ISMS in der Energiebranche

innogy Netze Deutschland · Kasper · 19. Januar 2017

innogy

1

Hacking-Angriffe auf die Ukraine

2

Maßnahmen zur Abwehr von IT-Angriffen auf Kritische Infrastrukturen

3

Wesentliche Prozesse eines ISMS

4

Ausblick

1 HACKING-ANGRIFFE AUF DIE UKRAINE

Bericht über den letzten Hacking-Angriff auf die Stromversorgung der Ukraine am 17.12.2016

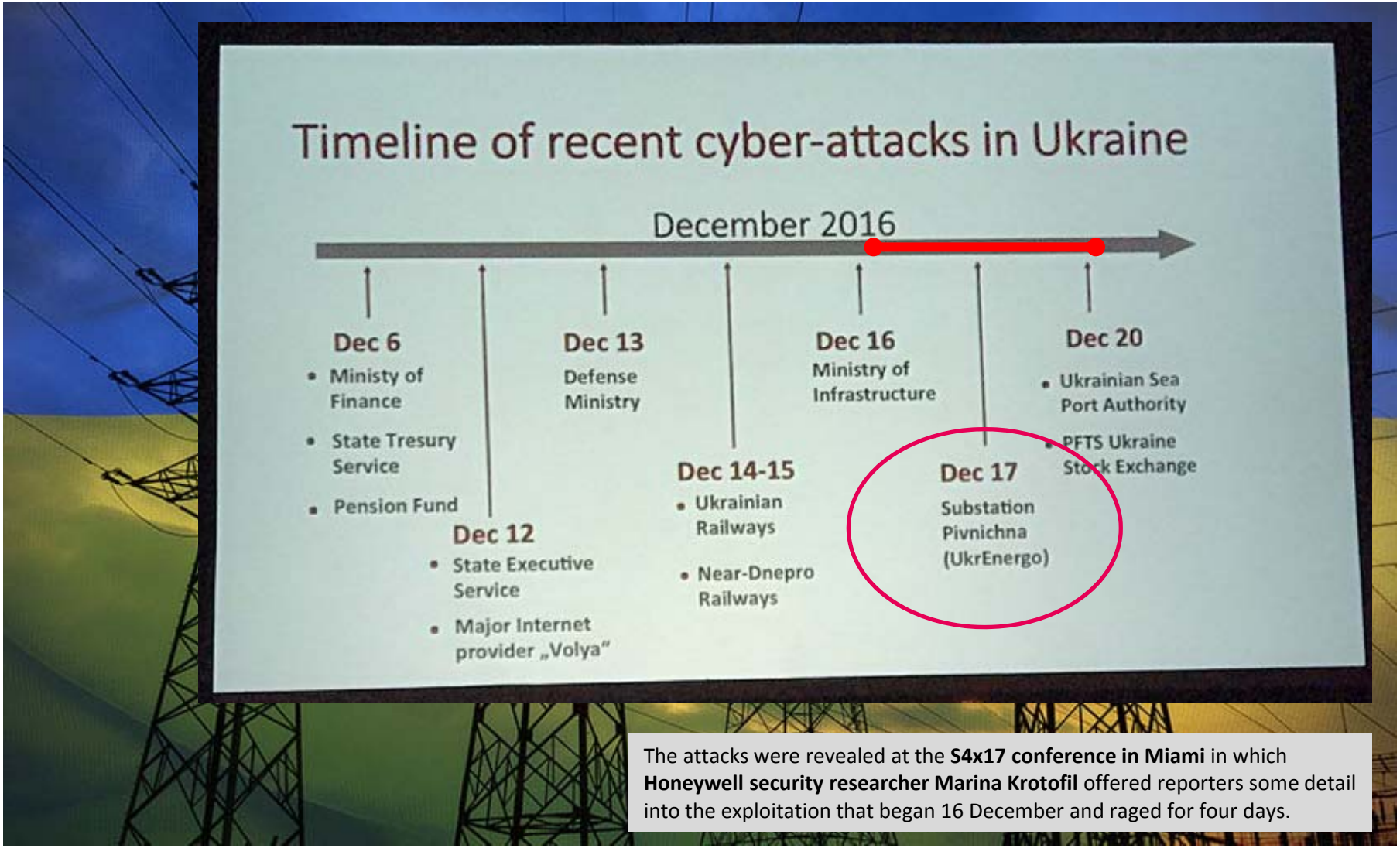
CBS News/ December 21, 2016, 7:27 PM / By Holly Williams

Russian hacks into Ukraine power grids a sign of things to come for U.S.?

… Last weekend, parts of the Ukrainian capitol Kiev went dark. Vasyl Pemchuk is the electric control center manager, and said that when hackers took over their computers, all his workers could do was film it with their cell phones.

"It was illogical and chaotic," he said. "It seemed like something in a Hollywood movie."

