IBM Security-Produkte: Intelligenz, Integration, Expertise

Ein umfassendes Framework für alle Systemumgebungen – mobil, cloudbasiert, sozial – bis hin zu derzeit noch unbekannten Weiterentwicklungen

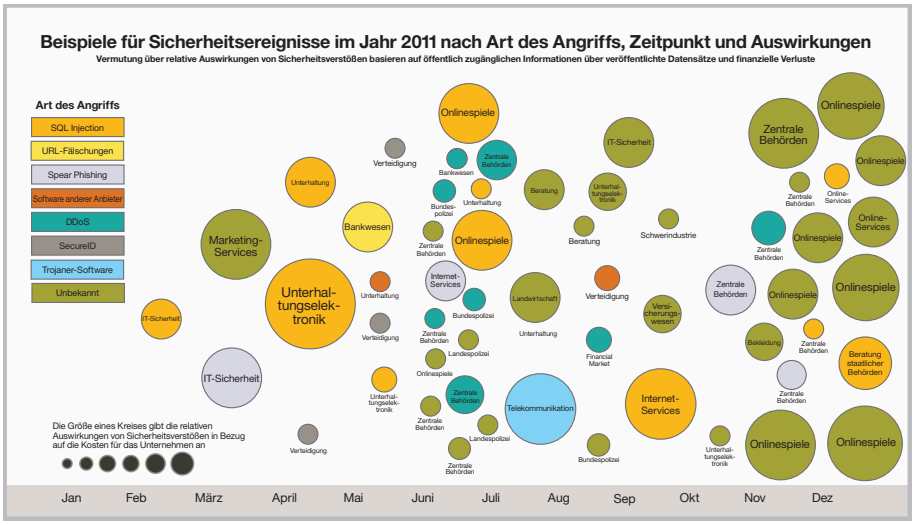
IBM

Inhalte

Eine vollständig vernetzte Geschäftswelt

Im vollständig vernetzten Geschäftsumfeld von heute wird ein vollkommen anderes Sicherheitskonzept für den Schutz des Unternehmens benötigt. Die enorme Zunahme digitaler geschäftlicher Informationen, auf die über virtualisierte cloudbasierte und soziale Plattformen zugegriffen wird und die dort gespeichert werden, die immer stärkere Instrumentierung und die Vielzahl an mobilen Geräten, die Teil des Endverbrauchergeschäfts sind, haben zu überaus komplexen IT-Umgebungen geführt – mit nahezu endlos vielen möglichen Angriffspunkten.

Die raffiniertesten Angreifer greifen inzwischen auf Advanced Persistent Threats (APTs) zurück, um gezielt Zugriff auf vertrauliche Geschäftsinformationen zu erhalten. Bei diesen Angriffen werden modernste Verfahren verwendet, sie können unbegrenzt lange dauern und sie sind äußerst gezielt. Die zunehmende Vielfalt der heutigen Sicherheitsbedrohungen hat dazu geführt, dass die Effektivität traditioneller IT-Schutzmaßnahmen abnimmt (z. B. Firewalls und Antivirus-Programme) und diese Kontrollen in vielen Fällen sogar vollständig umgangen werden. Es wird daher ein neues Konzept benötigt, bei dem Schutzmaßnahmen und Erkennung sowie moderne Technologie und ausgereifte Prozesse aufeinander abgestimmt sind.



Die Mitarbeiter in der Forschung und Entwicklung bei IBM X-Force bezeichneten 2011 als „das Jahr der Sicherheitsverstöße“, denn in diesem Jahr kam es zu sehr vielen schwerwiegenden und unterschiedlichen Sicherheitsangriffen.

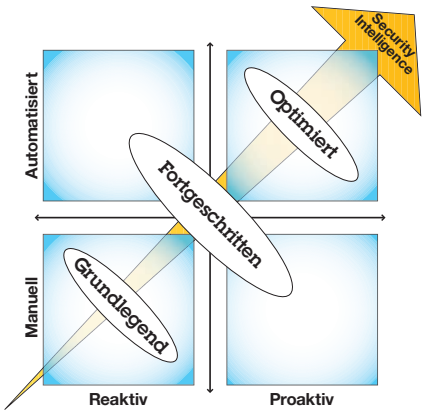
Security Intelligence für eine neue Welt

Nur die Unternehmen, die Lösungen zur Überwachung, Verknüpfung und Analyse der riesigen Mengen an Echtzeitereignissen eingeführt haben, die über eine umfassende, integrierte Sicherheitsinfrastruktur und über gut erforschte, externe Threat-Feeds generiert werden, sind in der Lage, kostengünstig ein extrem hohes Sicherheitsniveau zu gewährleisten. IBM® bezeichnet dies als *Security Intelligence*. Dieses Konzept bieten den Unternehmen neben dem Erkennen und Beseitigen von Sicherheitslücken, die andernfalls möglicherweise übersehen werden, folgende Vorteile:

- Umstellung von einer reaktiven Vorgehensweise auf ein proaktives Konzept, das besser auf die Geschäftsziele abgestimmt ist
- Schaffung der Grundlagen, um Initiativen für Innovationen weitaus schneller auf den Weg zu bringen
- Automatisierung von Compliancemaßnahmen
- Verringerung des Personalaufwands für Sicherheitsprozesse

