brivo

2024

Top Global Sicherheitstrends

CSOs und Sicherheitsteams befähigen, Technologie und KI bestmöglich zu nutzen

Inhaltsverzeichnis

Sich auf Innovationen einlassen

Eine neue Ära für Sicherheitsexperten im Jahr 2024

Das vergangene Jahr stand ganz im Zeichen sich weiterentwickelnder Technologien, von Robotik über Blockchain bis hin zu Quantencomputing. Doch keine davon wurde so gehypt wie die KI. KI und Automatisierung sind zwar nicht neu, aber sie bieten ein enormes Optimierungspotenzial für alle Arten von Anwendungen, und Sicherheitssysteme sind zweifellos eine davon. Datenanalyse, Gesichtserkennung, Authentifizierung, proaktive Sicherheitsmodelle und vieles mehr werden in Zukunft durch KI verbessert werden.

Die gute Nachricht ist, dass Sicherheitsexperten gut aufgestellt sind, um sich an diese Veränderungen anzupassen. Die Sicherheitsbranche strotzt mittlerweile vor Innovationen. Sie ist weit entfernt von dem „stagnierenden“ Markt, der sie früher einmal war. Nehmen wir als Beispiel die Umstellung auf cloudbasierte Lösungen. In den letzten Jahren hat sich der Trend weg von physischen Systemen vor Ort und hin zu integrierten Systemen in der Cloud deutlich verstärkt. Dies ist ein globaler Trend, auch wenn das Tempo des Wandels vielleicht nicht überall gleich ist.

Es gibt auch mehrere Treiber für diese Veränderung. Heutzutage haben Kunden höhere Erwartungen an die Leistung ihrer Zutrittskontrollsysteme. Die Anforderungen an die physische Sicherheit sind anspruchsvoller. Und die digitale Transformation ist nach wie vor eine treibende Kraft für die technologische Modernisierung, auch wenn der Begriff mittlerweile ein alter Hut zu sein scheint.

Daher befindet sich unsere Branche an einem Wendepunkt und wir brauchten 2024 einen neuen Ansatz für unsere jährliche Umfrage unter Sicherheitsexperten. In diesem Jahr haben wir mit mehr Menschen als je zuvor gesprochen und eine größere Gruppe von Befragten einbezogen, von Chief Security Officers (CSOs), die die großen Entscheidungen treffen, bis hin zu den Sicherheitsexperten und Gebäudeverwaltern (Facility-Administrators), die sie umsetzen. Wir haben auch den Umfang der von uns untersuchten Branchen erweitert, einschließlich Finanzdienstleistungen, Technologie & IT, Einzelhandel, Logistik, Gesundheit & Wellness und Fertigung/Produktion.

TOP 3
SICHERHEITSTRENDS

Sicherheitsteams priorisieren die Integration

Sicherheitsteams priorisieren die Integration für eine Modernisierung der Technik

Hohe Erwartungen an KI

Die Erwartungen an KI sind hoch, erfordern aber mehr Fähigkeiten und Daten, um das volle Potenzial auszuschöpfen

Bedarf an mehr Budget und Befugnissen

CSOs sind an Entscheidungen beteiligt, doch der Wandel vollzieht sich aufgrund mangelnder Mittel und Befugnisse nur langsam

In einem Jahr des technologischen Fortschritts entpuppt sich KI als Spitzenreiter und verspricht ein transformatives Potenzial für alle Branchen, insbesondere im Sicherheitsbereich. Sicherheitsexperten sind bereit, sich auf Veränderungen einzulassen, indem sie Trends wie cloudbasierte Lösungen nutzen und steigende Kundenerwartungen befriedigen. Anpassung ist unerlässlich, da die digitale Transformation die Sicherheitslandschaft umgestaltet, um den sich verändernden Anforderungen und Erwartungen gerecht zu werden.

Trend 1

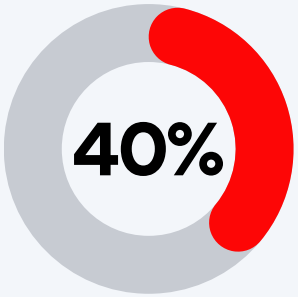
Sicherheitsteams priorisieren die Integration für eine Modernisierung der Technik

Wie bewerten Sicherheitsexperten den Stand ihrer Zutrittskontrolle und physischen Gebäude-sicherheit? Fast zwei von fünf Befragten haben kein volles Vertrauen in die Fähigkeit ihres Systems, die Sicherheit ihrer Mitarbeiter und Einrichtungen im Jahr 2024 zu gewährleisten (Abbildung 1). Betrachtet man die Sicherheitsexperten, die an vorderster Front stehen, d.h. die Systeme direkt ein und umsetzen, so steigt dieser Anteil auf fast die Hälfte, nämlich 49%.

Es scheint, dass außerhalb von Management-Teams und Sitzungssälen mehr Vorsicht und Sorge herrscht. Dieser Mangel an Vertrauen kann mehrere Gründe haben, angefangen bei nicht einheitlichen Systemen und veralteten Lösungen bis hin zu einer veränderten. Wahrnehmung von Sicherheit im Zeitalter der KI. Die wichtigste Erkenntnis hier ist jedoch der große Teil der Anwender, die kein volles Vertrauen in ihre Sicherheitssysteme haben.

Ebenso legen kleine Unternehme sowie große Unternehmen größten Wert auf die Integration ihrer Sicherheitssysteme mit funktionsübergreifenden Anwendungen. Die Verknüpfung der physischen Sicherheit mit anderen Teilen des Unternehmens, wie z. B. der Mitarbeitererfahrung, HR-Software oder Facility-Management-Anwendungen, ist ein durchgehendes Thema in diesem Bericht. Die gute Nachricht ist, dass sich die Sicherheitsteams diesen Anforderungen bewusst sind.

