Integrierter Schutz vor Cyberkriminalität: IBM Security Trusteer – Produktüberblick

Sorgen Sie mit dem umfassenden IBM Security Trusteer Portfolio für die Erkennung und Abwehr aller Angriffsvektoren

Highlights

- Verhindern Sie Angriffe von Cyberkriminellen, die sich mit alten Lösungen allein nicht stoppen lassen.
- Identifizieren Sie Betrugsversuche in Echtzeit mit einer umfassenden, integrierten Architektur zur Abwehr von Cyberkriminalität.
- Profitieren Sie von vier Grundsätzen: Ermöglichen Sie eine effektive und präzise Abwehr von Betrugsversuchen, passen Sie sich an neue Bedrohungen an, optimieren Sie die Erfahrung von Endbenutzern und sorgen Sie für eine rasche Amortisierungszeit.

Cyberkriminelle nehmen immer wieder Finanzinstitute, Unternehmen, E-Commerce-Anbieter und andere Organisationen ins Visier, um finanzielle und geschäftliche Informationen zu ergaunern. Alte Lösungen können solche Angriffe nur schwer verhindern, da es ihnen an Bedrohungsdaten sowie nahezu echtzeitbasierten Informationen zum gesamten Angriffszyklus fehlt.

IBM hat eine umfassende, integrierte Architektur zur Abwehr von Cyberkriminalität entwickelt, die in Hunderten von Unternehmen weltweit erfolgreich genutzt wird. Lösungen von IBM Security Trusteer helfen bei der Erkennung und Abwehr verschiedenster Angriffsvektoren – darunter Phishing und Malware, die auf Endbenutzer abzielen, sowie das Kapern von Konten durch Cyberkriminelle. Diese Angriffsvektoren sind für die meisten der onlinebasierten, mobilen und kanalübergreifenden Betrugsfälle verantwortlich. Unsere Architektur zur Abwehr von Cyberkriminalität basiert auf vier Grundsätzen, um Betrugsversuche zu verhindern, für nachhaltigen Schutz zu sorgen, das Kundenerlebnis zu optimieren und die Belastung der IT-Abteilung spürbar zu reduzieren:

Wehren Sie Betrugsversuche effektiv und präzise ab

- Bekämpft die Ursachen der häufigsten Betrugsversuche: Malware und Phishing.
- Erkennt aktive Bedrohungen in nahezu Echtzeit.
- Analysiert Risikofaktoren, die mit einzelnen Geräten, Benutzern, Konten und Transaktionen verbunden sind, um Kontoübernahmeversuche und hochriskante Transaktionen zu ermitteln.

Passen Sie sich an neue Bedrohungen an

- Nutzen Sie nahezu echtzeitbasierte globale Informationen von Abermillionen von Endpunkten.
- Sorgen Sie für eine dynamische Anpassung der verschiedenen Schutzebenen, um nachhaltigen Schutz zu erreichen.

Optimieren Sie das Endbenutzererlebnis

- Ermöglicht transparenten Schutz.
- Sorgt bei Kunden, die legitime Transaktionen ausführen, für deutlich weniger Beeinträchtigungen.
- Trägt zu einer höheren Effektivität der Support-, Betrugserkennungs- und Risikoteams des Unternehmens bei.

Sorgen Sie für eine schnelle Amortisierung

- Nutzen Sie für eine rasche Bereitstellung eine sofort einsatzbereite SaaS-Lösung.
- Ermöglicht eine unmittelbare Reaktion bei allen Online- und Mobilanwendungen.