Ein einzigartiges, umfassendes Konzept

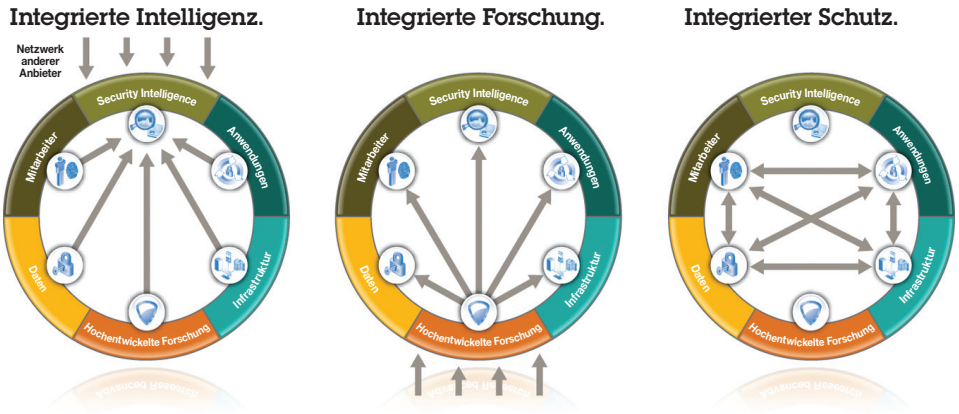
Mit IBM Produkten und Services sowie der übergreifenden Strategie, die auf den drei Grundprinzipien Intelligenz, Integration und Expertise basiert, kann eine echte Security Intelligence erreicht werden.



Durch die Umstellung von einem reaktiven und manuellen Ansatz auf einen proaktiven und automatisierten Ansatz erreichen Unternehmen ein höheres Sicherheitsniveau, das auf Security Intelligence basiert.

Intelligenz

Menschliche Intelligenz erfordert Know-how, Informationen und die Fähigkeit, diese Informationen analysieren zu können, um daraus Rückschlüsse zu ziehen. Im Bereich Unternehmenssicherheit bedeutet dies, dass Transparenz in relevanten Netzwerken und Infrastrukturen gegeben sein muss, Informationen über externe Sicherheitsbedrohungen vorliegen müssen und



Durch die Integration von sicherheitsspezifischen Informationen, Forschungsergebnissen von X-Force und zentralen Schutzfunktionen können die Diskrepanzen beseitigt werden, die durch unabhängige Einzelprodukte entstanden sind.

Funktionen für Echtzeitverknüpfungen und -analysen verfügbar sein müssen, um verdächtige Aktivitäten zu kennzeichnen und zu beheben. IBM Security bietet Folgendes:

- **Interne Transparenz:** IBM Security Intelligence-Lösungen analysieren Informationen aus Produkten und Services von IBM und anderen Herstellern in Echtzeit. Sie liefern umfassende Analysen und Erkenntnisse in allen vier Bereichen für Sicherheitsrisiken: Mitarbeiter, Daten, Anwendungen und Infrastruktur
- **Transparenz bei externen Sicherheitsbedrohungen:** Der IBM X-Force Threat Intelligence Feed liefert kritische Informationen aus einem der weltweit größten Repositorys mit Erkenntnissen über Sicherheitsbedrohungen und Sicherheitslücken. Grundlage hierfür ist die Überwachung von 13 Mrd. Sicherheitsereignissen in Echtzeit pro Tag. Diese Erkenntnisse können auf Verhaltensweisen im Zusammenhang mit Advanced Persistent Threats und einer Vielzahl von Angreifern hinweisen.
- **Genaue Analysen im Big Data-Zeitalter:** Mit IBM Security Intelligence-Lösungen können Sie bei Analysen und Abfragen unterschiedlicher Aktivitäten einzelne Datenelemente abfragen. Sie liefern Erkenntnisse über den Netzwerkzugriff an der Peripherie, externe Cloud-Services, mobile Geräte, zentrale Datenbankaktivitäten im Unternehmen und alle weiteren Aspekte.

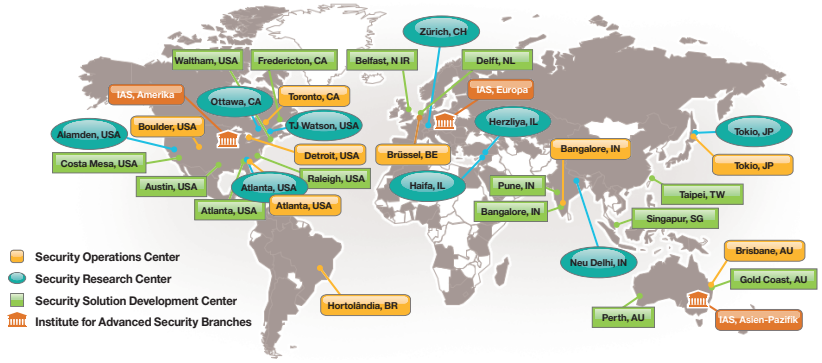
Integration

Durch die Integration des umfassenden IBM Produktportfolios mit sicherheitsspezifischen Informationen, Forschungsergebnissen von X-Force und zentralen Schutzfunktionen können Sie angreifbare Schwachstellen vermeiden, die sich aus der Verknüpfung voneinander unabhängiger Sicherheitsprodukte ergeben. Sie können damit die Implementierung einfacher gestalten, Datensilos im Hinblick auf die einfachere Erstellung von Complianceberichten vermeiden und eine bessere Security Intelligence gewährleisten, Komplexität reduzieren und die Kosten für den Erhalt eines hohen Sicherheitsniveaus senken. Weitere Funktionen für Kosteneinsparungen und eine höhere Sicherheit:

- Externe und interne Kontextinformationen zur Erkennung, Vorhersage und Beseitigung von Sicherheitslücken
- Automatische Geräte- und Software-Updates für ermittelte Sicherheitslücken
- Verknüpfung von Authentifizierung und Autorisierung mit verdächtigen Datenbankaktivitäten
- Automatisierte Maßnahmen zur Compliance und Risikoanalyse

Expertise

IBM betreibt mit über 5.500 Forschern, Entwicklern und Fachleuten, die in Sicherheitsinitiativen mitarbeiten, eine der weltweit größten Organisationen für Forschung, Entwicklung und Bereitstellung im Sicherheitsbereich. Hierzu gehören das mehrfach ausgezeichnete IBM X-Force Forschungs- und Entwicklungsteam (mit einer der branchenweit größten Datenbanken für Sicherheitslücken), 9 Security Operations Center, 10 IBM Security Research Center, 15 Security Solutions Development Labs und das Institute for Advanced Security mit Niederlassungen in den USA, in Europa und im asiatisch-pazifischen Raum. IBM überwacht derzeit für seine Kunden über 13 Mrd. Sicherheitsereignisse pro Tag in über

