12 | 17 Sonderdruck für telent

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Gefahren für Kritische Infrastrukturen abwehren

www.it-administrator.de

Gefahren für Kritische Infrastrukturen abwehren

Lebensadern

von Nico Werner und Jakob Schmidt

Angriffe auf IT-Netze für Kritische Infrastrukturen wie etwa Strom- und Wasserversorgung oder das Gesundheitswesen stellen eine große Gefahr dar. Anlagen in diesen Sektoren sind besonders sensibel, weil sie zum Teil mit Betriebssystemen arbeiten, die schon 20 und mehr Jahre alt sind und daher besonderen Schutz gegen Schadsoftware benötigen. Dieser Beitrag zeigt Security-Konzepte, die neben der Technik auch den Mensch und die Prozesse berücksichtigen.

Der Ausfall zentraler Hard- oder Software oder ein Angriff von Hackern und Organisationen, die sich Zugriff auf IT-Netze zwecks Spionage, zur Sabotage, Zerstörung oder Manipulation verschaffen wollen, kann verheerende Folgen nach sich ziehen. Dies gilt insbesondere für Kritische Infrastrukturen (KRITIS). Ist in diesem Bereich ein Angriff erfolgreich, kann dies eine Gefahr für die Bevölkerung nach sich ziehen. Das zeigte vor ein paar Monaten der Hackerangriff der Schadsoftware WannaCry auf Firmen und Behörden: Krankenhäuser in Großbritannien mussten ihre Patienten nach Hause schicken, 450 Computer der Deutschen Bahn waren lahmgelegt.

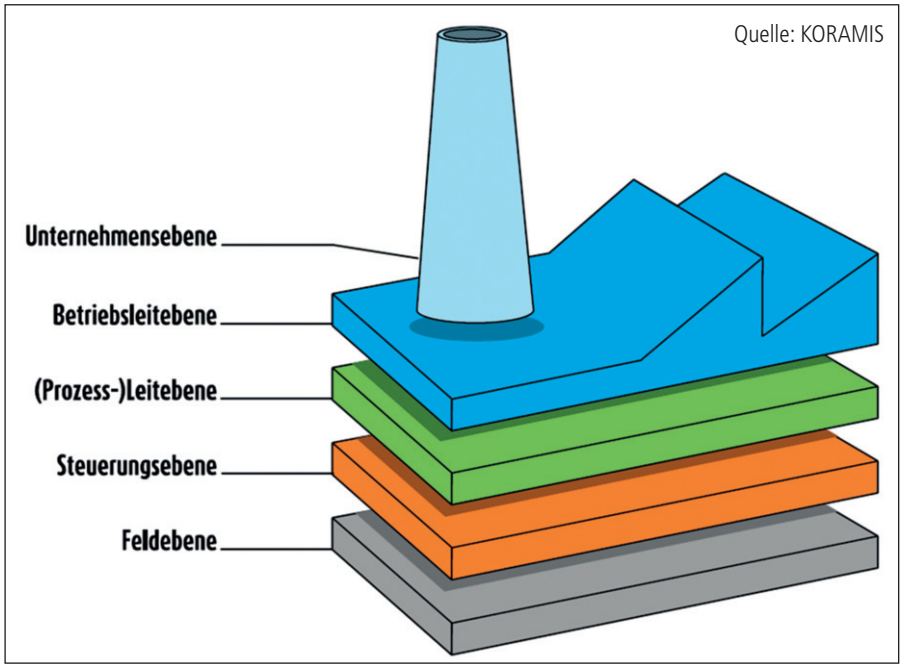
Seit das Internet of Things (IoT) in immer mehr Lebensbereiche vordringt und das Zusammenspiel von modernen Aktoren und Sensoren mit bestehenden, strategisch wichtigen IT-Systemen eine wachsende Rolle spielt, gewinnt die Sicherheit enorm an Bedeutung. Es ist daher von vitalem Interesse für Institutionen und hier insbesondere für KRITIS-Organisationen, für ein Höchstmaß an Sicherheit zu sorgen.

