IT-Sicherheit für Abfallentsorgungs- und Energieanlagen

Karl-Ulrich Martin

1. IT-Security in Abfallentsorgungs- und Energieanlagen (MHKW) – ist das relevant? 201

2. Gesetze – Stand der Technik 202

3. Sicherheitsunterschiede zwischen Produktions- und Office-Netzwerken 202

4. Ausgangsbasis: Istzustand und Ziel 204

5. Sechs-Phasen-Modell 205

5.1. Voraussetzung 205

5.2. Ermittlung des aktuellen Stands 205

5.3. Ermittlung des Ziels – Entwicklung des Sicherheitskonzepts – 206

5.4. Erstellung der IT-Sicherheitspolicy 206

5.5. Anwendung der IT-Sicherheitspolicy 207

5.6. Audit der Ergebnisse – IT-Sicherheitsaudit – 208

5.7. Reguläre Sicherheitsprüfungen 208

6. Ausblick 209

7. Quellen 209

Bedrohungen von IT-Systemen sind heute gravierender denn je. Immer öfter werden Vorfälle von erfolgreichen Hackerangriffen bekannt. Die Gefahren gehen von Innentätern oder erweiterten Innentätern aus, die mit ihrem Insiderwissen noch größeren Schaden anrichten könnten. In den letzten Jahren haben zusätzlich die Angriffe von Außentätern (Hacker on demand) zugenommen, die unterschiedliche Absichten verfolgen.

Der Beitrag beschäftigt sich mit Bedrohungen für Produktionsdatennetze. Ein allgemein bekanntes 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. [4]

Die Firma Detack beschäftigt sich seit dem Jahr 2000 mit IT-Sicherheit und agiert als Sparringspartner sowohl konzeptionell als auch praktisch, um das IT-Sicherheitsniveau langfristig zu erhöhen und Bedrohungspotentiale durch Beratung und Sicherheitsprüfungen zu verringern. In den letzten Jahren sind aufgrund der Erfahrung eigen praxisgerechte Sicherheit-Software und Applikationen entwickelt worden, die weltweit im Einsatz sind.

Dieser Beitrag liefert Denkanstöße, um eine allgemeine Sensibilisierung für Gefahren, denen Produktionssysteme ausgesetzt sind, zu schärfen. Potentielle Bedrohungen lediglich zu kennen, ist passiv. Vielmehr geht es in diesem Beitrag darum, Wege aufzuzeigen, wie auch konzeptionell und aktiv auf Bedrohungen 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 neuesten Stand zu bringen, um auch aktuellen Bedrohungen gerecht zu werden. Der stetige Wandel durch Veränderungen im Einsatz von IT-Technik und der Unternehmensorganisation muss hierbei 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 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. Dieser dynamische Prozess ist durch geeignete Standardisierung und Automatisierung mit Hilfe von maßgeschneiderter Software/Datenbank turnusmäßig durchzuführen.

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. [7]

- 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. IT-Security in Abfallentsorgungs-und Energieanlagen (MHKW) – ist das relevant?

Benötigen MHKWs überhaupt einer besonderen Betrachtung der IT-Security im Produktionsdaten-Netzwerk und/oder der Office-Infrastruktur?

Das Motto: wer hat schon Interesse an *meiner* MHKW, mein Produktionsnetz zu kompromittieren, an meinen Daten? Niemand. Da gibt es doch interessantere Angriffsziele… und deswegen halte ich mich mit Sicherheitsmaßnahmen zurück… und außerdem, bisher ist doch alles gut gegangen.

Das galt noch vor einigen Jahren. Inzwischen zeigt die Erfahrung: auch für die MHKWs ist die IT-Security wichtig

Grundsätzlich sind MHKWs nicht als *kritische Infrastrukturen* nach ITSiG mit den entsprechenden Meldepflichten einzustufen. [6] Doch das bedeutet nicht, dass MHKWs, ob durch gezielte Cyberangriffe, oder indirekte Cyberangriffe z.B. durch Unachtsamkeit des Personals oder Dienstleister, die somit Zugriff auf Bereiche der IT-Infrastruktur haben, von der Problematik ausgeschlossen sind. – auch MHKWs sind schon erfolgreich angegriffen worden.

Ein Blick in die Zukunft lässt erahnen, dass dieses Thema noch viel wichtiger werden wird und dass eine frühzeitige *Awareness* aller Beteiligten geboten ist.

