IT-Sicherheit in Produktionsnetzen (PDN)
– Aufspüren, einschätzen und beseitigen von Sicherheitsbedrohungen –

Ulrich Neider

Bedrohungen von IT-Systemen sind heute gravierender denn je. Immer öfter werden Vorfälle von erfolgreichen Hackerangriffen bekannt. Die Gefahren gehen jedoch immer stärker von Innentätern aus, die mit ihrem Insiderwissen noch größeren Schaden anrichten könnten.

Der Beitrag beschäftigt sich aus aktuellem Anlass mit Bedrohungen für Produktionsdatennetze. Ein konkretes Beispiel ist der Stuxnet-Angriff, der zentrale Steuerungssysteme der Firma Siemens in einer spezifischen Ausprägung im Visier hatte. Die massiven Auswirkungen auf Produktionsanlagen durch das Virus Stuxnet im Iran werden permanent in der Presse thematisiert. Diese enorme Beeinträchtigung durch das gezielte Ausnutzen von IT-Verwundbarkeiten eines zentralen Systems durch einen komplizierten Virus hat eine Dimension erreicht, die in der Vergangenheit unbekannt

war. Aus Sicht eines erfahrenen Experten im IT-Sicherheitsumfeld sind die Risiken für Produktionsdatennetze (PDN) Systeme jedoch nicht nur auf möglichen Virenbefall zurückzuführen.

Die Firma DETACK beschäftigt sich seit dem Jahr 2000 mit IT-Sicherheit und agiert als Sparringpartner sowohl konzeptionell als auch praktisch, um das IT-Sicherheitsniveau langfristig zu erhöhen und Bedrohungspotentiale durch Beratung und Sicherheitsprüfungen zu verringern.

Dieser Beitrag liefert Denkanstöße, um eine allgemeine Sensibilisierung für Gefahren, denen Produktionssysteme ausgesetzt sind, zu schärfen. Potentielle Bedrohungen lediglich zu kennen, ist passiv. Dem Autor geht es in diesem Beitrag darum, Wege aufzuzeigen, wie auch konzeptionell und aktiv herangegangen werden kann.

Die aktive Herangehensweise beginnt üblicherweise mit einer internen Sicherheitsuntersuchung der PDN Umgebung. Diese Analyse dient dann der Erstellung bzw. Aktualisierung einer Sicherheitspolicy für das Produktionsdatennetz, verbunden mit praktischen Handlungsanweisungen, Richtlinien und einfach umzusetzenden Checklisten. Dies ist keine einmalige Tätigkeit, sondern es empfiehlt sich diese Policy regelmäßig durch Analysen auf den neusten Stand zu bringen, um auch aktuellen Bedrohungen gerecht zu werden. Der stetige Wandel durch Veränderungen im Einsatz von IT-Technik und der Unternehmensorganisation muss auch berücksichtigt werden.

In diesen fortlaufenden Prozess können externe Dienstleister einbezogen werden, die in diesem Kreislauf die Wirksamkeit der Sicherheitspolicy und weitere organisatorische Maßnahmen verifizieren. Dies wird üblicherweise durch Audits und Sicherheitsprüfungen, auch Penetrationstests genannt, ermittelt. Organisatorische Audits gehören auch zu diesem Prozess. Die Ergebnisse dieser Prüfungen fließen dann inhaltlich in die strategisch-operativen Vorgaben ein, so dass ein stetiger Prozess entsteht, der dazu beiträgt, die IT-Sicherheit des PDN und der Gesamtunternehmung zu erhöhen.

Der Autor stellt ein Phasenmodell aus der eigenen Beratungspraxis vor, wie die Sicherheit von Produktionsdatensystemen durch die Einführung von Sicherheits-Controls erhöht werden kann.

Der Gesamtprozess wird in sechs Schritte unterteilt. Gemäß der Devise, dass nur geprüft werden kann, was als schützenswertes Objekt klassifiziert ist, steht am Anfang eine Bestandsaufnahme aller zu untersuchenden Systeme und Komponenten im PDN.

- Bestandsaufnahme-Ermittlung des aktuellen Stands
- Ermittlung des Ziels (Entwicklung des Sicherheitskonzepts)
- Erstellung der IT-Sicherheitspolicy
- Anwendung der IT-Sicherheitspolicy
- Audit der Ergebnisse (IT-Sicherheitsaudit)
- Reguläre Sicherheitsprüfungen

1. Aktuelle Bedrohungen der Produktionsdatennetze/ SCADA Umgebungen[1] – exemplarische Beispiele

Gefahren für Produktionsdatennetze sind allgegenwärtig. In PDN Umgebungen ist das A und O die Verfügbarkeit; alles wird diesem Ziel im Regelfall untergeordnet.

Der Wert, dem der IT-Sicherheit beigemessen wird, nimmt stetig zu, aber es stellt sich oft in Unternehmen die Frage, wer dafür zuständig ist: Sind es die Ingenieure im PDN, die ihre Prozesse und Systeme kennen oder ist es ein zentraler Sicherheitsbeauftragter, der im Regelfall stärker mit Office- und Bürokommunikationsnetzen vertraut ist?

