endbenutzer zur „Selbsthilfe“, bevor sie ein IT-Ticket einreichen.

Zusätzliche Ressourcen für ZTA und DEX

- Sonderveröffentlichung 800-207 („Zero Trust Architektur“)
- Das NIST Cybersecurity Framework (CSF): Abbildung der Ivanti-Lösungen auf die CSF-Kontrollen
- Bericht über die digitale Mitarbeitererfahrung 2022
- Erste Schritte mit DEX: Kernbereiche für ein großartiges digitales Mitarbeitererlebnis
- Mitarbeitererfahrung im Zeitalter des Everywhere Workplace: Warum die IT eine Vorreiterrolle spielen muss

03

Schulung für alle: Die menschlichen Lücken in der Cybersicherheit der Behörden

ivanti

Problem Today

Uneinheitliche Cybersicherheitsschulungen belasten die Abwehr der Behörden

Sicherheits- und Automatisierungstechnologien bieten leistungsstarken Schutz an vorderster Front – aber die Schulung der Mitarbeitenden, die die Augen und Ohren Ihres Unternehmens für die Sicherheit sein sollen, ist eine wichtige sekundäre Verteidigung. Die Untersuchungen von Ivanti zeigen, dass die Fortbildung im öffentlichen Sektor einfach nicht alle erreicht.

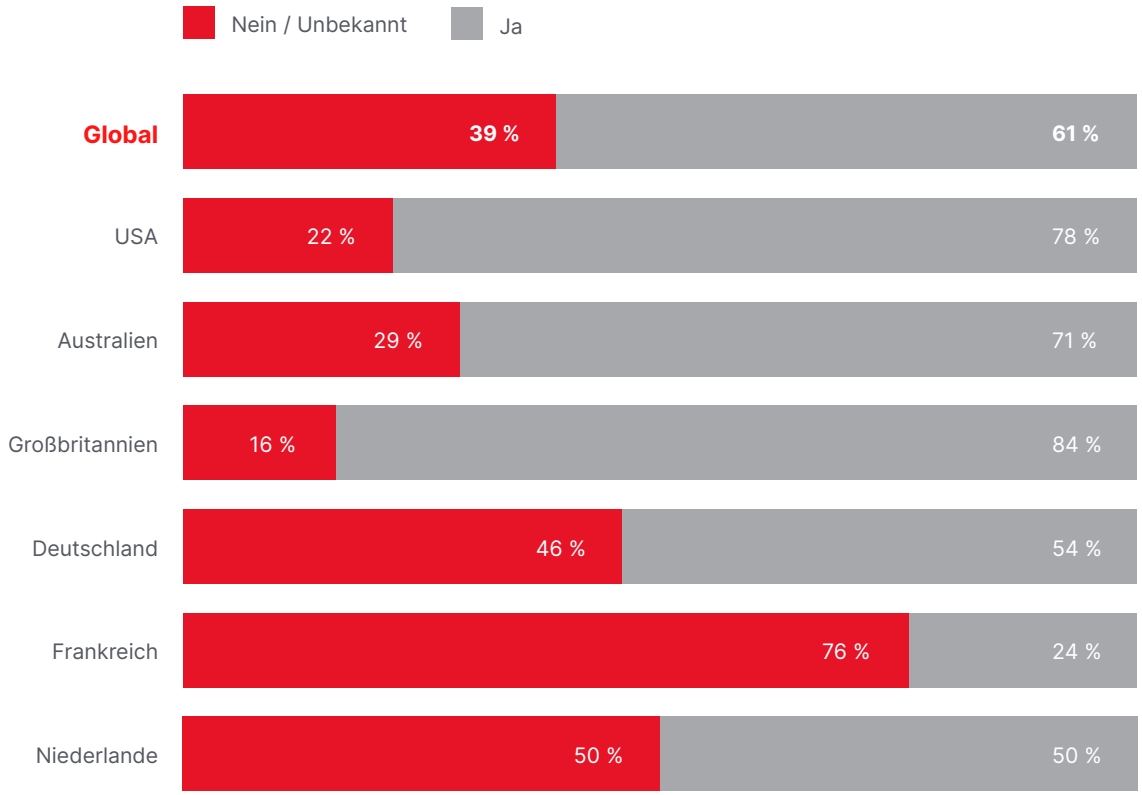
27 %

Nur 27 % der Regierungsmitarbeiter fühlen sich „sehr gut vorbereitet“, um Bedrohungen wie Malware und Phishing bei der Arbeit zu erkennen und zu melden.

ivanti

Schulungen für alle? Nicht einmal annähernd.

