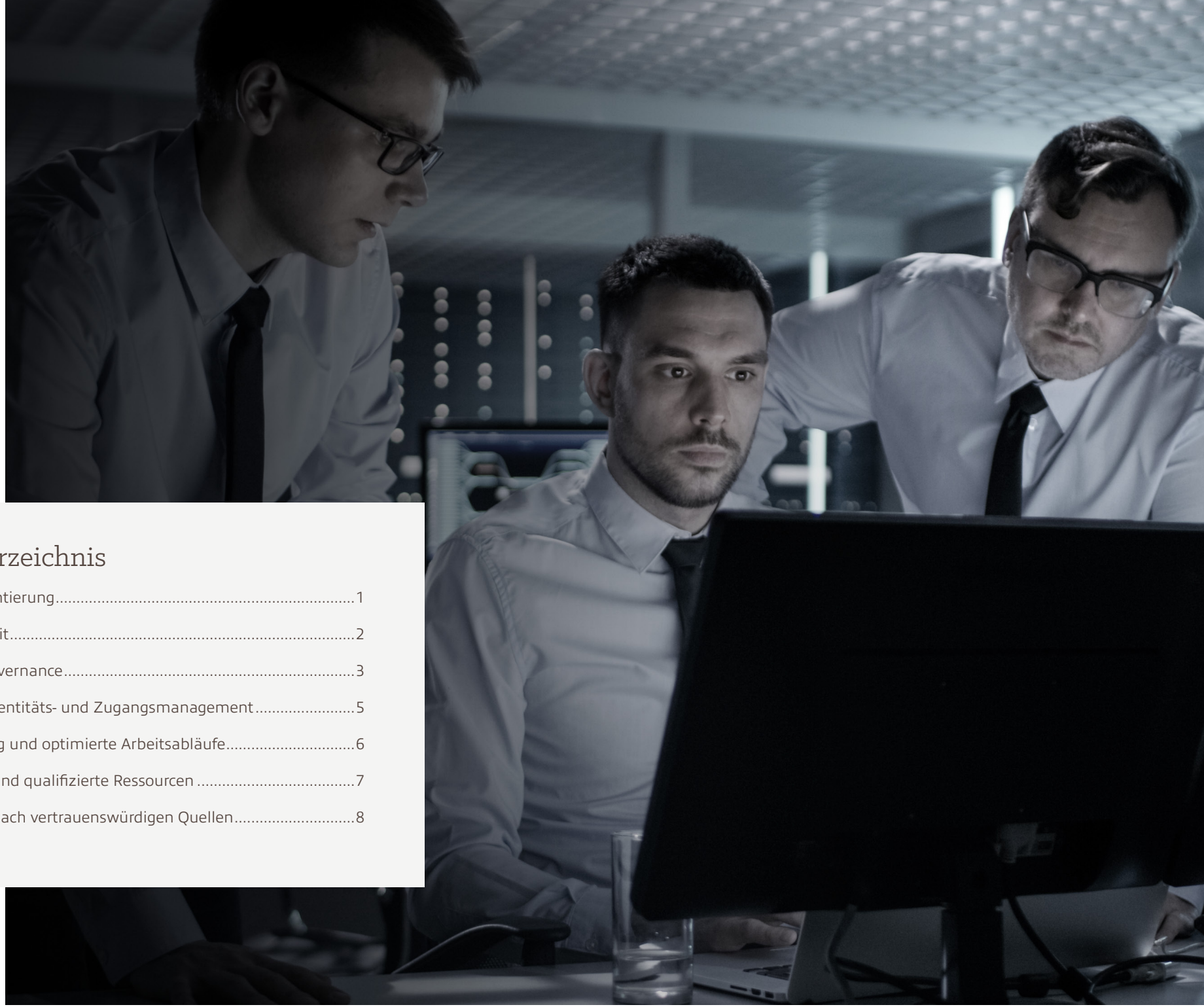
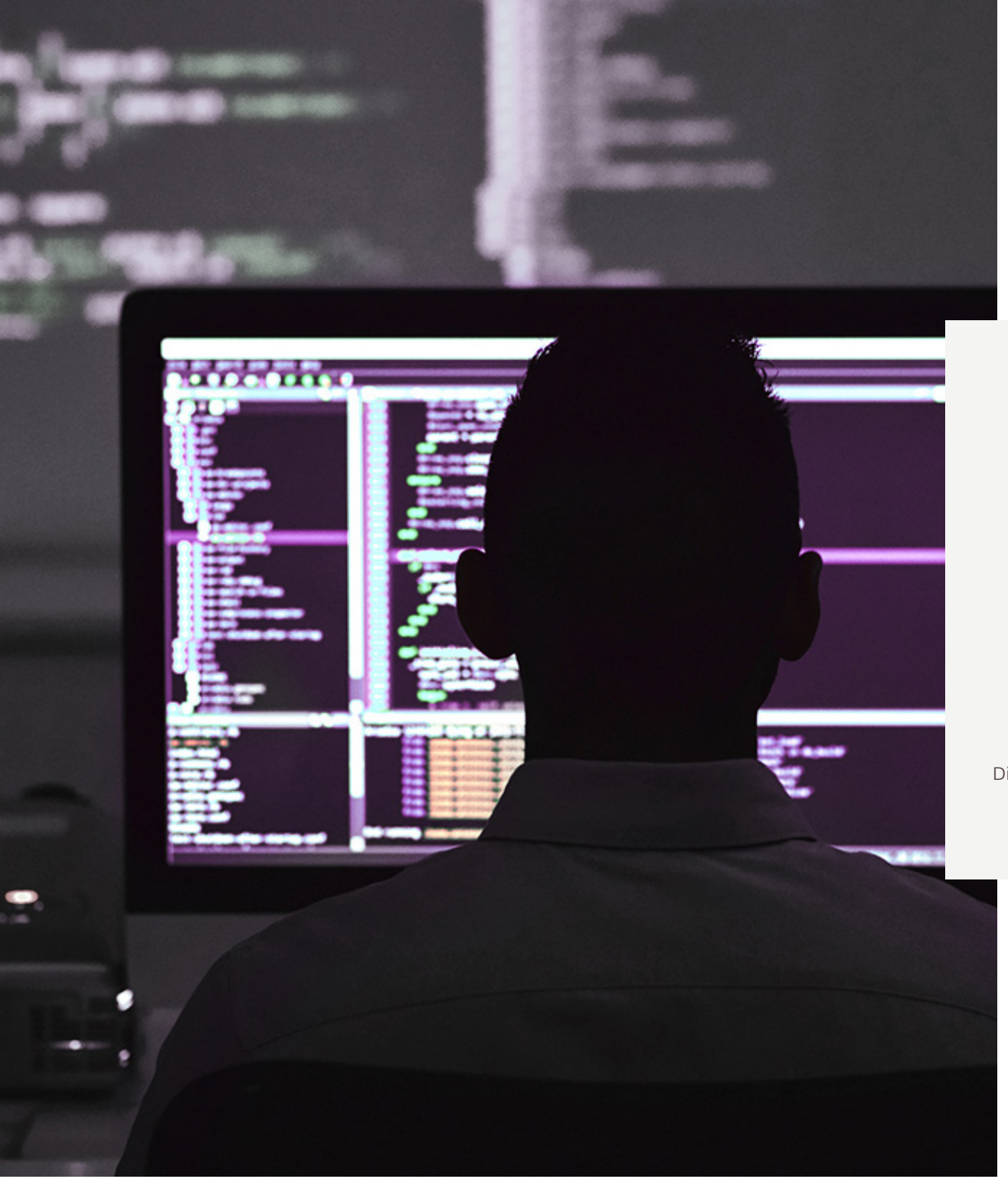
5 Attribute eines modernen Sicherheitsprogramms