VERTRAUEN DER SICHERHEITSEXPERTEN IN IHR SICHERHEITSSYSTEM



Mangelndes Vertrauen in ihr Sicherheitssystem

ABBILDUNG 1

Security Operations Center (SOCs) haben jetzt eine höhere Priorität als je zuvor, was den Drang nach Zentralisierung auf einer "einzigen Plattform" widerspiegelt. Dies ist nicht nur ein Sicherheitstrend, sondern ein allgemeiner Trend in der gesamten. Unternehmens-IT. Eine aktuelle Umfrage ergab beispielsweise, dass 57 % der Entscheider in Unternehmen die Implementierung eines Tools zur Zentralisierung von Daten planen. Derselbe Bericht ergab, dass 64 % der Fachkräfte eine höhere Effizienz und 75 % ein Geschäftswachstum als Ergebnis dieser Zentralisierung erwarten.

Sicherheitsteams sind entschlossen, Vertrauensprobleme durch Systemintegration und -modernisierung zu lösen, um die Effektivität zu erhöhen

2024 Top Ziele: Technische Sicherheit

- Integration von Sicherheitssystemen mit anderen funktionsübergreifenden Anwendungen innerhalb von Organisationen
- Modernisierung bestehender Sicherheitssysteme
- Aufbau eines Security Operations Center (SOC)

UMFRAGE ZU DEN TECHNISCHEN ZIELEN DER PHYSISCHEN SICHERHEIT 2024

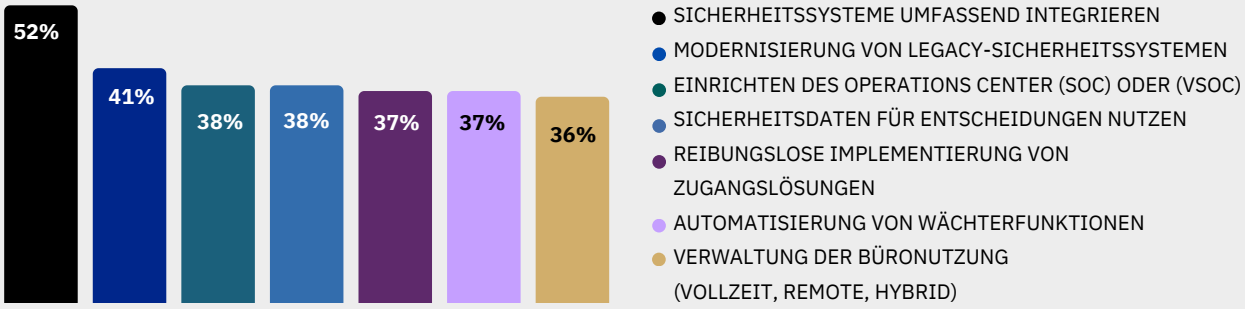


ABBILDUNG 2

Als größte Hindernisse für die Modernisierung der physischen Gebäudesicherheit wurden die Herausforderung der Integration neuer Lösungen in die vorhandene IT-Technologie, eine mangelnde Abstimmung zwischen der Sicherheitsabteilung und anderen Abteilungen sowie ein Mangel an Budget angesehen. Auch wenn die diesjährige Umfrage breiter angelegt ist, ist dies ein beständiger Trend, Jahr für Jahr.

Zu den größten Hindernissen für die Einführung neuer Technologien im Jahr 2023 gehörten Budgetbeschränkungen und der Nachweis der Rentabilität der Investitionen. Obwohl einige Fortschritte erzielt wurden, bestehen weiterhin ähnliche Herausforderungen. Budgetbeschränkungen bleiben ein Problem, insbesondere in wirtschaftlich benachteiligten Regionen.

Allerdings ist der Nachweis des ROI nicht mehr so problematisch. Dennoch hat sich der Widerstand gegen neue Technologien zu einem wichtigen Thema entwickelt, was möglicherweise auf einen schnelleren Wandel in der Branche und den technologischen Fortschritt hinweist.

Da sich die Unternehmen im digitalen Zeitalter weiterentwickeln, ist die Möglichkeit, den Return on Investment (ROI) darzustellen, immer einfacher und problemloser geworden. Trotz dieser Fortschritte hat sich jedoch eine neue Herausforderung in Form eines Widerstands gegen die Einführung neuer Technologien ergeben.

IDENTIFIZIERUNG VON HINDERNISSEN: EINFÜHRUNG NEUER PHYSISCHER SICHERHEITSTECHNOLOGIEN

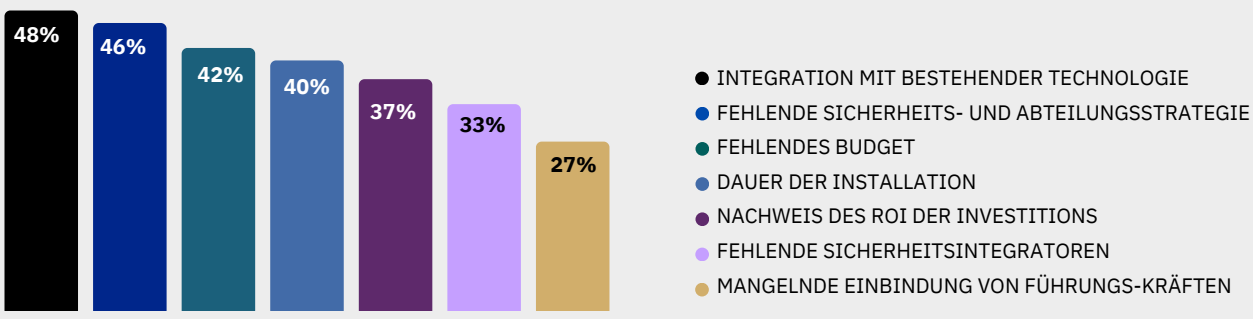


ABBILDUNG 3

Dieser Widerstand unterstreicht die Beschleunigung der Veränderungsgeschwindigkeit innerhalb der Branchen und den raschen Fortschritt der Technologie. Wenn sie diesen Wandel annehmen und Widerstände überwinden, können sich Organisationen und Sicherheitsintegratoren in einer Zeit raschen Umschwungs und lautstarker Botschaften von ihren Mitbewerbern abheben.

