BeyondTrust

Bericht über Bedrohung durch privilegierten Zugriff 2019

Größere Sichtbarkeit und eine verbesserte Integration sind entscheidend für die Bewältigung der modernen Bedrohungslandschaft

INHALTSVERZEICHNIS

DIE BEDROHUNGSLANDSCHAFT 2019 1

STELLUNGNAHME ZUM INSIDERZUGRIFF 3

DIE RICHTIGEN TOOLS FÜR DEN JOB 6

ERKENNUNG DER ZUNEHMENDEN BEDROHUNGEN 7

PRIVILEGED ACCESS MANAGEMENT IM JAHR 2020 UND DARÜBER HINAUS 10

ÜBER DIESEN BERICHT 11

DIE BEDROHUNGSLANDSCHAFT 2019

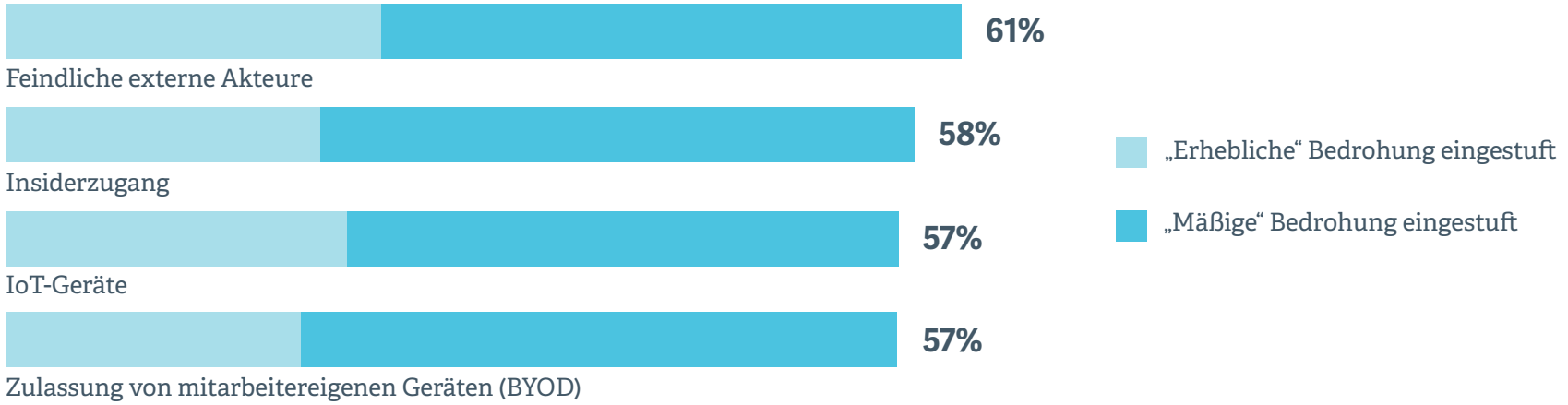
Einleitung

Die Welt ist ein unsicherer Ort. Vor allem für Cybersicherheitsexperten, von denen viele auf die harte Tour gelernt haben, dass sie sich nicht auf ihren Erfolgen ausruhen können. Es tauchen ständig neue Technologien und Bedrohungen auf. Diese Bedrohungen kommen sowohl von außen als auch von innen. In unserer Forschung 2019 zum Thema Bedrohungen durch privilegierten Zugriff haben wir festgestellt, dass fast zwei Drittel der Befragten (**64 %**) der Meinung sind, dass sie aufgrund des Mitarbeiterzugriffs wahrscheinlich von Sicherheitsverletzungen betroffen waren. **58 %** sagen das Gleiche über Lieferanten.

Auch die Geräte, die das Leben erleichtern sollen, können Unternehmen weiteren Risiken aussetzen. Obwohl feindliche externe Angriffe von **61 %** der Unternehmen als erhebliches oder mäßiges Risiko angesehen werden, folgt die Bedrohung durch unbefugte oder missbräuchliche Insiderzugriffe mit **58 %** sehr dicht dahinter. Gleichzeitig sehen **47 %** der Sicherheitsentscheidungsträger in den Bring Your Own Device (BYOD) Richtlinien und **57 %** im Internet der Dinge (IoT) ein mindestens mäßiges Risiko.

In dieser vierten Ausgabe des jährlichen Berichts über Bedrohung durch privilegierten Zugriff von BeyondTrust werden wir ausführlich die Bedrohungslandschaft 2019 untersuchen, wobei wir uns besonders darauf konzentrieren werden, wie Sicherheitsentscheidungsträger mit dem Thema Privileged Access Management (PAM) umgehen.

Wahrgenommene Bedrohungen



Von Mitarbeiterverletzungen über Lieferantenvertrauen, bevorzugte Lösungen bis hin zu neu auftretenden Bedrohungen - dieser Bericht erörtert nicht nur die Herausforderungen, vor denen Entscheidungsträger stehen, sondern auch die wirksamen Lösungen, um sie anzugehen.

