ivanti

Managen, Automatisieren und Priorisieren (M.A.P) Ihrer Reise zur Cybersicherheit

Sechs Schritte für einen umfassenden Ansatz zur Cybersicherheit für den Everywhere Workplace

Inhaltsverzeichnis

Warum sollten Sie dieses eBook lesen?

Angriffe durch Software-Schwachstellen, Malware, Diebstahl von Zugangsdaten und eine Vielzahl anderer Bedrohungen haben sowohl in ihrer Häufigkeit als auch in ihrer Raffinesse exponentiell zugenommen. Was das Problem noch verschärft: der Aufstieg des

Everywhere Workplace, mit der raschen Verlagerung auf Remote-Arbeit sowie den erheblichen Einschränkungen sowohl bei den Budgets als auch bei der Anzahl der verfügbaren qualifizierten Sicherheitskräfte. Früher war es schwierig, mit jeder Schwachstelle Schritt zu halten, jetzt ist es praktisch unmöglich geworden.

Für Unternehmen und letztlich auch für die IT-Abteilung erfordern die Umstände eine umfassende Sicherheitsstrategie, die die Sicherheitslage verbessert, ein kontinuierliches Cyber-Risikomanagement gewährleistet und Unterbrechungen reduziert. Das bedeutet, sich von Lösungen, die für eine von PCs und Rechenzentren dominierte Welt entwickelt wurden, hin zu Lösungen für den Everywhere Workplace zu bewegen, bei dem Mobil- und Cloud-Technologien eine zentrale Rolle spielen.

Dieser Leitfaden dient als Ausgangspunkt und Grundlage für eine Reihe von Schritten, die Sie auf Ihrer Reise zur Cybersicherheit unterstützen. Wenn Sie die Empfehlungen in diesem Leitfaden befolgen, können Sie Benutzer, Geräte, Netzwerke, Anwendungen und Daten vor den zunehmenden Bedrohungen im Everywhere Workplace schützen.

Die heutige Cybersicherheitslandschaft

Die Bedrohung steht nicht bevor. Sie ist bereits da. Wie sind wir dahin gekommen?

Der rasante Aufstieg des Everywhere Workplace hat zu einer außerordentlichen Zunahme der Schwachstellen geführt. Während man anfangs davon ausging, dass der abrupte Wechsel zu einer dezentralen, digitalen Unternehmenslandschaft nur vorübergehend sein würde, ist der Everywhere Workplace nun auf Dauer da. Laut Gartner[1] beabsichtigen 82 % der Unternehmen, Remote-Arbeit teilweise zuzulassen, und 47 % beabsichtigen, ihren Mitarbeitern in Zukunft die Möglichkeit zu geben, ganztägig aus der Ferne zu arbeiten. Es liegt auf der Hand, dass die PC- und datenbankbasierten Sicherheitslösungen, auf die man sich vor der Pandemie verlassen hat, angesichts von Remote-Mitarbeitern und der weit verbreiteten Nutzung von persönlichen mobilen Geräten und Cloud-Anwendungen nicht mehr ausreichen.

Ein gutes Beispiel dafür sind die QR-Codes. Sie sind überall erschienen, von Restaurants bis zu Arztpraxen, und werden oft mit denselben mobilen Geräten gescannt, die die Mitarbeiter für ihre Arbeit verwenden. Aber die Allgegenwärtigkeit und einfache Verwendung von QR-Codes hat sie auch zu einem idealen Mittel für Phishing-Angriffe gemacht. Wenn nur Lösungen für E-Mail-Phishing vorhanden sind, sind die Benutzer – und das Unternehmen – anfällig für Angriffe.

Erschwerend kommt hinzu, dass alle Arten von Bedrohungen immer raffinierter werden – oft speziell auf durch Remote-Arbeit erzeugte Schwachstellen abzielend – und in einem alarmierenden Tempo auftreten. Die Zahl der Phishing-Versuche ist beispielsweise im Vergleich zum Vorjahr um 85 % gestiegen (74 % der Unternehmen wurden Opfer davon), und 59 % der Unternehmen haben berichtet, dass sie 2021 Opfer von Ransomware wurden. Hinzu kommt ein weltweiter Mangel an Sicherheitsexperten in Verbindung mit knappen Budgets überall, sodass der einfache Akt des Organisierens und Priorisierens von Schwachstellen den Löwenanteil der Zeit von Sicherheits- und IT-Mitarbeitern in Anspruch nimmt – bis zu 53 %[2].

Dies sind echte Herausforderungen: ein sich verändernder Arbeitsplatz, zu viel zu sichern, und nicht genug Ressourcen, um zu handeln. Auf der Stelle treten ist keine Option. Unternehmen, die nicht handeln, werden wahrscheinlich mehr Datenschutzverletzungen erleiden, einschließlich Ransomware, Phishing, Hacks und Schwachstellen, die von internen Mitarbeitern (absichtlich oder unabsichtlich) verursacht werden, und möglicherweise mit den sich ständig ändernden Compliance-Vorschriften in Konflikt geraten.

