Checkliste für die Exposure Management-Strategie

Das Exposure Management kombiniert wirkungsvoll verschiedene Funktionen, in die viele Unternehmen bereits investieren. Daher sind Sie möglicherweise in Ihrem Exposure Management-Prozess bereits weiter fortgeschritten, als Ihnen bewusst ist.

Diese Checkliste bietet eine strukturierte Übersicht über die Produktkategorien, die im Exposure Management eine Rolle spielen, sowie deren zentrale Funktionen. Sie ist in vier Bereiche unterteilt – Sichtbarkeit, Priorisierung, Validierung und Behebung – und unterstützt Sie dabei, die relevanten Funktionen Ihrer bestehenden Cybersicherheits-Technologie zu erfassen und mögliche Lücken zu identifizieren.

Viele der aufgeführten Produkttypen fallen in mehrere Kategorien, was in den jeweiligen Einträgen entsprechend gekennzeichnet ist.

Sichtbarkeit

Ein einziger Blindspot kann einem Cyberangreifer den Zugang zu Ihrer IT-Umgebung ermöglichen. Die Technologien in diesem Abschnitt bieten einen Einblick in alle Cyber-Assets, Exposures und andere Elemente, die Ihre Angriffsfläche bilden. Beachten Sie, dass Sie nicht jede in diesem Abschnitt aufgeführte Technologie implementieren müssen. Einige Technologien bieten ähnliche Funktionen, während andere für Ihre Umgebung möglicherweise nicht relevant sind. Entscheidend ist, die optimale Kombination zu wählen, die Ihnen eine lückenlose Sicht auf Ihre Angriffsfläche verschafft.

IT Asset Discovery

Sichtbarkeit	**X**
Priorisierung	
Validierung	
Abhilfemaßnahmen	

Diese Tools identifizieren und inventarisieren automatisch Hardware- und Software-Assets innerhalb der IT-Umgebung eines Unternehmens. Allerdings können sie bestimmte Asset-Typen nicht erfassen und sind nicht darauf ausgelegt, Exposures zu erkennen. Daher sind zusätzliche Tools erforderlich, um eine umfassende Sicht auf die Angriffsoberfläche zu gewährleisten.

Unified Endpoint Management (UEM)

Sichtbarkeit	**X**
Priorisierung	
Validierung	
Abhilfemaßnahmen	**X**

UEM-Tools helfen IT-Teams, einen umfassenden Überblick über ihre Endgeräteumgebung – Desktops, Laptops, mobile Geräte und andere mit dem Internet verbundene Geräte – zu gewinnen und jedes Endgerät zu verwalten, zu konfigurieren und zu sichern.

Mobile Device Management (MDM)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

MDM-Tools (in diesem Fall die Abkürzung für Mobile Device Management) sind UEM-Tools, die auf die Erkennung und Verwaltung von mobilen Geräten wie Smartphones und Tablets spezialisiert sind.

Modern Device Management (MDM)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

Diese Art von MDM-Tool (in diesem Fall die Abkürzung für Modern Device Management) ermöglicht Ihnen Remote-Überwachung, -Bereitstellung, -Patching und -Sicherung einer breiteren Palette von angeschlossenen Netzwerkgeräten als die andere Art von MDM-Tool, einschließlich, aber nicht beschränkt auf Desktops, IoT-Sensoren, Wearables (z. B. Smartwatches), medizinische Geräte und Industriemaschinen.

Network Discovery

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

Diese Softwarelösungen erkennen und erfassen automatisch Hardware, Software und virtuelle Ressourcen in einem Netzwerk. Sie spielen eine zentrale Rolle bei der Erstellung eines vollständigen Überblicks über die Netzwerkinfrastruktur.

Netzwerk-Schwachstellen-Scanner

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

Netzwerk-Schwachstellen-Scanner erkennen und bewerten automatisch Sicherheitslücken in Netzwerkgeräten und Systemen und helfen Unternehmen dabei, potenzielle Risiken zu identifizieren.

IoT-Sicherheitstools (Internet der Dinge)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

Obwohl es keinen branchenüblichen Namen oder eine Definition für Tools gibt, die IoT-Assets und -Exposures aufdecken, gibt es eine Reihe solcher Tools. Eine schnelle Online-Suche nach „IoT-Sicherheitstools“ sollte eine Reihe von Optionen aufzeigen.

