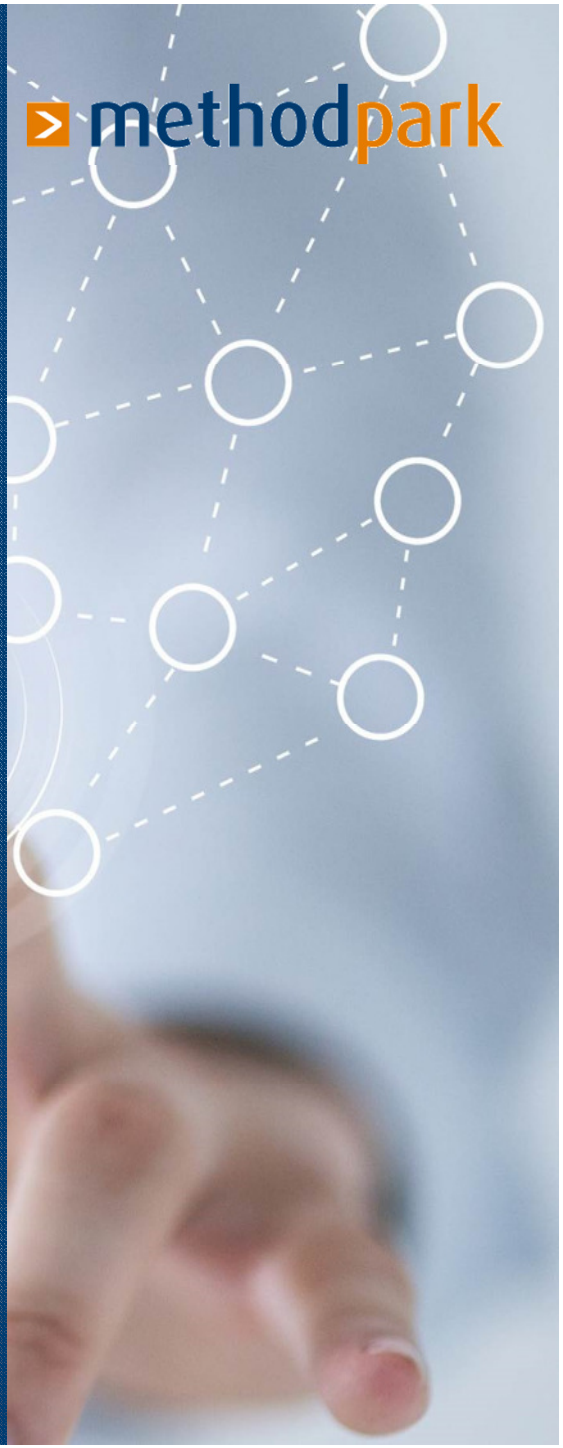
Cybersecurity – Was auf Engineering und Management zukommt

Talk im Park – Mai 2017

Jens Palluch, Method Park Consulting GmbH



Motivation

heise Security

Hacker steuern Jeep Cherokee fern

22.07.2015 06:20 Uhr – Ronald Eikenberg

Durch eine Schwachstelle im Infotainmentsystem konnten Sicherheitsforscher die Kontrolle über einen Jeep übernehmen – über das Internet. Anfällig sind möglicherweise weitere Modelle des Fiat-Chrysler-Konzerns. Ein erstes Update schafft Abhilfe.

Rückruf von 1,4 Millionen Fahrzeugen

Quelle: http://www.heise.de/security/meldung/Hacker-steuern-Jeep-Cherokee-fern-2756331.html?view=print

Was ist Security?

methodpark

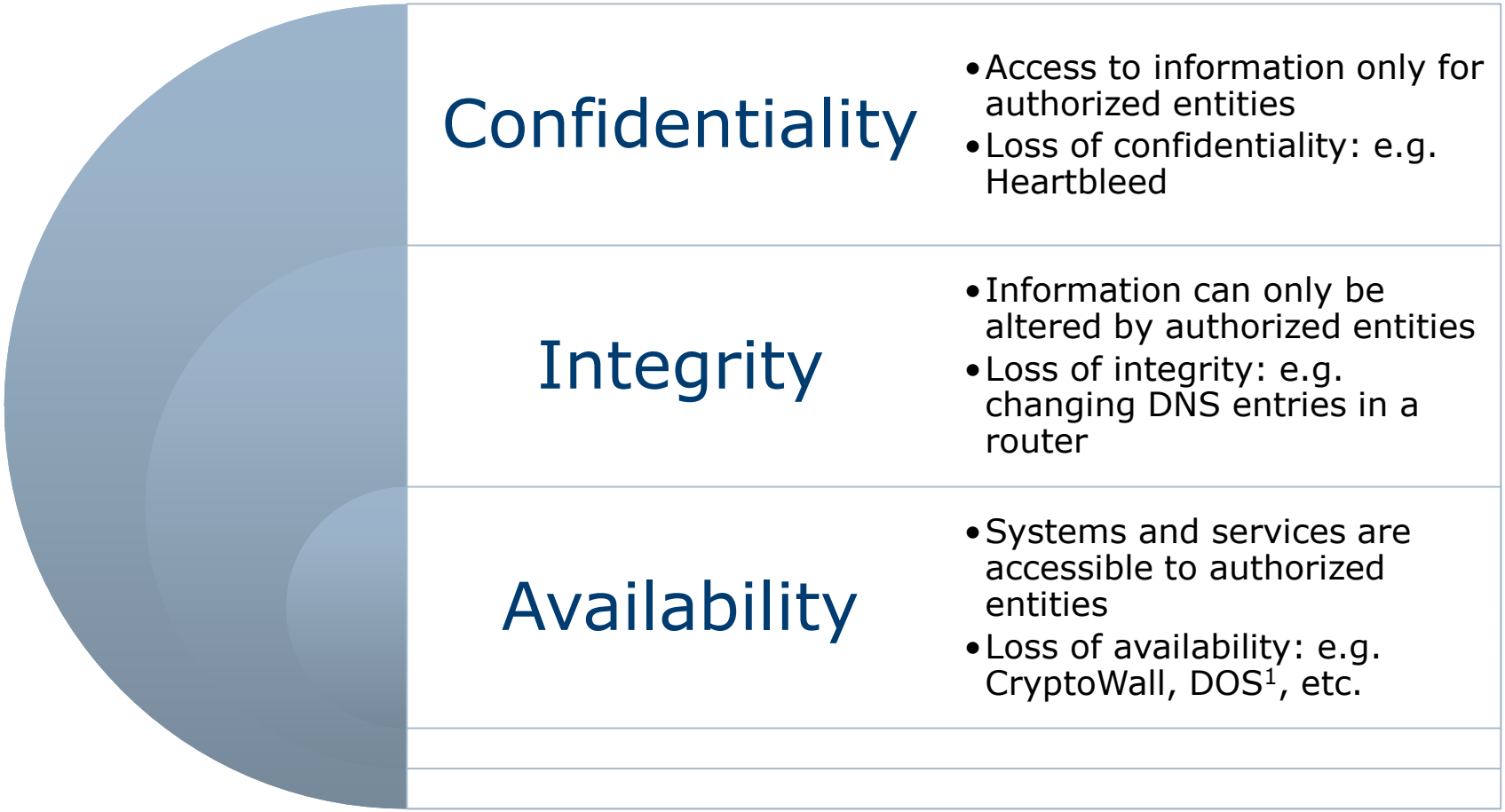
Security:

“The degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorisation.”