Übersicht über den Umfang der Hacking-Angriffe auf Behörden und Infrastruktur der Ukraine im Dezember 2016



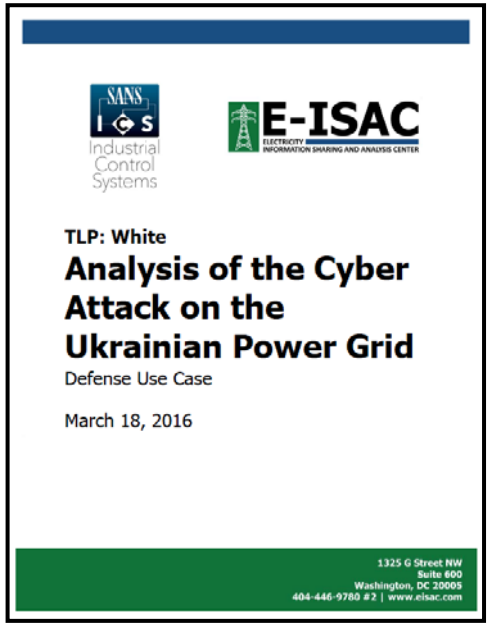
The attacks were revealed at the **S4x17 conference in Miami** in which **Honeywell security researcher Marina Krotofil** offered reporters some detail into the exploitation that began 16 December and raged for four days.

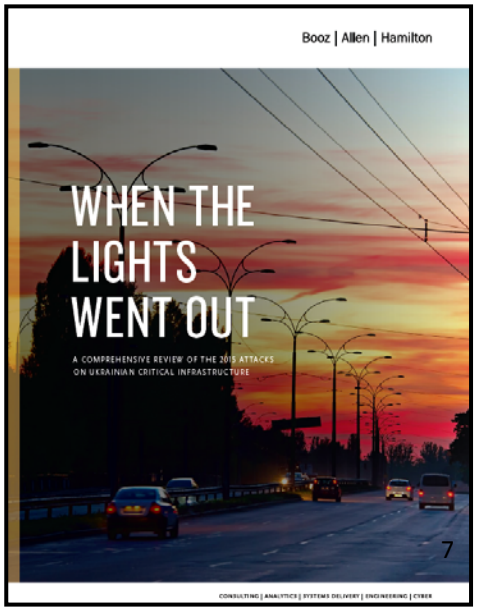
Hacking-Angriff auf die Stromversorgung der Stadt Kiew in der Ukraine am 17.12.2016

- Die Angreifer haben eine Umspann-station (Pivnichna substation) in den Außenbezirken von Kiew samstags gegen Mitternacht ausgeschaltet. Dadurch waren Teile der Stadt Kiew für ca. eine Stunde unversorgt.
- Erste Analysen zeigen, dass die Hacker die gleiche Strategie wie ein Jahr zuvor verfolgt haben. Allerdings haben die Angreifer nach Ausschalten der Leistungsschalter lediglich die Leittechnik in der Station heruntergefahren. Nach einem Reboot war die Netzstörung relativ schnell wieder zu beheben.
- Nach Aussagen des Betreibers sind in der Ukraine die gleichen Steuerungssysteme, Netzwerk- und Security-Komponenten wie überall eingesetzt.

Hacking-Angriff auf die Stromversorgung der Ukraine im Dezember 2015

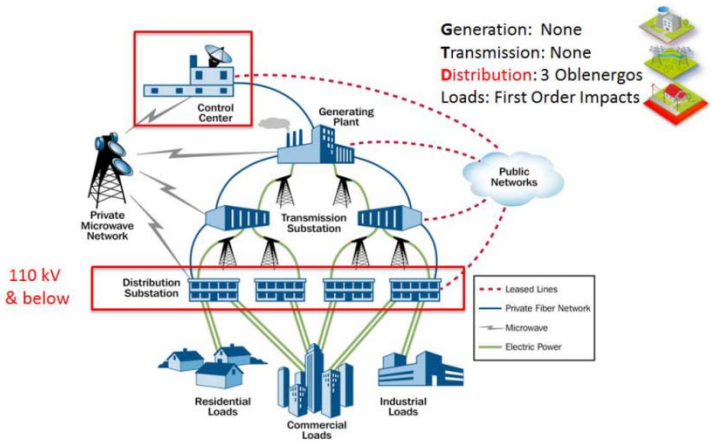
- **Sachverhalt:** Am 23. Dezember 2015 wurden zwischen 16:00 und 17:00 Uhr Ortszeit mindestens drei Stromverteilnetzbetreiber in der Ukraine Opfer eines gezielten Cyber-Angriffs. Es gelang den Angreifern, Schadsoftware auf Systemen mit veralteten Softwareständen aufzuspielen und zur Ausführung zu bringen.
- **Schadenswirkung:** Mindestens 225.000 Einwohner der Ukraine waren von einem mehrstündigen Ausfall der Stromversorgung betroffen. Aufgrund der Sabotage der Fernsteuerung der Umspannwerke musste in den Umspannwerken manuell geschaltet werden. Dadurch wurde die Wiederherstellung der Stromversorgung deutlich verzögert.
- Dokumentation: E-ISAC und SANS Bericht und Studie von Booz Allen Hamilton (Verfügbar auf den Webseiten der Organisationen)