Interessanterweise berichtet jeder Dritte (33 %) der weltweit Befragten, dass ihr Sicherheitsintegrator entweder keine Informationen über neue Technologien hat oder diese Informationen zurückhält (Abbildung 4). Dieses Problem ist ein Hindernis für die Einführung in allen Regionen, insbesondere in der DACH-Region (mit Deutschland, Österreich und der Schweiz) und in den BeNeLux-Ländern (bestehend aus Belgien, den Niederlanden und Luxemburg) mit jeweils 36 % für beide Regionen. Besonders hoch ist der Widerstand bei den sogenannten Sicherheitsdirektoren mit 51 Prozent.

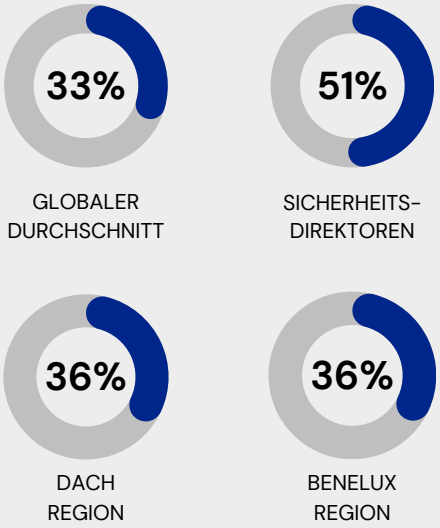
Dieses Ergebnis spiegelt möglicherweise eine Diskrepanz zwischen Branchenführern und Dritten, denen sie vertrauen sollten, wider, die durch eine bessere Kommunikation behoben werden könnte.

Fast die Hälfte, 49%, der Befragten gaben auch an, dass erfahrene Branchenexperten sich der Umstellung auf Systeme widersetzen, die sie ihre ganze Karriere lang gekannt haben (Abbildung 5). Das ist in jedem Beruf verständlich – warum sollte man etwas ändern, das bereits funktioniert?

Insbesondere für die Community der Sicherheitsintegratoren gilt, dass Veränderungen schwierig sein können, wenn man mit Organisationen zusammenarbeitet, die schon immer auf eine bestimmte Art und Weise an Gebäudeschutz und Gefahrenabwehr herangegangen sind. Doch diese Barriere könnte auch eine Chance sein. Integratoren sollten als vertrauenswürdige Berater gesehen werden, die den Kunden bei der Navigation durch die komplexen Zusammenhänge helfen, sie lehren, neue Technologien zu erforschen und die Angst vor Veränderungen durch Unterstützung und Aufklärung zu überwinden. Das geringe Vertrauen einiger Sicherheitsexperten in die Fähigkeiten der derzeitigen physischen Sicherheitssysteme zeigt, warum dies so wichtig ist.

Neue Technologien können ihnen, wenn sie richtig eingesetzt und integriert werden, einen wichtigen Vertrauensvorschuss geben. Sicherheitsintegratoren sollten diese Chance nutzen und ihr Verständnis für neue Technologien und die Bedürfnisse ihrer Kunden von Anfang an aktiv unter Beweis stellen. Andernfalls laufen sie Gefahr, in der Branche abgehängt zu werden.

NEUES TECHNOLOGIEBEWUSSTSEIN DURCH SICHERHEITSINTEGRATOREN



Den Sicherheitsintegratoren mangelt es an Bewusstsein für neue Technologien, insbesondere bei den Direktoren. Eine verbesserte Kommunikation ist entscheidend für Vertrauen und Technologieakzeptanz.

FIGUR 4

WIDERSTAND ERFAHRENER BRANCHENFACHLEUTE GEGEN VERÄNDERUNGEN

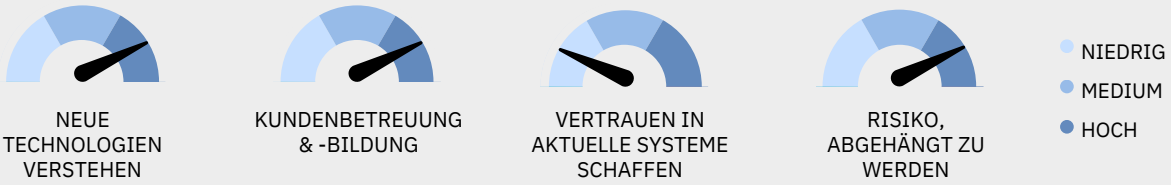
Branchenprofis, die sich dem Wandel widersetzen

ABBILDUNG 5

Sicherheitsintegratoren laufen Gefahr, in der Branche ins Hintertreffen zu geraten, wenn sie nicht in der Lage sind, ihr genaues Verständnis neuer Technologien zu demonstrieren.

ERFOLGSKONTROLLE

FAKTOREN, DIE SICH AUF DIE PERFORMANCE VON SICHERHEITSINTEGRATOREN AUSWIRKEN



DIESES DIAGRAMM ZEIGT, WELCH ENTSCHEIDENDE ROLLE SICHERHEITSINTEGRATOREN DABEI SPIELEN, KUNDEN BEI DER EINFÜHRUNG VON TECHNOLOGIEN ZU UNTERSTÜTZEN.

ABBILDUNG 6

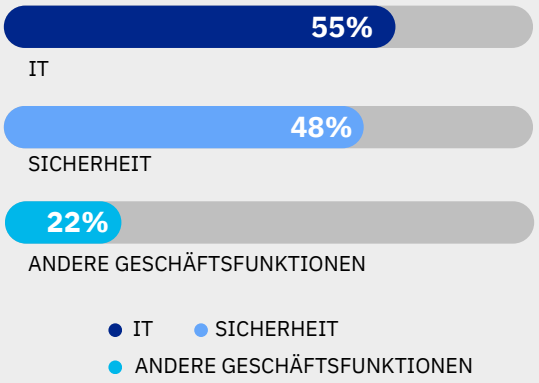
Trend 2

Die Erwartungen an KI sind hoch, erfordern aber mehr Fähigkeiten und Daten, um das volle Potenzial auszuschöpfen

Da KI und Automatisierung immer mehr an Bedeutung gewinnen, gibt es in der Sicherheitsbranche eine steigende Nachfrage nach erweiterten IT-Fähigkeiten sowie Zugang zu umfassenden Nutzer- und Analysedaten. Wir wollten herausfinden, wie Fachleute in verschiedenen Funktionen das sich abzeichnende Potenzial für Veränderungen in ihren Unternehmen inmitten dieses Übergangs zu KI und Automatisierung wahrnehmen.

