Viele Wege führen zur Unternehmenssicherheit

consistec – Ihr Partner für IT/OT-Security

Für Unternehmen stellen neben technischen Problemen Cyber-Attacken ein immer größer werdendes Risiko für den Ausfall von IT-Systemen dar. War man bisher noch nicht Opfer einer Cyber-Attacke, setzt Virenschutz-Software ein und schützt den Unternehmensperimeter durch eine halbwegs aktuelle Firewall, ist man schnell verleitet, sich sicher zu fühlen. Ein trügerisches Gefühl.
Durch stetig steigende Komplexität von IT- und OT-Infrastrukturen und wachsende Datenraten wird es immer schwerer, den Überblick zu behalten, was im Netzwerk tatsächlich passiert. Zudem steigt laut dem Bundesamt für Sicherheit in der Informationstechnik die Bedrohung durch Internet-Kriminalität stetig (BSI – Überblick IT-Grundschutz und ICS Bedrohungen 2019). Angreifer bleiben in der EMEA-Region im Durchschnitt 106 Tage unentdeckt (Fireeye M-Trends Report 2017).

Unternehmenssicherheit – womit sollte man anfangen?

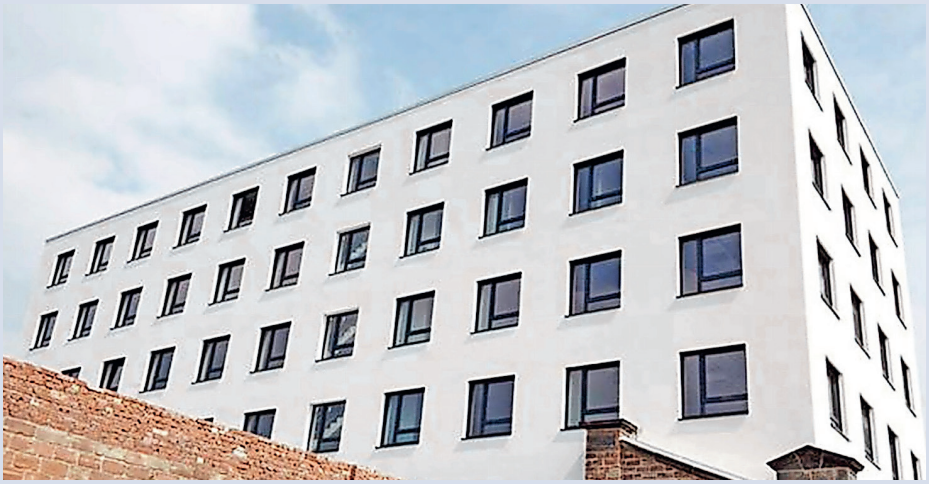
Zu diesen Fragen findet man beim BSI (IT-Grundschutz, Standards 200-1, 200-2, 200-3) oder beim National Institute of Standards and Technology (NIST) Antworten. Eine andere Möglichkeit ist, sich an den ISO/IEC 2700x Standards zu orientieren oder spezialisierte Dienstleister zu beauftragen. Egal welchen Standard man für die eigenen Maßnahmen heranzieht, man muss sowohl organisatorische als auch technische Maßnahmen treffen.

Initiale Maßnahmen

Zuerst geht es darum, eine Bestandsaufnahme zu machen und herauszufinden, welche Systeme in der IT/OT-Infrastruktur vorhanden sind, welche Anbindungen zum Internet oder anderen Standorten bestehen, welche Mitarbeiter für die Systeme zuständig sind. Daraus ergeben sich weitere Fragen: Wer hat Zugriff? Welcher Softwarestand läuft auf den Systemen? Werden zeitnah Sicherheits-Updates aufgespielt? Welche Systeme sind essentiell und besonders schützenswert? Wo könnte Know-how abfließen? Wie und in welchem Turnus werden Daten gesichert? Welche Systeme steuern die Produktion? Gibt es Schwachstellen und wie kritisch sind diese?

Die „Schwachstelle Mensch“

Parallel zur Bestandsaufnahme können bereits Awareness-Trainings für Mitarbeiter gestartet werden, um im Unternehmen ein Bewusstsein für IT/OT-Security zu erzeugen und um auf typische Gefahren, die mit der „Schwachstelle Mensch“ einhergehen, aufmerksam zu machen.



Der Firmensitz der consistec Engineering & Consulting GmbH am Standort Europaallee 5 in Saarbrücken. Foto: privat

Sinnvolle Schutzmaßnahmen

Wenn die Risiken bekannt und bewertet sind, können sinnvolle Schutzmaßnahmen erfolgen. Da Angreifer in der Regel sehr ökonomisch vorgehen, ist neben dem Einsatz einer professionellen Firewall und dem Einsatz von Virenschutzsoftware die Beseitigung von Schwachstellen ein naheliegender erster Schritt. Je weniger Schwachstellen, desto uninteressanter sind Unternehmen für den „Typischen Angreifer“.

Technische Hilfsmittel

Um einen Überblick über das, was in der IT-Infrastruktur passiert, zu bekommen, benötigt man technische Hilfsmittel: Monitoring-Systeme. Dabei variieren technische Konzepte, Lizenzkosten, Kosten für Dienstleistungen, Analysetiefe und -breite sowie Beherrschbarkeit für die Anwender bei unterschiedlichen Herstellern und Produktgruppen stark. Die Orientierung in diesem Technik-Labyrinth ist nicht einfach.

NIST National Institute of Standards and Technology	caplon©-Tools
IDENTIFY	service monitoring
PROTECT	
DETECT	service monitoring security monitoring
RESPOND	
RECOVER	

Sicherheitsempfehlungen des US National Institute of Standards and Technology (NIST)

Was das BSI empfiehlt: Anomalie-Erkennung

Seit diesem Jahr gibt es erstmals eine konkrete Empfehlung des BSI für Monitoring-Systeme im Bereich Produktionsnetzwerke (BSI-CS 134), die aber genauso für den Office-IT-Bereich sinnvoll ist: Der Einsatz von Systemen, die Anomalien erkennen können. Derartige Systeme überwachen das Verhalten in IT/OT-Infrastrukturen und ermöglichen es, auch neuartige Angriffe zu erkennen – im Gegensatz zu signaturbasierten Ansätzen, die nur bei bereits bekannten Angriffen funktionieren.

IT-Security – Made in Saarland

consistec Engineering & Consulting GmbH entwickelt seit 2001 Systeme zur Erfassung und Analyse von Netzwerkdaten. Die caplon© Produktlinie bietet Monitoring für die Anwendungsbereiche Network & Service, VoIP und IT/OT-Security. Das modulare Konzept ermöglicht in Kombination mit einem einfachen Lizenzmodell einen smarten Einstieg. Vorgaben der DSGVO werden durch innovative technische Konzepte eingehalten. Im Bereich Security liegt der Produkt-Fokus auf passiver Schwachstellenerkennung, auf Anomalie-Erkennung unter Einbeziehung von über 4 Mio. Netzwerkparametern und auf der Erkennung von Advanced Persistent Threads auf Basis von Deep Packet Inspection. Damit können auch kleinere IT/OT-Teams mit leistungsfähigen, beherrschbaren Monitoring-Systemen unterstützt werden.

red.

www.consistec.de