Ablauf des Angriffs

(Kurzfassung)



- Wahrscheinlich wurden einige Systeme der Betreiber mittels Spear-Phishing bereits im Frühjahr 2015 infiziert.
- Nach der Erstinfektion erlangten die Angreifer schrittweise Kontrolle über weitere Rechnersysteme im angeschlossenen Netz des Betreibers, bis hin zu den Systemen, auf denen die eigentliche Steuerungssoftware für die Umspannwerke bzw. Schaltanlagen ausgeführt wird.
- Der eigentlichen Angriff fand am 23. Dezember 2015 statt:
  - Schritt 1: Ausschalten der Hochspannungsleistungsschalter in etwa 30 Hochspannungs-Umspannwerken. Gleichzeitig wurden die Überwachungssysteme der Netzleitstellen „eingefroren“ bzw. abgeschaltet, so dass der Umfang der Störung nicht feststellbar war.
  - Schritt 2: Überlastung der Telefonleitungen durch einem TDoS-Angriff (Telephone Denial of Service), wodurch telefonische Störungsmeldungen verhindert wurden.
  - Schitt 3: Löschen aller Daten auf Windows-Systemen. Überschreiben der Betriebssoftware der Datenkonzentratoren für die Steuerungsnetze. Abschalten der Unterbrechungsfreien Stromversorgungen (USV) in den Netzleitstellen, wodurch die Störungsbeseitigung weiter erschwert und verzögert wurde.

Eingesetzte Hacking-Methoden und Fähigkeiten der Angreifer

- Methoden:
  - Spear phishing um Zugang zum Büronetz zu erhalten
  - Einsatz des Trojaners BlackEnergy in verschiedenen Versionen
  - Diebstahl von Anmeldeinformationen für das Büronetz
  - Benutzung des VPN-Zugangs zum Büronetz
  - Zugang zur Prozessnetzinfrastruktur über VPN und/oder das Büronetz
  - Manipulation der Firmware der eingesetzten Datenkonzentratoren
  - KillDisk zur gründlichen Bereinigung aller Spuren
  - Zeitgesteuertes Abschalten der USV-System in den Netzleitstellen
  - Telephone denial-of-service attack auf die Störungsannahmen

- Technische Fähigkeiten: Die technischen Fähigkeiten der Täter sind als hoch einzuschätzen. Zwar ist die eingesetzte Schadsoftware nicht sehr ausgefeilt, beispielsweise wurden keine Zero-Day-Schwachstellen ausgenutzt.

  Die Angreifer konnten sich jedoch über einen langen Zeitraum unbemerkt im Computernetz der Opfer ausbreiten und ihren Angriff vorbereiten.

  Die Täter gingen äußerst koordiniert vor und benutzten mehrere Angriffstechniken, um ihren Angriff zu verschleiern und eine Störungsbehebung zu erschweren (Quelle: BSI-Jahresbericht 2016).

2

MAßNAHMEN ZUR ABWEHR VON IT-ANGRIFFEN AUF KRITISCHE INFRASTRUKTUREN

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG, Juli 2015)

Ges. Regelungen für Energienetzbetreiber:

EnWG §11 Abs 1.a: … auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind.

BNetzA SiKat 08/2015: … Enthalten sind demnach zumindest alle TK- und EDV-Systeme des Netzbetreibers, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Daneben sind auch TK- und EDV-Systeme im Netz betroffen, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte…

Relativ einfach zu bestimmen

Je nach Größe der Organisation kann das beliebig komplex werden

Anforderungen an die Informationssicherheit nach BNetzA SiKat (08/2015)

- Netzbetreiber haben ein ISMS nach **DIN ISO/IEC 27001** zu implementieren, das mindestens die für einen **sicheren Netzbetrieb** notwendigen Telekommunikations- und EDV-Systeme umfasst.
- Bei der Implementierung des ISMS sind […] die Normen DIN ISO/IEC 27002 und **DIN ISO/IEC TR 27019** in der jeweils geltenden Fassung zu berücksichtigen → besondere PDV-Anforderungen
- Maßnahmenbereiche der **DIN ISO/IEC 27001 und DIN ISO/IEC TR 27019,** die in den Normen durch viele Einzelmaßnahmen untergliedert werden:

A5 Richtlinien Informationssicherheit
A6 Organisation der Informationssicherheit
A7 Sicherheit im Personalmanagement
A8 Asset Management
A9 Zugangskontrolle
A10 Kryptografie
A11 Physische Sicherheit
A12 Sicherer Betrieb
A13 Sichere Kommunikation
A14 Systembeschaffung, Entwicklung und Pflege
A15 Lieferantenbeziehungen
A16 Management von Informations-sicherheitsvorfällen
A17 Kontinuität der Informationssicherheit
A18 Compliance

Welche Wirkung bzgl. der Hacking-Angriffe in der Ukraine ?

