Foto: Westend61 - stock.adobe.com

Das IT-SIG 2.0 erweitert den Kreis der Kritis um den Sektor Abfallwirtschaft und um Unternehmen von besonderem öffentlichen Interesse.

Verschärfte Anforderungen

Das neue IT-Sicherheitsgesetz 2.0 erweitert den Kreis der Kritischen Infrastrukturen und verschärft die Anforderungen an die Betreiber.

NICO WERNER

Für die betroffenen Unternehmen bedeutet das neue IT-Sicherheitsgesetz 2.0 konkret: Mehr Pflichten, um die Cybersecurity stärken. Es gibt Szenarien, die mag man sich lieber nicht vorstellen: Erfolgreiche Hackerangriffe legen die Stromversorgung großflächig lahm, stören massiv die Rettungsdienste oder bewirken gesundheitsschädliche Konzentrationsveränderungen im Trinkwasser. Die Folgen für die Bevölkerung wären gravierend, und die Szenarien scheinen nicht unrealistisch angesichts der immer ausgefeilteren Cyberangriffe. Insofern ist es unumgänglich, dass sich Unternehmen und Organisationen, die den Sektoren der Kritischen Infrastruktur (Kritis) angehören, besser schützen.

Das Anfang des Jahres in Kraft getretene Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetzes 2.0 oder IT-SIG 2.0) zielt darauf ab, die IT-Infrastruktur in Deutschland zur sichersten der Welt machen – mit unterschiedlichsten Maßnahmen. Schon bisher unterlagen Kritis-Betreiber aus den Sektoren Energie, Wasser, Ernährung sowie Informations- und Telekommunikationstechnik besonderen Sicherheitsbestimmungen. Das IT-SIG 2.0 erweitert den Kreis der Adressaten um den Sektor Abfallwirtschaft und um Unternehmen von besonderem öffentlichem Interesse. Dazu gehören neben der Rüstungsindustrie Betriebe, die allein aufgrund ihrer Größe volkswirtschaftlich relevant sind, sowie deren wichtige Zulieferer. Zusätzlich steigt die Zahl der Kritis-Betreiber, da Schwellenwerte gesenkt wurden. Beispielsweise reichen für die Einstufung als Stromerzeugungsanlage statt der bisherigen 420 Megawatt jetzt schon 36 Megawatt aus.

20

MILLIONEN Euro oder bis zu vier Prozent des weltweit erzielten Jahresumsatzes kann als Strafe bei Verstößen fällig werden.

IT-SIG: Geldbußen kräftig erhöht

Die Betreiber, die sich selbst beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren müssen, bekommen mehr Pflichten, der Staat

hingegen mehr Rechte. Das bisher eher passiv agierende BSI erhält durch das IT-SIG 2.0 einen größeren Aufgabenbereich und mehr Handlungsbefugnisse. Dadurch soll es sich zur nationalen „Hackerbehörde“ mausern, die zukünftig mehr auf Angriff statt Verteidigung setzt. Die Behörde darf beispielsweise Portscans durchführen, um Sicherheitslücken in der IT zu identifizieren, die durch veraltete Software oder offene Ports entstehen. Unternehmen müssen dem BSI Schnittstellen öffnen, damit es die Systeme patchen kann. Das ist vor allem für den Anlagenbereich ein hochumstrittenes Thema, dessen genaue Umsetzung noch nicht spezifiziert ist.

Wer seinen Verpflichtungen nicht nachkommt, muss mit drastisch erhöhten Geldbußen rechnen. Lag das Maximum in der Vergangenheit bei 100.000 Euro, können Verstöße zukünftig mit bis zu 20 Milionen Euro oder mit bis zu 4 Prozent des weltweit erzielten Jahresumsatzes geahndet werden. Um bei diesen Summen nicht zur Kasse gebeten zu werden, sollten Unternehmen ihre neuen Pflichten im Auge behalten.