DIE BEDROHUNGSLANDSCHAFT 2019

Wesentliche Ergebnisse

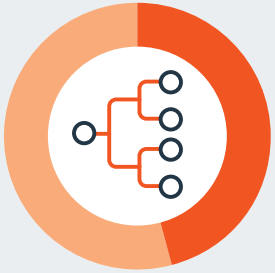
Bedrohungen durch Insider

64%

der Befragten glauben, dass sie durch unbefugten oder missbräuchlichen Zugriff von Mitarbeitern Sicherheitsverletzungen erlitten haben

90%

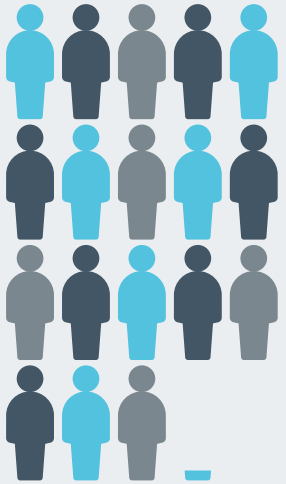
derjenigen mit voll integrierten PAM-Tools sind zuversichtlich, dass sie spezifische Bedrohungen von Mitarbeitern mit privilegiertem Zugriff identifizieren können – aber nur



46%

sind der Meinung, dass ihre Lösungen vollständig integriert *sind*

Lieferantenzugang



182

Lieferanten im Durchschnitt, die sich jede Woche bei IT-Systemen anmelden

58%

haben eine Verletzung aufgrund des Lieferantenzugriffs erlitten

Vertrauensebene

37% „Ich vertraue meinen Mitarbeitern voll und ganz“

25% „Ich vertraue meinen Lieferanten voll und ganz“

STELLUNGNAHME ZUM INSIDERZUGRIFF

Das Risiko von innen

Wenn man den Ausdruck „Cyber-Bedrohung“ hört, ist es natürlich, sich ein vorsätzliches, bösartiges, externes Risiko vorzustellen. Doch tatsächlich ist das Zugriffsmanagement für Mitarbeiter ebenfalls ein großes Problem.

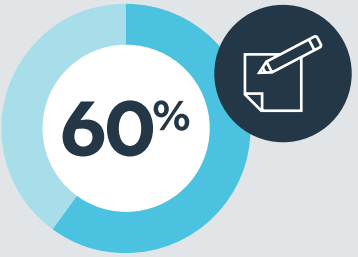
Der Grad der wahrgenommenen Bedrohung durch Insider ist im Jahresvergleich konstant geblieben. Zwei Drittel (**64 %**) unserer Umfrageteilnehmer glauben, dass sie in den letzten 12 Monaten wahrscheinlich entweder eine direkte oder indirekte Sicherheitsverletzung aufgrund des Mitarbeiterzugriffs erlitten haben, verglichen mit **66 %** im Jahr 2018. In Frankreich und APAC sind die Zahlen noch höher und steigen auf **69 %** bzw. **70 %**.

Aber sind diese Verstöße durch Insider die Folge von vorsätzlichen, bösartigen Handlungen oder unbeabsichtigten Fehlern?

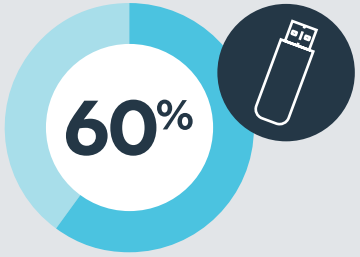
Besorgnis über den absichtlichen Missbrauch sensibler Daten zu persönlichen Zwecken ist gegenüber dem Vorjahr um **5 %** gesunken, und nur etwas mehr als die Hälfte (**52 %**) ist sehr oder ziemlich über die Sabotage durch einen ehemaligen Mitarbeiters besorgt. Unbeabsichtigte Mitarbeiterverstöße sind jedoch ein größeres Problem für unsere Befragten: **62 %** machen sich Sorgen über den unbeabsichtigten Missbrauch sensibler Daten durch einen Mitarbeiter.

Die Häufigkeit der einzelnen Bedrohungen variiert von Region zu Region. Nur **20 %** sind besorgt, dass Mitarbeiter im Vereinigten Königreich Daten auf einen Speicherstick herunterladen, während in der APAC-Region **42 %** dies als Problem sehen. Die Mitarbeiter in Deutschland geben ihre Passwörter am ehesten (**30 %**) an Kollegen weiter.