IT-Sicherheitsmaßnahmen zu den einzelnen Angriffs-schritten* des Hacking-Angriffs auf die Ukraine 2015

Step 1: Reconnaissance and Intelligence Gathering.
Prior to the attack, threat actors likelybegin open-source intelligence gathering andreconnaissance on potential targets.

- A05 Richtlinien Informationssicherheit
  - 5.1.1 Informationssicherheitsrichtlinien
  - 5.1.2 Überprüfung der Informationssicherheitsrichtlinien
- A06 Organisation der Informationssicherheit
  - 6.1.1 Rollen & Verantwortlichkeiten
  - 6.1.2 Aufgabentrennung
  - 6.2.1 Richtlinie zu Mobilgeräten
  - 6.2.2 Telearbeit
- A07 Sicherheit im Personalmanagement
  - 7.2.2 Informationssicherheitsbewusstsein, -ausbildung und –schulung
  - …
- A08 Asset Management
- A18 Compliance

Information Securiy Policy 6.1.1:
Miteinander in Konflikt stehende Aufgaben und Verantwortungs-bereiche sind zu trennen, um die Möglichkeiten unbefugter Änderung oder den Missbrauch von Unternehmenswerten zu reduzieren. In den Berechtigungs-vergabeprozessen sind, soweit technisch und organisatorisch möglich, Vorkehrungen zur Funktionstrennung zu treffen.

Folgende Aspekte in Bezug auf angemessene Aufgabentrennung sind…

Step 2: Malware Development and Weaponization.

…

* Gesamtliste basierend auf der Studie von Booz Allen Hamilton siehe Backup

Schutzwirkung der aus den Normen ISO/IEC 27001 und ISO/IEC TR 27019 anzuwenden Sicherheitsmaßnahmen

ISO/IEC 27001 Annex A Control Domains	in %	...
A05 Richtlinien Informationssicherheit	2%	
A06 Organisation der Informationssicherheit	3%	
A07 Sicherheit im Personalmanagement	2%	
A08 Asset Management	6%	
A09 Zugangskontrolle	17%	
A10 Kryptografie	3%	
A11 physische Sicherheit	5%	
A12 Sicherer Betrieb	18%	
A13 Sichere Kommunikation	11%	
A14 Systembeschaffung, Entwicklung und Pflege	15%	
A15 Lieferantenbeziehungen	6%	
A16 Management von Informationssicherheitsvorfällen	5%	
A17 Kontinuität der Informationssicherheit (> Notfall-, Krisen-Management)	6%	
A18 Compliance	2%	
Gesamtergebnis	**100%**	

- Bei dem Hacking-Angriff auf die Stromversorgung der Ukraine im Dezember 2015 wird die primäre Schutzwirkung durch die **geeignete** Umsetzung von Sicherheitsmaßnahmen aus den Bereichen A09, A12, A13 und A14 erzielt.
- Als flankierende Maßnahmen sind auch Sicherheitsmaßnahmen der Bereiche A08, A11, A15, A16 und A17 angemessen anzuwenden.
- In den vorliegenden Analysen wurden keine zusätzlichen Maßnahmen abgeleitet, die nicht bereits in den vorliegenden Normen adressiert werden.

3 WESENTLICHE PROZESSE EINES ISMS

Implementierung der ISMS Prozesse und Unterstützung durch das Management

- Ein ISMS nach den gesetzlichen Anforderungen in Deutschland erfordert einen erheblichen Aufwand:
  - an Personalressourcen in den betroffenen Bereichen
  - für die Ausbildung der eigenen Fachleute
  - für externe Unterstützung
    - beim ISMS Aufbau und Audits
    - und die Erarbeitung von Sicherheitskonzepten
- Die Managementunterstützung wird benötigt:
  - für den Aufbau und Betrieb der ISMS-Organisation und ihrer Gremien
  - für das Ausgestalten der Arbeitsprozesse nach den Maßgaben des Standards
  - für die benötigte Dokumentation und für den Verbesserungsprozess auf Grundlage des Reportings

Risiko-Management im ISMS

- Die allgemeinen Anforderungen an den Prozess zur Risikoeinschätzung sind in Kapitel 6.1.2. der DIN ISO/IEC 27001:2015-3 geregelt.
- Das Risiko-Management eines ISMS basiert auf den Information-Assets im ISMS-Asset-Register.
- Man kann bei den ISMS-Assets technische Systeme, Informationen und Prozesse geeignet zusammenfassen und so die Anzahl der im Risiko-Management zu behandelnden Objekte beherrschbar zu machen.
- Konzentriert man allerdings zu stark, bekommt man bei der Durchführung der Risikoanalyse so viele mögliche Einfluss-faktoren, dass die Nachvollziehbarkeit der Ergebnisse sehr schwierig wird.

