CYBER DEFENCE BESCHRÄNKT SICH NICHT NUR AUF TRADITIONELLE IT INFRASTRUKTUREN

Hacker machen auch vor kritischen Infrastrukturen nicht halt. Wenn es dabei um die Sicherheit geht, dürfen keine Kompromisse eingegangen werden – ansonsten drohen kritische Situationen wie ein «Blackout». Den Fokus nur auf präventive Massnahmen zu legen, wäre zu kurz gegriffen. Ein systematischer Sicherheitsansatz, der sowohl das Risikomanagement, den Schutz der Informationen, die Erkennung und Reaktion auf Sicherheitsvorkommnisse und die Wiederherstellung und Optimierung berücksichtigt, ist heute das A und O einer formulierten und erfolgreichen Cyber Security Strategie.

von Markus Limacher

Betreiber von kritischen Infrastrukturen, egal ob in den Bereichen Energie, Wasser oder Verkehr, etc. sind auf funktionierende Systeme der IT und der OT (Operational Technology) angewiesen. Dabei darf man sich aber nicht nur auf die traditionelle IT-Landschaft konzentrieren. Denn gerade ICS- und SCADA-Systeme benötigen durch die Zunahme der Cyber Bedrohung und Vernetzung in der Wertschöpfungskette einen umfassenden Schutz. Bislang bewegten sich solche Leit- und Steuerungs-Systeme in einer eigenen Welt proprietärer Protokolle, auf speziellen Plattformen und einer darauf zugeschnittenen Kommunikationsinfrastruktur. Sie waren von anderen Netzwerken – einschliesslich dem Internet – meistens isoliert. Heutzutage müssen Daten immer häufiger über Unternehmensgrenzen hinweg ausgetauscht werden, weil verschiedene Parteien Teiltätigkeiten übernommen haben, die früher an einer Stelle gebündelt waren. Die zunehmende Interoperabilität in der Wertschöpfung bietet ein wirtschaftlich enormes Potential, birgt aber auch Risiken und Gefahren.

CYBER SECURITY MIT SYSTEM

Seit Jahren hat sich in der Unternehmenswelt das Thema Cyber Security auf der Basis des ISO/IEC 27001 Standards oder des NIST Cyber Security Frameworks etabliert. Aber auch Betreiber kritischer Infrastrukturen sind gut beraten, sich konsequent mit aktuellen und neuen Risiken auseinander zu setzen und der Informationssicherheit das nötige Gewicht beizumessen. Internationale Standards bieten dazu ein anerkanntes Modell für die Errichtung, Umsetzung, Überprüfung und kontinuierlichen Verbesserung auf der Basis eines Informationssicherheits-Management-Systems (ISMS). Gleichzeitig werden die drei Dimensionen der Cyber Security beleuchtet – Technologie, Prozesse und nicht zuletzt der Mensch.

Die Einführung eines ISMS z. B. nach ISO/IEC 270xx oder NIST hilft Betreibern von kritischen Infrastrukturen, das Sicherheitsniveau systematisch zu steigern und dabei von Good Practice-Ansätzen zu profitieren. Es hat sich gezeigt, dass gerade das systematische Vorgehen einen erheblichen Mehrwert bietet. Dazu zählen u. a. ein gezieltes Risikomanagement, der Aufbau eines angemessenen Sicherheitskonzeptes und einer geeigneten Sicherheitsarchitektur, die Definition der Sicherheitsorganisation, -richtlinien und -prozessen, welche den (ICT-) Sicherheitsmassnahmen eine Ordnung und Führung verleihen, sowie der Aufbau einer Notfallplanung und die Sicherheitssensibilisierung der Mitarbeitenden.

CYBER DEFENCE IST MEHR ALS EINE HOHE (SICHERHEITS-)MAUER

Unternehmen können und müssen sich auf Cyber-Attacken vorbereiten – dies gilt insbesondere auch für Betreiber kritischer Infrastrukturen. Der Schutz der Netzwerke und der Informationen wird aber immer schwieriger – insbesondere der Schutz vor anspruchsvollen Attacken, die durch herkömmliche Sicherheitssysteme nicht mehr erkannt werden.

