Unter der Lupe

Monitoring und Sicherheitsanalyse kritischer Industrienetze aus der Box

Kai-Oliver Detken

Kritische Infrastrukturen (Kritis) sind auch in mittelständischen Betrieben (z.B. Wasserversorger, Stadtwerke) zu finden und müssen dementsprechend geschützt werden. Allerdings fehlt hier oftmals das entsprechende Expertenwissen, um BSI-Empfehlungen und notwendige Sicherheitslösungen umzusetzen. Aus diesem Grund wird im Forschungsprojekt ScanBox ein „Out-of-the-Box"-System entwickelt, das vollautomatisch eine Sicherheitsanalyse durchführen und die Ergebnisse anschließend visualisieren soll. Die empfohlenen Gegenmaßnahmen bzw. Handlungsempfehlungen werden dabei automatisch auf den Empfehlungen des BSI zum IT-Grundschutz basieren.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Die Automatisierungs- und Steuerungstechnik ist durch proprietäre Systeme sowie lange Lebenszyklen lange Zeit gekennzeichnet worden. Hierbei stand und steht die Verfügbarkeit der Systeme an erster Stelle. Laufende Aktualisierungen der eingesetzten Software durch Patches und Updates, kurze Einsatzzeiten von Rechnersystemen und Härtung der Komponenten und Systeme konnten aufgrund unterschiedlicher Restriktionen oft nicht genutzt werden. In Scada- bzw. PDN-Umgebungen (Scada – Supervisory Control and Data Acquisition, übergeordnete Steuerung und Datenerfassung; PDN – Produktionsdatennetze, gleichzusetzen mit Scada) werden daher viel restriktiver Softwarekomponenten aktualisiert, als das in Office-Netzen der Fall ist. Neue Standards müssen zudem erst durch langwierige Zertifizierungsprozesse, bevor sie für den Markt freigegeben werden. Hinzu kommt die Meldepflicht von Hackerangriffen, die das neue IT-Sicherheitsgesetz für Kritis-Betreiber vorsieht. Hier hätte ein Ausfall z.B. der Strom- und Wasserversorgung erhebliche Folgen für die Wirtschaft, den Staat und die Gesellschaft eines Landes. Die Verfügbarkeit und IT-Sicherheit spielen somit im Kritis-Umfeld eine wichtige und zentrale Rolle. Damit kommen auf solche Unternehmen aber auch ganz neue Anforderungen zu, die organisatorisch und technisch bewältigt werden müssen.

Stetig werden immer mehr IT-Techniken eingesetzt, die im Internetumfeld gebräuchlich sind, um die Vernetzung voranzutreiben. Dies bietet einige Vorteile für die Produktionsdatennetze:

- enge Integration von Produktions- und Geschäftsprozessen;
- bessere Steuerungsmöglichkeiten, Erhöhung der Agilität;
- Fernwartung und Remote-Monitoring zur schnellen Fehlerbehebung;
- bessere und zeitnahe Analysen.

In den Produktionsumgebungen stellt dabei der Verlust von sensiblen Daten nur einen kleinen Teil der Gefährdungen dar. Dadurch, dass Automatisierungs- und Steuerungstechnik direkt auf den Produktionsprozess einwirken, ergeben sich andere Gefahren als in der sog. Office-IT:

- Ausfall der Produktion;
- Lebensgefahr für Mitarbeiter;
- Konsequenzen für die Umwelt;
- Ausfall strategischer Infrastrukturen.

Beim Einsatz von Standardprotokollen aus dem Internetumfeld, ergeben sich auf einmal aber die gleichen Gefährdungsvektoren wie für die Office-IT. Im Gegensatz zu den Netzen in der Verwaltung ist in Produktionsnetzen aber die Zuständigkeit oft nicht geklärt: Sind es die technischen Mitarbeiter der Produktionsnetze, die ihre Prozesse und Systeme genau kennen, oder ist es der Sicherheitsbeauftragte des Unternehmens, der sich aber besser in der Office-IT-Umgebung auskennt?

