controlware

Controlware GmbH

IT-Sicherheit – Cyber Security

3 Schritte zum Schutz vor Cyber Security-Risiken

www.controlware.de ■ blog.controlware.de

Verfasser: Christian Bohr, Controlware GmbH

Klassifizierung: EXTERN

Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Telefon +49 6074 858-00
info@controlware.de
www.controlware.de
blog.controlware.de

Sitz: Controlware GmbH Kommunikationssysteme ■ Waldstraße 92 ■ 63128 Dietzenbach ■ GERMANY
Tel. +49 6074 858-00 ■ Fax +49 6074 858-108 ■ info@controlware.de ■ www.controlware.de
Sitz Dietzenbach ■ Registergericht Offenbach a.M. ■ HRB Nr. 6431 ■ USt-IdNr. DE 113 539 225 ■ Steuernummer 3523035235
Geschäftsführer: Bernd Schwefing

3 Schritte zum Schutz vor Cyber Security-Risiken

Wie wichtig IT-Security für alle Unternehmen ist, sollte jedem IT-Verantwortlichen inzwischen bewusst sein. Dazu tragen zweifelsohne schon die zahlreichen Berichte über Cyber-Angriffe und Schäden durch Malware in den Medien bei. Nachfolgend soll in 3 Schritten aufgezeigt werden, wie eine strukturierte Vorgehensweise aussehen kann.

Schritt 1: Bewerten Sie Ihre individuelle Situation

Zuerst ist es wichtig, die eigenen Beweggründe ehrlich zu hinterfragen: Sind überwiegend externe Compliance-Anforderungen der Treiber oder ist der bestmögliche Schutz vor Cyber-Gefahren das Ziel?

Nach wie vor wird die IT-Security häufig als begleitende Maßnahme zur Erreichung von Zertifizierungen wie ISO 27001 oder TISAX gesehen oder dient der Erfüllung gesetzlicher Verordnungen wie dem IT-Sicherheitsgesetz oder der KRITIS-Verordnung. Ist dies der Fall, liegt der Fokus meist auf der Erfüllung der jeweiligen Mindestanforderungen und das Budget wird sich demzufolge am Notwendigen und nicht am Machbaren orientieren. In diesen Fällen finden sich in Schritt 2 geeignete Hinweise. Wird Cyber Defense von der Unternehmensleitung strategisch gesehen und ein hohes oder sehr hohes Schutzniveau angestrebt, finden sich in Schritt 3 Hinweise auf wirkungsvolle Maßnahmen.

Unabhängig von den Beweggründen geht es in Schritt 1 zunächst darum, bestehende Sicherheitskonzepte und -Maßnahmen zu dokumentieren. Eine Reifegrad-Analyse zeigt momentane Stärken und Schwächen in der Cyber-Sicherheit des Unternehmens auf. Auf dieser Basis kann ein Leitfaden mit Checkliste als valide Entscheidungsgrundlage erstellt werden. Unterstützung bieten in dieser Phase auch Compromise Assessments. Diese liefern nicht nur Informationen zur individuellen Sicherheitslage, sondern helfen auch, geeignete Maßnahmen festzulegen und zu priorisieren.

Schritt 2: Setzen Sie Mindestanforderungen um

Auf Basis der Bewertungen lassen sich in Schritt 2 erste Maßnahmen zur Verbesserung des Sicherheitsniveaus durchführen. In praktisch allen Zertifizierungsanforderungen wird eine Sammlung und strukturierte Auswertung von Logdaten sowie eine regelmäßige Überprüfung auf Schwachstellen gefordert. Die genaue Ausgestaltung mag unterschiedlich sein, allerdings werden diese beiden Maßnahmen zur aktiven Erkennung von Schwachstellen und Anomalien grundsätzlich gefordert.

SIEM-Lösungen

Die Mindestanforderung bei der Einführung von SIEM-Lösungen besteht darin, Verstöße gegen Compliance-Richtlinien oder Auffälligkeiten im Benutzerverhalten zu erkennen, die auf Security Incidents hindeuten. Somit lässt sich eine Basisüberwachung sicherstellen, jedoch keine vollständige Erkennung von Cyber-Gefahren. Professionelle SIEM-Anbieter verfügen meistens über Use Case-Kataloge, die eine Auswahl entsprechend den jeweiligen Anforderungen erlauben.

Schwachstellen-Management

Vulnerability Management- oder Schwachstellen-Management-Lösungen überwachen die IT-Infrastruktur regelmäßig aktiv auf bekannte Schwachstellen. Es wird eine transparente Sicht auf vorhandene Schwachstellen und damit verbundene Risiken erreicht, gleichzeitig wird die Grundlage für eine strukturierte Bearbeitung geschaffen. Das Ergebnis – ein kontinuierlich steigendes Sicherheitsniveau. Zusätzlich lassen sich neu aufgetretene Schwachstellen schnell identifizieren.

Vulnerability Management-Lösungen liefern jedoch selbst bei kleineren Unternehmensgrößen eine sehr hohe Anzahl von Schwachstellen, deren Bearbeitung und Beseitigung die Kunden-IT oft vor unüberwindbare Hürden stellt. Aus diesem Grund ist die Realisierung als Managed Service zu empfehlen, wobei insbesondere darauf zu achten ist, dass der Anbieter neben dem Betrieb auch die Bewertungen und Priorisierungen der Schwachstellen übernimmt.

Schritt 3: Schützen Sie sich umfassend

Der nächste große Schritt hin zu einem umfassenden Schutz vor Cyber-Gefahren stellt die professionelle, kontinuierliche Bewertung und Priorisierung durch Security-Analysten im Security Operations Center (SOC) dar.