Gesetz definiert Kritische Infrastrukturen

Mit dem 2015 verabschiedeten IT-Sicherheitsgesetz (IT-SiG) hat die Bundesregierung neue Standards für den Schutz der Informationstechnologie formuliert. Die Verfügbarkeit und Sicherheit der IT-Systeme und Prozesse im Bereich der Kritischen Infrastrukturen spielt hier eine zentrale Rolle. Und der erste Teil der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) regelt, welche Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung unter das IT-Sicherheitsgesetz fallen. Die zweite KRITIS-Verordnung vom 30. Juni 2017 legt zusätzlich die Kritischen Infrastrukturen in den Sektoren Transport und Verkehr, Gesundheit, Finanz- und Versicherungswesen fest. Die von der Verordnung betroffenen Unternehmen sind mit dem Inkrafttreten verpflichtet, dem BSI innerhalb von sechs Monaten eine zentrale Kontaktstelle zu benennen und innerhalb von zwei Jahren die Einhaltung eines Mindeststandards an IT-Sicherheit nachzuweisen.

Gehört eine Anlage oder Teile davon zu den Kritischen Infrastrukturen, sind für sie Werte festgelegt, bei deren Erreichen oder Überschreiten der Versorgungsgrad für die Allgemeinheit nicht mehr garantiert ist. Diese Schwellenwerte sind abhängig vom jeweils zugeordneten Sektor und betreffen etwa die Trinkwassermenge in Millionen Kubikmetern im Jahr.

Unternehmen aus betroffenen Sektoren müssen ermitteln, ob sie oder Teile ihrer Anlagen und Einrichtungen in den Anwendungsbereich des IT-Sicherheitsgesetzes fallen und wie ihr Stand der Technik im Sinne des Gesetzes bezüglich IT-Sicherheit ist – konkret:



Die Schwachstellenanalyse sollte alle Ebenen einer Organisation beleuchten.

1. Sie identifizieren die kritischen Dienstleistungen, die bei einem "Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen" würden (vergleiche BSI-KritisV, Paragraf 1),
2. bestimmen die dafür notwendigen Anlagen und
3. erkennen anhand der Schwellenwerte, ob ihre Anlage als Kritische Infrastruktur einzustufen ist oder nicht.

Die Anhänge der Rechtsverordnung liefern Angaben für alle Anlagentypen inklusive deren Schwellenwerte. Allerdings gibt es auch Branchen, für die es keine Schwellenwerte gibt; sie werden durch ihre Systeme identifiziert, wie die Verkehrssteuerungs- und Leittechnik für das Netz der Bundesautobahnen. Mit Inkrafttreten von Teil 1 und Teil 2 der Verordnung haben die betroffenen Betreiber sechs Monate Zeit, die Voraussetzungen der Meldepflicht zu erfüllen. Nach weiteren zwei Jahren müssen sie die notwendigen Sicherheitsmaßnahmen umsetzen (unter anderem Informationssicherheitsmanagementsystem etwa auf Grundlage der ISO 27001).

Die neu eingefügten Paragrafen 8a und 8b des IT-Sicherheitsgesetzes des Bundesamts für Sicherheit in der Informationstechnik (BSI-Gesetzes, BSIG) sehen vor, dass die KRITIS-Unternehmen durch angemessene organisatorische und technische Vorkehrungen die informationstechnischen Systeme absichern, die für die Funktionsfähigkeit ihrer Kritischen Infrastrukturen maßgeblich sind. Ebenso müssen sie erhebliche IT-Vorfälle, wie beispielsweise Cyberangriffe, an das BSI melden.

KRITIS-Betreiber müssen also Angriffe und Sicherheitslücken schnellstmöglich erkennen und umgehend darauf reagieren können, um größeren Schaden oder die Ausbreitung der Vorfälle zu verhindern. IT-Sicherheitsvorfälle haben sie an das BSI zu melden, wo Spezialisten die Eingaben auswerten und wiederum den Betreibern Informationen zur Verfügung stellen, damit sie entsprechende Aktivitäten einleiten. Damit die Betreiber diesen besonderen Sicherheitsanforderungen gerecht werden, müssen sie – gegebenenfalls zusammen mit externen Partnern – entsprechende Konzepte erarbeiten. Dies beginnt in der Regel mit einer ganzheitlichen Schwachstellenanalyse der gesamten IT-Infrastruktur per kontinuierlicher Sicherheitsüberwachung in Echtzeit.