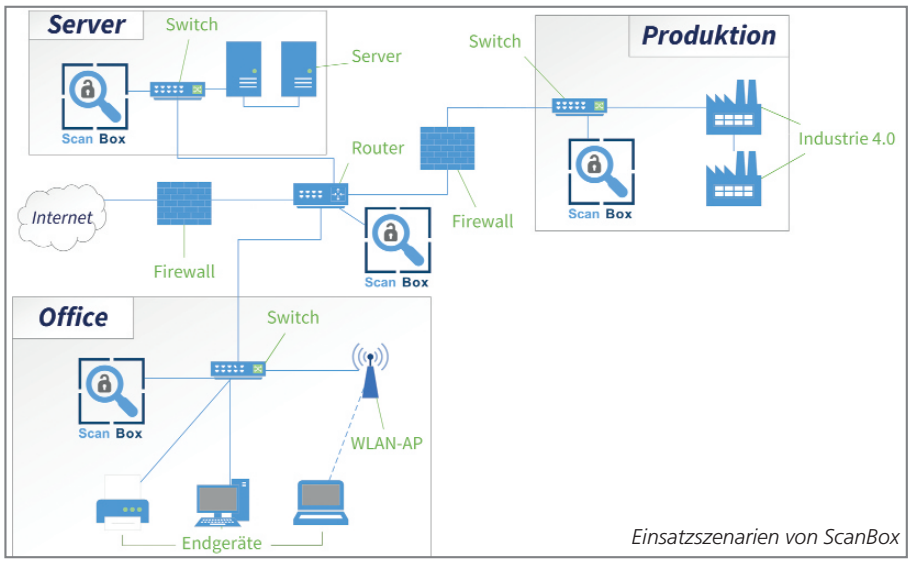
Zusätzlich werden vermehrt Netze verwendet, die auf einen gemeinsamen Verzeichnisdienst (LDAP, AD) zugreifen. Dadurch könnte sich ein Angreifer Zugang zu den Basisdiensten verschaffen, um anschließend auf die kritischen Produktionsumgebungen zugreifen zu können. Hier bieten sich besonders Wartungszugänge an, die den direkten Zugriff auf die PDN-Umgebung ermöglichen und direkt attackiert werden können.

Durch die zunehmende Vernetzung sind aber grundsätzlich IT-basierte Überwachung und Steuerung von Produktionskapazitäten einem höheren Risiko ausgesetzt. So könnte ein Hacker z.B. die Verteilung von Gas oder Strom gezielt attackieren, um einen Blackout auszulösen. Steuerung und Abruf von Produktionsständen werden heute vermehrt über Webservices abgewickelt

und erfolgen nicht mehr über hermetisch abgeriegelte interne Systeme der Energiehersteller und Netzbetreiber. Diese webbasierten Anwendungen müssten kontinuierlich auf dem neuesten Stand gehalten werden, will man Sicherheitslücken vermeiden. Trotzdem kann es immer wieder zu ungewollten Risiken kommen, wie Stuxnet (Computerwurm, der 2010 entdeckt und speziell zum Angriff auf Scada-Systeme von Siemens hergestellt wurde. Über ihn wurde gezielt in die Steuerung von Frequenzumrichtern in Industrieanlagen eingegriffen, um die Geschwindigkeit von Motoren zu beeinflussen.) und dessen Nachfolger Flame (Virus von 2012, der verschiedene Malware-Techniken wie Backdoor-, Trojaner- und Wurm-Funktionalitäten in sich vereint und dadurch ein ganzes Malware-Toolkit abgibt. Die Software konnte die Betriebssysteme Windows XP, Windows Vista und Windows 7 über die Update-Funktion infizieren.) effektiv gezeigt haben. Daran erkennt man, dass Kritis-Netze wesentlich besser abgesichert werden sollten, als dies momentan der Fall ist.

Sicherheitsmaßnahmen

Die IT-Systeme von Firmen können heute vor zahlreichen Bedrohungen geschützt werden, indem eine entsprechende Sicherheitsarchitektur realisiert wird. Speziell das Zusammenspiel zwischen Produktions- und Office-Netz sollte darin geregelt werden, wenn ein Unternehmen beide Varianten besitzt. Dabei spielt die Netzsegmentierung mithilfe von virtuellen Netzen (Virtual LAN – VLAN) eine wichtige Rolle, um über Firewalls eine Trennung zwischen verschiedenen Netzbereichen vornehmen zu können. Dadurch wäre ein Virus nicht in der Lage, alle Netzbereiche gleichzeitig zu infizieren, sondern befällt erst einmal nur einen Teilbereich. Diese Strukturierung ist bereits bei reinen Office-Netzen wichtig. Hier sollte man das Backup-System z.B. nicht im gleichen Subnetz positionieren, in dem sich auch der zentrale Dateiserver befindet. Denn falls einmal ein Verschlüsselungstrojaner den Weg ins interne Netz gefunden haben sollte, ist wenigstens das



Einsatzszenarien von ScanBox

Backup noch vorhanden und kann zum Einspielen der Datensicherung wiederverwendet werden. Um eine Trennung von Produktions- und Office-Netzen zu ermöglichen, sollten daher ein oder mehrere VLANs eingesetzt werden. Durch die Einteilung z.B. der Bereiche PDN und Office-Netz in weitere VLANs hätten Clients in Office-Netz 1 keinen Zugriff auf die Clients in Office-Netz 2, könnten aber gemeinsame Ressourcen, wie z.B. Dienteserver verwenden. Über die VLANs können alle physisch erreichbaren Endpunkte verfügbar oder unzugänglich gemacht werden.