Die Ingenieure im PDN sind oft keine spezifischen IT-Sicherheitsexperten. Diese Lücke gilt es zu füllen, damit ein hohes IT-Sicherheitsniveau auch für das PDN erreicht werden kann. In den letzten Jahren wurden eine Reihe von Vorfällen auch in der Presse thematisiert. Neben dem überall zu Recht erwähnten Beispiel Stuxnet, gibt es aber eine Vielzahl weiterer Bedrohungen für die IT-Sicherheit von Produktionsdatennetzen.

Den letztendlich Verantwortlichen (die Geschäftsleitung) fällt es oft schwer, eine realistische Einschätzung zu treffen, da viele Vorfälle in Unternehmen unter Verschluss bleiben und durch mangelnde Transparenz der Gesetzgebung keine Notwendigkeit gegeben ist, diese Praxis zu modifizieren.

Dies könnte sich jedoch schnell ändern, wenn die neuen Vorschläge der EU-Kommission vom 26. November 2012 in nationales Recht umgesetzt werden sollten:

EU-Kommissarin will Meldepflicht für Hackerangriffe – Gesetz gegen Cyber-Attacken: Beim Schutz ihrer IT-Sicherheit will EU-Kommissarin Neelie Kroes die Unternehmen stärker in die Pflicht nehmen – und schließt auch eine Meldepflicht für Hackerangriffe nicht aus. Solange dies jedoch national nicht der Fall ist, wird sich an der jetzigen Intransparenz nichts ändern, die für die Verantwortlichen von PDN unter Umständen eine Scheinsicherheit erzeugt. Diese kann dazu führen, dass das Management bzw. die Geschäftsleitung die Risiken nicht hoch genug einschätzt, um adäquate Sicherheitsprozesse zu initialisieren, die das PDN in den Mittelpunkt stellen [1].

Es gibt genügend kritische Infrastrukturen im Energiesektor, die ein großes PDN betreiben und unter Umständen in diese Transparenzvorschrift einbezogen werden könnten. Aus den USA ist bekannt, dass z.B. im Finanzdienstleistungssektor Sicherheitsvorfälle veröffentlicht werden müssen und damit auch ein erhöhter Reputationsschaden für die betroffenen Unternehmen, aber auch für den Finanzdienstleistungssektor in seiner Gesamtheit, entstanden ist. Aber es wurden auch aus dem Energiesektor Vorfälle publik wie z.B. ein großflächiger Stromausfall in den USA/Kanada im Jahr 2003.

Eine gute Zusammenstellung erfolgreicher Angriffe gegen SCADA Systeme findet sich in dem wissenschaftlichen Beitrag *Cyberthreats, Vulnerabilities and Attacks on SCADA*

[1] Der Autor verwendet in diesem Beitrag die Begriffe Produktionsdatennetz (PDN) und Supervisory Control and Data Acquisition (SCADA) Systeme mehr oder weniger als Synonyme, weil je nach Adressat darunter eine vergleichbare IT-Systemlandschaft bzw. wichtige Systeme innerhalb eines Produktionsnetzwerks verstanden werden.

Networks von Rose Tsang [2]. Hier wird unter anderem ein kompletter Stromausfall in den USA und Kanada im Jahre 2003 dokumentiert, der Schätzungen zufolge zwischen 3 und 10 Mrd. US Dollar Schäden nach sich gezogen hat. Etwa 50 Mio. Bürger waren von dem Stromausfall betroffen. Der Grund hierfür war ein Fehler im Leitstand des SCADA Systems des Energieversorgers First Energy, Ohio.

Der gezielte Virus Stuxnet und dessen legitimer Nachfolger Flame1 *Wege in den digitalen Abgrund, Frankfurter Allgemeine Zeitung (FAZ), 13.06.2012* [3] hat es vermocht das Bewusstsein für Risiken von Produktionsanlagen, die bis dahin in der Öffentlichkeit als gekapselt/abgeschottet galten, aufzudecken und Gefahrenpotentiale aufzuzeigen. Steuerung bedeutet in diesem Zusammenhang die Bereitstellung von aggregierten Daten des Produktionsprozesses, die dann zwischen den involvierten Parteien untereinander verrechnet werden bzw. mit denen die verbundenen Prozesse gesteuert werden.

Über Jahrzehnte waren diese Steuerungssysteme autark und wurden so wenig wie möglich verändert bzw. aktualisiert. Die Vorzüge von Bürokommunikationsnetzen wie vergleichsweise kurze Einsatzzeiten von Servern, laufende Aktualisierung der eingesetzten Software durch Patches und Upgrades, regelmäßige Härtung der Komponenten und Systeme, Dienste und Services konnten aufgrund unterschiedlicher Restriktionen nicht genutzt werden. In SCADA bzw. PDN-Umgebungen wird viel restriktiver aktualisiert. Standards, die einmal Gültigkeit hatten, müssen erst langwierig durch eine erneute Zertifizierung der Produktionsdatennetzanbieter bzw. Anbieter der SCADA Systeme freigegeben werden.