Schutzplattformen für cyber-physische Systeme (CPS)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

CPS-Schutzplattformen sind darauf ausgelegt, cyber-physische Systeme zu erkennen, zu kategorisieren, zu erfassen und zu schützen. Dazu gehören industrielle Kontrollsysteme (ICS) und intelligente Gebäudelösungen, die physische und rechnerische Komponenten integrieren.

Cloud Security Posture Management (CSPM)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

Unternehmen mit einer umfangreichen Cloud-Infrastruktur können CSPM-Tools nutzen, um Transparenz und Kontrolle über ihre Cloud-Umgebungen sicherzustellen. Diese Lösungen erfassen und katalogisieren Cloud-Assets in Private-, Public-, Hybrid- sowie Multi-Cloud-Umgebungen und überwachen sie kontinuierlich anhand von Sicherheits- und Compliance-Frameworks, um Schwachstellen und Bedrohungen frühzeitig zu identifizieren.

Cloud Workload Protection Platform (CWPP)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

CWPP-Lösungen identifizieren und beheben automatisch Bedrohungen, Schwachstellen und Fehlkonfigurationen, die cloudbasierte Workloads – also Anwendungen und Programme in der Cloud – betreffen. Dabei schützen sie virtuelle Maschinen, Container und serverlose Funktionen gleichermaßen.

Cloud-Native Application Protection Platform (CNAPP)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

CNAPP-Lösungen vereinen die Funktionen von CSPM- und CWPP-Tools sowie weiterer cloudspezifischer Lösungen, wie beispielsweise Cloud Infrastructure Entitlement Management (CIEM)-Tools. Sie sind im Grunde eine umfassende Lösung für Cloud-Sicherheit.

External Attack Surface Management (EASM)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

Die „externe Angriffsfläche" – also alle mit dem Internet verbundenen Assets – wird häufig von Unternehmen, nicht aber von Angreifern übersehen. EASM-Tools identifizieren alle über das Internet auffindbaren Assets, einschließlich Domains, IP-Adressen und offene Ports, sowie die damit verbundenen Exposures, um Unternehmen eine Angreiferperspektive zu ermöglichen. Sie können auch dazu genutzt werden, mit dem Internet verbundene Assets und Exposures von Drittparteien, mit denen Ihr Unternehmen in Verbindung steht – wie Lieferanten oder potenzielle Übernahmekandidaten – auf nicht-invasive Weise zu identifizieren.

Digital Risk Protection Services (DRPS)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

DRPS-Lösungen identifizieren digitale Risiken, die mit kompromittierten Unternehmens-Assets verbunden sind – auch wenn diese nicht zu den klassischen IT-Assets zählen. Dennoch können sie die Marke, die Reputation oder die Sicherheit eines Unternehmens beeinträchtigen, etwa durch kompromittierte Domains, Zugangsdaten, geistiges Eigentum oder Kreditkartendaten. Diese Lösungen bieten Überwachungsfunktionen für Exposures im Open Web, Deep Web, Dark Web und in sozialen Medien sowie Abhilfemaßnahmen zur Behebung dieser Exposures.

Cyber Asset Attack Surface Management (CAASM)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

CAASM-Tools aggregieren Asset- und Exposure-Daten aus bestehenden Asset-Management-Tools- und Sicherheitstools mithilfe von API-Integrationen (CAASM-Tools bieten keine nativen Scanfunktionen). Sie korrelieren diese Daten, um ein vollständiges Bild der Assets und Exposures eines Unternehmens zu erstellen.

SaaS Security Posture Management (SSPM)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

Durch kontinuierliches Scannen und Bewerten der Sicherheitseinstellungen und -konfigurationen von Software-as-a-Service (SaaS)-Anwendungen können SSPM-Tools potenzielle Schwachstellen und Fehlkonfigurationen erkennen. Außerdem setzen sie automatische Abhilfemaßnahmen ein, um Sicherheitsprobleme zu beheben und Best Practices umzusetzen.

Static Application Security Testing (SAST)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

SAST-Tools analysieren den Code auf Sicherheitslücken, ohne ihn auszuführen. Sie werden zu Beginn des Softwareentwicklungszyklus (SDLC) eingesetzt, da sie keine funktionierende Anwendung erfordern.