Schwachstellen identifizieren

Die Schwachstellenanalyse deckt Angriffspunkte sowohl in der physikalischen Infrastruktur als auch in der organisatorischen Struktur der Security-Strategie eines Unternehmens auf. Experten analysieren dabei die Sicherheit der technischen Anlagen und Prozesse und bestimmen so den tatsächlichen Sicherheitsstand der IT- und Telekommunikationsinfrastruktur:

1. In einer ersten Analyse werden die sicherheitsrelevanten Elemente der ITK-Infrastruktur festgelegt und Risiken und Abhängigkeiten im Zusammenhang mit dem Einsatz von IT-Systemen und -Prozessen grob eingeschätzt.
2. Im nächsten Schritt erfolgt eine systematische und detaillierte Erhebung aller Schwachstellen. Beispielsweise werden mithilfe von Interviews und Workshops mögliche Gefährdungen identifiziert. Zudem erfolgt eine technische Prüfung der ITK-Infrastruktur.
3. Im Anschluss werden die Erhebungen analysiert, Risiken klassifiziert, bewertet und dokumentiert. Ein Workshop thematisiert die identifizierten Schwachstellen und erläutert einen Plan mit empfohlenen Korrekturmaßnahmen für die gefundene Schwachstelle.

Diese Schwachstellenanalyse sollte nach Möglichkeit von einem externen, neutralen Dienstleister vorgenommen werden. Er hat nicht nur eine systematische Vorgehensweise, etwaige Risiken zu erkennen, sondern auch eine unvoreingenommene Sicht von außen. Neben zahlreichen Maßnahmen wie Schulung, optimierte Zutrittskontrolle, umfangreichere Dokumentation et cetera helfen technische Maßnahmen wie etwa zur Systemhärtung, Gefahren abzuwehren.

Die Schwachstellenanalyse ist für alle Bereiche von Industrie- und KRITIS-Anlagen ausgelegt:

- In der Feldebene finden sich alle Sensoren und Aktoren zur Steuerung der Produktionsprozesse. Neben Prozessdaten, etwa Temperatur oder Füllstand, werden hier auch Daten zu Sicherheit und Qualität erhoben und an die Steuerungsebene weitergeleitet.
- In der Steuerungsebene werden die Daten der Feldebene gesammelt, aufbereitet und verarbeitet. Dazu gehören unter anderem das Verwalten der Steuer- und Regelgruppen, das Ausführen entsprechender Vorgänge dieser Gruppen sowie das Weiterleiten ausgewählter Daten an die höher gelegenen Ebenen.

- In der (Prozess-)Leitebene befinden sich die automatisierenden Teile der Wertschöpfungskette. Hier werden Daten an die Planungs- und Steuerprozesse übermittelt und in einer zentralen Visualisierung dargestellt.
- In der Betriebsleitungs- und Unternehmensebene finden sich alle wesentlichen Geschäftsprozesse – typischerweise aufgeteilt nach verantwortlichen Fachbereichen und einzelnen Aktivitäten.

Systemhärtung und Sandboxing

Bei Kritischen Infrastrukturen bieten klassische Sicherheitsstrategien, wie beispielsweise das Scannen durch Antiviren-Software, kein hinreichendes Schutzniveau. Das Patchen von Betriebssystemen ohne einen Neustart ist meistens auch nicht möglich, da hierfür die Produktion heruntergefahren werden muss. Gegen Zero-Day-Exploits und zielgerichtete Angriffe von Organisationen mit entsprechenden Ressourcen und Motivation (etwa durch kriminelle Organisationen) sind tiefergehende Sicherheitsstrategien notwendig. Maßnahmen zur Systemhärtung helfen, derartige Gefahren abzuwehren, und schützen gleichzeitig vor Risiken, die Mitarbeiter oder Fremdfirmen durch Fehlverhalten verursachen.

Bei der Systemhärtung geht es, vereinfacht gesagt, darum, Regeln festzulegen, wer auf welche Systeme und deren Unterbereiche Zugriff hat und wer nicht. Insbesondere geht es darum, zu definieren, welche kritischen Anwendungen in einer Sandbox laufen sollen. Das Sandboxing 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 Sandboxes segmentiert, sodass Betriebssystem und kritische Anwendungen isoliert betrieben werden können. Dadurch ist gewährleistet, dass Eindringlinge und Malware nicht auf diese Bereiche zugreifen können. Der große Vorteil dieser Methode: Sie schützt auch vor Zero-Day-Attacken, wie etwa den durch WannaCry genutzten SMB-Exploit.