Der Autor erlebte in den vergangenen Jahren mehrere Fälle in der Praxis, bei denen es quasi unmöglich wurde, die erneute Zertifizierung zu erlangen, da die Instanzen, die die Zertifizierungsvorschriften entwickelt haben, nicht mehr existierten. Verbesserungsvorschläge an den Hersteller der Software zur Behebung der Verwundbarkeiten bzw. zur Erhöhung der Sicherheitseinstellungen waren nicht durchsetzbar, weil es einem einzelnen betroffenen Unternehmen nicht möglich ist, die spezifische Implementierung des Standards zu ändern, da dann die Interoperabilität zu Dritten, die sich auch an diesem Standard orientieren, gefährdet ist. Gleichzeitig kann aber kein neuer Standard vereinbart werden, weil der Standard seit Jahrzehnten nicht weiterentwickelt wurde. Im transnationalen Zahlungsverkehr trat diese Situation ein und führte zu Stagnation, obwohl nachweislich Handlungsbedarf besteht.

Diese Ausgangssituation führte dazu, dass neue IT-Techniken am Standard vorbei entwickelt wurden, um neue Funktionalitäten zu ermöglichen. Nun stehen z.B. Java Code Entwicklungen neben proprietären, über Jahrzehnte erprobten Softwareumgebungen, die nur einem ausgewählten Kreis von Softwareherstellern zugänglich waren, zur Verfügung. Die rasante und fortwährende Entwicklung der Java-Technologie trägt dann unter Umständen dazu bei, dass bewährte Schutzmechanismen der *sicheren* proprietären Altsysteme ausgehebelt werden und damit die PDN-Umgebung an sich gefährdet ist.

Durch steigende Vernetzung der Büro-und Produktionsnetze entstehen neue Risiken, vormals komplett nach außen abgeschottete PDN/SCADA-Systeme öffnen sich.

IT-technisch nutzen beide Umgebungen vermehrt gemeinsame Netze und dort eingerichtete Basisdienste wie Microsoft Domänen. Ein versierter Angreifer kann diese Basisdienste nutzen, um sich Zugang zu den kritischen Produktionsumgebungen zu verschaffen. Dabei kann er dann die typischen Schutzmechanismen wie lokale Firewalls aushebeln. Ein weiteres Einfallstor sind remote Wartungszugänge, die Zugriff auf die PDN Umgebungen herstellen und auch von außen gezielt angegriffen werden können.

Gefahren drohen aber nicht nur den einzelnen Unternehmen, sondern die zunehmende Vernetzung und IT-gestützte Überwachung und Steuerung von Produktionskapazitäten (z.B. kann die Verteilung von Gas oder Strom gezielt angegriffen werden). Die Steuerung und der Abruf von Produktionskapazitäten werden heute auch über Webservices bzw. Webanwendungen abgewickelt und erfolgen damit nicht mehr in hermetisch abgeriegelten internen Systemen der Energiehersteller und Netzbetreiber.

Ein Beispiel, wie kriminelle Energie in Zukunft großen Schaden anrichten könnte, wird hier skizziert: Es wird erwartet, dass große Strommengen aus Windkraft, die im Norden Deutschlands erzeugt werden, über intelligente Steuerungssysteme und dafür geschaffene Leitungen vorwiegend in den Süden geleitet werden. Es drohen Gefahren, falls es einem Hacker gelingen sollte, die zusammengekoppelten Windparkkapazitäten zu manipulieren und zu Spitzenlastzeiten einen *Stillstand* zu erzeugen oder bei einem Überfluss an Strom im Gesamtnetz die Einleitung des Stroms der Windparks nicht zu drosseln, sondern zu erhöhen. Als Folge könnte ein Blackout nationalen bis zu internationalen Ausmaßes eintreffen. Hier sind besonders die Monitoring- und Steuerungssysteme großen Gefahren ausgesetzt.

2. Was es zu schützen und zu beachten gilt

Schutz von Unternehmenswerten und Menschen

Dies ist hauptsächlich ein Sicherheits-Grundbedürfnis: Sicherstellung, dass die Menschen und die Unternehmenswerte gegen absichtlich und unabsichtlich herbeigeführte Risiken oder Risiken, die durch den Ausfall von Komponenten im PDN verursacht werden, geschützt sind. Obwohl die Implikationen dieses Konzepts sehr ausgeweitet sind, ist das Prinzip einfach verständlich, insbesondere in einer Umgebung in der Menschen und Güter Maschinen vertrauen und die Maschinen, zumindest teilweise, durch automatisierte Computerprozesse kontrolliert werden. Die IT-Sicherheitskontrollen und Prozesse müssen die potentiellen Risiken und deren tatsächliches Gefährdungspotential identifizieren und daraus ableiten, wie diese Risiken vermieden oder zumindest auf ein akzeptables Maß minimiert werden können.

