Foto: Adobe Stock / Gorodenkoff

Unternehmen stehen bei der konkreten Umsetzung des IT-Sig 2.0 vor einigen Ungewissheiten. Vieles ist noch nicht klar definiert, manches bleibt ein Blick in die Glaskugel, sicher ist nur eins – betroffene Unternehmen müssen die Security-Anforderungen in Kürze umsetzen.

Herausforderungen bei der Umsetzung des IT-SiG 2.0

Wie gut lassen sich die Vorgaben des neuen IT-Sicherheitsgesetzes und des BSI in der Praxis erfüllen? Eine erste Zwischenbilanz.

NICO WERNER

Der Countdown läuft: Angesichts rasant steigender Cyberangriffe und der fortschreitenden Digitalisierung zielt das novellierte IT-Sicherheitsgesetz (IT-SiG) 2.0 darauf, die IT/OT-Sicherheit der kritischen Infrastrukturen (Kritis) zu erhöhen. Für Kritis-Betreiber, deren Kreis der Gesetzgeber durch Unternehmen von besonderem öffentlichem Interesse, niedrigeren Schwellenwerten und mehr Anlagentypen deutlich erweiterte, hat das weitreichende Konsequenzen. Zu den neuen Pflichten gehören ab dem immer näher rückenden Stichtag – dem 1. Mai 2023 – ein System zur Angriffserkennung, die Berücksichtigung der Liste kritischer Komponenten und die aktive Registrierung beim Bundesamt für Sicherheit (BSI). Die Kompetenzen der Behörde wurden ebenfalls ausgedehnt, damit sie aktiver agiert als bisher. Dazu gehört, dass das BSI von sich aus Unternehmen als Kritis einzustufen kann. Erste Fälle gibt es bereits. Zudem bekommt die Behörde die Hoheit darüber, was der „Stand der Technik" für sicherheitstechnische Anforderungen bei IT-Produkten ist und wird gemäß dem Cyber Security Act der EU zur nationalen Stelle für Cybersicherheitszertifizierungen.

> „Die Verpflichtung, eine Angriffserkennung einzusetzen, ist zwar in Stein gemeißelt. Doch das Gesetz beschreibt nicht, was es darunter versteht."

Konkrete Umsetzung des IT-Sig 2.0

Unternehmen stehen bei der konkreten Umsetzung des IT-SiG 2.0 vor einigen Herausforderungen. Das beginnt mit der Unsicherheit, welche technischen Maßnahmen genügen. Zwar ist die Verpflichtung, eine Angriffserkennung einzusetzen, in Stein gemeißelt, doch das Gesetz beschreibt nicht, was es darunter versteht. Angesichts der zahlreichen Nachfragen veröffentlichte das BSI im vergangenen Herbst eine finale Orientierungshilfe, die die Anforderungen definiert, Nachweisformulare enthält und ein Reifegradmodell erläutert, über das die implementierten Maß-

nahmen bewertet werden können. Demnach muss eine Angriffserkennung zwingend drei Aufgaben erfüllen: Protokollierung, Detektion und Reaktion.

Der Leitfaden eröffnet also mehrere Optionen. Eine davon ist die Kombination aus Intrusion Detection System (IDS) und Intrusion Prevention System (IPS). Jede Next Generation Firewall beinhaltet ein IDS/IPS, das in der IT-Welt unerwünschten Datenverkehr recht gut abwehrt, aber nicht ausreichend in der OT-Welt. Ausdrücklich weist das Gesetz darauf hin, das die kritischen Komponenten von Produktionsanlagen vor Cyberkrimininalität zu schützen sind. Dafür braucht es ein auf die OT spezialisiertes IDS/IPS, das die Sprache der proprietären Protokolle, Maschinen und Steuerung spricht. Eine andere Möglichkeit ist eine anomalisierte Angriffserkennung, die Abweichungen im Netzwerk erkennt, Einbruchsalarm auslöst und nicht autorisierte Datenpakete blockiert. Eine Angriffserkennunung im Sinne des IT-SiG 2.0 sind auch Honeypots, die Angreifer gezielt anlocken, ohne dass diese bemerken, dass sie sich auf einer virtuellen Maschine und nicht auf einem Livesystem befinden. Damit gewinnen attackierte Unternehmen Zeit, um Gegenmaßnahmen zu treffen und können aus dem Verhalten der Angreifer lernen.