Q: „Bietet Ihr Unternehmen obligatorische Schulungen zur Cybersicherheit an?“



Warum das wichtig ist

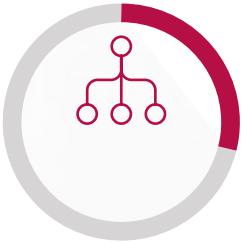
Behördenmitarbeiter und Auftragnehmer berichten über wenig oder ineffektive Schulungen, obwohl sie dazu verpflichtet sind

Die globale Studie *„Reset drücken“* von 2023 unter Sicherheitsexperten weltweit ergab, dass ein erheblicher Anteil der Unternehmen bei der Aufklärung und Schulung der Mitarbeitenden über Cybersecurity-Risiken und Meldeverfahren weit hinterherhinkt.

Und es bedarf nur eines einzigen Menschen, der einen einzigen Fehltritt begeht, um unbeabsichtigten, aber katastrophalen Schaden anzurichten – und innerhalb der Behörden wirkt sich dieser Schaden auf jeden unterstützten Bürger aus.

32 %

der Sicherheitsexperten geben an, dass eine ineffektive oder unvollständige Schulung der Mitarbeitenden ein wesentliches Hindernis für herausragende Leistungen im Bereich der Cybersicherheit in ihrer Organisation darstellt.



29 %

der Unternehmen weltweit verlangen von ihren Partnern und/oder Lieferanten keine Cybersecurity-Schulungen – eine exponierte Position für Behörden, die mit Drittanbietern zusammenarbeiten.

Einblicke aus
Reset drücken: Ein Bericht zum Stand der Cybersicherheit im Jahr

Auswirkungen in der Praxis

„Whalephishing 101“ für Behörden

Beim Whalephishing werden manipulative Mitteilungen an hochrangige, risikoreiche Ziele oder „Wale“ gesendet. Zu den üblichen Whalephishing-Zielen gehören Abteilungsleiter, Persönlichkeiten des öffentlichen Lebens und Finanzchefs– oder sogar deren Assistenten oder Verwaltungspersonal innerhalb einer gewünschten Abteilung.

Indem sie dem Ziel vorgaukeln, dass die Kommunikation echt ist, können Angreifer Anmeldedaten, sensible Informationen oder sogar betrügerische Überweisungsgenehmigungen erlangen.

Ein solcher Zugriff bleibt oft über längere Zeit unentdeckt und ungemeldet, so dass fortgeschrittene, hartnäckige Bedrohungen (Advanced Persistent Threats, APTs) monatelang… oder sogar jahrelang in Behördennetzwerken lauern können.[7]

Und Untersuchungen zeigen, dass gerade die Personen, die den meisten Zugang zu sensiblen Informationen und Netzwerken haben, häufig die schlechtesten Sicherheitsgewohnheiten aufweisen.

Mitarbeitende in Führungspositionen zeigen häufiger unsicheres Sicherheitsverhalten als andere Arbeitnehmer

Mehr als 1 von 3 Führungskräften hat auf einen Phishing-Link geklickt … viermal so häufig wie der durchschnittliche Mitarbeitende!

Fast 1 von 4 Führungskräften use verwendet leicht zu merkende Geburtstage als Teil ihrer Passwörter.

Bei Führungskräften ist die Wahrscheinlichkeit, dass sie Passwörter jahrelang aufbewahren, viel größer als bei anderen Arbeitnehmern –1 von 4 befragten Führungskräften tut dies.

Bei Führungskräften ist die Wahrscheinlichkeit, dass sie ihre Passwörter mit Personen außerhalb des Unternehmens teilen, fünfmal höher.

