A 2595

NET

Zeitschrift für Kommunikationsmanagement

Sonderdruck

Sicherheitsnetze und kritische Infrastrukturen

BREKO Bundesverband Breitbandkommunikation e.V.

PMeV NETZWERK SICHERE KOMMUNIKATION

NET Verlagsservice, PF 11 13, D-15567 Woltersdorf; Postvertriebsstück, Entgelt bezahlt

Systemhärtung schützt

Gefahren für kritische Infrastrukturen und ihre Abwehr

Nico Werner, Jakob Schmidt

Angriffe auf IT-Netze kritischer Infrastrukturen (Kritis) wie etwa Behörden, Netzbetreiber und Unternehmen können eine große Gefahr für die Bevölkerung darstellen. Diese Anlagen sind besonders anfällig, weil sie oftmals mit Betriebssystemen arbeiten, die viele Jahre alt sind und außerhalb des Support-Zeitraums durch den Hersteller liegen. Daher benötigen sie besonderen Schutz gegen Schadsoftware. Dabei ist die technische Seite nur ein Aspekt: Umfassende Security-Konzepte sollten einen ganzheitlichen Ansatz verfolgen und sowohl Technik als auch Mensch und Prozesse berücksichtigen.

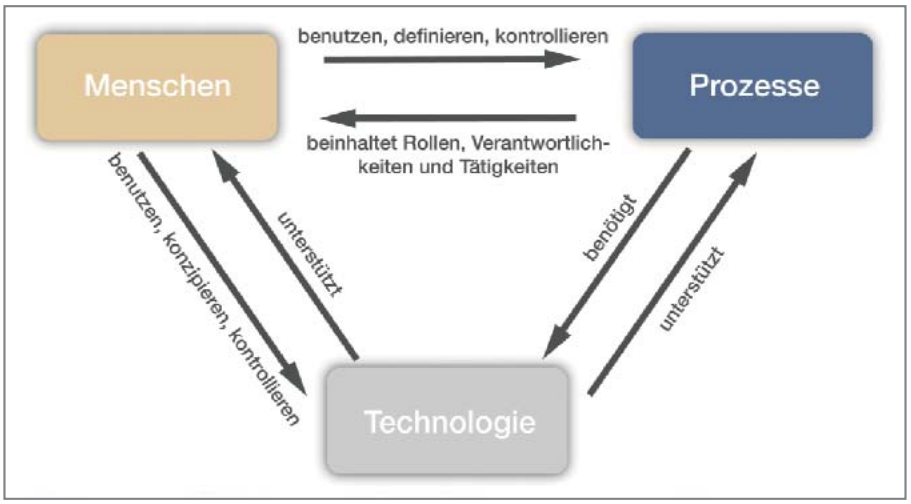

Bild 1: Ein gesamtheitliches Sicherheitskonzept muss Menschen, Prozesse und Technologie einbeziehen (Grafik: Telent)

Der Ausfall zentraler Hard- oder Softwarekomponenten oder ein Angriff von Hackern, die sich Zugriff auf Betriebsnetze verschaffen, sei es zu Spionage- oder Sabotagezwecken, kann verheerende Folgen haben – insbesondere, wenn kritische Infrastrukturen betroffen sind. Kommt es hier zu Ausfällen oder Beeinträchtigungen, kann das zur Gefahr für die Bevölkerung werden. Einen Vorgeschmack lieferte Anfang Mai der Angriff mit der Schadsoftware WannaCry. Der Kryptotrojaner konnte sich innerhalb von Netzen ohne weiteres Zutun der Nutzer wurmartig verbreiten und attackierte weltweit Privatrechner, aber auch solche von Behörden, Unternehmen und Organisationen, wie beispielweise der Deutschen Bahn oder von Krankenhäusern.

Seit das Internet of Things (IoT) in immer mehr Lebensbereiche vordringt und das Zusammenspiel von modernen Aktoren und Sensoren mit bestehenden, historisch gewachsenen Anlagen (Legacy-Systemen) eine wichtige Rolle spielt, gewinnt das Thema Cybersecurity enorm an Bedeutung. Es ist daher von vitalem Interesse – vor allem im Bereich Kritis – für ein Höchstmaß an Sicherheit zu sorgen, um die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu jedem Zeitpunkt zu gewährleisten (*Bild 1*).

Individuelle Strategien für komplexe Sicherheitsanforderungen

Je mehr Anlagen und Systeme miteinander vernetzt sind, desto wichtiger sind durchdachte und umfangreiche IT-Sicherheitskonzepte. Mit dem 2015 verabschiedeten IT-Sicherheitsgesetz (IT-SiG) und den zugehörigen Verordnungen hat die Bundesregierung neue Standards für den Schutz in der Informationstechnologie formuliert. Die Schutzziele der IT-Systeme und Prozesse im Bereich der kritischen Infrastrukturen spielen hier eine zentrale Rolle.