Compliance

Die Sicherheit einer Produktionsdatennetzumgebung/SCADA System ist nicht nur eine Angelegenheit von internem Interesse – zahlreiche externe Stellen und Faktoren erfordern zumindest eine minimale Sicherheitsstufe (falls dies noch nicht der Fall sein sollte, ist dies nur eine Frage der Zeit, bis solche Anforderungen zwingend eingehalten

werden müssen). Es gibt eine Reihe von externen Compliance-Anforderungen, die berücksichtigt werden müssen: Die übergeordnete Sicherheitspolicy für die Gesamtunternehmung und mögliche Gesetze oder Vorschriften von Regulierungsbehörden, die jeweils eigene Regelwerke für ihre Branche definiert haben, gilt es, einzuhalten. Diese Regularien gibt es in unterschiedlichen Ausprägungen für eine Reihe von Branchen wie z.B. Pharma, Finanzdienstleistung etc.

Sichere Produkte und Dienstleistungen von Dritten

Das Produktionsdatennetzwerk ist eine dynamische Umgebung, die aus verschiedenen Komponenten Dritter besteht. Solche Komponenten werden hinsichtlich mechanischer Defekte und Compliance, Zuverlässigkeit, umgebungsbedingter Charakteristiken, elektrischer Spezifikationen etc. analysiert. Viele solcher Komponenten beinhalten Computer oder zumindest Microcontroller, die Hard- und Software umfassen. Zusätzlich werden externe Dienste in Anspruch genommen, die die Wartung, Reparaturen, Upgrades, neue Prozesse etc. abdecken; einige dieser Dienste besitzen die Form von IT-Services, und werden remote oder lokal vor Ort erbracht. Es ist selbstverständlich, dass die IT-Aspekte von Produkten und Dienstleistungen Dritter genauso umfassend auf den Prüfstein gestellt werden müssen wie ihre mechanischen und umgebungsbedingten Charakteristiken. Die Verantwortlichen für das PDN sollten in der Lage sein, von den externen Dritten einzufordern und nachprüfen, ob deren externen Produkte und Dienstleistungen eine minimal akzeptierte Schutzstufe aufweisen. Darüber hinaus sollten die Verantwortlichen verifizieren ob die externen Vertragspartner überhaupt Sicherheitskontrollfunktionen eingeführt haben für ihre eigene Produktions- und Dienstleistungsprozesse.

Entscheidend sind jedoch die schon bereits erwähnten signifikanten Unterschiede zwischen Produktions- und Bürokommunikations/Office-Netzwerken. Diese gilt es, in der Sicherheitsanalyse zu betrachten, damit jeweils adäquat auf deren Eigenheiten eingegangen werden kann.

3. Unterschiede der Sicherheit zwischen Produktions- und Office-Netzwerken

Menschen

- Das IT-Netzwerk ist nur eine Komponente eines bestimmten Projekts/Bereichs/Prozesses des Produktionsnetzwerks, während es in einer Office-Umgebung Teil der gesamten Unternehmung ist;
- Die IT-Komponenten sind lediglich einige der technischen Hilfsmittel, die in den Prozess involviert sind, während in einer Office-Umgebung IT-Anwendungen annähernd alles sind;
- Elektronik, Mechanik, IT (Hardware und Software) müssen aufeinander abgestimmt sein, während in einer Office-Umgebung die IT meistens für sich selbst steht;

- Nur Personen mit tiefgehendem Prozesswissen können die Komponenten verwalten, während in einer Office-Umgebung geschulte IT-Sicherheitsspezialisten alle Belange adressieren können;
- Prozessingenieure kennen den technischen Prozess, aber nicht zwingend die IT-Sicherheitsbelange, während in einer Office-Umgebung die IT-Spezialisten die Rolle der Ingenieure einnehmen;
- IT-Sicherheit kann nicht vom Prozess externalisiert werden, in einer Office-Umgebung hingegen schon, entweder an die IT-Abteilung, Unternehmenssicherheit oder einen externen Vertragspartner.

In einem Produktionsnetzwerk ist die Sicherheit an jeden technischen Prozess gebunden und jegliche IT-Sicherheit muss durch die Prozessingenieure und deren Teams implementiert werden, da diese über tiefgehendes Verständnis über den Prozess und die involvierten technischen Komponenten verfügen. Jegliche Sicherheitspolicy und Richtlinien müssen durch Ingenieure ohne tiefgehendes IT-Sicherheitswissen umsetzbar sein.