Insight®



Inhaltsverzeichnis



Eine kurze Orientierung

Da Daten weiterhin exponentiell wachsen, gibt es auch eine Zunahme derjenigen, die von böswilligen Angriffen profitieren wollen. Für Unternehmen ist es heute mehr denn je entscheidend, ihre Sicherheitsstrategie zu evaluieren.

In der ersten Jahreshälfte 2021 wurden

1.767 Verstöße gemeldet,

was zu einer Exposition von **mehr als 18,8 Milliarden Datensätzen führte.**[1]

Die durchschnittlichen Kosten waren

1,07 Millionen US-Dollar höher

bei Verstößen, bei denen Remote-Arbeit ein Faktor für die Ursache des Verstoßes war.[2]

Die durchschnittlichen Gesamtkosten einer Datenschutzverletzung –

4,24 Millionen USD.[2]

In Zeiten wie diesen ist es hilfreich, einen Schritt zurückzumachen. Was sollte ein Sicherheitsprogramm leisten? Welche Ziele sind realistisch – und welche nicht? Wie sollten Sicherheitsinvestitionen getätigt und gemessen werden?

Wir glauben, dass es fünf Schlüsselattribute für ein erfolgreiches und modernisiertes Sicherheitsprogramm für Unternehmen jeder Art und Größe gibt.

[1] Risk Based Security. (August 2021). Schnellansicht des Berichts über Datenschutzverletzungen zur Jahresmitte 2021.
[2] Ponemon-Institute. (2021). 2021 Cost of a Data Breach Report. Gesponsert von IBM Security.

KAPITEL 1

Volle Sichtbarkeit

IT-Umgebungen werden immer größer. Wir beobachten ein Wachstum bei Datenvolumen, Geräteanzahl, Plattformen und Datenverkehr. Jede Erweiterung führt neue Bedrohungsvektoren und zusätzliche Herausforderungen in Bezug auf die Sichtbarkeit ein.

Fakten:	Berücksichtigung:
Die weltweite Datenerstellung **wird von 64,2 ZB im Jahr 2020 auf 180 ZB im Jahr 2025 anwachsen**.[3]	**Wie werden all diese Daten überwacht und gesichert,** insbesondere wenn sie sich in IT-Umgebungen bewegen?
Bis 2027 wird es mehr als 41 Milliarden Geräte für das Internet der Dinge (IoT) geben, gegenüber etwa 8 Milliarden im Jahr 2019.[4]	**Welches Maß an Sichtbarkeit können wir** angesichts dieses Wachstums bei vernetzten Geräten vernünftigerweise anstreben?
87 % der Unternehmen haben im vergangenen Jahr einen Multi-Cloud-Ansatz (unter Verwendung von mehr als einem Public Cloud Provider) eingeführt oder damit begonnen.[5]	**Wie machen Sie die Sichtbarkeit** mit mehreren Plattformen unterschiedlichen Typs in derselben IT-Umgebung einfach oder sogar möglich?

Dennoch ist es entscheidend, vollständige Sichtbarkeit zu haben. Wenn eine IT-Umgebung Qualitätstransparenz bietet und Aktivitäten überwacht werden, können viele Vorteile realisiert werden.

Zum einen können Angriffsversuche vereitelt und potenzielle Schäden gemildert werden. Ein erfolgreicher Angriff beginnt in der Regel mit der Ausnutzung einer Schwachstelle und durchdringt dann von diesem einzigen Ausgangspunkt aus mehrere Systeme. Wenn ein Verstoß früher erkannt wird, kann das Ausmaß des Schadens besser kontrolliert werden. Im Jahr 2019 dauerte es durchschnittlich 206 Tage, bis ein Verstoß erkannt wurde.[2] Stellen Sie sich die Anzahl der Datensätze, Systeme und Benutzer vor, die ein Cyberangreifer im Laufe von mehr als sechs Monaten erreichen könnte – es ist beunruhigend, darüber nachzudenken.

Sichtbarkeit, gepaart mit Überwachungs- und/oder Bedrohungsanalyse-Tools, trägt ebenfalls wesentlich zur Effektivität von Präventionsbemühungen bei. Das Benutzerverhalten ist in der Regel gemustert und bewegt sich auf logische und sich wiederholende Weise. Ungewöhnliche Aktivitäten oder Bewegungen können auf die Anwesenheit von böswilligen Akteuren hinweisen und IT-Sicherheitsmanagern dabei helfen, Angriffe zu verhindern und Zugriffs- oder Richtlinienänderungen vorzunehmen, die zuvor unbemerkte Sicherheitslücken schließen können.

[3] Statista. (Mai 2022). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025.
[4] Newman, S. (März 2020). The Internet of Things 2020. Business Insider Intelligence.
[5] Marketpulse Research by IDG Research Services. (Februar 2020). The State of IT Modernisation 2020. In Auftrag gegeben von Insight.