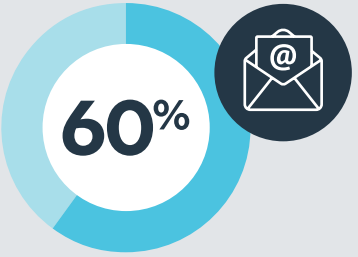
Unabsichtliche Sicherheitsverletzungen



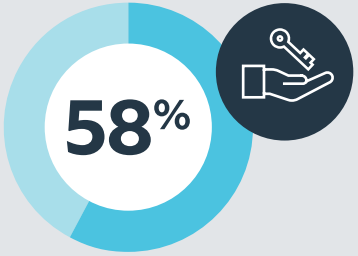
Aufschreiben der Passwörter



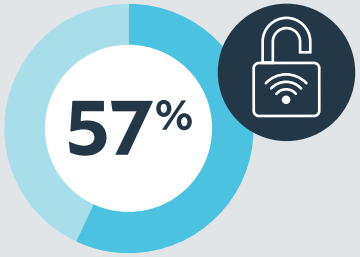
Daten auf externe USB speichern



Dateien an persönliche E-Mailadressen senden



Passwörter den Kollegen mitteilen



Einloggen über ungesichertes WLAN

Über längeren Zeitraum eingeloggt bleiben

Das Risiko von innen

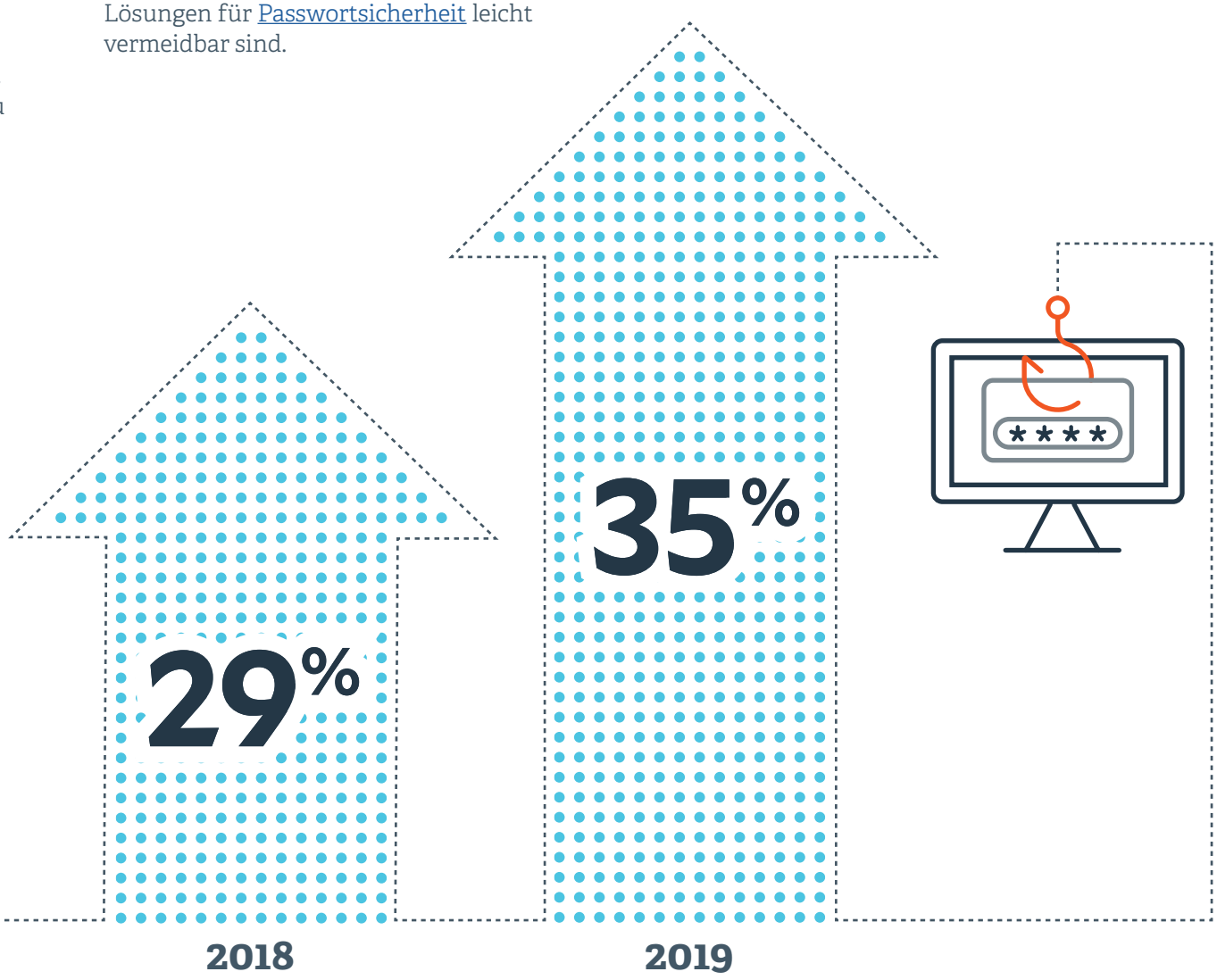
Im Endeffekt sind sich **71 %** der Unternehmen einig, dass sie sicherer wären, wenn sie den Zugriff auf Mitarbeitergeräte einschränken würden.

Dies ist jedoch in der Regel nicht realistisch, geschweige denn produktivitätsfördernd. Was können Sicherheitsentscheidungsträger also tun, um die Risiken des Mitarbeiterzugriffs zu reduzieren?

Ständige Mitarbeiterausbildung in Bezug auf bewährte Praktiken ist entscheidend, aber auch PAM-Tools können helfen, insbesondere da viele der von den Mitarbeitern ausgeführten Verhaltensweisen mit den richtigen Lösungen für Passwortsicherheit leicht vermeidbar sind.

Im Jahr 2019 waren sich **35 %** sicher, dass sie aufgrund von direktem oder indirektem Verhalten eine Sicherheitsverletzung erlebt hatten, eine Steigerung gegenüber **29 %** im Vorjahr.