Zusätzliche Anforderungen an das Risikomanagement im ISMS nach BNetzA SiKat (08/2015)

- Für die Komponenten, Systeme und Anwendungen, die für einen sicheren Netzbetrieb notwendig sind, ist grundsätzlich von einer Einstufung in die Kategorie „hoch“ auszugehen. Im Einzelnen ist zu prüfen, ob ggf. eine Einstufung als „kritisch“ notwendig ist…

In normalen Betrieben sind rund 70% aller Assets in der Kategorie „normal“ d.h. dann ist ein Grundschutz umzusetzen, für den es viele Beispiele gibt.

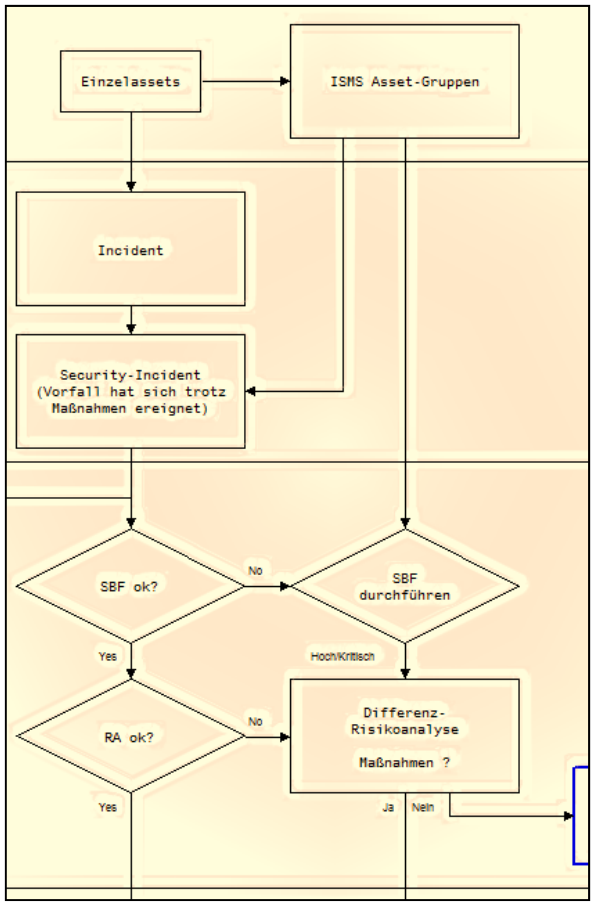
- Zusätzlich zu berücksichtigende Schadenskategorien u.a.
  - Beeinträchtigung der Versorgungssicherheit,
  - Einschränkung des Energieflusses,
  - Betroffener Bevölkerungsanteil,
  - Auswirkungen auf weitere Infrastrukturen (z. B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung),

Ein normales ISMS betrachtet Einflüsse , die keine direkten Rückwirkungen auf die eigene Organisation haben nicht weiter. Hier sind Methoden der Umsetzung zu entwickeln

- Erkannte Risiken sind i. d. Regel durch Maßnahmen nach dem allgemein anerkannten „Stand der Technik“ zu behandeln.

Da ist eine hohe Anforderung für eine Flächeninfrastruktur mit einen Life-Cycle größer 25 Jahren

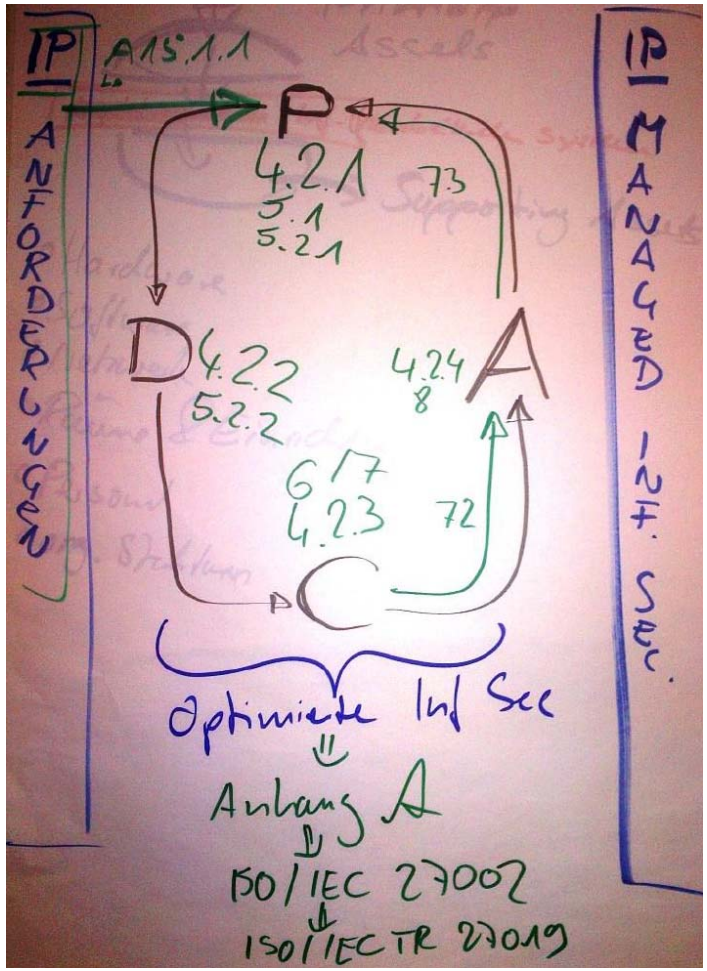
Einführung von Standard-Betriebsprozessen für Incident-, Change-, Key-, und BCM-Management



