Grundsätze der Cybersicherheit von Operational Technology*

Eine Kurzanleitung

Kritische Infrastrukturen sind für die Aufrechterhaltung und Verbesserung unseres Lebensstils unerlässlich. Operational Technology (OT) steuert und regelt viele wichtige Dienstleistungen innerhalb unserer kritischen Infrastrukturen. Hierzu gehören das Wasser, das wir trinken, die Energie, auf die wir angewiesen sind und der Verkehr, der uns alle bewegt. International betrachtet nehmen maliziöse Cyberaktivitäten auf OT-Systeme und -Komponenten zu.

Die Grundsätze der Cybersicherheit von OT sollen Entscheidungsträgern auf allen Ebenen helfen, Cybersicherheitsrisiken angemessen zu berücksichtigen und die Systeme, die unsere Nation am Leben halten, bestmöglich zu schützen. Wenn beim Verändern oder Erweitern der OT-Umgebung ein oder mehrere der Grundsätze der OT-Cybersicherheit beeinträchtigt werden oder sogar dagegen verstoßen wird, dann wird voraussichtlich eine Schwachstelle in die OT-Umgebung eingebracht.

Prinzip 1: Safety (Funktionale Sicherheit) ist oberstes Gebot – ***Stellen Sie sicher, dass von dem System keine Gefahr für Mensch und Umwelt ausgeht!***

Safety ist in physikalischen Umgebungen von entscheidender Bedeutung. Dazu gehören der Schutz von Menschenleben, Anlagen/Geräten und der Umwelt sowie die Zuverlässigkeit und Verfügbarkeit eines Prozesses. Cybersicherheitsmaßnahmen dürfen die Safety nicht stören und die Safety muss sich an der Cyberbedrohungslage orientieren.

Prinzip 2: Profunde Kenntnisse der Geschäftsprozesse und Technik sind entscheidend – ***Kennen und verteidigen Sie unverzichtbare Systeme.***

Kenntnisse über den Geschäftsbetrieb, Prozessabläufe, Verbindungen zwischen Systemen und welche Bereiche kritisch sind, helfen Unternehmen beim Planen und Umsetzen einer effektiven Cybersicherheit mit den vorfügbaren Ressourcen. Unternehmen sollten in der Lage sein ihre unverzichtbaren Systeme zu identifizieren. Die Cybersicherheitsarchitektur sollte so geplant werden, dass sie die Systeme schützt und einen Wiederherstellungsprozess umfasst, der die Anforderungen der Geschäftsprozesse erfüllt.

Prinzip 3: OT-Daten sind äußerst wertvoll und müssen geschützt werden – ***Schützen Sie OT-Daten.***

Für einen böswilligen Cyber-Akteur ist das Wissen darüber, wie ein System eingerichtet ist, wie das Netzwerk aufgebaut ist, wie die Steuerungen konfiguriert sind und welche Anbieter und Geräte mit welchen Protokollen untereinander kommunizieren, wie eine Schatzkarte. Sie zeigt, wo und wie Schaden angerichtet werden kann. Führen Sie daher Prozesse ein, um den Zugang zu und die Verbreitung von OT-Daten zu minimieren und gleichzeitig die Integrität dieser Daten zu gewährleisten.

Prinzip 4: OT muss von allen anderen Netzwerken segmentiert und getrennt sein – ***Halten Sie die Hintertür geschlossen.***

Segmentieren und trennen Sie die OT von allen anderen Netzen, dies schließt auch andere OT-Bereiche, IT und das Internet ein. Berücksichtigen Sie insbesondere die Zuweisung von Verwaltungs- und Managementrollen in OT-Umgebungen.

Prinzip 5: Die Lieferkette muss sicher sein – ***Sichern Sie die Cyberlieferkette.***

Die Cybersicherheit der Lieferkette geht über Software und Geräte großer Anbieter hinaus. Berücksichtigen Sie in der OT alle Software, Geräte und Serviceanbieter, einschließlich ihrer Unterstützung, Verwaltung und Wartung, vom Kauf und der Integration bis zur Außerbetriebnahme und Entsorgung.

Prinzip 6: Menschen mit ihrer Erfahrung und Expertise sind für die Cybersicherheit der OT unerlässlich – *Menschen sind die erste Verteidigungslinie.*

Ein Cybervorfall in der OT kann nicht verhindert, abgewehrt, identifiziert, darauf reagiert und rechtzeitig behoben werden, wenn die Mitarbeitenden nicht über die notwendigen Werkzeuge und Schulungen verfügen. Die Investition in das eigene Personal ist für die Cyberabwehr eines Unternehmens von entscheidender Bedeutung. Dies muss von einer ausgereiften und organisationsweiten Cybersicherheitskultur entsprechend unterstützt werden.

*Dies ist eine Übersetzung der Publikation, die vom australischen Australian Cyber Security Centre des Australian Signals Directorate (ASD's ACSC) stammt und in Zusammenarbeit mit der US-amerikanischen Cybersecurity and Infrastructure Security Agency (CISA), der US-amerikanischen National Security Agency (NSA), dem US-amerikanischen Federal Bureau of Investigation (FBI), dem US-amerikanischen Multi-State Information Sharing and Analysis Center (MS-ISAC), dem englischen National Cyber Security Centre (NCSC-UK), dem kanadischen Centre for Cyber Security (Cyber Centre), dem neuseeländischen National Cyber Security Centre (NCSC-NZ), dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem niederländischen National Cyber Security Centre (NCSC-NL), dem japanischen National Center of Incident Readiness and Strategy for Cybersecurity (NISC) und der japanischen National Police Agency (NPA) sowie dem koreanischen National Intelligence Service (NIS) und dem koreanischen NIS' National Cyber Security Center (NCSC) erstellt wurde.