Komponenten

- Die IT-Komponenten sind spezialisiert und nicht standardisiert, (Hardware und/oder Software), während in einer Office-Umgebung Standard Hard- und Software verwendet werden
- Aufgrund physikalischer Limitierungen haben und können einige IT-Komponenten kein Hot-Backup. Deshalb ist eine System-Ausfallzeit im Falle von Änderungen keine Option, in einer Office-Umgebung hingegen kann jede kritische Komponente ein Hot-Failover haben;
- Herkömmliche Sicherheitsmethoden können innerhalb eines Produktionsnetzwerks nicht zu 100 % angewendet werden, da die üblichen Standards und Sicherheitskontrollfunktionen sehr spezialisierte Systeme nicht abdecken können.
  Die Umgebung und der physikalische Standort von Produktionsnetzwerk-Komponenten setzen diese physischen wie auch IT bezogenen Sicherheitsrisiken aus, in einer Office-Umgebung hingegen können diese, im Hinblick darauf, relativ einfach abgesichert werden.

Die Sicherheitsregeln und Spezifikationen eines Produktionsnetzwerks müssen spezifisch für jede Komponente und jeden Prozess ausgelegt sein und alle spezifischen Charakteristiken und Einsatzszenarien berücksichtigen. Standardisierte, allgemeine Sicherheitsregularien der Unternehmung sind im Regelfall innerhalb eines Produktionsnetzwerks nicht anwendbar.

4. Aufspüren, einschätzen und beseitigen von Sicherheitsbedrohungen

Die Praxis zeigt, dass in vielen Unternehmen, die ein PDN betreiben, folgende Ausgangsbasis herrscht:

Derzeitige Situation

Die IT-Komponenten des Produktionsnetzwerks gehören typischerweise zu verschiedenen Projekten, die sich in unterschiedlichen Lebenszyklen befinden und durch unterschiedliche Teams geleitet werden. In manchen Fällen sind externe Vertragspartner involviert. Es existiert im Regelfall kein Sicherheitskatalog über die Systeme und Komponenten, ebenso gibt es keine regulatorischen Aspekte je Komponente, um diese bei der Implementierung anzuwenden. Ebenso sind für viele Komponenten und interne Umgebungen die Sicherheitsanforderungen unbekannt (technisch und prozessbezogen). Dies schließt nicht aus, dass einige Komponenten und Prozesse faktisch sicher sein können. Das bedeutet demnach, dass die aktuelle IT-Sicherheitssituation sich in einem unbekannten Status befindet, in der IT-Sicherheit ist dies das Äquivalent von unsicher.

Ziel

Ziel ist, das Risiko weit möglichst zu minimieren. Dies wird durch den Schutz der Menschen und der Unternehmenswerte, der Sicherstellung eines gewissen Grades an Compliance und dass externe Vertragspartner sichere Produkte und Dienstleistungen liefern, erreicht. Dies ist einfach einzufordern, aber schwierig umzusetzen. Es kommt oft vor, dass unklar ist, was genau für jede Prozesskomponente notwendig ist, um diese abzusichern. Die Compliance Aspekte sind unklar und die externen Vertragspartner können nicht kontrolliert werden, bis die interne Umgebung eine gewisse Eigenkontrolle/Selbstkontrolle erreicht hat. Die Schlussfolgerung daraus ist, dass es derzeitig oft nicht ersichtlich ist, was als Ziel angestrebt wird.

Diese Ausgangsbasis ist aus sicherheitstechnischer Sicht nicht als positiv zu bewerten, so dass die Umsetzung der sechs Phasen Abhilfe schaffen kann.

Der Autor stellt nun einen möglichen Ansatz zur Implementierung von IT-Sicherheitskontrollfunktionen innerhalb eines typischen Produktionsnetzwerks dar.

Eingangs wurde darauf hingewiesen, dass die Verantwortlichkeiten für die Sicherheit des PDN oft nicht organisatorisch geklärt sind und es oft keinen direkten Verantwortlichen gibt. Aus der Praxis empfiehlt es sich, eine solche Funktionsstelle zu schaffen, die dann nach Innen und Außen als Sicherheitsbeauftragter agiert. Dieser Experte hat dann unter anderem die Aufgabe, die internen Anstrengungen zur Entwicklung und Implementierung der IT-Sicherheitspolicy zu überwachen und zu kontrollieren. Diese Person wird zusammen mit dem externen Dienstleister arbeiten und später für die Erstellung eines Spezialistenteams verantwortlich sein, das sich mit der weiteren internen Verwaltung und Unterstützung der internen IT-Sicherheitsprozesse befassen wird.