- Die Anforderungen aus dem ISMS für diese Standard-Betriebsprozesse sind meist deutlich formaler und zuverlässiger einzuhalten und stringenter zu dokumentieren, als das bisher im Betrieb üblich war.
- Bei knappen Ressourcen diese Anforderungen in den Fachabteilungen umzusetzen, ist meist die größte Herausforderung für die betroffenen Fachbereiche und am langwierigsten.
- Es hat sich bewährt, zunächst mit einfachen Strukturen zeitnah zu beginnen, statt nach langem Planen den perfekten Prozess nicht umgesetzt zu haben.
- Von Anfang an sollten die kritischen Parameter und die Ergebnisse der Prozesse ausgewertet werden, um damit einen Verbesserungsprozess aufzusetzen.

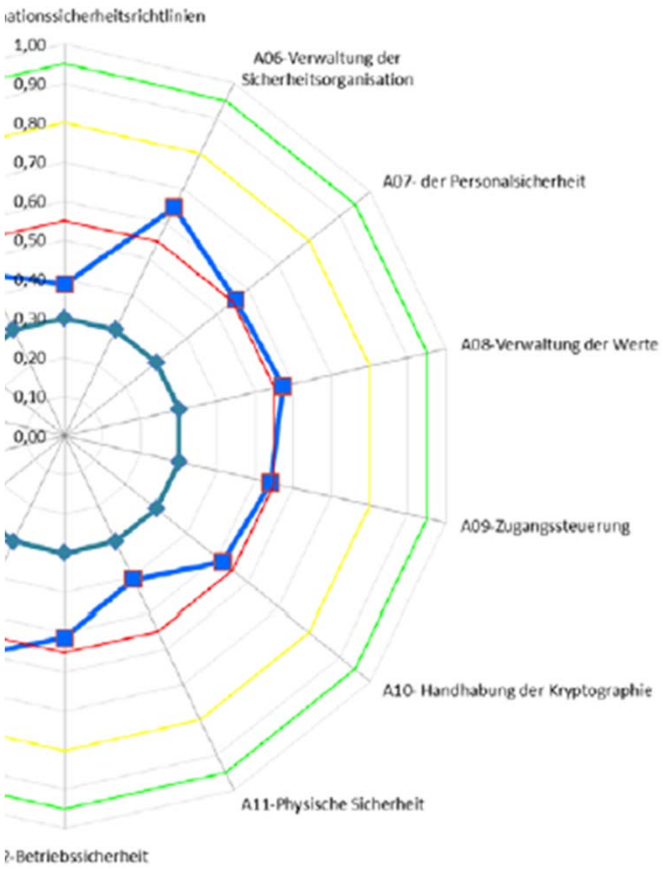
Schulungen

- Schulungen für Sicherheitsexperten
  - ISMS Lead Auditor: ISO27001:2013
  - ISMS Implementierung: ISO 27001:2013
  - Technisches Know-How für ISMS-Beauftragte und Auditoren
  - Hacking & Penetration Testing
- Schulungen Mitarbeiter im Scope des ISMS
  - Interne Schulungstage und Workshops mit eigenen und externen Experten
  - Z.B: Social Engineering und Security Awareness
- Schulungen für alle Mitarbeiter
  - Schulung „über die Line“
  - Aktuelle Cybersicherheitskampagne: “The Human Firewall“



Das Messen der Sicherheitsleistung der ISMS-Prozesse und der Informationssicherheitsprozesse

- ISO/IEC 27001:2013, Kapitel 9
  Bewertung der Leistung:
  - Die Organisation muss die Informationssicherheitsleistung und die Wirksamkeit des ISMS bewerten…
  - Die Organisation muss bestimmen: … die Methoden zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen
- Einsatz eines prozessorientierten Messverfahrens sowohl für die Managementprozesse des ISMS als auch für die Informationssicherheitsprozesse (Annex A der 27001)
- Alle umgesetzten Sicherheitsmaßnahmen werden für jeweils ein Jahr auf die Informationssicherheits-prozesse gemappt, so dass vom ISMS-Scope und von der Größe des ISMS unabhängige und vergleichbare ISMS-Kennzahlen ermittelt werden können.