Die weitere Vernetzung/Digitalisierung als Voraussetzung für Durchsetzung und Steuerung von Optimierungsprozessen der Integration in andere Infrastrukturen (Stichwort 4.0) zeigt die steigende Komplexität für Maßnahmen zur IT-Security. [1] Ferner ist der Real-Time Datenaustausch zwischen unterschiedlichen PDNs und die Verzahnung des Produktionsnetzes (PND) mit dem Verwaltungsnetz externer Dienstleister immer häufiger gefordert – dadurch erhöht sich natürlich zusätzlich das Risiko.

Während vor zehn Jahren fast nur Banken, Versicherungen und staatliche Institutionen vereinzelt von Hackern angriffen wurden, z.T. als sportive Handlung, existiert inzwischen eine wachsende Dienstleistungs-Industrie für *Hackerangriffe auf Bestellung*.

Folgende Anforderungen waren gestern, heute für jede MHKW, unabdingbar:

- Kein Risiko für Leib und Leben,
- Unternehmenswerte sind zu schützen,
- Wirtschaftlichkeit durch optimierte Prozesse, z.B. kein ungeplanter Stillstand,
- Erfüllung aller Gesetze,
- Exzellente Reputation und *nicht in der Zeitung stehen.*

Alle dieser Forderungen können durch einen direkten oder indirekten IT-Angriff auf die Infrastruktur, entweder von innen oder von außen, erheblich beeinflusst werden.

Fazit: Das Thema IT Security ist über das *normale Maß* hinaus auch für MHKWs relevant und wird in Zukunft immer wichtiger.

2. Gesetze – Stand der Technik

Gesetzliche Anforderungen werden durch das IT-Sicherheitsgesetz – ITSiG beschrieben. Hierbei ist zu interpretieren, dass MHKWs nicht zu den **Kritischen Infrastrukturen** (KRITIS) mit Meldepflicht gehören, denn die Definition heißt:

KRITIS sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei KRITIS deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (ITSiG).

Unabhängig aber, ob ein Betreiber zu den kritischen Infrastrukturen zählt oder nicht, verpflichtet das Sicherheitsgesetz, bei Auswahl, Implementierung und Betrieb von IT-Sicherheitsmaßnahmen den Stand der Technik zu berücksichtigen.

Aber wie ist heute der Stand der Technik für MHKWs? Und wie in zwei, drei Jahren? – Aufgrund der schnelllebigen Entwicklung der IT-Sicherheitslösungen und der intelligenteren Angriffsmethoden ist das ein sehr dynamischer Prozess.

Deshalb wird auch gesetzlich gefordert, dass alle Unternehmen (*KRITIS* und *Nicht-KRITIS*) ihre Sicherheitsmaßnahmen *aktuell* halten – es gibt kein Ruhekissen.

MHKWs müssen nach ITSiG *dem Stand der Technik* in der IT-Security entsprechen. Nun ist das interpretierbar: eine Basis wären z.B. die Erfüllung von CIN ISO 27001 BSI (Bundesamt für Sicherheit in der Informationstechnik) Grundschutz und die Empfehlungen für die *Fernwartung im Industriellem Umfeld* sehen. [3, 5] Darüber hinaus sind Ausarbeitungen des VGB`s *IT Sicherheit für Erzeugungsanlagen* oder Empfehlungen vom Tele Trust (Bundesverband IT –Sicherheit e.V.) und der Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) hilfreich. [2, 8, 9] Unabhängig von der Einhaltung der Gesetzte und Berücksichtigung der Empfehlungen ist regelmäßig die Wirksamkeit des IT-Sicherheitsschutzes, die Widerstandsfähigkeit gegen Angriffe, zu überprüfen und gegebenenfalls durch geeignete Maßnahmen nach zu justieren.

