Next Stop: Exposure Management

Stellen Sie Ihr etabliertes Schwachstellen-Management auf den Prüfstand

Alexander Wagner, Senior Security Consultant, Controlware GmbH

Was treibt uns an?

„Die Frage ist nicht **ob**, sondern **wann** ein Sicherheitsvorfall eintritt!“

Herausforderungen

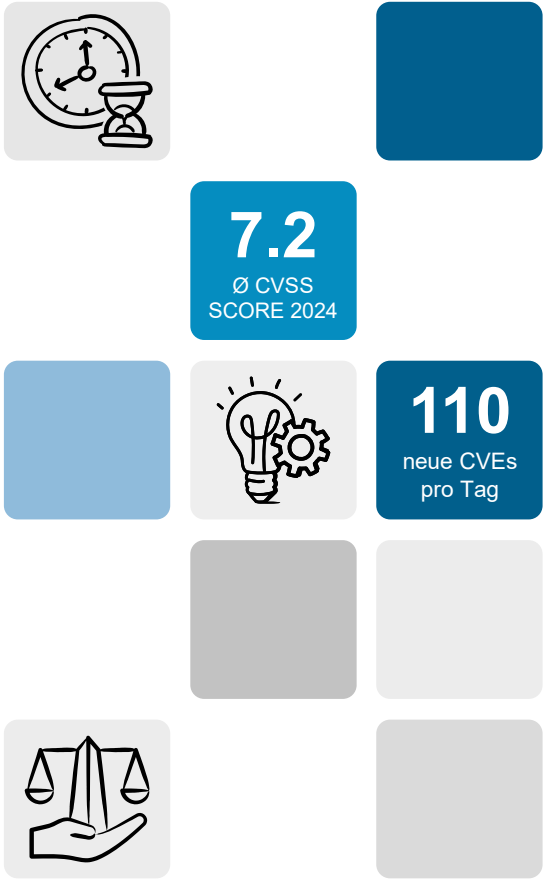
- Stetige Zunahme an Cyber-Kriminalität
- Angreifbare Systeme sind unbekannt
- Unzureichende Change- und Patch-Management-Prozesse

Auswirkungen

- Großteil der Angriffsoberfläche ist unbekannt
- Risiko eines erfolgreichen Cyber-Angriffs steigt

Unsere Empfehlungen

- Risiko systematisch identifizieren, analysieren und minimieren
- Etablierung eines Vulnerability Managements
- Weiterentwicklung zu einem **Exposure Management**



Controlware Vulnerability Management – Überblick Service-Module

Business Process

- Erfassung & Priorisierung der Prozesse
- Geschäftsprozessabhängige Risikobewertung
- Benachrichtigung bei Business-Gefährdung

Asset Inventory

- Kontinuierliche Asset-Erfassung & -Inventarisierung
- Identifizierung & Pflege von Verantwortlichkeiten

Threat Advisor

- Dedizierter Security Consultant
- Regelmäßiger gemeinsamer Austausch
- Bewertung & Priorisierung der Findings

Scan & Remediate

- Regelmäßige Vulnerability Scans
- Individualisierbare Untersuchungstiefe
- Bewertungssysteme: CVSS & VPR

On-Demand Scans

- Durchführung kurzfristiger Vulnerability Scans bei veränderter Bedrohungslage

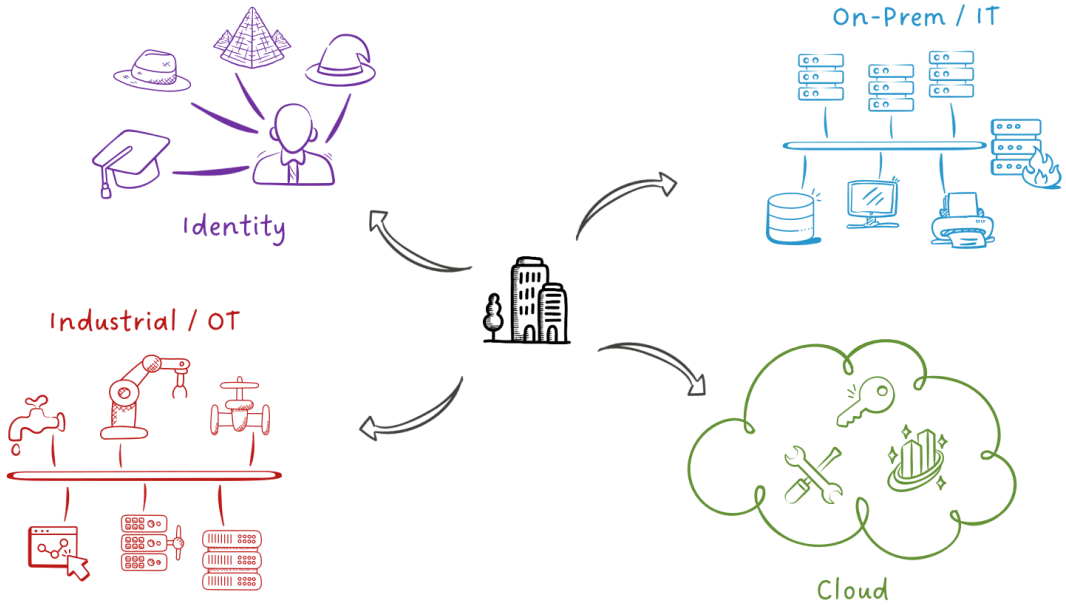
Alert & Report

- Zielgruppenorientierte Dashboards & Reports
- Alarmierung bei kritischen Schwachstellen

