SECURITY BY DESIGN

Software von Anfang an sicher entwickeln

Dr. Masud Fazal-Baqaie, Dr. Matthias Becker

PVM-Tagung, 15. Oktober 2018, Düsseldorf

GESELLSCHAFT FÜR INFORMATIK

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Dr. Masud Fazal-Baqaie

Gruppenleiter
Softwaretechnik und IT-Sicherheit
Fraunhofer IEM

masud.fazal-baqaie@iem.fraunhofer.de

@masudfb

- GI-Fachgruppe Vorgehensmodelle
  - Stv. Sprecher der Fachgruppe
  - Co-Chair der Tagung Projektmanagement & Vorgehensmodelle

- Forschungsinteressen und Themen
  - Entwicklungsprozesse
  - Anforderungsmanagement
  - Agilität

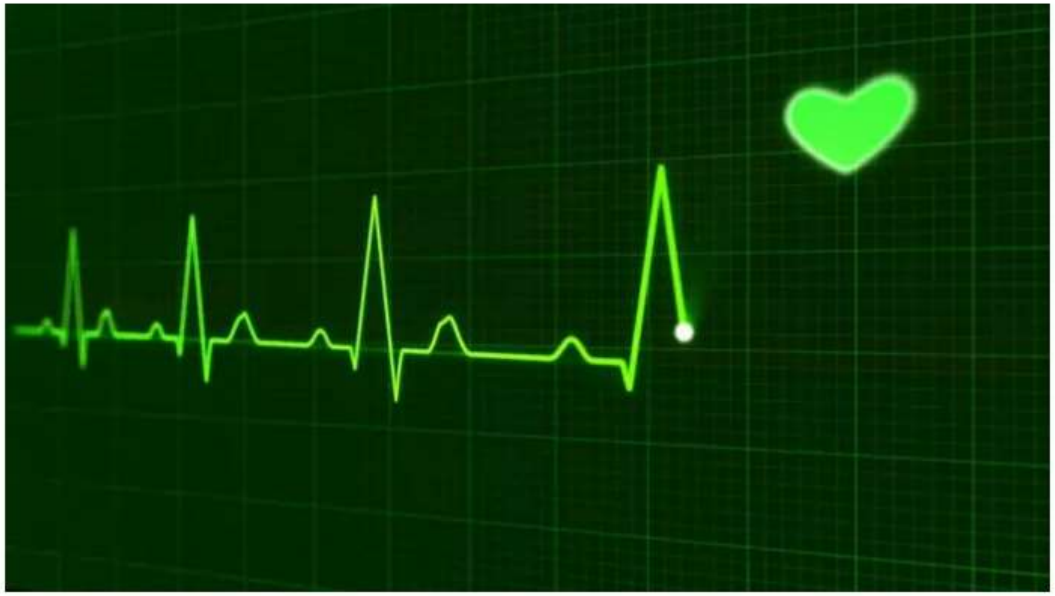
HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Warum ist sichere Software ein wichtiges Thema?

Unsichere Software kann Leben gefährden
Beispiel: Medizintechnik

Herzschrittmacher von St. Jude Medical: Firmware-Patches gegen Sicherheitslücken

31.08.2017 15:17 Uhr – Olivia von Westernhagen vorlesen



Versierte Hacker können Herzschrittmacher der Marke Abbott angreifen, um Befehle auszuführen und Patientendaten zu stehlen. Implantatträgern wird ein baldiger Arztbesuch empfohlen, um wichtige Firmware-Updates zu installieren.

Quelle: https://www.heise.de/newsticker/meldung/Herzschrittmacher-von-St-Jude-Medical-Firmware-Patches-gegen-Sicherheitsluecken-3817954.html, 31.08.2017

Unsichere Software kann Leben gefährden
Beispiel: Industriesteuerungen

Cyberangriff in Saudi-Arabien hätte Explosion auslösen können – Ermittler sind alarmiert

Vor wenigen Monaten hat es in Saudi-Arabien angeblich einen Hackerangriff gegeben, der Menschen ihr Leben hätte kosten können. Dass es die angepeilte Explosion in einem Kraftwerk nicht gegeben hat, war einem Bericht zufolge nur glückliche Fügung.

Quelle: https://www.heise.de/newsticker/meldung/Saudi-Arabien-Cyberangriff-haette-Explosion-ausloesen-koennen-Ermittler-sind-alarmiert-3996010.html, 15.03.2018.

Das Thema Sicherheit wird zunehmend reguliert…
Beispiele KRITIS, IEC 62443, DSGVO

Verordnete Sicherheit

Neue gesetzliche Anforderungen an den Schutz kritischer Infrastrukturen

WISSEN | RECHT

Joerg Heidrich 19.08.2016

BSI, IT-Sicherheit, IT-Sicherheitsgesetz, KRITIS, Kritische

Nachdem Deutschland mit seinem IT-Sicherheits vorausgegangen war, hat nun die EU eine Richtli verabschiedet. Die neuen Regelungen stellen Be hierzulande vor erhebliche Herausforderungen.

Quelle: https://www.heise.de/ct/ausgabe/2016-18-Ne kritischer-Infrastrukturen-3293714.html

HOME / IEC-NORMEN / IEC 62443-4-1:2018

größer

IEC 62443-4-1:2018

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

Ausgabedatum: **2018-01**

Edition: **1.0**

Sprache: **EN**

Seitenzahl:

Inhaltsve

Quelle: https://www.vde-verlag.de/ie

PASSWÖRTER GELEAKT

Datenschützer prüft Sanktionen gegen Knuddels

Das Datenleck beim Chatanbieter Knuddels ruft nun auch die Aufsichtsbehörden auf den Plan. Nach der Datenschutz-Grundverordnung sind hohe Bußgelder möglich.

11. September 2018, 10:22 Uhr, Friedhelm Greis

Quelle: https://www.golem.de/news/passwoerter-geleakt-datenschuetzer-prueft-sanktionen-gegen-knuddels-1809-136501.html

HEINZ NIXDORF INSTITUT UNIVERSITÄT PADERBORN Fraunhofer IEM

Schwerpunkt des Vortrags heute:
„Software von Anfang an sicher entwickeln“

Security = Angriffs-

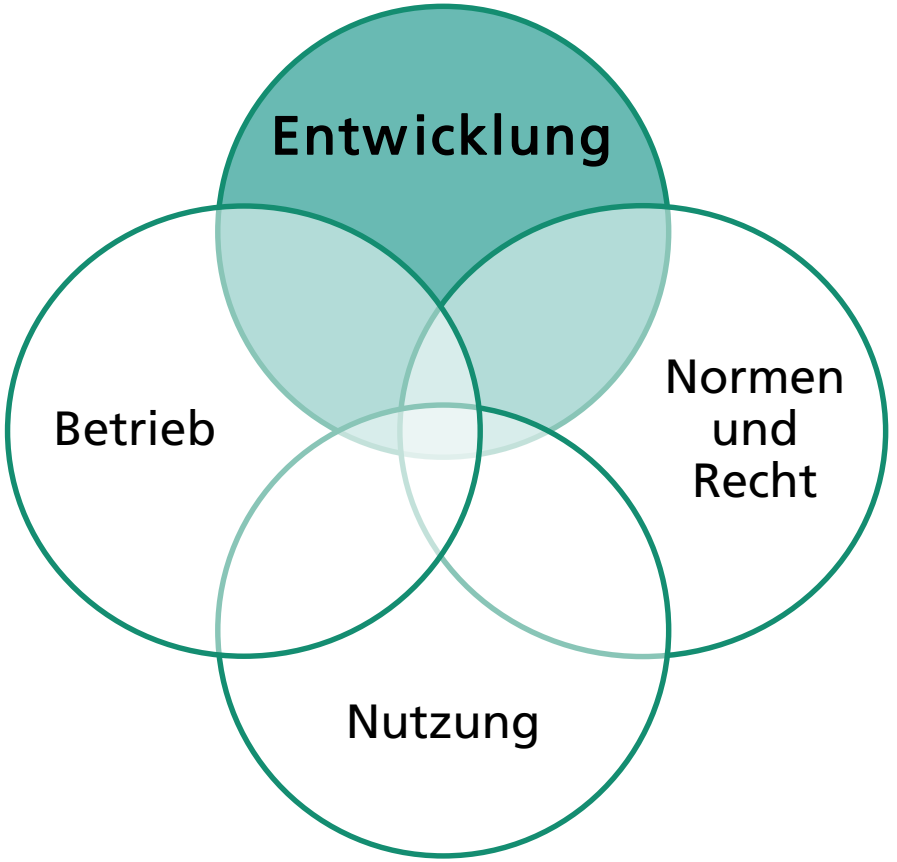
Safety = Betriebs-

Sicherheit

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Schwerpunkt des Vortrags heute:
„Software von Anfang an sicher entwickeln“

„BSI Grundschutz“, „ISO/IEC 27001“, „Backups“, „Intrusion Detection“



„DSGVO“, „KRITIS“, „Haftungsrecht“

„Social Engineering“, „Phishing“

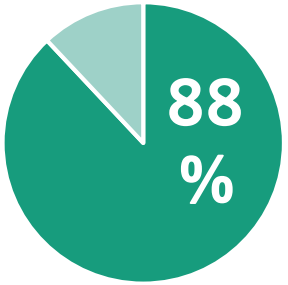
HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Warum ist sichere Software ein wichtiges Thema?

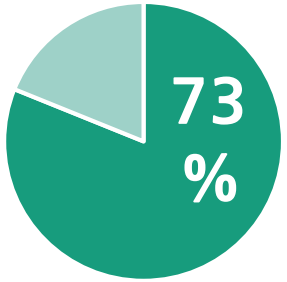
Warum ist sichere Software-Entwicklung ein wichtiges Thema?

Warum ist sichere Software-Entwicklung ein wichtiges Thema?

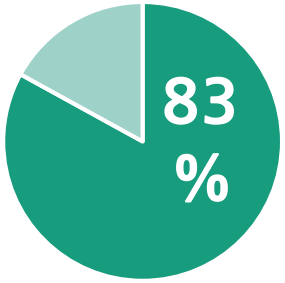
Größenordnungen am Beispiel „Security-Lücken durch falsche Nutzung von Krypto-Bibliotheken“



der Android-Apps mit mindestens einer Krypto-Fehlbenutzung[1]



der 2,7 Mio. Artefakte in Maven Central benutzen Java-Standard-Krypto-Bibliothek falsch[3]



der Kryptographie-bezogenen Lücken wegen Fehlbenutzung[2]

Selbst namhafte Anbieter benutzen TLS-Bibliotheken falsch[4]

[1] M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel. An empirical study of cryptographic misuse in android applications. CCS 2013.
[2] D. Lazar, H. Chen, X. Wang, and N. Zeldovich. Why does cryptographic software fail?: A case study and open problems. APSys 2014.
[3] S. Krüger, J. Spaeth, K. Ali, E. Bodden, M. Mezini. Large-Scale Study of Non-Trivial Misuses of the Java Cryptography Architecture. In Preparation
[4] S. Fahl, M. Harbach, T. Muders, M. Smith, L. Baumgärtner, B Freisleben. Why Eve and Mallory Love Android: An Analysis of SSL (In)Security. CCS 2012.

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Was können wir für sichere Software-Entwicklung tun?

Was können wir für sichere Software-Entwicklung tun?

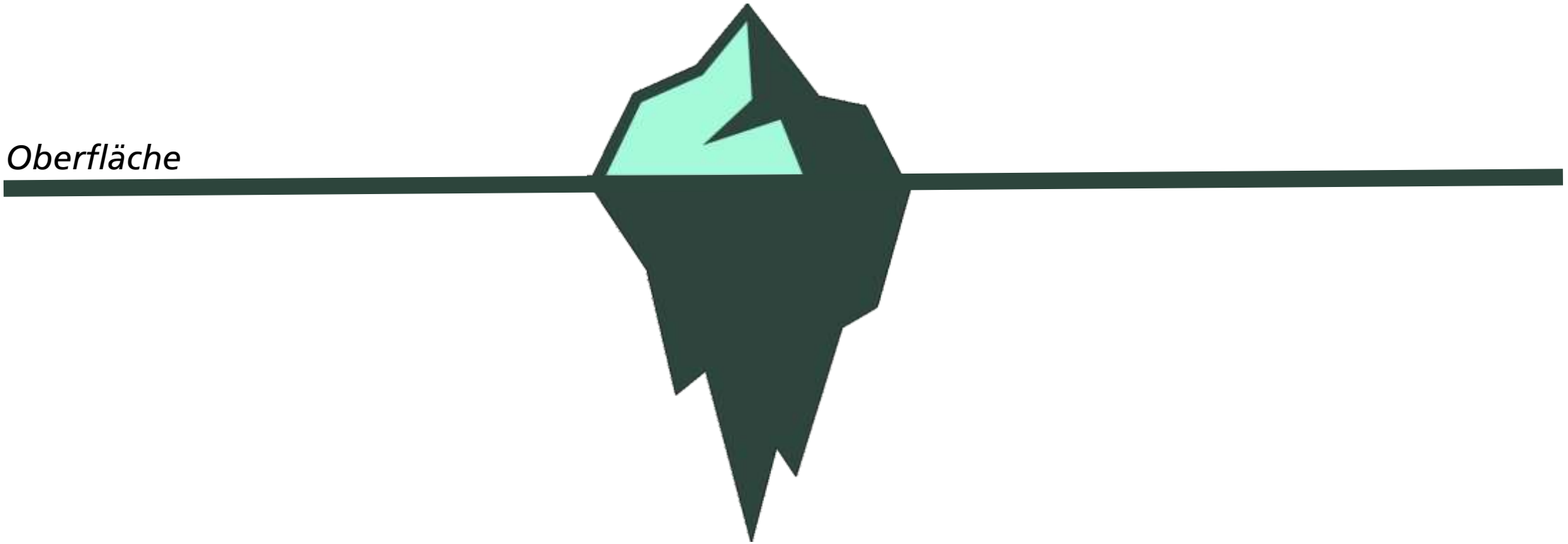
Penetrations-Tests!

Was können wir für sichere Software-Entwicklung tun?

Penetrations-Tests!?

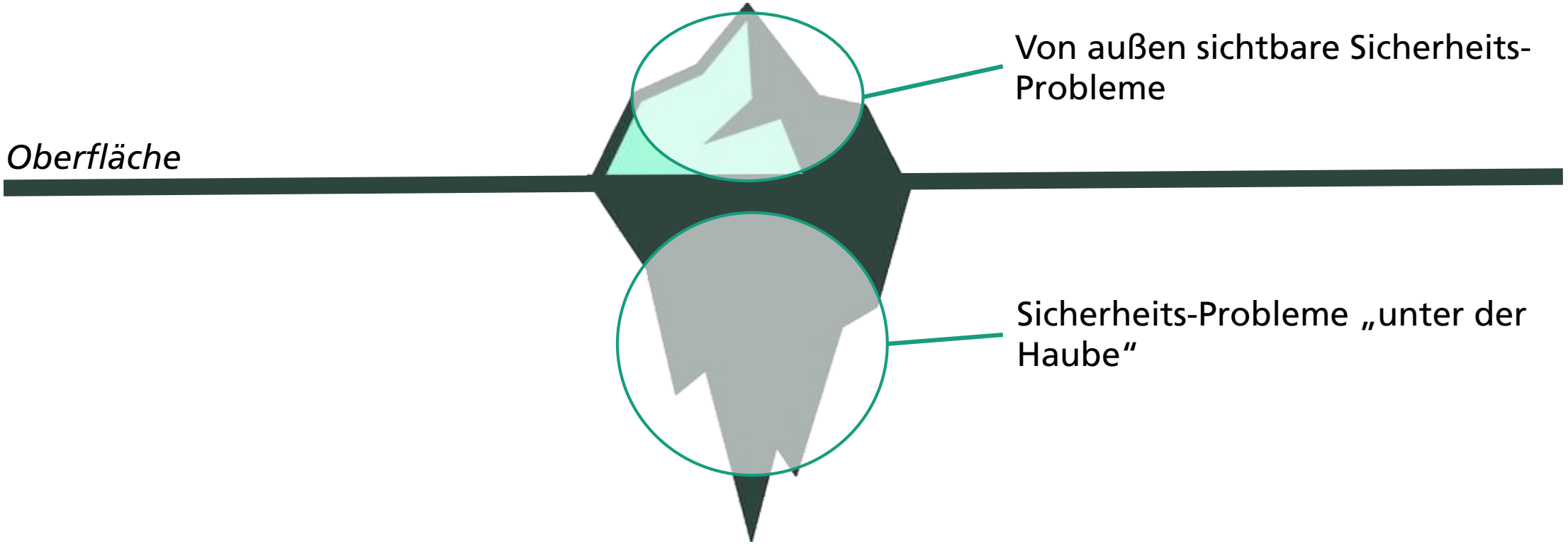
Warum Penetrations-Tests nicht ausreichen…

Tests können nur Probleme nachweisen – nicht deren Abwesenheit



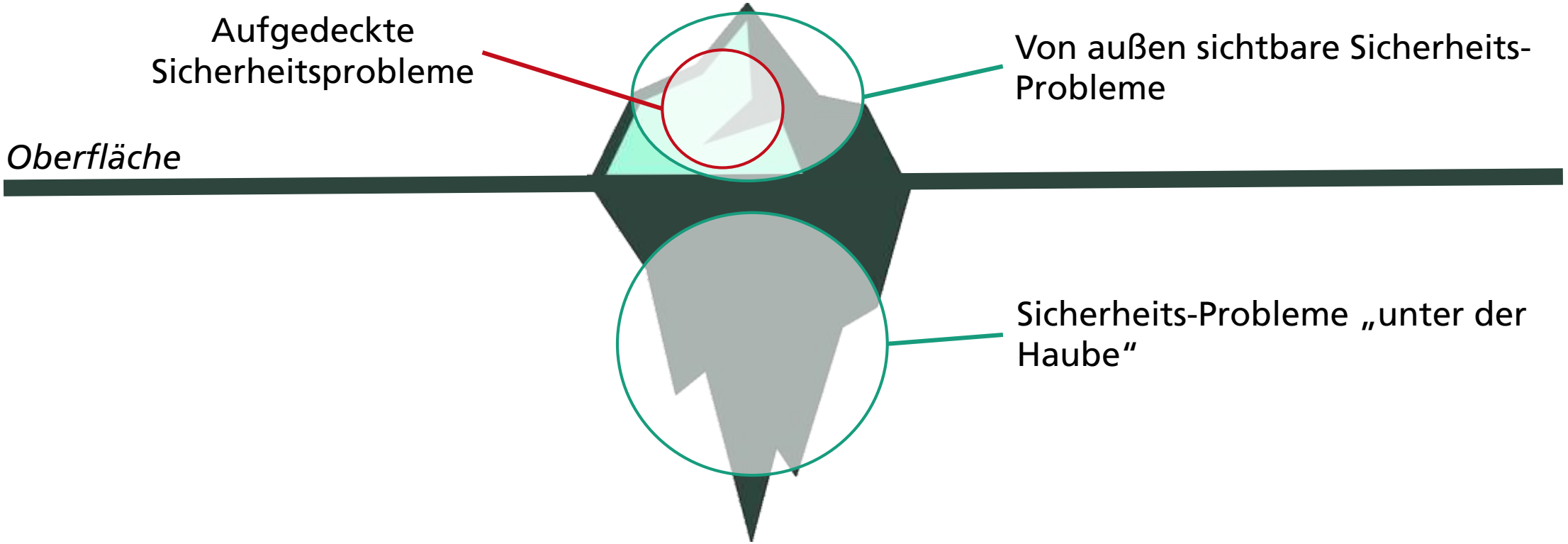
Warum Penetrations-Tests nicht ausreichen…

Tests können nur Probleme nachweisen – nicht deren Abwesenheit



Warum Penetrations-Tests nicht ausreichen…

Tests können nur Probleme nachweisen – nicht deren Abwesenheit



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Warum Penetrations-Tests nicht ausreichen…
Security lässt sich nicht nachträglich hineintesten

Fluggesellschaften

08.05.2012, 12:15 Uhr

Kein Plan B für Eröffnung in Schönefeld

Der Eröffnungstermin für den neuen Flughafen ist geplatzt. Noch vor zwei Wochen war das für die beiden Fluggesellschaften Lufthansa und Air Berlin undenkbar. VON KLAUS KURPJUWEIT

Der Start des neuen Flughafens verzögert sich nun doch. Die Fluggesellschaften haben keinen Plan. FOTO: DAPD

Quelle: https://www.tagesspiegel.de/berlin/fluggesellschaften-kein-plan-b-fuer-eroeffnung-in-schoenefeld/6555934.html

Warum Penetrations-Tests nicht ausreichen…

Security lässt sich nicht nachträglich hineintesten

Fluggesellschaften

08.05.2012, 12:15 Uhr

Kein Plan B für Eröffnung in Schönefeld

Der Eröffnungstermin für den neuen Flughafen ist geplatzt. Noch vor zwei Wochen war das für die beiden Fluggesellschaften Lufthansa und Air Berlin undenkbar. VON KLAUS KURPJUWEIT

Der Start des neuen Flughafens verzöger

Quelle: https://www.tagesspiegel.de/be
schoenefeld/6555934.html

UPDATE 17.01.2018 12:30 Uhr

Fataler Konstruktionsfehler im besonderen elektronischen Anwaltspostfach

Markus Drenger und Felix Rohrbach vom Chaos Darmstadt haben ihre Erkenntnisse zum beA am Dienstagabend an der TU Darmstadt erneut präsentiert. Und es sieht ganz danach aus, dass die Client-Software einen irreparablen Konstruktionsfehler hat.

von Volker Weber

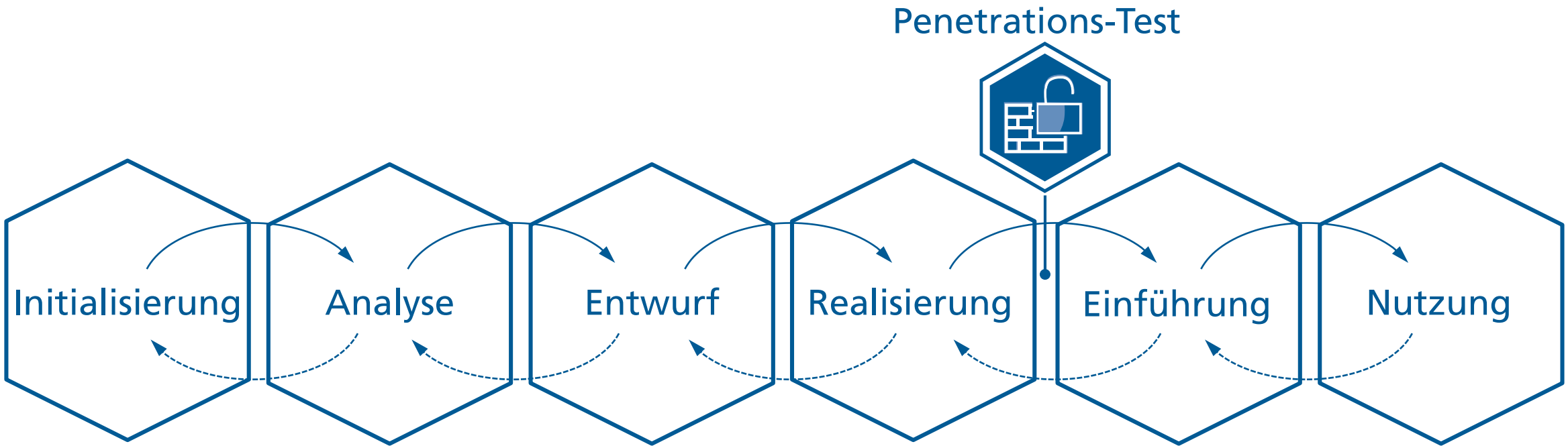
846

Quelle: https://www.heise.de/newsticker/meldung/Fataler-Konstruktionsfehler-im-besonderen-elektronischen-Anwaltspostfach-3944406.html

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Können wir mehr tun als Penetration Tests?