*Diese Statistiken gelten für Führungskräfte aller Branchen, einschließlich des öffentlichen Sektors, und stammen aus *Reset drücken: Ein Bericht zum Stand der Cybersicherheit im Jahr 2023*

Handeln Sie

Schulungen für alle Mitarbeitenden von Behörden senken das Sicherheitsrisiko und verbessern die Einstellung

Einer der besten Wege, um an sensible Informationen zu gelangen, auf die „Wale“ (oder andere privilegierte Benutzer) Zugriff haben, können die Mitarbeitenden sein, die mit ihnen zusammenarbeiten:

- Ein einflussreiche Verwaltungsassistentin.
- Ein neuer Mitarbeiter am Empfang.
- Fachkundige Fremdfirmen, die einen Tag lang zu Besuch sind.

Selbst wenn diese Mitarbeiter offiziell keinen direkten Zugang zu privaten Informationen oder Datenträgern haben, bieten schlechte Sicherheitsgewohnheiten, die aus Bequemlichkeit entstanden sind – und die Nähe zu hochrangigen Zielen – einen leichten Zugang zu den sensibelsten Informationen und Unterlagen einer Behörde.

Das beste Sicherheitstraining bietet sowohl ...

Was

Spezifische Arten von Angriffen und wie man sie erkennt und abwehrt.

Warum

Die entscheidende Rolle, die jeder Mitarbeiter spielt, unabhängig von seinem Titel, seiner Rolle oder seinem Standort.

Nächste Schritte

„Schulungen für alle“ ohne in Einheitsgrößen zu denken

1

Botschafter ausbilden

Schulen Sie gut ausgebildete „Sicherheitsbotschafter“ – Menschen, die nicht im Sicherheitsbereich arbeiten, aber ein Interesse daran haben.

2

Achten Sie besonders auf Mitarbeiter mit hohem Risiko

Identifizieren Sie Ihre Hochrisikosegmente und entwickeln Sie für jedes einzelne einen maßgeschneiderten Lehrplan, der sich auf realistische Szenarien für eine bestimmte Behörde auf der Grundlage der jüngsten Bedrohungen konzentriert.

3

Gestalten Sie es positiv

Machen Sie Schulungsveranstaltungen unvergesslich. Schulungen im Stil von Vorlesungen haben ihre Berechtigung, aber ziehen Sie auch wettbewerbsorientierte Aktivitäten oder eine Szenarienplanung mit „Gamification” in Betracht.

04

Zukunftssichere Behördenorganisationen

ivanti

Problem heute

Alte Systeme, komplexe Technologien, Datensilos, Talentmangel … sollen wir weitermachen?

Viele gehen davon aus, dass Behörden – Stadtverwaltungen, Bundesbehörden, militärische oder öffentliche Einrichtungen – die Cybersicherheit im Griff haben müssen.

(Schließlich befinden sich einige der fortschrittlichsten Talente und Technologien im Bereich der Cybersicherheit in militärischen Abteilungen und Anwendungen!)

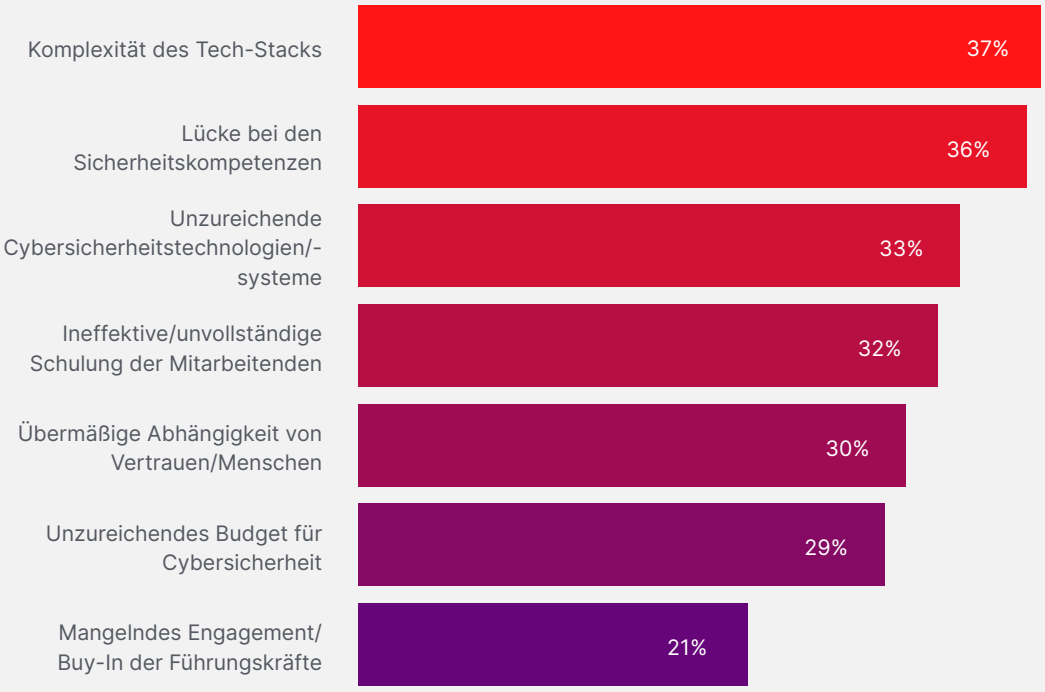
In Wirklichkeit fehlt es den meisten staatlichen Organisationen an nachhaltigen Mitteln für:

- Mitarbeitende
- Neue Technologie
- Schulungen
- Arbeitskultur

ivanti

Die am häufigsten genannten Hindernisse für herausragende globale Cybersicherheit

Q: Welches sind die größten Hindernisse für eine hervorragende Cybersicherheit in Ihrem Unternehmen?



Einsichten aus
Reset drücken: Ein Bericht zum Stand der Cybersicherheit im Jahr 2023

Warum das wichtig ist

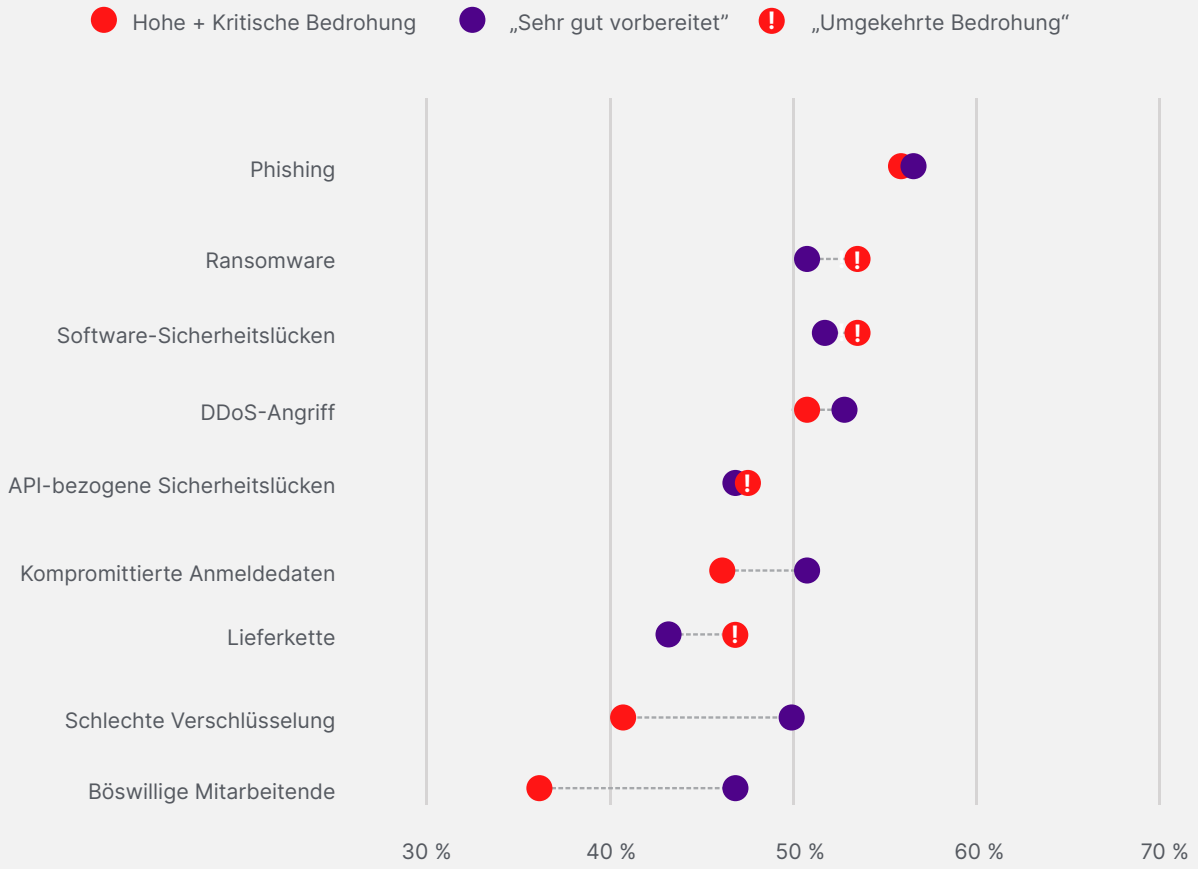
Angreifer entwickeln ihre Waffen gegen alte Verteidigungssyste me weiter