[ISO 25010 product quality model]

CIA – wünschenswerte Eigenschaften

methodpark



[1] DOS = Denial of Service

ISO 25010 Konzepte

methodpark

Product quality model

- **Confidentiality**
  - "degree to which a product or system ensures that data are accessible only to those authorized to have access"
- **Integrity**
  - "degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data"
- **Non-repudiation**
  - "degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later"
- **Accountability**
  - "degree to which the actions of an entity can be traced uniquely to the entity"
- **Authenticity**
  - "degree to which the identity of a subject or resource can be proved to be the one claimed"

Motivation

Weitere Sicherheitslücke in Hospira-Infusionspumpen

heise online 09.06.2015 07:38 Uhr – Denise Bergert

(Bild: Hospira)

In mehreren Infusionspumpen der Firma Hospira wurde eine weitere kritische Sicherheitslücke entdeckt. Über diese könnten Hacker die Dosierung von zu verabreichenden Medikamenten manipulieren.

Quelle: http://www.heise.de/newsticker/meldung/Weitere-Sicherheitsluecke-in-Hospira-Infusionspumpen-2682272.html

Was ist Cybersecurity?

methodpark

“4.20 Cybersecurity:

Cyberspace security

***preservation of confidentiality, integrity and availability of information** in the Cyberspace*

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

*Note 2 to entry: Adapted from the definition for **information security** in ISO/IEC 27000:2009.”*

ISO 27032:2012 – IT - Security techniques - Guidelines for cybersecurity

“4.21 the Cyberspace
complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”

Was ist Cybersecurity?

Cyber-Sicherheit:

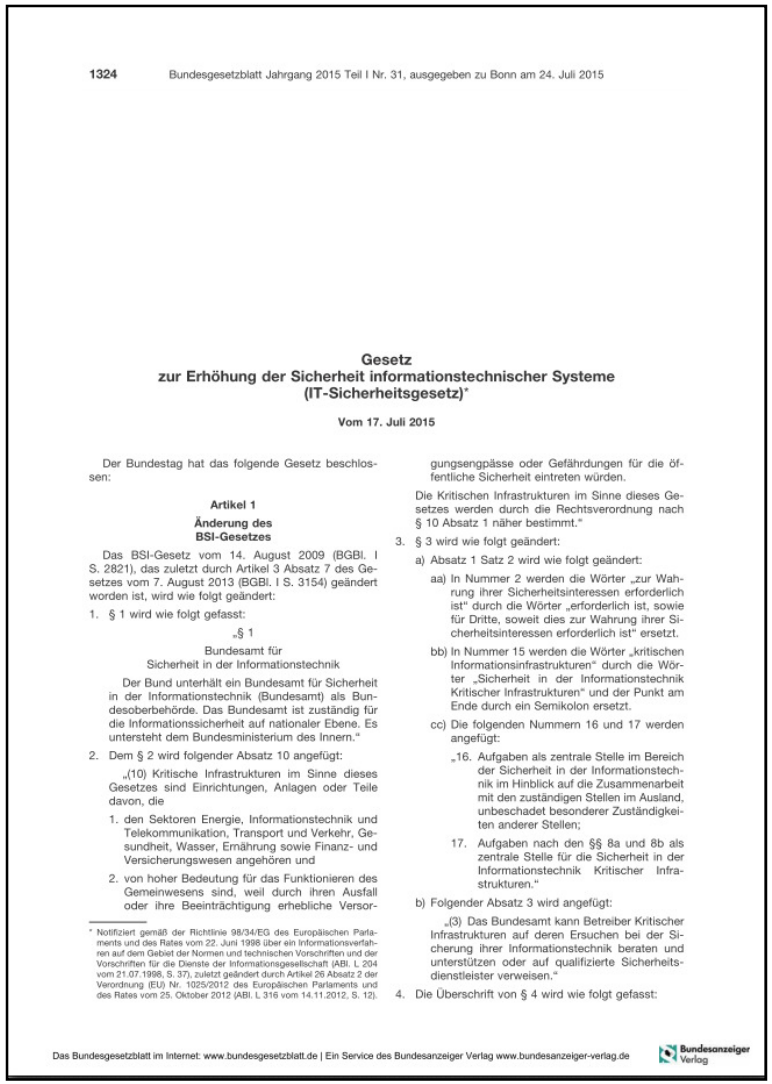
“Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik.
Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. ”

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html

Cyber-Sicherheitsstrategie

- Digitale Kompetenz bei allen Anwendern fördern
- Digitaler Sorglosigkeit entgegenwirken
- Kritische Infrastrukturen sichern
- Unternehmen in Deutschland schützen
- …

IT-Sicherheitsgesetz



1324 Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, ausgegeben zu Bonn am 24. Juli 2015

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*

Vom 17. Juli 2015

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des BSI-Gesetzes

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„§ 1

Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern."

2. Dem § 2 wird folgender Absatz 10 angefügt:

„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt."

3. § 3 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folgt geändert:

aa) In Nummer 2 werden die Wörter „zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" durch die Wörter „erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" ersetzt.

bb) In Nummer 15 werden die Wörter „kritischen Informationsinfrastrukturen" durch die Wörter „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" und der Punkt am Ende durch ein Semikolon ersetzt.

cc) Die folgenden Nummern 16 und 17 werden angefügt:

„16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen."

b) Folgender Absatz 3 wird angefügt:

„(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen."

4. Die Überschrift von § 4 wird wie folgt gefasst:

* Notifiziert gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204 vom 21.07.1998, S. 37), zuletzt geändert durch Artikel 26 Absatz 2 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 (ABl. L 316 vom 14.11.2012, S. 12).

Das Bundesgesetzblatt im Internet: www.bundesgesetzblatt.de | Ein Service des Bundesanzeiger Verlag www.bundesanzeiger-verlag.de

Bundesanzeiger Verlag

Maßnahmen

- Angemessene organisatorische und technische Maßnahmen

Nachweis

- Nachweis bzgl. der Maßnahmen

Meldepflicht

- Meldepflicht erheblicher Störungen

methodpark

Wer ist betroffen?

