Foto: Telent

Um Kritische Infrastrukturen zu schützen, wurde das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme ITSiG 2.0 entworfen.

Cybersecurity für Kritis

Tritt das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme dieses Jahr in Kraft, müssen Kritis-Betreiber ihre Systeme maximal absichern. Eine Herausforderung – besonders für KMU.

NICO WERNER

Intakte Infrastrukturen für die Mobilität, die Energie- und Gesundheitsversorgung oder das Finanzwesen sind die Grundlage moderner Gesellschaften. Um sie bestmöglich zu schützen, legte Bundesinnenminister Horst Seehofer 2019 den Referentenentwurf für das ITSiG 2.0 vor. Das Gesetz stärkt nicht nur die Rolle des Bundesamts für Sicherheit in der Informationstechnik (BSI), sondern richtet auch den Fokus auf allgemein vernetzte Systeme wie Industrial Control Systems oder IoT-Geräte. Ein neues Siegel soll die IT-Sicherheit von Produkten kennzeichnen. Im Kritis-Bereich muss die gesamte Zulieferkette strengere Sicherheitskriterien einhalten und beispielsweise Systeme zur Angriffserkennung und -bewältigung (Security Incident & Event Management Systeme, kurz SIEM) betreiben. Es dürfen nur Komponenten von Herstellern verwendet werden, die das Sicherheitskennzeichen des BSI tragen. Kurzum – für maximalen Schutz müssen vor allem Kritis-Betreiber eine Menge Regularien berücksichtigen.

Was Unternehmen beachten müssen

Der Schutz von Kritischen Infrastrukturen erfordert nicht nur technische Sicherheitsmaßnahmen, sondern auch die Früherkennung und Minimierung von Schäden. Klassische Informationstechnologien (IT, EDV) und der OT-Bereich (Operational Technology, zum Beispiel zur Prozesssteuerung, Automatisierung) unterscheiden sich grundlegend in der Auslegung ihrer Kommunikation. Bei der herkömmlichen IT stehen Kommunikation und Vertraulichkeit im Mittelpunkt, während in der Produktion insbesondere Verfügbarkeit und Safety wichtig sind. Durch die zunehmende Digitalisierung und Vernetzung von Prozessen verschmelzen IT- und OT-Umgebungen zunehmend miteinander wie beispielsweise die Betriebs- und Steuertechnik kritischer Dienste in Versorgungsunternehmen.

> „Besonders kleine und mittelständische Unternehmen (KMU) haben Probleme, ihren Bedarf an Digitalkompetenz zu decken."
>
> **Nico Werner,** Head of Cybersecurity bei der Telent GmbH.

Hinzu kommt, dass OT-Infrastrukturen im Vergleich zu IT-Systemen für Bürokommunikation häufig eine längere Nutzungsdauer haben, aber mit neuen Sicherheitsanforderungen kompatibel sein müssen. Die Sicherheit von Software ist längst kein Add-on mehr, sondern eine explizite Anforderung im Entwicklungsprozess. Qualitative Sicherheitsmaßnahmen sind aber auch mit hohen Investitionen verbunden, was kleinen und großen Unternehmen gleichermaßen zu schaffen macht. Nicht zuletzt spielen ein passgenaues Konzept und Usability eine wichtige Rolle, damit Schutzmaßnahmen richtig eingesetzt werden.

Mangelnde Digitalkompetenz

Die Umsetzung der zusätzlichen Regularien erfordert interne Ressourcen und Know-how. Besonders kleine und mittlere Unternehmen stehen nicht nur vor der Herausforderung, den Überblick über die (neuen) Vorschriften des Gesetzgebers und ihre eigenen, mit der Zeit wachsenden Anforderungen zu behalten – sie haben auch Pro-

bleme, ihren Bedarf an Digitalkompetenz zu decken. Einer neuen repräsentativen Studie der staatlichen Förderbank KfW zufolge verfügt aktuell ein Drittel dieser Unternehmen nicht über ausreichendes Wissen über die digitale Transformation und deren Begleiterscheinungen. Besonders gravierend sei die Situation bei komplexeren Kenntnissen, zum Beispiel für Spezialsoftware. So suchen fast die Hälfte (45 Prozent) der Mittelständler dringend qualifizierte Datenanalysten.