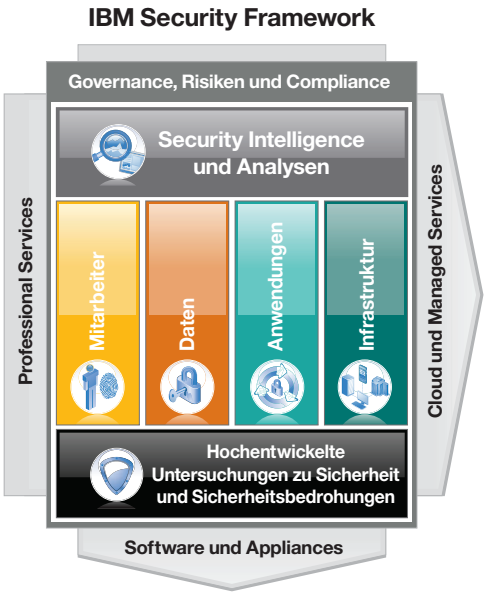


IBM arbeitet mit einem der weltweit umfassendsten Prozesse für Forschung, Entwicklung und Bereitstellung im Sicherheitsbereich.

130 Ländern. IBM verfügt über die Berater und das Know-how, um Unternehmen bei der Umstellung auf optimierte, integrierte Sicherheitskontrollen mit Security Intelligence zu unterstützen.

Produktportfolio

Das IBM Security Framework wurde so konzipiert, dass die richtigen Personen zum richtigen Zeitpunkt Zugriff auf die richtigen Ressourcen haben. Kritische Daten sind daher geschützt, wenn sie übertragen oder abgelegt werden, neue Sicherheitsbedrohungen werden identifiziert, um Sicherheitslücken vermeiden und beseitigen zu können, und alle IT-Ressourcen sind dauerhaft geschützt. Das integrierte Konzept zur Unternehmenssicherheit umfasst Systeme, Softwareprodukte und Managed Services. Es wird im Rahmen von technischen Services und von Services zur Risikoberatung und Implementierung bereitgestellt. Die zentrale Komponente ist jedoch das IBM Produktportfolio.



Das IBM Security Framework ist ein methodischer und effizienter Ansatz zur Bewältigung sicherheitsspezifischer Anforderungen und Herausforderungen im gesamten Unternehmen.

Security Intelligence und Analysen

Sicherheitsverstöße und Compliancerisiken vermeiden, erkennen und beseitigen.

Herausforderungen und Lösungen

IBM Security Intelligence-Produkte bieten Vorteile in folgender Hinsicht:

- **Erkennen hochentwickelter Sicherheitsbedrohungen:** Schützen Sie Ihr Unternehmen mit umfassender und präziser Security Intelligence
- **Einhalten gesetzlicher Bestimmungen:** Automatisieren Sie die Datensammlung und -berichte für Audits und Risikoanalysen
- **Erkennen von Sicherheitsbedrohungen und Betrugsfällen durch Insider:** Identifizieren und verstehen Sie verdächtige Benutzeraktivitäten im jeweiligen Kontext
- **Vorhersehen von Risiken für das Unternehmen:** Identifizieren und priorisieren Sie proaktiv Sicherheitslücken und Diskrepanzen
- **Konsolidieren von Datensilos:** Sammeln, verknüpfen und dokumentieren Sie Daten im Rahmen einer einzigen integrierten Lösung.

Produkte

Zur Produktfamilie mit integrierten Security Intelligence-Produkten basierend auf SIEM (Security Information and Event Management) und Log-Management der nächsten Generation gehören folgende Produkte:

- **IBM Security QRadar SIEM:** SIEM (Security Information and Event Management) mit Log-Management , Threat-Management und Compliance-Management, Verknüpfung fortschrittlicher Ereignis- und Netzwerkabläufe, integrierte Verhaltensanalysen und Erkennen von Unregelmäßigkeiten im Netzwerk
- **IBM Security QRadar Log Manager:** Sofort verwendbares Log-Management für Hunderte von Datenquellen, vorkonfigurierte Berichte und Dashboards, einfache Anpassung
- **IBM Security QRadar Risk Manager:** Überwachung und Prüfung von Sicherheitskonfigurationen, vorausschauende Modellierung und Simulation von Sicherheitsbedrohungen, erweiterte Visualisierung von Sicherheitsbedrohungen und Analyse der Auswirkungen

- **IBM Security QRadar Network Anomaly Detection:** Erkennen von Unregelmäßigkeiten bei Netzwerkübertragungen und Echtzeitverknüpfung von Sicherheits- und Netzwerkdaten – zur Erweiterung des IBM Security SiteProtector System
- **IBM Security QRadar QFlow und VFlow Collectors:** Integrierte Sammlung und Inhaltserfassung von Netzwerkübertragungen, einschließlich Layer 7-Anwendungsanalysen für physische und virtuelle Umgebungen

Mitarbeiter

Steuerung, Überwachung und Authentifizierung des Benutzerzugriffs auf geschützte Daten und Anwendungen.

Herausforderungen und Lösungen

IBM Security Identity- und Access-Management-Produkte bieten folgende Vorteile:

- **Management von Benutzern und deren Zugriffsrechte:** Sie können Benutzerprofile und Zugriffsrechte während des gesamten Lebenszyklus effizient registrieren, verwalten und beenden. Abgelaufene Benutzerkonten und Rollenkonflikte können gekennzeichnet werden.
- **Optimieren/Nachverfolgen von Benutzerzugriffen auf geschützte Ressourcen:** Integrieren Sie Zugriffsrechte für den gesamten Lebenszyklus mit Single Sign-on- und Kennwortmanagement sowie mit Zugriffsprüfungen und -berichten. Durch die zuverlässige Authentifizierung von Geräten ergibt sich ein zusätzliches Maß an Sicherheit.
- **Schutz des Zugriffs in cloudbasierten, mobilen und SaaS-Umgebungen (Software-as-a-Service):** Stellen Sie einen einheitlichen Identitätsservice für die Bereitstellung von Benutzern, den rollenbasierten Zugriff und zusammengefasste Identitäten zur Verfügung. Zentralisieren Sie das Sicherheitsmanagement für Benutzerberechtigungen und-richtlinien.