IT und OT ganzheitlich schützen

Was ist zu tun? Um sich im Sinne des IT-SIG 2.0 zu schützen, brauchen Kritis-Betreiber ab dem 1. Mai 2023 eine Angriffserkennung auf dem aktuellen Stand der Technik und ein Monitoring der kritischen Komponenten. In Großkonzernen ist der dafür notwendige Technologie-Mix verbreitet, nicht aber in kleineren Organisationen und mittelständischen Betrieben. Ein großes Sicherheits-Gap gibt es auch zwischen der IT und der OT (Operational Technologie). Die Anlagen- und Steuerungstechnik wird häufig sträflich vernachlässigt, da viele Unternehmen glauben, dass ihre Betriebstechnologie nicht mit dem Internet verbunden ist. Ein Trugschluss! Denn durch die Digitalisierung wachsen IT und OT immer mehr zusammen, und die vielen Endgeräte, die in OT-Umgebungen Daten unverschlüsselt über allgemein bekannte Industrieprotokolle austauschen, sind für Hacker leicht zu knacken, sind sie erst einmal ins Netzwerk eingedrungen.

Firewalls allein reichen nicht aus

Herkömmliche Firewalls, die in der IT-Welt unerwünschten Datenverkehr außen vor halten, reichen für die OT nicht aus. Für den Schutz der Betriebstechnologie braucht es Next-Generation Firewalls mit einer integrierten Deep-Packet-Inspection (DPI), die übertragenen Daten in den Netzwerkpaketen detailliert inspiziert. Ein DPI ist die Voraussetzung für ein kombiniertes System aus Intrusion Detection System (IDS) und Intrusion Prevention System (IPS) – eine mögliche Angriffserkennung, die den Vorgaben des IT-SIG 2.0 entspricht. Ein auf die OT spezialisiertes IDS/IPS-System versteht die proprietären Protokolle der Anlagen und Steuerungen. Da es dieselbe Sprache spricht, kann es sowohl Angriffe als auch Fehlkonfigurationen, die auf menschlichem Versagen basieren, erkennen. Bei Anomalien löst es einen Einbruchsalarm aus oder blockiert nicht autorisierte Datenpakete.

Eine andere Form der Angriffserkennung sind Honeypots, die als virtuelle Maschinen bewusst mit Sicherheitslücken konfiguriert wurden, um Hacker gezielt anzulocken und in die Irre zu leiten. Honeypots wirken wie Feuerlöscher. Wie in einem Haus sollten auch in einem Netzwerk am besten mehrere Feuerlöscher auf jeder Ebene vorhanden sein, um zu löschen beziehungsweise um Angreifer zu erkennen und abzuwehren. Dazu wird jeder Honeypot ständig überwacht. So lassen sich IP-Adressen von Eindringlingen identifizieren, um sie dann für das gesamte System zu blockieren, und Informationen zur Vorgehensweise von Angreifern sammeln.

Ein SOC überwacht Netze kompetent

Zu den neuen Pflichten der Kritis-Betreiber gehört es auch, sicherheitsrelevante Ereignisse zu monitoren, etwa über ein Security-Incident-Event-Management-System (SIEM). Das technische Tool erhält von zahlreichen Datenkollektoren eine Fülle an Informationen, bereinigt diese zu einem „normalisierten Stream“ und gibt bei Auffälligkeiten Fehlermeldungen ab. Richtig implementiert und betrieben verbessert das die Cybersecurity. Doch in der Praxis scheitern gerade kleinere und mittelständische Betriebe daran, dass ihnen Know-how und Personal fehlen, um die zahlreichen Fehlermeldungen dezidiert zu prüfen. Nur dann kann richtig reagiert werden. Hilfe bieten auf Cybersecurity spezialisierte Dienstleister wie die Telent GmbH. Sie bündeln Expertenwissen in einem Security Operation Center (SOC), in dem sie die von einem SIEM und anderen Systemen gesammelten Daten auswerten, die Netzwerke ihrer Kunden rund um die Uhr überwachen, aktiv nach Bedrohungen suchen, diese entfernen und weitergehende Handlungsempfehlungen aussprechen.

Trotz der zweijährigen Übergangsfrist sollten Kritis-Unternehmen zügig darangehen, die vom IT-SIG 2.0 eingeforderte Angriffserkennung und das Monitoring umzusetzen. Damit schlagen sie gleich zwei Fliegen mit einer Klappe: Sie erfüllen die vorgegebenen Sicherheitsanforderungen rechtzeitig und schützen sich selbst so schnell wie möglich vor den ständig steigenden Cyberbedrohungen. ■

Nico Werner, Head of Cybersecurity bei der Telent GmbH

telent GmbH:
www.telent.de

Foto: Telent

Zu den neuen Pflichten der Kritis-Betreiber gehört es auch, sicherheitsrelevante Ereignisse zu monitoren, etwa über ein Security-Incident-Event-Management-System (SIEM).