Mitarbeiter verursachen versehentlich oder bewußt einen Verstoß

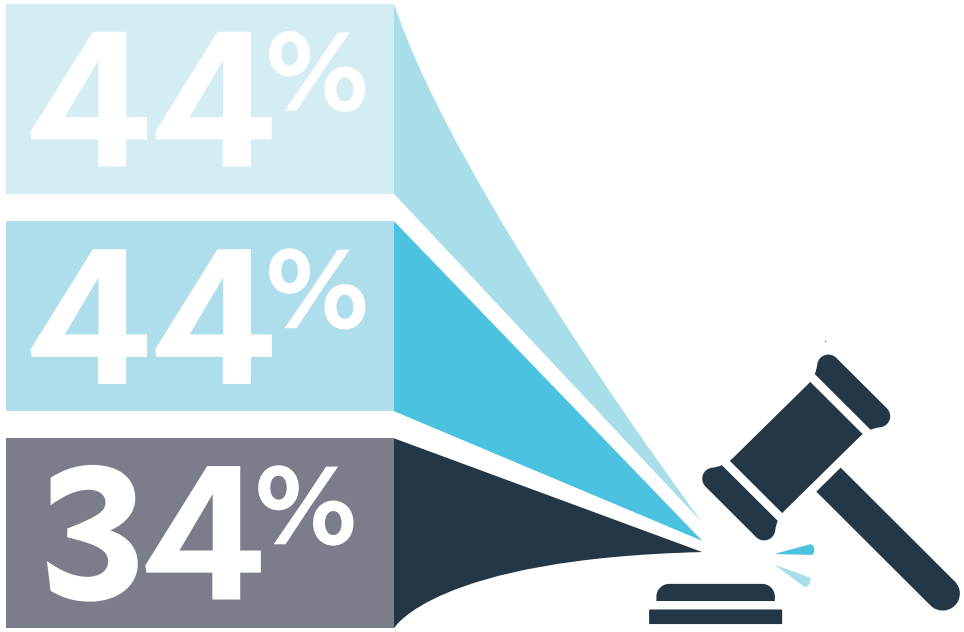


Was hat größeren Einfluss: Interne Probleme oder externe Faktoren?

Externe Faktoren wie Compliance-Mandate haben einen großen Einfluss auf die Zugriffspraktiken der Mitarbeiter. Fast die Hälfte (**44 %**) gibt an, dass die Einhaltung externer Standards einen erheblichen Einfluss auf die Art und Weise hat, wie sie den Zugriff der Mitarbeiter regeln. Dies ist in Deutschland (**54 %**) und Frankreich (**53 %**) noch deutlicher zu erkennen, was eine Folge der gestiegenen Bedenken hinsichtlich der DSGVO oder anderer Rechtsvorschriften sein kann.

Darüber hinaus sind ebenfalls **44 %** der Befragten der Meinung, dass eine größere Aufmerksamkeit in der IT-Community die Strategie vorantreibt – obwohl vier von zehn gegen unbeabsichtigten Datenverlust durch Mitarbeiter kämpfen, die ungesicherte Geräte verwenden. Die tatsächliche Erfahrung mit Datenschutzverletzungen durch Mitarbeiter oder ehemalige Mitarbeiter beunruhigt sie weitaus weniger: nur **34 %** geben an, dass sie sich auf ihre Vorgehensweisen und Richtlinien auswirken. Diese steigt jedoch deutlich auf **53 %** in APAC – einer Region, in der Entscheidungsträger auch wesentlich stärker vom Fokus des Vorstands getrieben werden (**41 %**).

Ausgangspunkt Motivation für Richtlinien



Ein Jahr nach der Umsetzung zeigt die DSGVO Wirkung: 65 % stimmen zu, dass die Einhaltung der DSGVO weiterhin Auswirkungen auf ihre Geschäftstätigkeit hat, während 58 % sagen, dass die Einhaltung der DSGVO schwieriger als erwartet ist.

BEKÄMPFUNG DES LIEFERANTENRISIKOS

Mehr Lieferanten, mehr Gefahren – und weniger Vertrauen

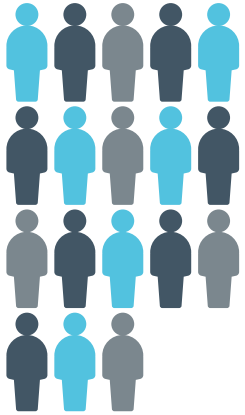
Neben der Verwaltung des Mitarbeiterzugriffs müssen Entscheidungsträger auch den Lieferantenzugriff berücksichtigen, bei dem die wahrgenommene Bedrohung hoch bleibt. Im Jahr 2018 glaubten **62 %**, dass sie aufgrund von Lieferantenzugriff einen Verstoß hatten. In diesem Jahr sagen **58 %** das Gleiche, wobei ein Viertel angibt, dass sie aufgrund eines Verhaltens der Lieferanten definitiv eine Sicherheitsverletzung erlitten haben. Die Zahlen variieren je nach Region, wobei man im Vereinigten Königreich und in Deutschland die geringste Anzahl von Sicherheitsverletzungen durch Lieferanten wahrnahm. In den APAC-Staaten war dies deutlich mehr.