Die Auswirkungen auf die Marke sind astronomisch: unvorhergesehene Ausfallzeiten, Probleme mit der Einhaltung von Vorschriften, Verlust von Ansehen und Kunden und geschätzte Kosten in Höhe von 4,24 Millionen Dollar pro Datensicherheits-verletzung[3]. Ransomware-Angriffe verursachen eine

Unterbrechung von durchschnittlich 22 Tagen[4]. Und Compliance-Verstöße haben die Unternehmen mehr als 1,3 Milliarden Dollar gekostet … Tendenz steigend.[5]

“Dies sind echte Herausforderungen: ein sich verändernder Arbeitsplatz, zu viel zu sichern und nicht genug Ressourcen, um zu handeln.”

M.A.P. – Es ist Zeit für Ihre Reise zur Cybersicherheit

M.A.P., ein Akronym, das für Managen, Automatisieren und Priorisieren steht, ist ein dreistufiger Weg zum Aufbau einer umfassenden, skalierbaren und auf die Rahmen-bedingungen abgestimmten Cybersicherheitsstrategie für den Everywhere Workplace.

Managen, die erste Phase, befasst sich mit der Schaffung Ihrer Cybersicherheitsgrundlage. Ihr Ziel ist es, von einem unbekannten Zustand zu einem bekannten zu gelangen. Das bedeutet, dass Sie sich einen Überblick darüber verschaffen müssen, wer Ihre Benutzer sind und welche Geräte und Anwendungen sie nutzen, um besser zu verstehen, wo Ihre Schwachstellen liegen. Es bedeutet auch, dass Sie auf Praktiken verzichten müssen, die Ihr Unternehmen gefährden könnten, wie z.B. nicht verwaltete Geräte, die auf Unternehmensressourcen zugreifen (insbesondere auf solche in der Cloud) oder die nicht mit den neuesten Patches auf dem neuesten Stand gehalten werden.

In der zweiten Phase, der **Automatisierung**, geht es um die Verringerung von Belastungen. Sobald Sie einen bekannten Zustand erreicht haben, besteht der nächste Schritt darin, Ressourcen freizusetzen, indem Sie sich wiederholende, manuelle Prozesse wie die Pflege des Inventars, das Onboarding von Geräten und die Bereitstellung von Arbeitsbereichen und Anwendungen automatisieren. Sie können auch selbstreparierende und Self-Service-Lösungen hinzufügen, um die Notwendigkeit von IT-Eingriffen weiter zu reduzieren.

Bei der **Priorisierung** geht es schließlich darum, einen Zustand zu erreichen, in dem die IT-Abteilung über die Informationen und die Fähigkeit verfügt, die wichtigsten Risikobereiche zu identifizieren und anzugehen. Trotz der Automatisierung wird es immer noch Bereiche geben, in denen die IT eingreifen muss.

Anstatt einen nicht-strategischen Ansatz zur Risikobewältigung zu verfolgen, gibt die Priorisierung der IT-Abteilung die richtigen Daten und Risikobewertungen an die Hand, um einen intelligenten, strategischen Ansatz zur Reaktion und Abhilfe zu wählen M.A.P. sieht für jedes Unternehmen anders aus, sollte aber in jedem Fall die wichtigsten Säulen, also Benutzer, Geräte, Netzwerk, Anwendungen und Daten umfassen sowie konsistente Faktoren wie z.B.:

- Entdeckung.
- Management.
- Durchsetzung und Überprüfung der sicheren Konfiguration.
- Aktualisierte, risikobasierte Patching-Systeme.
- Verringerung des von Mitarbeitern verursachten Risikos durch Methoden, wie verifizierte Ausweise.
- Adaptive Kontrolle und Lebenszyklusmanagement.

Dieser Ansatz kann zwar nicht jeden Angriff verhindern, er minimiert jedoch die Angriffsfläche und ermöglicht ein proaktives, intelligentes Risikomanagement, damit Sie so gut wie möglich vorbereitet sind. Und wenn Bedrohungen auftauchen, reduziert ein kontinuierliches Cyber-Risikomanagement, das auf schnelles Handeln ausgelegt ist, das Sicherheitsrisiko und begrenzt Geschäftsunterbrechungen.

Zu den potenziellen Vorteilen gehören auch eine bessere Übersicht, weniger nicht verwaltete und nicht konforme Geräte, die auf Geschäftssysteme zugreifen, weniger Zeitaufwand für Patches, ein geringeres Risiko von Audit-Fehlern und finanzielle Einsparungen. Mit den richtigen Tools ist all dies mit weniger manuellen Eingriffen möglich – nicht mit mehr.

Das Dilemma, in dem Unternehmen feststecken – und sechs Schritte, um es zu lösen

Das klingt zwar hervorragend, aber wir verstehen, dass es auch entmutigend sein kann. Auf den ersten Blick liest es sich wie ein Dilemma ohne klare Antwort. Wir müssen die Sicherheit erhöhen, Bedrohungen reduzieren, die Produktivität verbessern und Ressourcen sparen, aber weil wir so dünn gesät sind und mit einer wachsenden Bedrohungslandschaft und Angriffsfläche konfrontiert sind, haben wir nicht die Bandbreite, um jetzt neue Programme zu implementieren.