Produkte

Zu den integrierten Lösungen, die die Zugriffsaktivitäten und -berechtigungen von Benutzern während des gesamten Lebenszyklus steuern, gehören folgende:

- **IBM Security Identity Manager:** Management von Benutzerkonten, Zugriffsrechten, Berechtigungen und Kennwörtern von deren Erstellung bis zu Beendigung
- **IBM Federated Identity Manager:** Benutzerorientiertes, zusammengefasstes Single Sign-on für den Austausch von Informationen zwischen vertrauenswürdigen Business Partnern und zur Vereinfachung der Anwendungsintegration in verteilten Portal- und Mainframeumgebungen
- **IBM Security Access Manager for Web:** Umfassend skalierbares Management von Benutzerzugriffen und Schutz von Webanwendungen, um das Unternehmen vor hochentwickelten Sicherheitsbedrohungen zu schützen
- **IBM Security Access Manager for Cloud and Mobile:** Erweiterung des Benutzerzugriffsschutzes mithilfe föderierter SSO-Funktionen (Single Sign-on), Benutzerauthentifizierung und Risikobeurteilungen auf mobile und cloudbasierte Umgebungen
- **IBM Security Access Manager for Enterprise Single Sign-On:** Integrierte Authentifizierung, Automatisierung des Zugriffsworkflows, Umschalten zwischen Benutzern und Prüfberichten, um die Zugriffssicherheit zu vereinfachen und zu verbessern
- **IBM Security Identity und Access Assurance:** Management von Benutzerkonten, Zugriffsberechtigungen und Kennwörtern mit komfortablem Single Sign-on auf Unternehmensanwendungen und -ressourcen

Daten

Schutz kritischer Daten an wichtigen Kontrollpunkten ohne Produktivitätseinbußen.

Herausforderungen und Lösungen

IBM Datensicherheitsprodukte bieten Vorteile in folgender Hinsicht:

- **Vermeiden von Datenschutzverletzungen:** Überwachen Sie Transaktionen, ohne Änderungen an Datenbanken oder Anwendungen vornehmen zu müssen. Erstellen Sie realistische Tests, bei denen vertrauliche Daten verdeckt bleiben. Verschlüsseln Sie regulierte Daten, um Datenverluste zu vermeiden – insbesondere durch Diebstähle von Datensicherungen und Datenträgern. Geben Sie eigenständige oder integrierte unstrukturierte, vertrauliche Daten in Formularen und Dokumenten aus.
- **Bewahrung der Integrität vertraulicher Daten:** Vergleichen Sie alle Transaktionen mit Richtlinien und verhindern Sie Datenschutzverletzungen in Echtzeit.
- **Verringerung der Compliancekosten:** Automatisieren und zentralisieren Sie Kontrollen zur Optimierung von Compliancеprüfungen.

Produkte

Zu den IBM InfoSphere Guardium-Produkten, die dazu beitragen, den Datenschutz und die Datenintegrität vertrauenswürdiger Informationen im Rechenzentrum zu gewährleisten, gehören folgende:

- **IBM InfoSphere Guardium Database Activity Monitoring:** Eine einfache, zuverlässige Lösung, mit der die Offenlegung vertraulicher Daten aus Datenbank und Dateien verhindert werden kann, die Integrität von Informationen im Rechenzentrum gewahrt bleibt und Compliancekontrollen in heterogenen Umgebungen automatisiert werden
- **IBM InfoSphere Guardium Vulnerability Assessment:** Automatisierte Erkennung von Sicherheitslücken in Datenbanken mit priorisierten Maßnahmen zur Fehlerbehebung in heterogenen Infrastrukturen
- **IBM InfoSphere Guardium Data Redaction:** Schutz vor der versehentlichen Offenlegung vertraulicher Daten in Dokumenten und Formularen durch das Erkennen und Entfernen von Daten aus öffentlich gemeinsam genutzten Dokumentversionen
- **IBM InfoSphere Guardium Data Encryption:** Verschlüsselung von Unternehmensdaten ohne Einbußen bei der Anwendungsleistung oder zusätzlicher Komplexität bei der Schlüsselverwaltung
- **IBM InfoSphere Optim Data Masking:** Funktionen zur Unkenntlichmachung vertraulicher Informationen, um den Datenschutz zu gewährleisten und Compliance-Initiativen zu unterstützen
- **IBM Security Key Lifecycle Manager:** Lifecycle-Management von Verschlüsselungsschlüsseln mit zentralisierten und optimierten Prozessen, die auf das Key Management Interoperability Protocol nach Branchenstandard zurückgreifen
- **IBM InfoSphere Discovery:** Ein Tool, mit dem identifiziert und dokumentiert werden kann, welche Daten vorhanden sind, wo sich diese befinden und wie sie auf den Systemen miteinander verknüpft sind. Dies erfolgt durch die intelligente Erfassung von Beziehungen und die Festlegung angewendeter Transformationen und Geschäftsregeln.

Anwendungen

Schützen
Testen
Kontrollieren

Dauerhafter Schutz von Anwendungen vor böswilliger oder betrügerischer Verwendung und Hackerangriffen.