Leider ist die Zuversicht, die die Entscheidungsträger bei der Verwaltung des Lieferantenzugriffs empfinden, im Jahresvergleich gefallen. Nur **29 %** sind sich sehr sicher, dass sie wissen, wie viele externe Lieferanten auf ihre Systeme zugreifen, gegenüber **38 %** im Vorjahr. Lediglich **31 %** sind sehr zuversichtlich, dass sie wissen, wie viele einzelne Logins Drittanbietern zugeordnet werden können.

Das Vertrauen in den Lieferantenzugriff ist auch geringer als das gegenüber Mitarbeitern: nur **20%** geben an, dass sie den Lieferanten voll und ganz vertrauen, während **37 %** dies über ihre Mitarbeiter sagen.

Da zwei Drittel der Unternehmen glauben, dass sie durch den Lieferantenzugriff Sicherheitsverletzungen ausgesetzt waren, besteht ganz klar die Notwendigkeit, sich mit der Kontrolle des Lieferantenzugriffs zu befassen. Unternehmen können es zwar nicht vermeiden, Lieferanten und anderen berechtigten Benutzern den benötigten Zugriff zu gewähren, aber sie müssen Wege finden, einen sicheren Fernzugriff bereitzustellen, der die Integrität der Sicherheit eines Unternehmens gewährleistet.

Lieferantenzugriffe



182

durchschnittliche Anzahl von Lieferanten, die sich jede Woche bei IT-Systemen anmelden

58%

glauben, dass sie eine Sicherheitsverletzung über einen Lieferantenzugriff erlitten

29%

sind sich sehr sicher, dass sie wissen, wie viele externe Lieferanten auf ihre Systeme zugreifen

In Unternehmen mit mehr als 5.000 Mitarbeitern geben 23 % an, dass sich mehr als 500 Lieferanten regelmäßig anmelden, was den Umfang ddes Risikos unterstreicht.

Die magische Zahl: 3

Wie unsere Forschung zeigt, sind Unternehmen eindeutig mit einer Reihe von Herausforderungen konfrontiert, die sich aus dem privilegierten Zugriff sowohl für Mitarbeiter als auch für Auftragnehmer ergeben. Was tun die Entscheidungsträger derzeit, um diese Bedrohungen zu bekämpfen? Und welche Strategien sollten sie verfolgen, um die PAM-Lösungen in Zukunft optimal zu nutzen?

Im Durchschnitt verwenden Unternehmen derzeit vier verschiedene Methoden des Passwortmanagements für privilegierte Anmeldeinformationen. Wenn es darum geht, Verletzungen zu verhindern, versuchen fast alle Unternehmen (**96 %**), den Zugriff durch privilegierte Tools zur Verwaltung von Berechtigungen zu kontrollieren. Drei Viertel schränken das Verwenden von gemeinsamen Admin-Passwörtern ein, während **72 %** regelmäßig Admin-Passwörter wechseln.

Nur ein kleiner Teil (**7 %**) der Unternehmen verfügt über keine eigenen PAM-Tools. Mehr als die Hälfte hat ein oder zwei PAM-bezogene Tools, während **40 %** drei oder mehr installiert haben. Für diese letzte Gruppe scheinen Fernzugriff und Passwortverwaltung die am weitesten verbreiteten Technologien zur Bewältigung von PAM zu sein. Die weitaus meisten (**91 %**) verfügen über einen sicheren Fernzugriff bzw. Support, während **87 %** über eine Lösung für privilegierte Passwort-Manager bzw. Zugangsdatenspeicher verfügen.

Der Wert dieser Lösungen liegt auf der Hand. Unternehmen mit drei oder mehr PAM-Tools haben mehr Vertrauen in die Sichtbarkeit von Bedrohungen und deren Ursprung, so dass sie diese Risiken erfolgreicher angehen können. Von dieser Gruppe glauben **43 %**, dass sie definitiv sagen können, dass sie eine Cyber-Verletzung aufgrund des Mitarbeiterzugriffs erlebt haben, im Vergleich zu nur **15 %** derjenigen ohne PAM-Tools. Ebenso könnten **61 %** mit drei oder mehr Tools Cyber-Verletzungen möglicherweise oder definitiv auf den Lieferantenzugriff zurückführen, während nur ein Viertel (**26 %**) derjenigen ohne Tools dasselbe sagen könnten.

Derweil fühlen sich diejenigen mit mehr PAM-Tools deutlich sicherer, die den unternehmensweiten Einblick in den privilegierten Benutzerzugriff überwachen, über individuelle Benutzeraktivitäten berichten und spezifische Bedrohungen von Mitarbeitern mit erhöhten Benutzerrechten identifizieren.

Taktiken zur Bekämpfung von Bedrohungen

96%

versuchen den Zugriff durch privilegierte Tools zur Verwaltung von Berechtigungen zu kontrollieren

66%

schränken die Verwendung gemeinsamer Admin-Passwörter ein

72%

wechseln regelmäßig Admin-Passwörter

40 % der Befragten verwenden drei oder mehr PAM-Tools in ihrem Unternehmen.

Integration ist die Grundlage für den Erfolg

Unternehmen benötigen nicht nur eine größere Auswahl an PAM-Tools. Die Lösungen, die sie bereits haben, müssen besser integriert werden, um eine größere strategische Wirkung zu erzielen. Fast alle Unternehmen (**93 %**) halten es für wichtig, dass PAM-Lösungen integriert werden, und fast zwei Drittel (**63 %**) glauben, dass eine „Integration mit den bereits vorhandenen Tools" die Sicherheit stärker erhöhen würde als mit „besseren Tools, aber ohne Integration". Und wie bei denen mit mehr als drei PAM-Tools ist auch die Integration mit einer verbesserten Sichtbarkeit verbunden.