Damit die Mitarbeiter aus dem PDN Internetzugriff haben, die Produktion aber abgesichert wird, könnte zusätzlich eine demilitarisierte Zone (DMZ) zum Einsatz kommen. Dann haben die Benutzer aus dem Internet keinen Zugriff auf das interne Netz, sondern nur auf gezielt freigegebene Ressourcen. In der DMZ befinden sich üblicherweise Server wie Web-, Proxy-, Mail-, Authentifizierungsserver oder Application Gateways. Ein Proxyserver wird dann z.B. die Informationen zwischen dem Office-Netz und Webservern im Internet austauschen. Er wird die Anfragen entgegennehmen und in beide Richtungen weiterleiten, ohne einen direkten Zugriff zu ermöglichen.

Das ScanBox-Projekt

Das ScanBox-Projekt ist ein BMWI-Projekt, das aus dem Kooperationsprojekt DiSiNet hervorging und eine Laufzeit von zwei Jahren (2018-2020) hat. Ziel ist die Entwicklung einer Hardware-Appliance zur Erhebung und Dokumentation des Sicherheitsniveaus in Klein- und mittelständischen Unternehmen (KMU). Das Gerät soll, im Gegensatz zu üblicherweise statischen Erhebungen, ohne manuellen Eingriff das Sicherheitsniveau der überwachten Infrastruktur permanent evaluieren und automatisiert Handlungsempfehlungen ableiten. Dafür wurden existierende Scan-, Analyse- und Penetrationswerkzeuge analysiert, implementiert sowie selbst entwickelt. Ein zentrales Managementmodul übernimmt die Koordination sämtlicher Funktionen und verhindert Risiken für die überwachten Netze. Die konsolidierten Scan- und Monitoring-Ergebnisse sollen in zielgruppenspezifischen Berichten zusammengefasst werden.

Der innovative Teil des Projektes verfolgt somit den Ansatz einer Sicherheitsanalyse, die auf den Empfehlungen des BSI zum IT-Grundschutz basiert. Über die Integration der Datenbank Common Vulnerabilities and Exposure (CVE) soll ein Bezug zu den vom BSI entsprechend empfohlenen Gegenmaßnahmen hergestellt werden. Die CVE-Datenbank ist inzwischen ein Industriestandard, dessen Ziel die Einführung einer einheitlichen Namenskonvention für Sicherheitslücken und andere Schwachstellen in Computersystemen ist. Mehrfachbenennung gleicher Gefahren durch verschiedene Unternehmen oder Institu-

tionen werden um eine laufende Nummer (z.B. CVE-2019-2105) ergänzt, um eine eindeutige Identifizierung einer bestimmten Schwachstelle zu gewährleisten. Dadurch ist ein reibungsloser Informationsaustausch zwischen den verschiedenen Datenbanken einzelner Hersteller möglich geworden.

Im *Bild* wird die generische Darstellung verschiedener Einsatzszenarien verdeutlicht. So ist die ScanBox-Appliance in der Lage, zwischen Produktions- und Office-Netz zu unterscheiden. Das ist notwendig, da man z.B. in Produktionsnetzen keine aktiven Scans ausführen darf, um Anomalien aufzuspüren. Grund ist, dass die IT-Systeme von PDNs oft viel zu „schwachbrüstig" ausgelegt sind, um viele Anfragen gleichzeitig zu beantworten, weshalb ein solcher Scan Verzögerungen oder gar den Ausfall eines Systems verursachen könnte. Dies gilt es unbedingt zu vermeiden. Ein weiteres Leistungsmerkmal wird sein, dass die ScanBox-Appliance in verschiedenen Netzsegmenten nach Anomalien suchen kann, um diese an ein zentrales System zu schicken. So lassen sich auch gekapselte Netzsegmente mit in das Monitoring einbetten.

Während die agentenbasierte Untersuchung der Netzsegmente und des Netzverkehrs auf bekannte Angriffssignaturen lediglich Aussagen zu bereits existierenden Gefährdungen liefern kann, sind gezielt eingesetzte moderierte Penetrationstests bzw. Anomalieanalyseverfahren in der Lage, auch Gefährdungen zu identifizieren, die im Netz noch keine Wirkung entfaltet haben. Dies soll ebenfalls durch ScanBox geleistet werden. Die Funktionen sollen dabei automatisiert ablaufen. Sensoren scannen aktiv oder passiv (je nach Anforderung) das entsprechende Netzsegment und liefern Loginformationen, die in einer Datenbank zusammengefasst und normalisiert werden. Die Auswerteeinheit fasst die relevanten Ergebnisse zusammen, bewertet diese und visualisiert sie in einem Endbericht. So lässt sich kontinuierlich die interne IT-Sicherheit eines Unternehmensnetzes erfassen, analysieren und einheitlich ausgeben.