Die IT ist die Geschäftsfunktion, von der die meisten erwarten, dass sie in den nächsten drei Jahren durch KI und Automatisierung verändert werden wird. Dieses Ergebnis ist nicht überraschend, da die potenziellen Fortschritte für die allgemeine IT durch KI oft klar hervorgehoben werden. Dicht dahinter lag die erwartete Veränderung im Sicherheitsbereich mit 48 % (Abbildung 7). Dies unterstreicht, dass Fachleute die bedeutenden Vorteile erkennen, die GenAI, maschinelles Lernen und natürliche Sprachverarbeitung in naher Zukunft für Anwendungsfälle der physischen Gebäudesicherheit haben werden. Die Erwartungen sind eindeutig hoch.

ERWARTETE VERÄNDERUNG DURCH KI & -AUTOMATISIERUNG

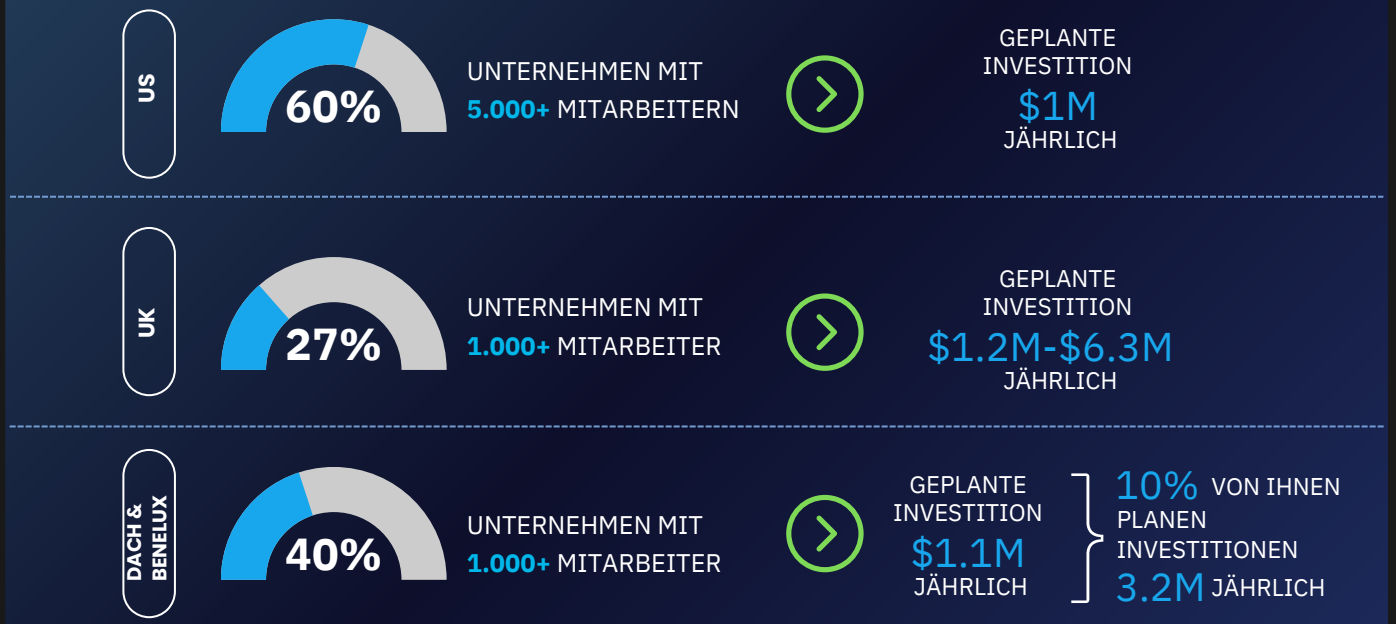


HOHE ERWARTUNGEN AN DIE DISRUPTIVE WIRUNG VON KI UND AUTOMATISIERUNG, BESONDERS AUF IT UND SICHERHEIT.

ABBILDUNG 7

KI-INVESTITIONSPLÄNE NACH UNTERNEHMENSGRÖSSE UND REGION

IN DEN NÄCHSTEN 3 JAHREN WERDEN GROSSE BUDGETS FÜR INVESTITIONEN IN KI UND AUTOMATISIERUNG BEREITGESTELLT



DIE DATEN ZEIGEN EIN ERHEBLICHES FINANZIELLES ENGAGEMENT IN DIESEN SPEZIFISCHEN REGIONEN.

ABBILDUNG 8

Obwohl das Bewusstsein für die Möglichkeiten der künstlichen Intelligenz weit verbreitet und die Budgetplanung im Gange ist, herrscht nach wie vor große Verwirrung bei Entscheidern. Nur 36% der weltweit Befragten haben großes Vertrauen in die Fähigkeit ihres Unternehmens, KI und Automatisierung zu verstehen und zu nutzen. In der DACH-Region sinkt dieses Vertrauen auf lediglich 28 %.

Darüber hinaus prognostizieren viele Teilnehmer zwar erhebliche Investitionen, um dieses Problem zu lösen. Aber das Budget ist immer noch eine häufige Einschränkung und die größte organisatorische Herausforderung bei der Einführung von KI (von 56% der Befragten genannt). Die zweitgrößte Sorge betrifft die Wartungskosten für die KI-Anwendungen, die von etwas mehr als der Hälfte (52%) der Befragten genannt wurden. Diese Marktstudie erscheint in einer Zeit wirtschaftlicher Unsicherheit für einige Regionen, was zu den Vorbehalten beitragen kann. Investitionen in neue Technologien können als gefährdet angesehen werden, wenn Unternehmen ihre Ausgaben reduzieren und Bargeld sparen müssen.