Herausforderungen und Lösungen

IBM Produkte zur Anwendungssicherheit bieten Vorteile in folgender Hinsicht:

- **Feststellen und Beseitigen von Sicherheitslücken in mobilen und webbasierten Anwendungen:** Verwendung statischer, dynamischer, laufzeitspezifischer und clientseitiger Analysen und Verknüpfung der Ergebnisse
- **Entwickeln von Anwendungen mit integrierter Sicherheit:** Integrieren Sie Sicherheitstests frühzeitig und während des gesamten Designprozesses. Ermöglichen Sie Sicherheits- und Entwicklungsteams einen effektiven Informationsaustausch.
- **Kontrollieren des Zugriffs auf Anwendungsdaten:** Steuerung und Umsetzung eines differenzierten Richtlinienmanagements zur Sicherheit von Berechtigungen und Mitteilungen.

Produkte

Ein vollständiges Portfolio mit Lösungen zum Schutz Ihrer Anwendungen. Dazu gehören folgende Produkte:

- **IBM Security AppScan Standard:** Automatisierte Tests zur Sicherheit von Webanwendungen für IT-Sicherheit, Auditoren und Penetrationstester
- **IBM Security AppScan Enterprise:** Auf Großunternehmen zugeschnittene Tests zur Sicherheit von Anwendungen und Risikomanagement mit Governance, Zusammenarbeit und Security Intelligence
- **IBM Security AppScan Source:** Statische Tests zur Anwendungssicherheit, um bei der Entwicklung Sicherheitslücken in webbasierten und mobilen Anwendungen zu ermitteln
- **IBM Security Policy Manager:** Funktionen für die Erstellung von Anwendungsberechtigungen und differenzierte Richtlinien für die Zugriffskontrolle bei dezentralen Richtlinienentscheidungen basierend auf einem Identitäts-, Transaktions- und Service-/Ressourcenkontext
- **IBM WebSphere DataPower XML Security Gateway:** Eine appliance-basierte Lösung, die die Sicherheit von Web-Services in Echtzeit und den Schutz vor XML-spezifischen Sicherheitsbedrohungen bietet.

Infrastruktur: Netzwerk

Präventiv
Schnell
Erweiterbar

Sicherheit für die gesamte Netzwerkinfrastruktur.

Herausforderungen und Lösungen

IBM Produkte zur Netzwerksicherheit bieten Vorteile in folgender Hinsicht:

- **Bei neuen Sicherheitsbedrohungen auf dem aktuellen Stand bleiben:** Vermeiden von Netzwerkmanipulationen durch Schutz vor neuen Sicherheitsbedrohungen auf der Grundlage von Forschungsergebnissen von IBM X-Force, das beim Schutz vor Zero-Day-Sicherheitslücken auf eine lange Erfolgsgeschichte verweisen kann
- **Abstimmung zwischen Sicherheit und Leistung ohne Unterbrechung geschäftskritischer Anwendungen und Infrastrukturen:** Bis zu 20 Gbps geprüfter Durchsatz (und mehr) mit Network Intrusion Prevention, sodass selbst anspruchsvollste Anforderungen an die Servicequalität erfüllt werden können – ohne Einbußen beim Sicherheitsniveau
- **Niedrigere Infrastrukturkosten und weniger Komplexität:** Konsolidierung von Einzellösungen und Abbau komplexer Strukturen durch die Integration mit anderen Sicherheitslösungen
- **Schneller Schutz netzwerkunabhängiger Ressourcen angesichts neuer Sicherheitsbedrohungen:** Schutz von Daten-, Client-, Web- und Unternehmensanwendungen mithilfe der erweiterbaren Engine im IBM Security Network Intrusion Prevention System.

Produkte

Zu den IBM Angeboten für die Sicherheit von Netzwerkinfrastrukturen gehören folgende:

- **IBM Security Network Protection:** Zentraler Schutz vor Sicherheitsbedrohungen in Kombination mit innovativen Funktionen zur Transparenz und Kontrolle von Anwendungen, um Risiken zu vermeiden und Bandbreite zu erhalten
- **IBM Security Network Intrusion Prevention System:** Zentrales Element einer Strategie zur Vermeidung von Netzwerkmanipulationen; bietet appliance-basierten Schutz vor einer Vielzahl von Angriffen auf die Netzwerkinfrastruktur
- **IBM Security SiteProtector System:** Zentralisiertes Management von IBM Security Network Intrusion Prevention-Lösungen, mit einem einzigen Steuerungspunkt, einschließlich Sicherheitsrichtlinien, -analysen, -mitteilungen und -berichten.

Infrastruktur: Endpunkte

Analysieren
Beheben
Umsetzen
Dokumentieren

Schutz und Management verteilter Endpunkte.

Herausforderungen und Lösungen

IBM Endpoint-Management- und Security-Produkte bieten Vorteile in folgender Hinsicht:

- **Kontinuierliche Compliance an allen Endpunkten, unabhängig von deren Standort oder Verbindung:** Nutzen Sie einen intelligenten Agenten, um den Compliancestatus zu überwachen und zu dokumentieren, führen Sie bei Bedarf korrigierende Maßnahmen automatisiert durch.
- **Ein hohes Maß an Patch-Compliance in heterogenen Umgebungen:** Patching-Funktionen für Microsoft® Windows®-, UNIX®-, Linux®- und Mac-Umgebungen und für mobile Geräte – über eine zentrale Managementkonsole und einen zentralen Management-Server
- **Schutz von Endpunkten mit kurzen Reaktionszeiten:** Automatische Identifizierung betrügerischer oder falsch konfigurierter Endpunkte und Identifizierung/Beseitigung/Verlagerung in Quarantäne von Endpunkten, an denen Zwischenfälle auftreten, innerhalb weniger Minuten
- **Optimierung von Maßnahmen für Compliance und Risikomanagement:** Automatisierte und aussagekräftige Audit- und Complianceberichte mit umfassender, proaktiver Überprüfung von Sicherheitskonfigurationen
- **Schutz virtualisierter Endpunkte:** Eine zentrale Sicherheitsanzeige der physischen und virtuellen Serverumgebungen mit automatischem Schutz für virtuelle Maschinen (VMs), sobald diese online gestellt oder verlagert werden.