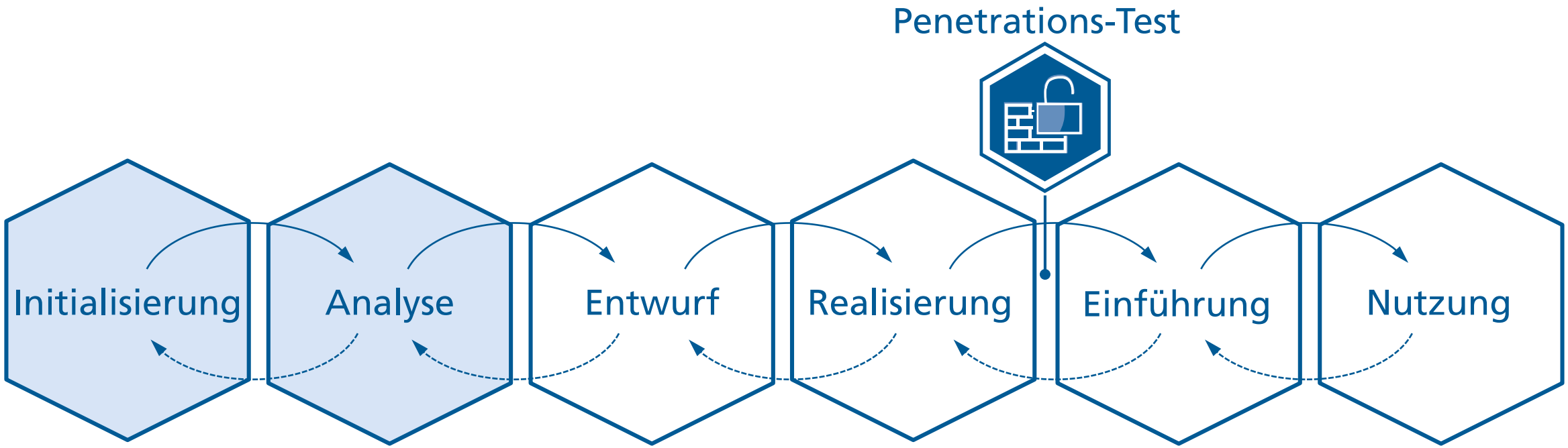
Security-by-Design: Security über den gesamten Prozess berücksichtigen



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Security-by-Design: Security über den gesamten Prozess berücksichtigen

Initialisierung & Analyse



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

„Was ist bedeutet Security für meine Anwendung?“
Security-Anforderungen systematisch ableiten

- Anforderungen an Security bleiben in der Praxis oft abstrakt:
  - *„Die Software soll sicher sein.“*
  - *„Die Anwendung soll nach dem Stand der Technik abgesichert sein.“*

„Was ist bedeutet Security für meine Anwendung?“
Security-Anforderungen systematisch ableiten

- Anforderungen an Security bleiben in der Praxis oft abstrakt:
  - *„Die Software soll sicher sein“*
  - *„Die Anwendung soll nach dem Stand der Technik abgesichert sein“*

- Security ist relativ:

„Wenn er auf seinem Laptop das Passwort eingebe, ziehe er ein grosses, rotes Tuch über den Kopf und den Laptop, damit das Passwort nicht von versteckten Kameras erfasst werden könne, erzählt er.“

Quelle: https://www.20min.ch/ausland/news/story/28603849, 10.06.2013

„Was ist bedeutet Security für meine Anwendung?“
Security-Anforderungen systematisch ableiten

- Anforderungen an Security bleiben in der Praxis oft abstrakt:
  - *„Die Software soll sicher sein“*
  - *„Die Anwendung soll nach dem Stand der Technik abgesichert sein“*

- Security ist relativ:

„Wenn er auf seinem Laptop das Passwort eingebe, ziehe er ein grosses, rotes Tuch über den Kopf und den Laptop, damit das Passwort nicht von versteckten Kameras erfasst werden könne, erzählt er.“

Quelle: https://www.20min.ch/ausland/news/story/28603849, 10.06.2013

Überzogen?

„Was ist bedeutet Security für meine Anwendung?“
Security-Anforderungen systematisch ableiten

- Anforderungen an Security bleiben in der Praxis oft abstrakt:
  - *„Die Software soll sicher sein“*
  - *„Die Anwendung soll nach dem Stand der Technik abgesichert sein“*

- Security ist relativ:

„Wenn er auf seinem Laptop das Passwort eingebe, ziehe er ein grosses, rotes Tuch über den Kopf und den Laptop, damit das Passwort nicht von versteckten Kameras erfasst werden könne, erzählt er.“

Quelle: https://www.20min.ch/ausland/news/story/28603849, 10.06.2013

„Was ist bedeutet Security für meine Anwendung?“
Security-Anforderungen systematisch ableiten

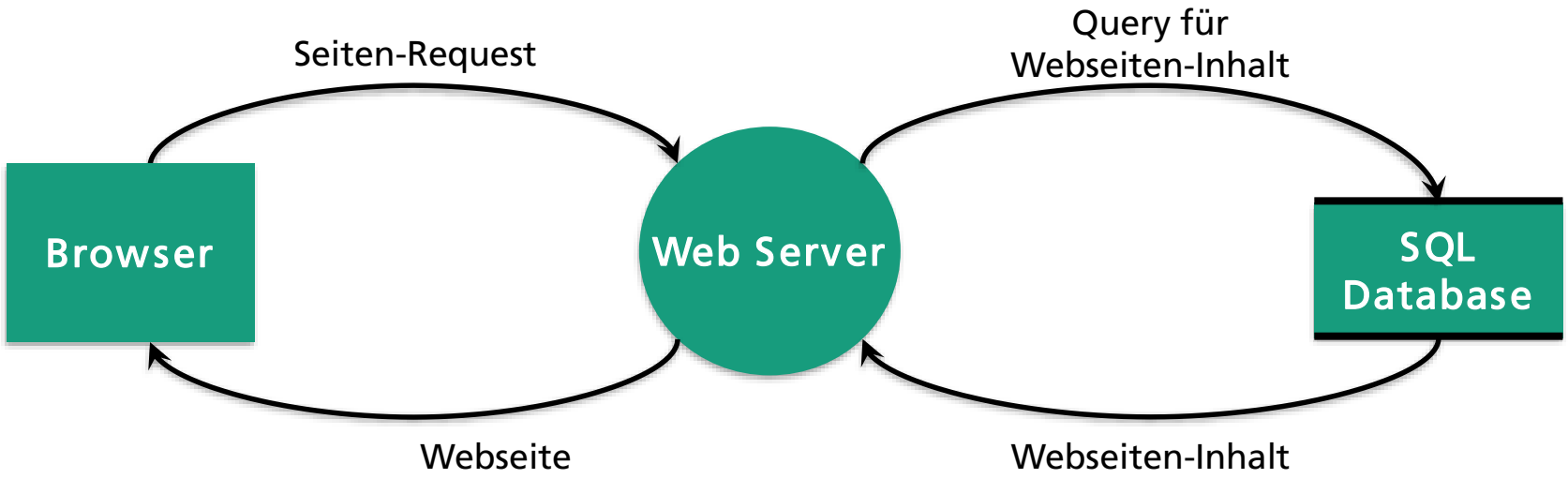
- Anforderungen an Security bleiben in der Praxis oft abstrakt:
  - *„Die Software soll sicher sein“*
  - *„Die Anwendung soll nach dem Stand der Technik abgesichert sein“*

- Security ist relativ:

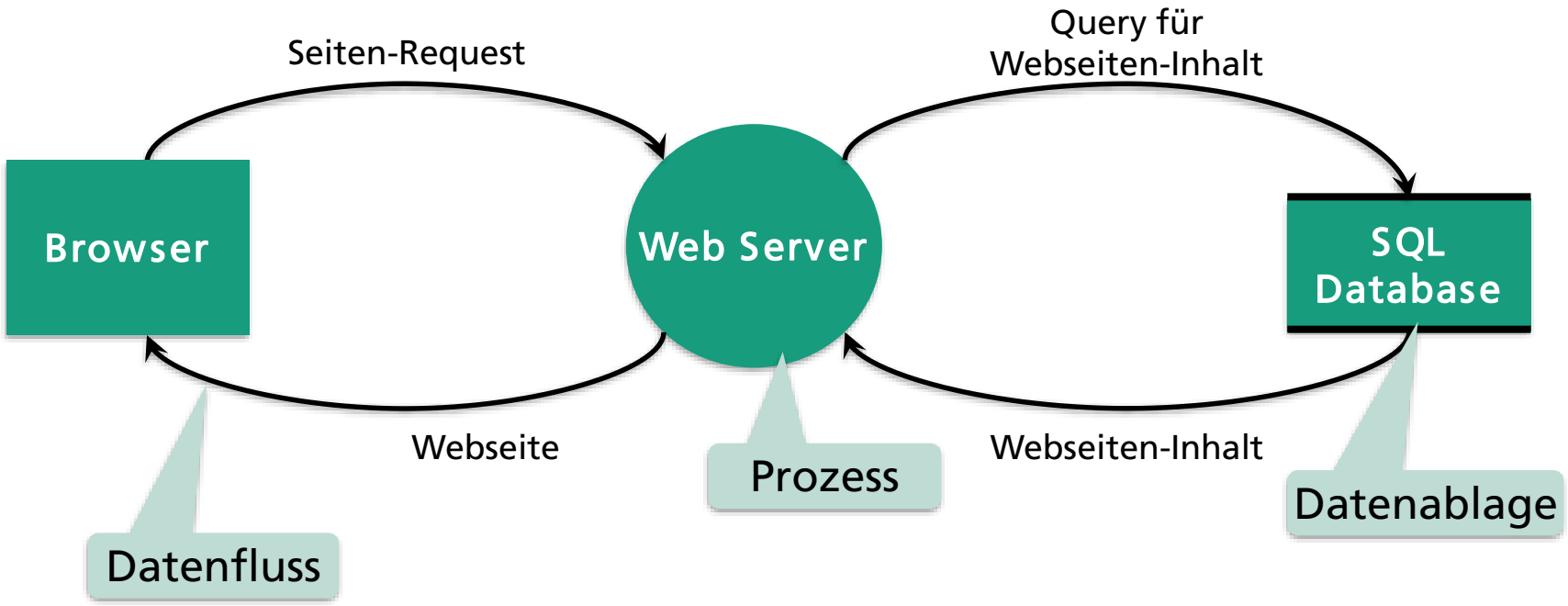
> „Wenn er auf seinem Laptop das Passwort eingebe, ziehe er ein grosses, rotes Tuch über den Kopf und den Laptop, damit das Passwort nicht von versteckten Kameras erfasst werden könne, erzählt er.“
>
> Quelle: https://www.20min.ch/ausland/news/story/28603849, 10.06.2013

- Notwendige Security ergibt sich aus Lagebericht:
  - Schutzbedürftigen Assets
  - Potentiellen Gefahren / Wer könnte mich wie angreifen?

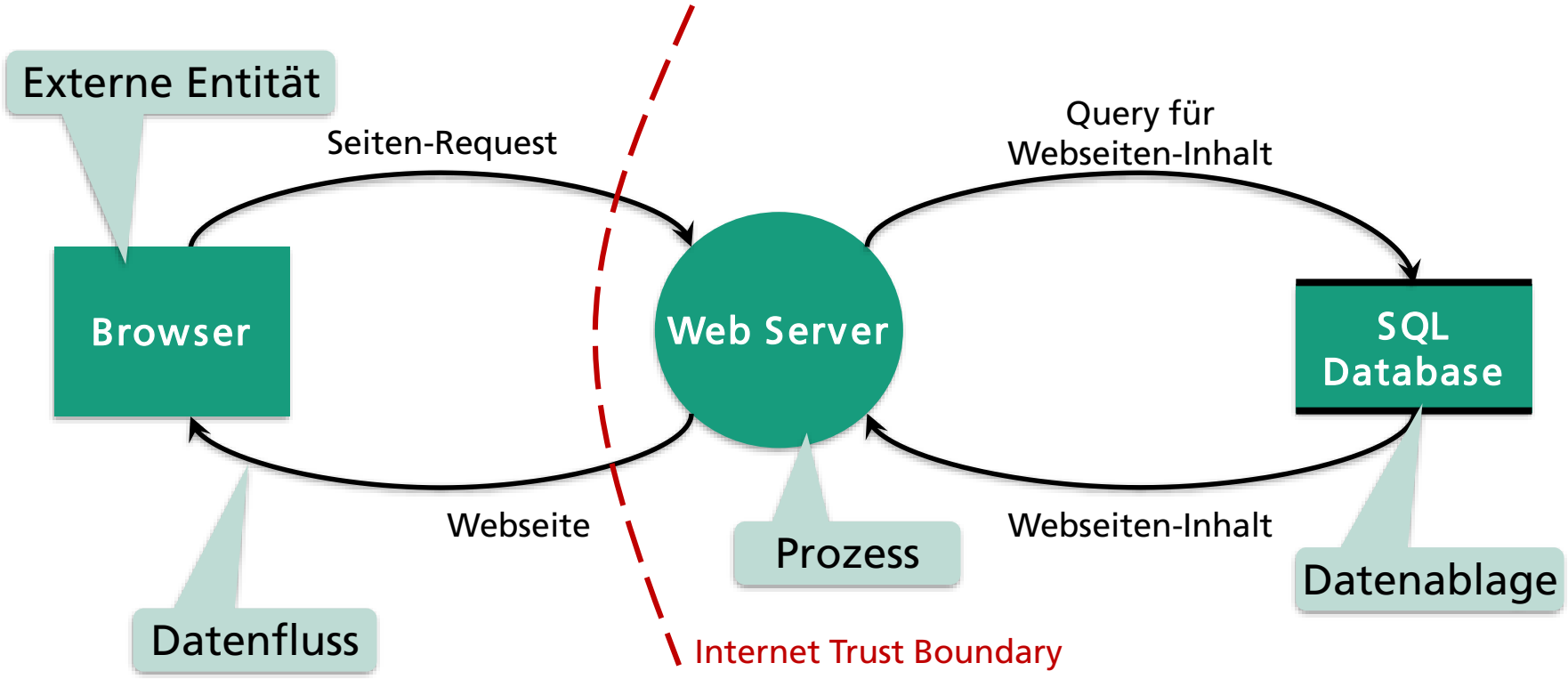
Bedrohungsanalyse
Systemmodellierung und Identifikation von Assets



Bedrohungsanalyse
Systemmodellierung und Identifikation von Assets

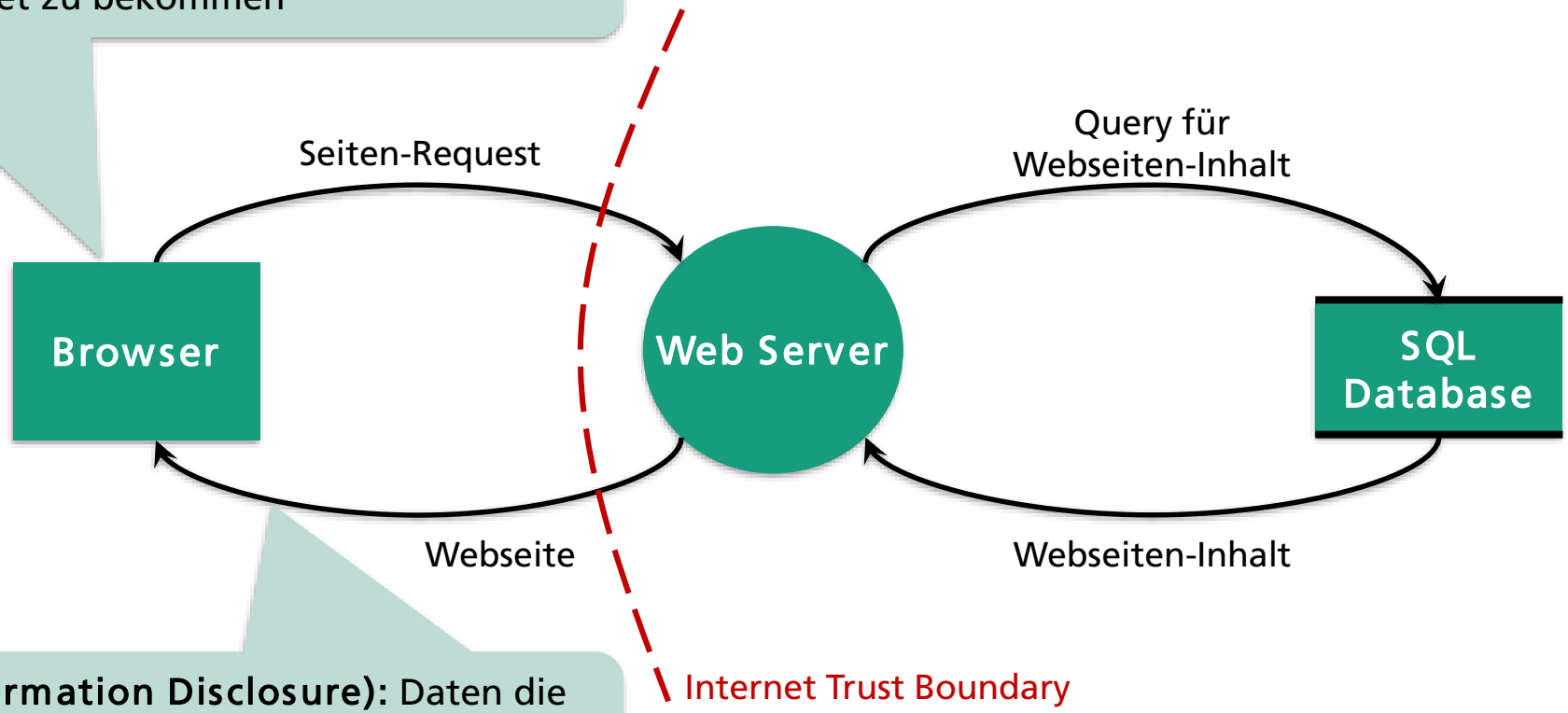


Bedrohungsanalyse
Systemmodellierung und Identifikation von Assets



Bedrohungsanalyse
Identifikation möglichen Gefahren und Schutzzielen

Gefahr 1 (Spoofing): Angreifer könnte sich als "Browser" ausgeben um Daten vom "Web Server" gesendet zu bekommen



Gefahr 2 (Information Disclosure): Daten die vom "Web Server" an "Browser" verschickt werden könnten abgehört werden

Gefahrenklassen (STRIDE)