5. Sechs-Phasen-Modell

Die einzelnen Phasen eines solchen Projektes werden nun vorgestellt:

5.1. Ermittlung des aktuellen Stands

Identifizierung der sicherheitsrelevanten Komponenten und deren Sicherheitsanforderungen und des aktuellen Sicherheitsstands:

- Vor Ort Erstellung eines IT-Inventars und Erfassung einer Liste mit den Charakteristiken jedes Netzwerks, dessen Umgebung, System ,Komponente und Prozesse – aus Sicht der IT-Sicherheit;
- Überblick über die grundlegenden Konfigurationsaspekte, Verwendungsarten, Zugriffsperspektiven, in welchen Prozessen die Komponenten verwendet werden und welche Anwendungen sich im Einsatz befinden;
- Überblick über jegliche sicherheitsrelevante Dokumentation in Bezug auf die IT-Komponenten und Prozesse;
- Überblick über die derzeitige Ausgestaltung der IT-Sicherheit und bereits existenter sicherheitsrelevanter Maßnahmen und Ressourcen (Hard- und Software wie z.B. Firewalls und VPN-Systeme);
- Überblick über die aktuellen Verantwortlichkeiten des Personals und Ermittlung der Freigabestufen/Freigabehierarchien bezogen auf IT-Sicherheit.

Alle oben genannten Punkte werden in ein einzelnes Inventar aufgenommen, das präzise die aktuelle Situation der IT-Umgebung hinsichtlich der IT-Sicherheit beschreibt, inklusive der bereits verfügbaren Ressourcen.

5.2. Ermittlung des Ziels – Entwicklung des Sicherheitskonzepts –

Herausarbeiten, was hinsichtlich der IT-Sicherheit angestrebt wird, eine Kombination von:

- Jegliches schon vorhandene Material einer Sicherheitspolicy;
- Firmen-Sicherheitsregularien;
- Unternehmens- und Verantwortlichkeitsstruktur;
- Spezifische Gesetze, die z.B. nur für diese Branche Anwendung finden (Übersetzung der zutreffenden Regularien in Bezug auf die IT-Steuerung);
- IT-Sicherheit Best Practice, basierend auf langjähriger Erfahrung des externen Beraters;
- Spezifikationen für externe Vertragspartner bezüglich Hardware, Software und Dienstleistungen;
- Interne Anforderungen, basierend auf Interviews mit Prozessmanagern/Ingenieuren und Teams;
- Zuverlässigkeit, Failover und Umgebungsspezifikationen.

Das Obige resultiert in einer Reihe von generellen Sicherheitsanforderungen, die auf oberster Ebene die Sicherheitsanforderungen spezifizieren; dies wird das gesamte Sicherheitskonzept darstellen und beschreibt, welche Ziele mit den jeweiligen Prozessverantwortlichkeiten erreicht werden sollen. Das Dokument muss von allen involvierten Parteien akzeptiert und vom Management durchgesetzt werden. Es wird später in der IT-Sicherheitspolicy als Hauptkriterium integriert.

5.3. Erstellung der IT-Sicherheitspolicy

Die IT-Sicherheitspolicy wird eine Dokumentensammlung, die Maßnahmen und Kontrollen sowie die detaillierte Implementierung und Verifizierung von Sicherheitsaspekten spezifiziert, um die derzeitige Situation auf den durch das Sicherheitskonzept spezifizierten Stand zu bringen. Das entwickelte Sicherheitskonzept wird die theoretischen Sicherheitsanforderungen für die Komponenten und Prozesse innerhalb der analysierten Umgebung definieren;

Die Sicherheitsanforderungen der Konzeptstufe werden in exakte, anwendbare und verifizierbare Sicherheitsmaßnahmen durch eine Reihe von *Sicherheitsvorlagen* übersetzt; Die Vorlagen werden spezifizieren, wie die Sicherheitskonzepte für jede Art sicherheitsrelevanter Komponenten und Prozesse anzuwenden sind;

Erstellung von Vorlagen für jede Art sicherheitsrelevanter Komponenten; Betriebssystem, Anwendung, Rolle, Schnittstelle, Netzwerkkomponenten, etc.

Erstellung von Vorlagen für jede Perspektivenart: prozessintern, firmenspezifisch, extern, Dienstleistungspartner, Internet, DMZ, kritisches Produktionssystem, Utility-System, Office-System etc.

Erstellung von Vorlagen für jede Art sicherheitsrelevanter Prozesse: neue Komponente in das Netzwerk eingefügt, externen Computer eingebracht und Verbindung an Firmen-LAN, VPN-Berechtigungen, Videoüberwachung, Backup-Prozesse etc. Für jede Vorlage zu definieren:

- Theoretischer Hintergrund und Gründe für die Sicherheitskontrollprüfungen, basierend auf den anwendbaren Teilen des *Sicherheitskonzepts*;
- Was sind die genauen technischen und organisatorischen Sicherheitsmaßnahmen, die für die bezogene Komponente oder den Prozess durchgesetzt werden sollen;
- Eine verwendbare Checkliste zur Anwendung der in den Vorlagen enthaltenen Sicherheitsmaßnahmen;
- Eine verwendbare Checkliste zur Verifizierung der in den Vorlagen enthaltenen Sicherheitsaspekte;

Die Vorlage kann durch jeden Mitarbeiter mit IT-Grundwissen bis mittlerem IT-Wissen angewendet werden.

