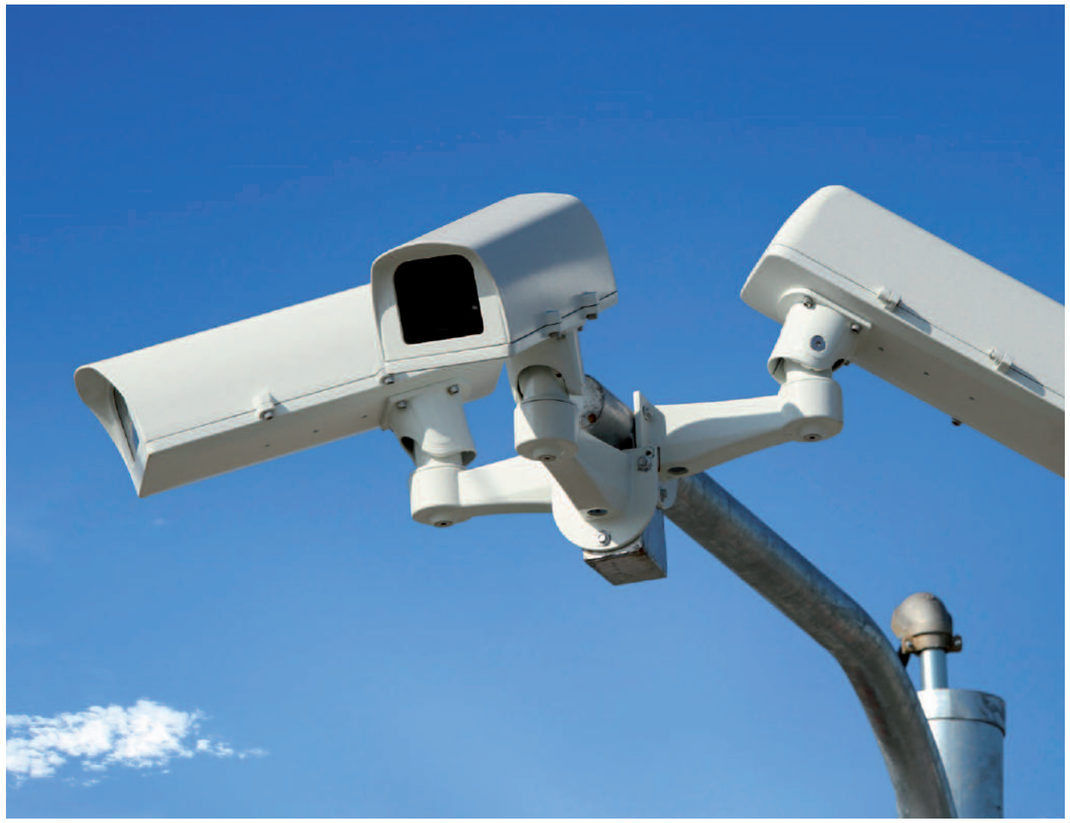

Bild: Shutterstock/Winai Tepsuttinun

Umfassendes Sicherheitskonzept

# Alles im Auge behalten

Heute ist jeder Tag ein Zero Day. Unternehmen brauchen einen weit gefassten, systematischen Sicherheitsansatz. Ein Überblick über die wichtigsten Bausteine. **Von Markus Limacher**

Meldungen zu Hackerangriffen, Ransomware, APT-Angriffen oder DDoS-Attacken nehmen kein Ende. Betroffen sind längst nicht mehr nur globale Grosskonzerne, sondern vermehrt auch Schweizer Unternehmen. Erfolgreiche Angriffe zeigen immer wieder, wie geschickt Cyber-Kriminelle in vermeintlich geschützte Netze eindringen, um vertrauliche Informationen zu stehlen oder die Systeme zu sabotieren. Solche Vorfälle sind mehr als nur ärgerlich: Sie können enorme Kosten und Imageschäden nach sich ziehen. Und die Bedrohungen für vertrauliche Firmendaten durch Cyber-Angriffe nehmen weiter zu. Die Unternehmen müssen sich bewusst werden, dass es auch sie treffen kann. Dabei gilt es, dafür zu sorgen, dass die Folgen so gering wie nur irgendwie möglich ausfallen – verhindern lassen sich Angriffe nicht.

## Cyber Security mit System

Um sich konsequent mit aktuellen und neuen Risiken auseinanderzusetzen und der Informationssicherheit die nötige Relevanz beizumessen, können sich Unternehmen an internationalen Standards orientieren. ISO/IEC 27001 oder NIST Cyber Security Frameworks bieten anerkannte Modelle für die Errichtung, Umsetzung, Überprüfung und kontinuierliche Verbesserung der Cyber Security, basierend auf einem Informationssicherheits-Management-System (ISMS). Dabei werden alle drei Dimensionen der Cyber Security betrachtet und einbezogen: die Technologie, die Prozesse und nicht zuletzt den Menschen.