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

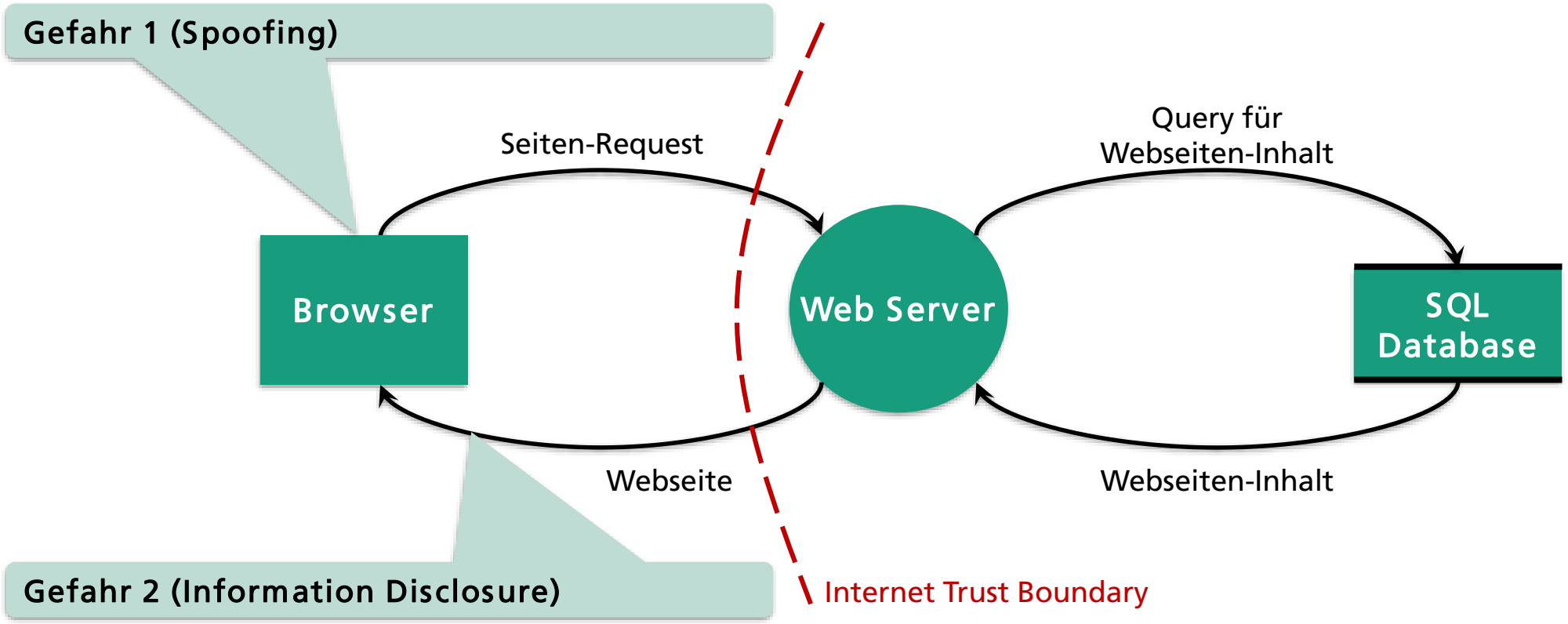
Elevation of Privilege

Bedrohungsanalyse
Identifikation möglichen Gefahren und Schutzzielen

Gefahrenklassen (STRIDE)	Schutzziele
Spoofing	**Authentizität** der Kommunikationspartner
Tampering	**Integrität** übermittelter / gespeicherter Daten
Repudiation	**Auditierbarkeit** empfangener / gesendeter Daten
Information Disclosure	**Vertraulichkeit** übermittelter / gespeicherter Daten
Denial of Service	**Verfügbarkeit** der Kommunikationskanäle und -Partner
Elevation of Privilege	**Autorisierung** der Kommunikationspartner

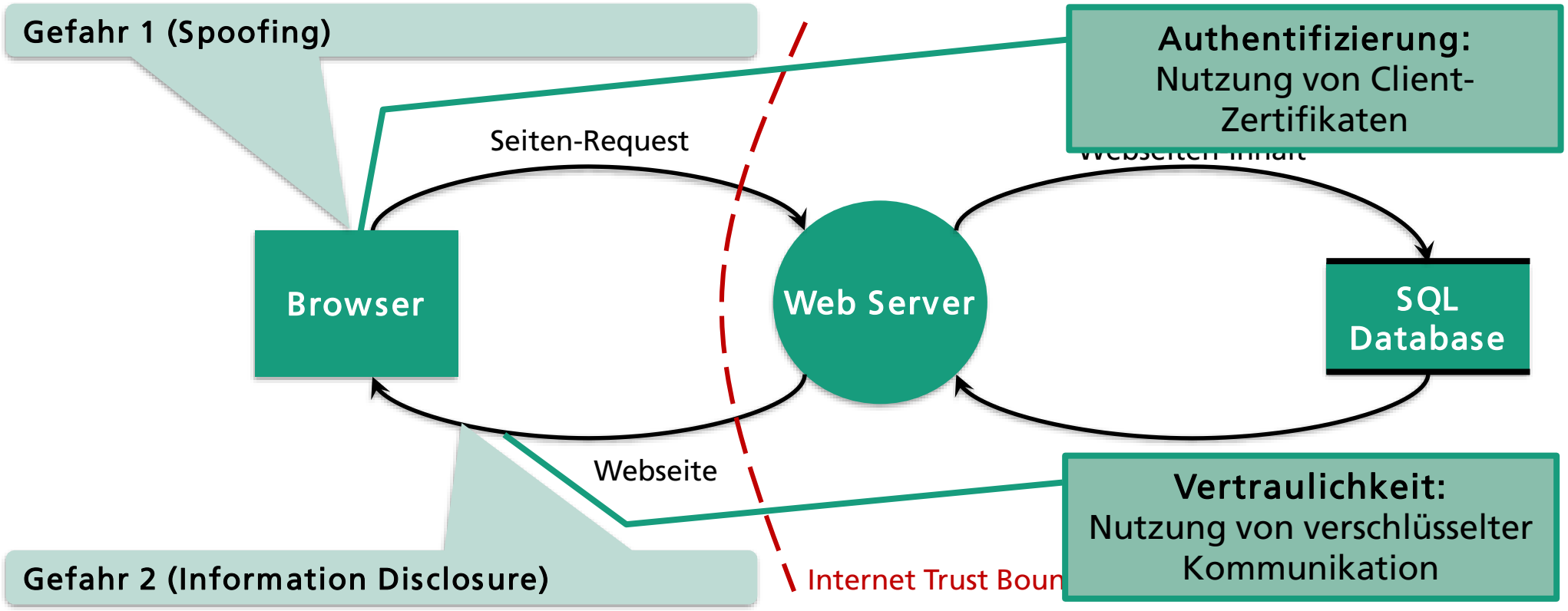
HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Bedrohungsanalyse
Identifikation von Schutzzielen und notwendigen Gegenmaßnahmen



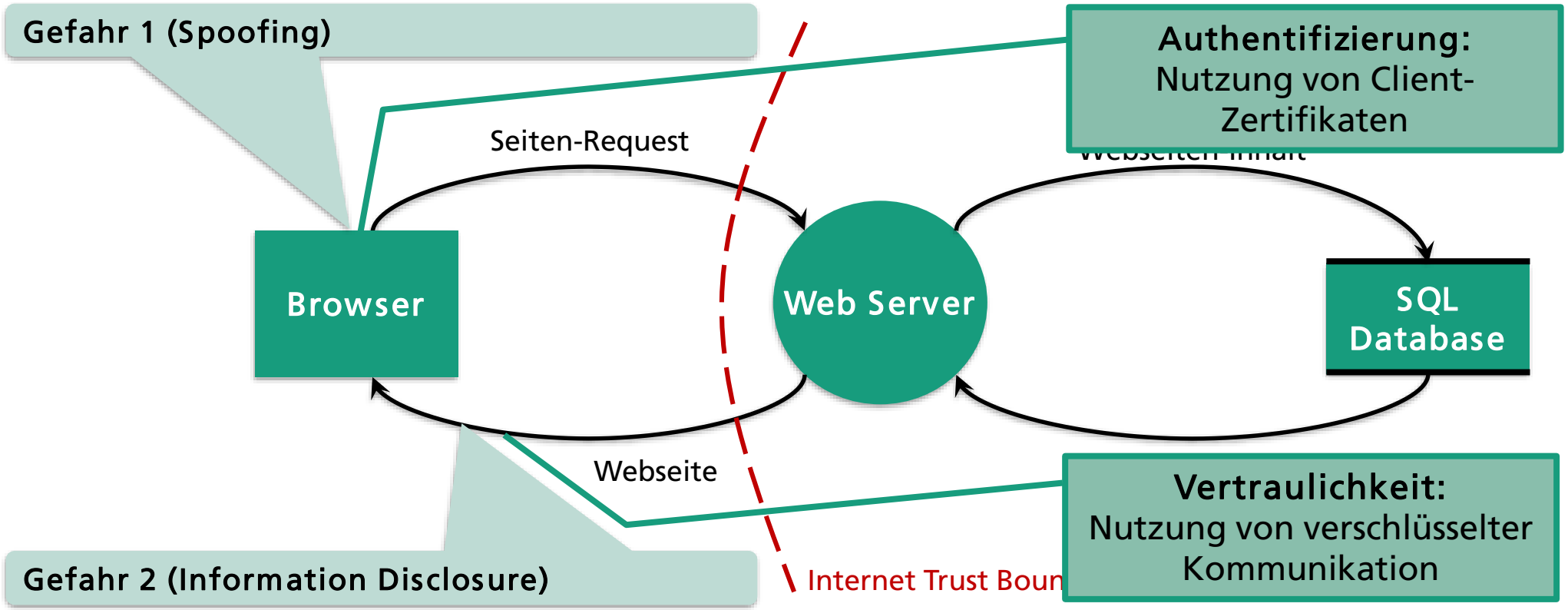
HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer
IEM

Bedrohungsanalyse
Identifikation von Schutzzielen und notwendigen Gegenmaßnahmen



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

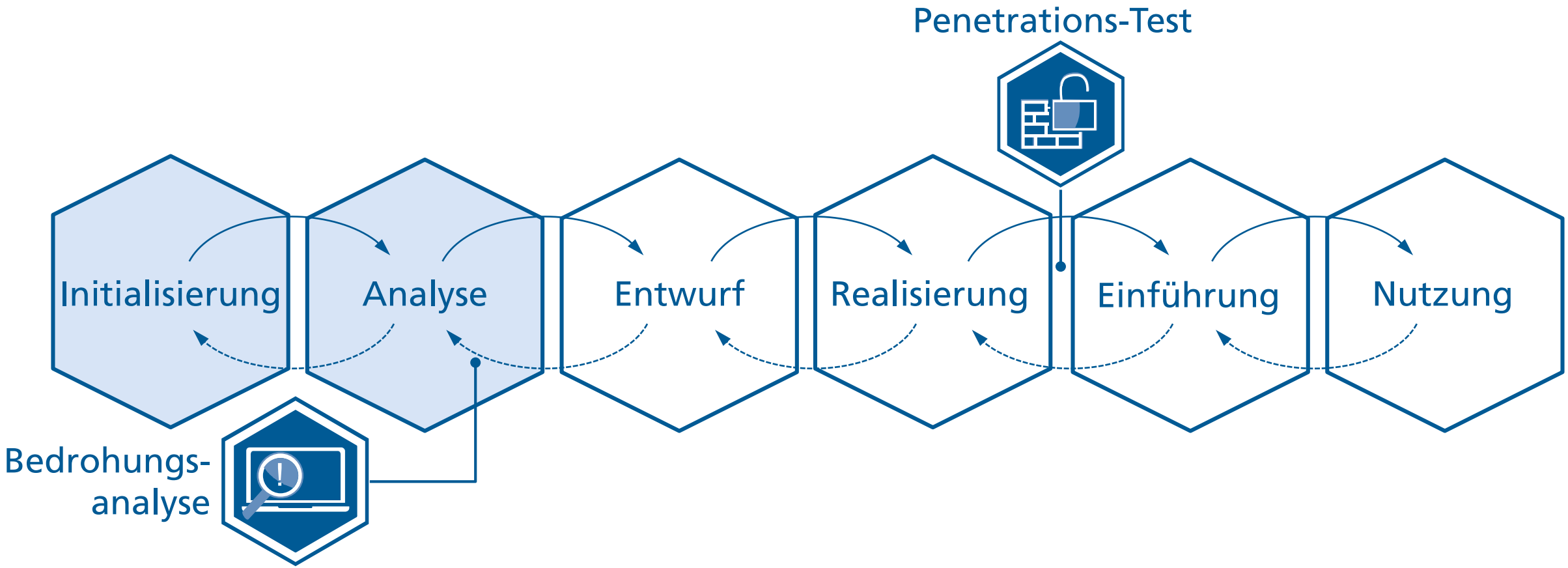
Bedrohungsanalyse
Identifikation von Schutzzielen und notwendigen Gegenmaßnahmen



Also: Mit Bedrohungsanalyse einen „Lagebericht Security“ erstellen

Security-by-Design: Security über den gesamten Prozess berücksichtigen

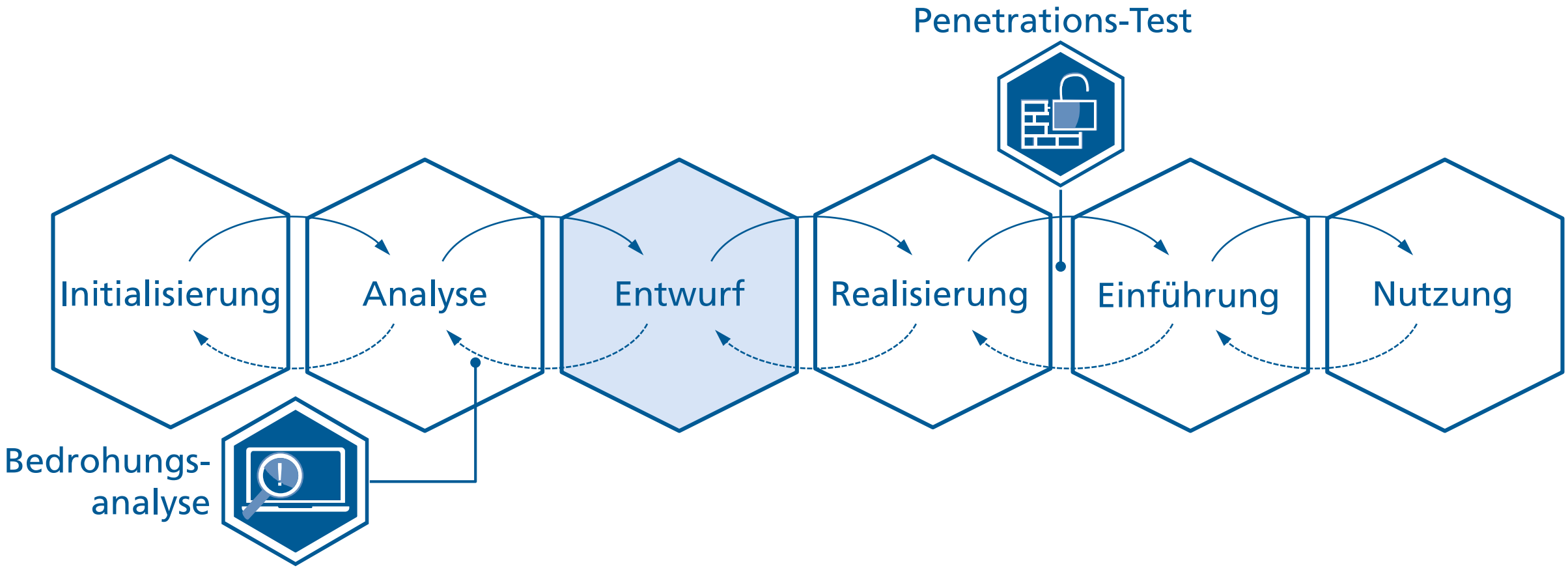
Initialisierung & Analyse



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Security-by-Design: Security über den gesamten Prozess berücksichtigen

Entwurf



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sichere Architektur

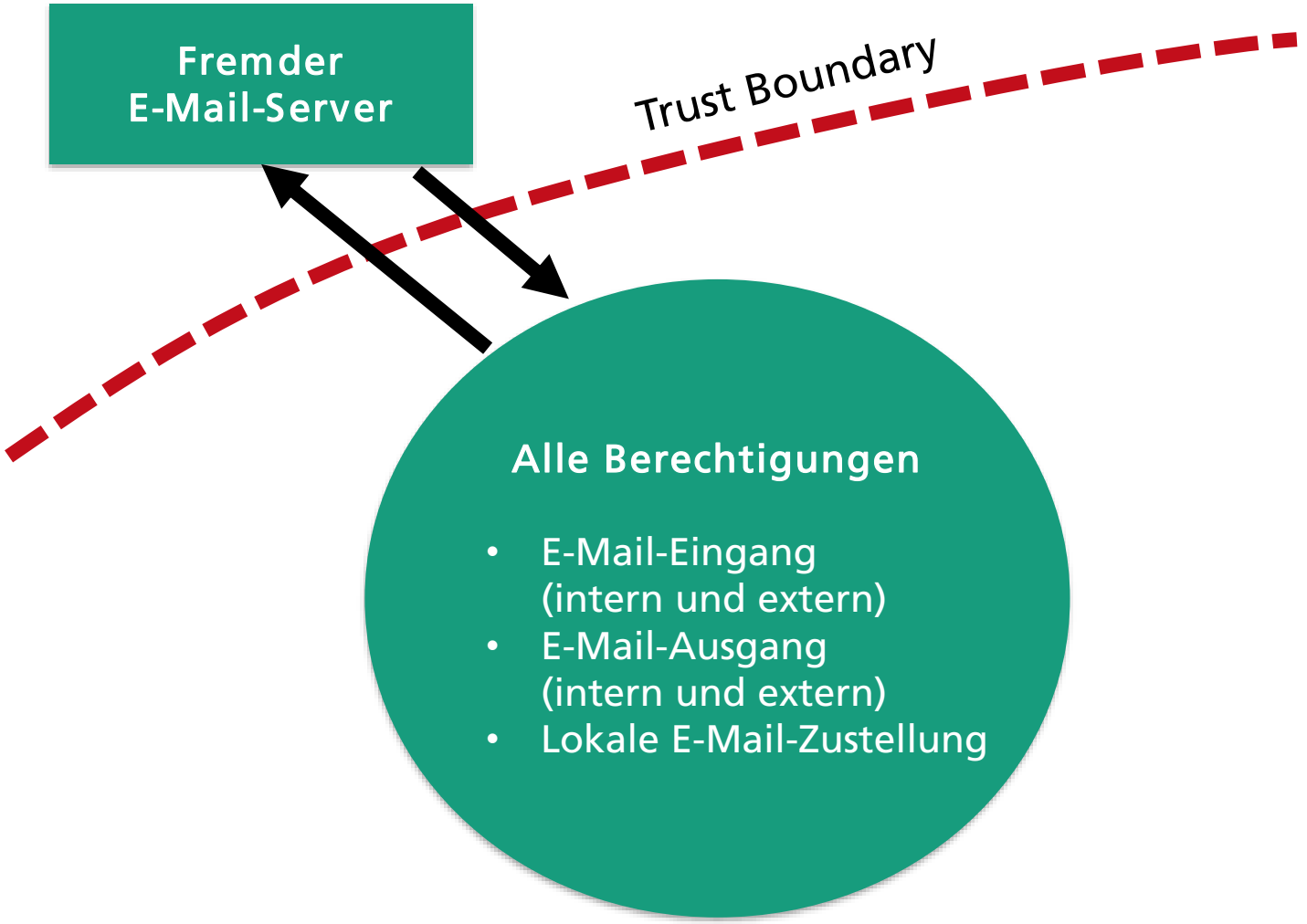
Was hat die Architektur von Sendmail mit Sicherheit zu tun?

Bulletin	Software	Vulnerability
CA-1988-01	Sendmail 5.58	run any command
CA-1990-01	SUN Sendmail	unknown
CA-1991-01	SUN /bin/mail	root shell
CA-1991-13	Ultrix /bin/mail	root shell
CA-1993-15	SUN Sendmail	write any file
CA-1993-16	Sendmail 8.6.3	run any command
CA-1994-12	Sendmail 8.6.7	root shell, r/w any file
CA-1995-02	/bin/mail	write any file
CA-1995-05	Sendmail 8.6.9	any command, any file
CA-1995-08	Sendmail V5	any command, any file
CA-1995-11	SUN Sendmail	root shell
CA-1996-04	Sendmail 8.7.3	root shell
CA-1996-20	Sendmail 8.7.5	root shell, default uid
CA-1996-24	Sendmail 8.8.2	root shell
CA-1996-25	Sendmail 8.8.3	group id
CA-1997-05	Sendmail 8.8.4	root shell
CA-2003-07	Sendmail 8.12.7	remote root privilege
CA-2003-12	Sendmail 8.12.8	remote root privilege
CA-2003-25	Sendmail 8.12.9	remote root privilege

Sichere Architektur

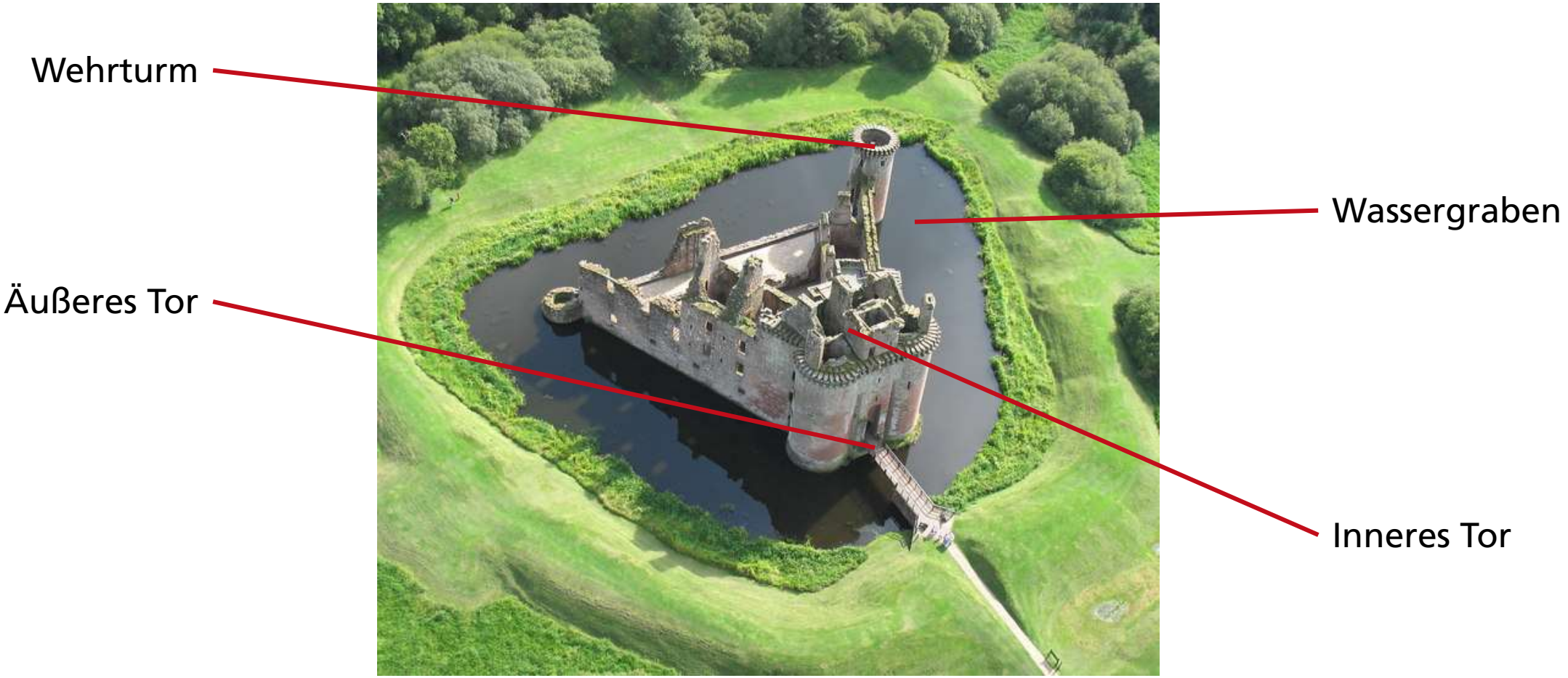
Was hat die Architektur von Sendmail mit Sicherheit zu tun?