Einem Bericht des US Government Accountability Office (GAO) zufolge hat die US-Bundesregierung seit 2010 immer noch mehr als die Hälfte der Empfehlungen des GAO nicht umgesetzt.[8]

Q: Bitte bewerten Sie das für 2023 prognostizierte Bedrohungsniveau in Ihrer Branche für jeden der folgenden Bereiche ...

Q: Wie gut ist Ihre Organisation auf jede der hier aufgeführten Arten von Bedrohungen vorbereitet?

Sicherheitsbedrohungen versus Sicherheitsvorkehrungen



Einsichten aus *Reset drücken: Ein Bericht zum Stand der Cybersicherheit im Jahr 2023*

Auswirkungen in der Praxis

Der öffentliche Sektor bleibt für staatlich gesponserte Hacker anfällig

Der öffentliche Sektor ist besonders anfällig für Angriffe von staatlich geförderten Cyberkriminellen, die gegen jede mit ihm verbundene Behörde (und sei sie noch so weit entfernt) vorgehen.

Weitere Informationen über andere aktive Angreifer, die über die drei rechts aufgeführten hinausgehen, sowie über deren Methoden, ausgenutzte Sicherheitslücken und öffentlich bekannte staatliche Angriffe finden Sie im vollständigen *2023 Cyberstrategy Tool Kit.*

„Unsere Energie-, Gesundheits- und Finanzsysteme [...] sind alle mit Cyberrisiken durch böswillige Akteure konfrontiert. Angriffe wie diese könnten den Menschen, unserer Umwelt, der nationalen Sicherheit und vor allem unserer Wirtschaft schweren Schaden zufügen.“ [8]

Marisol Cruz Cain
Director, GAO Information Technology and Cybersecurity Team

Zu den ausgewählten Advanced Persistent Threats (APTs) **und Cyber-Banden**, die globale Regierungen angreifen, gehören:

ALPHV

Eine cyberkriminelle Bande, die ein „Ransomware-as-a-Service“-Modell (RaaS) entwickelt, verkauft und einsetzt. Hackerlösungen von der Stange wie diese ermöglichen einer Vielzahl von Angreifern den Zugriff.

APT29

Staatlich geförderte Hacker, die mit dem russischen Auslandsgeheimdienst in Verbindung stehen und Spionage- und Geheimdienstaktivitäten betreiben.

Conti

Ein mit Russland assoziierter Angreifer, der sich auflöste, nachdem sein Playbook durchgesickert war ... aber mit Conti assoziierte Hacker und ihre Code stellen immer noch eine Bedrohung dar. Ransomware-Taktiken im Stil von Conti waren auch im letzten Jahr bei mehreren Cyberkriminellen zu beobachten.

Handeln Sie

Bekämpfung von Fehlinformationen und beschleunigten Angriffen durch strategische Technologie und Kultur

Wir leben in einer Welt, in der Fehlinformationen Macht bedeuten:

- Bot-gestützte Fehlinformationskampagnen in sozialen Medien in großem Maßstab
- Hochgradig glaubwürdige Phishing-Angriffe, die auf individuelle Präferenzen abgestimmt sind
- Deepfakes, die den unabhängigen Journalismus untergraben und Wahlen stören
- Ransomware, die die globale Logistik und Gesundheitsversorgung unterbricht

All dies kann die öffentliche Sicherheit, den globalen Handel und die Diplomatie beeinträchtigen – und sogar Menschenleben kosten. Regierungsorganisationen sind besonders gefährdet, da sie die Schlüssel zu Systemen und Nachrichten besitzen, die von bösartigen Akteuren gestört und ausgenutzt werden sollen.