Die Lösung ist „Managed Security", um mit der Unterstützung eines kompetenten Spezialisten ein zukunfts- und bedarfsorientiertes Konzept aufzustellen und sich als vertrauenswürdige Geschäftspartner zu positionieren. Als langjähriger Systemintegrator für Kritis hat beispielsweise die Telent GmbH umfangreiche Erfahrungen mit regulatorischen Verfahren: Von der Schwachstellenanalyse über die Netzplanung mit Notfallkonzept bis zur Umsetzung von Managed-Security-Konzepten inklusive Echtzeitüberwachung unterstützt man Kunden ganz nach Bedarf.

Die bestmögliche Vorbeugung

Lösungen für Managed Security beinhalten SIEM-Tools beziehungsweise professionelle Supportleistungen für die kontinuierliche Überwachung und Schutz von IT-/OT-Umgebungen. Spezialisierte Systemintegratoren wie Telent setzen dabei fortschrittliche Hard- und Software ein, inklusive maschinelles Lernen und Künstliche Intelligenz (KI), um den Datenfluss lückenlos zu überwachen. Zahlreiche detaillierte Korrelationsinformationen und Algorithmen lösen Alarme aus und zeigen verdächtige Bedrohungen auf. Netzwerkplattformen, die solche Funktionen in ihrer Architektur implementiert haben, sind unter anderem Cisco Digital Network Architecture (DNA), Cisco Identity Services Engine (ISE) oder Cisco Firewall der neusten Generation mit gegebenenfalls speziellen Industrial Security Appliances für ICS-Umgebung.

Ein Sicherheitsansatz für sensible Infrastrukturen sind „Anomaly-Detection-Systeme" (deutsch: Anomalie-Erkennungssysteme). Ob ein Netzwerkgerät plötzlich ein anderes Kommunikationsprotokoll nutzt oder Datenverkehr ungeplant eine neue Route nimmt – ein solches System kann diese Vorgänge zeitnah erkennen und Alarm schlagen. Um eine Normabweichung erfolgreich zu identifizieren, muss das System zunächst den Normalzustand erfassen, indem es die IT-Architektur analysiert und im Hintergrund lernt.

Schutzmaßnahmen

Vor zielgerichteten Angriffen durch kriminelle Organisationen schützen auch Maßnahmen zur Isolierung, Systemhärtung und Sandboxing. Sie helfen, tiefergreifende Gefahren abzuwehren und schützen vor Risiken, die durch Fehlverhalten von Mitarbeitern oder Hackerangriffen entstehen.

Bei der Netzsegmentierung werden Unternehmensnetze in Segmente unterteilt und die Verbindungen zwischen diesen Segmenten so gering wie möglich gehalten. Im Rahmen der Systemhärtung geht es, vereinfacht gesagt, darum, Regeln festzulegen, wer auf welche Systeme und deren Unterbereiche Zugriff hat und wer nicht. Insbesondere muss definiert werden, welche kritischen Anwendungen in einer Sandbox laufen sollen. Sandboxing („Sandkasten") steht für eine Technik, mit der eine Software oder ein Prozess innerhalb einer isolierten, von den restlichen System- oder Netzwerkressourcen abgeschotteten, Laufzeitumgebung ausgeführt wird. Das gesamte System ist in mehrere Sandboxen unterteilt, sodass das Betriebssystem und kritische Anwendungen isoliert betrieben werden können. Eindringlinge und Malware können so nicht auf diese Bereiche zugreifen. Der große Vorteil dieser Methode: Sie schützt auch vor Zero-Day-Exploit-Attacken, bei denen Sicherheitslücken ausgenutzt werden, bevor sie geschlossen werden können.

Zusätzlich zu technischen Maßnahmen sollte zum Beispiel durch Awareness-Trainings und -Kampagnen dafür gesorgt werden, dass die organisatorische Sicherheit bezüglich des Faktors Mensch erhöht wird. Ein System zu härten bedeutet auch, nur die Komponenten einzusetzen, die für den Systembetrieb notwendig sind; denn es sind Menschen, die die Prozesse definieren und die Technologie kontrollieren.

Eine Security Policy beinhaltet daher nicht nur technische Aspekte, sondern ist auch eine strategische und organisatorische Entscheidung seitens der Unternehmensführung. ■

telent GmbH:
www.telent.de