Aus diesem Grund haben wir sechs Schritte festgelegt, die Unternehmen auf ihrem Weg begleiten sollen. Jeder deckt eine Komponente ab, die für eine effektive Cybersicherheit von entscheidender Bedeutung ist, und zusammen bilden sie die Grundlage für eine umfassende und skalierbare Strategie für das Cybersicherheitsmanagement.

Schritt 1

Vollständige Transparenz der Assets erhalten

Sie können nicht managen, wovon Sie nichts wissen. Das Fehlen eines präzisen und konsolidierten Cloud- und Asset-Inventars (Hardware und Software) macht Ihr Unternehmen anfällig für Sicherheitsrisiken, Compliance-Mängel, übermäßig komplexe Nachverfolgung und unübersichtliche Daten.

Angesichts der weltweit angespannten IT-Ressourcen ist es jetzt an der Zeit, in eine automatisierte Plattform zu investieren, die die Fähigkeiten Ihres Teams optimal nutzt. Eine umfassende Erkennungsinitiative findet alle Ressourcen in Ihrem Netzwerk, sowohl unternehmenseigene als auch BYOD-Geräte, und ordnet sie dem Kontext zu, sodass Sie wissen, wer welches Gerät benutzt, wie und wann der Benutzer dieses Gerät bei der Interaktion mit Ihrem Unternehmen verwendet und worauf er Zugriff hat.

Zu den Vorteilen der Entdeckung gehören:

- Verschaffen Sie sich in Echtzeit einen vollständigen Überblick über alle angeschlossenen Geräte und Software sowie deren Kontext.
- Ermöglichen Sie die effiziente Verwaltung, den Schutz und die Wartung von Assets überall.
- Rationalisieren und organisieren Sie alle Daten aus jeder Quelle.
- Verfolgen und fordern Sie Softwarelizenzen zurück.
- Optimieren Sie die Gesamtausgaben für IT-Ressourcen (Hardware, Software, Cloud).

Worauf Sie bei Ihrer Discovery-Lösung achten sollten:

- Die Fähigkeit, Geräte innerhalb und außerhalb des Netzwerks zu erkennen, zu verwalten und zu sichern. Dazu gehören auch Geräte, die sich mit Cloud-Diensten verbinden.
- Ermitteln Sie automatisch die Verbindungen zwischen wichtigen Hardware- und Software-Assets und den Diensten und Anwendungen, die von diesen Assets abhängen, und stellen Sie sie her.
- Eine konsolidierte Asset-Datenbank, die Informationen aus einer Vielzahl von Systemen wie Unified Endpoint Management (UEM), Netzwerk-Gateways, Cloud Services und ITSM abrufen kann.
- Abgleich zwischen dem, was von der IT beschafft wird, und dem, was aktiv mit den Dienstleistungen verbunden wird.
- Konnektoren zu Datenquellen (Anbieter, Vertragsdatenbanken, Hardware-Garantie, usw.)
- Integration mit ITSM- und Sicherheitsprozessen zur proaktiven Behebung von IT-Problemen und Sicherheitsschwachstellen.

Schritt 2

Die Geräteverwaltung mit einheitlichem Endpunktmanagement modernisieren

Da immer mehr Unternehmen zu hybriden Arbeitsumgebungen übergehen, sind Sicherheit und Verwaltung von Endgeräten sowohl für IT-Mitarbeiter als auch für Mitarbeiter wichtiger denn je. Ein modernes Gerätemanagement ist notwendig, um die Produktivität der Benutzer und der IT-Abteilung zu steigern, IT-Administratoren in die Lage zu versetzen, die Bereitstellung von Geräten und Software zu automatisieren und Benutzerprobleme schnell zu beheben.

Um die Supportzeiten zu verkürzen und sicherzustellen, dass alle Geräte nach denselben Standards verwaltet werden, wählen Sie eine UEM-Lösung mit Verwaltungsfunktionen für eine breite Palette von Betriebssystemen, darunter iOS, Android, Windows, macOS, Linux, Chrome OS, spezielle Geräte für Frontline-Worker, Wearables und IoT-Geräte, mit Unterstützung für modernes Management und Client-basierte Verwaltung.

Eine einheitliche Endpunktverwaltungslösung sollte sowohl vor Ort als auch als SaaS-Angebot verfügbar sein, um die Anforderungen Ihres Unternehmens gerecht zu erfüllen. UEM hilft, die Privatsphäre der Mitarbeiter durch die Trennung von geschäftlichen und persönlichen Daten auf den Endgeräten. UEM unterstützt auch BYOD-Initiativen und maximiert gleichzeitig die Privatsphäre der Benutzer und den Schutz der Unternehmensdaten.