Sicherheitsverantwortliche müssen ihre Position schützen, indem sie präzise vorgehen: Sie müssen Strategien, Systeme, Tools, Schulungen und Unternehmensführung entwickeln, die zusammenarbeiten, um bösartige Akteure fernzuhalten.

Und es ist von entscheidender Bedeutung, diese Verteidigungsmaßnahmen in vergleichsweise „friedlichen“ Zeiten aufzubauen – zu viele Unternehmen unternehmen kritische Schritte erst nach einem katastrophalen Angriff.

Die Zeit zum Handeln ist jetzt gekommen.

Nächste Schritte

Machen Sie Ihre Tech-Stacks zukunftssicher

1

Resilienz

Entwerfen Sie Reaktions- und Wiederherstellungspläne, um Ausfälle zu verkürzen und Folgewirkungen zu begrenzen.

2

Automatisierung

Setzen Sie die Automatisierung ein, um die Sichtbarkeit von Assets zu erhöhen, und setzen Sie eine risikobasierte Priorisierung für Patches ein – beides Grundvoraussetzungen für sichere Unternehmen im Jahr 2023.

3

Ermächtigung

Geben Sie dem Cybersicherheitsteam mehr Unabhängigkeit und Budget, um die Sicherheitsagenda festzulegen – keine gedankenlosen Reaktionen mehr auf die neuesten Bedrohungen, die gerade in den Schlagzeilen sind.

4

Ganzheitliches Risikomanagement

Denken Sie an die Sicherheit jenseits der Mauern der Regierung - von Mitarbeitenden, die von überall aus arbeiten (Work From Everywhere – WFE), über hybride Mitarbeitende bis hin zu externen Auftragnehmern und Anbietern.

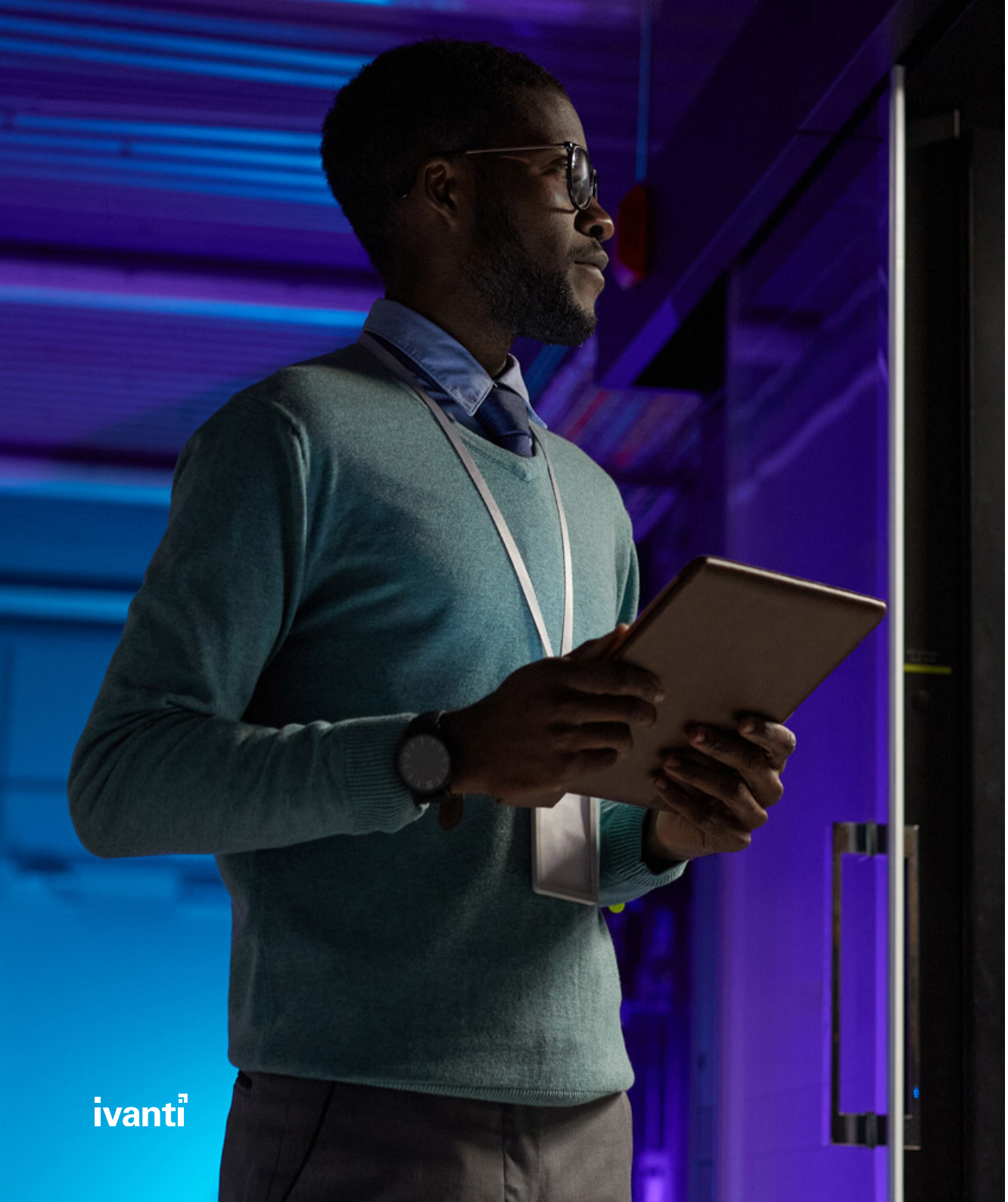
Angesichts des Ausmaßes und der Dringlichkeit der Situation müssen Regierungsorganisationen die Cybersicherheit als Teamarbeit angehen – und diese Arbeit mit Technologien unterstützen, die die Mitarbeiter nicht zusätzlich belasten.