Die Einführung eines ISMS hilft Unternehmen, das Sicherheitsniveau systematisch zu verbessern und dabei von Good-Practice-Ansätzen zu profitieren. Zu den Massnahmen zählen ein gezieltes Risikomanagement, der Aufbau eines Sicherheitskonzeptes und einer Sicherheitsarchitektur, die Definition von Sicherheitsrichtlinien und -prozessen, welche den (ICT-) Sicherheitsmassnahmen Ordnung und Führung verleihen, sowie der Aufbau eines Notfallplans und die Sicherheitssensibilisierung der Mitarbeitenden.

Der Architektur innerhalb des Unternehmensnetzwerks kommt dabei eine enorme Bedeutung zu. Einer der wichtigsten Aspekte neben der Systemredundanz stellt die optimale Segmentierung der Netzwerke und Überwachung der damit geschaffenen Zonenübergänge dar, welche die Business-Prozesse optimal abdeckt und unterstützt.

## Schwachstellen-Management

In der Vergangenheit haben sich viele Unternehmen darauf konzentriert, Cyber-Risiken zu identifizieren und entsprechende Sicherheitsmassnahmen zu integrieren. Aber auch ein ausgeklügeltes Sicherheitsdispositiv bringt nichts, wenn (Sicherheits-)Systeme und Applikationen verwundbar sind. Viele erfolgreiche Angriffe in jüngerer Vergangenheit nutzten Schwachstellen in ICT-Komponenten, die seit mehr als einem Jahr bekannt waren. Dies zeigt, wie wichtig – nebst geeigneten Sicherheitssystemen – ein funktionierendes Schwachstellen-Management ist.

Die Bedrohungslage ändert sich stetig. Aus diesem Grund sind regelmässige Überprüfungen des Sicherheitsdispositivs unerlässlich. Zur Kontrolle sollten, zusätzlich zu den erwähnten Vulnerability Scans, regelmässig System Audits, Penetration Tests oder gar eine simulierte Cyber-Attacke durchgeführt werden. Nur so kann die Sicherheit an die aktuelle Risikosituation angepasst und optimiert werden. Natürlich garantiert auch dies keinen hundertprozentigen Schutz vor Eindringlingen, doch werden damit die Eintrittsbarrieren erheblich erhöht.

## Aufdecken und reagieren

Zusätzlich zu hohen Mauern und einem funktionierenden Schwachstellen-Management braucht es Konzepte zur Detektion und zur schnellen Reaktion auf Angriffe. Dies ist entscheidend, um das Schadensausmass auf ein Minimum zu reduzieren.

Eine gute Möglichkeit, um Angreifer nach einem erfolgreichen Angriff aufzuspüren, bieten Breach-Detection-Lösungen, bei denen der Netzwerkverkehr mittels Data Science, maschinellem Lernen und Verhaltensanalysen durchsucht und ausgewertet wird. Moderne und professionelle Network-Behavior-Analysesysteme geben Sicherheitsverantwortlichen den notwendigen Überblick, um schnell auf Bedrohungen zu reagieren.

Retrospektive Informationen helfen darüber hinaus, sich schnell ein Bild der im Angriff involvierten Prozesse zu machen. So lässt sich die Infrastruktur im Bedarfsfall flächendeckend nach «Indicators of Compromise» (IoC) durchsuchen. Solche Indikatoren sind beispielsweise Prozess- und File-Hashes, Verzeichnispfade oder auch involvierte, externe IP-Adressen.

**«Ein systematisches Vorgehen bezieht alle drei Dimensionen der Cyber Security ein: die Technologie, die Prozesse und den Menschen»**

**Markus Limacher**

Um all diese Aufgaben erfolgreich zu meistern, empfiehlt es sich, ein Team von Experten und entsprechende Tools zur Breach Detection, für das Security Information & Event Management (SIEM), aber auch für den Incident Response in einem dedizierten Cyber Defence Center zu vereinen. Security Operation ist jedoch eine anspruchsvolle Arbeit und benötigt hochspezialisierte Skills. Der Betrieb dieser Infrastruktur ist zudem zeitintensiv. Oftmals fehlt es Unternehmen dafür schlicht an Ressourcen. Abhilfe schaffen da professionelle Services von spezialisierten Anbietern. Dort setzen sich Analysten tagtäglich mit der aktuellen Bedrohungslage auseinander. So können Unternehmen von der grossen Erfahrung profitieren, ohne ein eigenes Cyber Defence Center aufbauen zu müssen.

## Fazit: Fokus erweitern

Unternehmen müssen davon ausgehen, dass ihre Systeme bereits infiltriert sind oder sie früher oder später Opfer einer Attacke werden. Daher ist es wichtig, eine Infiltration zu erkennen und schnell darauf zu reagieren. Rein präventive Massnahmen greifen heute eindeutig zu kurz. Ein systematischer Sicherheitsansatz, der sowohl das Risikomanagement, den Schutz der Informationen, die Erkennung und Reaktion auf Sicherheitsvorkommnisse sowie die Wiederherstellung und Optimierung berücksichtigt, ist heute das A und O einer erfolgreichen Cyber Security Strategie. ■

**Markus Limacher**
ist Principal Cyber Security Consultant bei InfoGuard AG:
**www.infoguard.ch**