IS/IT-SICHERHEIT

Sicherheit für KRITIS-Branchen

Sicherheit ist Existenz- und Wettbewerbsfaktor

Die Sicherheit und Verfügbarkeit von Anlagen, Informationen und die von technischen Systemen stellt eine der zentralen Aufgabenstellungen der digitalen Welt, heute und in Zukunft, dar. Insbesondere für KRITIS-Branchen gelten, wegen ihrer tragenden gesellschaftlichen Funktionen und der daraus erwachsenen außerordentlichen Verantwortung, deutlich höhere Anforderungen.

Sicherheitsstrategie und -konzept erforderlich

Das Erreichen eines hohen Sicherheitsniveaus stellt einen sukzessiven, lebendigen Prozess dar, für dessen Umsetzung es erfahrener Spezialisten bedarf. Adhoc-Maßnahmen erbringen nur minimale Effekte, was am Beispiel von 400.000! täglich neu hinzukommenden Schadcodeprogrammen verdeutlicht werden soll. Neben Schadprogrammen existieren eine Vielzahl weiterer, diffiziler Penetrations- und Störereignisse im Zusammenwirken Mensch, Unternehmen und Digitaler Raum. Zur wirksamen Absicherung bedarf es neben einer Digitalstrategie eines fundierten Sicherheitskonzeptes, welches die Grundlage für alle digitalen und existentiellen Funktionsprozesse des Unternehmens bildet.

Architektur & Schutz: Digitaler Raum

Wind- und Regenschutzkonstruktionen sowie Abdeckungen aus Zweigen und Blättern wurden bereits von den Ur-Menschen beim Bewohnen bzw. Bewohnbarmachen von Höhlen verwandt, um sich gegen Witterung, Tiere, andere Artgenossen bzw. Gruppierungen zu schützen bzw. sich eine Privatsphäre zu schaffen (…).
Die „schützende Haut“ richtet sich nach den Proportionen und Skalierungen derjenigen, welche Schutz benötigen.

Ein vollständiges Sicherheitskonzept betrachtet auch die Standort-, Objekt- und Personalsicherheit. Ebenso bedarf es eines Havarie- und Notfallkonzeptes bei möglichem Eintritt eines Störereignisses und den dann erforderlichen Prozessketten, bis hin zur Einschränkung bzw. Einstellung digitaler Services sowie Regeln zu Verhaltensweisen und zur weiteren Austauschkommunikation mit Kunden- und Verbundpartnern.

Das Fundament von Sicherheit

- Bewusstsein,
- Unternehmensstrategie,
- Budgetmittel,
- Prozesse,
- Technologieeinsatz,
- Überwachung,
- Verbesserung.

Eine Übersicht zum Einsatz verfügbarer und wirksamer Technologien zur Schadcode- und Störereignis-Abwehr sowie zur Wahrung der Informationssicherheit, des Datenschutzes und der Systemintegritäten gibt auszugsweise die nachfolgende Übersicht:

- Firewall,
- Web Proxy, Email Proxy,
- Email-Verschlüsselung,
- Laufwerks- und Container-Verschlüsselung,
- Zonierung bzw. Isolierung,
- Datenschleuse (Diode),
- Multiple Antimalware Engines, Multi-Scanning,
- Quarantäne, Desinfektion,
- (Advanced) Threat Protection (ATP),
- Ausbreitungseindämmung,
- Monitoring, Alarmierung.
- Zentrale Policierung (Server-Richtlinien, Softwarerollout),
- Inhaltsanalyse (CDR),
- Datenabflusskontrolle,
- Deep Learning (maschinelle Analyse), u.v.m.

Sicherheit: Definition

Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken ist oder als gefahrenfrei angesehen wird. Mit dieser Definition ist Sicherheit sowohl auf ein einzelnes Individuum als auch auf andere Lebewesen, auf unbelebte reale Objekte oder Systeme wie auch auf abstrakte Gegenstände bezogen.

Diese beispielhaft aufgeführten Technologien sind je nach Umgebung, Schutzbedarf und Sicherheitsanspruch zum Einsatz zu bringen und müssen sowohl in die bestehenden technischen Systeminfrastrukturen sowie auch in die Funktionsprozesse des Unternehmens individuell eingepasst werden.

Maximale Stabilität und Verfügbarkeit

Für exponierte KRITIS-Umgebungen der kommerziellen IT (Office IT, Rechenzentren, Webservices) und insbesondere für die operationelle IT (Leitstellen, Umspannwerke, Netzebenen, isolierte Bereiche) muss eine sehr hohe Stabilität und Verfügbarkeit der Systeme erreicht werden. Hier müssen zudem spezifische und individuell ausgelegte Stabilisierungs-, Härtungs- und Redundanzkonzepte zum Ansatz gebracht werden.

Aufgaben und Verantwortung der KRITIS-Sektoren

- Aufrechterhaltung gesellschaftlicher Funktionen und Ordnung,
- Gewährleistung der eigenen Geschäftsgrundlage und Schutz geistigen Kapitals,
- Bereitstellung eines „Fundamentes“ für andere Nutzer (Kunden) und deren Dienste.

Informationssicherheitsmanagementsystem

Die strategische, nachhaltige und messbare Etablierung von Informationssicherheit kann mit einem Informationssicherheitsmanagementsystem (ISMS gemäß ISO/IEC 27001 bzw. ISO/IEC 27019) im Unternehmen erreicht werden. KRITIS-Branchen, wie Erzeuger und Netzbetreiber im Sektor der Energiewirtschaft sind dazu ab Januar 2018 gesetzlich verpflichtet (ITSiKat 1a BNetzA, EnWG § 11 Abs. 1a, Meldepflichten EnWG § 11 Abs. 1c , ISO/IEC 27019:2017).

Wir unterstützen Sie auf dem Weg zur nachhaltig sicheren und stabilen Digitalisierung Ihrer Branche durch Qualifizierung Ihrer Risiken, Aufstellung einer Sicherheitsstrategie, Ermittlung Ihres Schutzbedarfes sowie durch die Unterstützung beim ISMS-Management.

CONTROLNET

CONTROLNET GmbH
Bauhausstraße 7c, 99423 Weimar
Central: +49 (0) 3643 9085 051
Fax: +49 (0) 3643 9085 052
CRITICAL INFRASTRUCTURE PROTECTION
ENERGY | KRITIS | UTILITY | INDUSTRY
www.controlnet.de info@controlnet.de