USB-Sticks sind ein potenzielles Einfallstor für Schadsoftware.

Digitale Pförtner

Effektiver Schutz von ITK-Infrastrukturen

NICO WERNER UND JAKOB SCHMIDT

Wir leben in einer vernetzten Gesellschaft, in der moderne IT- und Kommunikationstechnik (ITK) die Lebensadern sind. Sie sorgen für schnellen Informationsaustausch, flexible Datenverarbeitung und effiziente Prozesse. Ein Ausfall der ITK-Infrastruktur stellt ein erhebliches Sicherheitsrisiko dar. Die Zahl der Bedrohungen durch Schadsoftware steigt seit einigen Jahren, wie eine Veröffentlichung des BSI (Bundesamt für Sicherheit in der Informationstechnik) zur Cybersicherheit zeigt. Längst stehen auch Kritische Infrastrukturen von Energieversorgern, Transportunternehmen oder Verwaltungsorganisationen im Fokus von Hackern. Cyberkriminelle haben alle wichtigen Objekte unserer Wirtschaft und Gesellschaft im Visier. Die Folgen können enorm sein.

Kontrolle von Wechselmedien notwendig

Der Schutz von ITK-Infrastrukturen erfordert nicht nur technische Sicherheitsmaßnahmen, sondern auch die Früherkennung und Minimierung von Schäden. Klassische Informationstechnologien (IT, EDV) und der OT (Operational Technology)-Bereich (Prozesssteuerung, Automatisierung) unterscheiden sich grundlegend in der Auslegung ihrer Kommunikation. Bei der herkömmlichen IT liegt der Fokus auf Kommunikation und Vertraulichkeit, während in der Produktion insbesondere Verfügbarkeit und Safety wichtig sind. Das BSI verweist unter anderem darauf, dass Wechseldatenträger wie USB-Sticks und externe Festplatten ein häufiges und problemlos einsetzbares Mittel für Angriffe im IT- und OT-Bereich sind.

Ohne die Kontrolle von Wechselmedien können Viren oder Schadprogramme auf das Firmennetzwerk übertragen werden und gravierenden Schaden anrichten. Vor allem in sensiblen Umgebungen, wie in industriellen Anlagen oder Kritischen Infrastrukturen, in Entwicklungsabteilungen oder Forschungseinrichtungen, aber auch in Verwaltungen und Büroumgebungen, kann es zu drastischen Datenverlusten kommen – mit unberechenbaren wirtschaftlichen Folgen.

> „Der Schutz von ITK-Infrastrukturen erfordert nicht nur technische Sicherheitsmaßnahmen, sondern auch die Früherkennung und Minimierung von Schäden.
>
> **Nico Werner,**
> Head of Cybersecurity bei Telent

Foto: Koramis

Die Datenschleuse „InDEx“ besteht aus einem dedizierten Rechner mit einem gehärteten Gehäuse für die Fabrikumgebung mit Schnittstellen und hochprofessioneller Software für das Scannen von Wechseldatenträgern.

Foto: Adobe Stock

Ganzheitliche Lösungen

Die Systemspezialisten Telent und Koramis bieten umfassende Cybersecurity-Lösungen aus einer Hand. Telent plant, baut und betreibt sichere Netzinfrastrukturen unterschiedlicher Hersteller. Koramis ist Anbieter von ganzheitlichen Industrial-Security-Lösungsangeboten mit den Kernkompetenzfeldern Security Solutions, Security Management, Industrial Software und Industrial Automation.

Sicherheitskiosk für mobile Datenträger

Mit einer speziellen Datenschleuse wird die Möglichkeit geboten, den wechselseitigen Datenstrom in und aus der eigenen Infrastruktur zu überwachen. Die Lösung, wie etwa die Datenschleuse „InDEx“ (Intelligent Data Exchange) der Koramis GmbH, besteht aus einem dedizierten Rechner mit einem gehärteten Gehäuse robust für die Fabrikumgebung mit Schnittstellen und hochprofessioneller Software für das Scannen von Wechseldatenträgern. Das System kann automatisch Updates und Virensignaturen durch eine sichere, getrennte VPN-Verbindung aktualisieren. Die Schleuse hat eine einfache Bedienungsoberfläche mit Touchscreen und dient so als Sicherheitskiosk, quasi als digitaler Pförtner, für Wechselmedien in Unternehmen.

Die Lösung kann beispielsweise im Eingangsbereich von Unternehmen platziert werden. Die Daten auf Wechseldatenträgern werden dann überprüft und gereinigt – und zwar bevor sie mit internen Systemen in Verbindung kommen. Besonders Unternehmen mit sensiblen Infrastrukturen stehen vor der Herausforderung, einen immer aktuellen Virenschutz bereitzustellen. Dies ist mit „InDEx“ möglich, weil die Datenschleuse autark arbeitet und zeitnah mit den neuesten Updates versorgt wird. Die Kiosk-Lösung bietet mit seinem Rundum-Service aus Maintenance, Monitoring, Fernwartung, Patchmanagement, Signaturen-Updates und Vor-Ort-Austausch-Service einen wichtigen Baustein in einer ganzheitlichen Cybersecuritystrategie.

Managed Security: die beste Absicherung kritischer Systeme

Kritische Infrastrukturen benötigen ein hohes Schutzniveau, um zielgerichteten Angriffen von Organisationen mit entsprechenden Ressourcen standhalten zu können. Neben dem Einsatz einer Datenschleuse helfen weitere Maßnahmen, wie etwa solche zur Systemhärtung, um Gefahren abzuwehren und das Schutzlevel zu erhöhen. Unter Systemhärtung ist die Umsetzung von Maßnahmen zu verstehen, die dazu dienen, die Angriffsfläche eines Systems so weit wie möglich zu reduzieren. Das System wird dadurch resistenter gegen Angriffe und Schäden durch Fehlbedienungen. Da viele Bausteine und Maßnahmen eines ganzheitlichen Cybersecurity-Konzepts einen hohen Grad an Expertenwissen benötigen, bietet es sich an, auf diesem Feld auf Managed Security Services zurückzugreifen. ■

> „Das System kann automatisch Updates und Virensignaturen durch eine sichere, getrennte VPN-Verbindung aktualisieren.“
>
> **Jakob Schmidt,** Coordinator Awareness, Koramis

» **telent GmbH – ein Unternehmen der euromicron Gruppe:** www.telent.de

» **KORAMIS GmbH:** www.koramis.de