3. Sicherheitsunterschiede 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 nur 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 getrennt und damit delegiert werden; in einer Office-Umgebung ist die Delegation möglich, z.B. an die IT-Security Abteilung oder an 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 nur diese über tiefgehendes Verständnis des Prozesses und die involvierten technischen Komponenten verfügen. Die Sicherheitspolicy und die Konzepte/Richtlinien müssen durch Prozess-Ingenieure ohne tiefer gehendes IT-Sicherheitswissen umsetzbar sein; sie müssen bei der Policy-Erstellung aktiv einbezogen werden

Komponenten

- Die IT-Komponenten (Hardware und/oder Software) sind im PND spezialisiert, nicht standardisiert und häufig älteren Datums, während in einer Office-Umgebung Standard Hard- und Software verwendet werden und regelmäßig auf einen neueren Stand gebracht werden.
- Aufgrund physikalischer Limitierungen haben und können einige IT-Komponenten kein Hot-Backup durchführen. 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 Prozent 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. Ausgangsbasis: Istzustand und Ziel

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 Prozesse, die sich in unterschiedlichen Lebenszyklen befinden und durch unterschiedliche Teams geleitet werden. In manchen Fällen sind externe Vertragspartner involviert. Ex existiert z.T. kein vollständiges Inventarverzeichnis und im Regelfall kein Sicherheitskatalog über die Systeme und Komponenten, ebenso gibt es keine regulatorischen Aspekte je Komponente, um diese bei der Implementierung anzuwenden. Für viele Komponenten und interne Umgebungen sind 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 und nicht dokumentierten Status befindet. Für die Klassifizierung der IT-Sicherheit bedeutet das: Der Prozess ist unsicher.

Der *Stand der Technik* wird selten erfüllt oder wenn dann nur partiell.

Ziel

Ziel ist, das Risiko soweit als möglich zu minimieren sowie den Stand der Technik und die Gesetze zu erfüllen.

Dies ist einfach einzufordern, aber schwierig umzusetzen. Oft fehlt es schon an der qualifizierten Zielsetzung der Geschäftsführung und somit die Ressourcen wie Finanzen, Kapazität und Fachkompetenz. Als Folge fehlen ganz rudimentäre Grundlagen wie IT Security relevante Policy/Konzepte und die regelmäßige Schulung der Mitarbeiter u.a. Es kommt oft vor, dass unklar ist, was genau für Prozesskomponente notwendig ist, um diese abzusichern; und dies sollte im jährlichen Turnus geschehen. Die IT sicherheitstechnischen Anforderungen an die externen Vertragspartner können nicht kontrolliert werden – auch weil jede es keine Vertragsgrundlage gibt.

Die Schlussfolgerung daraus ist, dass es derzeit oft nicht ersichtlich ist, was als Ziel definiert, angestrebt wird. Es fehlen die Grundlagen sowohl im organisatorischen als auch im prozesstechnischen Bereich.

Zwischen dem Soll, dem Stand der Technik und dem Istzustand ist eine in vieler Hinsicht große Lücke, die mit jedem Tag größer wird.

Detack hat eine praxisnahe Bottum Up Methode, unterteilt in sechs Phasen, entwickelt, mit der Schritt für Schritt die Lücke zwischen Soll- und Istzustand geschlossen werden kann. Die begleitende Mitarbeit von Prozessingenieuren ist dabei Voraussetzung – auch, für die in der Praxis wichtige Akzeptanz.

Mit der Vorgehensweise Analysieren – Standardisieren – Automatisieren entsteht ein integrierter softwareunterstützter Workflow, der ein vorgegebenes durchgängiges

Sicherheitslevel mit geringem Aufwand ermöglicht und dokumentiert und mit Unterstützung geeigneter Software aufrechterhalten werden kann.

5. Sechs-Phasen-Modell

5.1. Voraussetzung

Die Geschäftsleitung muss in jeder Hinsicht die IT-Security relevanten Unternehmensziele definieren und als Konsequenz der Organisation ihre volle Unterstützung geben, da es sich um einen längeren, dauerhaften Prozess handelt und Ressourcen fordert.

Die Verantwortung für die Sicherheit des PDN ist oft nicht organisatorisch geklärt. Aus der Praxis empfiehlt es sich, eine solche Funktionsstelle zu schaffen, die dann nach Innen und Außen als Sicherheitsbeauftragter agiert. Dieser Experte – dieser kann auch angelernt sein – hat 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.

5.2. 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 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 Dokumentationen.

5.3. Ermittlung des Ziels – Entwicklung des Sicherheitskonzepts –

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

- Jeglichem schon vorhandenem 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 Practise/Stand der Technik, basierend auf branchenspezifischen Veröffentlichungen und 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 fragmentierten Sicherheitsanforderungen, die auf oberster Ebene die Sicherheitsanforderungen *Top Level* spezifizieren; dies wird das gesamte Sicherheitskonzept darstellen und beschreibt, welche Ziele mit den jeweiligen Prozessverantwortlichkeiten erreicht werden sollen.