Dynamic Application Security Testing (DAST)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

DAST-Tools analysieren laufende Anwendungen, um Schwachstellen und Sicherheitslücken zu ermitteln. Dynamische Tests zur Anwendungssicherheit werden typischerweise während der Testphase des Softwareentwicklungszyklus (SDLC) oder sogar in Produktionsumgebungen durchgeführt, um sicherzustellen, dass Anwendungen unter realen Betriebsbedingungen sicher sind.

Mobile Application Security Testing (MAST)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

MAST-Tools kombinieren statische Analyse, dynamische Analyse und Penetrationstests, um Schwachstellen in mobilen Anwendungen auf Plattformen wie Android und iOS zu identifizieren.

Software Composition Analysis (SCA)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

SCA-Tools identifizieren Open-Source-Komponenten in einer Codebasis und gleichen diese Komponenten dann mit Datenbanken für bekannte Schwachstellen ab, um Sicherheitsprobleme oder bekannte Exploits zu finden.

Identity and Access Management (IAM)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

Der Hauptzweck von IAM-Tools besteht darin, Benutzeridentitäten sicher zu verwalten und den Zugriff auf geschäftskritische Informationen, Anwendungen und Netzwerke zu kontrollieren. Aus Sicht des Exposure Managements tragen IAM-Tools dazu bei, ein klares Bild der identitätsbasierten Angriffsfläche eines Unternehmens zu zeichnen. Sie speichern Identitäts- und Zugriffsdaten wie Benutzerprofile, Zugangsdaten, Rollen und Berechtigungen. Einige Lösungen erfassen zudem Risikodaten zu Anmeldeversuchen, Zugriffsmustern und verdächtigen Aktivitäten.

Identity Provider (IdP)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

IdP ist eine Komponente von IAM. IdP-Lösungen konzentrieren sich in erster Linie auf die Überprüfung von Benutzeridentitäten und die Bereitstellung von Authentifizierungsdiensten. In Fällen, in denen eine umfassende IAM-Lösung nicht verfügbar oder nicht realisierbar ist, kann eine IdP-Lösung eingesetzt werden, um Transparenz über die Identitäts-Angriffsfläche eines Unternehmens zu gewährleisten.

Data Loss Prevention (DLP)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	

DLP-Tools identifizieren sensible Daten, die geschützt werden müssen, wie personenbezogene Daten, Finanzdaten oder geistiges Eigentum. Sie überwachen, wie diese Daten genutzt und abgerufen werden – sowohl innerhalb als auch außerhalb des Unternehmens – und können Warnmeldungen und Reports erstellen, wenn verdächtige Aktivitäten erkannt werden.

Data Security Posture Management (DSPM)

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

Ein DSPM-Produkt kann ermitteln, wo sich Ihre Daten befinden – sei es in Datenbanken, Cloud-Services oder anderen Speicherorten – und die damit verbundenen Sicherheitsrisiken bewerten, etwa Schwachstellen, Fehlkonfigurationen oder unzureichende Zugriffskontrollen. Zudem bieten diese Lösungen Empfehlungen und Tools zur Behebung von Sicherheitsproblemen und zur Verbesserung der gesamten Datensicherheit.

API-Schutzlösungen

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X*

API-Schutzlösungen erkennen und inventarisieren die Anwendungsprogrammierschnittstellen (APIs) eines Unternehmens. Sie enthalten auch Listen mit empfohlenen Abhilfemaßnahmen für API-Exposures.

*API-Schutzlösungen bieten Anleitungen zur Behebung von Sicherheitsproblemen, führen jedoch keine automatischen Maßnahmen durch. Stattdessen geben sie Empfehlungen für manuelle Schritte, die Sie ergreifen können.

API Security Posture Tools

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X*

API Security Posture Tools identifizieren und erfassen automatisch alle APIs in einer Umgebung, einschließlich nicht dokumentierter oder sogenannter Schatten-APIs. Sie nutzen sowohl statische als auch dynamische Schwachstellenscans, um Schwachstellen und andere Probleme aufzudecken. Anschließend geben sie Empfehlungen zur Behebung dieser Schwachstellen, damit Unternehmen ihre API-Sicherheit gezielt verbessern können.