Diejenigen mit vollständig integrierten Tools sind zuversichtlicher in Bezug auf ihre Fähigkeit, Bedrohungen durch Mitarbeiter und Lieferanten zu überwachen. Leider glauben derzeit nur **46%**, dass ihre Lösungen bereits vollständig integriert sind. Die Mehrzahl der anderen Befragten arbeitet entweder auf eine Integration hin oder verfolgt einen Ad-hoc-Ansatz. Mit mehr Sichtbarkeit haben Unternehmen eine bessere Kontrolle über den privilegierten Zugriff sowohl auf individueller als auch auf Unternehmensebene. Sie haben auch eine verbesserte Fähigkeit, Bedrohungen zu erkennen und so schneller zu bekämpfen.

Die Botschaft ist klar: Alle Unternehmen sollten prüfen, welche Arten von Tools sie einsetzen und wie sie diese in Zukunft besser integrieren können. Eine Vielzahl gut integrierter Tools aus verschiedenen PAM-Kategorien bietet umfassende Transparenz und Kontrolle für die Sicherheitsverantwortlichen.

Perspektiven zur PAM-Integration

93%

halten die Integration von PAM-Lösungen für wichtig

46%

glauben derzeit, dass ihre Lösungen bereits vollständig integriert sind

Unternehmen benötigen nicht nur eine größere Auswahl an PAM-Tools. Die Lösungen, die sie bereits haben, müssen besser integriert werden, um eine größere strategische Wirkung zu erzielen.

Die nächsten großen Themen im Bedrohungsmanagement für die Cybersicherheit

Obwohl das Ausmaß der wahrgenommenen Bedrohung sowohl für Insider als auch für Lieferanten ziemlich konstant geblieben ist, entwickelt sich die Bedrohungslandschaft selbst weiter und sind eine Reihe neuer Bedrohungen zu berücksichtigen.

Neue Technologien und Plattformen bringen oft neue Risiken mit sich. Das Internet der Dinge (IoT) verspricht beispielsweise viele Vorteile und Anwendungsfälle – aber es bringt auch eine Reihe von Sicherheitsrisiken mit sich. Mit der zunehmenden Nutzung des IoT wachsen auch die damit verbundenen Bedrohungen. Die Sichtbarkeit von Logins der IoT-Geräte wird nicht als das dringendste Problem angesehen. Drei Viertel (**76 %**) unserer Umfrageteilnehmer sind zuversichtlich, dass sie wissen, wie viele IoT-Geräte auf ihre Systeme zugreifen, während vier von fünf überzeugt sind, dass sie wissen, wie viele einzelne Logins diesen Geräten zugeordnet werden können. Die Fertigungsindustrie ist der Sektor mit der größten Zuversicht (**85 %**), während Behörden und der öffentliche Sektor eher unsicher sind (**68 %**).

Aber sowohl hinsichtlich der Anzahl der IoT-Geräte, die auf ihre Systeme zugreifen, als auch der zugehörigen IoT-Logins kann weniger als ein Drittel absolut sicher sein. Und selbst bei dieser wahrgenommenen Sichtbarkeit stellen IoT-Geräte eine ernsthafte Bedrohung dar, insbesondere wenn der Zugriff nicht effektiv verwaltet wird.

Weniger als jeder fünfte Entscheidungsträger glaubt, die von der IoT-Geräten ausgehenden Gefahren beseitigt zu haben. Sechs von zehn geben an, dass in IoT gespeicherte Standardpasswörter eine mittlere oder erhebliche Bedrohung darstellen. Die gleiche Anzahl von Befragten befürchtet, dass Passwörter von IoT-Geräten als Klartext gespeichert werden. Dieses Risiko wird noch dadurch verstärkt, dass Managementsysteme zur Kontrolle des Zugriffs auf IoT-Geräte immer noch manuell sind. Obwohl meisten Unternehmen eine Art von Zugriffsverwaltungsprogramm im Einsatz haben, geschieht die Zugriffsverwaltung bei **40 %** manuell, während **13 %** überhaupt nichts haben. Da der Einsatz von IoT-Geräten am Arbeitsplatz nur noch zunehmen wird, müssen Sicherheitsentscheidungsträger handeln und nach verbesserten Lösungen suchen.

Glücklicherweise ist auch klar, dass das Verwenden von Lösungen zur Verwalten von IoT-Geräten den Entscheidungsträgern mehr Vertrauen in ihre Fähigkeit zur Überwachung und Kontrolle des Zugriffs gibt. Die überwiegende Mehrheit (**91 %**) der Unternehmen, die eine spezialisierte Lösung einsetzen, ist von ihrer Fähigkeit überzeugt, dies zu tun, verglichen mit nur **71 %** derjenigen, die manuell arbeiten, und **57 %** derjenigen, die keine IoT-Management-Lösung installiert haben. Diejenigen, die sich für eine IoT-Sicherheitslösung entschieden haben, sind auch eher zuversichtlich in Bezug auf die Anzahl der einzelnen Anmeldungen und die Anzahl der an ihr Netzwerk angeschlossenen IoT-Geräte.