Die resultierende Sammlung der Dokumente *Sicherheitskonzept* und *Sicherheitsvorlagen* bildet die IT-Sicherheitspolicy des jeweiligen Produktionsnetzwerks. Jede Komponente, jedes Netzwerk, jeder Prozess und jede Aktivität, egal wie komplex, kann aus Sicht der Sicherheit durch eine Kombination von „Sicherheitsvorlagen" definiert werden und wird demnach für alle Mitarbeiter mit IT-Grundwissen bis mittlerem IT-Wissen anwendbar.

5.4. Anwendung der IT-Sicherheitspolicy

Die IT-Sicherheitspolicy wird in der existierenden Infrastruktur und den Prozessen angewendet, um den innerhalb des *Sicherheitskonzepts* spezifizierten Sicherheitsstand zu erreichen.

- Für jeden Prozess/Aktivität, System, Netzwerkbereich und Umgebung soll eine Aufteilung des Objekts in separate Komponenten erfolgen (z.B. O/S, Software, Ort der DMZ, Schnittstellen etc.);
- Für jede Komponente ist die anwendbare Sicherheitsvorlage auszuwählen und ein Inventarprofil für das Objekt, das aus den anwendbaren Sicherheitsvorlagen gebildet wurde, zu erstellen;
- Implementierung der resultierenden Inventarprofile oder Sicherheitsvorlagenreihen unter Befolgung der in jeder Vorlage beinhalteten Checklisten;
- Verwendung der definierten Profile oder Vorlagenreihen, immer wenn ein Prozess stattfindet; z.B. wenn ein neues Produkt von einem Vertragspartner bestellt wird oder wenn ein neuer Dienstleistungspartner mit externen Geräten in das Unternehmen eintritt.

Sobald alle *Sicherheitsvorlagen* auf die Objekte angewendet wurden und für die alltäglichen Prozesse allmählich eingesetzt werden, wird die Umgebung als sicher und konform zu dem *Sicherheitskonzept* betrachtet. Während der Implementierungsphase ist es sehr wahrscheinlich, dass einige Komponenten nicht zu 100 % in die Vorlagen passen oder einige Vorlagen können aufgrund produktionstechnischer Gründe nicht angewandt werden – dies wird zu Korrekturen oder Aktualisierungen in den Vorlagen führen, um vollständig zur Umgebung zu passen. Da die Umgebung dynamisch ist, wird im Falle einer neuen Komponente oder dem Beginn eines Produktionsprozesses, bei denen die Vorlagen nicht alle Details abbilden können, die Policy dementsprechend aktualisiert. Neue Sicherheitsverwundbarkeiten und neue Sicherheitstools führen ebenso zu Änderungen der Policy. Solche Aktualisierungen werden Aufgabe der IT-Abteilung und wann immer erforderlich, mit Unterstützung durch den externen Dienstleister.

5.5. Audit der Ergebnisse – IT-Sicherheitsaudit –

Auditierung, wie effektiv und korrekt die Implementierung der IT-Sicherheitspolicy vorgenommen wurde durch eine Reihe von Tests gegen verschiedene Komponenten. Diese werden als repräsentative Beispiele aus verschiedenen Netzwerkbereichen ausgewählt, die sich auf verschiedene Produktionsprozesse beziehen.

Das Audit wird in einer Reihe von korrigierenden Maßnahmen resultieren; einige davon werden zu Korrekturen in den untersuchten Testzielen führen während andere zu Änderungen in der IT-Sicherheitspolicy und den beinhalteten Sicherheitsvorlagen führen. Der Auditprozess sollte in regelmäßigen Abständen wiederholt werden, ebenso bei größeren Änderungen oder wenn neue Produktionsprozesse gestartet wurden.

5.6. Reguläre Sicherheitsprüfungen

Das IT-Personal definiert einen Testzeitplan, um zu verifizieren, ob und wie effektiv die IT-Sicherheitspolicy in der Praxis umgesetzt wurde. Dies kann z.B. durch die Selektion von zufälligen Testzielen und der Durchführung von limitierten Sicherheitsverifikationen gegen die Policy erreicht werden. Zu diesem Zweck wird die Checklistenvorlage zur Verifizierung der Sicherheitsmaßnahmen angewandt.

Die regulären Prüfungen werden üblicherweise in einer Reihe von korrigierenden Maßnahmen resultieren; diese Aktionen werden die Sicherheitsmaßnahmen gering und die Gesamtsicherheit auf der angestrebten Stufe halten.

6. Ausblick

Die Durchführung eines langfristigen Sicherheitsprojektes bietet direkten unmittelbaren praktischen Nutzen für das Unternehmen und muss als notwendige zukunftssichernde strategische Investition betrachtet werden. Sie ist nicht nur eine operative Optimierung von Prozessen.

Letztendlich führt ein solcher Ansatz zu einem hohen Sicherheitsniveau im Produktionsdatennetz. Weitere Vorteile für das Unternehmen ist die positive Aussendarstellung, gegenüber Kunden und Geschäftspartnern. Durch die Umsetzung der Sicherheitsmaßnahmen nehmen die Bedrohungen des PDN signifikant ab und die oberste Priorität im PDN *Verfügbarkeit* wird durch eine auf das Unternehmen zugeschnittene Sicherheitspolicy flankierend aufrechterhalten.