- Betreiber kritischer Infrastrukturen
- Betreiber kommerzieller Webangebote
- Ausnahme: Kleinstunternehmen
  [bis 9 MA und (bis 2 Mio € Jahresumsatz oder –bilanz)]

© Method Park Consulting GmbH / Jens Palluch / Cybersecurity – Was auf Engineering und Management zukommt / Talk im Park - Mai 2017

Betreiber kritischer Infrastrukturen (KRITIS)

- **Angemessene Maßnahmen** nach Stand der Technik zur Vermeidung von Störungen der
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
  - Authentizität

- **Nachweis der Maßnahmen** alle 2 Jahre gegenüber dem BSI

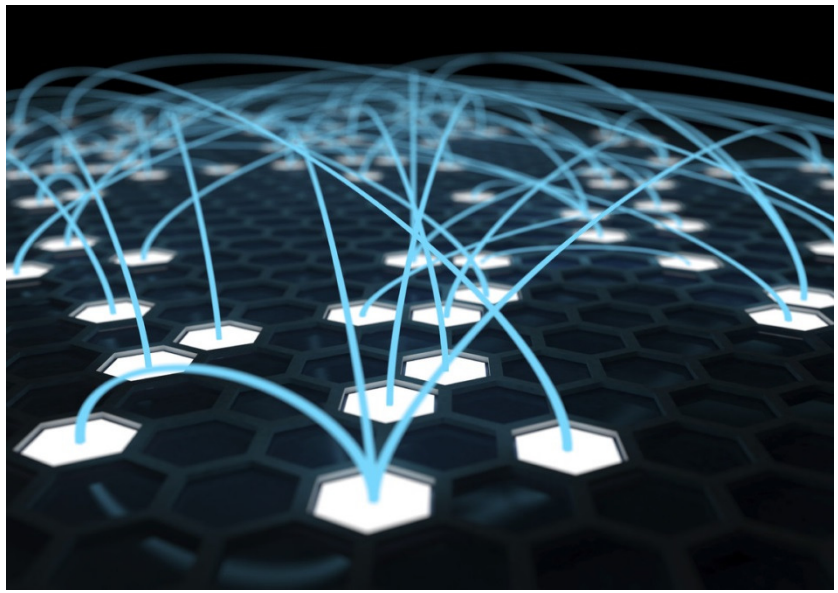
- **Meldepflicht erheblicher Störungen** gegenüber dem BSI

Kritische Infrastrukturen ?!?

methodpark

1. Branchen

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen



2. Von hoher Bedeutung für Funktionieren des Gemeinwesens

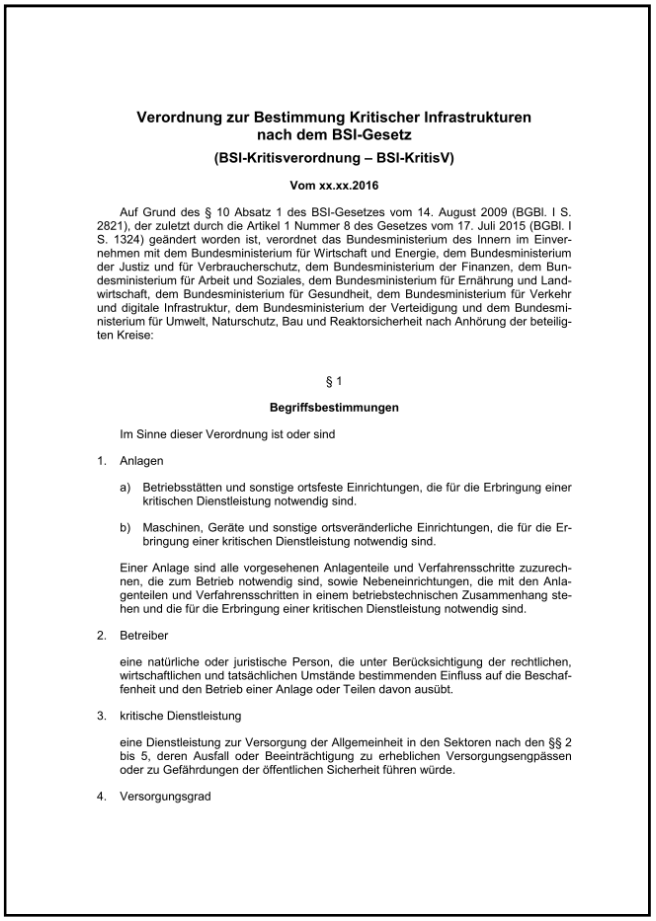
- Erhebliche Versorgungsengpässe
- Gefährdung der öffentlichen Sicherheit

Kritische Infrastrukturen ?!?

BSI-Kritisverordnung (BSI-KritisV) definiert seit 03. Mai 2016 **Kriterien** für die Branchen

- Energie
- Informationstechnik und Telekommunikation
- Wasser
- Ernährung

⇒ Betroffene Unternehmen müssen bis zum 03. Mai 2018 die gemäß IT-Sicherheitsgesetz geforderten Nachweise erbringen



Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz

(BSI-Kritisverordnung – BSI-KritisV)

Vom xx.xx.2016

Auf Grund des § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), der zuletzt durch die Artikel 1 Nummer 8 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, verordnet das Bundesministerium des Innern im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit nach Anhörung der beteiligten Kreise:

§ 1

Begriffsbestimmungen

Im Sinne dieser Verordnung ist oder sind

1. Anlagen

   a) Betriebsstätten und sonstige ortsfeste Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind.

   b) Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind.

   Einer Anlage sind alle vorgesehenen Anlagenteile und Verfahrensschritte zuzurechnen, die zum Betrieb notwendig sind, sowie Nebeneinrichtungen, die mit den Anlagenteilen und Verfahrensschritten in einem betriebstechnischen Zusammenhang stehen und die für die Erbringung einer kritischen Dienstleistung notwendig sind.

2. Betreiber

   eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.

3. kritische Dienstleistung

   eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren nach den §§ 2 bis 5, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.