Zu den Vorteilen der Verwaltung von Geräten mit einem einheitlichen Ansatz für die Endgeräteverwaltung gehören:

- Konsistente Verwaltung und Sicherheit für alle Ihre Geräte.
- Einfaches Onboarding, Bereitstellung von
- Anwendungen und Konfigurationen von Geräte-einstellungen im großen Maßstab, was sowohl die IT-Produktivität als auch die Benutzererfahrung verbessert.
- Überwachung des Zustands der Geräte und Sicherstellung der Einhaltung der Vorschriften zu jeder Zeit.
- Behebung von Problemen schnell und aus der Ferne.
- Automatisierung von Software-Updates und OS-Bereitstellungen.
- Bereitstellung umfassender Dashboards und Echtzeitinformationen zur Verbesserung der IT-Entscheidungsfindung.
- Erkennung und Behebung von Schwachstellen in Betriebssystemen und Anwendungen von Drittanbietern.
- Reduzierung der Unterbrechungen für den Endbenutzer und nahtloses Onboarding-Erlebnis.

Funktionen, auf die Sie bei Ihrer Lösung zur Geräteverwaltung achten sollten:

- Einfacher Einführungs- und Bereitstellungsprozess für die IT-Abteilung durch die Nutzung von Diensten wie Apple Business Manager (ABM), Google Zero-Touch Enrollment und Windows AutoPilot, um Benutzern eine automatische Geräteanmeldung zu ermöglichen.
- Die Fähigkeit, beliebige Endgeräte mit iOS, Android, macOS, Windows, Linux und ChromeOS sowie andere immersive und robuste Geräte wie HoloLens, Oculus und Zebra zu erkennen, zu verwalten und zu sichern.
- Unterstützung von Modellen für Mehrgerätebesitz, sodass Sie unternehmenseigene, BYOD- und gemeinsam genutzte Geräte verwalten, konfigurieren und sichern können.
- Die Möglichkeit, Außendienstmitarbeiter zu unterstützen und Geschäftsanwendungen auf deren Geräten zu sichern, ohne dass eine Geräteverwaltung erforderlich ist.
- Ermöglichung des sicheren Zugriffs auf Daten und Anwendungen auf beliebigen Geräten.
- Umfassende Transparenz und Kontrolle über alle verwalteten Geräte durch benutzerdefinierte Berichte und automatische Abhilfemaßnahmen.

Schritt 3

Gerätehygiene etablieren

Zu einer guten Gerätehygiene gehört ein proaktiver Ansatz, der sicherstellt, dass nur Geräte, die definierte Sicherheitsanforderungen erfüllen, auf Unternehmensressourcen zugreifen dürfen. Dazu gehören Systeme, die Geräte mit Software-Schwachstellen entweder automatisch patchen oder unter Quarantäne stellen können, sowohl im Betriebssystem als auch in den Anwendungen. Eine gute Gerätehygiene erfordert den Einsatz seriöser Lösungen zur Reduzierung der digitalen Angriffsfläche.

Andererseits kann eine schlechte Gerätehygiene Ihr Unternehmen anfällig für Cyberattacken wie Ransomware machen. Bei Unternehmen mit unzureichender Gerätehygiene liegt die Verantwortung für das aktive Aufspüren von Schwachstellen und den Schutz des Unternehmens vor Cyberangriffen eher bei der IT-Abteilung, als bei speziell entwickelten Lösungen.

Hygiene für mobile Geräte

Während 71 % der Berufstätigen der Meinung sind, dass mobile Geräte für ihre Arbeit essenziell sind, sind sich die Sicherheitsverantwortlichen fast einstimmig einig, dass Remote-Mitarbeiter einem größeren Risiko ausgesetzt sind als Mitarbeiter im Büro. Und dennoch haben sich drei von vier Sicherheitsexperten dem Druck gebeugt, die Sicherheit mobiler Geräte der Zweckmäßigkeit zuliebe zu opfern.[6]

Das ist ein großes Problem. Eine solide Hygiene für mobile Geräte ist entscheidend für die Bekämpfung von Schwachstellen auf dem Gerät (z. B. Jailbreak, Root-Erkennung, anfällige Betriebssystem-versionen usw.), Schwachstellen im Netzwerk (z. B. Man-in-the-Middle-Angriffe, bösartige Hotspots, ungesichertes Wi-Fi usw.) und Schwachstellen bei Anwendungen (Bewertung des hohen Sicherheitsrisikos, Bewertung des hohen Datenschutzrisikos, verdächtiges App-Verhalten, seitlich geladene App und so weiter).

Zu den Vorteilen der Einführung einer Hygiene für mobile Geräte gehören:

- Begrenzung der menschlichen Fehler und der IT-Investitionen durch automatisierte, umsetzbare, risikobasierte Informationen.
- Zero-Day-Erkennung und -Beseitigung, damit Sie nicht raten müssen, was auf Sie zukommt.
- Erkennung und Behebung von Problemen auch auf Geräten, die ausgeschaltet oder nicht verbunden sind.
- Schutz Ihrer Daten, Ihrer Ressourcen und Ihrer Marke durch Reduzierung der Angriffsfläche.

