Cyber Security Advisory Services

Finden Sie heraus, ob Ihr Unternehmen auf moderne Cyber Angriffe vorbereitet ist.

Warum Unternehmen eine Sicherheitsbewertung benötigen

Je mehr digitale Initiativen in einem Unternehmen umgesetzt werden, umso größer wird naturgemäß die Angriffsfläche für Cyber Attacken. Außerdem werden die Methoden der Angriffe immer raffinierter und die Anzahl der neuen Bedrohungen größer. Bei so vielen Variablen ist es für Unternehmen wichtig, eine starke Sicherheitsstrategie zu haben.

Eine schwache Sicherheitsstrategie kann diese Folgen haben:

- Finanzieller Verlust aufgrund von Lösegeldforderungen
- Hohe Kosten aufgrund von Ausfallzeiten
- Verlust von Geschäftsdaten und -informationen
- Verlust von Kundenvertrauen und Reputation
- Rechtliche und Compliance-Hürden

Durchschnittliche Kosten eines Datenlecks: US**$ 4,35 Mio.**

Durchschnittliche Kosteneinsparungen durch verbesserte Sicherheit: US**$ 3,05 Mio.**

* Quelle: https://www.ibm.com/in-en/reports/data-breach

Um sich gegen moderne Cyber Angriffe zu verteidigen, müssen Unternehmen zunächst wissen, ob sie über eine passende Sicherheitsarchitektur verfügen. Mit Sicherheitsbewertungen kann die Architektur analysiert und Lücken identifiziert werden.

Sicherheitsbewertungen umfassen die Auswertung zahlreicher Prozesse, wie z.B. Netzwerk-Scans, Penetrationstests, Schwachstellenbewertung, Bedrohungsmodellierung, Cloud-Sicherheit, Operation Technology (OT) Analysen und vielen mehr.

Die verschiedenen Bewertungen dienen unterschiedlichen Zwecken. Bei einer Schwachstellenbewertung wird beispielsweise nach Lücken in Ihren Einstellungen, Konfigurationen, Setups usw. gesucht. Bei einem Penetrationstest wird hingegen ein Angriff auf Ihre Systeme simuliert, um die Reaktion Ihrer Verteidigung zu prüfen.

Was Sie von einer Sicherheitsbewertung erwarten können

Ein Unternehmen mit einem eigenen, kleinen Sicherheitsteam und eingeschränkten Möglichkeiten wird es schwer haben, mit den ständig wachsenden Cyber Risiken alleine fertig zu werden. Daher kann es sein eigenes Sicherheitsniveau nicht beurteilen.

Mit Sicherheitsbewertungen können wir folgendes feststellen:

- Wie hoch das Risiko für Ihre Systeme und Ihr Unternehmen ist
- Wie gut die aktuelle Sicherheitslösung funktioniert
- Ob es Lücken in der derzeitigen Sicherheitsarchitektur gibt
- Wie diese Lücken verringert werden können
- Wie Sie effektive Sicherheitsinvestitionen tätigen können
- Welche Möglichkeiten zur Messung der Sicherheitsleistung sinnvoll sind
- Wie höhere Sicherheitsreifegrade erreicht werden können.

Um Ihnen eine Vorstellung vom Bewertungsprozess zu geben, sind hier einige Standardschritte:

1. Erster Kontakt: Festlegung der Agenda
2. Überprüfung der Architektur: Interviews mit den Beteiligten (Architekten, operatives Team, C-Level, GRC-Team) und Workshops
3. Bewertungen: Durchführung von Umfragen und Bewertungen
4. Analyse: Identifizierung der Korrelation zwischen Bedrohungen, Assets und Schwachstellen
5. Veröffentlichung: Veröffentlichung eines Berichts mit den Ergebnissen
6. Durchführung: Angepasste Empfehlungen und ein Fahrplan basierend auf den Ergebnissen

T Systems

Let's power higher performance

Sicherheitsexpertise

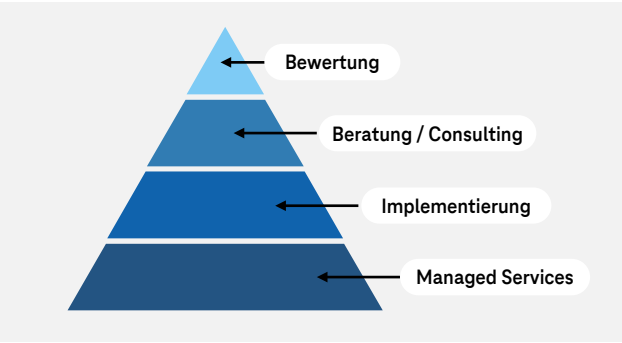
Haben Sie Fragen zu Sicherheitsbewertungen? Oder benötigen Sie Beratung, um Ihre Sicherheitsarchitektur zu überprüfen? Wir helfen Ihnen gerne.

Wir unterstützen Sie bei:

- Bewertung der aktuellen IT-Architektur
- Bewertung der OT-Architektur
- Bewertung der SASE-Architektur
- Bewertung der Zero Trust-Architektur
- Cloud- & Netzwerk-Konfiguration
- Penetration Tests
- CISO-as-a-Service und mehr.

Wir können Sie bei der Auswahl der für Sie passenden Cybersicherheitslösungen unterstützen.

Gemeinsam erstellen wir einen Fahrplan, um das Sicherheitsniveau Ihres Unternehmens zu steigern. Dadurch schützen Sie nicht nur Daten und Anwendungen, sondern bewegen sich auch mit einem strategischen Sicherheitsvorteil hin zur sicheren digitalen Transformation.



Ihre Cybersicherheit in sicheren Händen:

- Ein Pool erfahrener Sicherheits-berater:innen
- Die neuesten Tools und Plattformen für Bewertungen
- Eines der größten Security Operations Center (SOC)
- 200+ Cybersicherheits-expert:innen, allein im SOC
- Umfangreiches Partnernetzwerk und beste Lösungen für die Implementierung
- Nachgewiesene Erfahrung in Managed Security Services

Expertenkontakt

Andreas Pecka
Head of International Expert Sales & Presales Cyber Security
a.pecka@t-systems.com

Herausgeber

T-Systems International GmbH
Hahnstraße 43d, 60528 Frankfurt am Main, Deutschland
E-Mail: cyber.security@t-systems.com
Internet: www.t-systems.com

Letzte Aktualisierung: 10/2023

T Systems

Let's power higher performance