KAPITEL 2

Umfassende Governance

Viele denken vielleicht an Frameworks wie COBIT oder ITIL, wenn sie an Governance denken. Im High Level geht es bei Governance darum, wie IT-Entscheidungen an Geschäftszielen oder -anforderungen ausgerichtet werden. Governance sollte sich auch mit Eigentum und Verantwortlichkeit befassen – wer ist verantwortlich und wer sind die Stakeholder

Governance ist für die Sicherheit von entscheidender Bedeutung, da sie Organisationen dabei hilft:

- Sicherheitsziele zu definieren und auszurichten
- Sicherheitslösungen auszuwählen und zu validieren
- Schulungen, Richtlinien und andere Benutzersicherheitsprogramme zu organisieren
- Sicherheit in Gespräche über Plattformakzeptanz, Netzwerkarchitektur und andere Komponenten der IT-Strategie zu bringen
- Sicherheitslage durch definierte Rollen und Prozesse zu verbessern

Eine effektive Governance kann jedoch schwierig zu erreichen sein. In der jüngsten von Insight in Auftrag gegebenen IDG-Umfrage berichteten die Befragten, dass die größte Herausforderung bei der IT-Modernisierung darin besteht, neue Governance-Strategien und -Prozesse zur Unterstützung der IT-Modernisierung und der Cloud zu etablieren.[5]

Ein schwieriger Aspekt bei der Entwicklung einer effektiven Governance ist in der Tat die verstärkte Nutzung der Cloud. Unternehmen haben möglicherweise seit Jahren funktionierende Governance-Frameworks eingerichtet, die sich nur auf das Rechenzentrum und seinen klar definierten Perimeter bezogen.

Laut Flexera 2022 Bericht zum Stand der Cloud

89 % der Organisationen haben eine Multicloud-Strategie eingeführt

und

80 % wählen einen hybriden Cloud-Ansatz, indem Sie Public und Private Clouds kombinieren.[6]

Die Ausweitung traditioneller Governance auf die Cloud ist unerlässlich und erfordert Investitionen in Zeit und Ressourcen.

Dies hat Auswirkungen auf die Cloud-Sicherheit oder zumindest deren Wahrnehmung. Die IDG-Umfrage ergab, dass die Verwaltung der Public-Cloud-Sicherheit die größte Herausforderung bei der Optimierung der Cloud-Erfahrung und -Ergebnisse ist, dicht gefolgt von Governance- und Prozessherausforderungen.[5]

Durch die Einrichtung einer umfassenden Governance, einschließlich aller Plattformen, Rollen, Stakeholder usw., kann eine Organisation sicherstellen, dass ihre Sicherheitsabläufe robust, relevant und unterstützt bleiben.

[6] Flexera. (2022). 2022 State of the Cloud Report.

KAPITEL 3

Strategisches Identitäts- und Zugangsmanagement

Jedes System ohne böswillige Absicht hat oder sollte eine Identität und spezifische Zugriffsrechte haben. Da sich IT-Softwareumgebungen ausbreiten und Endgeräte immer mehr werden, wird das Identitäts- und Zugriffsmanagement zu einem zentralen Thema von Sicherheitsgesprächen.

Die meisten Organisationen haben Active Directory® und haben verschiedene Dienste von Drittanbietern verwendet. Dies führt zu mehreren Identitäten, Systemen und Lösungen – und zu einer Menge Komplikationen, insbesondere wenn manuelle Anstrengungen erforderlich sind, um alles zu verwalten.

Hier sind einige Überlegungen, die bei der Identitäts- und Zugriffsverwaltung angestellt werden sollten, wenn es um Sicherheit geht:

Denken Sie an die Daten.

Wie sensibel sind sie? Wer braucht wirklich Zugriff darauf? Wann und wie lange? Wer ist der erste Ansprechpartner, und ist dies die beste Option? Organisationen müssen möglicherweise als ersten Schritt eine Datenklassifizierungsinitiative verfolgen.

Denken Sie an Ihre Benutzer.

Haben Sie Benutzertypen festgelegt? Wann haben Sie zuletzt die Berechtigungen überprüft? Wie verifizieren Sie Identitäten und gewähren Zugriff? Von tiefgreifender Verteidigung bis Zero Trust gibt es viele praktikable Modelle.

Denken Sie an die Authentifizierung.

Passwörter sind schnell überholt. Welche Alternativen haben Sie in Betracht gezogen? Würden Mechanismen wie Biometrie für Ihr Unternehmen funktionieren? Wie könnten Sie in naher Zukunft von Ihrem aktuellen Authentifizierungsansatz zu einem sichereren wechseln?

Für ein strategisches und erfolgreiches Identitäts- und Zugriffsmanagement sollten Unternehmen alle Identitäten in einem einzigen Repository verwalten, die Implementierung einer Cloud Access Security Broker (CASB)-Lösung in Betracht ziehen und einen mehrschichtigen Sicherheitsansatz implementieren.