Kritis-Betreiber müssen Angriffe und Sicherheitslücken schnellstmöglich erkennen und umgehend darauf reagieren können, um größeren Schaden oder die Ausbreitung der Vorfälle zu verhindern. Schwerwiegende IT-Sicherheitsvorfälle haben sie an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Damit die Betreiber diesen besonderen

Nico Werner ist Head of Cybersecurity bei der Telent GmbH in Backnang,
Jakob Schmidt ist Coordinator Documentation & Public Relations bei der Koramis GmbH in Saarbrücken

Sicherheitsanforderungen gerecht werden, können sie zusammen mit externen Experten entsprechende Konzepte erarbeiten. Dies kann mit einer ganzheitlichen Sicherheitsanalyse der gesamten IT-Infrastruktur, -Prozesse und der Organisation beginnen. Im Rahmen dieser übergeordneten Analyse überprüfen Experten auch das individuelle Sicherheitskonzept von Unternehmen (*Bild 2*). Erkennen sie Schwachstellen, dokumentieren und bewerten sie diese und entwickeln einen entsprechenden Maßnahmenplan.

Sicherheit auch in heterogenen Netzstrukturen

Ein Beispiel für die Veränderungen, die die Digitalisierung mit sich bringt, sind beispielsweise Kommunikationsnetze. Sie wandeln sich vom klassischen Bürokommunikationsnetz hin zum hochkomplexen Multiservice-Betriebsnetz, innerhalb dessen Daten, Sprache, Video und Sensorinformationen gleichzeitig übertragen werden. Charakteristisch für solche Netze ist der Einsatz unterschiedlicher Übertragungstechniken wie etwa PDH (Plesiochrone Digitale Hierarchie), SDH (Synchrone Digitale Hierarchie), Richtfunk, IP (Internetprotokoll) und MPLS (Multiprotocol Label Switching).

Erschwerend kommt hinzu, dass die eingesetzten Netzelemente häufig von verschiedenen Herstellern stammen. Gleichzeitig müssen Betriebsnetze im Bereich Kritis spezielle Anforderungen hinsichtlich Zuverlässigkeit, Sicherheit und Vertraulichkeit bei der Übertragung von Daten und Sprache erfüllen.

Aus diesen Gründen sind ein entsprechendes Managementkonzept sowie die kontinuierliche Netzüberwachung und -steuerung essenziell. Es muss sowohl die moderne IoT-/IP-basierte, als auch die traditionelle TDM-basierte Welt (TDM – Time Division Multiplexing) umfassen und vereinen. 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.

Priorität: Schwachstellen erkennen

Die Schwachstellenanalyse erkennt Angriffspunkte sowohl in der physischen Infrastruktur als auch in der organisatorischen Struktur der Security-Strategie eines Unternehmens. Experten analysieren dabei die Sicherheit der technischen Anlagen und Prozesse und bestimmen so den tatsächlichen Sicherheitsstand der IKT-Infrastruktur (Informations- und Telekommunikationstechnik).

Bild 2: Das Nationale IT-Lagezentrum im Bundesamt für Sicherheit in der Informationstechnik (BSI)

(Foto: BSI)

Wie sieht eine Schwachstellenanalyse aus?

- Zunächst werden das Ziel, der Umfang und die Objekte der Analyse festgelegt. Diese Phase umfasst zudem eine grobe Aufnahme zur ersten Einschätzung der Risiken und Abhängigkeiten im Zusammenhang mit dem Einsatz von IT-Systemen und -Prozessen.
- Im nächsten Schritt werden vorhandene Dokumente und Informationen geprüft und darauf aufbauend die Vor-Ort-Analyse vorbereitet.
- Danach erfolgt eine breit angelegte, systematische und detaillierte Erhebung der Schwachstellen. Beispielsweise werden mithilfe von Interviews und Workshops mögliche Gefährdungen in den Gesamtprozessen identifiziert. Dies erfolgt durch Fragebögen, deren Umfang und Inhalt individuell an das jeweilige Unternehmen angepasst wird. Eine zielgerechte und effiziente Bearbeitung wird dadurch ermöglicht. Zudem erfolgt eine technische Prüfung der IKT-Infrastruktur.
- Im Anschluss 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 gefundene Schwachstelle.

Die Schwachstellenanalyse sollte von einem externen, neutralen Dienstleister vorgenommen werden, da er die unvoreingenommene Sicht eines Außenstehenden mitbringt. Neben zahlreichen Maßnahmen wie etwa Schulungen, Awareness-Maßnahmen und Optimierung der Zutrittskontrollen helfen auch Maßnahmen zur Systemhärtung, um Gefahren abzuwehren.

Schutz durch Systemhärtung

Bei kritischen Infrastrukturen bieten klassische Sicherheitsanwendungen, wie Antivirensoftware kein hinreichendes Schutzniveau. Gegen Zero-Day-Exploits und zielgerichtete Angriffe sind alternative 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 darum, Maßnahmen umzusetzen, die die potenzielle Angriffsfläche so weit wie möglich reduzieren.

Zur Systemhärtung gehört u.a. das Scannen der Systeme. Dadurch lassen sich Systeme identifizieren, die bereits durch Schadsoftware befallen sind.