Interne Audits

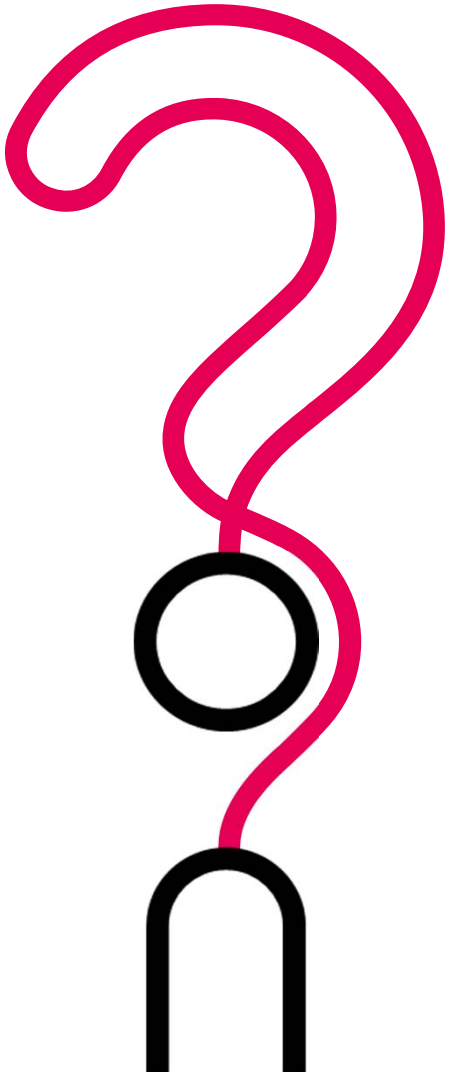
- ISO/IEC 27001 Kap 9.2 Internes Audit:
  - Die Organisation muss in geplanten Abständen interne Audits durchführen, um Informationen darüber zu erhalten, ob das ISMS:
  - a) die Anforderungen
    - 1) der Organisation an ihr ISMS und
    - 2) dieser Internationalen Norm erfüllt;
  - b) wirksam verwirklicht und aufrechterhalten wird.
- Bei einem zertifizierten ISMS sind alle ISMS-Assets mindestens einmal im Drei-Jahres-Zyklus auch intern zu auditieren.
- Auditoren sind so auszuwählen und Audits so durchzuführen, dass die Objektivität und Unparteilichkeit des Auditprozesses sichergestellt ist.
- Die Ergebnisse der Audits werden gegenüber der zuständigen Leitung berichtet.
- Dokumentierte Informationen und Ergebnisse des Audits sind aufzubewahren.

4 AUSBLICK

Ausblick

- Die breite Einführung von Informationssicherheitsmanagement-Prozessen in allen Unternehmen in diesen Bereich der Kritischen Infrastrukturen in Deutschland ist ein wichtiger Beitrag zur Verbesserung des IT-Sicherheitsniveaus im Land.
- Wesentlich zum Erreichen der angedachten Schutzwirkung ist neben dem Einsatz aktueller technischer Schutzsysteme vor allem die sorgfältige Ausgestaltung von Regelprozessen und ihre nachhaltige Umsetzung.
- Weitere kritische Faktoren sind die fundierte Ausbildung und Motivation der Security-Experten und die Awareness aller Mitarbeiter in Unternehmen bzgl. ungewöhnlicher Vorgänge und das Einhalten der gesetzten Regel in Unternehmen.
- Aktuell gibt einen ungedeckten Bedarf von Security-Experten in der Industrie mit deutlich steigender Tendenz.

Rolf-Dieter Kasper
Netztechnik und Security
Sparte Netz & Infrastruktur
rolf-dieter.kasper@innogy.com
T +49 201 12-29386 · M +49 172 2311977
innogy SE
Kruppstraße 5 · 45128 Essen
innogy
am Rolf-Dieter



FRAGEN?

X BACKUP

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phasen 1 und 2 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

Step 1*: Reconnaissance and Intelligence Gathering.

Prior to the attack, threat actors likelybegin open-source intelligence gathering andreconnaissance on potential targets.

- A05 Richtlinien Informationssicherheit
- A06 Organisation der Informationssicherheit
- A07 Sicherheit im Personalmanagement
- A08 Asset Management
- A18 Compliance

Step 2: Malware Development and Weaponization.

Threat actors acquire or independently develop the malware tobe used in the attack, as weil as the weaponized documents to deliver the malicious files.

- A14 Systembeschaffung, Entwicklung und Pflege
- A15 Lieferantenbeziehungen
- A16 Management von Informationssicherheitsvorfällen

* Die Schritte basieren auf der Studie von Booz Allen Hamilton; siehe Folie 7

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phasen 3 und 4 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

Step 3: Deliver Remote Access Trojan (RAT).

Threat actors initiate phishing campaignagainst electricity distributors.

- A12 Sicherer Betrieb
- A13 Sichere Kommunikation
- A16 Management von Informationssicherheitsvorfällen

Step 4: Install RAT.