Funktionen, auf die Sie bei Ihrer Lösung zur Abwehr mobiler Bedrohungen achten sollten:

- Bevorzugen Sie Software, die vor allen Arten von mobilen Angriffen schützt, einschließlich Phishing-Angriffen sowie Angriffen auf Geräte-, Netzwerk- und Anwendungsebene.
- Schutz sowohl für Android-als auch für iOS-Geräte ist wichtig. Suchen Sie eine einzelne Anwendung mit einer geräteeigenen Engine für maschinelles Lernen, die mit einem UEM-Client kombiniert ist. Es ist viel wahrscheinlicher, dass die Benutzer eine einzige Anwendung einsetzen, als zwei – oder mehr.
- Achten Sie auf einen mehrschichtigen Schutz durch eine Lösung, die Bedrohungen auf Geräte-, Netzwerk- und Anwendungsebene sowie Phishing-Bedrohungen abwehrt und sowohl geräte- als auch cloudbasierte Funktionen zur Erkennung von Bedrohungen bereitstellt. Der geräteinterne Schutz benötigt keine Internetverbindung, um Bedrohungen zu erkennen und zu beseitigen.
- Essenziell ist eine abgestufte Compliance-Richtlinie, die den Endbenutzer und den Administrator darauf hinweist, dass sein Gerät nicht mehr konform ist. Bei Nichteinhaltung werden abgestufte Maßnahmen ergriffen, von der Sperrung des Zugriffs auf Unternehmensressourcen über die Quarantäne bis hin zur Stilllegung des Geräts und der Entfernung aller von UEM bereitgestellten Anwendungen, Inhalte, Einstellungen usw.

Hygiene für Desktop/Laptop-Geräte

Bis Ransomware-Angriffe und andere Datenschutzverletzungen der Vergangenheit angehören – eine Situation, die bei der derzeitigen Entwicklung vielleicht nie auftreten wird – müssen Unternehmen Maßnahmen ergreifen, um sich vor ihnen zu schützen. Patches zur Behebung von CVEs (Common Vulnerabilitäten and Exposures) gehören zu den besten Maßnahmen, die ein Unternehmen zur Abwehr von Ransomware-Angriffen ergreifen kann. Leider zeigt eine Studie von Ivanti[7], dass 71 % der IT- und Sicherheitsexperten das Patchen als zu komplex und zeitaufwendig empfinden. Das mag an der überwältigenden Anzahl von Sicherheitslücken liegen, die es gibt.

In der U.S. National Vulnerability Database (NVD) sind weit über 100.000 Schwachstellen aufgelistet.

Obwohl nur ein kleiner Prozentsatz dieser Schwachstellen mit Ransomware in Verbindung steht und ein noch kleinerer Prozentsatz trendige/aktive Exploits sind, kann es schwierig sein, herauszufinden, welche Schwachstellen das größte Risiko für ein Unternehmen darstellen. Ein Bericht von Ivanti zeigt[8], dass eine Organisation, die nur kritische Schwachstellen patchen würde, von 2018 bis 2020 lediglich zu 35 % gegen Ransomware geschützt wäre, wenn sie die CVSS v3-Bewertung verwenden würde. Automatisiertes, risikobasiertes Patching ist essenziell für die Hygiene von Desktop-/Laptop-Geräten.

Zu den Vorteilen einer Desktop/Laptop-Gerätehygiene gehören:

- Wie bei der Hygiene von mobilen Geräten begrenzen Sie sowohl menschliche Fehler als auch IT-Investitionen mit automatisierten, umsetzbaren risikobasierten Informationen.
- Verringerung der Wahrscheinlichkeit von Ransomware-Angriffen durch Patches zur Behebung von CVEs auf der Grundlage des realen Risikos.
- Gehen Sie über das Patchen hinaus und automatisieren Sie Reaktionen, damit eine Bedrohung ohne menschliches Eingreifen abgewehrt werden kann.

Funktionen, auf die Sie bei einer Lösung für Ihre Desktop-/Laptop-Gerätehygiene achten sollten:

- Für Desktop-/Laptop-Geräte ist es essenziell, die Software regelmäßig zu aktualisieren, um Schwachstellen zu beseitigen – oder zumindest einzudämmen. Da das Patchen von Sicherheitslücken schnell überfordernd werden kann, ist es hilfreich, eine Lösung zu finden, die Risiken automatisch bewertet und verwertbare Informationen liefert, wobei die dringendsten Schwachstellen nach Priorität geordnet werden.
- Die risikobasierte Priorisierung macht die riskantesten Schwachstellen in einer Umgebung sichtbar. So können Unternehmen gezielt die wichtigsten Patches einsetzen. Aktiver Bedrohungskontext, d. h. die Zuordnung von Schwachstellen zu realen Bedrohungsdaten ist von entscheidender Bedeutung, da er IT-/Sicherheitsteams dabei hilft, bei der Bekämpfung von Bedrohungen, die wahrscheinlich den größten Schaden anrichten werden, Prioritäten zu setzen.