Bulletin	Software	Vulnerability
CA-1988-01	Sendmail 5.58	run any command
CA-1990-01	SUN Sendmail	unknown
CA-1991-01	SUN /bin/mail	root shell
CA-1991-13	Ultrix /bin/mail	root shell
CA-1993-15	SUN Sendmail	write any file
CA-1993-16	Sendmail 8.6.3	run any command
CA-1994-12	Sendmail 8.6.7	root shell, r/w any file
CA-1995-02	/bin/mail	write any file
CA-1995-05	Sendmail 8.6.9	any command, any file
CA-1995-08	Sendmail V5	any command, any file
CA-1995-11	SUN Sendmail	root shell
CA-1996-04	Sendmail 8.7.3	root shell
CA-1996-20	Sendmail 8.7.5	root shell, default uid
CA-1996-24	Sendmail 8.8.2	root shell
CA-1996-25	Sendmail 8.8.3	group id
CA-1997-05	Sendmail 8.8.4	root shell
CA-2003-07	Sendmail 8.12.7	remote root privilege
CA-2003-12	Sendmail 8.12.8	remote root privilege
CA-2003-25	Sendmail 8.12.9	remote root privilege

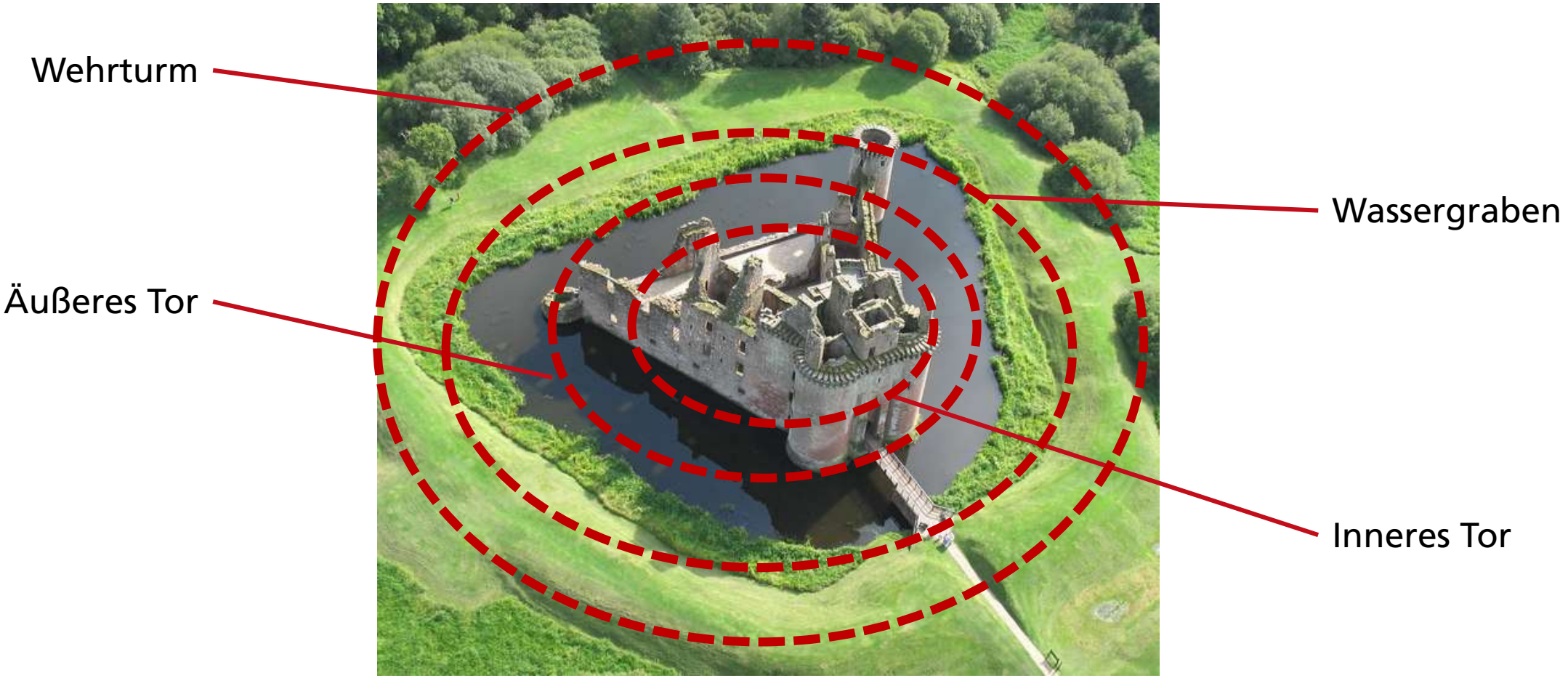


HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sichere Architektur
Defense in Depth



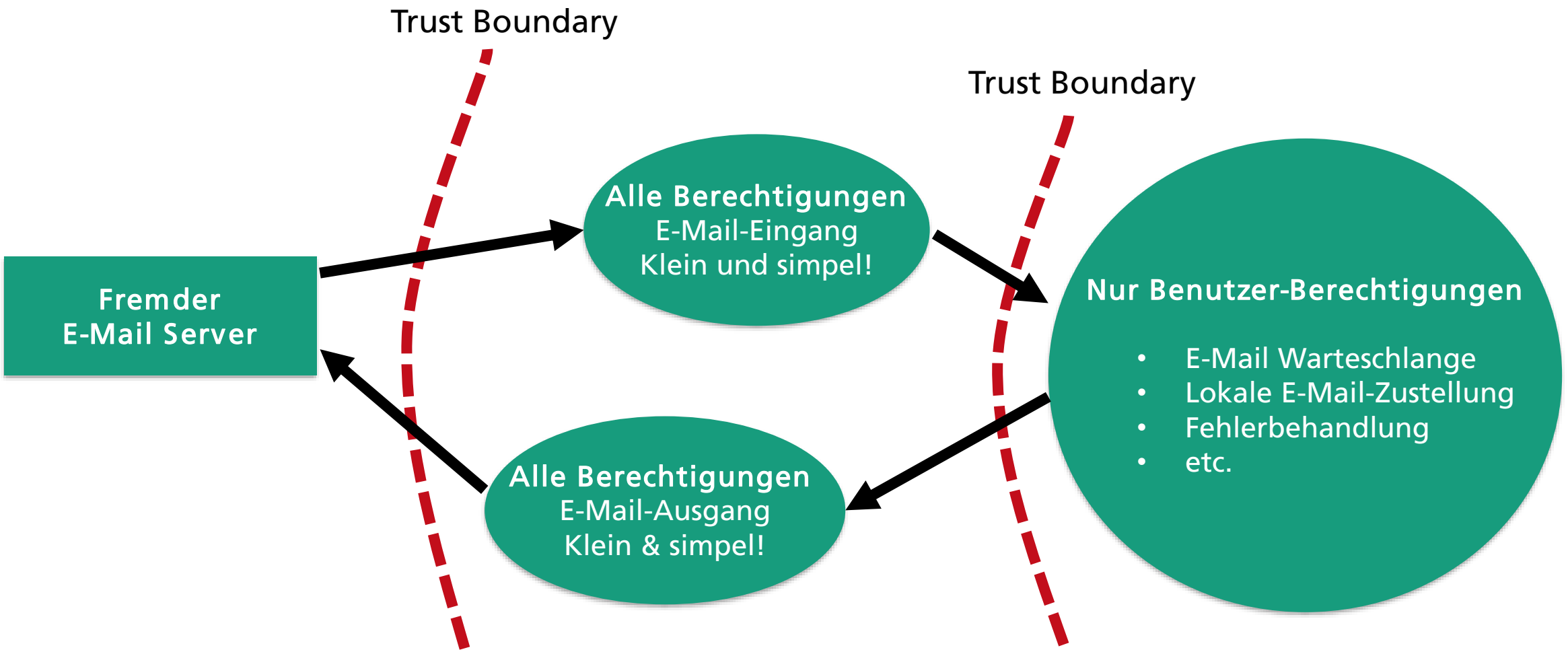
Sichere Architektur
Defense in Depth



Bildrechte: Simon Ledingham / *Caerlaverock Castle* / CC BY-SA 2.0

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sichere Architektur
Defense in Depth am Beispiel QMail



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

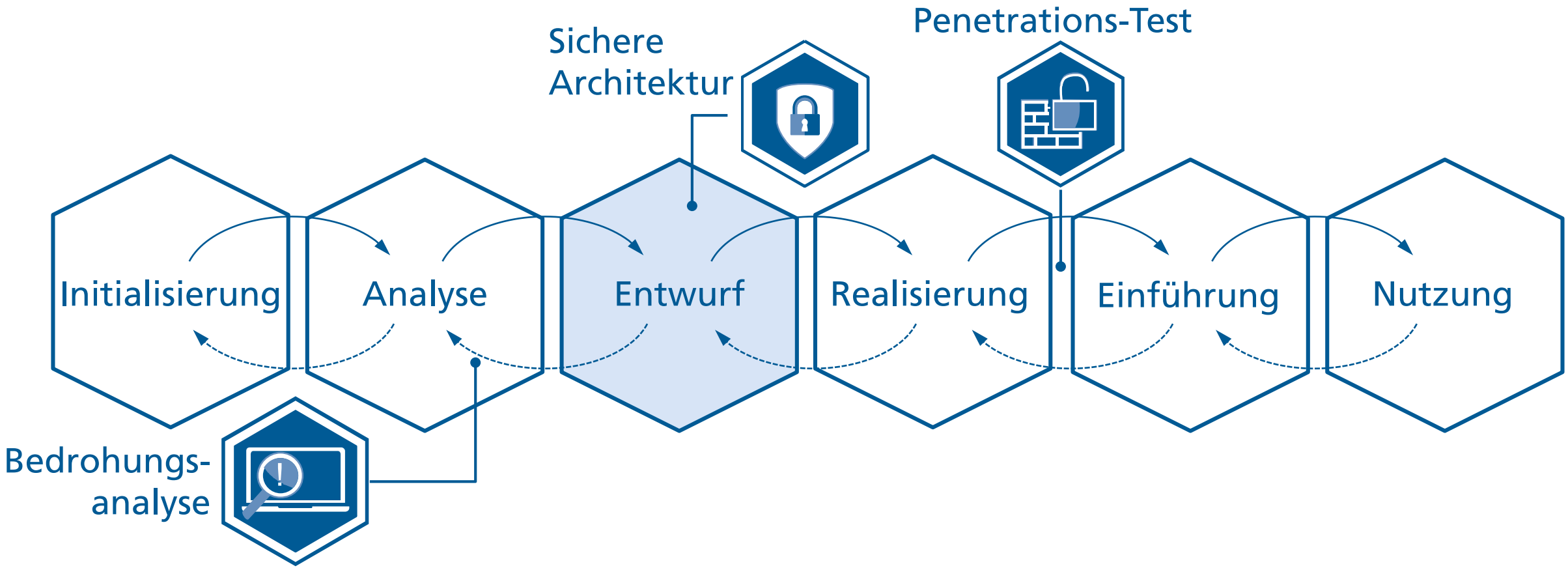
Sichere Architektur
Defense in Depth

- **Prinzip "Distrustful Decomposition"**
  - Schneiden der Software in Komponenten
  - Komponenten „trauen" sich gegenseitig nicht
    - Eingaben werden erneut geprüft
    - Autorisierung wird erneut geprüft
- **Prinzip "Least Privilege"**
  - Minimale Berechtigungen
  - Hohe Berechtigung → minimale Komplexität gefordert

Also: Bei der Software-Architektur gilt wie bei einer Burg „Defense in Depth"

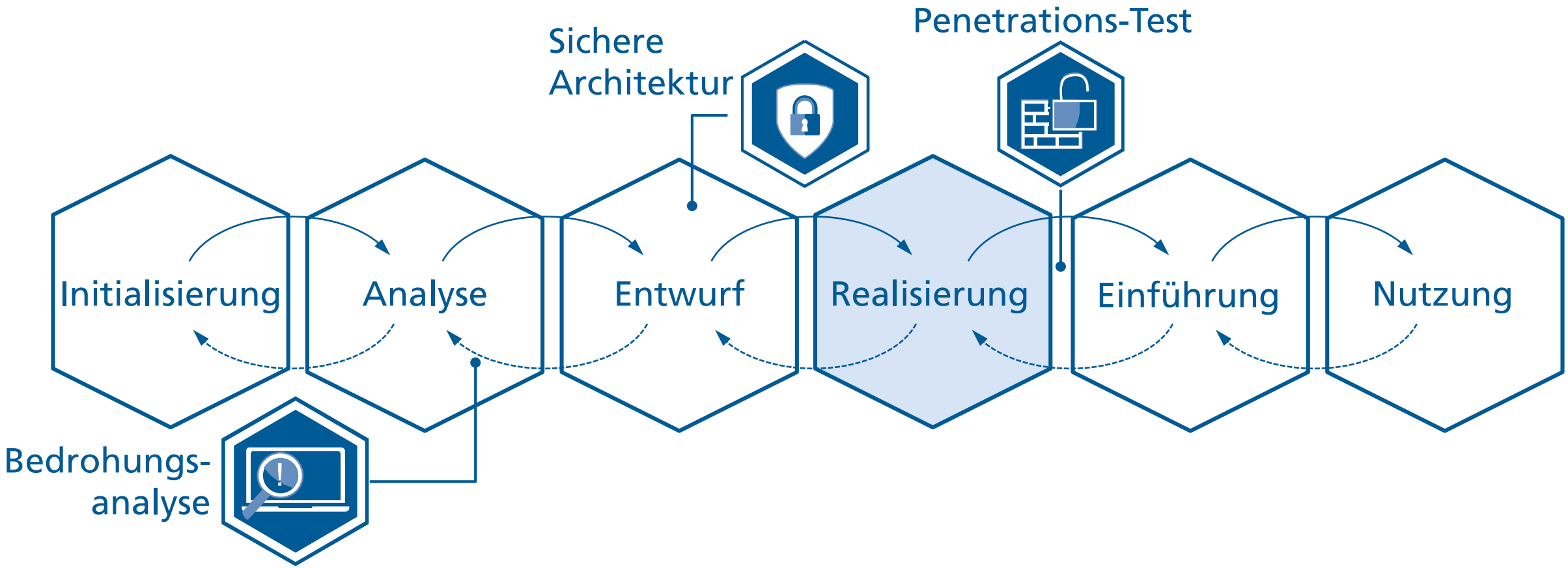
Security-by-Design: Security über den gesamten Prozess berücksichtigen

Entwurf



Security-by-Design: Security über den gesamten Prozess berücksichtigen

Realisierung



Realisierung
Häufige Schwachstellen

Jetzt patchen! SQL-Injection-Lücke bedroht WordPress

Alert! 01.11.2017 11:31 Uhr – Dennis Schirrmacher

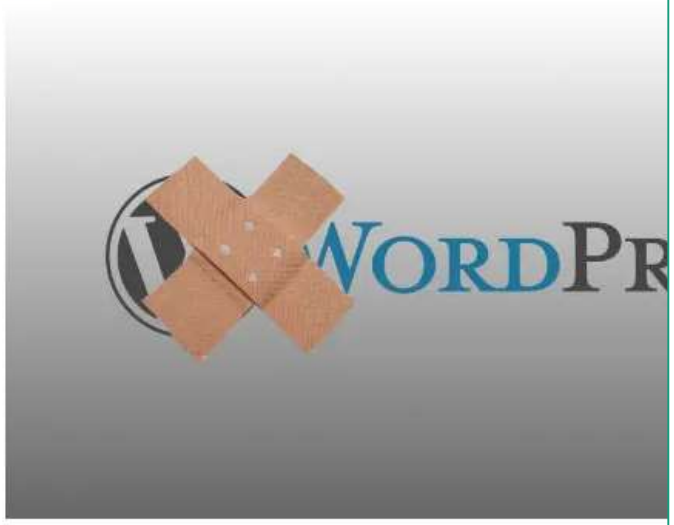
Die abgesicherte WordPress-Version 4.8.3 ist erschienen. Nutzer sollten diese zügig installieren, da Angreifer Webseiten via SQL-Injection-Attacke übernehmen könnten.

Quelle: https://www.heise.de/security/meldung/Jetzt-patchen-SQL-Injection-Luecke-bedroht-WordPress-3876623.html

Realisierung
Häufige Schwachstellen

Jetzt patchen! SQL-Injection-Lücke

Alert! 01.11.2017 11:31 Uhr – Dennis Schirrmacher

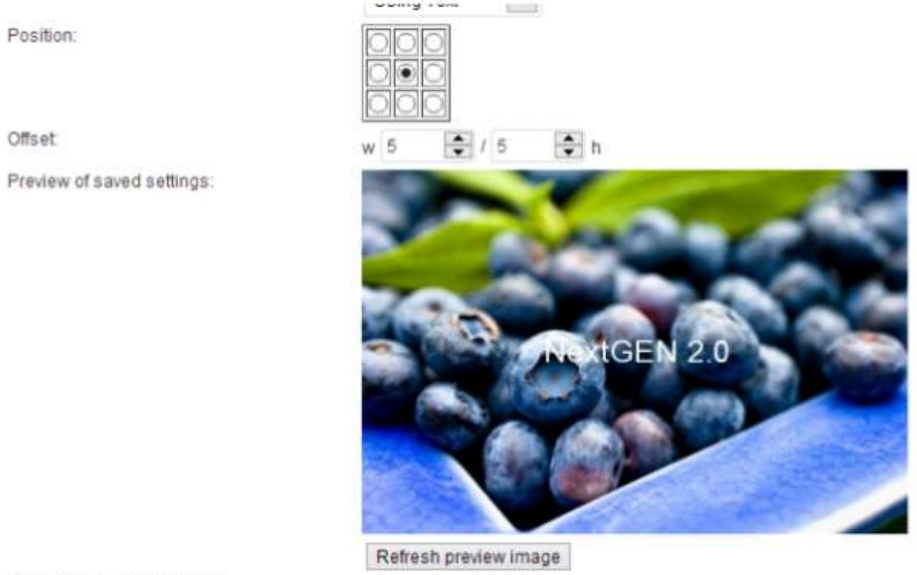


Die abgesicherte WordPress-Version 4.8.3 ist erschienen
installieren, da Angreifer Webseiten via SQL-Injection-Attacke übernehmen könnten.

Quelle: https://www.heise.de/security/meldung/Jetzt-patchen-SQL-Injection-Luecke-bedroht-WordPress-3876623.html

WordPress-Plug-in NextGEN Gallery kann sich an SQL-Anfragen verschlucken

Alert! 06.03.2017 14:41 Uhr – Dennis Schirrmacher



(Bild: WordPress)

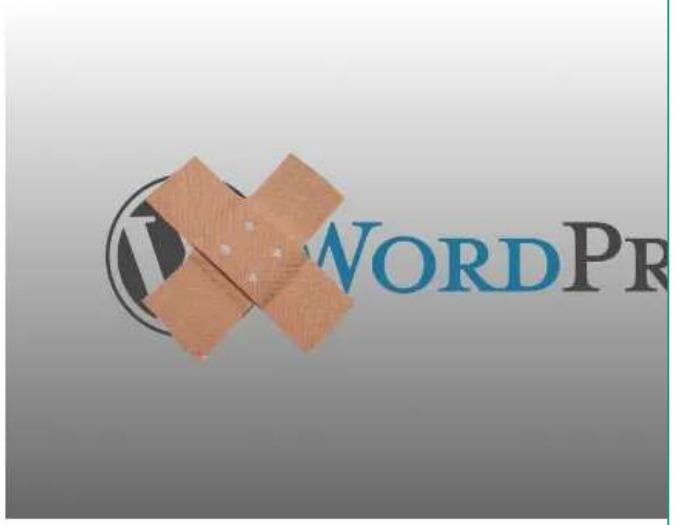
Unter gewissen Voraussetzungen können Angreifer mittels manipulierter SQL-Anfragen Nutzerdaten von WordPress-Webseiten abgreifen.

Quelle: https://www.heise.de/security/meldung/WordPress-Plug-in-NextGEN-Gallery-kann-sich-an-SQL-Anfragen-verschlucken-3645075.html

Realisierung
Häufige Schwachstellen

Jetzt patchen! SQL-Injection-Lücke l

Alert! 01.11.2017 11:31 Uhr – Dennis Schirrmacher

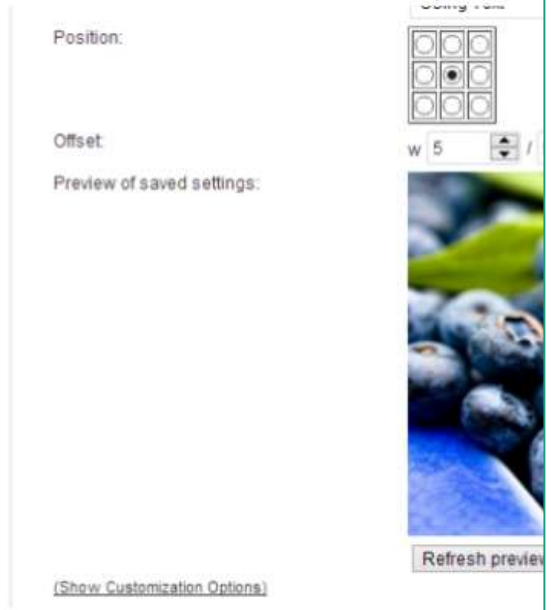


Die abgesicherte WordPress-Version 4.8.3 ist erschienen
installieren, da Angreifer Webseiten via SQL-Injection-Attacke übernehmen könnten.