*API Security Posture Tools bieten Anleitungen zur Behebung von Sicherheitsproblemen, führen jedoch keine automatischen Maßnahmen durch. Stattdessen geben sie Empfehlungen für manuelle Schritte, die Sie ergreifen können.

Priorisierung

Priorisierungstools nutzen die von den Sichtbarkeitstools erfassten Asset- und Exposure-Daten und machen sie für Ihr Unternehmen nutzbar. Zunächst benötigen Sie einen vollständigen Überblick – ganz nach dem Motto: „Man kann nur schützen, was man sieht." Doch erst Priorisierungstools helfen Ihnen dabei, die richtigen Maßnahmen abzuleiten und zu entscheiden, welche Risiken zuerst angegangen werden sollten.

Beachten Sie, dass einige Sichtbarkeitstools behaupten, Priorisierung zu bieten – und das ist bis zu einem gewissen Grad korrekt. Viele dieser Tools ermöglichen es, die Behebung von Exposures innerhalb ihres eigenen, begrenzten Bereichs zu priorisieren, jedoch nicht alle Exposures, denen ein Unternehmen über seine gesamte Angriffsfläche hinweg ausgesetzt ist. So priorisieren EASM-Tools beispielsweise ausschließlich Exposures, die mit extern erreichbaren Assets verbunden sind.

Exposure Assessment Platform (EAP)

Sichtbarkeit	X
Priorisierung	X
Validierung	
Abhilfemaßnahmen	X

EAPs sind eine neue Produktkategorie im Bereich des Exposure Managements. Während dieses Konzept auf der Integration bereits existierender Technologien basiert, wurden EAPs gezielt als Plattformen entwickelt, die mehrere Exposure Management-Funktionen vereinen. Diese Plattformen bieten eine ganzheitliche Sicht auf sämtliche Assets und Exposures über die gesamte Angriffsoberfläche hinweg – unabhängig davon, ob diese durch eigene Scans oder Drittanbieter-Tools erfasst wurden. Zudem ermöglichen sie eine priorisierte Maßnahmenplanung zur Behebung von Exposures, wobei sowohl die Kritikalität der betroffenen Assets als auch der geschäftliche Kontext berücksichtigt werden. Ferner erlauben sie die Orchestrierung dieser Aktivitäten oder deren direkte Ausführung.

Risk-Based Vulnerability Management (RBVM)

Sichtbarkeit	X
Priorisierung	X
Validierung	
Abhilfemaßnahmen	

RBVM-Tools priorisieren Schwachstellen basierend auf ihrem Risiko für das Unternehmen. Sie aggregieren die Ergebnisse von Scannern und anderen Sicherheitstools, konsolidieren diese und gleichen sie mit relevanten Datenpunkten wie Threat Intelligence (Bedrohungsdaten) und der Kritikalität der betroffenen Assets ab. So unterstützen sie Unternehmen dabei, fundierte Maßnahmen zur Risikominimierung zu entwickeln. Einige dieser Tools verfügen zudem über Funktionen zur Erkennung von Exposures.

Application Security Posture Management (ASPM)

Sichtbarkeit	X
Priorisierung	X
Validierung	
Abhilfemaßnahmen	

ASPM-Tools sind im Wesentlichen das Pendant zu RBVM-Tools im Bereich der Anwendungssicherheit. Sie erfassen Asset- und Exposure-Daten aus verschiedenen Anwendungsscannern – wie SAST, DAST, SCA und Container-Scannern – und verknüpfen diese mit Threat Intelligence (Bedrohungsdaten) sowie mit der Kritikalität der betroffenen Assets. Auf dieser Grundlage helfen sie, Risiken gezielt zu priorisieren und geeignete Maßnahmen zur Behebung festzulegen. Einige Anbieter kombinieren RBVM- und ASPM-Funktionen, um Unternehmen eine ganzheitliche Sicht auf ihr Cyber-Risiko über die gesamte Angriffsfläche hinweg zu ermöglichen. Zudem integrieren manche Lösungen native Exposure-Scanning-Funktionen, etwa SAST, direkt in ihre ASPM-Tools.