Die spezifische Art der benötigten Lösung hängt von den Anforderungen des Unternehmens ab. Privilege Remote Access kann zur Kontrolle und Überwachung des Zugriffs verwendet werden, während Endpoint Privilege Management dazu beitragen kann, eine Strategie des geringstes Privileg zu implementieren, die es Unternehmen ermöglicht, Administratorrechte zu entfernen und zu verwalten, welche Aktionen an bestimmten Endpunkten ausgeführt werden können. Darüber hinaus kann eine Lösung wie Password Safe zum Speichern, Verwalten und Rotieren von Passwörtern für privilegierte Konten verwendet werden, wodurch das Risiko von Standardanmeldeinformationen minimiert wird.

IoT Access Threats

60%

halten konstante Standard-IoT-Passwörter für eine mäßige oder erhebliche Bedrohung

40%

verwalten den IoT-Zugang manuell

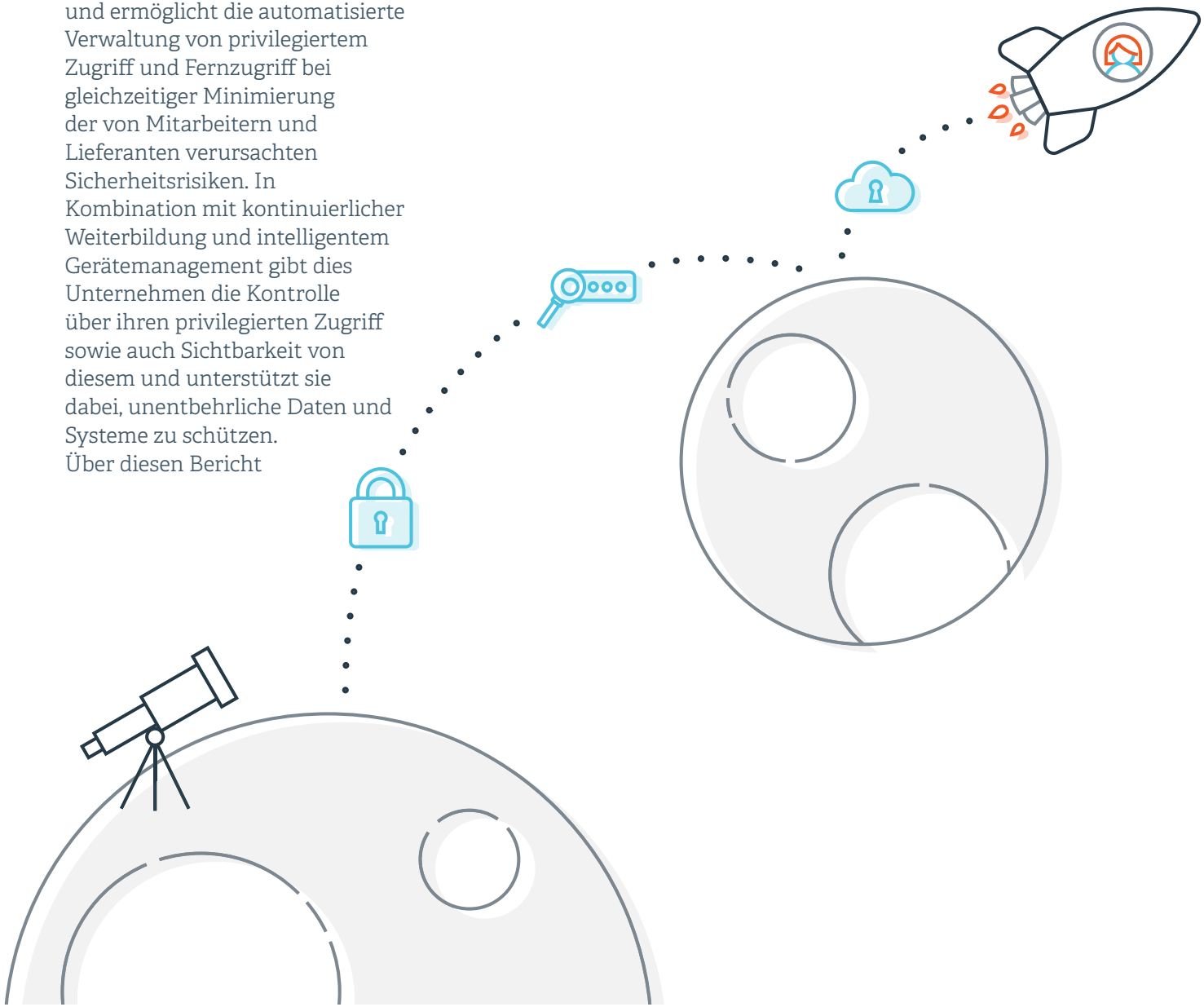
PAM IM JAHR 2020 UND DARÜBER HINAUS

Wie geht es mit dem Zugriffsmanagement weiter?

Probleme mit dem Zugriff von Mitarbeitern und Lieferanten werden auch im nächsten Jahrzehnt nicht verschwinden. Solange Unternehmen über zu schützende Daten und IT-Ressourcen verfügen, werden weiterhin neue Bedrohungen auftauchen.