Quelle: https://www.heise.de/security/meldung/Jetzt-patchen-SQL-Injection-Luecke-bedroht-WordPress-3876623.html

WordPress-Plug-in NextGEN Gallery kann sich an SQL-Anfragen verschlucken

Alert! 06.03.2017 14:41 Uhr – Dennis Schirrmacher



(Bild: WordPress)

Unter gewissen Voraussetzungen können Angr
Nutzerdaten von WordPress-Webseiten abgreif

Quelle: https://www.heise.de/security/meldung/WordPress-Plug-in-NextGEN-

Datenleck: 47.000 sensible Dokumente von Autobauern im Internet öffentlich

21.07.2018 12:29 Uhr

Was geht ab bei VW & Co.? Sensible Informationen vieler Autobauer fanden sich öffentlich im Netz – dank eines Datenlecks bei einem Dienstleister.

von Oliver Bünte 124

Quelle: https://www.heise.de/security/meldung/Spectre-NG-Intel-dokumentiert-spekulativen-Buffer-Overflow-4108008.html

Sichere Realisierung
Typische Schwachstellen und ihre etablierten Lösungen

- Open Web Application Security Project (OWASP)
  - Sammlung von Top-Bedrohungen / typischen Schwachstellen
  - Umfangreiche Dokumentation mit Abhilfe

A safe version of the above SQL statement could be coded in Java as:

```
String firstname = req.getParameter("firstname");
String lastname = req.getParameter("lastname");
// FIXME: do your own validation to detect attacks
String query = "SELECT id, firstname, lastname FROM authors WHERE forename = ? and surname
= ?";
PreparedStatement pstmt = connection.prepareStatement( query );
pstmt.setString( 1, firstname );
pstmt.setString( 2, lastname );
try
{
        ResultSet results = pstmt.execute( );
}
```

SQL Injection

This is an Attack. To view all attacks, please see the Attack Category page.

Last revision (mm/dd/yy): 04/10/2016

Overview

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Threat Modeling

- SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.
- SQL Injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. Due to the nature of programmatic interfaces available, J2EE and ASP.NET applications are less likely to have easily exploited SQL injections.
- The severity of SQL Injection attacks is limited by the attacker's skill and imagination, and to a lesser extent, defense in depth countermeasures, such as low privilege connections to the database server and so on. In general, consider SQL Injection a high impact severity.

Related Security Activities

How to Avoid SQL Injection Vulnerabilities

See the OWASP SQL Injection Prevention Cheat Sheet.
See the OWASP Query Parameterization Cheat Sheet.
See the OWASP Guide article on how to Avoid SQL Injection Vulnerabilities.

How to Review Code for SQL Injection Vulnerabilities

See the OWASP Code Review Guide article on how to Review Code for SQL Injection Vulnerabilities.

Quelle: https://www.owasp.org/index.php/SQL_Injection

Sichere Realisierung

Schwachstellen erkennen: Vier Augen sehen mehr als zwei!

Code-Reviews

Manuelle
Code-Reviews

Automatische Reviews mit
Statischer Code-Analyse

Sichere Realisierung
Welche Vor- und Nachteile haben die Review-Methoden?

Manuelle Code-Reviews

Automatische Code-Reviews mit Statischer Code-Analyse

Manuell, nicht (unbedingt) vollständig

Automatisiert, vollständig

Alles **echte** Schwachstellen

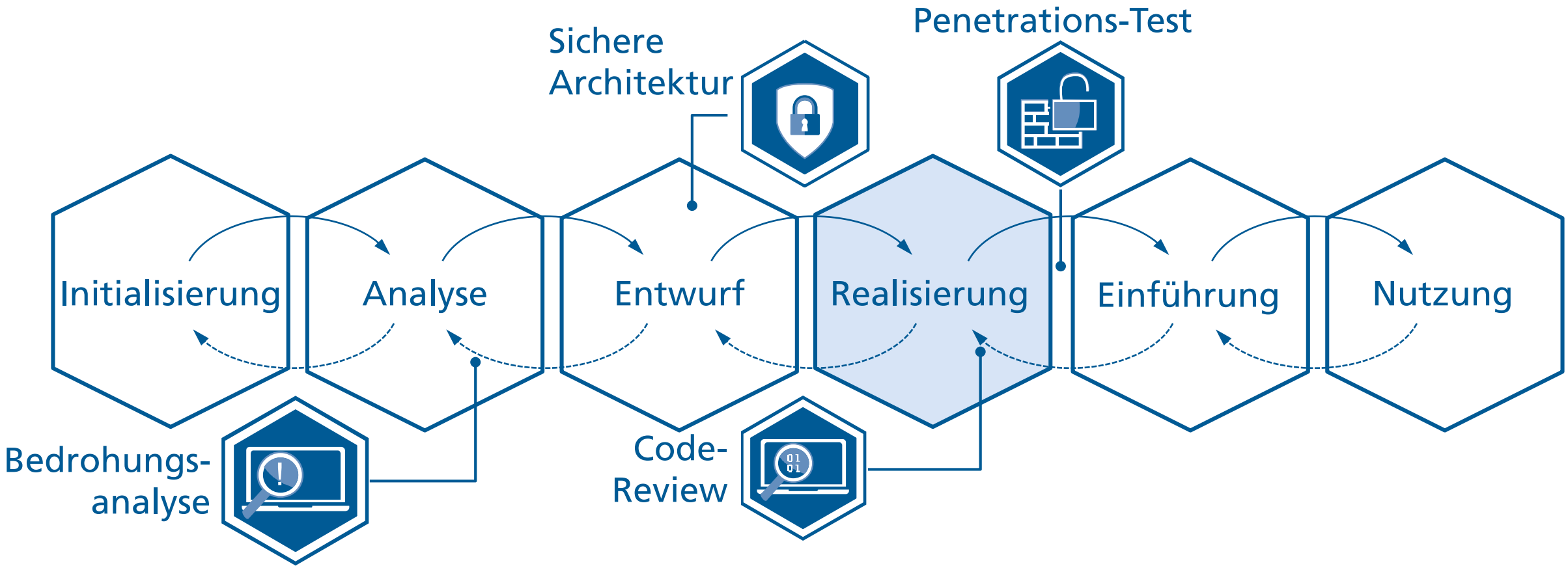
Nicht alles echte Schwachstellen

Also: Einsatz von manuellen und automatischen Code-Reviews, z.B. mit

- VeraCode, CheckMarx, Fortify, AppScan, …
- FindBugs
- Soot, FlowDroid, CogniCrypt

Security-by-Design: Security über den gesamten Prozess berücksichtigen

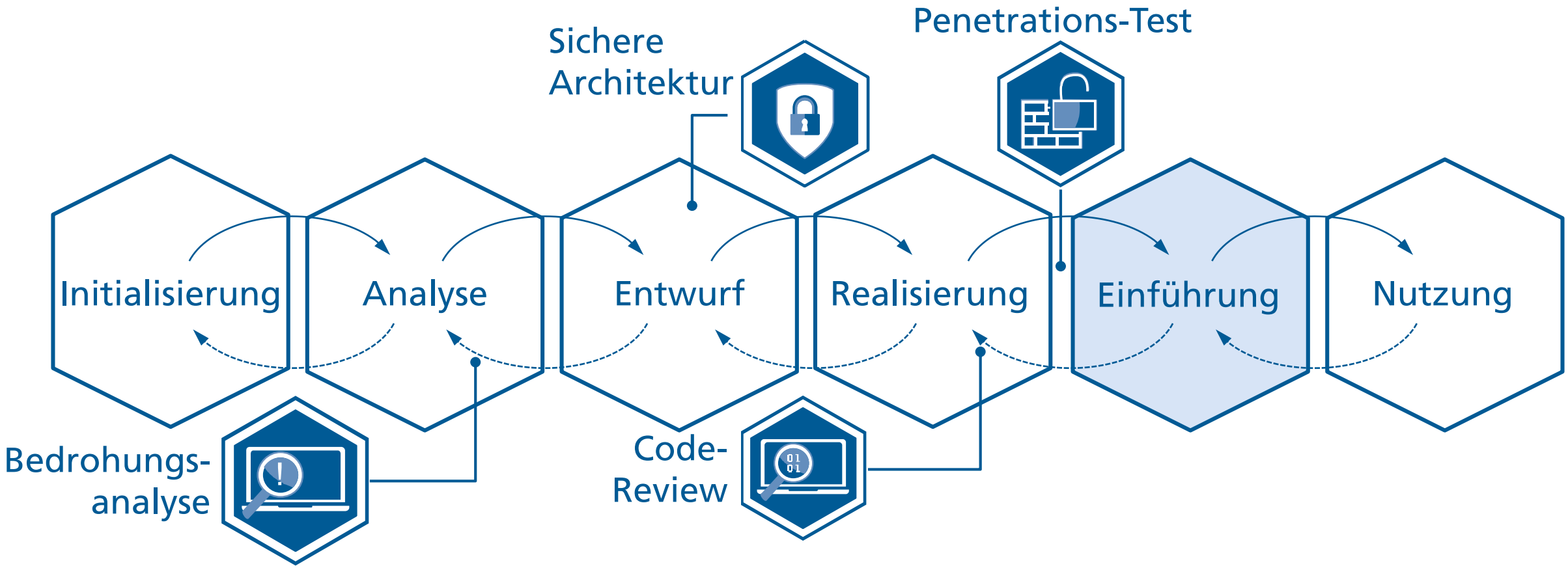
Realisierung



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Security-by-Design: Security über den gesamten Prozess berücksichtigen

Einführung



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sichere Konfiguration und Einführung
Kann jetzt wirklich noch was schief gehen?

> Before version 2.6.0, that wasn't true. By default, MongoDB was left open to remote connections. Authentication is also not required by default, which means that out of the box installs of MongoDB before version 2.6.0 happily accept unauthenticated remote connections.

Quelle: https://snyk.io/blog/mongodb-hack-and-secure-defaults/

„Standardmäßig war MongoDB offen für entfernte Verbindungen. Authentifizierung war in der Standardkonfiguration nicht notwendig, so dass die Datenbank unauthentifizierte Verbindungen annahm."

Sichere Konfiguration und Einführung
Kann jetzt wirklich noch was schief gehen?

Before version 2.6.0, that wasn't true. By default, MongoDB was left open to remote connections. Authentication is also not required by default, which means that out of the box installs of MongoDB before version 2.6.0 happily accept unauthenticated remote co

Quelle

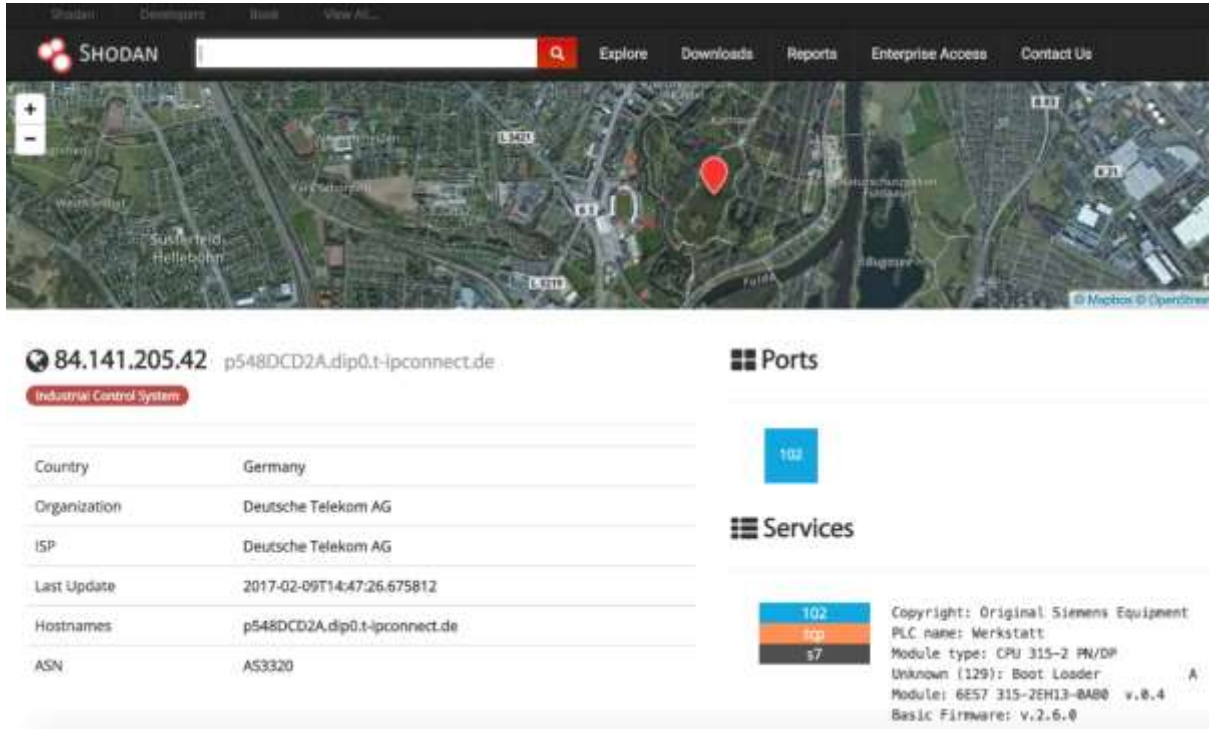
15.10.2016 14:07 Uhr

Offene Datenbank: 58 Millionen Datensätze im Umlauf

Durch eine ungeschützte MongoDB-Datenbank des texanischen Dienstleisters Modern Business Solutions sind mindestens 58 Millionen Einträge aus der Automobilbranche und Personalvermittlung geleakt.

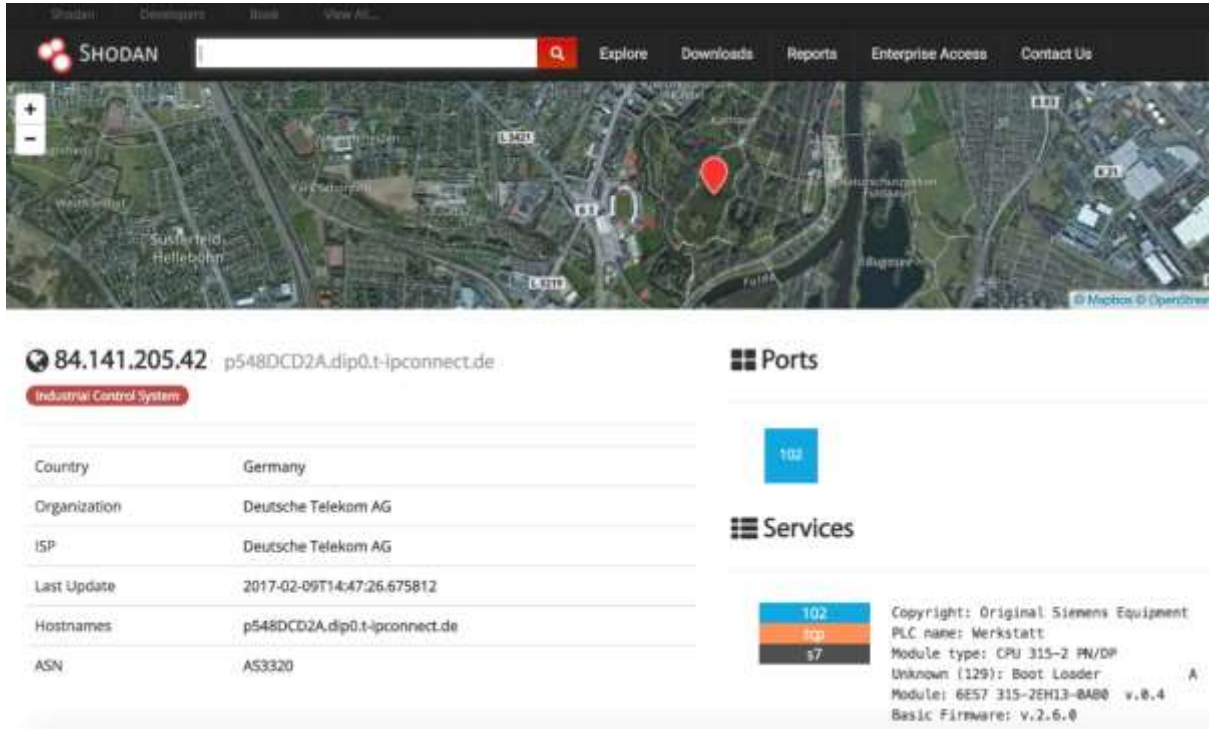
Quelle: https://www.heise.de/newsticker/meldung/Offene-Datenbank-58-Millionen-Datensaetze-im-Umlauf-3351104.html

Sichere Konfiguration und Einführung
Kann jetzt wirklich noch was schief gehen?



Quelle: https://www.shodan.io/

Sichere Konfiguration und Einführung
Kann jetzt wirklich noch was schief gehen?



Quelle: https://www.shodan.io/

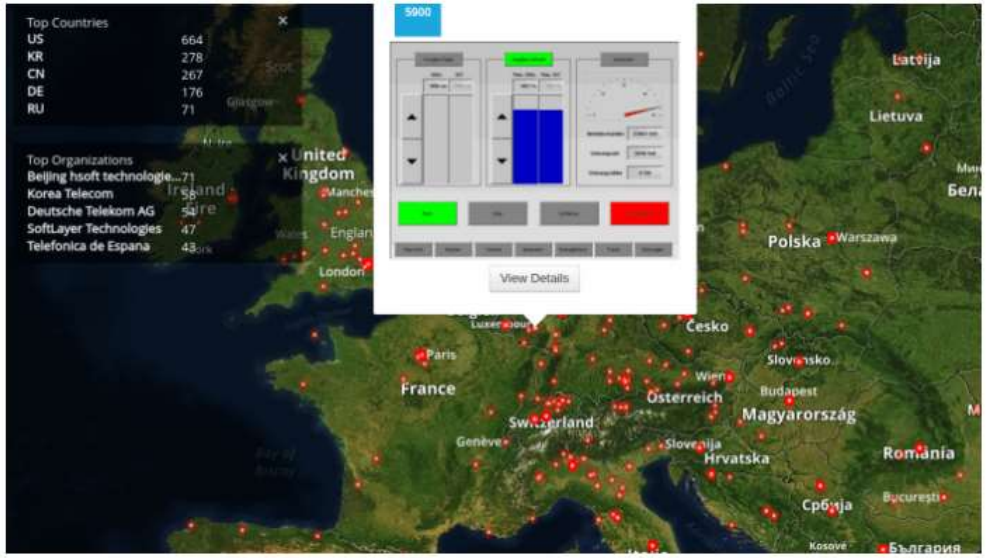
Also: Sicherheitsrelevante Konfigurationseinstellungen dokumentieren und prüfen

In eigener Software sichere Standardeinstellungen wählen (Security-by-Default)

Sichere Konfiguration und Einführung
Die Gefahr von vermeidbaren Programmen und Diensten

VNC-Roulette – was wollen Sie fernsteuern?

01.04.2016 07:00 Uhr – Jürgen Schmidt



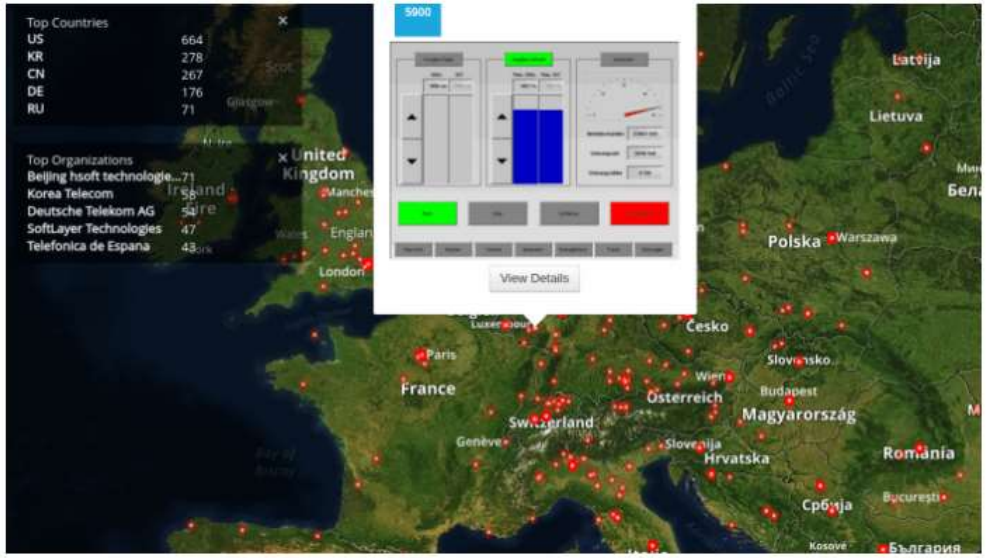
Ein Sicherheitsproblem, das es eigentlich nicht geben sollte und trotzdem: Industrielle Steuerungssysteme, Linux-Desktops, Spammer auf Facebook – es gibt fast nichts, was man nicht entdecken kann, wenn man einfach nach offenen VNC-Servern sucht.

Quelle: https://www.heise.de/security/meldung/VNC-Roulette-was-wollen-Sie-fernsteuern-3159811.html

Sichere Konfiguration und Einführung
Die Gefahr von vermeidbaren Programmen und Diensten

VNC-Roulette – was wollen Sie fernsteuern?