Schritt 4

Benutzer absichern

Die einzigen, die Passwörter mögen, sind die Angreifer, die sie als Waffe einsetzen. Die passwortbasierte Authentifizierung ist nicht nur mühsam für die Benutzer, sondern es fehlt auch der Kontext von Gerät, Anwendung, Netzwerk und Bedrohung. Es gibt keine Möglichkeit herauszufinden, ob es sich bei der Person, die das Passwort eingibt, um einen Mitarbeiter oder einen Angreifer handelt, der sich das Passwort eines Mitarbeiters verschafft hat. Selbst die komplexesten Passwörter lassen sich relativ leicht durch Brute-Force-, Phishing- und andere Angriffe kompromittieren.

Zugangsdaten wie Passwörter gehören nach wie vor zu den begehrtesten Datentypen bei Sicherheitsverletzungen – sie waren in 61 % der Fälle betroffen[9].

Zugangsdaten werden schneller kompromittiert als jede andere Art von Daten. Dies gilt insbesondere für Phishing, das in der Regel auf Zugangsdaten abzielt, um sich weiteren Zugang zum Unternehmen des Opfers zu verschaffen.

SSO-Lösungen schaffen eine einzige Schwachstelle, die von Hackern ausgenutzt werden kann, um Zugang zu den meisten oder allen Unternehmensanwendungen zu erhalten. Untersuchungen[10] zufolge verwenden 42 Prozent der Befragten ihre Passwörter für mehrere Konten und 17 Prozent verwenden zwei bis fünf Passwörter für alles. Das bedeutet, dass Ihr Unternehmen gefährdet ist, wenn jemand ein Konto außerhalb des Arbeitsumfelds kompromittiert hat, aber dieselben Passwörter bei der Arbeit verwendet.

Mit der Zunahme der Remote-Arbeit könnte man annehmen, dass Unternehmen ihre Passwortprotokolle verschärfen, aber in einer Untersuchung von Verizon[11] gab mehr als ein Drittel der Befragten an, dass ihr Unternehmen die Authentifizierungsanforderungen gelockert hat, um die COVID-19-Beschränkungen bewältigen zu können.

Es ist Zeit für die passwortlose Authentifizierung über Zero Sign-On.

Zero Sign-On ist eine Authentifizierungsmethode, bei der keine Passwörter verwendet werden (so wie bei Single Sign-On ein einziges Passwort verwendet wird).

Die Vorteile der passwortlosen Authentifizierung für Ihre Benutzer sind unter anderem:

- Keine Passwörter = keine Zugangsdaten, die gestohlen oder gefälscht werden können.
- Keine Passwörter = zufriedenere Benutzer, die sich keine Passwörter merken müssen oder aus ihren Konten ausgesperrt werden.
- Erhöht den Reifegrad Ihrer Zero-Trust-Sicherheit.

„Es gibt keine Möglichkeit herauszufinden, ob es sich bei der Person, die das Passwort eingibt, um einen Mitarbeiter oder einen Angreifer handelt, der sich das Passwort eines Mitarbeiters verschafft hat“.

- Spart Geld, das bisher für das Zurücksetzen von Passwörtern und den Umgang mit Sicherheitsverletzungen ausgegeben wurde.

Funktionen, auf die Sie bei Ihrer Authentifizierungslösung achten sollten:

- Die ideale Lösung bietet passwortlosen Zugang zu Geräten, Geschäftsanwendungen und Cloud-Diensten.
- Ein effektiver passwortloser Zugang beruht auf einer Multifaktor-Authentifizierung, die den Besitz (was Sie haben, z. B. ein mobiles Gerät), die Inhärenz (biometrische Daten wie Fingerabdruck, Face ID usw.) und den Kontext (Standort, Tageszeit usw.) anstelle von Wissensfaktoren (wie Passwörter oder Sicherheitsfragen) einbezieht, um die Authentifizierung zu gewährleisten.
- Für einen Zero-Trust-Sicherheitsansatz mit kontextbezogenem Zugriff nutzen Sie eine Lösung, die sich in eine einheitliche Endpunktverwaltungslösung integrieren lässt, die Benutzer, Gerät, Anwendung, Netzwerk und Bedrohungen überprüfen kann, bevor sie den Zugriff gewährt.
- Achten Sie auf passwortlose Authentifizierungslösungen, die sich nahtlos in bestehende Identitätslösungen wie IdP/IAMs, MTD/XDR/EDR, SOAR, SIEMs und mehr integrieren lassen.

Schritt 5

Einen sicheren Zugang ermöglichen

Die Netzwerkgrenzen, die funktionierten, als Ihr Team noch im Büro war, reichen im Everywhere Workplace nicht mehr aus. Da Mitarbeiter von verschiedenen (und oft unvorhersehbaren) Standorten aus arbeiten, muss eine moderne Netzwerkumgebung diese Dynamik widerspiegeln, Einschränkungen und Komplexität beseitigen und gleichzeitig Sicherheit gewährleisten.

Heutige Netzwerke sollten auf den Prinzipien des Software-definierten Perimeters (SDP) aufgebaut sein. Ein SDP bietet eine integrierte Sicherheitsarchitektur, die mit bestehenden Sicherheitsprodukten wie Anti-Malware nur schwer zu erreichen ist. Es ist so konzipiert, dass es bewährte, auf Standards basierende Komponenten wie Datenverschlüsselung, Remote-Attestierung, wechselseitige Transport Layer Security und Security Assertion Markup Language nutzt. Durch die Integration dieser und anderer standardbasierter Technologien wird sichergestellt, dass SDP in Ihre bestehenden Sicherheitssysteme integriert werden kann.