Monitoring kritischer IT-Vorfälle

Neben der Angriffserkennung dürfen Kritis-Unternehmen ein weiteres Thema nicht vernachlässigen: das Monitoring sicherheitsrelevanter Ereignisse. Dieser Pflicht erfüllt ein Security-Incident-Event-Management-System (SIEM), das Logdaten aus dem gesamten Netzwerk sammelt, kategorisiert und bei Auffälligkeiten warnt. Dabei kommt es häufig zu dem Phänomen False Positives – also, Fehlalarmen, die Sicherheitsexperten dezidiert bewerten müssen, damit richtig reagiert werden kann. Eine vor allem für kleine und mittlere Unternehmen kaum zu bewältigende Aufgabe, da ihnen zumeist die entsprechenden Fachleute fehlen. In diesem Fall unterstützen auf Cybersecurity spezialisierte Partner wie die Telent GmbH, die im eigenen Security Operation Center (SOC) die Netzwerke ihrer Kunden rund um die Uhr überwachen und für eine reibungslose Infrastruktur sorgen. Die Hoffnung, dass das BSI angegriffenen Unternehmen zur Seite springt, wird sich angesichts der begrenzten personellen Kapazitäten der Behörde nicht erfüllen. Sie nutzt die Monitoringdaten vielmehr für die statistische Auswertung, um Angriffswellen zu erkennen und davor zu warnen.

Einsatz kritischer Komponenten

Das IT-SiG 2.0 verpflichtet Kritis-Betreiber, einen geplanten, erstmaligen Einsatz von kritischen Komponenten dem Bundesinnenministerium anzuzeigen, das diese unter bestimmten Voraussetzungen untersagen kann. Die Liste kritischer Komponenten ist das beste Beispiel dafür, wie unzureichend etliche Vorgänge bisher sind. Aktuell gibt es nur eine Liste in rudimentärer Fassung für den Sektor Telekommunikation. Fachkreise erwarten im Laufe des Jahres die Veröffentlichung für weitere Bereiche. Aber wann und für wen – das ist noch ungewiss. Eine Erkenntnis seit Inkrafttreten des IT-SiG 2.0 ist: Unternehmen, die beispielsweise ein neues Core-Netzwerk ausschreiben, sollten für die ausgewählten Produkte von den Herstellern eine Garantie- oder Konformitätserklärung verlangen, um so weit wie möglich auf der sicheren Seite zu sein. Denn da die Prozesse rund um die neue Zertifizierung ebenfalls noch in der Schwebe sind, ist es für Unternehmen und Systemintegratoren schwierig, die Sicherheitsstandards von Produkten zu beurteilen. Hier bleibt zu hoffen, dass die Zertifizierungsnorm nicht nur für Deutschland, sondern international gelten wird, und dass ausreichend Zertifizierungsstellen geschaffen werden.

„Das IT-SiG 2.0 legt den Betroffenen deutlich mehr Pflichten auf, die sie nicht nur angesichts der spürbar erhöhten Bußgelder, sondern vor allem für ihre eigene Cyberabwehr zügig umsetzen sollten."

Nico Werner,
Head of Cybersecurity bei der telent GmbH.

Patchingbefugnis bleibt umstritten

Heftig diskutiert wird nach wie vor die Befugnis des BSI zu tiefergehenden Untersuchungen. Ein mögliches Szenario verdeutlicht die Brisanz: Das Leit- und Steuerungssystem eines Betriebs läuft auf einer veralteten Version, da es nach einem Update nicht mehr reibungslos funktionieren würde. Da das BSI die Möglichkeit erhalten soll, das System zu patchen, muss das Unternehmen der Behörde dafür eine Schnittstelle öffnen. Dieses Tor steht somit auch Hackern offen. Eine weitere Gefahr ist der Ausfall des upgedaten Systems und die ungeklärte Frage, wer im Fall einer Produktionsbeeinträchtigung für den wirtschaftlichen Schaden aufkommt. Mehrere Branchenverbände klagen gegen die Patchingbefugnis des BSI. Allerdings sind sich Sicherheitsexperten einig, dass es mehr Kontrolle braucht. Portscans oder der Blick in die Computer-Suchmaschine Shodan zeigen, wie erschreckend offen im Internet die Zugänge von zahlreichen Unternehmen sind. Die Frage ist nur, ob die Zuständigkeit für Sicherheitspatches bei einer Behörde liegen sollte oder nicht besser bei einer gesonderten Instanz.

Das IT-SiG 2.0 legt den Betroffenen deutlich mehr Pflichten auf, die sie nicht nur angesichts der spürbar erhöhten Bußgelder, sondern vor allem für ihre eigene Cyberabwehr zügig umsetzen sollten. Nicht ignoriert werden dürfen die gesetzlichen Anforderungen, die noch mit offenen Fragen verbunden sind. Hier empfiehlt es sich, auf dem Laufenden zu bleiben und sich, auch mithilfe externer Kompetenz, gut vorzubereiten. ■

Foto: Telent

telent GmbH:
www.telent.de