4. Versorgungsgrad

Motivation

heise online

Massiver Hacker-Angriff auf Thyssenkrupp

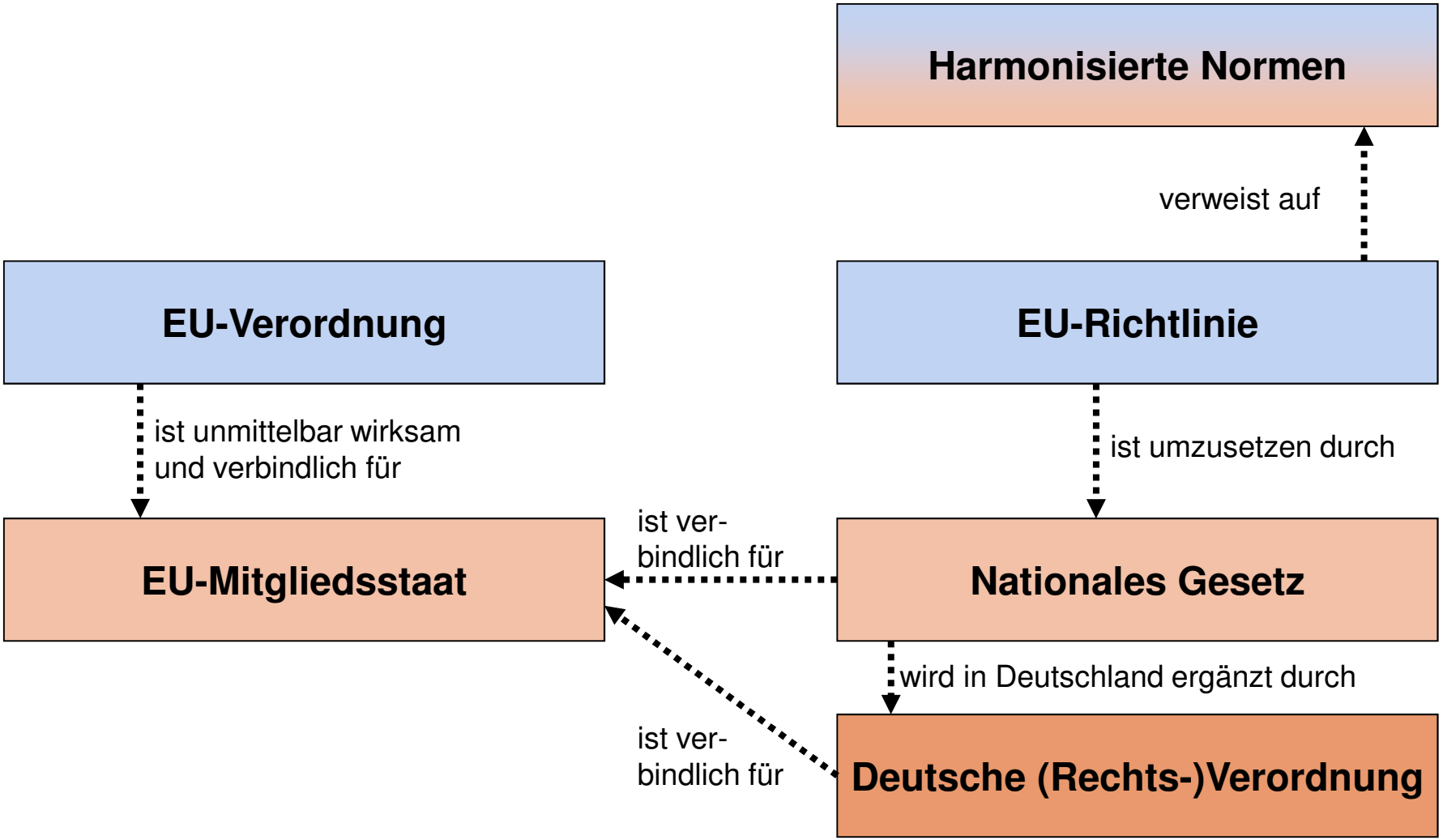
08.12.2016 11:47 Uhr

(Bild: thyssenkrupp.com)

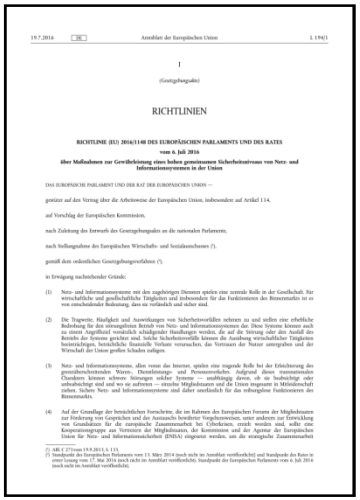
Straff organisierten Cyberkriminellen ist es laut einem Medienbericht gelungen, in die IT-Systeme des Industriekonzerns einzudringen.

Quelle: https://www.heise.de/newsticker/meldung/Massiver-Hacker-Angriff-auf-Thyssenkrupp-3565857.html

EU-Richtlinie vs. EU-Verordnung



EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie)



RICHTLINIEN

RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 6. Juli 2016
über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

Maßnahmen
- Angemessene organisatorische und technische Maßnahmen

Nachweis
- Nachweis bzgl. der Maßnahmen

Meldepflicht
- Meldepflicht erheblicher Störungen

Betreiber wesentlicher Dienste

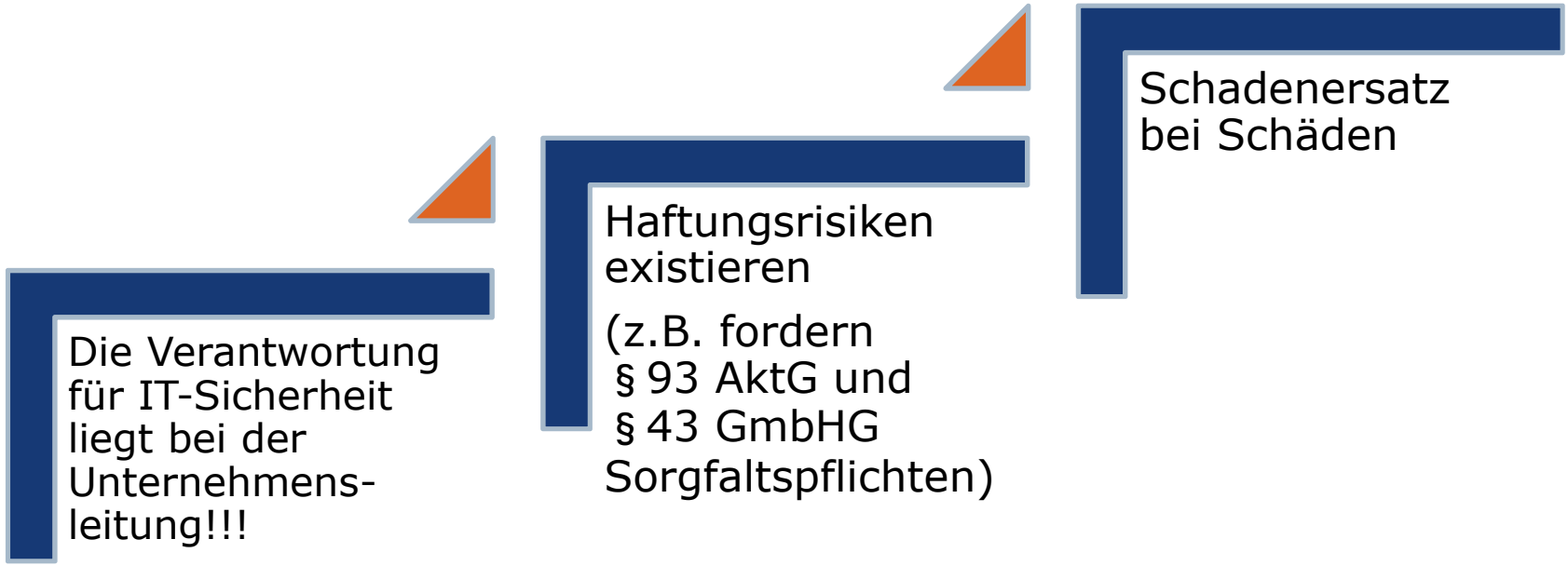
1. Online-Marktplatz
2. Online-Suchmaschine
3. Cloud-Computing-Dienst