IBM Security Trusteer Produktübersichten und Hauptfunktionen

Produkt	Überblick	Hauptfunktionen
IBM® Security Trusteer Pinpoint Criminal Detection	Zuverlässiger Schutz vor Kriminellen und Kontoübernahmeversuchen	• Ermittelt neue, manipulierte (Proxy) und bekannte kriminelle Systeme mithilfe komplexer Geräte-IDs • Erkennt Phishing-Vorfälle in nahezu Echtzeit • Für die Unterstützung der Integration erweiterter Malware- und Phishing-Risikoindikatoren aus Trusteer Pinpoint Malware Detection und Trusteer Rapport (falls verfügbar) vorgesehen • Korreliert Geräterisiken (d. h. neue, manipulierte und bekannte kriminelle Systeme) mit Kontorisiken (d. h. Phishing-Ereignisse und Malware-Infektionen), um Cyberkriminelle und Kontoübernahmeversuche zuverlässig zu erkennen • Pflegt eine globale Datenbank mit kriminellen Systemen – basierend auf den Informationen Hunderter von Unternehmen weltweit
IBM® Security Trusteer Pinpoint Malware Detection	Genaue Erkennung von aktiven, mit Man-in-the-Browser-Malware infizierten Geräten in nahezu Echtzeit	• Ermittelt aktive Man-in-the-Browser-Infektionen auf PCs, Macs und mobilen Geräten • Sendet Malware-Erkennungsereignisse per E-Mail, Batchdateien oder direkte Feeds an Trusteer Pinpoint Criminal Detection sowie Risiko-Engines anderer Anbieter
IBM® Security Trusteer Mobile Risk Engine	Zuverlässige Erkennung mobiler Betrugsrisiken, die mit kompromittierten Geräten von Endbenutzern und Kriminellen zusammenhängen	• Identifiziert Zugriffe per Smartphone oder Tablet, die ein hohes Risiko aufweisen • Erstellt Risikoanalysen anhand von geräte-, sitzungs- und benutzerbasierten Risikofaktoren, die von Trusteer Mobile SDK, Trusteer Mobile App und Anwendungen anderer Anbieter erfasst werden • Korreliert kanalübergreifend Risikofaktoren wie Malware-Infektionen und Phishing-Ereignisse im Online-Kanal, um komplexe Angriffsszenarien im Online- und Mobile-Bereich bewältigen zu können
IBM® Security Trusteer Rapport	Client-basierter Schutz für Endpunkte vor finanziellen Malware- und Phishing-Angriffen	• Verhindert und beseitigt Infektionen durch aktive und inaktive Man-in-the-Browser-Malware aus infizierten Geräten • Schützt Browsing-Sitzungen selbst dann, wenn aktive Malware vorhanden ist • Erkennt Phishing-Seiten und kompromittierte Kontoanmeldedaten sowie Kreditkartendaten • Meldet Malware-Infektionen und -Beseitigungen an das Betrugserkennungsteam, damit Benutzer neue Anmeldedaten erhalten und zukünftige Bedrohungen eliminieren lassen können
IBM® Security Trusteer Mobile SDK	Dedizierte Sicherheitsbibliothek für Apple iOS- und Google Android-Plattformen, die sich in proprietäre Mobile-Banking-Anwendungen integrieren lassen, damit kompromittierte und anfällige Geräte erkannt sowie dauerhafte Geräte-IDs erzeugt werden	• Ermittelt folgende Risikofaktoren: – Geräte mit entferntem Schutzmechanismus/Root-Zugriff – Malware-Infektionen – Installationen schädlicher Anwendungen – Unsichere WLAN-Verbindungen – Veraltete Betriebssysteme – Geografische Standorte • Erzeugt anhand von Hardware- und Softwareattributen eine dauerhafte Geräte-ID, die auch eine Neuinstallation von Anwendungen übersteht
IBM® Security Trusteer Mobile Browser	Risikobasierte Analysen für Webzugriffe und Transaktionen mit mobilen Geräten	• Beinhaltet Trusteer Mobile SDK, damit Webanwendungen die Risikofaktoren von Geräten sowie die dauerhaften Geräte-IDs kennen • Verhindert Man-in-the-Middle-Angriffe (um sicherzustellen, dass Benutzer die echte Website aufrufen) • Weist Benutzer auf gerätespezifische Risikofaktoren hin und bietet Ratschläge zur Behebung
IBM® Security Trusteer Apex Advanced Malware Protection	Schützt Endgeräte von Mitarbeitern vor intelligenter Malware	• Schützt Webbrowser sowie Java, Adobe, Microsoft Office und andere Anwendungen vor Zero-Day-Bedrohungen • Verhindert das Herausfiltern von Daten durch Malware • Verhindert den Diebstahl von Anmeldedaten via Spear-Phishing sowie die Wiederverwendung geschäftlicher Anmeldedaten für private Websites • Unterstützt verwaltete und nicht verwaltete Endgeräte von Mitarbeitern