Der Architektur von ICS- und SCADA-Systemen innerhalb des Unternehmensnetzwerks kommt eine enorme Bedeutung zu. Einer der wichtigsten Aspekte neben der System-Redundanz stellt dabei die optimale Segmentierung der Netzwerke, Betriebsfunktionen, Einzelelemente und Überwachung der so geschaffenen Zonenübergänge dar, welche die Business-Prozesse optimal abdeckt und unterstützt.

Es gilt verschiedene Verteidigungslinien (Lines of Defense) aufzubauen. Zu diesen zählen die Verbindung der kritischen Infrastrukturen und der ICT mit einer End-zu-End-Sicherheit, kontrollierte Remote-Zugänge für Lieferanten und Partner, einem Perimeter-Schutz bestehend u. a. aus Firewalls, dem Intrusion Detection/Prevention System, einem VPN und geschützte Netzwerk- und Zonenübergänge sowie einem umfassenden Malware-Schutz auf vernetzten und geschlossenen Systemen. Den Fokus nur auf den Perimeter zu legen, wäre zu kurz gegriffen.

CYBER ATTACKEN ABZUWEHREN REICHT NICHT MEHR AUS

Heutzutage muss man davon ausgehen, dass bereits ein Angriff und damit verbunden eine Infiltration stattgefunden hat. Es geht somit darum, diese umgehend zu erkennen, schnell darauf zu reagieren und anschliessend die Sicherheitsmassnahmen gezielt zu optimieren. Dies schafft man aber nicht ohne technologische Unterstützung in Form einer zentralen Security Intelligence Plattform und entsprechenden Agenten auf den Endgeräten. Sie sammelt automatisch alle Informationen aus den Infrastrukturkomponenten, vergleicht diese mit externen Threat Feeds und untersucht sie

in Echtzeit auf Angriffe. Ergänzt wird dieses System mit Breach Detection Systemen, welche den Datenverkehr mit Hilfe von Data Science, maschinellem Lernen und Verhaltensanalysen durchsuchen und auswerten. Wird ein Angriff erkannt oder befindet sich ein Angreifer bereits im internen Netz, muss ein Unternehmen in der Lage sein, schnell zu reagieren. Dazu braucht es retrospektive Informationen. Nur so lässt sich die gesamte Infrastruktur flächendeckend nach «Indicators of Compromice» (IOC) wie Prozess-, File-Hashes, Directory Pfade oder involvierte externe IP-Adressen, etc. durchsuchen.

GEZIELTE OPTIMIERUNG UND SCHWACHSTELLENBESEITIGUNG

Die Risikosituation und Bedrohungslage ändert sich stetig. Aus diesem Grund sind regelmässige Überprüfungen des Sicherheitsdispositivs nach neuen Bedrohungen und Schwachstellen unerlässlich. Zur Kontrolle sollten regelmässig System Audits, Penetration Tests und Vulnerability Scans durchgeführt werden. Nur so kann die Sicherheit an die aktuelle Risikosituation angepasst und optimiert werden.

IN DER HEUTIGEN WELT IST JEDER TAG EIN «ZERO DAY»

Eine effiziente und zuverlässige Cyber Security muss auf verschiedenen Lösungen und Ansätzen wie Perimeter Security, Sandboxes und Malware-Protection aufbauen; kombiniert mit Cyber Defence Services, wie APT Detection & Response, Cyber Threat Intelligence und der systematischen Analyse von Bedrohungen mittels SIEM- und Incident Response. Nur so lässt sich die «Nadel im Heuhaufen» finden und beseitigen.

Betreiber von Infrastrukturen sind gut beraten, die bewährten Best Practice-Ansätze der Cyber Security auch auf die ICS- und SCADA-Netze zu adaptieren. Die Cyber Security Strategie bildet dabei den bereichsübergreifenden, strategischen Rahmen. Sie sollte die Ziele und Massnahmen zur Verbesserung der Cyber-Sicherheit für Anwender fassbar, nachvollziehbar und schlussendlich auch umsetzbar machen. Denken Sie daran: Hackerangriffe sind nicht nur ärgerlich, sondern können auch enorme Kosten und einen riesigen Imageschaden verursachen.

KONTAKT AUTOR

Markus Limacher
Principal Cyber Security Consultant
InfoGuard AG

www.infoguard.ch