01.04.2016 07:00 Uhr – Jürgen Schmidt



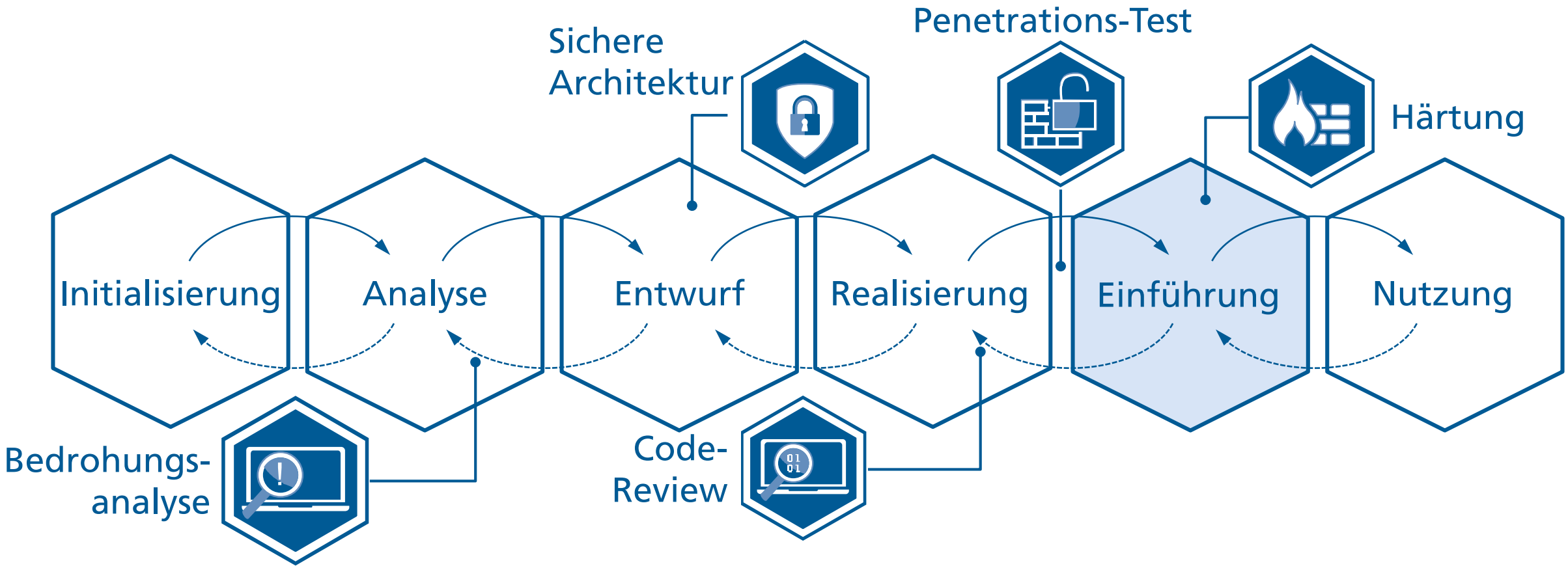
Ein Sicherheitsproblem, das es eigentlich nicht geben sollte und trotzdem: Industrielle Steuerungssysteme, Linux-Desktops, Spammer auf Facebook – es gibt fast nichts, was man nicht entdecken kann, wenn man einfach nach offenen VNC-Servern sucht.

Quelle: https://www.heise.de/security/meldung/VNC-Roulette-was-wollen-Sie-fernsteuern-3159811.html

Also: Nicht benötigte Dienste deaktivieren (Härtung)!

Security-by-Design: Security über den gesamten Prozess berücksichtigen

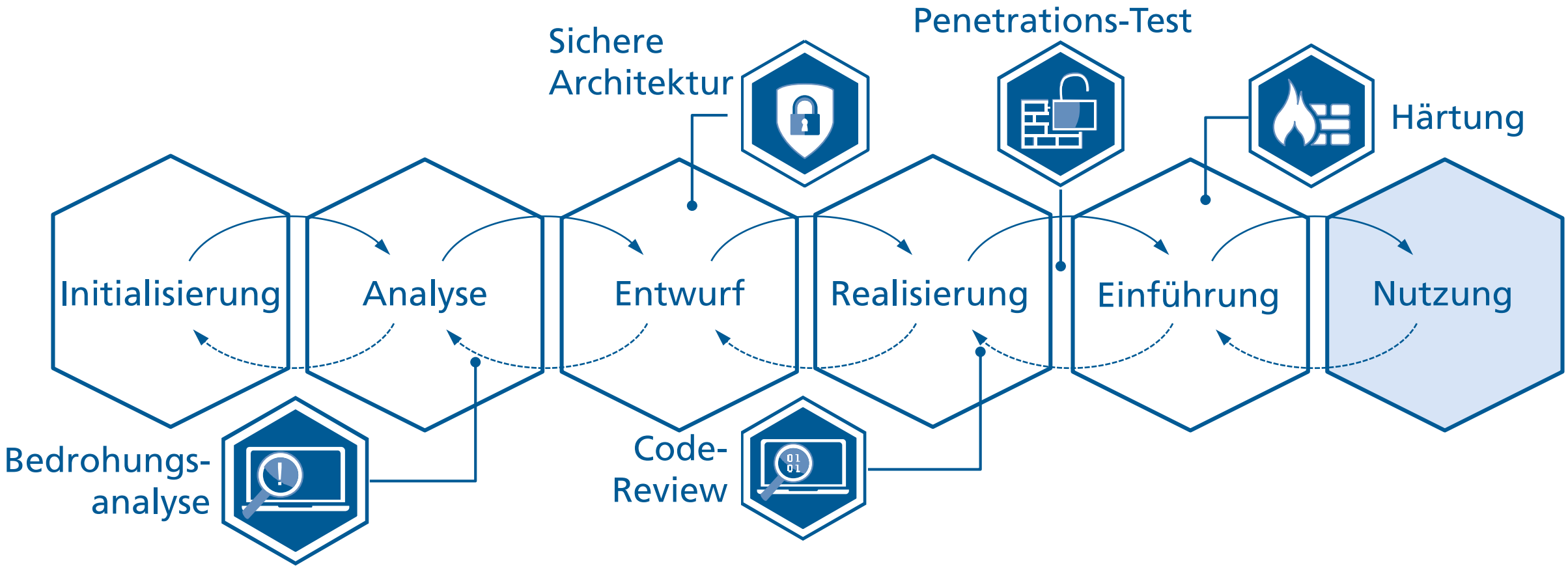
Einführung



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Security-by-Design: Security über den gesamten Prozess berücksichtigen

Nutzung



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Was wenn doch Mal was schief geht?

29.03.2017 12:47 Uhr

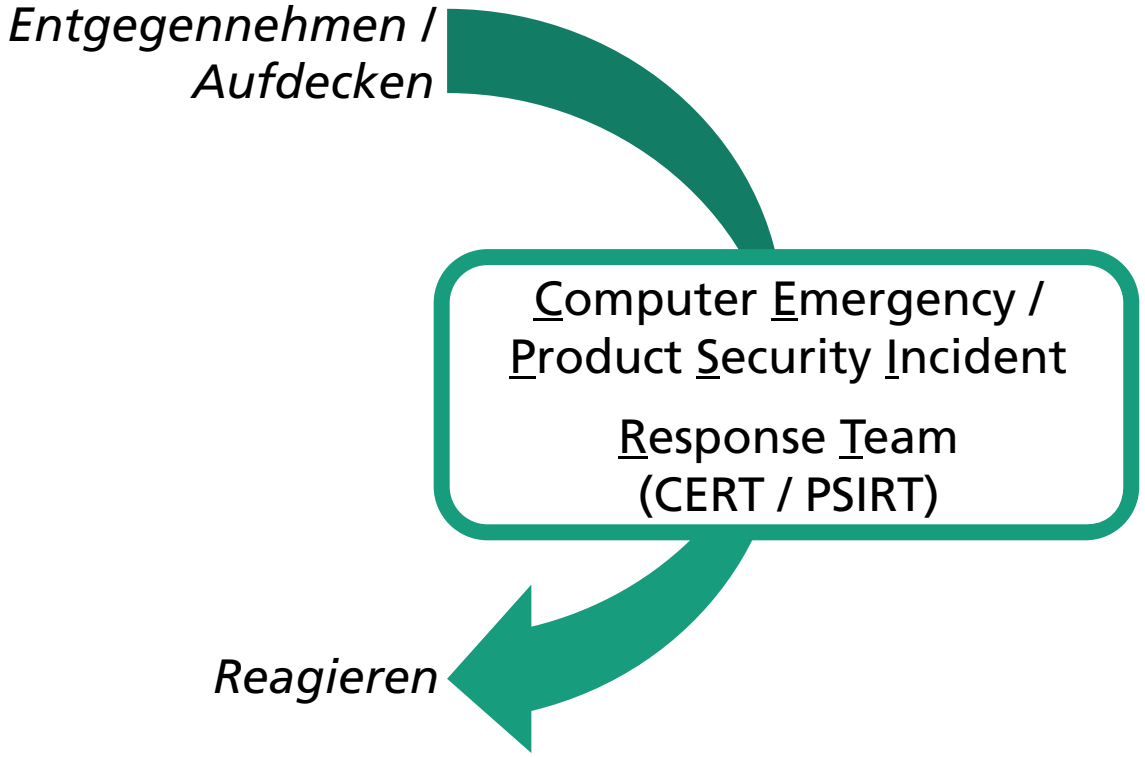
Miele verspricht Sicherheits-Update für Desinfektionsautomaten

In den Geräten ist ein gänzlich ungesicherter Webserver aufgefallen. Der Bugreport eines Security-Consultants war jedoch über Monate ignoriert worden.

Quelle: https://www.heise.de/newsticker/meldung/Miele-verspricht-Sicherheits-Update-fuer-Desinfektionsautomaten-3669611.html

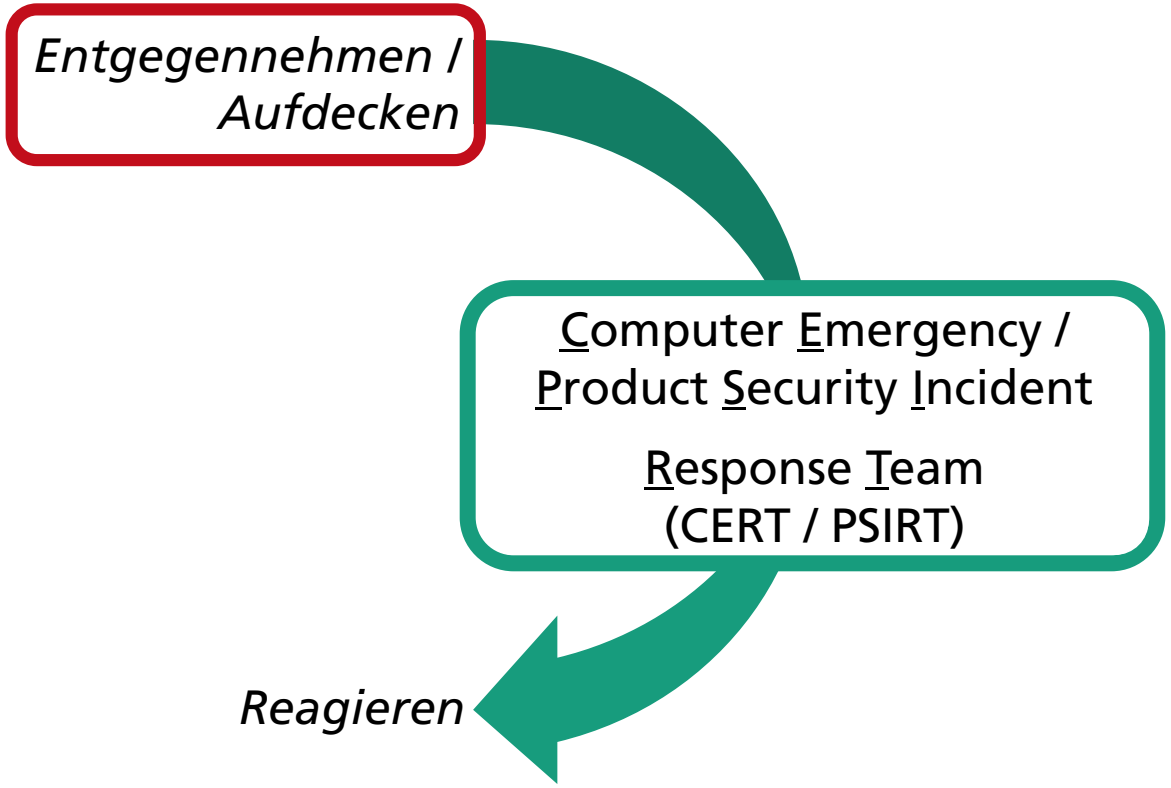
Sicherer Betrieb

Gemeldete Schwachstellen entgegennehmen, bewerten und geeignet reagieren



Sicherer Betrieb

Gemeldete Schwachstellen entgegennehmen, bewerten und geeignet reagieren



Sicherer Betrieb
Gemeldete Schwachstellen entgegennehmen

Introduction

Symantec is committed to resolving security vulnerabilities in our products quickly and carefully. We take the necessary steps to minimize customer risk, provide timely information, and deliver vulnerability fixes and mitigations required to address security threats in Symantec software.

As a founding member of the Organization for Internet Safety (OIS), Symantec is committed to following the Responsible Disclosure guidelines developed by OIS and described in ISO 29417 for externally reported vulnerabilities in Symantec products. These guidelines encourage open communication between finders and vendors, clarify responsibilities between parties, and protect individuals, enterprises, and internet infrastructure from exploitation whenever possible. We work closely with researchers who communicate vulnerabilities to us, and we give credit to finders who follow responsible disclosure.

How to report a security vulnerability

If you believe you have found a vulnerability in a Symantec product, cloud service, or IT infrastructure that has not been resolved, please contact Symantec via the email addresses provided below:

- Vulnerability reports for Symantec **on-premise** products should be sent to the Symantec Product Security Incident Response Team (PSIRT) at secure@symantec.com.
- Vulnerability reports for Symantec **cloud services and IT infrastructure** should be sent to the Symantec GSO Security Operations Center (SOC) at security@symantec.com.

Quelle: https://www.symantec.com/security-center/vulnerability-management

Sicherer Betrieb
Gemeldete Schwachstellen entgegennehmen

Introduction

Symantec is committed to resolving security vulnerabilities in our products quickly and carefully. We take the necessary steps to minimize customer risk, provide timely information, and deliver vulnerability fixes and mitigations required to address security threats in Symantec software.

As a founding member of the Organization for Internet Safety (OIS), Symantec is committed to following the Responsible Disclosure guidelines developed by OIS and described in ISO 29417 for externally reported vulnerabilities in Symantec products. These guidelines encourage open communication between finders and vendors, clarify responsibilities between parties, and protect individuals, enterprises, and internet infrastructure from exploitation whenever possible. We work closely with researchers who communicate vulnerabilities to us, and we give credit to finders who follow responsible disclosure.

How to report a security vulnerability

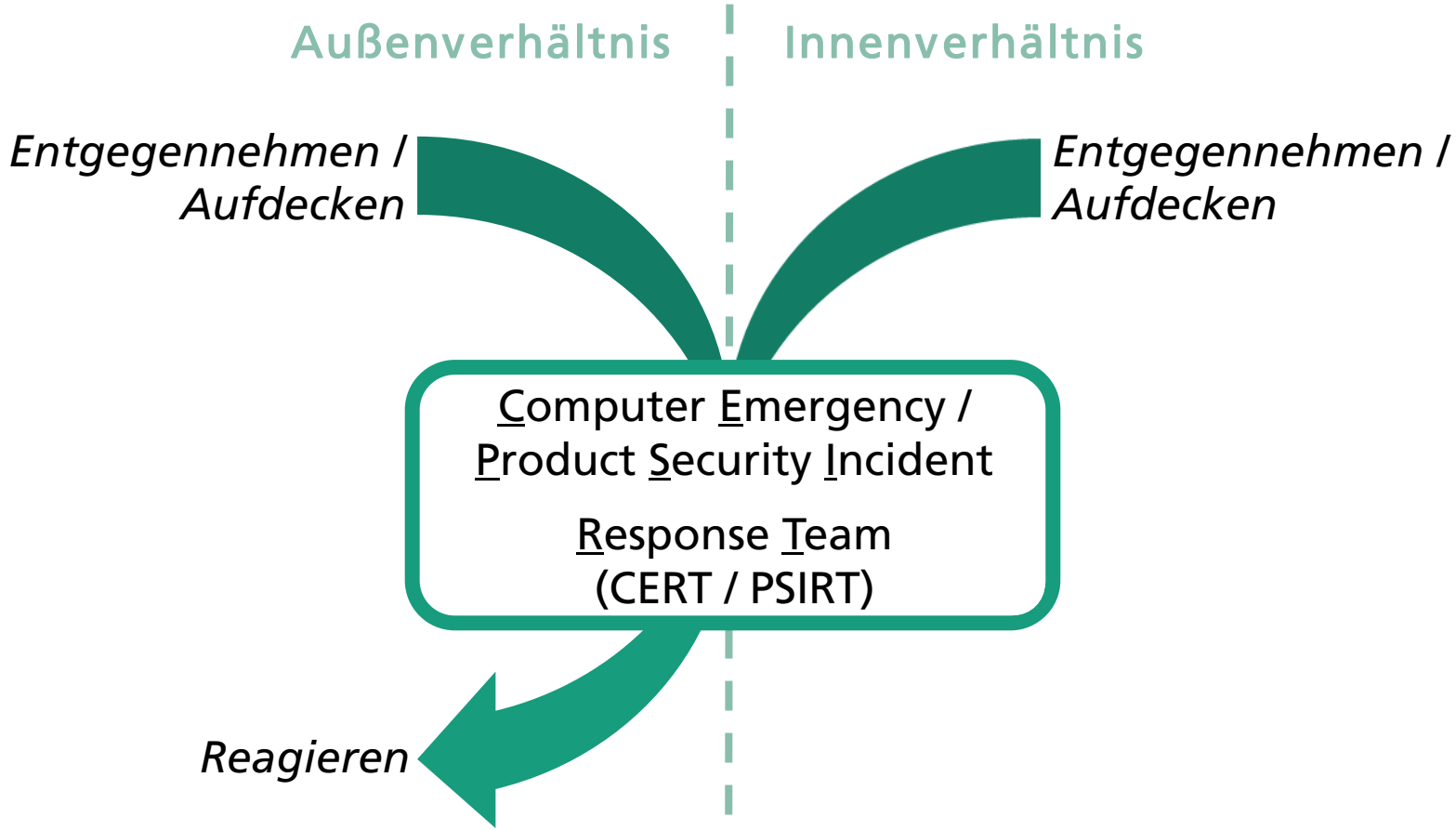
If you believe you have found a vulnerability in a Symantec product, cloud service, or IT infrastructure that has not been resolved, please contact Symantec via the email addresses provided below:

- Vulnerability reports for Symantec **on-premise** products should be sent to the Symantec Product Security Incident Response Team (PSIRT) at secure@symantec.com.
- Vulnerability reports for Symantec **cloud services and IT infrastructure** should be sent to the Symantec GSO Security Operations Center (SOC) at security@symantec.com.