Viele Befragte (45 %) sehen auch Risiken bei der Eingabe von Daten in KI-Modelle sowie begrenztes KI-Know-how (41 Prozent) als zentrale Herausforderungen für die Einführung. Diese Ängste sind bei neuen Technologien zu erwarten, da Bildung und Gesetzgebung mit der Innovation nicht Schritt halten können. Diese Lücken müssen jedoch geschlossen werden, um das Vertrauen der Sicherheitsexperten zu stärken.

Klare Richtlinien- und Data-Governance-Prozesse werden dazu beitragen, diese Herausforderungen zu meistern. Mit der KI-Exekutiv-Verordnung von Präsident Biden in den USA und dem EU-KI-Gesetz, das in Europa auf den Weg gebracht wurde, gibt es bereits gute Fortschritte in diesem Bereich. Es liegt nun an den Unternehmen, dies auch in ihrer internen Politik zu berücksichtigen. Upskilling bietet eine längerfristige Verbesserungsmöglichkeit, erfordert allerdings eine Kombination aus Investitionen, strategischen Personaleinstellungen und einem Kulturwandel, der von der Vorstandsetage bis hinunter zu allen Ebenen des Unternehmens vorangetrieben werden muss.

GLOBAL VS DACH REGION

UNTERSCHIEDLICHES VERTRAUEN IN KI

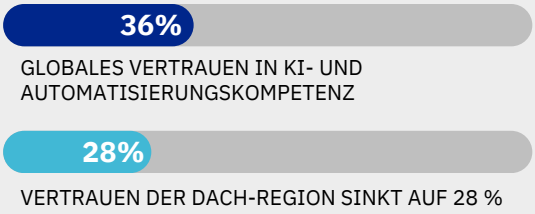


ABBILDUNG 9

DIE GRÖSSTEN ORGANISATORISCHEN HERAUSFORDERUNGEN BEI DER KI-EINFÜHRUNG

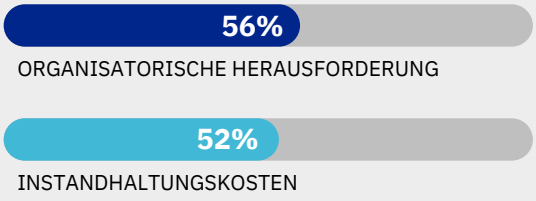


ABBILDUNG 10

WAHRGENOMMENE RISIKEN & HERAUSFORDERUNGEN BEI DER EINFÜHRUNG VON KI

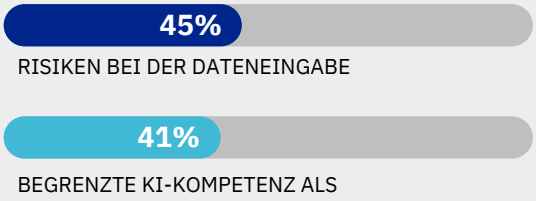


ABBILDUNG 11

Es gibt gute Nachrichten. Auch wenn die Befragten Vorbehalte haben, wie gut ihr Unternehmen die erwähnten Veränderungen umsetzen kann, sind sie optimistisch, was das Potenzial von KI angeht. Sie gehen davon aus, dass ein Drittel der Effizienzgewinne ihres Unternehmens in den nächsten drei Jahren auf KI und Automatisierung zurückzuführen sein werden. Dementsprechend prognostizieren 63 % von ihnen auch, dass KI- und Automatisierungsanwendungen nur eine minimale menschliche Aufsicht erfordern werden.

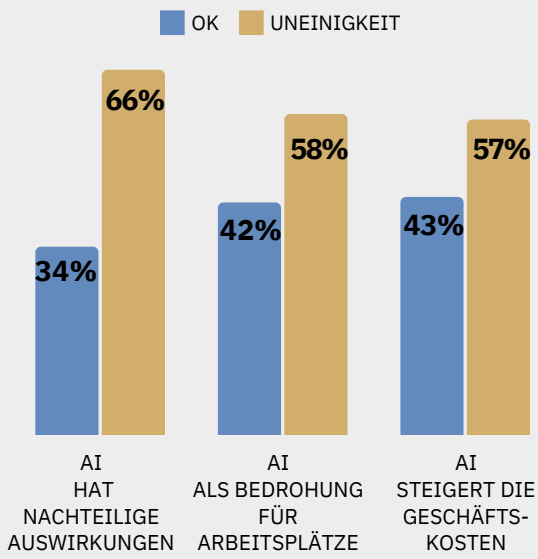
Positive Erwartungen bestehen weiterhin, wenn es um die allgemeineren Bedenken rund um KI geht. Zwei Drittel der Befragten (66 %) lehnen die Vorstellung ab, dass KI-“Gerüchte" schädliche Auswirkungen haben könnten, während mehr als die Hälfte (58 %) KI nicht als Bedrohung für Arbeitsplätze sehen.

Ähnlich viele, nämlich 57 %, sind nicht der Meinung, dass KI-Integrationen die Geschäftskosten in die Höhe treiben würden.

Vielleicht überwiegen für diese Sicherheitsexperten die Vorteile der KI deren potenzielle Risiken. Die Daten deuten auch darauf hin, dass Sicherheitsteams gängige Ängste im Zusammenhang mit Arbeitsplatzverlust oder “Gerüchten” nicht als relevant für die Branche erachten. Unabhängig davon deuten die Ergebnisse darauf hin, dass die Sicherheitsexperten das Potenzial der Technologie sehr optimistisch einschätzen.

Bei der Gebäudesicherheit ist es eher eine Frage des "Wann" als des "Ob", wenn es um KI geht. Es gibt eine klare Dynamik und den Wunsch, dass sie Teil der physischen Sicherheitstechnologie wird. Die Budgets wurden im Prinzip beiseite gelegt, und viele Anwender sehen klare Effizienzvorteile. Aber um die wichtigsten Herausforderungen zu meistern, braucht es CSOs, die die Befugnis haben, Veränderungen herbeizuführen.