Produkte

Zu den IBM Produkten für den Schutz verteilter Endpunkte gehören folgende:

- **IBM Endpoint Manager:** Endpunkt- und Sicherheitsmanagement in einer einzigen Lösung, die die Transparenz und die Kontrolle physischer und virtueller Endpunkte ermöglicht; schnelles Beseitigen, Schützen und Berichten an Endpunkten in Echtzeit; Automatisierung zeitintensiver Aufgaben in komplexen Netzwerken, um die Kosten zu senken, Risiken zu verringern und die Compliance zu gewährleisten.

- **IBM Security Virtual Server Protection for VMware:** Schutz auf allen Ebenen der virtuellen Infrastruktur mithilfe eines gestaffelten Sicherheitskonzepts, dynamischer Sicherheit mit Rootkit-Erkennung auf virtuellen Maschinen, Überprüfung virtueller Infrastrukturen und Überwachung von Netzwerkübertragungen durch Einbindung von Hypervisoren
- **IBM Security Host Protection:** Schutz vor internen und externen Sicherheitsbedrohungen für Netzwerkressourcen, z. B. Server und Desktopsysteme

Infrastruktur: Mainframe

Nutzung des Mainframe als unternehmensweiten Sicherheitshub zum Schutz geschäftskritischer Produktionssysteme und -daten.

Herausforderungen und Lösungen
IBM Produkte zur Mainframesicherheit bieten folgende Vorteile:

- **Manuelle Überprüfung der Compliance, mit Benachrichtigungen nur bei Auftreten eines Problems:** Sie erhalten Benachrichtigungen über externe Sicherheitsbedrohungen, unangemessene Datenzugriffe oder fehlerhafte Konfigurationen in Echtzeit, mit automatischer Überwachung der Compliance. Missbräuche durch privilegierte Benutzer werden durch Blockieren von IBM RACF-Befehlen (Resource Access Control Facility) in Echtzeit verhindert.
- **Bewältigen der Komplexität bei der Identifizierung und Analyse von Sicherheitsbedrohungen in Mainframeumgebungen:** Automatische Analysen und Berichte zu Sicherheitsereignissen auf dem Mainframe und Erkennen von Sicherheitslücken. Überwachung von Eindringlingen. Identifizierung fehlerhafter Konfigurationen.
- **Qualifizierte IT-Mitarbeiter, die die Mainframesicherheit manuell gewährleisten:** Einfachere Verwaltung mithilfe einer Windows-basierten GUI (Graphical User Interface) für die RACF-Administration.

Produkte
Zur IBM Security zSecure Suite für die infrastrukturspezifische Mainframesicherheit gehört Folgendes:

- **IBM Security zSecure Admin:** Effiziente und effektive RACF-Administration mit deutlich geringerem Personalaufwand
- **IBM Security zSecure Visual:** Geringere Notwendigkeit für seltenes, RACF-spezifisches Fachwissen durch eine Windows-basierte GUI für die RACF-Administration
- **IBM Security zSecure CICS Toolkit:** Mainframe-Administration über eine IBM CICS-Umgebung (Customer Information Control System), sodass Mitarbeiter mit RACF-Fachwissen entlastet werden
- **IBM Security zSecure Audit:** Automatische Analysen und Berichte zu Sicherheitsereignissen und Erkennen von Sicherheitslücken
- **IBM Security zSecure Alert:** Echtzeitüberwachung von Sicherheitsbedrohungen auf dem Mainframe, um Eindringlinge überwachen und fehlerhafte Konfigurationen ermitteln zu können, die Compliancemaßnahmen behindern könnten
- **IBM Security zSecure Command Verifier:** Umsetzung von Richtlinien zur besseren Einhaltung von unternehmensspezifischen und regulatorischen Richtlinien durch die Vermeidung falscher Befehle
- **IBM Security zSecure Manager for RACF z/VM:** Eine benutzerfreundliche, zusätzliche Ebene auf dem Mainframe, die eine erstklassige Administration sowie Prüffunktionen für z/VM RACF und Linux auf IBM System z ermöglicht.

Hochentwickelte Untersuchungen zu Sicherheit und Sicherheitsbedrohungen

Das weltweit anerkannte IBM X-Force Forschungs- und Entwicklungsteam ist die Grundlage für das präventive IBM Konzept zur Internetsicherheit. Diese Gruppe von Sicherheitsexperten konzentriert sich auf die Untersuchung und Auswertung von Sicherheitslücken und -problemen, die Entwicklung von Analysen und Gegenmaßnahmen für IBM Produkte (sie werden über den X-Force Threat Intelligence Feed in Echtzeit aktualisiert) und die Vermittlung neuer Sicherheitsbedrohungen und Trends im Internet.

Das IBM X-Force Forschungs- und Entwicklungsteam leistet einen wichtigen Beitrag für den Schutz von IBM Kunden vor Sicherheitsbedrohungen. In der X-Force-Datenbank mit Sicherheitslücken sind über 63.000 Sicherheitslücken dokumentiert, einschließlich einer detaillierten Analyse aller bekannt gewordenen öffentlichen Sicherheitslücken seit 1994. Der IBM X-Force Trend and Risk Report erscheint zwei Mal pro Jahr und ist einer der ältesten und umfangreichsten Sicherheitsberichte seiner Art. Darin werden Herausforderungen im Sicherheitsbereich detailliert vorgestellt, z. B. Sicherheitsbedrohungen, geschäftliche und entwicklungsspezifische Verfahren und aktuelle Trends.

Lösungen für die Herausforderungen von heute

Das IBM Security Framework mit integrierten Produkten und Services wurde entwickelt, um Security Intelligence zu bieten. Es kann für den Schutz heutiger und künftiger Unternehmensplattformen vor bekannten und unbekannten Sicherheitsbedrohungen verwendet werden. Im heutigen Geschäftsumfeld lauten die wichtigsten Trends und Herausforderungen in puncto Sicherheit: Sicherheit mobiler Geräte, Sicherheit in der Cloud, Sicherheit großer Datenmengen und hochentwickelte Sicherheitsbedrohungen.