KAPITEL 4

Automatisierung und optimierte Arbeitsabläufe

Sicherheit hat keinen zweiten Versuch. Schwachstellen oder Lücken können jederzeit ausgenutzt werden. Menschliche Fehler, die zu erfolgreichen Angriffen führen, sind nicht zu verzeihen. In der Sicherheit sind Fehler kostspielig. Ironischerweise kann die Vermeidung solcher Kosten je nach Vorgehensweise auch ziemlich kostspielig sein.

Was meinen wir damit? Security Operations Centers (SOCs) müssen modernisiert werden, einschließlich Toolsets, Technologien, Prozesse/Methoden und Ressourcen. In der Umfrage „The State of IT Modernization 2020" gaben 57 % der Befragten an, dass die Aktualisierung der Sicherheitsinfrastruktur und -prozesse ein Haupthindernis für die Modernisierung der IT-Betriebsumgebung sei.[5] Aber wo interne Ressourcen knapp sind, müssen Unternehmen externe Partner finden, die dringend benötigte Automatisierungs- und andere Fachkenntnisse einbringen können.

Die Automatisierung innerhalb des SOC bringt klare Vorteile:

- Schnellere Erkennungs-, Reaktions- und Behebungsfunktionen
- Weniger Fehler aufgrund manueller Bemühungen
- Freigesetzte Sicherheitsressourcen für strategische Prioritäten
- Bessere Benutzererfahrung und -zufriedenheit

Einige Aufgaben eignen sich besonders gut für die Automatisierung. Nehmen Sie zum Beispiel das Reagieren auf Warnungen. In einer Studie von CRITICALSTART gaben 70 % der Befragten an, dass sie jeden Tag mehr als 10 Warnungen untersuchen, deren Untersuchung jeweils mehr als 10 Minuten dauert (Zahlen, die 45 % bzw. 64 % höher waren als im Vorjahr). Alarmmüdigkeit ist eine häufige Beschwerde in solchen IT-Umgebungen, die dazu führt, dass SOC-Experten Alarme ignorieren, mehr Personal einstellen, um die Last zu verteilen, oder sogar ihren Posten ganz verlassen.[7]

Durch die Reduzierung der Anzahl sich wiederholender Aufgaben, die vom Personal ausgeführt werden, und die Automatisierung gemeinsamer Sicherheitsprozesse können Unternehmen die Moral stärken, ein strategischeres SOC aufbauen und einfacher einen mehrschichtigen Sicherheitsansatz mit weniger Ressourcen verfolgen.

[7] CRITICALSTART. (2019). The Impact of Security Alert Overload.

KAPITEL 5

Effektive Tools und qualifizierte Ressourcen

Ohne die richtigen Tools, Technologien und Ressourcen kann ein Unternehmen nur begrenzt viel erreichen. Das entscheidende Wort ist „richtig“ Ein Bericht des Ponemon Institute ergab, dass Unternehmen durchschnittlich 47 verschiedene Cybersicherheitslösungen und -technologien einsetzen.[8] Derselbe Bericht stellt fest, dass mehr als die Hälfte (53 %) der IT-Experten nicht wissen, wie gut die von ihnen bereitgestellten Cybersicherheitstools funktionieren, und nur 39 % sagen, dass sie den vollen Wert aus ihren Sicherheitsinvestitionen ziehen.

Was ist das Problem? Es gibt mehrere:

- Die Zeit oder das Fachwissen zu haben, um fundierte Entscheidungen in Bezug auf Sicherheitsprodukte oder -plattformen zu treffen
- Verstehen der Fähigkeiten, die zum Bereitstellen, Annehmen, Integrieren, Anpassen und Optimieren von Sicherheitsinvestitionen erforderlich sind
- Komplexe IT-Softwareumgebungen (durch schnelles Wachstum, M&A-Aktivitäten etc.) mit unzähligen Angriffsvektoren
- IT-Investitionen an Budgets auszurichten, was manchmal zu unglücklichen Kompromissen führt
- Erwerb von Punktlösungen, die jeweils einen begrenzten Spielraum bieten und zur Tool-Ermüdung beitragen
- Wichtige Sicherheitstalente zu finden und zu binden

IT-Direktoren müssen ihre Risikolage und ihre Fähigkeiten zur Reaktion auf Bedrohungen ständig neu bewerten und gleichzeitig die Vorteile der neuesten Sicherheitsangebote nutzen. Durch eine enge Abstimmung mit den Geschäfts- und Fachbereichsleitern können IT-Organisationen auch die notwendige Akzeptanz sicherstellen, um eine sicherheitsbewusste Organisation zu entwickeln und das Auftreten von Schatten-IT und anderen riskanten Verhaltensweisen zu minimieren.