EINSTELLUNGEN VON SICHERHEITSEXPERTEN ZU KI-PROBLEMEN



DATEN ZEIGEN OPTIMISMUS: DIE MEISTEN BEFRAGTEN LEHNEN KI-BEDENKEN AB:

ABBILDUNG 12

KI in der Sicherheit: Eine Frage des „Wann“, nicht des „Ob“

Die Integration von KI ist unvermeidlich und wird von einer klaren Dynamik und einem festen Wunsch angetrieben. Die Budgets sind bereits auf Effizienz ausgerichtet, aber Veränderungen brauchen fähige und handlungsfähige CSOs.

Trend 3

CSOs sind an Entscheidungen beteiligt, doch der Wandel vollzieht sich aufgrund mangelnder Mittel und Befugnisse nur langsam

Die Einführung von KI-Sicherheitstechnologien in Gebäuden erfordert eine starke Führung. Der CSO ist am besten in der Lage, die erforderliche Aufsicht zu gewährleisten. Wir wollten wissen, wie diese Rolle von Sicherheitsexperten wahrgenommen wird.

Fast drei Viertel (74%) der Sicherheitsexperten stimmten zu, dass CSOs in den letzten Jahren eine immer wichtigere Rolle gespielt haben. Dies kann auf verschiedene Faktoren zurückzuführen sein. Laut dem Beratungsunternehmen Security Executive Council sind dies die Herausforderungen, die die Weiterentwicklung der Rolle der CSO vorantreiben:

- COVID-19 führte zu einer Neudefinition des Arbeitsplatzes
- Eine Kündigungswelle und Stellenabbau erhöhen die Möglichkeit eines Informationsdiebstahls
- Nationalstaatliche Cyberangriffe werden immer häufiger, geopolitische Spannungen nehmen zu

Gebäudesicherheit braucht eine dedizierte Rolle auf der Führungsebene, um Risiken und Potenzial der KI zu managen. Jetzt, da KI für jedermann zugänglich ist, muss es organisatorische Richtlinien geben, die beachtet werden müssen. CSOs werden bei der Führung von Teams zur sicheren Integration dieser Technologie von entscheidender Bedeutung sein.

Die wachsende Bedeutung der CSOs beinhaltet, dass sie sich in allen Geschäftsbereichen stärker engagieren. Die Daten zeigen beispielsweise eine verstärkte Abstimmung zwischen Sicherheits- und Personalabteilungen bei der Entscheidungsfindung. Die meisten Befragten waren sich einig, dass die Sicherheits- und Personalabteilungen heute enger zusammenarbeiten als je zuvor.

ENTWICKLUNG DER ROLLE DES CSOs
FAKTOREN, DIE ZU VERÄNDERUNGEN FÜHREN

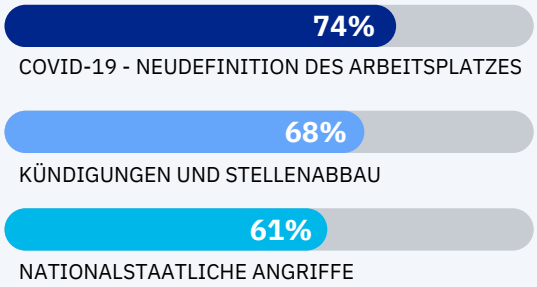


ABBILDUNG 13

ABSTIMMUNG VON SICHERHEITS- UND HR-ABTEILUNG BEI DER ENTSCHEIDUNGSFINDUNG

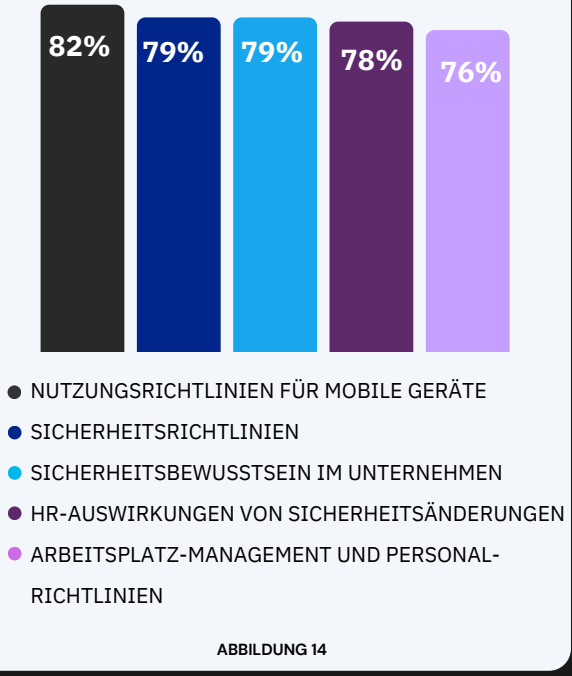


ABBILDUNG 14

Abstimmung zwischen Sicherheits- und Personalabteilung. Richtlinien und Arbeitsplatz-Management umfassen:

- Nutzungs- und Sicherheitsrichtlinien für Mobilgeräte
- Auswirkungen von Sicherheitsentscheidungen oder Systemänderungen auf das Personal
- Verwaltung und Nutzung des physischen Arbeitsplatzes und der Zugangskontrolle

Wenn wir uns jedoch eingehender mit der Rolle des CSO befassen, fangen wir an, einige Herausforderungen zu entdecken. Aus Sicht des Managements haben CSOs zwar in den meisten Organisationen eine Führungsposition inne, aber die Budget- und Entscheidungsbefugnisse spiegeln dies nicht wider. Diese Führungskräfte sind nur für 42% des Sicherheitsbudgets einer Organisation verantwortlich, und 56% der Befragten glauben, dass sie Teil eines Entscheiderteams für Beschaffungsfragen und nicht die alleinigen Entscheider sind. Nur 32 % der Studienteilnehmer sind der Meinung, dass der CSO der ultimative Entscheidungsträger ist.

Aber können CSOs wirklich effektiv sein, wenn sie nicht die volle Verantwortung für die Gesamtheit der Sicherheitsbudgets und die Entscheidungsfindung tragen? Die steigende Bedeutung von CSOs ist sicherlich positiv. Auch wenn sie heute nicht unbedingt das letzte Wort haben, so ist doch klar, dass sie stärker in den Entscheidungsprozess eingebunden sind als vor der Pandemie. Die Daten zeigen, dass CSOs heute häufiger als früher in anderen Unternehmensbereichen eingesetzt und bei wichtigen Entscheidungen zur Sicherheitspolitik konsultiert werden. Auch wenn die Verantwortung für den Schutz eines Unternehmens bei den CSOs liegt, müssen diese Führungskräfte mit anderen Entscheidern zusammenarbeiten, um die Sicherheit zu erhöhen.