Anbieter digitaler Dienste

Ausnahme: Kleinstunternehmen und kleine Unternehmen als Anbieter digitaler Dienste
[bis 49 MA und (bis 10 Mio € Jahresumsatz oder –bilanz)]

Wer ist verantwortlich?

methodpark



Was kann man tun?!?

methodpark

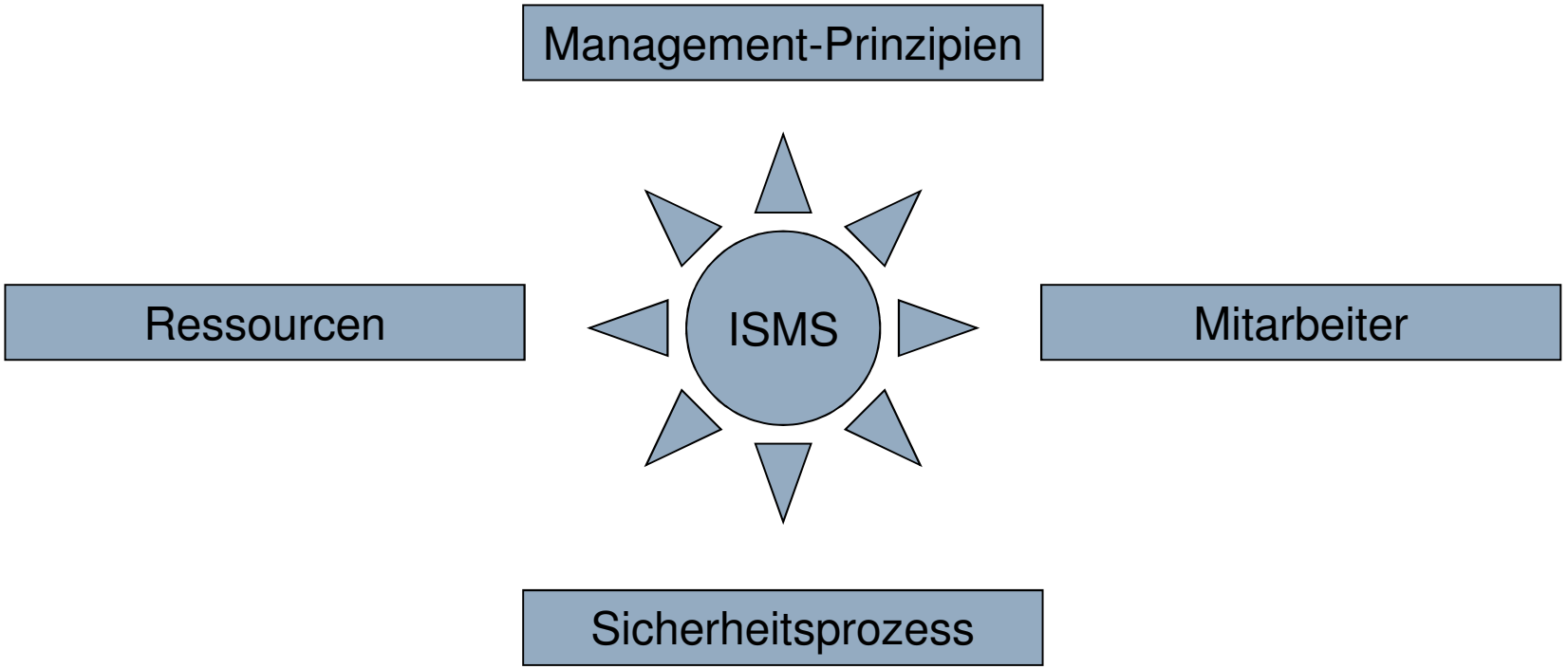
> "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."

Gene Spafford

[https://en.wikiquote.org/wiki/Gene_Spafford]

Einrichten eines ISMS (Informationssicherheitsmanagementsystem)

Grundlegende Komponenten eines ISMS



- Leitlinie zu Informationssicherheit
- Sicherheitskonzept
- Informationssicherheitsorganisation

IT-Grundschutz-Vorgehensweise

A) Grundstein legen

- Leitungsebene übernimmt Verantwortung
- Konzeption und Planung
  - Rahmenbedingungen ermitteln
  - Analyse der Geschäftsprozesse
  - allgemeine Informationssicherheitsziele definieren
  - Sicherheitsniveau der Geschäftsprozesse grob festlegen
- Leitlinie zur Informationssicherheit erstellen
- IS-Organisation aufbauen (Rollen, Aufgaben, Zuordnungen)
- Ressourcen bereitstellen (IT-Sicherheitsbeauftragter!)
- Einbindung aller Mitarbeiter
  - Mitarbeiter bzgl. IS schulen und sensibilisieren

B) Sicherheitskonzept planen

- Geltungsbereich definieren
- **Strukturanalyse**
  - Geschäftsprozesse, Anwendungen und Informationen
  - Netzplan
  - IT-Systeme
  - Räume
- **Schutzbedarf feststellen** für
  - Anwendungen, IT-Systeme, Räume, Kommunikationsverbindungen
- **Auswahl und Anpassung von Maßnahmen**
- **Basis-Sicherheitscheck**

© Method Park Consulting GmbH / Jens Palluch / Cybersecurity – Was auf Engineering und Management zukommt / Talk im Park - Mai 2017

IT-Grundschutz-Vorgehensweise

C) Sicherheitskonzept umsetzen

- Maßnahmen konsolidieren, Kosten- und Aufwandsschätzung
- Umsetzung planen (wer, was, bis wann) und kontrollieren
- Mitarbeiter schulen und sensibilisieren