Üblicherweise wird das häufig vorhandene flache PDN nach der unterschiedlichen betrieblichen Relevanz des Prozesses und Komponenten in Zonen segmentiert – z.B. von absolut unbedingter bis begrenzter Notwendigkeit für den ununterbrochenen, sicheren Betrieb, damit verbundenen *IT Security Risiko Potential* und der Kritikalität für einen sicheren Prozess.

Verbunden ist z.B. damit die übersichtliche Kommunikation und definierten, protokollierten Zugriffen zwischen den Sicherheit-Segmenten.

Das Dokument/Konzept muss von allen involvierten Parteien akzeptiert und vom Management durchgesetzt werden. Es wird nachfolgend bei der Erarbeitung IT-Sicherheitspolicy als Hauptkriterium/Leitfaden genutzt und integriert.

5.4. Erstellung der IT-Sicherheitspolicy

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

Die Sicherheitsanforderungen der Konzeptstufe werden in exakte, anwendbare und verifizierbare Sicherheitsmaßnahmen mittels einer Reihe von *Sicherheitsvorlagen* übersetzt; Diese 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, usw.

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

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 usw. Für jede Vorlage ist 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 einzelnen Sicherheitsmaßnahmen;
- Eine verwendbare Checkliste zur Verifizierung der in den Vorlagen enthaltenen Sicherheitsaspekte;

Die Vorlagen sind so zu verfassen, dass sie durch jeden Mitarbeiter mit IT-Grundwissen bis mittleren IT-Wissen angewendet werden können.

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 mit mittlerem IT-Wissen anwendbar.

5.5. 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 usw.);
- Für jede Komponente und Zugehörigkeit zu einem Sicherheitssegment 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/Vertrag 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 Prozent 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 praxisgerecht zur neuen 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.

5.6. Audit der Ergebnisse – IT-Sicherheitsaudit –

Auditierungen, wie effektiv und korrekt die Implementierung der IT-Sicherheitspolicy vorgenommen wurde, ist durch eine Reihe von Tests gegen verschiedene Komponenten durchzuführen.

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 (jährlich) wiederholt werden, ebenso bei größeren Änderungen oder wenn neue Produktionsprozesse gestartet wurden.

5.7. 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 und Wertschöpfung für das Unternehmen und muss als notwendige Investition betrachtet werden. Sie ist nicht nur eine operative Optimierung von Prozessen.

Letztendlich führt ein solcher Ansatz zu einem hohen Sicherheitsniveau im Produktionsdatennetz. Weiterer Vorteil 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 kann die Investition 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. Außerdem greift seit kurzem das ITSiG.

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.

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.

7. Quellen

[1] Beckmann, M.; Widder, T.; Pieper, C.; Treppe, K.: Waste-to-Energy 4.0. In: Thomé-Kozmiensky, K. J.; Beckmann, M. (Hrsg.): Energie aus Abfall, Band 13. Neuruppin: TK Verlag Karl Thomé-Kozmiensky, 2016, S. 29-42. ISBN 978-3-944310-24-4

[2] Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) diverse Veröffentlichungen

[3] BSI-CS 108 Fernwartung im industriellen Umfeld

[4] Gebauer, M.; von Hammerstein, K.; Hoffmann, C.; Rosenbach, M.; Schindler, J.: Kühler Krieg. In: Der Spiegel, 39/2016

[5] ISO/IEC 27001 BSI (Bundesamt für Sicherheit in der Informationstechnik)

[6] IT Sicherheitsgesetz (ITSiG) – Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

[7] Neider, U.: IT-Sicherheit in Produktionsnetzen (PDN) – Aufspüren, einschätzen und beseitigen von Sicherheitsbedrohungen. In: Thomé-Kozmiensky, K. J.; Beckmann, M. (Hrsg.): Energie aus Abfall, Band 10. Neuruppin: TK Verlag Karl Thomé-Kozmiensky, 2013, S. 287-299

[8] Tele Trust (Bundesverband IT-Sicherheit e.V.): Handreichung zum Stand der Technik bezüglich ITSiG; 2016

[9] VGB-Standard IT Sicherheit für Erzeugungsanlagen

Besuchen Sie uns unter

www.vivis.de

Wir widmen uns aktuellen verfahrens- und anlagentechnischen sowie politischen, rechtlichen und wirtschaftlichen Themen, soweit sie die Abfall- und Kreislaufwirtschaft, die Energie- und Rohstoffwirtschaft und den Immissionsschutz betreffen. Unsere Aufgabe sehen wir in der Kommunikation zwischen Politik, Verwaltung, Wirtschaft, Technik und Wissenschaft.