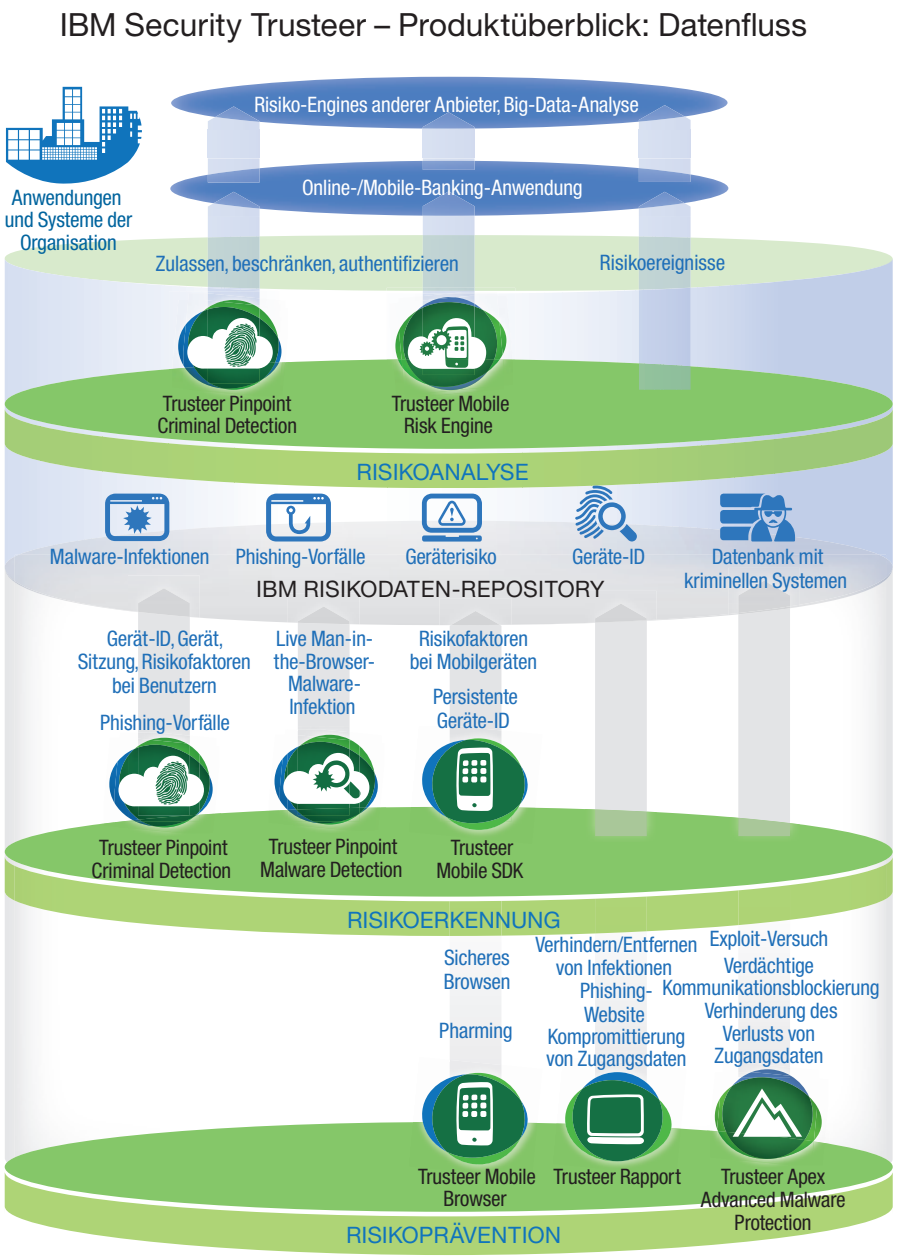

Abbildung 1: Der IBM Ansatz für eine umfassende Sicherheitsarchitektur sorgt für einen Strom von Daten und Informationen zwischen IBM Security Trusteer Produkten

Warum IBM?

IBM Security Lösungen werden von Unternehmen weltweit für die Abwehr von Betrugsversuchen sowie für die Identitäts- und Zugriffsverwaltung genutzt. Mit diesen bewährten Technologien können Unternehmen Kunden, Mitarbeiter und geschäftskritische Ressourcen vor neuesten Sicherheitsbedrohungen schützen. Angesichts ständig neuer Risiken hilft IBM Unternehmen dabei, ihre grundlegende Sicherheitsinfrastruktur mit einem umfassenden Portfolio an Produkten, Dienstleistungen und Business Partner Lösungen spürbar zu verbessern. Mit IBM können Unternehmen Sicherheitslücken schließen und sich auf den Erfolg ihrer strategischen Initiativen konzentrieren.

Weitere Informationen

Weitere Informationen über die IBM Security Trusteer Lösungen erhalten Sie von Ihrem IBM Ansprechpartner, Ihrem IBM Business Partner oder unter: **ibm.**com/security

Über IBM Security Lösungen

IBM Security bietet eines der modernsten und perfekt integrierten Portfolios mit Sicherheitsprodukten und -services für Unternehmen an. Das Portfolio, das von der weltweit bekannten IBM® X-Force® Forschungs- und Entwicklungsabteilung unterstützt wird, umfasst umfangreiche Sicherheitsexpertise, damit Unternehmen Mitarbeiter und Kunden, Infrastrukturen, Daten und Anwendungen zuverlässig schützen können. Wir bieten Lösungen für die