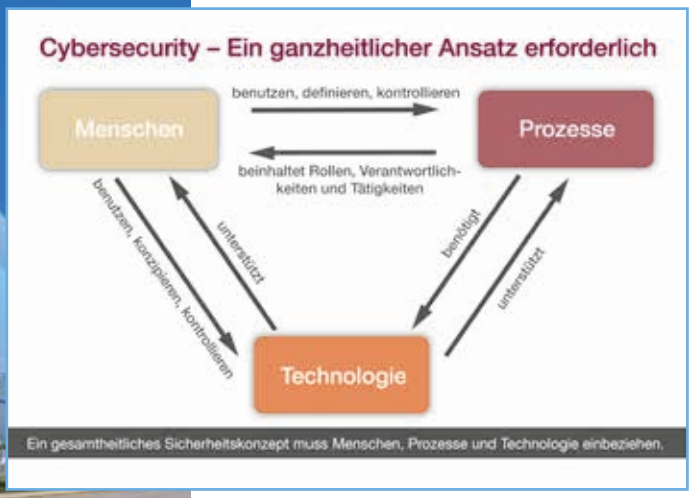
Grafik: Telent GmbH

Telent integriert Lösungen zum Schutz vor Drohnenangriffen auf Kritische Infrastrukturen.



Damit die Betreiber diesen besonderen Sicherheitsanforderungen gerecht werden, müssen sie entsprechende ganzheitliche Security-Konzepte erarbeiten, die Menschen, Prozesse und Technologie berücksichtigen.

Gefahren für Kritische Infrastrukturen und ihre Abwehr

Risiken erkennen, Maßnahmen ergreifen

Nico Werner

Informationstechnik durchdringt alle Bereiche von Wirtschaft und Gesellschaft. Der Ausfall zentraler Hard- oder Software oder ein Angriff von Hackern und Organisationen, die sich Zugriff auf IT-Netze zur Spionage, zur Sabotage oder schlicht zum Zeitvertreib verschaffen wollen, kann verheerende Folgen haben. Dies gilt insbesondere für Kritische Infrastrukturen (KRITIS).

Kommt es im Bereich Kritischer Infrastrukturen zu Störungen, kann dies eine Gefahr für die Bevölkerung darstellen. Das zeigt unter anderem auch der Hackerangriff Mitte Mai, bei dem die Schadsoftware Wannacry weltweit Organisationen, Firmen und Behörden lahm gelegt hat. Es ist daher von vitalem Interesse, in diesen Bereichen für ein Höchstmaß an Sicherheit zu sorgen, um Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu jedem Zeitpunkt zu schützen.

Getrieben durch die hohe Innovationsgeschwindigkeit und zunehmende Vernetzung von Anlagen und Systemen wächst der Stellenwert von IT-Sicherheitskonzepten. Mit dem 2015 verabschiedeten IT-Sicherheitsgesetz (IT-SiG) hat die Bundesregierung neue Standards für den Schutz der Informationstechnologie formuliert. Insbesondere im Bereich der Kritischen Infrastrukturen hätte ein Ausfall oder eine Beeinträchtigung der Versorgungsleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland. Die Verfügbarkeit und Sicherheit der IT-Systeme und Prozesse spielt daher in diesen Bereichen eine zentrale Rolle. KRITIS-Betreiber müssen Angriffe und Sicherheitslücken schnellstmöglich erkennen und umgehend darauf reagieren zu können, um größeren Schaden oder die Ausbreitung der Vorfälle zu verhindern. Schwerwiegende IT-Sicherheitsvorfälle haben sie an das BSI zu melden. Dort werden diese Informationen ausgewertet und wiederum den Betreibern zur Verfügung gestellt, damit sie entsprechende Gegenmaßnahmen einleiten. Damit die Betreiber diesen besonderen Sicherheitsanforderungen gerecht werden, müssen sie entsprechende ganzheitliche Security-Konzepte erarbeiten, die Menschen, Prozesse und Technologie berücksichtigen. Dazu gehört eine Schwachstellenanalyse der gesamten IT-Infrastruktur inklusive kontinuierlicher Sicherheitsüberwachung in Echtzeit. Neben dieser physikalischen Analyse überprüfen die Experten auch die individuelle Security-Strategie. Erkennen sie dabei Schwachstellen oder Verbesserungspotenti-

ale, dokumentieren und bewerten sie diese und entwickeln bei Abweichungen von den relevanten Sicherheitsstandards einen entsprechenden Maßnahmenplan.