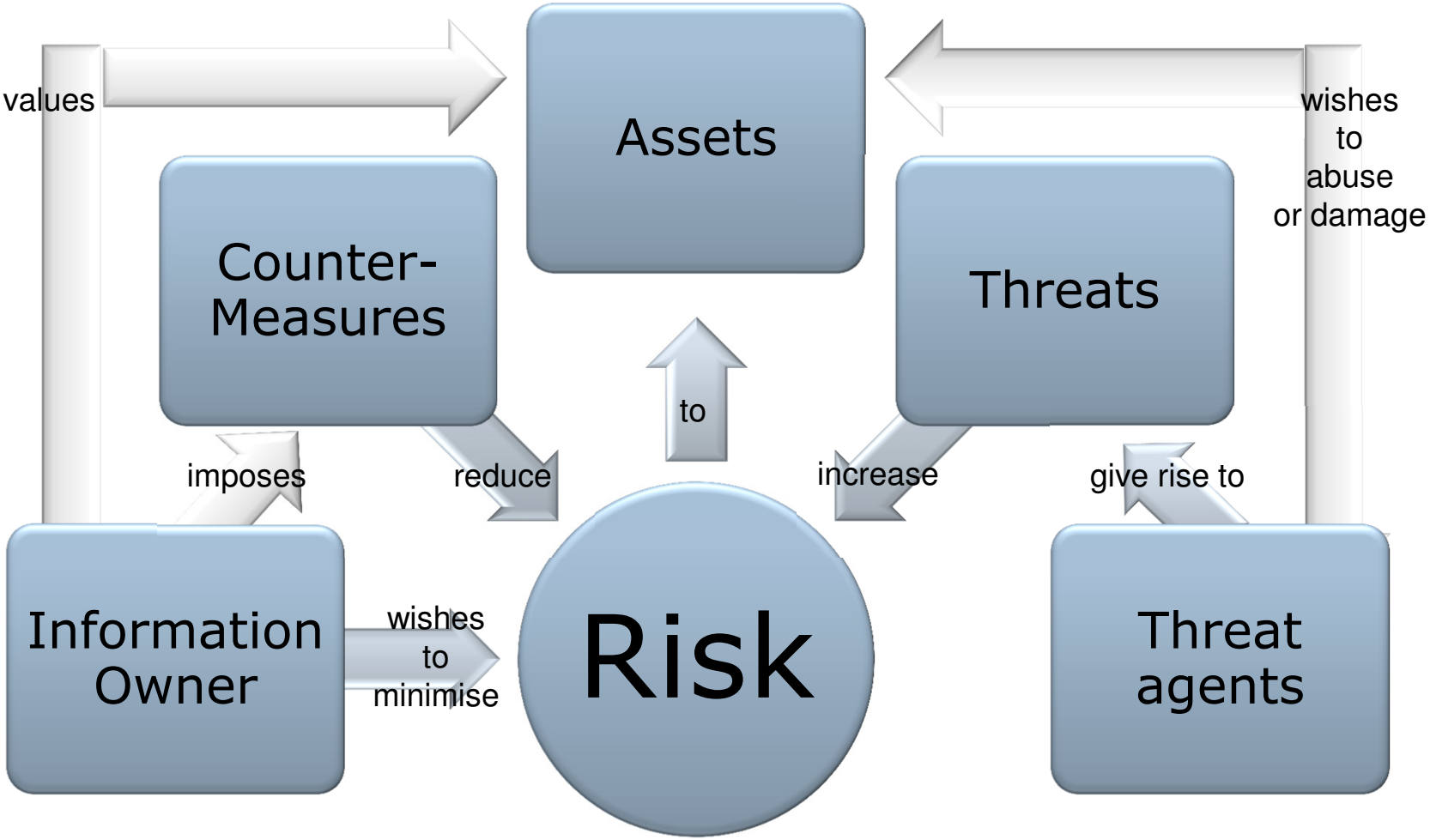
D) Aufrechterhaltung und kontinuierliche Verbesserung

- Zielerreichung messen
- Wirksamkeit und Effizienz der Maßnahmen überprüfen
- Sicherheitsziele, -strategie und –konzept auf Eignung prüfen
- Leitungsebene über Status des IS-Prozesses informieren
- Synergien zwischen IS-Prozess und anderen Management-prozessen (QM, Arbeitsschutz, Umwelt) ermitteln

Common Criteria (CC) – ISO/IEC 15408

- History – CC originated from three standards
  - ITSEC (France, Germany, the Netherlands, UK), 1990's.
  - CTCPEC, Canada, 1993.
  - TCSEC, Orange Book or DoD 5200.28 Std, 1985
- Comprised of three parts providing a methodology for
  - defining security requirements for product types (called protection profiles) e.g. a firewall or an operating system)
  - defining security requirements for specific products (called security targets)
  - evaluating and certifying software products and hardware-software-systems. For certification in Germany see the webpages of Federal Office for Information Security (BSI)
- download under http://www.commoncriteriaportal.org/cc/

Common Criteria – Part I
Security concept



[Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, v3.1, Sept. 2012]

Security by Design – Security Engineering

methodpark

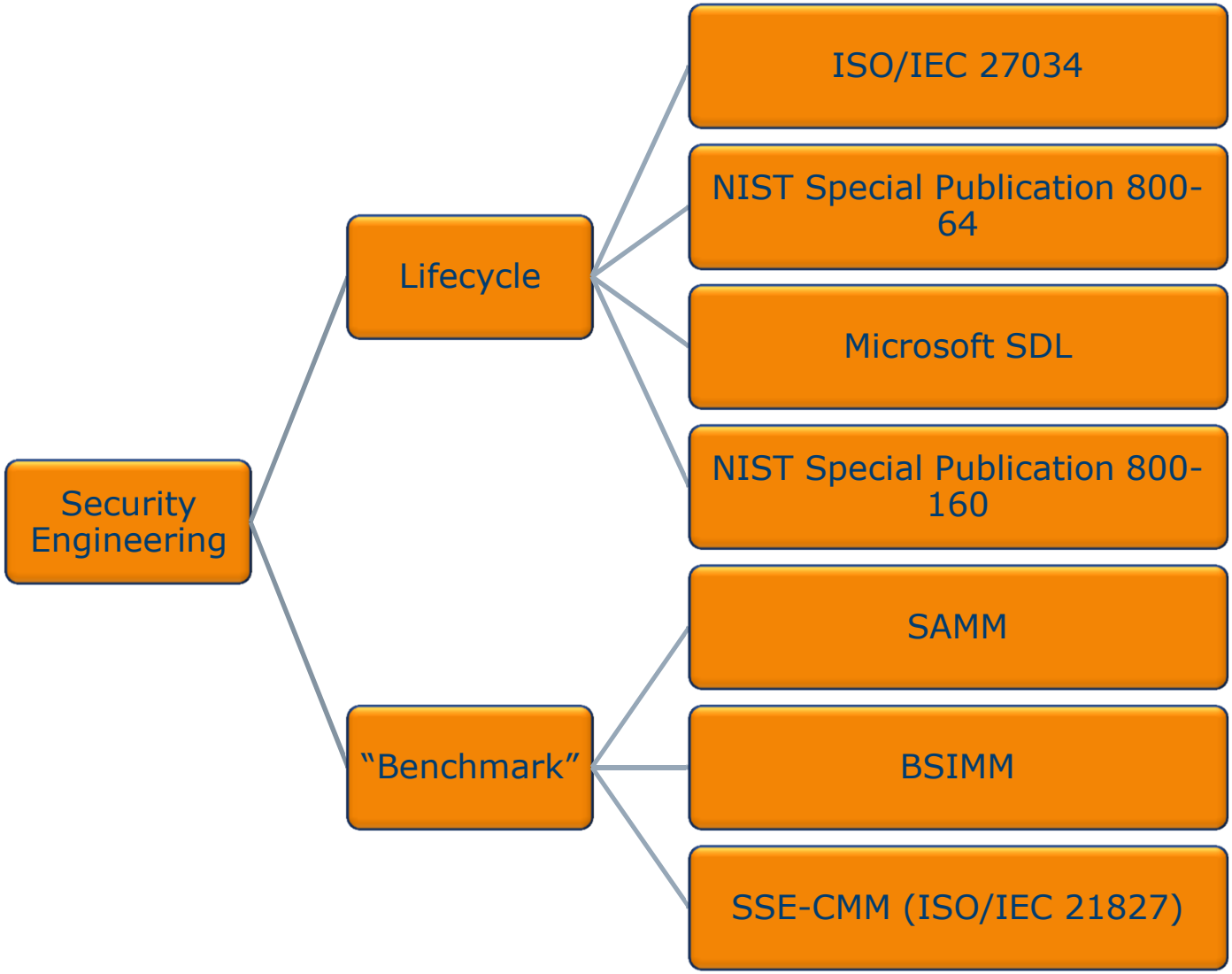
> "We wouldn't have to spend so much time, money, and effort on network security if we didn't have such bad software security."