Identitäts- und Zugriffsverwaltung, Datenbanksicherheit, Anwendungsentwicklung, Risikoverwaltung, Endpunktverwaltung, Netzwerksicherheit und vieles mehr an. Mit unseren Lösungen können Unternehmen Risiken erfolgreich verwalten und integrierte Sicherheitsverfahren für mobile und Cloud-basierte Umgebungen, soziale Medien sowie andere geschäftliche Architekturen implementieren. IBM verfügt über eine der weltweit größten Abteilungen für Forschung, Entwicklung und Bereitstellung im Bereich Sicherheit, überwacht in über 130 Ländern 15 Milliarden Sicherheitsereignisse am Tag und kann mehr als 3.000 Sicherheitspatente vorweisen. Mithilfe von IBM Global Financing können Sie die für Ihr Unternehmen erforderlichen Softwarelösungen strategisch und kosteneffizient erwerben. Wir bieten kreditfähigen Kunden individuelle Finanzierungslösungen, die auf ihre Geschäfts- und Entwicklungsziele abgestimmt sind und ihnen helfen, ihre Finanzmittel effektiv zu verwalten und die Betriebskosten zu senken. Finanzieren Sie entscheidende IT-Investitionen mithilfe von IBM Global Financing, um die Geschäfte Ihres Unternehmens weiter voranzutreiben. Weitere Informationen finden Sie im Internet unter: **ibm.com**/financing/de

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

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

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in den Vereinigten Staaten von Amerika
August 2014

Trusteer wurde im August 2013 von IBM übernommen.

Bitte der Wiederverwertung zuführen

WGS03018-DEDE-02