Threat actors successfully insfall BlackEnergy 3 (BE3) on each of the three targeted electricity distributors after employees open the weaponized MS Office email attachments and enable macros.

- A09 Zugangskontrolle
- A12 Sicherer Betrieb
- A14 Systembeschaffung, Entwicklung und Pflege
- A16 Management von Informationssicherheitsvorfällen

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phasen 5 und 6 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

Step 5: Establish Command-and-Control(CC) Connection.

Malware establishes connection from malicious im plant on targeted network to attacker-controlled command-and-control (CC) server.

- A10 Kryptografie
- A12 Sicherer Betrieb
- A13 Sichere Kommunikation

Step 6: Deliver Malware Plugins

Following installation of BE3 implant, threat actors likely import plugins to enable credential harvesting and internal network reconnaissance.

- A09 Zugangskontrolle
- A12 Sicherer Betrieb
- A13 Sichere Kommunikation
- A14 Systembeschaffung, Entwicklung und Pflege

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phasen 7 und 8 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

innogy

Step 7: Harvest Credentials.

Delivered BE3 malware plugins conduct credential harvesting and network discovery functions.

- A09 Zugangskontrolle
- A10 Kryptografie
- A13 Sichere Kommunikation

Step 8: Lateral Movement and Target Identification on Corporate Network.

Threat actors conduct internal reconnaissance on corporate network to discover potential targets and expand access.

- A08 Asset Management
- A09 Zugangskontrolle
- A12 Sicherer Betrieb
- A14 Systembeschaffung, Entwicklung und Pflege

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phasen 9 und 10 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

Step 9: Lateral Movement and Target Identification on ICS network.

Threat actors use stolen credentials to access the control environment and conduct reconnaissance on deployed systems.

- A08 Asset Management
- A09 Zugangskontrolle
- A11 physische Sicherheit
- A12 Sicherer Betrieb
- A14 Systembeschaffung, Entwicklung und Pflege

Step 10: Develop Malicious Firmware.

Threat actors develop malicious firmware update for identified serial-to-Ethernet converters.

- A08 Asset Management
- A14 Systembeschaffung, Entwicklung und Pflege
- A15 Lieferantenbeziehungen

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phasen 11 und 12 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

Step 11: Deliver Data Destruction Malware.

Threat actors likely deliver Kill-Disk malware to network share and set policy on domain controller to retrieve malware and execute upon system reboot.

- A09 Zugangskontrolle
- A12 Sicherer Betrieb
- A13 Sichere Kommunikation
- A14 Systembeschaffung, Entwicklung und Pflege

Step 12: Schedule Uninterruptable Power Supply (UPS) Disruption.

Threat actors schedule unauthorized outage of UPS for telephone communication server and data center servers.

- A09 Zugangskontrolle
- A11 physische Sicherheit
- A12 Sicherer Betrieb

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phasen 13 und 14 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

Step 13: **Trip Breakers**.

Threat actors use native remote access services and valid credentials to open breakers and disrupt power distribution to over 225,000 customers within three distribution areas.

- A09 Zugangskontrolle
- A12 Sicherer Betrieb
- A13 Sichere Kommunikation
- A17 Kontinuität der Informationssicherheit (> Notfall-, Krisen-Management)

Step 14: Sever Connection to Field Devices.

After opening the breakers, threat actors deliver malicious firmware update to serial-to-Ethernet communications devices. The malicious updates render the converters inoperable, and sever connections between the control center and the substations.

- A09 Zugangskontrolle
- A12 Sicherer Betrieb
- A13 Sichere Kommunikation
- A14 Systembeschaffung, Entwicklung und Pflege
- A17 Kontinuität der Informationssicherheit (> Notfall-, Krisen-Management)

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phasen 15 und 16 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

Step 15: Telephony Denial-of-Service Attack.

Threat actors initiate DoS attack on telephone call center at one of the targeted distributors.

- A06 Organisation der Informationssicherheit
- A14 Systembeschaffung, Entwicklung und Pflege
- A15 Lieferantenbeziehungen

Step 16: Disable Critical Systems via UPS Outage.

Previously scheduled UPS outage cuts power to targeted telephone communications server and data center servers.

- A09 Zugangskontrolle
- A11 Physische Sicherheit
- A12 Sicherer Betrieb
- A17 Kontinuität der Informationssicherheit (> Notfall-, Krisen-Management)

Hacking-Angriff auf die Stromversorgung der Ukraine im Dez. 2015: Phase 17 mit Schutzmaßnahmen nach ISO/IEC 27001 Annex A (auf Domain-Ebene)

Step 17: Destroy Critical System Data.

Scheduled execution of Kill-Disk malware erases the master boot records and deletes systemlog data on targeted machines across the victims' corporate and ICS network.

- A09 Zugangskontrolle
- A12 Sicherer Betrieb
- A14 Systembeschaffung, Entwicklung und Pflege
- A15 Lieferantenbeziehungen
- A17 Kontinuität der Informationssicherheit (> Notfall-, Krisen-Management)