Maßnahmen zur Systemhärtung helfen, Gefahren für Kritische Infrastrukturen abzuwehren, die von zielgerichteten Angriffen ausgehen – und schützen gleichzeitig vor Risiken, die Mitarbeiter oder Fremdfirmen durch Fehlverhalten verursachen können. Härten bedeutet, die Sicherheit eines Systems zu erhöhen, indem nicht benötigte Dienste und Schnittstellen deaktiviert oder abgesichert werden, ein Softwaremanagment eingesetzt wird, oder Anwendungen und Systeme durch spezielle Maßnahmen wie Sandboxing oder Whitelisting geschützt werden.

Sichere Netze trotz Heterogenität

An Kommunikationsnetze für Kritische Infrastrukturen werden spezielle Anforderungen bezüglich Zuverlässigkeit, Sicherheit und Vertraulichkeit gestellt. Charakteristisch für solche Netze ist der Einsatz unterschiedlicher Übertragungsprotokolle, wie etwa PDH, SDH, IP-MPLS, IP-Ethernet und andere. Zudem stammen die eingesetzten Netzelemente häufig von verschiedenen Herstellern. In KRITIS-Kommunikationsnetzen werden, wie eingangs erwähnt, spezielle Anforderungen an Zuverlässigkeit, Sicherheit und Vertraulichkeit bei der Übertragung von Daten und Sprache gestellt. Deshalb sind – um die Dienste mit mindestens derselben Qualitätsstufe betreiben zu können, wie das bei klassischen Telefonnetzen üblich ist – ein entsprechendes Cybersecurity-Konzept sowie kontinuierliche Netzüberwachung und -steuerung essentiell. Diese Konzepte müssen sowohl die moderne, IP-basierte, als auch die traditionelle TDM-basierte Welt berücksichtigen. Das ist wichtig, weil der Übergang zu neuen Netzstrukturen sukzessive stattfindet und bestehende Netze in der Regel eine Lebensdauer von 15 bis 20 Jahren haben und die Betriebsprozesse teilweise eng mit einer bestimmten (schon vorhandenen) Technologie verknüpft sind.

Bedrohung aus der Luft

Gefahr droht Kritischen Infrastrukturen auch aus einer völlig anderen Richtung, nämlich von oben: Die zunehmende Zahl unkontrollierter Drohnen im Luftraum stellt eine neue Bedrohung dar. Unbemannte Fluggeräte können für Spionage- und Terroranschläge missbraucht werden. Nach aktuellen Schätzungen der Deutschen Flugsicherung sind jährlich rund 400.000 Drohnen im deutschen Luftraum unterwegs. Nicht gewerblich genutzte Drohnen mit einem Gewicht von bis zu fünf Kilogramm kann praktisch jeder erwerben und steuern. Mit der steigenden Zahl der Flugobjekte nimmt auch das Risiko von Unfällen und Missbrauch zu. Besonders gefährdet sind Kritische Infrastrukturen wie Flughäfen, Fabrikgelände, Stadien, Rechenzentren oder Kraftwerke. Sie vor Spionage oder Sabotage durch Drohnen oder vor deren Absturz zu schützen, ist Teil des Sicherheitskonzepts. Das System überwacht den Luftraum und erkennt Drohnen mithilfe verschiedener Sensoren wie Videokameras, Frequenzscannern und Mikrofonen. Die externen Sensor- und Flugdaten gehen permanent und in Echtzeit an ein Sicherheitssystem, das diese Daten auswertet, analysiert und dann das unbemannte Flugobjekt klassifiziert. Je nach Sicherheitslage können in einem zweiten Schritt beispielsweise Alarme ausgelöst oder Sicherheitskräfte verständigt und die Drohne gegebenenfalls durch Störsender manipuliert werden. So entsteht eine Art Sicherheitskuppel über dem geschützten Gebiet, die es Piloten erschwert, in gesperrte Lufträume einzudringen.

Sicherheit „made in Germany“

Auf Basis unterschiedlicher Übertragungstechnologien entwickelt die Telent GmbH – ein Unternehmen der Euromicron-Gruppe – sichere Lösungen für Kritische Infrastrukturen, integriert Systeme unterschiedlicher Hersteller und unterstützt bei Konzeption, Planung, Installation, Integration, Betrieb und Wartung sowie mit weiterführenden Services.

Nico Werner, Head of Cybersecurity, Telent GmbH, www.telent.de