Quelle: https://www.symantec.com/security-center/vulnerability-management

Sicherer Betrieb

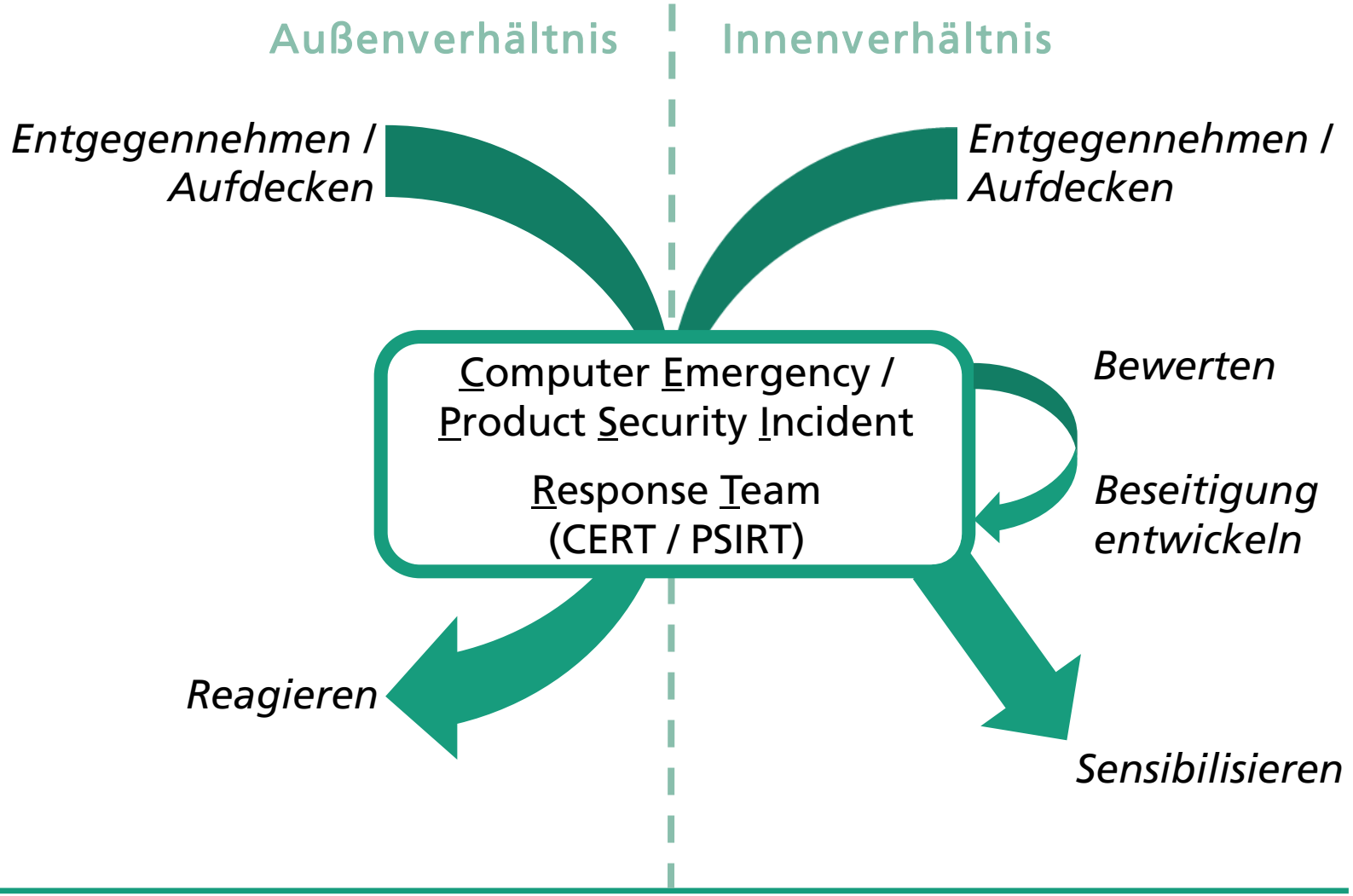
Gemeldete Schwachstellen entgegennehmen, bewerten und geeignet reagieren



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sicherer Betrieb

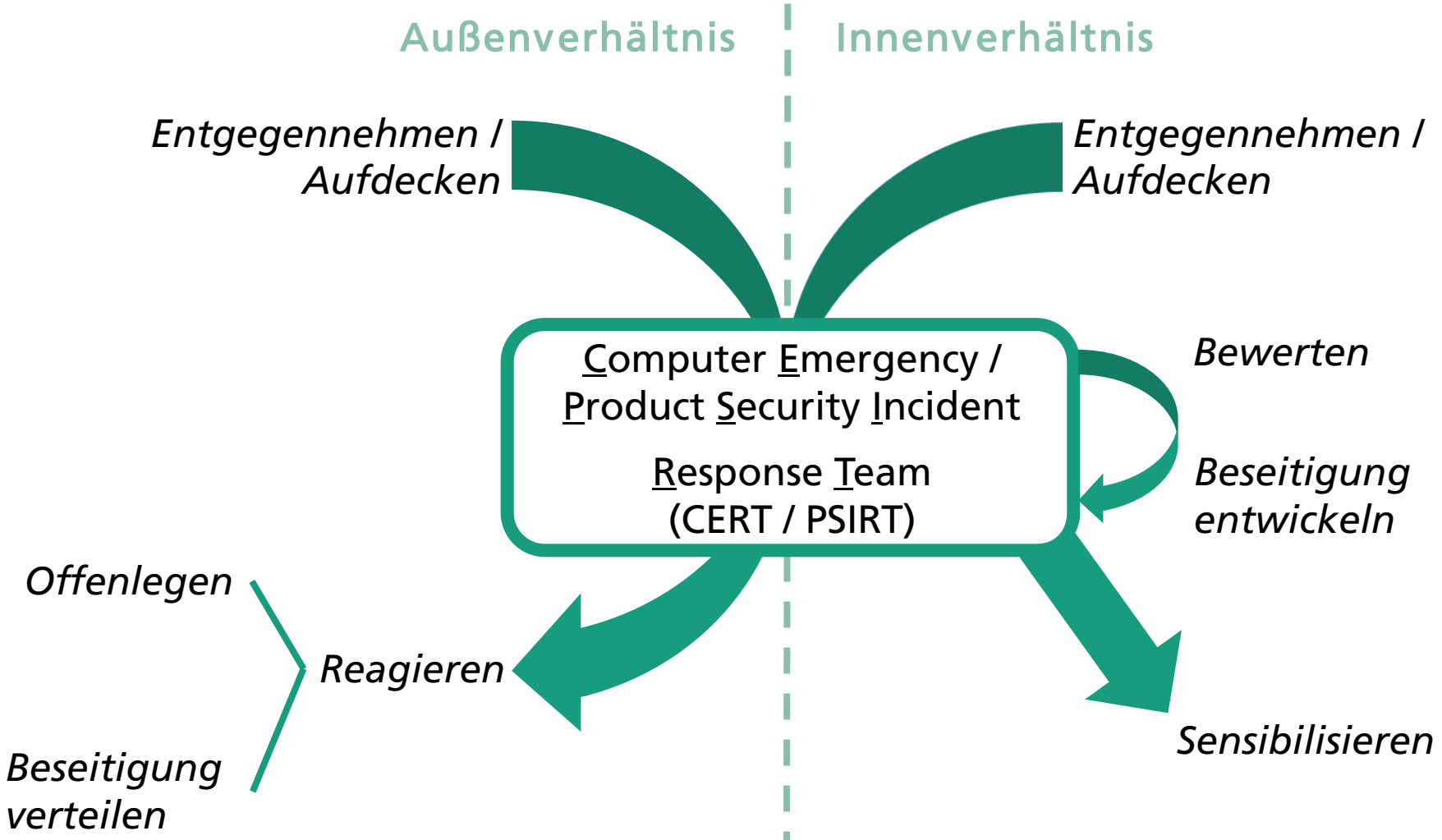
Gemeldete Schwachstellen entgegennehmen, bewerten und geeignet reagieren



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sicherer Betrieb

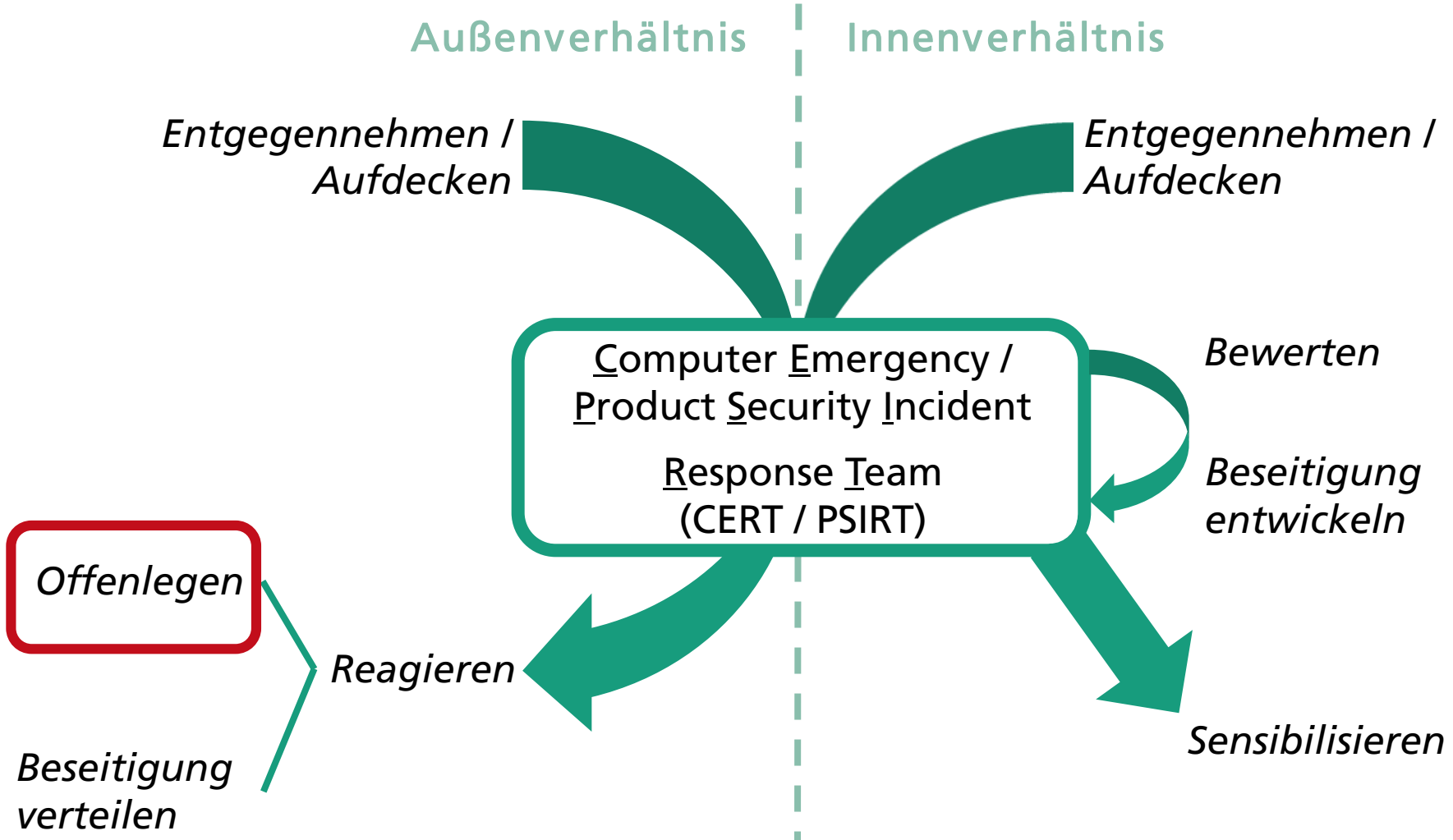
Gemeldete Schwachstellen entgegennehmen, bewerten und geeignet reagieren



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sicherer Betrieb

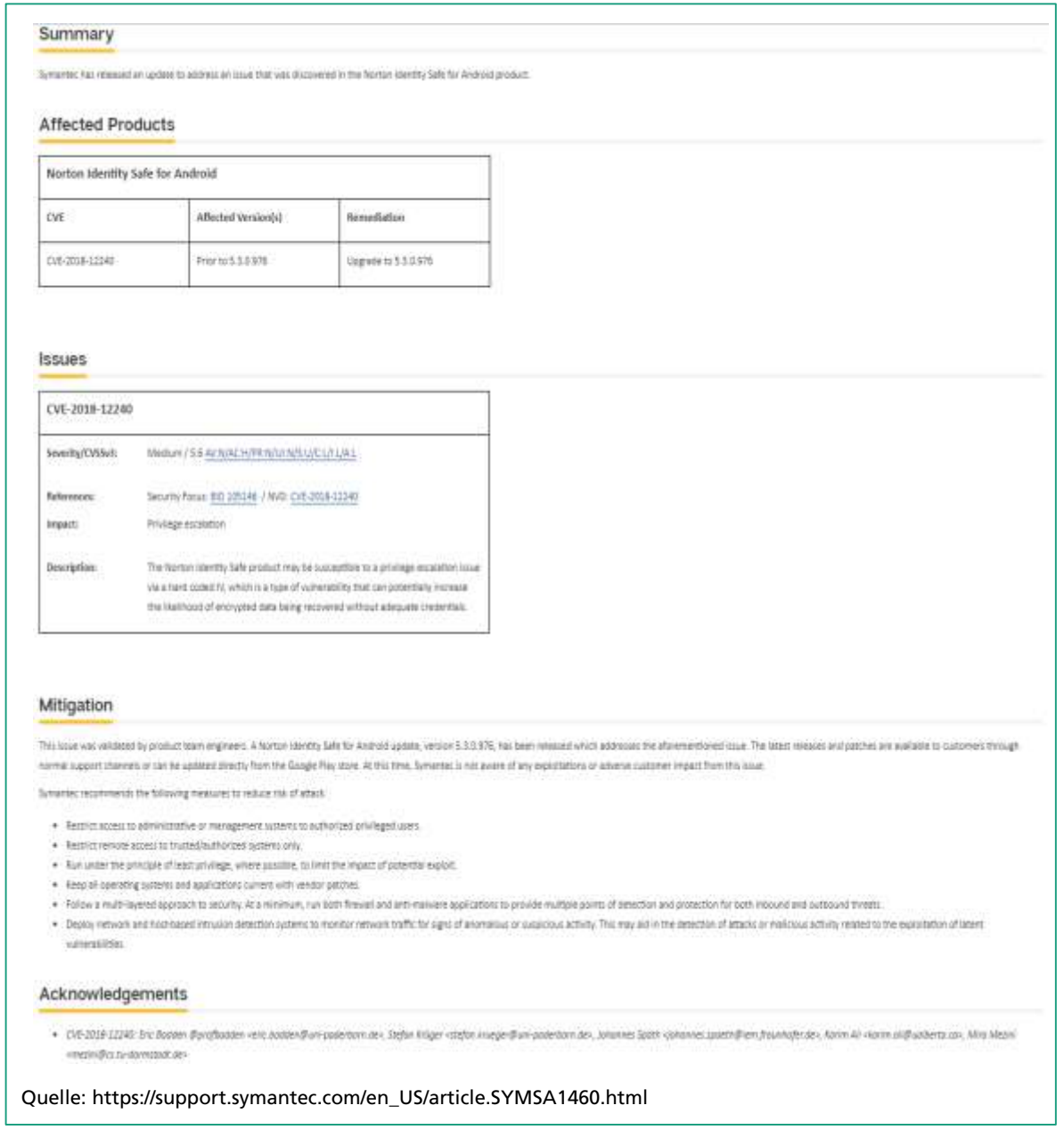
Gemeldete Schwachstellen entgegennehmen, bewerten und geeignet reagieren



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sicherer Betrieb
Aufgedeckte Schwachstellen offenlegen

- Security Advisories / Common Vulnerabilities and Exposures (CVE)
  - Problemzusammenfassung
  - Betroffene Produktversionen
  - Security-Schwachstellen
  - Lösung / Work Arounds



Summary

Affected Products

Norton Identity Safe for Android		
CVE	Affected Version(s)	Remediation
CVE-2018-12240	Prior to 5.3.0.978	Upgrade to 5.3.0.976

Issues

CVE-2018-12240

Severity/CVSSv3: Medium / 5.6 AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

References: Security Focus: BID 105146 / NVD: CVE-2018-12240

Impact: Privilege escalation

Description: The Norton Identity Safe product may be susceptible to a privilege escalation issue via a hard coded IV, which is a type of vulnerability that can potentially increase the likelihood of encrypted data being recovered without adequate credentials.

Mitigation

This issue was validated by product team engineers. A Norton Identity Safe for Android update, version 5.3.0.976, has been released which addresses the aforementioned issue. The latest releases and patches are available to customers through normal support channels or can be updated directly from the Google Play store. At this time, Symantec is not aware of any exploitations or adverse customer impact from this issue.

Symantec recommends the following measures to reduce risk of attack:

- Restrict access to administrative or management systems to authorized privileged users.
- Restrict remote access to trusted/authorized systems only.
- Run under the principle of least privilege, where possible, to limit the impact of potential exploit.
- Keep all operating systems and applications current with vendor patches.
- Follow a multi-layered approach to security. At a minimum, run both firewall and anti-malware applications to provide multiple points of detection and protection for both inbound and outbound threats.
- Deploy network and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in the detection of attacks or malicious activity related to the exploitation of latent vulnerabilities.

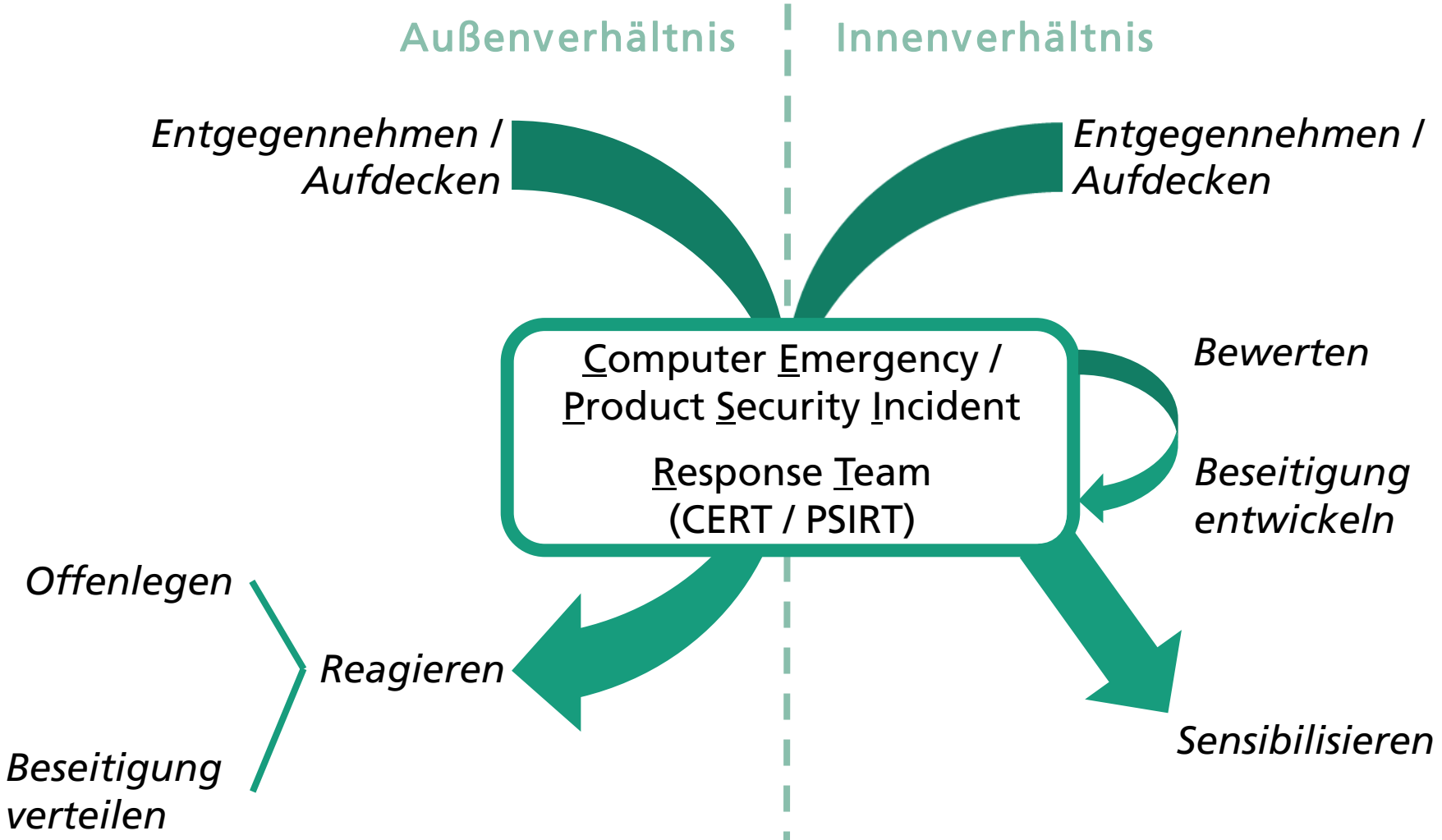
Acknowledgements

- CVE-2018-12240: Eric Bodden <eric.bodden@uni-paderborn.de>, Stefan Krüger <stefan.krueger@uni-paderborn.de>, Johannes Späth <johannes.spaeth@iem.fraunhofer.de>, Karim Ali <karim.ali@ualberta.ca>, Mira Mezini <mezini@cs.tu-darmstadt.de>

Quelle: https://support.symantec.com/en_US/article.SYMSA1460.html

Sicherer Betrieb

Gemeldete Schwachstellen entgegennehmen, bewerten und geeignet reagieren



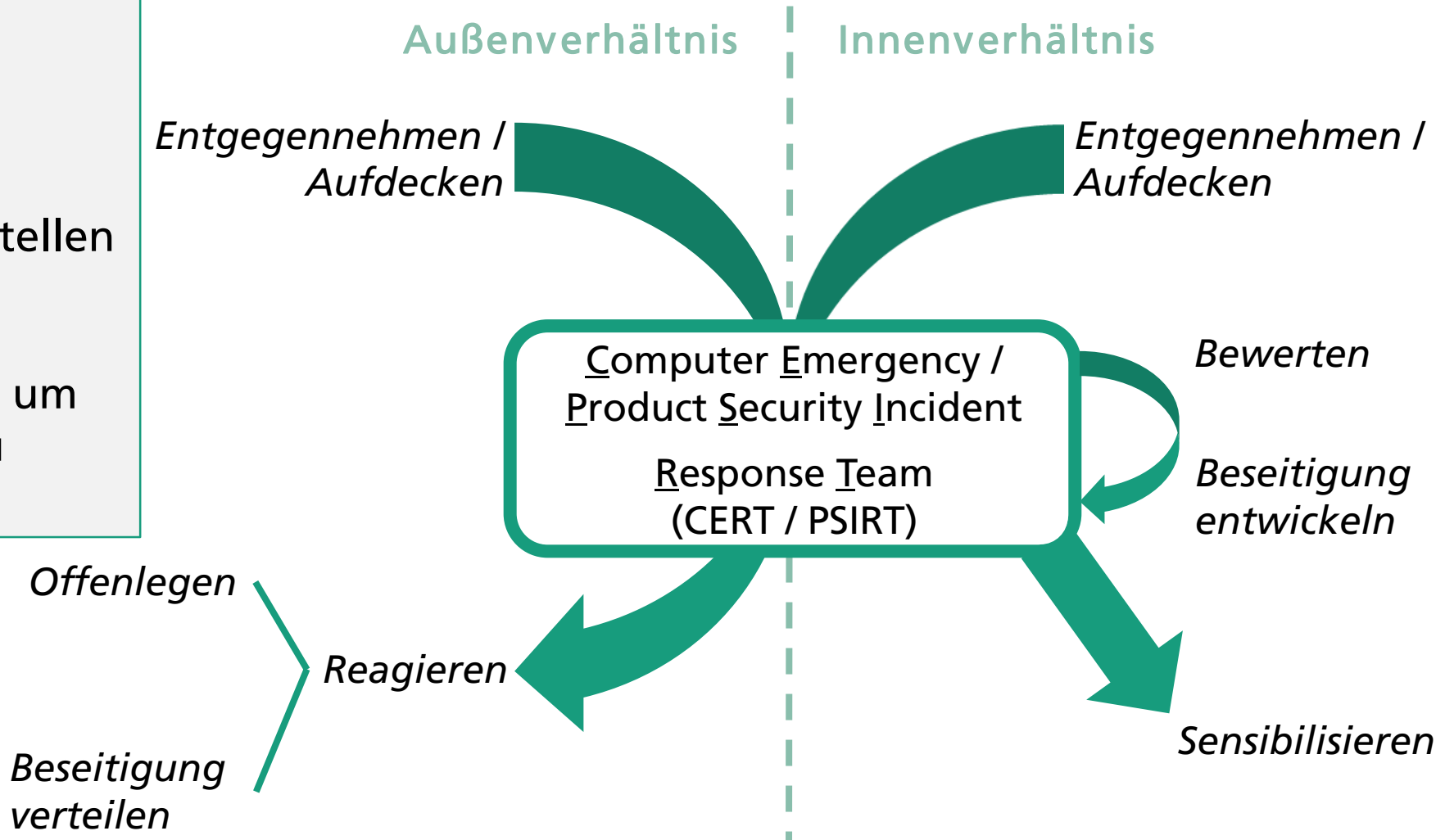
HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Sicherer Betrieb