Zu wichtigen Themen veranstalten wir Konferenzen und Congresse – dazu geben wir Bücher heraus.

Stets sind wir auf der Suche nach interessanten Referenten, aktuellen Themen und spannenden Projekten um unser Angebot weiterzuentwickeln. Gern lassen wir uns von neuen Ideen inspirieren und diskutieren deren Realisierbarkeit.

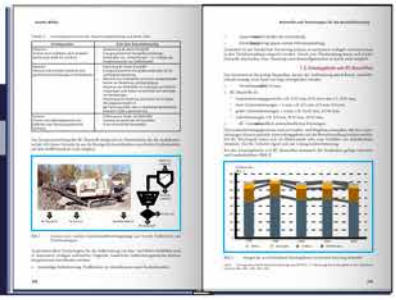
Der TK Verlag gibt seit dreißig Jahren Fachbücher zu zahlreichen Themen des technischen Umweltschutzes heraus:

- Thermische Abfallbehandlung & energetische Verwertung
- Dokumentation von Abfallverbrennungsanlagen
- MBA & Ersatzbrennstoffe
- Recycling & Rohstoffe
- Mineralische Nebenprodukte & Abfälle
- Strategie & Umweltrecht
- Immissionsschutz
- Biologische Abfallbehandlung...

Unsere Konferenzen im Überblick:

- Berliner Abfallwirtschafts- und Energiekonferenz
- Berliner Recycling- und Rohstoffkonferenz
- Berliner Konferenz Mineralische Nebenprodukte und Abfälle
- IRRC – Waste-to-Energy
- Berliner Klärschlammkonferenz (in Planung)

Insgesamt sind bislang bei uns etwa zweitausend Fachbeiträge erschienen, die in ihrer Gesamtheit einen guten Überblick über technische, wirtschaftliche, rechtliche und politische Entwicklungen geben. Seit Kurzem stellen wir Ihnen die Fachbeiträge kostenlos auf unserer Internetseite zur Verfügung.



vivis
TK Verlag Karl Thomé-Kozmiensky

Dorfstraße 51
D-16816 Nietwerder-Neuruppin
Tel. +49.3391-45.45-0 • Fax +49.3391-45.45-10
E-Mail: tkverlag@vivis.de

UHLIG

Solutions for tubes | fittings | boilers

Vertrauen, Fairness und Stabilität sind die Basis für erfolgreiche Geschäftsbeziehungen. Als mittelständisches Unternehmen verfolgen wir langfristige Ziele und bauen auf vertrauensvolle Partnerschaften.

UHLIG WEL-COR

Schweißplattierung von

- Membranwänden
- Einzelrohren | Überhitzern
- Rohrleitungskomponenten

Herstellung von

- Druckteilen
- Wellrohren

Background photo by Yvonne Saltmann, Wolfenbüttel, Germany

Die gelungene Synthese aus niedrigster Aufmischung, gleichmäßiger Schichtdicke und Wirtschaftlichkeit garantieren eine lange Standzeit der schweißplattierten Bauteile - basierend auf der Erfahrung in der Herstellung von 95.000 m² abgewickelter Schweißplattierfläche.

Uhlig Rohrbogen GmbH
Innerstetal 16 | D-38685 Langelsheim | Phone +49 5326 501 0 | Fax +49 5326 25 | info@uhlig.eu |www.uhlig.eu

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar

Karl J. Thomé-Kozmiensky, Michael Beckmann (Hrsg.):

Energie aus Abfall, Band 14

ISBN 978-3-944310-32-9 TK Verlag Karl Thomé-Kozmiensky

Verlag: TK Verlag Karl Thomé-Kozmiensky • Neuruppin 2017
Redaktion und Lektorat: Dr.-Ing. Stephanie Thiel, Elisabeth Thomé-Kozmiensky, M.Sc.
Erfassung und Layout: Sandra Peters, Anne Kuhlo, Janin Burbott-Seidel, Claudia Naumann-Deppe, Ginette Teske, Gabi Spiegel, Cordula Müller
Druck: Universal Medien GmbH, München