Steuerungsanlagen, wie sie in Kraftwerken und anderen Großanlagen zum Einsatz kommen, sind nicht selten mehrere Jahrzehnte im Einsatz. Einen ähnlich langen Lebenszyklus haben Systeme in Produktionsumgebungen, medizinische Ausrüstung und Geldautomaten. Hier kommen oft inzwischen veraltete Betriebssysteme wie Windows XP zum Einsatz, die etliche Schwachstellen aufweisen. Insbesondere bei solchen Systemen empfiehlt sich eine zusätzliche Absicherung durch Sandboxing. Nicht nur Legacy-Systeme lassen sich auf diese Weise schützen; auch Workstations, Server, Cloud Systeme und komplette Data Center können in eine Sandbox isoliert werden, um den Schutz vor Angriffen von außen zu erhöhen. In allen Fällen ist es unerheblich, welche Betriebssysteme – Windows oder Linux – eingesetzt sind: Das Sandboxing ist für alle gängigen Betriebssysteme möglich.

Neben den technischen Härtungsmaßnahmen ist es unabdingbar, die organisatorische Sicherheit zu erhöhen. Darunter sind alle Mittel und Schritte zu verstehen, die das Risiko seitens des Faktors Mensch einschränken. Diese können von Awareness-Trainings und -Kampagnen bis hin zum Assessment reichen. Härten bedeutet auch, die Sicherheit eines Systems zu erhöhen, indem nur dedizierte Software oder benötigte Systemkomponenten eingesetzt werden, die für den Betrieb des Systems notwendig sind und deren unter Sicherheitsaspekten korrekter Ablauf garantiert ist. Das System wird dadurch besser vor Angriffen geschützt – auch vor Gefahren, die Mitarbeiter oder Fremdfirmen durch Fehlverhalten verursachen könnten.

Fazit

ITK-Systeme Kritischer Infrastrukturen sind hochgradig gefährdet, gleichzeitig hätte ihr Ausfall womöglich verheerende Auswirkungen. Umfassende Security-Konzepte sind notwendig, um im Sinne des IT-Sicherheitsgesetzes Gefahren zu erkennen und zu beseitigen. Die Analyse möglicher Schwachstellen, die Systemhärtung und die Abwehr von neuen Gefahren wie Drohnenangriffen sollten die Verantwortlichen in Zusammenarbeit mit einem Dienstleister mit ausgewiesener Expertise angehen. *(dr)*

Nico Werner ist Head of Cybersecurity bei der telent GmbH, einem Unternehmen der euromicron Gruppe.

Jakob Schmidt ist Coordinator Documentation & Public Relations bei der KORAMIS GmbH.

Anforderungen an KRITIS-Netzwerke

Die Netze Kritischer Infrastrukturen verändern sich vom klassischen verbindungsorientierten Netz oder reinen Datennetz hin zur Multiservice-Autobahn, auf der Daten, Sprache, Video und Sensorinformationen gleichzeitig übertragen werden. Charakteristisch für solche Netze ist der Einsatz unterschiedlicher Übertragungsprotokolle wie etwa PDH, SDH, Richtfunk, IP-MPLS, IP-Ethernet et cetera. Zudem stammen die eingesetzten Netzelemente häufig von verschiedenen Herstellern.

KRITIS-Kommunikationsnetze bringen jedoch spezielle Anforderungen an Zuverlässigkeit, Sicherheit und Vertraulichkeit bei der Übertragung von Daten und Sprache mit sich. 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 essenziell. Sie müssen sowohl die moderne IoT-/IP-basierte als auch die traditionelle TDM-basierte Welt umfassen und vereinen. Das ist darum wichtig, weil der Übergang zu neuen Netzstrukturen sukzessive stattfindet und bestehende Netze in der Regel eine Lebensdauer von 15 bis 20 Jahren haben. Noch dazu sind die Betriebsprozesse teilweise eng mit einer bestimmten Technologie verknüpft.

Rechtlicher Rahmen

Bestandteile des IT-Sicherheitsgesetzes

- Mindestniveaus IT-Sicherheit
- IT-Störungen an das BSI melden
- IT nach "Stand der Technik" absichern
- IT mindestens alle zwei Jahre prüfen
- gegebenenfalls branchenspezifische Mindeststandards definieren
- Schwellenwerte für KRITIS beachten

Aufgaben für Unternehmen

- Verpflichtende Berichterstattungen: Meldestelle, Vorfallberichterstattung, Kontaktstelle für das BSI
- Mindestniveau IT-Sicherheit
- Umsetzung von Mindeststandards