Das Problem liegt darin, dass Abteilungen isolierte Entscheidungen treffen, ohne sich gegenseitig zu konsultieren. Wir sehen zwar eine wachsende Abstimmung zwischen der Personalabteilung und dem CSO, aber andere Ergebnisse deuten nach wie vor auf eine Trennung zwischen verschiedenen Teams hin. Eine fehlende Abstimmung zwischen der Sicherheitsabteilung und anderen Abteilungen wurde von 46% der Befragten als Hindernis für die Einführung neuer physischer Sicherheitstechnologien genannt. Diese Umfrageergebnisse unterstreichen die Notwendigkeit einer stärkeren Zusammenarbeit. Vielleicht könnte ein CSO mit mehr Entscheidungsbefugnis diesen Wandel vorantreiben.

Eine bessere Abstimmung zwischen den Abteilungen wird auch andere positive Auswirkungen auf die Verwendung von Unternehmensdaten in der physischen Gebäudesicherheit haben. Sicherheits-experten nutzen Zugangsdaten heute nur rudimentär, aber es gibt einen starken Wunsch, diese Daten für komplexere Zwecke zu nutzen. Dies bietet das Potenzial, Entscheidungen zu treffen und Veränderungen voranzutreiben. Dazu gehören die Erkennung anomaler Aktivitäten, die Anwendung von Analysen auf physische Sicherheitsrichtlinien, die Erfassung von Zugangstrends und Raumnutzung und vieles mehr.

Wo geht die Reise hin?

Wir können optimistisch sein, was die Einstellung der Sicherheitsbranche zur technologischen Modernisierung und ihr Interesse an der Erforschung neuer Technologien wie KI angeht. Sicherheitsexperten verstehen die Vorteile, wollen erhebliche Investitionen tätigen und zeigen mehr Positivität als andere Branchen.

Es gibt jedoch echte Bedenken hinsichtlich der Hindernisse für Veränderungen. Dazu gehören die praktische Integration neuer Lösungen, die Qualifikationslücke und die Sorge, dass Sicherheitsintegratoren nicht in der Lage sind, die richtige Hilfe anzubieten. Hinzu kommt, dass der Nachweis des ROI zwar kein so großes Problem mehr darstellt, der allgemeine Widerstand gegen Veränderungen jedoch schon. Dies deutet darauf hin, dass sich das Argument für eine bessere Technologie zwar durchgesetzt hat, aber die natürliche Trägheit bleibt.

Wichtige Takeaways

Diese Erkenntnisse zeigen, dass die Branche auf dem richtigen Weg ist. Es mag einige Hindernisse für Innovationen geben, aber diese Probleme zu erkennen ist der erste Schritt zu ihrer Überwindung. Sicherheitsexperten sind sich der Hindernisse bewusst, mit denen sie konfrontiert werden, und sind auf dem Weg zur Modernisierung der physischen Gebäudesicherheit.

01 **Ein klarer Modernisierungsbedarf zur Verbesserung der Sicherheit**

Integrierte Systeme, die Modernisierung des Tech-Stacks und eine einheitliche Lösungsplattform können das Vertrauen der Sicherheitsexperten stärken, insbesondere das der fast 40 %, die aktuell kein Vertrauen in ihre Sicherheitstechnologie haben.

02 **Budgetplanung für KI-Vorteile**

Die Bereitstellung von Budgets und ein umfassendes Verständnis der Effizienzgewinne durch KI sind entscheidend, damit Sicherheitsexperten eher früher als später von der disruptiven Wirkung KI-basierter Lösungen profitieren können. Dazu gehört auch ein Budget für die Weiterbildung der Mitarbeiter, um den Bedarf von morgen zu decken.

03 **Bildungs- und Richtlinienänderungen, die erforderlich sind, um die Einführung von Technologien zu steuern**

Wenn man mit Budgetbeschränkungen und Unsicherheiten hinsichtlich der Nutzung von KI konfrontiert ist, sollte man sich an Bildungsinitiativen wenden und interne politische Rahmenbedingungen ausnutzen, um Orientierung und Unterstützung zu erhalten.

04 **CSOs sind bereit, den technologischen Wandel anzuführen**

Während sich die Rolle des CSO ständig weiterentwickelt, gibt es eindeutig noch viel zu tun. Unternehmen müssen die wachsende Bedeutung dieser C-Level Führungsrolle verstehen und angemessen in sie investieren.

05 **Stärkung der CSOs**

Es liegt an den Sicherheitsintegratoren, die Rolle des CSO zu unterstützen und ihn mit Wissen und Werkzeugen auszustatten, damit er eine verantwortlichere Position erreichen kann.

06 **Sicherheitsintegratoren verlieren als vertrauenswürdige Berater an Boden**

Integratoren sollten die Gelegenheit ergreifen, zu vertrauenswürdigen Beratern zu werden, da ein Drittel der Fachleute noch nicht die richtige Unterstützung von ihren Sicherheitspartnern erhält.

07 **Sicherheitsintegratoren, die sich an die Technologie anpassen, werden sich durchsetzen**

Mit dem Innovationstempo Schritt zu halten, wird für Integratoren den Unterschied zwischen Erfolg und Scheitern ausmachen.

Über die Umfrage

Die Umfrage wurde in Zusammenarbeit mit dem unabhängigen Marktforschungsunternehmen Coleman Parkes im Oktober und November 2023 durchgeführt. Sie sammelt Daten von 850 Sicherheitsexperten aus acht Ländern (Großbritannien, USA, Deutschland, Österreich, der Schweiz, Belgien, den Niederlanden und Luxemburg) und 20 Sektoren.