[Vorwort von Bruce Schneier in: Viega & McGraw: Building Secure Software - How to Avoid Security Problems the Right Way, Addison Wesley, 2001]

> "Present software development methods lack in-depth security awareness, discipline, best practice, and rigor, and this is evidenced by the sheer quantity of security patches issued each year by all software vendors."

[Howard & Lipner: The Security Development Lifecycle - SDL: A Process for Developing Demonstrably More Secure Software, Microsoft Press, 2006]

Security Engineering Standards

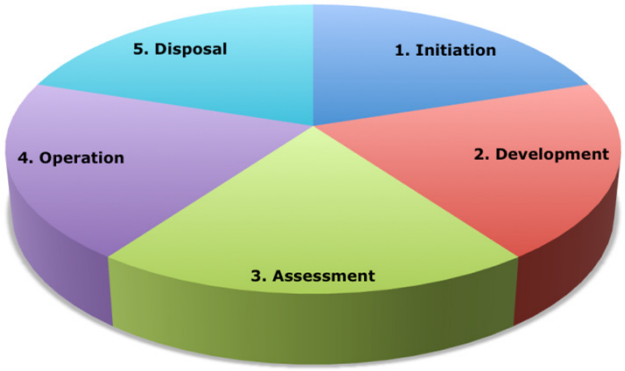


NIST Special Publication 800-64

Security Considerations in the System Development Life Cycle

- definiert Security-Aktivitäten und Kontrollpunkte
  für jede der 5 Lebenszyklusphasen

1. Initiation – Security mehr aus Sicht von Geschäftsrisiken berücksichtigen
2. Development/Acquisition – Entwicklungs- und Test-Aktivitäten
3. Implementation/Assessment – Aktivitäten zur Integration des Systems in die Produktivumgebung
4. Operations and Maintenance – Aktivitäten für Betrieb und Wartung
5. Disposal – Aktivitäten bzgl. Archivierung, usw.