Wie gehen Sie mit diesen Bedenken um und treiben sinnvolle Verbesserungen in Ihren Sicherheitsabläufen voran?

[8] Ponemon Institute. (2019). The Cybersecurity Illusion: The Emperor Has No Clothes. Gesponsert von AttackIQ.

Suchen Sie nach vertrauenswürdigen Quellen

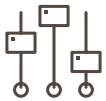
Insight hilft Unternehmen wie Ihrem, ihre Sicherheitsumgebung zu bewerten, eine umsetzbare Roadmap zu entwickeln, die optimalen Lösungen zu implementieren und ein erstklassiges SOC zu verwalten, das alle fünf hier beschriebenen Attribute aufweist. Unsere Prämisse ist, dass Sicherheit nicht nur ein Technologieproblem, sondern eine geschäftliche Priorität ist – wir kombinieren technische und beratende Erfahrung und Wissen, um Ihr gesamtes Sicherheitsprogramm zu erweitern.

Eine Möglichkeit, die wir liefern, ist Microsoft® Sentinel™, eine Cloud-native Security Information and Event Management (SIEM) und Security Orchestration and Automated Response (SOAR)-Lösung, die Sicherheitsdaten im gesamten hybriden Unternehmen sammelt und die Leistungsfähigkeit der künstlichen Intelligenz (KI) nutzt, um Bedrohungen schnell zu identifizieren und zu untersuchen.

Warum Insight und Microsoft Sentinel?

Maximieren Sie die Vorteile und Fähigkeiten Ihrer Sicherheitsinvestition.

Bessere Abstimmung der Sicherheitsbemühungen mit den Geschäftszielen



Verbesserte Sicherheit, Transparenz und Kontrolle Ihrer gesamten IT-Umgebung

Beschleunigen und automatisieren Sie die Suche und Erkennung von Cyberbedrohungen.

Übertragen Sie die Aufgabe der Überwachung Ihres Netzwerks, Ihrer Systeme, Anwendungen und Daten.

Reduzieren Sie Risiken und machen Sie sicherheitsbezogene Kosten vorhersehbarer.

Über Insight

Mehr als 20 Jahre der Lieferung/Bereitstellung von Support Services

PCI DSS-konform, SOC 2 Type II-zertifiziert, ISO 27000-zertifiziert und Mitglied von TSANet und TSIA

Ein führender Microsoft-Partner mit **18 Gold- und Silber-Kompetenzen**

Gold Microsoft Partner Microsoft | Azure Expert MSP

Ein Azure-Expert Managed Services Provider (MSP) und g**rößter Azure-Partner**

Microsoft Security 20/20 Award-Gewinner für die Kategorie Azure Security Deployment Partner of the Year

Was sagt Microsoft?

Ann Johnson, Corporate Vice President of Cybersecurity Solutions bei Microsoft, sagte: „Durch die Kombination unseres Microsoft-Sicherheitsportfolios mit den Sicherheitsdiensten von Insight ermöglichen wir unseren Kunden, ihre Sicherheitsabläufe zu modernisieren. Cybersicherheit ist komplex, muss aber nicht kompliziert sein. Die Weiterentwicklung unserer Sicherheitsbeziehung mit Insight hilft Unternehmen, ihre Sicherheitsabläufe zu vereinfachen und mit ihrem Wachstum zu skalieren."

Über Microsoft Sentinel

- Schnell und relativ einfach bereitzustellen, Neuinvestition oder per Protokollumleitung
- Flexibel und skalierbar, ermöglicht dynamische Anpassungen an Workloads oder Compliance
- Kostengünstig, ohne Vorabkosten oder Hardwareanforderungen
- Von führenden Unternehmen der IT- und Sicherheitsbranche entwickelt und ständig verbessert
- Nutzt die neuesten, hochmodernen KI- und maschinellen Lernfunktionen

Erwerben Sie die Tools und das Fachwissen, die Sie benötigen, um alle fünf in diesem E-Book beschriebenen Attribute zu erfüllen. Beginnen Sie noch heute mit Insight und Microsoft Sentinel.

Kontaktieren Sie uns

at.insight.com

MKT6270_AT