Obwohl SPD eine Netzwerkstruktur ist, erfordert sie dennoch eine Sicherheitsebene, um die Vorteile zu maximieren. An dieser Stelle kommt Zero Trust – und insbesondere Zero Trust Network Access (ZTNA) - ins Spiel. Gartner definiert ZTNA als ein Produkt oder eine Dienstleistung, die eine identitäts- und kontextbasierte, logische Zugriffsgrenze um eine Anwendung oder eine Reihe von Anwendungen herum schafft. SDP kann zur Implementierung von Zero-Trust-Netzwerken verwendet werden.

Zu den Vorteilen der Einrichtung eines an jedem Ort sicheren Zugangs gehören:

- Überprüfung, dass nur vertrauenswürdige, authentifizierte Benutzer Zugriff auf Ressourcen haben.
- Das Netzwerk kann die äußere Begrenzung verwischen, was eine flexiblere Bereitstellung und einfachere Arbeitsabläufe für den Endbenutzer ermöglicht.
- Vermeidung der Einschränkungen und der Komplexität harter Perimeter, einschließlich ihrer Neigung, einen zusätzlichen, unnötigen Zugang zu Teilbereichen des Netzwerks zu eröffnen.
- Erhaltung von Sicherheit und Sichtbarkeit bei gleichzeitiger Erleichterung des Zugangs.

Merkmale, auf die Sie in Ihrem Zero-Trust-Netzwerk achten sollten:

- Datenhoheit: Die Anwendungsdaten werden nicht durch das Netzwerk des Anbieters übertragen und sind nicht dem Internet ausgesetzt. Dieser direkte Weg maximiert die Leistung und das Benutzererlebnis.
- Ganzheitliche Sichtbarkeit: Aktivitäten pro Benutzer, pro Gerät und pro Anwendung, einschließlich der von SaaS bereitgestellten Ressourcen.
- Kontinuierliche und anpassungsfähige Bewertung der Sicherheitslage des Clients mit automatischer Durchsetzung von Richtlinien auf der Grundlage verschiedener sich ändernder Kontextelemente wie Verhalten und Standort.

Schritt 6

Ihre Compliance und Risiken verwalten

Um die Vorschriften einzuhalten und Bedrohungen abzuschwächen, ist es unerlässlich, das Governance-, Risiko-und Compliance-Management (GRC-Management) in den Griff zu bekommen.

Zu oft verwalten Unternehmen die Einhaltung von Vorschriften manuell ... sage und schreibe in Tabellenkalkulationen. Außerdem geben sie in der Regel viel Geld für einzelne Sicherheitsprodukte aus, ohne wirklich zu wissen, wie sie diese integrieren und nutzen können. Das entspricht dem sprichwörtlichen Ansatz „Spaghetti an die Wand werfen, um zu sehen, was kleben bleibt“.

Es ist essenziell, sich einen Überblick über das Risiko zu verschaffen. Die meisten Bewertungen der Sicherheitslage werden nach einem Angriff vorgenommen und beziehen sich auf den Angriffsvektor. Dieser reaktive Ansatz in Verbindung mit zu vielen leeren Stellen in der IT ist ein großes Problem.

„Allzu oft verwalten Unternehmen die Einhaltung von Vorschriften manuell ... sage und schreibe in Tabellenkalkulationen.“

Zu den Vorteilen des Verständnisses von Compliance und Risiko gehören:

- Ersetzen Sie manuelle Aufgaben durch automatisierte Compliance-Prozesse.
- Schaffen Sie die Voraussetzungen für reibungslosere Audits.
- Verringern Sie proaktiv das Risiko.
- Passen Sie Ihr Budget an das tatsächliche Risiko an, ohne zu raten.
- Schaffen Sie einen strategischeren und zuverlässigeren Compliance-Rahmen.
- Erfüllen Sie die sich ständig ändernden Anforderungen ohne Entwickler.
- Setzen Sie Personalressourcen frei, um sich auf strategischere Aufgaben zu konzentrieren.