Threat Intelligence (Bedrohungsdaten)

Sichtbarkeit	
Priorisierung	X
Validierung	
Abhilfemaßnahmen	

Threat Intelligence-Lösungen liefern Informationen über die Bedrohungslandschaft im Allgemeinen. Im Gegensatz zu den anderen in diesem Dokument aufgeführten Priorisierungslösungen arbeiten sie nicht mit Daten, die speziell auf die Umgebung eines Unternehmens zugeschnitten sind. Stattdessen bieten sie eine globale Perspektive, damit Sicherheitsteams potenzielle Bedrohungen proaktiv priorisieren können – noch bevor diese in der eigenen IT-Umgebung identifiziert werden.

Validierung

Validierung dient als Kontrollinstanz für die Priorisierung. Durch die Überprüfung, wie potenzielle Angreifer eine identifizierte Schwachstelle tatsächlich ausnutzen könnten und wie Überwachungs- sowie Kontrollsysteme darauf reagieren würden, hilft die Validierung einem Unternehmen zu bestimmen, welche Exposures tatsächlich behoben werden müssen, um das Risiko auf einem mit der Risikobereitschaft abgestimmten Niveau zu halten.

Beachten Sie, dass die Validierung mithilfe von Lösungen – allgemein bekannt als AEV-Technologien (Adversarial Exposure Validation) – oder über manuelle Prozesse erfolgen kann, die entweder an einen Anbieter ausgelagert oder von internen Teams durchgeführt werden. Am besten ist es, verschiedene Validierungsmethoden zu kombinieren, um möglichst umfassende Ergebnisse zu erhalten.

Unabhängig davon, welchen Validierungsansatz Sie wählen, gilt es als Best Practice, die Validierung von einer anderen Instanz durchführen zu lassen als die Priorisierung. So lassen sich objektive und unverzerrte Ergebnisse gewährleisten. Man kann die Validierung mit einer Zweitmeinung vor einer Operation vergleichen.

Attack Path Analysis (APA)

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

APA-Tools visualisieren die Wege, die Angreifer nutzen könnten, um sich innerhalb der IT-Umgebung eines Unternehmens zu bewegen. Sie ermöglichen Sicherheitsteams, potenzielle Angriffswege zu identifizieren, die Cyberkriminelle verfolgen könnten, um einen Angriff auszuführen. Zudem zeigen sie auf, welche Exposures nicht ausnutzbar sind und somit ins Leere laufen.

Breach and Attack Simulation (BAS)

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

BAS-Tools validieren kontinuierlich die Exposures eines Unternehmens, indem sie ein breites Spektrum von Cyberangriffen simulieren. Im Gegensatz zu manuellem Red Teaming und Pen-Tests bietet die BAS-Software einen vollständig automatisierten Ansatz zur Validierung.

Red Teaming

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

Red Teaming bezeichnet eine Methode, bei der eine Gruppe ethischer Hacker – das sogenannte Red Team – reale Cyberangriffe simuliert, um die Abwehrmechanismen eines Unternehmens zu testen, Schwachstellen aufzudecken und die Wirksamkeit der Sicherheitsmaßnahmen zu bewerten.

Continuous Automated Red Teaming (CART)

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

Während beim Red Teaming ethische Hacker Cyberangriffe manuell simulieren, automatisieren CART-Tools diese simulierten Angriffe und bieten häufige Echtzeittests, die skalierbarer und kostengünstiger sein können. Während BAS-Tools testen, wie gut Sicherheitskontrollen mit bekannten Angriffsmethoden umgehen können, konzentrieren sich CART-Tools auf das Auffinden und sichere Ausnutzen von Schwachstellen, um festzustellen, ob und wie ein Angreifer die Verteidigungsmaßnahmen eines Unternehmens durchbrechen könnte.

Penetrationstests

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

Ähnlich wie beim Red Teaming führen ethische Hacker beim Penetrationstest – oft als „Pen Testing“ abgekürzt – simulierte Angriffe auf die Systeme eines Unternehmens durch. Der Unterschied liegt darin, dass sich Penetrationstests speziell auf das Auffinden und Ausnutzen von Exposures konzentrieren, während Red Teaming die gesamte Sicherheitslage bewertet. Es ist außerdem ratsam, von Anbietern, Partnern und anderen Drittparteien Penetrationstestergebnisse anzufordern, da ihre Angriffsflächen ebenfalls Teil Ihrer eigenen Angriffsfläche sind.