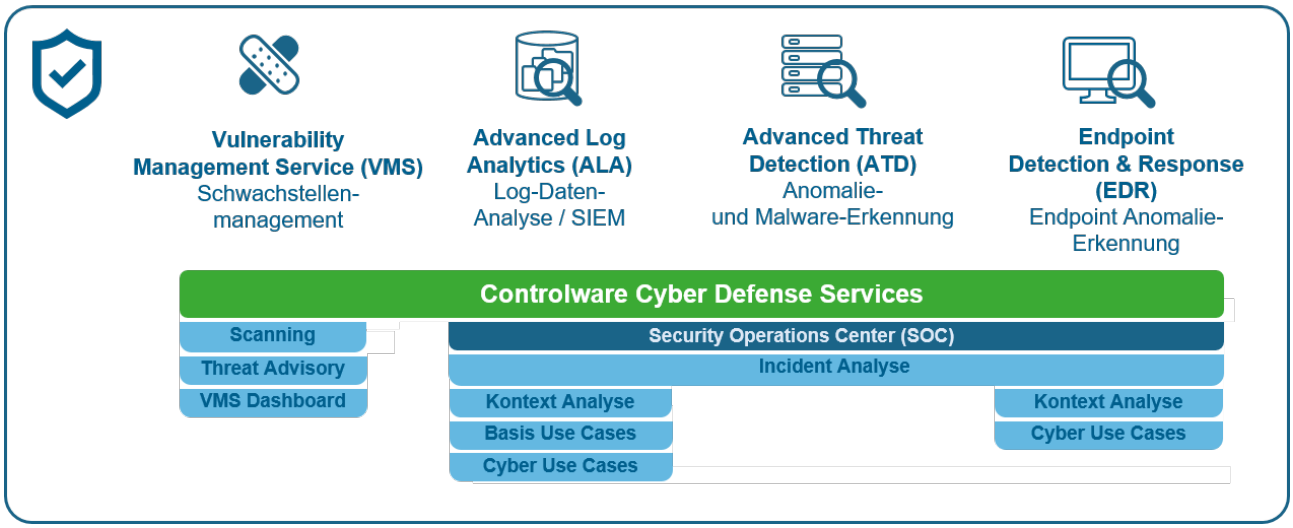
Wurde bereits eine SIEM-Plattform implementiert, lässt sich diese verhältnismäßig einfach erweitern, um die typischen Angreifer-Techniken in den unterschiedlichen Phasen eines Cyber-Angriffs zu erkennen. Für die Erkennung sind jedoch erweiterte Logquellen wie Sysmon- oder Powershell-Logs erforderlich. Alternativ oder in Ergänzung ist es ratsam, auch KI-basierte Ansätze zur Anomalie-Erkennung zu berücksichtigen. Endpoint-basierte Detection & Response-Lösungen gewinnen dabei deutlich an Bedeutung. Zum einen kann am Endpoint unverschlüsselter Datenverkehr analysiert werden, zum anderen lässt sich die Erkennung von Angreifern und Malware deutlich vereinfachen, da Informationen zu aktiven Prozessen und Usern vorliegen.

In der Regel ist der Betrieb eines SOC für Unternehmen sehr anspruchsvoll und in den meisten Fällen auch unwirtschaftlich. Daher ist es sinnvoll, qualifizierte Security-Analysten im Rahmen eines Managed Service für die Bewertungen und Priorisierungen einzusetzen. Diese verfügen über ein profundes Verständnis der Angreifer-Techniken und gleichzeitig über Erfahrungen in Bezug auf Angriffsreaktionen. Ein weiterer Vorteil von Managed Services besteht darin, dass Service Provider auf Erkenntnisse aus anderen Kundenumgebungen zurückgreifen und die weltweite Bedrohungslage bei der Bewertung von Incidents berücksichtigen können. Somit sind sie häufig in der Lage, den Schadenseintritt bereits präventiv zu verhindern.

Zusammenfassung:

- Die richtige Herangehensweise an Cyber Defense ist vom individuellen Motiv abhängig.
- Cyber-Security-Checks helfen, den eigenen Reifegrad zu ermitteln und die weiteren Schritte zu planen.
- Modulare Lösungen lassen sich sinnvoll erweitern und schützen bereits getätigte Investitionen.
- Managed Services tragen dazu bei, den betrieblichen Aufwand zu minimieren und die Bewertung und Priorisierung von Security Incidents zu verbessern.

Cyber Defense Services – Managed Service Lösungsportfolio



Unsere Standorte

Zentrale
Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf:

Deutschland

Berlin
Tel. +49 30 67097-0
info-ber@controlware.de

Düsseldorf
Tel. +49 2159 9696-0
info-due@controlware.de

Frankfurt/Main
Tel. +49 6074 858-206
info-ffm@controlware.de

Hamburg
Tel. +49 40 251746-0
info-ham@controlware.de

Hannover
Tel. +49 511 726092-0
info-han@controlware.de

Ingolstadt
Tel. +49 841 23222-0
info-ing@controlware.de

Kassel
Tel. +49 561 47576-0
info-kas@controlware.de

Leipzig
Tel. +49 341 98387-30
info-lei@controlware.de

München
Tel. +49 89 666367-0
info-muc@controlware.de

Stuttgart
Tel. +49 711 770568-0
info-stu@controlware.de

Wolfsburg
Tel.: +49 5362 9993413
info-wey@controlware.de

Österreich

Graz
Tel. +43 1 890 0724-0
info@controlware.at

Innsbruck
Tel. +43 512 345200
info@controlware.at

Wien
Tel. +43 1 890 0724-0
info@controlware.at

Schweiz

Zürich
Tel. +41 55 4156476
info@controlware.ch