Sicherheit mobiler Geräte

Mobile Endgeräte und Tablet-PCs haben sich schnell zum wichtigsten Produktivitätstool für Unternehmen und deren Mitarbeiter entwickelt. Sie ermöglichen jederzeit und überall einen flexiblen Zugriff auf Informationen. Ungeschützte Endpunktgeräte sind daher mit einem freien Zugang zu vertraulichen Informationen vergleichbar. Unternehmen müssen die auf diesen Geräten befindlichen Daten schützen – unabhängig davon, ob die Daten abgelegt wurden oder über ungeschützte Netzwerke und Infrastrukturen übertragen werden. IBM bietet Unternehmen die Möglichkeit, sowohl unternehmenseigene als auch private mobile Endgeräte in einer Umgebung mit hohem Sicherheitsniveau zu verwenden. Die Unternehmen profitieren dabei von folgendem Leistungsspektrum:

- **Sicherheit und Management von Geräten:** Schutz der Daten und der Geräte
- **Sicherer Zugriff:** Schutz von Unternehmensressourcen, -daten und -anwendungen
- **Anwendungssicherheit:** Sicherheit in Bezug auf Konzeption, Entwicklung, Test, Bereitstellung, Verwendung und Management mobiler Anwendungen
- **Security Intelligence:** Unternehmensweite Transparenz und ein anpassungsfähiges Sicherheitsniveau für mobile Endgeräte

Besondere Angebote:

- **IBM Security AppScan Source:** Hilft bei der Erkennung von Sicherheitslücken in mobilen Webanwendungen
- **IBM Security Access Manager for Cloud and Mobile:** Weitet den Benutzerzugriffsschutz mithilfe föderierter SSO-Funktionen, Benutzerauthentifizierung und Risikobeurteilungen auf mobile und cloudbasierte Umgebungen aus
- **IBM Endpoint Manager for Mobile Devices:** Führt Konfigurationen zur Gerätesicherheit und Kontrollen der unternehmensweiten Verwaltung durch.

Sicherheit in der Cloud

Unternehmen sind an Lösungen zur Sicherheit in der Cloud interessiert, die Transparenz, Kontrolle, Fehlereingrenzung und Automatisierung für mehrere Cloudinfrastrukturen bieten. Mit Sicherheitslösungen von IBM kann Ihr Unternehmen eine Cloudinfrastruktur einrichten, die Kosteneinsparungen ermöglicht und so dynamisch ist, wie es das heutige Geschäftsumfeld erfordert. IT-Abteilungen können folgendermaßen Risiken im Zusammenhang mit Cloud-Computing verringern und steuern:

- Management von Identitäten und SSO-Zugriff für mehrere Cloud-Services
- Überwachen des Zugriffs auf gemeinsam genutzte Datenbanken
- Überprüfen von Webanwendungen, die über die Cloud bereitgestellt wurden, auf aktuelle Sicherheitslücken
- Schutz der Benutzer und Workloads in der Cloud vor hochentwickelten Netzwerkangriffen
- Überwachen cloudbasierter und traditioneller Ressourcen im Rahmen eines einzigen, einheitlichen Konzepts
- Endpunkt- und Patch-Management virtualisierter Maschinen zur Einhaltung von Sicherheitsbestimmungen
- Höhere Transparenz und bessere Überprüfung von Cloudaktivitäten in Multi-Tenant-Umgebungen

Besondere Angebote:

- **IBM Security Virtual Server Protection for VMware:** Schutz vor Sicherheitsbedrohungen auf allen Ebenen einer virtuellen Infrastruktur
- **IBM Tivoli Federated Identity Manager:** Authentifizierung für mehrere Cloudanwendungen innerhalb und außerhalb des Unternehmens über eine einzige ID
- **IBM Endpoint Manager:** Effiziente Sicherheit und Compliance auf verteilten, virtuellen Cloudplattformen

Sicherheit großer Datenmengen

Die enorme Zunahme an Unternehmensdaten stellt im Hinblick auf die Datenverwaltung eine große Herausforderung dar. Gleichzeitig bietet sie aber auch viele Chancen, da sich hieraus sicherheitsspezifische Erkenntnisse gewinnen lassen. IBM Lösungen liefern Erkenntnisse aus riesigen Mengen an Echtzeit- und Protokolldaten – im jeweiligen Kontext und über die bisherigen Möglichkeiten hinaus. Daten sind gewissermaßen

die neue Währung eines Unternehmens. IBM kann folgendermaßen dazu beitragen, diese wertvolle Ressource zu schützen und das Sicherheitsniveau im Unternehmen zu verbessern:

- Verknüpfung großer Mengen an sicherheitsrelevanten Daten (z. B. Protokoll und Netzwerkübertragungen) von mehreren Einzelsystemen mithilfe integrierter und intelligenter Sicherheitsanalysen, um Risiken für das Unternehmen besser vorhersehen und erkennen zu können
- Verringerung geschäftlicher Risiken aufgrund von Sicherheitsbedrohungen für strukturierte Daten (Datenbanken) und unstrukturierte Daten (Dokumente), um Datenverluste und nicht autorisierte Zugriff zu vermeiden

Besondere Angebote

- **IBM Security QRadar:** Integrierte, automatisierte Security Intelligence und Analysen für das gesamte Unternehmen
- **IBM InfoSphere Guardium:** Sicherheit und Überwachung von Datenbanken in Echtzeit, differenzierte Überprüfung von Datenbanken, automatisierte Complianceberichte