Die Sicherheitslage von Regierungen und Behörden wird gestärkt, wenn Cybersicherheit ein Thema ist, das alle Mitarbeitenden verstehen, für das sie sich interessieren und für das sie sich verantwortlich fühlen – gekoppelt mit proaktiven Sicherheitsmaßnahmen, die eine bessere Mitarbeitererfahrung ermöglichen.

Für weitere Informationen:

Reset drücken: Ein Bericht zum Stand der Cybersicherheit im Jahr 2023

ivanti



Referenzen

1. Partnership for Public Service: “Engaging employees at federal agencies,” July 14, 2022. https://ourpublicservice.org/blog/engaging-employees-at-federal-agencies/

2. Ivanti: “2023 Cyberstrategy Tool Kit for Internal Buy-in.” October 2022. https://www.ivanti.com/resources/v/doc/ebooks/ivi-2702-cybersecurity-tool-kit-internal-buy-in-budget-influence-non-infosec

3. Sharon Ben-Moshe, Gil Gekker, Golan Cohen / Check Point Research: “OPWNAI: AI That Can Save the Day or Hack It Away.” Dec. 19, 2022. https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/

4. VOA: “Research: Deepfake ‘News Anchors’ in Pro-China Footage.” Feb. 8, 2023. https://www.voanews.com/a/research-deepfake-news-anchors-in-pro- china-footage/6953588.html

5. U.S. Government Accountability Office: “Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data,” Feb. 14, 2023. https://www.gao.gov/products/gao-23-106443

6. Partnership for Public Service: “Employee Engagement,” July 13, 2022. https://ourpublicservice.org/our-solutions/employee-engagement/
Federal News Network: “Return-to-office plans a major cause for decline in 2021 Best Places to Work results,” July 13, 2022. https://federalnewsnetwork.com/workforce/2022/07/return-to-office-plans-a-major-cause-for-decline-in-2021-best-places-to-work-results/

7. Ivanti: “2023 Cyberstrategy Tool Kit for Internal Buy-in.” October 2022. https://www.ivanti.com/resources/v/doc/ebooks/ivi-2702-cybersecurity-tool-kit-internal-buy-in-budget-influence-non-infosec

8. U.S. Government Accountability Office: “Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight,” Jan. 19, 2023. https://www.gao.gov/assets/gao-23-106415.pdf

Government Cybersecurity Status Report

4 Important Ways to Take Action and Drive Change in 2023

ivanti

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