UMFRAGE-ERGEBNISSE NACH JOB-TITEL

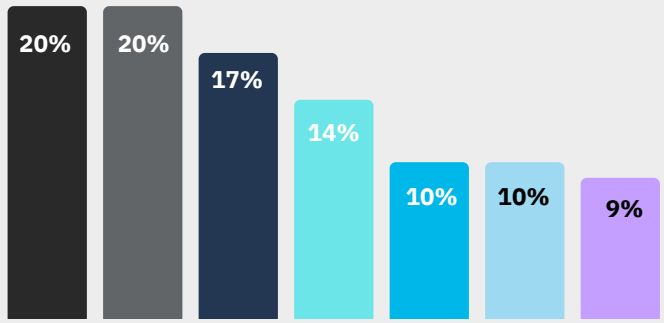
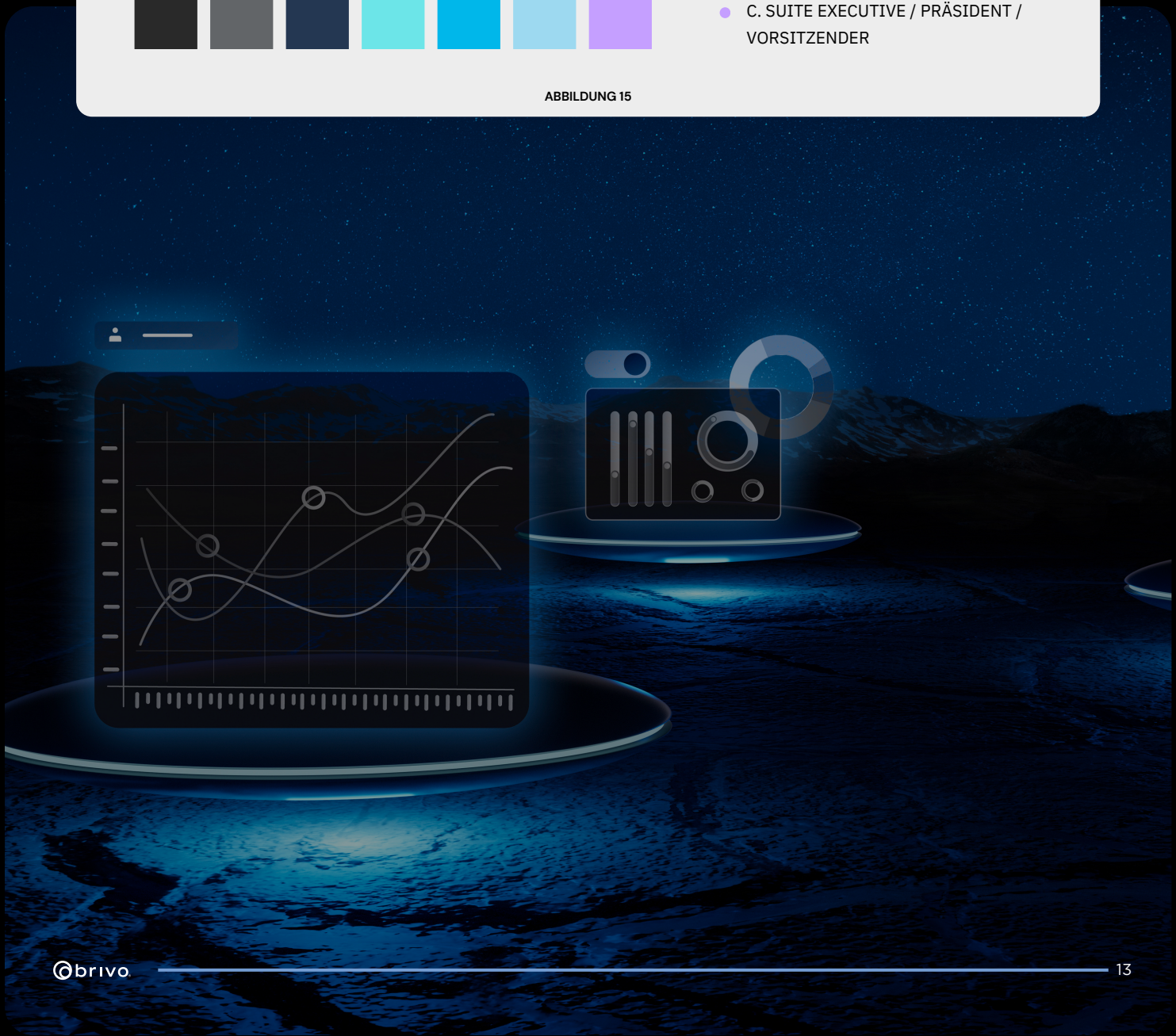


ABBILDUNG 15



Lassen Sie Brivo helfen

- Cloud-native Lösungen
- Datensicherheit und Überprüfbarkeit
- Zentralisierte Zugriffsverwaltung
- Integration in Videosysteme
- Einhaltung neuer und aufkommender Regeln
- Automatische Software-Updates
- Unbegrenzte Skalierung – überall auf der Welt
- Fernverwaltung aller Einrichtungen
- SOC2-Zertifizierung

ÜBER BRIVO

Brivo, Inc. hat vor über 20 Jahren die Kategorie der cloudbasierten Zugangskontroll- und Smart Spaces-Technologie geschaffen und ist nach wie vor ein weltweit führender Anbieter für Gewerbeimmobilien, Mehrfamilienhäuser und große dezentral aufgestellte Unternehmen. Das umfassende Produkt-Ökosystem und die offene API des Unternehmens bieten Unternehmen leistungsstarke digitale Tools, um die Automatisierung der Gebäudesicherheit zu erhöhen, die Erfahrung von Mitarbeitern und Mietern zu verbessern und die Sicherheit aller Menschen und Vermögenswerte in der bebauten Umgebung zu erhöhen. Die Brivo-Plattform für den Gebäudezugang ist heute die digitale Grundlage für die weltweit größte Sammlung von Kundeneinrichtungen, die mehr als 550 Mio. Quadratmeter an Immobilien in über 60 Ländern schützen. Erfahren Sie mehr unter **www.brivo.com**

Weitere Brivo-Lösungen finden Sie unter

Besuchen Sie brivo.com