Hochentwickelte Sicherheitsbedrohungen

Unternehmen müssen immer komplexere Strukturen bewältigen, um sich vor qualifizierten und entschlossenen Angriffen zu schützen. Die Angreifer können mithilfe raffinierter und standardmäßiger Verfahren auf kritische IT-Ressourcen und öffentliche Infrastrukturen abzielen, um Zugriff zu erhalten. Die Herausforderung besteht darin, dass eine einzige Lösung nicht ausreicht. Unternehmen müssen über das traditionelle Aktualisieren, Überwachen und Korrigieren hinausdenken und sowohl fortlaufend überwachen als auch auf mehreren Ebenen Schutzmaßnahmen ergreifen, die zusammen die Möglichkeit bieten, zielgerichtete Sicherheitsbedrohungen zu identifizieren, zu analysieren und darauf zu reagieren. IBM bietet folgendermaßen Schutz vor hochentwickelten Sicherheitsbedrohungen:

- Identifizierung und Abwehr von bekannten und unbekannten Angriffen durch die Verknüpfung von Netzwerksicherheit, weltweiten Informationen über Sicherheitsbedrohungen und erweiterten Sicherheitsanalysen

Besondere Angebote

- **IBM Advanced Threat Protection Platform**: Beinhaltet IBM Security Network Intrusion Prevention System, IBM Security SiteProtector System, IBM Security QRadar Network Anomaly Detection und IBM Security X-Force Threat Insight
  - Integriert Informationen aus X-Force in QRadar, um Sicherheitsbedrohungen im Zusammenhang mit falschen IP-Adressen zu identifizieren
  - Schutz vor netzwerkbasierten Sicherheitsbedrohungen, die in allgemeinen Netzwerkübertragungen verborgen sind; Schutz vor Angriffen durch die Ausnutzung von Sicherheitslücken auf Netzwerk-, Host- und Anwendungsebene

Gartner führt IBM Security im Leaders Quadrant

Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms, von French Caldwell, John Wheeler, 4. Oktober 2012

Magic Quadrant for User Administration/Provisioning, von Earl Perkins, Perry Carpenter, 22. Dezember 2011

Magic Quadrant for Static Application Security Testing, von Joseph Feiman, Neil MacDonald, 12. Dezember 2010

Magic Quadrant for Dynamic Application Security Testing, von Joseph Feiman, Neil MacDonald, 17. Dezember 2011

Magic Quadrant for Security Information & Event Management, von Mark Nicolett, Kelly Kavanagh, 24. Mai 2012

Fazit

Im Big Data-Zeitalter, in dem Informationen der wichtigste Faktor zur Durchführung der Geschäftstätigkeit sind und dauerhafte Angriffe auf Unternehmensdaten und IT-Ressourcen die Effektivität traditioneller IT-Schutzmaßnahmen in Frage stellen, wird ein grundlegend neues Sicherheitskonzept benötigt. Ein solches Konzept muss auf drei Grundprinzipien basieren: Intelligenz, Integration und Expertise. Sie bieten Transparenz in der Infrastruktur, bereichsübergreifende Verknüpfungen und optimierte Kontrollen, die nicht nur für den Schutz geschäftskritischer Daten benötigt werden, sondern auch im Hinblick auf Maßnahmen zur Einhaltung gesetzlicher Bestimmungen. Das IBM Security Framework bietet ein einheitliches Konzept zur Unternehmenssicherheit, das die wesentlichen Funktionen steuert – von der Erkennung von Sicherheitsbedrohungen bis zum Benutzerzugriff, zur Verringerung der Compliancekosten, zum Konfigurationsmanagement und vieles mehr. Die Grundlage hierfür sind weltweit erstklassige Ergebnisse aus Forschung und Entwicklung, mit denen die Risiken im Zusammenhang mit hochentwickelten Sicherheitsbedrohungen von heute verringert werden können.

Weitere Informationen

Wenn Sie mehr über IBM Security erfahren möchten, wenden Sie sich bitte an den zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com**/security

Weitere Informationen zum Institute for Advanced Security finden Sie unter: www.instituteforadvancedsecurity.com

Mithilfe von IBM Global Financing (IGF) können Sie die Software, die Ihr Unternehmen benötigt, kosteneffizient erwerben. Wir bieten Kunden individuelle Finanzierungslösungen, die auf ihre geschäftlichen Zielsetzungen abgestimmt sind und ihnen helfen, ihren Cashflow zu verbessern und die Gesamtkosten zu senken. Finanzieren Sie wichtigeIT-Anschaffungen mit IGF und verschaffen Sie Ihrem Unternehmen einen Vorsprung. Weitere Informationen finden Sie im Internet unter: **ibm.com**/financing/de/

IBM leistet keine rechtliche Beratung oder Beratung bei Fragen der Buchführung und Rechnungsprüfung. IBM gewährleistet und garantiert nicht, dass seine Produkte oder sonstigen Leistungen die Einhaltung bestimmter Rechtsvorschriften sicherstellen. Der Kunde ist für die Einhaltung anwendbarer Sicherheitsvorschriften und sonstiger Vorschriften des nationalen und internationalen Rechts verantwortlich.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
Germany
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie im Internet unter: **ibm.com**

IBM, das IBM Logo, ibm.com, AppScan, DataPower, Guardium, InfoSphere, Optim, SiteProtector, System z, Tivoli, WebSphere, X-Force, zSecure und z/VM sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein.

Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter: **ibm.com**/legal/copytrade.shtml

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken von anderen Unternehmen sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern.

Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

Bei IBM heißt Dienst am Kunden zugleich auch Dienst an unserer Umwelt: Wir nehmen Ihre IBM Altgeräte und Zubehörteile zurück und stellen deren umweltfreundliche Entsorgung zum Selbstkostenpreis sicher. Sie können neben neuen auch wiederverwendete Teile enthalten.

Diese Veröffentlichung dient nur der allgemeinen Information.
Die in dieser Veröffentlichung enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Aktuelle Informationen zu IBM Produkten und Services erhalten Sie bei der zuständigen IBM Verkaufsstelle oder dem zuständigen Reseller.

Bei abgebildeten Geräten kann es sich um Entwicklungsmodelle handeln.

© Copyright IBM Corporation 2013

Bitte der Wiederverwertung zuführen

WGB03004-DEDE-00