Vor der Umsetzung weiterer Maßnahmen werden diese bereinigt. Eine weitere der Systemhärtung zuzurechnende Maßnahme ist die Mikrosegmentierung. Dabei stellen vor die Systeme geschaltete Hardware-Firewalls sicher, dass nur über zuvor spezifizierte Ports kommuniziert werden kann. Diese Firewalls sind der einzige Weg, um über das Netz auf das System zuzugreifen. Secure Boot überträgt das System auf einen Flash-Speicher, von dem aus es ausschließlich gestartet wird; auch diese Vorgehensweise ist der Systemhärtung zuzurechnen. Da keine Schreibrechte bestehen, hat Malware, die während der Laufzeit des Systems aktiviert wird, keine Chance, nach einem Reboot des Systems weiter aktiv zu sein.
Jede Schnittstelle bietet eine mögliche Angriffsfläche, daher sollte ihre Anzahl so gering wie möglich gehalten werden. Unter dem Begriff Schnittstellenreduzierung fasst man mehrere physische Schutzmaßnahmen zusammen, etwa das Absichern von nicht benötigten USB-Ports mithilfe von Schlössern oder die Deaktivierung nicht benötigter Dienste des Betriebssystems.
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.

Sicherheit im Sandkasten

Sandboxing („Sandkasten") steht für eine Technik, mit der eine Software innerhalb einer isolierten – von den restlichen System- oder Netzressourcen abgeschotteten – Laufzeitumgebung ausgeführt wird. Das gesamte System ist in mehrere Sandboxes segmentiert, so dass Betriebssystem und kritische Anwendungen isoliert betrieben werden können. Dadurch ist gewährleistet, dass Eindringlinge und Malware nicht auf diese Bereiche zugreifen können. Diese Methode schützt auch vor Zero-Day-Attacken, wie etwa den durch WannaCry genutzten SMB-Exploit.

Die Steuerungsanlagen, wie sie in Kraftwerken und anderen Großanlagen zum Einsatz kommen, sind oft mehrere Jahrzehnte im Einsatz. Einen ähnlich langen Lebenszyklus haben Systeme in Produktionsumgebungen, Medizingeräte und Geldautomaten. Hier kommen oft veraltete Betriebssysteme zum Einsatz, die etliche Schwachstellen aufweisen. Insbesondere hierbei empfiehlt sich eine zusätzliche Absicherung durch Sandboxing. Nicht nur Legacy-Systeme lassen sich auf diese Weise schützen, auch Workstations, Server, Cloud-Systeme und ganze Datacenter können in eine Sandbox isoliert werden, um den Schutz vor Angriffen von außen zu erhöhen.

Bild 3: Durch den Einsatz von speziellen Detektionssystemen kann man den Luftraum überwachen und mithilfe verschiedener Sensoren wie Videokameras und Frequenzscannern Drohnen erkennen

(Grafik: Dedrone)

Bedrohung aus der Luft

Gefahr droht kritischen Infrastrukturen auch aus der Luft. Die zunehmende Zahl unkontrollierter Drohnen im Luftraum stellt eine neue Bedrohung dar, der Missbrauch der unbemannten Fluggeräte wächst. 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 5 kg kann praktisch jedermann erwerben und steuern.
Mit der steigenden Zahl der Flugobjekte nimmt auch das Risiko von Unfällen und Missbrauch zu. Besonders gefährdet sind Flughäfen, Rechenzentren oder Kraftwerke. Sie vor Spionage oder Sabotage durch Drohnen zu schützen, sollten zukünftige Sicherheitskonzepte ebenfalls berücksichtigen.
Durch den Einsatz von speziellen Detektionssystemen kann man den Luftraum überwachen und mithilfe verschiedener Sensoren wie Videokameras und Frequenzscannern Drohnen erkennen. Die erfassten Daten gehen permanent an ein zentrales Kontrollsystem, das diese Daten auswertet, analysiert und das unbemannte Flugobjekt klassifiziert. Abhängig von der Sicherheitslage werden in einem zweiten Schritt Alarme ausgelöst, Sicherheitskräfte verständigt und die Drohnen gegebenenfalls durch Störsender manipuliert. So entsteht eine virtuelle Sicherheitskuppel über dem geschützten Gebiet, die es erschwert, unbefugt Gelände zu überfliegen oder in gesperrte Lufträume einzudringen (*Bild 3*).

Fazit

IKT-Systeme kritischer Infrastrukturen sind mehr denn je hochgradig gefährdet, gleichzeitig hätte ihr Ausfall verheerende Auswirkungen auf Wirtschaft, Gesellschaft und die innere Sicherheit. Umfassende Security-Konzepte sind notwendig, um im Sinne des IT-SiG Gefahren zu erkennen und zu beseitigen. Die Analyse möglicher Schwachstellen, die Systemhärtung und die Abwehr von „neuen" Gefahren wie Drohnenangriffe sollten die Verantwortlichen in enger Zusammenarbeit mit einem externen Dienstleister mit ausgewiesener Expertise angehen. *(bk)*