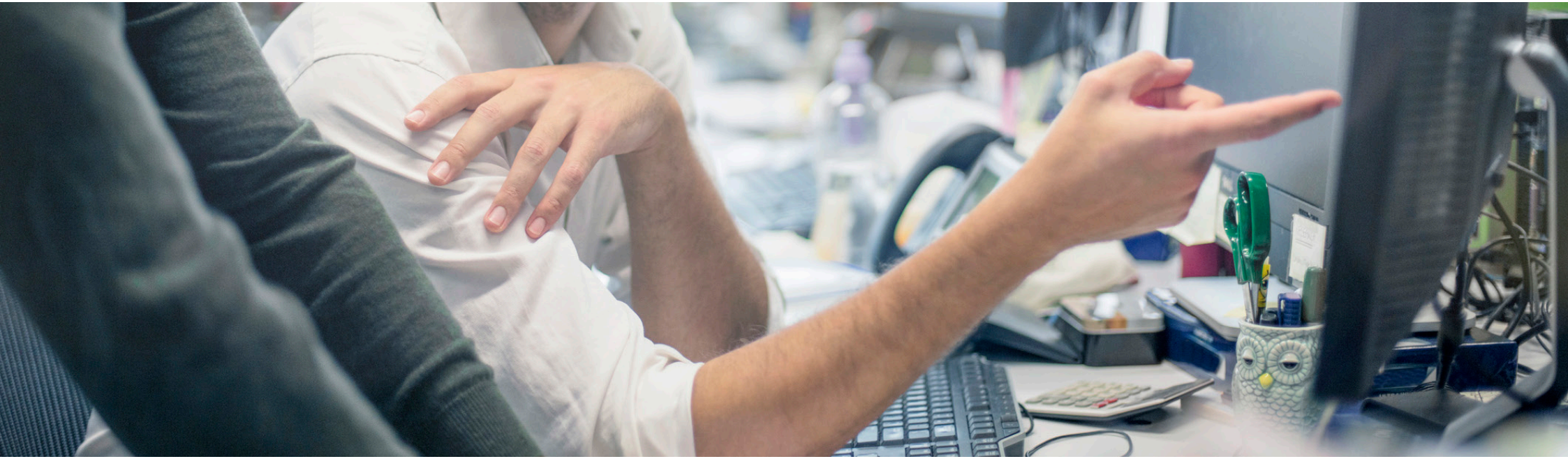
Funktionen, auf die Sie bei Ihrer Compliance-Lösung achten sollten:

- Eine leistungsstarke Lösung erleichtert die Einhaltung von Vorschriften durch schnelle und einfache Importe von Dokumenten zu M.A.P. mit Sicherheits- und Compliance-Kontrollen.
- Die Fähigkeit zum proaktiven Risikomanagement bedeutet, sich zur richtigen Zeit am richtigen Ort zu engagieren.
- Ersetzen Sie manuelle Aufgaben durch automatisierte, sich wiederholende Verwaltungsaktivitäten, damit Ihre Compliance reibungslos läuft.
- Das Management der Prozessreife bedeutet, dass Sie den Reifegrad Ihrer kritischen Sicherheitsprozesse und -kontrollen bewerten und je nach Priorität und Risiko optimieren können.
- Um effiziente und genaue Ergebnisse zu erzielen, suchen Sie nach einer Lösung, die Sie automatisch durch die Risikobewertung führt.

M.A.P. – Ihre Reise zur Cybersicherheit

Jeder dieser Schritte ist essenziell für die Verwaltung, Automatisierung und Priorisierung Ihrer Cybersicherheitsaktivitäten. Sie fühlen sich überfordert? Sie wissen nicht, wo Sie anfangen sollen? Es ist wichtig, dass Sie sich Partner suchen und Lösungen nutzen, die Sie auf Ihrem Weg unterstützen. Die richtigen Lösungen sind umfassend und integriert, um Ihre IT-Mitarbeiter zu entlasten. Optimale Lösungen sorgen auch für eine produktive, intuitive Benutzererfahrung, die die Integrität bewahrt, unabhängig davon, wo, wann und wie Ihre Mitarbeiter arbeiten.

Überall arbeiten. Überall sicher sein.



Über Ivanti

Ivanti macht den Everywhere Arbeitsplatz möglich. Im Everywhere Workplace nutzen Mitarbeiter unzählige Geräte für den Zugriff auf IT-Netzwerke, Anwendungen und Daten, um von überall aus produktiv arbeiten zu können. Die Ivanti-Automatisierungsplattform verbindet die branchenführenden Lösungen von Ivanti für Unified Endpoint Management, Zero Trust Security und Enterprise Service Management und bietet Unternehmen damit eine zentrale Plattform für die Selbstheilung und den Schutz von Geräten sowie die Selbstbedienung von Endbenutzern. Mehr als 40.000 Kunden, darunter 96 der Fortune 100, haben sich für Ivanti entschieden, um ihre IT-Ressourcen von der Cloud bis zu den Endgeräten zu entdecken, zu verwalten, zu sichern und zu warten und ihren Mitarbeitern hervorragende Endbenutzererfahrungen zu bieten, wo und wie auch immer sie arbeiten. Weitere Informationen find Sie auf ivanti.de

ivanti

ivanti.de
+49 (0)69 66 77 80 134
contact@ivanti.de

1. Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time
2. Ivanti: Patch Management Challenges. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges
3. Statista: Global average cost of a data breach 2021.
4. Statista: Average https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/ length of downtime after a ransomware attack 2021.
5. The biggest data breach fines, penalties, and settlements so far | CSO Online
6. 2021 Data Breach Investigations Report | Verizon
7. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges
8. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw?_ga=2.114312003.538830105.1638796042-898995573.1638285247
9. 2021 Data Breach Investigations Report | Verizon
10. Best Password Managers 2021 | The Strategist (nymag.com)
11. People and behaviors | Verizon