Problematisch ist allerdings in PDNs, dass diese immer noch von proprietären Systemen beherrscht werden, die eine gewisse Herstellerabhängigkeit beinhalten und wenige offene Schnittstellen zulassen. Zusätzlich steht in diesen Systemen die Verfügbarkeit an oberster Stelle. Dadurch lassen sich neue Monitoring-Systeme nicht einfach integrieren, sondern müssen erst von dem jeweiligen Hersteller freigegeben werden. Denn ein Scada-Hersteller legt die Verfügbarkeit seiner Systeme gegenüber dem Kunden fest und möchte diese durch den Einsatz von Fremdsystemen nicht gefährden. Hinzu kommt, dass Switche im Produktionsumfeld nicht immer den Standards von Office-Netzen genügen. So gibt es durchaus Switch-Hersteller, die keinen Mirroring-Port anbieten, um den Netzverkehr dieser Komponente komplett analysieren zu können. Dadurch wird die Sichtbarkeit auf alle Netzsegmente eingeschränkt oder zumindest steigt der Aufwand, diese im Monitoring mit zu erfassen.

Ausblick

Allerdings gilt es auch, neue Herausforderungen zu meistern, die durch die Projektziele aufgetreten sind. So lassen sich z.B. die BSI-Handlungsempfehlungen nur schwer direkt auf Unternehmensrichtlinien anpassen. Einer der Hauptgründe liegt darin, dass die Handlungsempfehlungen zu abstrakt beschrieben sind. Das BSI gibt keine konkrete Vorgehensweise vor, wie im Fall einer bestimmten Anomalie technisch vorgegangen werden soll. Demzufolge muss der IT-Administrator oder Sicherheitsbeauftragte über die erforderlichen Kenntnisse verfügen, um Maßnahmen richtig verstehen und anwenden zu können. Dies ist aber oft nicht gegeben. Bei dem SIEM-Hersteller Logrhythm z.B. (SIEM – Security Information and Event Management, kombiniert die zwei Konzepte Security Information Management und Security Event Management für die Echtzeitanalyse von Sicherheitsalarmen aus den Quellen Anwendungen und Netzkomponenten) wird daher die BSI-Maßnahme „Audit und Protokollierung der Aktivitäten im Netz" z.B. folgendermaßen umgesetzt: Alle Logfiles werden vom SIEM-System zyklisch geprüft und jede Komponente im Netz soll entsprechende Protokolldaten schreiben. Bei einem Verstoß wird eine Alarmierung durchgeführt.

Ähnlich will man auch bei ScanBox die Umsetzung der einzelnen BSI-Maßnahmen vornehmen. Dabei sollen CIS-Benchmarks (CIS – Center for Internet Security, Zusammenschluss von Organisationen und Einzelpersonen, um Materialien und Ressourcen zum Thema Internetsicherheit zur Verfügung zu stellen; besondere Beachtung finden dabei die sog. Benchmarks, um spezifische Computersysteme im Rahmen eines Einsatzes im Internet gegen Bedrohungen abzusichern, **https://www.cisecurity.org**) mit einfließen, die öffentlich verfügbar sind und konkrete Handlungsanweisungen enthalten, um Systeme entsprechend abzusichern. Neben technischen werden auch organisatorische Maßnahmen einbezogen. CIS-Benchmarks liefern zudem detaillierte Konfigurationen für BSI-Maßnahmen, wodurch der IT-Grundschutzkatalog des BSI mit einbezogen werden kann. CIS-Benchmark-Dokumente können direkt von der CIS-Webseite oder von einem GitHub-Repository (**https://github.com/cismirror/benchmarks**) heruntergeladen werden.

Eine weitere Herausforderung ist die Erkennung von Anomalien, die noch nicht bekannt sind und dementsprechend auf keine Mustererkennung reagieren. Dazu muss das Normalverhalten eines Netzes bekannt und die Protokollierung aller Komponenten aktiviert sein. Hier besitzen Produktionsnetze einen Vorteil gegenüber Office-Netzen, da der Netzverkehr relativ statisch ist und daher das Normalverhalten einfacher definiert werden kann. Allerdings ist oft in diesem Umfeld auch die Protokollierung deaktiviert, um keine unnötige Netz- und Komponentenlast zu erzeugen. Daher muss man letztendlich einen Kompromiss zwischen Verfügbarkeit und IT-Sicherheit auf sich nehmen, will man sich kontinuierlich gegen Anomalien wappnen. *(bk)*