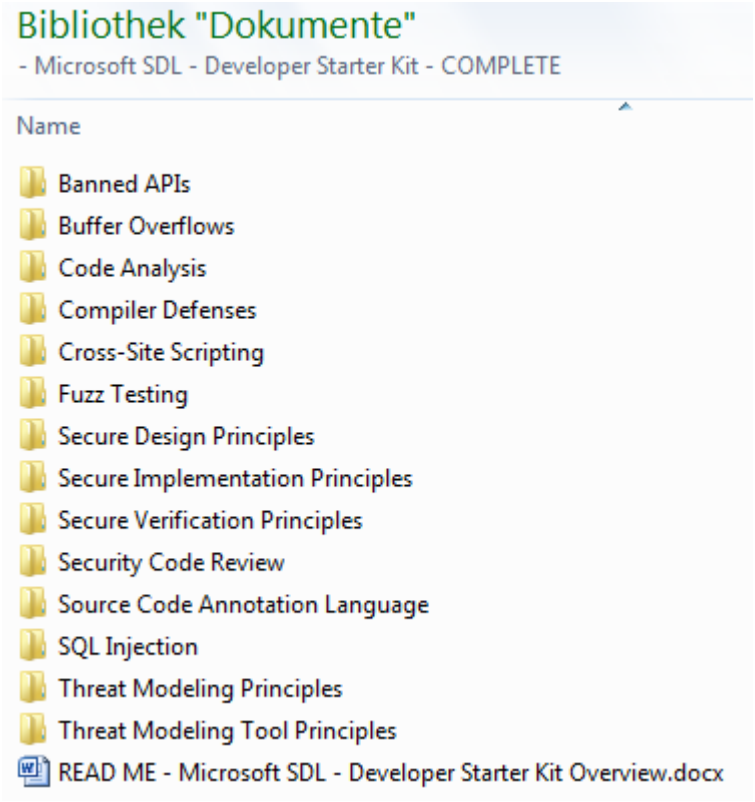


MS Security Development Lifecycle

methodpark

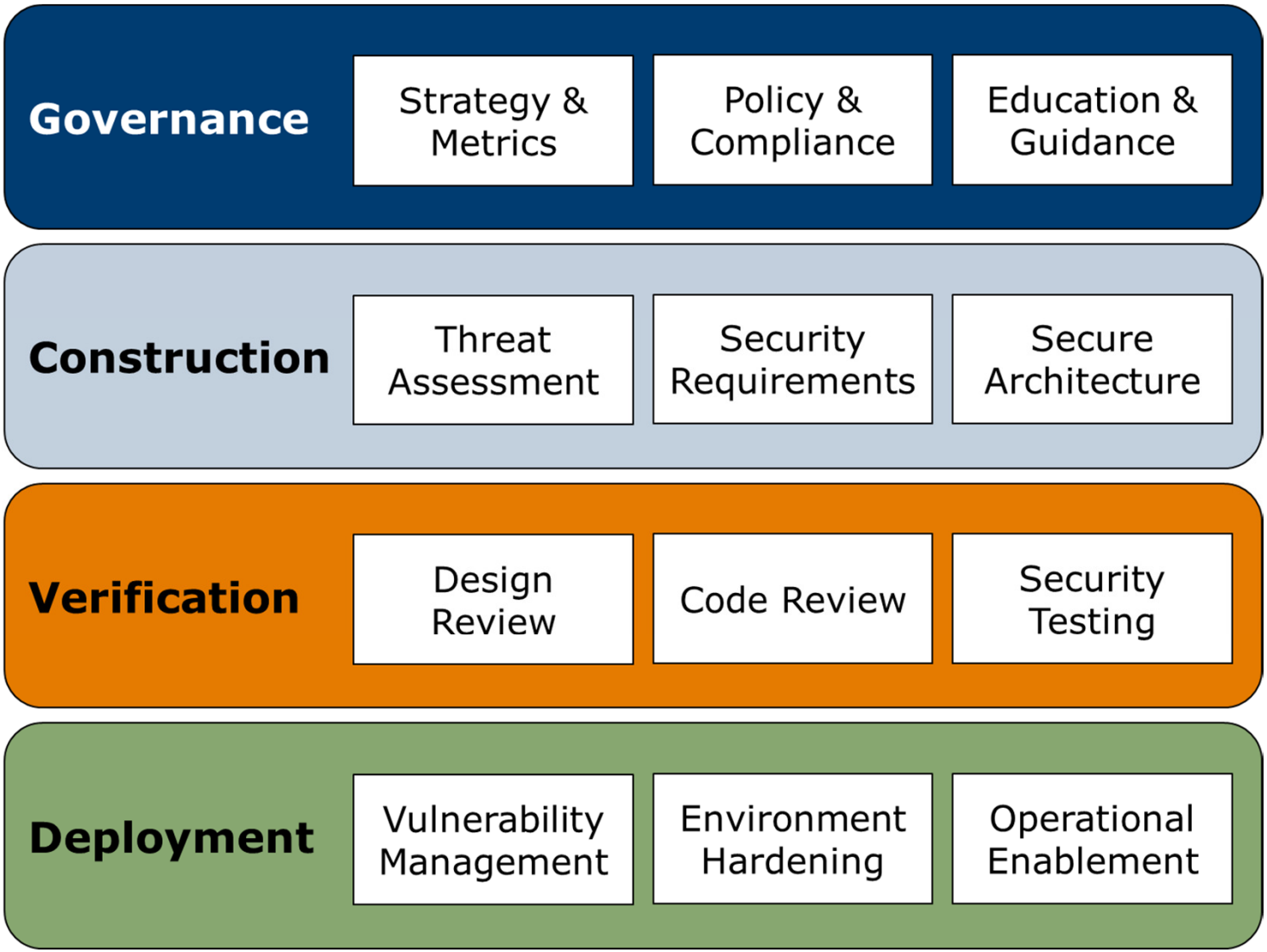
Training | Require-ments | Design | Implemen-tation | Verifi-cation | Release | Response

- Umsetzung der ISO/IEC 27034
- Dokumentation im Internet
- Microsoft SDL - Developer Starter Kit
  - 14 Themen
  - Jedes Thema:
    - Powerpoint-Präsentation
    - Traineranleitung
    - Aufgezeichnete Präsentation
    - Verständnisfragen (inkl. Antworten)



Software Assurance Maturity Model (SAMM)

methodpark



Bedrohungen und Schwachstellen

methodpark

Bedrohung (Threat):

Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann.

Schwachstelle (Vulnerability):

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen.

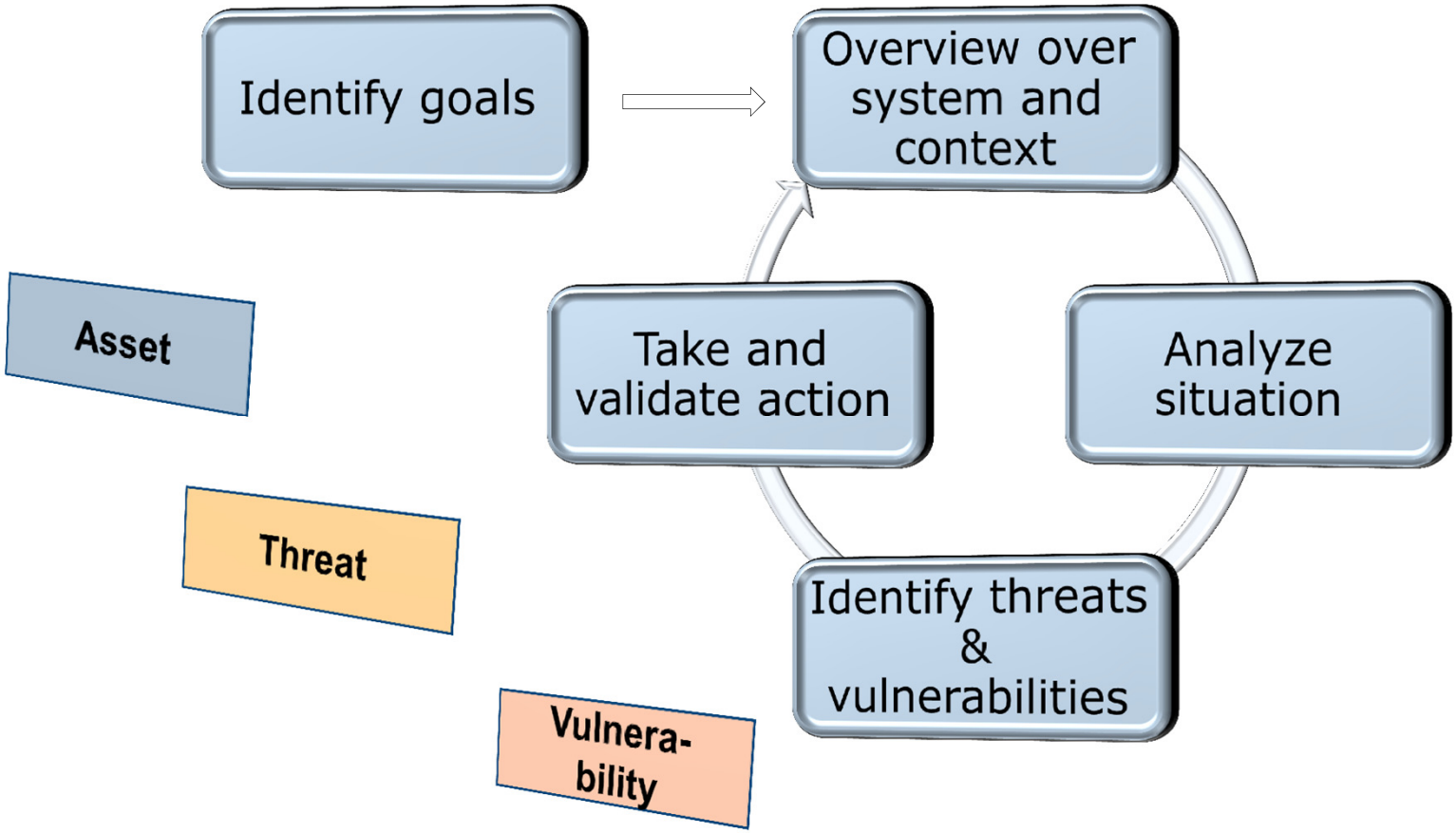
Wert (Asset)

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

[Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html]

Bedrohungsmodellierung

[oriented on OWASP threat assessment and C. Graf, Security Testing – Nur eine Aufgabe für geborene Hacker?, SQ-Magazin, Issue 39, June 2016]



Zum Ende

Jens Palluch
Method Park
Consulting GmbH
jens.palluch@methodpark.de