Smarter Schutz aus der Cloud

Netzbetreiber müssen ihre IT-Infrastruktur besonders gut gegen Cyber-Attacken schützen. Um Sicherheitslücken zu erkennen, ist eine kontinuierliche Netzüberwachung notwendig. Spezialisierte Unternehmen bieten dafür Managed-Services aus der Cloud an.

IT-Systeme der kritischen Infrastruktur für die Energieversorgung müssen besonders gut vor Angriffen geschützt werden. Um größeren Schaden effektiv unterbinden zu können, müssen die Energieversorger und -netzbetreiber Angriffe auf ihre IT-Infrastruktur und deren Sicherheitslücken schnellstmöglich erkennen und umgehend darauf reagieren. Dies ist keine einfache Aufgabe, handelt es sich doch bei ihren Kommunikationsnetzen in der Regel um hochkomplexe Multiservice-Betriebsnetze, über die Daten, Sprache, Video und Sensorinformationen gleichzeitig übertragen werden.

Für den sicheren Betrieb sind deshalb ein passendes Management-Konzept sowie die kontinuierliche Netzüberwachung und -steuerung essenziell. Auch braucht es Expertenwissen, damit Betreiber den besonderen Sicherheitsanforderungen gerecht werden können. Als Systemintegrator hat das Unternehmen telent mit der Tochterfirma Koramis umfangreiche Erfahrungen mit regulatorischen Verfahren. Es unterstützt seine Kunden von der Schwachstellenanalyse über die Netzplanung bis hin zur Umsetzung von Managed-Security-Konzepten inklusive Echtzeitüberwachung mit einem ganzheitlichen Sicherheitskonzept.

Um ein Sicherheitskonzept erstellen zu können, wird zunächst eine Schwachstellenanalyse durchgeführt. Vorgenommen werden sollte sie von einem externen, neutralen Dienstleister. Im Rahmen dieser Analyse untersuchen Fachleute die Sicherheit der technischen Anlagen und Prozesse und identifizieren dabei mögliche Angriffspunkte sowohl in der physikalischen Infrastruktur als auch in der organisatorischen Struktur sowie der Security-Strategie des Versorgungsunternehmens. Nach einer ersten groben Einschätzung der Risiken und Abhängigkeiten bezüglich der IT-Systeme und -Prozesse wird auf Basis vorhandener Dokumente eine Vor-Ort-Analyse vorbereitet. In deren Rahmen erfolgt eine breit angelegte, systematische und detaillierte Erhebung der Schwachstellen. Beispielsweise werden mithilfe von Interviews mögliche Gefährdungen in den Prozessen identifiziert. Zudem findet eine technische Prüfung der ITK-Infrastruktur statt. Anschließend werden die Erhebungen analysiert, Risiken klassifiziert, bewertet und dokumentiert. Ein

abschließender Workshop thematisiert die identifizierten Schwachstellen und erläutert einen Plan mit empfohlenen Korrekturmaßnahmen für jede dieser Stellen.

Bei kritischen Infrastrukturen bieten klassische Sicherheitsanwendungen wie Antiviren-Software kein hinreichendes Schutzniveau; gegen zielgerichtete Angriffe sind alternative Strategien notwendig. Maßnahmen zur Systemhärtung helfen, Gefahren abzuwehren, indem sie potenzielle Angriffsflächen soweit wie möglich reduzieren. Dazu zählt das Scannen der Systeme. Auf diese Weise lassen sich zunächst solche Systeme identifizieren, die bereits von Schad-Software befallen sind. Noch bevor weitere Schritte umgesetzt werden, werden diese Systeme bereinigt. Eine andere der Systemhärtung zuzurechnende Maßnahme ist die Mikrosegmentierung. Vor die Systeme geschaltete Hardware Firewalls stellen hier sicher, dass nur über zuvor spezifizierte Ports kommuniziert werden kann. Diese Firewalls sind der einzige Weg, um über das Netzwerk auf das System zuzugreifen.

Da jede Schnittstelle eine mögliche Angriffsfläche bietet, sollte ihre Anzahl so gering wie möglich gehalten werden. Unter dem Begriff der Schnittstellenreduzierung werden mehrere physikalische Schutzmaßnahmen zusammengefasst, etwa das Absichern nicht-benötigter USB-Ports mithilfe von Schlössern oder die Deaktivierung nicht-benötigter Dienste des Betriebssystems. Maßnahmen zur Systemhärtung erhöhen aber auch die organisatorische Sicherheit, indem sie vor Risiken schützen, die Mitarbeiter oder Fremdfirmen durch Fehlverhalten verursachen.

Sicherheit im Sandkasten

Steuerungsanlagen, wie sie in Kraftwerken und anderen Großanlagen zum Einsatz kommen, sind zuweilen mehrere Jahrzehnte im Einsatz und arbeiten oft mit veralteten Betriebssystemen wie Windows XP. Ein Lösungsansatz ist hier das so genannte Sandboxing. Dabei handelt es sich um eine Technik, die es erlaubt, eine Software innerhalb einer isolierten – von den restlichen System- oder Netzwerkressourcen abgeschotteten – Laufzeitumgebung auszuführen. Das gesamte System ist dazu in mehrere Sandboxes segmentiert, sodass sich Betriebssystem und kritische Anwendungen isoliert betreiben lassen. Dadurch wird verhindert, dass Eindringlinge und Malware auf diese Bereiche zugreifen können.

Durch Sandboxing lassen sich nicht nur Legacy-Systeme schützen. Es können auch Workstations, Server, Cloud-Systeme und ganze Datacenter in einer Sandbox isoliert werden, um den Schutz vor Angriffen von außen zu erhöhen. Die Methode schützt sogar vor so genannten Zero-Day-Exploit-Attacken, bei denen die Angreifer Sicherheitslücken ausnutzen, noch bevor sie vom Software-Hersteller geschlossen werden können.

Energieversorger und -netzbetreiber müssen künftig noch strengere Sicherheitskriterien und Prozesse einhalten. Sie sind dazu angehalten, neben Informationssicherheits-Management-Systemen (ISMS) auch so genannte SIEM-Systeme (Security Incident and Event Management) zur Angriffserkennung und -bewältigung wirksam zu betreiben. SIEM-Systeme sammeln durch maschinelles Lernen und künstliche Intelligenz Meldungen, Alarme und Logfiles verschiedener Netzkomponenten, Anwendungen und Security-Systeme in Echtzeit, korrelieren diese, werten sie aus und erkennen so Angriffe, außergewöhnliche Muster oder gefährliche Trends.

Netzbetreiber müssen die genannten Maßnahmen nicht zwingend selbst umsetzen und auch kein aufwendiges, eigenes SOC aufbauen. Spezialisierte Unternehmen wie telent bieten Managed-Security-Services an, die exakt auf die Bedürfnisse ihrer Kunden zugeschnitten sind und von diesen nach Bedarf aus der Cloud abgerufen werden können. Das Managed-Security-Portfolio von telent beinhaltet unter anderem die 24/7-Netzwerküberwachung mit Bedrohungserkennung und Echtzeit-Alarmierung sowie einen integrierten Incident Management Workflow für die umgehende Behebung von Ausfällen nach Angriffen. ■

Der Autor: Nico Werner

Nico Werner ist Head of Cybersecurity bei der telent GmbH in Backnang. Zuvor war er als Projektleiter, IT-Leiter und Managing Consultant bei mehreren IT-Unternehmen tätig. Auch ist er als Speaker und Blogger zu Themen rund um ITK-Sicherheit aktiv.