Exposure Management – Die moderne Angriffsoberfläche

Ganzheitliche Herausforderungen

- Übergreifende Sichtbarkeit der Assets, Identitäten, Ressourcen und Schwachstellen
- Kontinuierliche Erfassung von Schwachstellen verschiedener Angriffsoberflächen
- Priorisierung und systematische Reduzierung von Risiken



First Stop: Cloud

Arbeitsbereich

- Multi-Cloud-Infrastruktur mit einer gemeinsamen / geteilten Security-Verantwortung
- Schnell wachsende Umgebung mit vielen Ressourcen und Identitäten
- Schatten-IT und mangelnde Sichtbarkeit

Crew & Technik

- Haben Sie Fehlkonfigurationen in der Cloud-Infrastruktur?
- Ist eine vollständige Visibilität von den Workloads bis zu den Identitäten vorhanden?
- Besteht die Möglichkeit zur kontextbasierten Priorisierung der Security Findings?

Ausstattung

- Cloud Security Assessment
- Cloud-Native Application Protection Platfrom (CNAPP)

Second Stop: Identitäten

Arbeitsbereich

- Das Herzstück der IT-Infrastruktur
- Historische gewachsene Infrastruktur
- Hochdynamische Umgebung mit einer Vielzahl von Benutzern und Gruppen

Crew & Technik

- Erfüllen Sie die aktuellen Sicherheitsrichtlinien und Security Best Practices?
- Sind Ihnen die überprivilegierten Gruppen / Benutzer bekannt?
- Haben Sie die Möglichkeit einen laufen Angriff auf die Identitäten zu erkennen?

Ausstattung

- Active Directory und Microsoft Entra ID Penetrationstest
- Identity Exposure / Exposure Management Plattform

Third Stop: Perimeter

Arbeitsbereich

- Potenziell von außen und für alle erreichbare Systeme
- Systeme stehen dauerhaft unter Beobachtung
- Über die Jahre gesammelte Systeme

Crew & Technik

- Kennen Sie alle registrierten Domains und Netzbereiche?
- Werden die Systeme täglich auf Schwachstellen und Fehlkonfigurationen untersucht?
- Erkennen Sie zeitnah einen Angriff auf diese Systeme?

Ausstattung

- Security Assessment / Penetrationstest
- Kontinuierliches Attack Surface Management und Vulnerability Management

Fourth Stop: Künstliche Intelligenz

Arbeitsbereich

- „Security-Neuland“
- Gesamte IT-Landschaft, von On-Premises bis SaaS
- Künstliche Intelligenz wird zu einer weiteren Angriffsoberfläche

Crew & Technik

- Welche KI-Lösungen befinden sich im Einsatz?
- Können Sie die nicht genehmigten KI-Lösungen identifizieren?
- Wie schützen Sie sich vor „der KI“ und den anfallenden Sicherheitsrisiken?

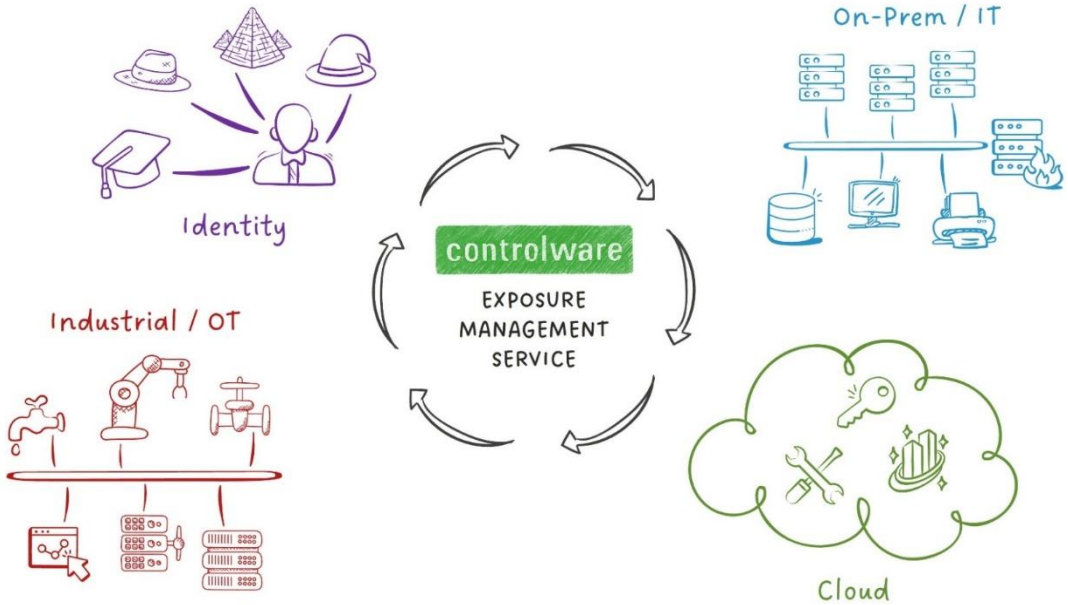
Ausstattung

- Penetrationstest / Shadow AI Assessment
- AI Exposure

Exposure Management – Die moderne Angriffsoberfläche

Exposure Management

- Übergreifende Sichtbarkeit der Assets, Identitäten, Ressourcen und Schwachstellen
- Kontinuierliche Erfassung von Schwachstellen verschiedener Angriffsoberflächen
- Priorisierung und systematische Reduzierung von Risiken



IT-Security
Roadshow 2026

controlware

Danke für Ihre Aufmerksamkeit.