Doch wie der Bericht von 2019 deutlich gemacht hat, ist es möglich, die Sichtbarkeit von Bedrohungen zu verbessern und das Vertrauen in die Sicherheit einer IT-Umgebung zu stärken. Mit einer angemessenen Anzahl gut integrierter PAM-Lösungen können Unternehmen größere Transparenz und Kontrolle über privilegierte Insider und Drittanbieter erlangen, ohne die Produktivität zu beeinträchtigen.

BeyondTrust entwickelt marktführende PAM-Lösungen für die Benutzerfreundlichkeit und ermöglicht die automatisierte Verwaltung von privilegiertem Zugriff und Fernzugriff bei gleichzeitiger Minimierung der von Mitarbeitern und Lieferanten verursachten Sicherheitsrisiken. In Kombination mit kontinuierlicher Weiterbildung und intelligentem Gerätemanagement gibt dies Unternehmen die Kontrolle über ihren privilegierten Zugriff sowie auch Sichtbarkeit von diesem und unterstützt sie dabei, unentbehrliche Daten und Systeme zu schützen.
Über diesen Bericht



ÜBER DIESEN BERICHT

Erkenntnis von vier Jahren

Die erste Ausgabe dieses Berichts erschien 2016 unter dem Titel „Vendor Vulnerability Index“, um die Risiken im Zusammenhang mit dem Vendor Access Management zu quantifizieren. Danach wurde der Themenbereich des Berichts erweitert, um Trends in anderen Risikobereichen im Zusammenhang mit dem privilegierten Zugriff zu erkennen und die gesamte Bedrohungslandschaft aufzudecken. Der Bericht über Bedrohung durch privilegierten Zugriff, der jetzt in der vierten Ausgabe erscheint, ist eine jährliche Veröffentlichung, die für alle zugänglich ist, die ein besseres Verständnis der Risiken im Zusammenhang mit nicht verwalteten Privilegien und deren Verringerung wünschen.

4
Jahre
Erkenntnis

Forschungsansatz

Wir haben 1.006 Entscheidungsträger für Netzwerkzugriff und Sicherheit befragt, um ihre Wahrnehmungen, Verhaltensweisen, Absichten und das Verwenden verschiedener Lösungen für das Verwalten von privilegiertem Zugriff zu verstehen.

Die Teilnehmer kamen aus einer Reihe von Branchen, darunter Finanzen, Produktion, Gesundheitswesen, Behörden, Einzelhandel und professionelle Dienstleistungen.

In Zusammenarbeit mit Loudhouse, einem unabhängigen Forschungsinstitut, wurde die Umfrage in den USA und den Wirtschaftsregionen EMEA und APAC durchgeführt.

Der Bericht über Bedrohung durch privilegierten Zugriff ist eine jährliche Veröffentlichung, die für alle zugänglich ist, die ein besseres Verständnis der Risiken im Zusammenhang mit nicht verwalteten Privilegien und deren Verringerung wünschen.

1.006
Teilnehmer an der Umfrage in 2019

Über BeyondTrust

BeyondTrust ist der weltweit führende Anbieter von Privileged Access Management und bietet den nahtlosen Ansatz zur Verhinderung von Datenschutzverletzungen im Zusammenhang mit gestohlenen Zugangsdaten, missbräuchlichen Privilegien und kompromittiertem Fernzugriff. Unsere erweiterbare Plattform ermöglicht es Unternehmen, die Sicherheit von Privilegien einfach zu skalieren, wenn sich Bedrohungen in Endgeräte-, Server-, Cloud-, DevOps- und Netzwerkgeräteumgebungen entwickeln. BeyondTrust gibt Unternehmen die Sichtbarkeit und Kontrolle, die sie benötigen, um Risiken zu reduzieren, Compliance-Ziele zu erreichen und die operative Leistung zu steigern. 20.000 Kunden, darunter die Hälfte der Fortune 100-Unternehmen, und ein globales Partnernetzwerk vertrauen uns.

Über Endpoint Privilege Management

Lösungen für das Endpoint Privilege Management von BeyondTrust bieten Ihnen die Möglichkeit, die geringstmöglichen Berechtigungen durchzusetzen und lokale Administratorrechte zu beseitigen. Machen Sie Schluss mit übermäßigen Endbenutzerrechte und steuern Sie Anwendungen auf Windows-, Mac-, Unix-, Linux- und Netzwerkgeräten – ohne die Produktivität Ihrer Endbenutzer zu beeinträchtigen.

Über Password Safe

Password Safe BeyondTrust vereinheitlicht die Verwaltung von privilegierten Passwörtern und privilegierten Sitzungen und bietet sichere Erkennung, Verwaltung, Prüfung und Überwachung für alle privilegierten Anmeldedaten. Mit Password Safe können Unternehmen die vollständige Kontrolle über privilegierte Konten erlangen und diese auch nachweisen.

Über Privileged Remote Access

Privileged Remote Access von BeyondTrust sorgt für Transparenz und Kontrolle über den Zugriff von externen Lieferanten sowie über den internen Remotezugriff, so dass Unternehmen den Zugriff auf wichtige Ressourcen gewähren können, ohne jedoch die Sicherheit zu gefährden.

beyondtrust.com