Automatisierte Penetrationstests

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

Wie der Name schon sagt, führt automatisierte Software-Penetrationstests automatisch durch. Dadurch können Tests schneller und regelmäßiger erfolgen als mit manuellen Methoden.

Penetration Testing as a Service (PTaaS)

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

PTaaS ist ein cloudbasiertes Modell, bei dem Unternehmen auf Penetrationstests nach Bedarf zugreifen können. PTaaS-Angebote kombinieren sowohl automatisierte als auch manuelle Testverfahren. Und mit PTaaS- Anbietern, die den Testprozess verwalten, können Unternehmen regelmäßige Sicherheitsbewertungen durchführen, ohne ein eigenes Team von Sicherheitsexperten zu benötigen.

Bug Bounty

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

Einige Unternehmen motivieren ethische Hacker dazu, Schwachstellen in ihren Systemen, ihrer Software oder ihren Websites aufzudecken und verantwortungsbewusst zu melden - gegen Belohnungen oder Anerkennung. Treffend als „Bug Bounties“ bezeichnet.

Cyber-Range

Sichtbarkeit	
Priorisierung	
Validierung	X
Abhilfemaßnahmen	

Ein Cyber-Range ist eine virtuelle Umgebung, in der Unternehmen reale Cyberangriffe simulieren und in einer kontrollierten Sandbox-Situation die Reaktion auf Sicherheitsvorfälle üben können.

Abhilfemaßnahmen

Abhilfemaßnahmen bilden ist die letzte Phase des Exposure Management-Prozesses. Sobald Sie festgelegt haben, welche Exposures basierend auf Ihrer Risikobereitschaft behoben werden müssen, unterstützen Abhilfetools Sie bei der Behebung.

Patch Management

Sichtbarkeit	X
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

Patch Management-Lösungen wenden Updates oder Patches auf die Software an, um Schwachstellen zu beheben oder die Funktionalität zu verbessern. Einige enthalten auch Discovery-Funktionen, die Einblicke in Betriebssysteme und Anwendungen von Drittanbietern ermöglichen.

Konfigurationsmanagement

Sichtbarkeit	
Priorisierung	
Validierung	
Abhilfemaßnahmen	X

Konfigurationsmanagement-Tools automatisieren den Prozess der Pflege und Durchsetzung konsistenter Systemkonfigurationen. Durch einheitliche Systemkonfigurationen wird sichergestellt, dass alle Geräte und Systeme innerhalb einer IT-Umgebung gemäß von vordefinierten Sicherheitsrichtlinien und Best Practices eingerichtet sind und funktionieren.

Über Ivanti

Ivanti baut die Barrieren zwischen IT und Sicherheit ab, damit Everywhere Work erfolgreich ist. Ivanti hat die erste eigens entwickelte Technologieplattform für CIOs und CISOs geschaffen, die IT- und Sicherheitsteams umfassende Softwarelösungen bietet. Diese skalieren mit den Anforderungen ihrer Unternehmen, um die positiven digitalen Erfahrungen der Mitarbeitenden zu ermöglichen, zu sichern und zu verbessern. Die Ivanti-Plattform wird von Ivanti Neurons betrieben – einer intelligenten, Cloud-fähigen Hyper-Automatisierungsebene, die eine proaktive Fehlerbehebung ermöglicht, benutzerfreundliche Sicherheit im gesamten Unternehmen bietet und ein herausragendes Mitarbeitererlebnis schafft. Mehr als 35.000 Kunden, darunter 85 der Fortune-100-Unternehmen, haben sich für Ivanti entschieden, um die Herausforderungen mit den eigenen End-to-End-Lösungen zu meistern. Unser Ziel bei Ivanti ist, ein Umfeld zu schaffen, in dem alle Meinungen gehört, respektiert und geschätzt werden. Und wir setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten ein. Weitere Informationen finden Sie unter www.ivanti.com und folgen Sie @GoIvanti.

ivanti

Für weitere Informationen oder um Ivanti zu kontaktieren, besuchen Sie bitte ivanti.com.