Die Praxis zeigt, dass IT-Sicherheit in Produktionsdatennetzen immer eine Top-Down-Unterstützung durch die Geschäftsleitung benötigt. Ohne diese nachhaltige Unterstützung können die Investitionen in IT-Sicherheit erfahrungsgemäß nur ungenügend getätigt werden selbst wenn die Initiative das Sicherheitsniveau im PDN zu erhöhen, oft von den sensibilisierten und engagierten Fachverantwortlichen ausgeht.

Gesetzlich ist die Notwendigkeit für IT-Sicherheit im PDN zu sorgen eindeutig geregelt. Der Geschäftsführer bzw. der Vorstand ist verantwortlich für die operationellen Risiken, die jedes Jahr in dem Lagebericht eindeutig dargestellt und bewertet werden müssen. In KonTraG und § 91 Abs. 2 AktG und § 317 Abs. 4 HGB ist dies unter Anderem geregelt.

Datenverarbeitungssicherheit erstreckt sich auch auf kritische Infrastrukturen wie ein SCADA System oder ein PDN. Damit ist die IT-Sicherheit der kritischen Infrastrukturen einer Unternehmung immer ein fester Bestandteil der operationellen Risiken. Die Geschäftsleitung muss demnach die operationellen Risiken mit Instrumenten der Risikosteuerung handhaben, und sich zu jedem Zeitpunkt sicher sein, dass immer Maßnahmen getroffen werden, die diese Risiken beherrschbar machen. Konkret ist eine Notfallplanung – in IT Bereich *Disaster Recovery* immer nachzuweisen. Die Schaffung einer Position im Unternehmen für IT-Sicherheit dient dann dazu diese Aufgaben an einen Spezialisten zu delegieren und die notwendigen Sicherheitsmaßnahmen für das PDN umzusetzen[2]. Die Existenz einer Sicherheitspolicy für das PDN verbunden mit der Einführung von Sicherheitskontrollfunktionen zeigt ein verantwortungsvolles Handeln auf und minimiert die Haftungsrisiken für die Geschäftsleitung.

[2] Eine gute Broschüre zu diesem Thema wurde vom Bundesministerium des Inneren herausgeben. Sie ist erhältlich unter http://www.verfassungsschutz.brandenburg.de/sixcms/media.php/4055/Leitfaden_Schutz_kritischer_Infrastrukturen.pdf (Bundesministerium des Inneren, Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Berlin, 2008)

7. Quellen

[1] Bernau, V.: EU-Kommissarin will Meldepflicht für Hackerangriffe. Süddeutsche Zeitung, München, (26.11.2012)

[2] Tsang, R.: Cyberthreats, Vulnerabilities and Attacks on SCADA Networks. http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf, (2009)

[3] Welchering, P.: Wege in den digitalen Abgrund. Frankfurter Allgemeine Zeitung, Frankfurt, (13.06.2012)

Engines and Marine Systems **Power Plants** **Turbomachinery** **PrimeServ**

Ökologisch und ökonomisch. MAN Diesel & Turbo bietet maßgeschneiderte Energiekonzepte in der Leistungsklasse bis 160 MW. Ganz gleich, ob Sie Ihren Strom mit fossilen Brennstoffen, Abfall, Biomasse oder Sonnenlicht erzeugen wollen, unsere Dampfturbinen erlauben die besonders wirtschaftliche Realisierung Ihrer speziellen Anforderungen. Kein Wunder, dass unsere Dampfturbinen auch in puncto Betriebssicherheit, Effizienz und Verfügbarkeit weit vorne liegen. Für verlässliche und umweltfreundliche Energie zu jeder Zeit. Erfahren Sie mehr auf www.mandieselturbo.com

Engineering the Future – since 1758.

MAN Diesel & Turbo

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Energie aus Abfall – Band 10
Karl J. Thomé-Kozmiensky, Michael Beckmann.
– Neuruppin: TK Verlag Karl Thomé-Kozmiensky, 2013
ISBN 978-3-935317-92-4

ISBN 978-3-935317-92-4 TK Verlag Karl Thomé-Kozmiensky

Verlag: TK Verlag Karl Thomé-Kozmiensky • Neuruppin 2013
Redaktion und Lektorat: Professor Dr.-Ing. habil. Dr. h. c. Karl J. Thomé-Kozmiensky,
Dr.-Ing. Stephanie Thiel, M.Sc. Elisabeth Thomé-Kozmiensky
Erfassung und Layout: Petra Dittmann, Sandra Peters,
Martina Ringgenberg, Ginette Teske, Ulrike Engelmann, LL. M., Ina Böhme
Druck: Mediengruppe Universal Grafische Betriebe München GmbH, München