Gemeldete Schwachstellen entgegennehmen, bewerten und geeignet reagieren

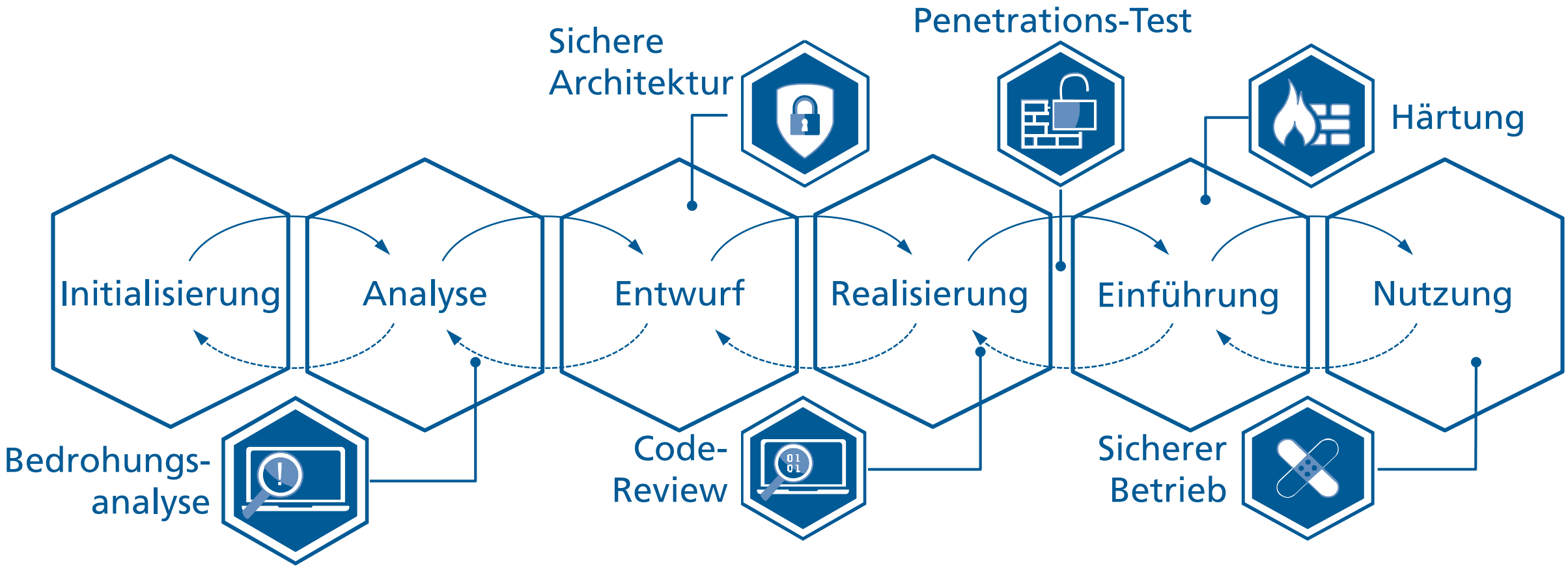
Also:

- CERT / PSIRT für verantwortungsvollen Umgang mit Schwachstellen etablieren
- Prozesse vordefinieren um im Krisenfall schnell zu reagieren



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Security-by-Design: Security über den gesamten Prozess berücksichtigen



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

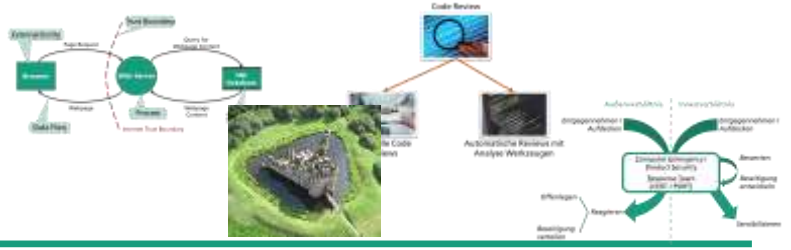
Take Aways

- Security gewinnt zunehmend an Bedeutung…

- … und bleibt eine Herausforderung für viele Unternehmen

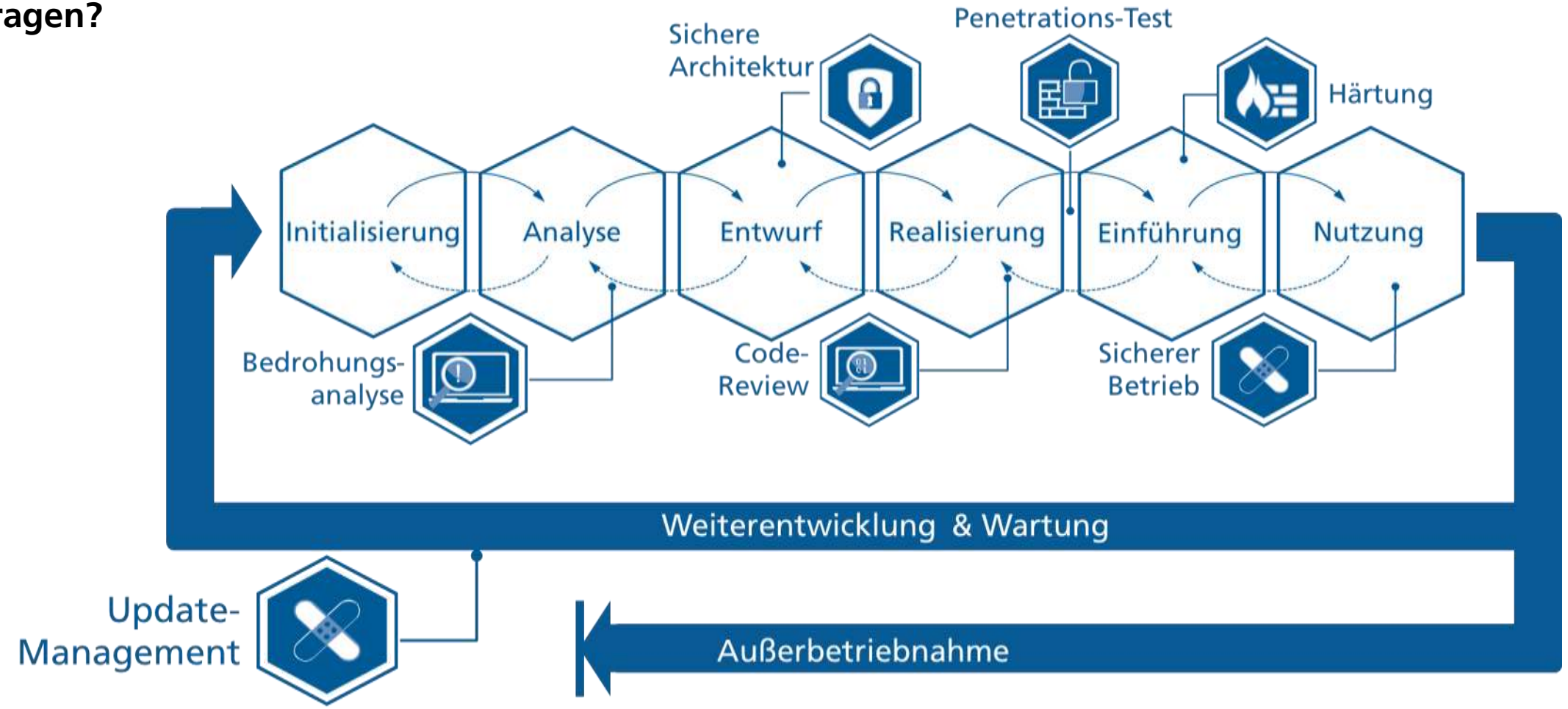
- **Security sollte über den gesamten Prozess berücksichtigt werden**

- Entsprechende Maßnahmen kann jede Organisation durchführen



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Fragen?

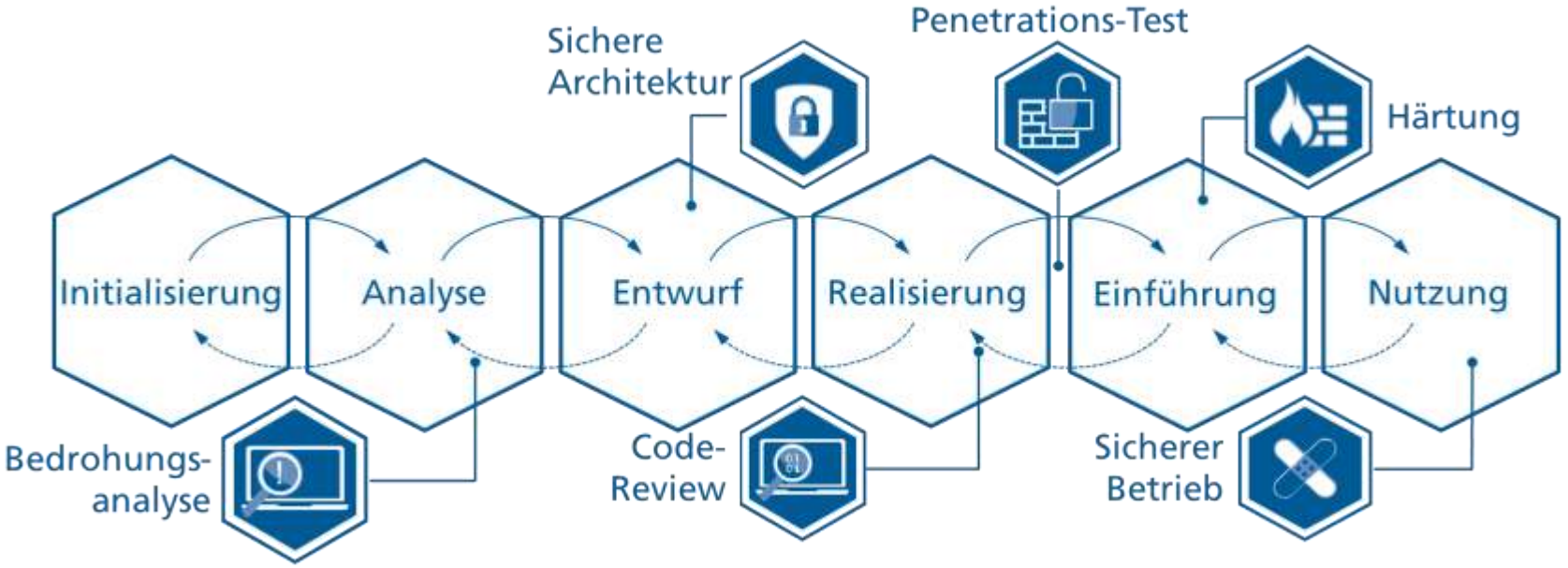


masud.fazal-baqaie@iem.fraunhofer.de
@masudfb

Themenseite: IT-Security am Fraunhofer IEM
https://www.iem.fraunhofer.de/de/forschung/kernkompetenzen/it-security.html

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Security-by-Design: Security über den gesamten Prozess berücksichtigen



Ist das alles?

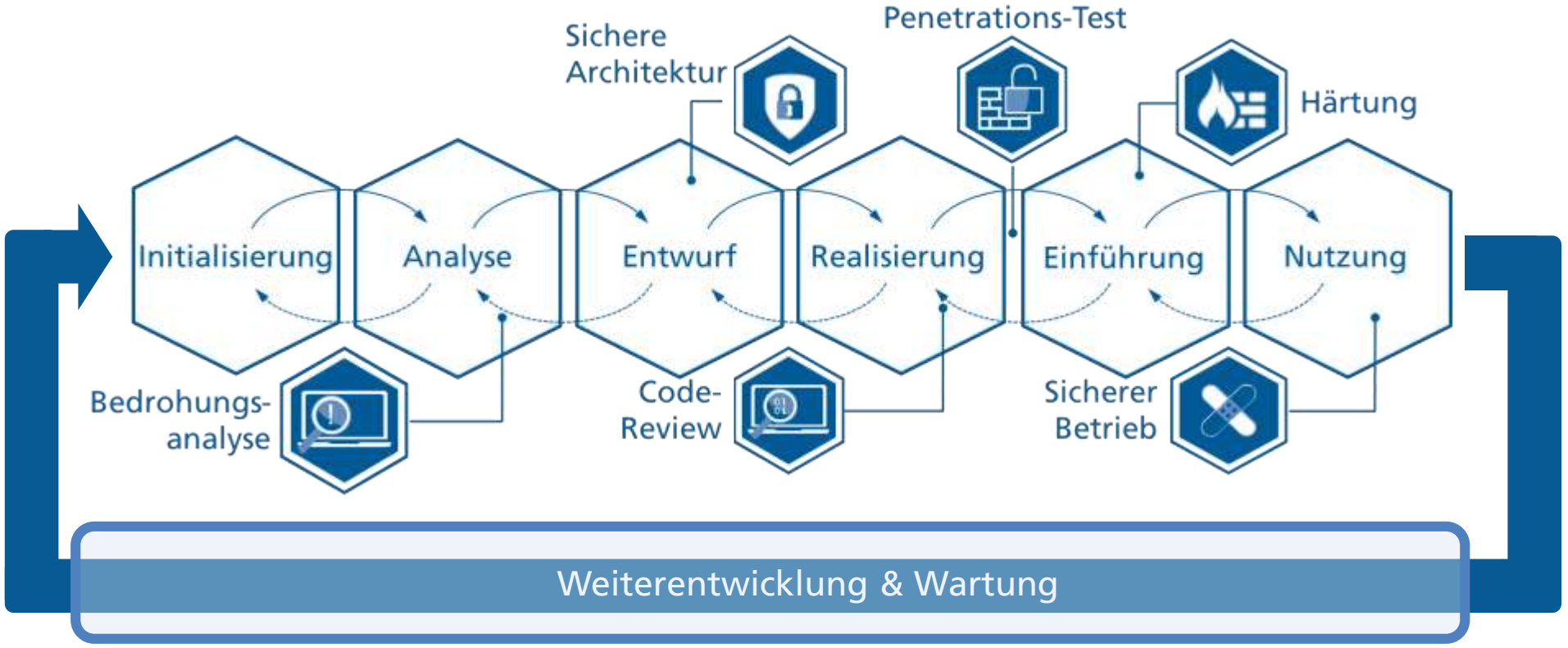
Security-by-Design: Security über den gesamten Prozess berücksichtigen

Noch nicht!

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Security-by-Design: Security über den gesamten Prozess berücksichtigen

Weiterentwicklung & Wartung



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Weiterentwicklung & Wartung
Keine Security-Lücken nachträglich einbauen!

Windows Defender verschluckt sich an RAR

06.04.2018 14:32 Uhr – Olivia von Westernhagen

Microsofts Malware Protection Engine ermöglichte dank missglückter Bugfixes zeitweise die Remote Code Execution mittels präparierter RAR-Archive. Mittlerweile ist jedoch ein Update verfügbar, das automatisch verteilt wird.

Quelle: https://www.heise.de/security/meldung/Windows-Defender-verschluckt-sich-an-RAR-4012228.html

Weiterentwicklung & Wartung
Keine Security-Lücken nachträglich einbauen!

Windows Defender verschluckt sich an RAR

06.04.2018 14:32 Uhr – Olivia von Westernhagen

Microsofts Malware Protection Engine ermöglichte dank missglückter Bugfixes zeitweise die Remote Code Execution mittels präparierter RAR-Archive. Mittlerweile ist jedoch ein Update verfügbar, das automatisch verteilt wird.

Quelle: https://www.heise.de/security/meldung/Windows-Defender-verschluckt-sich-an-RAR-4012228.html

Also: Security-by-Design-Maßnahmen auch bei Updates anwenden!

Weiterentwicklung & Wartung
Sicheren Update-Mechanismus bereitstellen

26.08.2018 16:26 Uhr

Schwachstelle Royale: Fortnite-Installer für Android offen für freies Nachladen

Bei der Android-Version von Fortnite Battle Royale umging Epic Games den Play Store und lieferte einen eigenen Installer – mit gravierender Sicherheitslücke.

https://www.heise.de/newsticker/meldung/Schwachstelle-Royale-Fortnite-Installer-fuer-Android-offen-fuer-freies-Nachladen-4145876.html

Sicheren Update-Mechanismus bereitstellen

26.08.2018 16:26 Uhr

Schwachstelle Royale: Fortnite-Installer für Android offen für freies Nachladen

Bei der Android-Version von Fortnite Battle Royale umging Epic Games den Play Store und lieferte einen eigenen Installer – mit gravierender Sicherheitslücke.

https://www.heise.de/newsticker/meldung/Schwachstelle-Royale-Fortnite-Installer-fuer-Android-offen-fuer-freies-Nachladen-4145876.html

„Die Anwendung untersucht die heruntergeladene Datei zunächst per Prüfsumme auf Manipulation und speichert sie.
Bei der anschließenden Installation jedoch verlässt sie sich offenbar auf den Dateinamen und installiert, was auch immer unter diesem Namen im Dateisystem abgelegt ist.“

Weiterentwicklung & Wartung
Sicheren Update-Mechanismus bereitstellen

26.08.2018 16:26 Uhr

Schwachstelle Royale: Fortnite-Installer für Android offen für freies Nachladen

Bei der Android-Version von Fortnite Battle Royale umging Epic Games den Play Store und lieferte einen eigenen Installer – mit gravierender Sicherheitslücke.

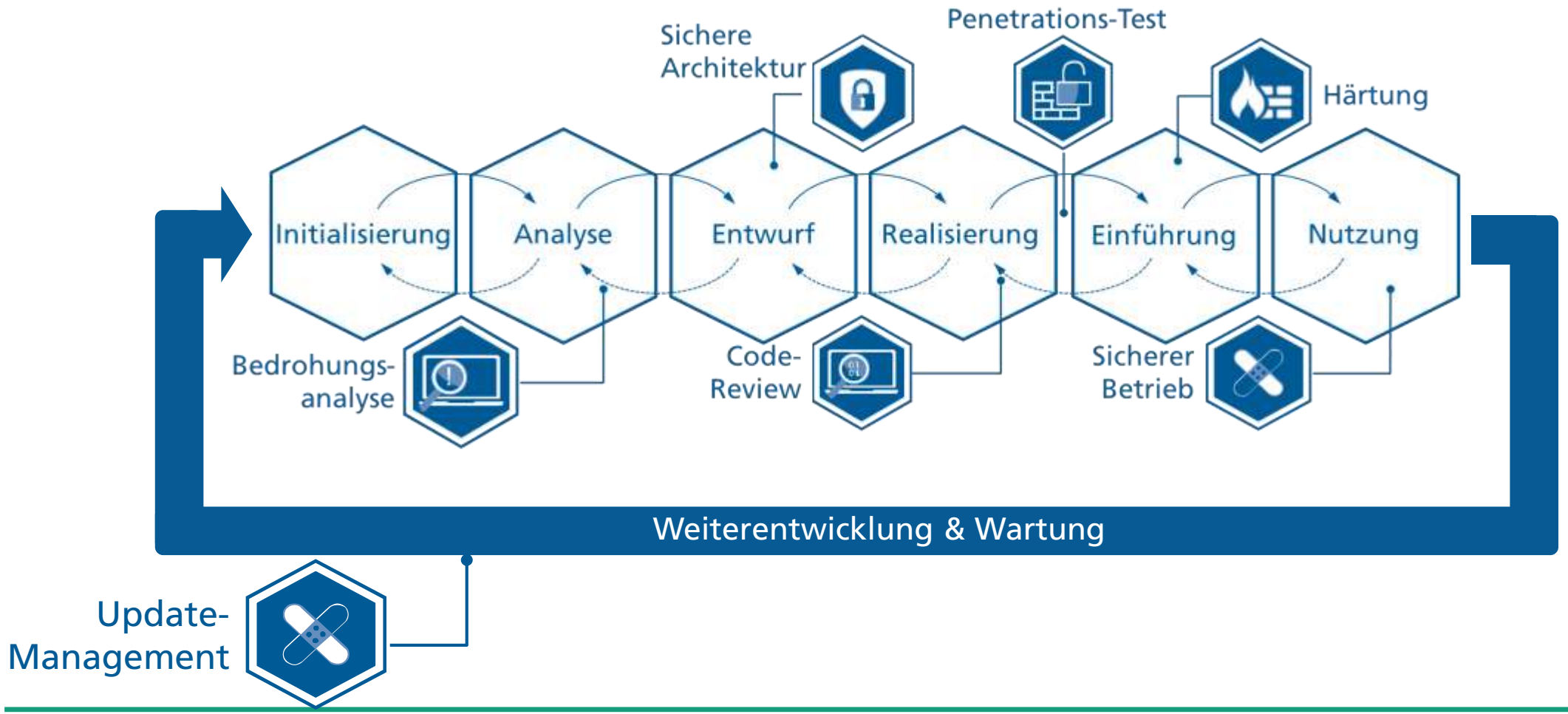
https://www.heise.de/newsticker/meldung/Schwachstelle-Royale-Fortnite-Installer-fuer-Android-offen-fuer-freies-Nachladen-4145876.html

„Die Anwendung untersucht die heruntergeladene Datei zunächst per Prüfsumme auf Manipulation und speichert sie.
Bei der anschließenden Installation jedoch verlässt sie sich offenbar auf den Dateinamen und installiert, was auch immer unter diesem Namen im Dateisystem abgelegt ist.“

Also: Bei Remote-Updates auf sicheren Update-Mechanismus achten!

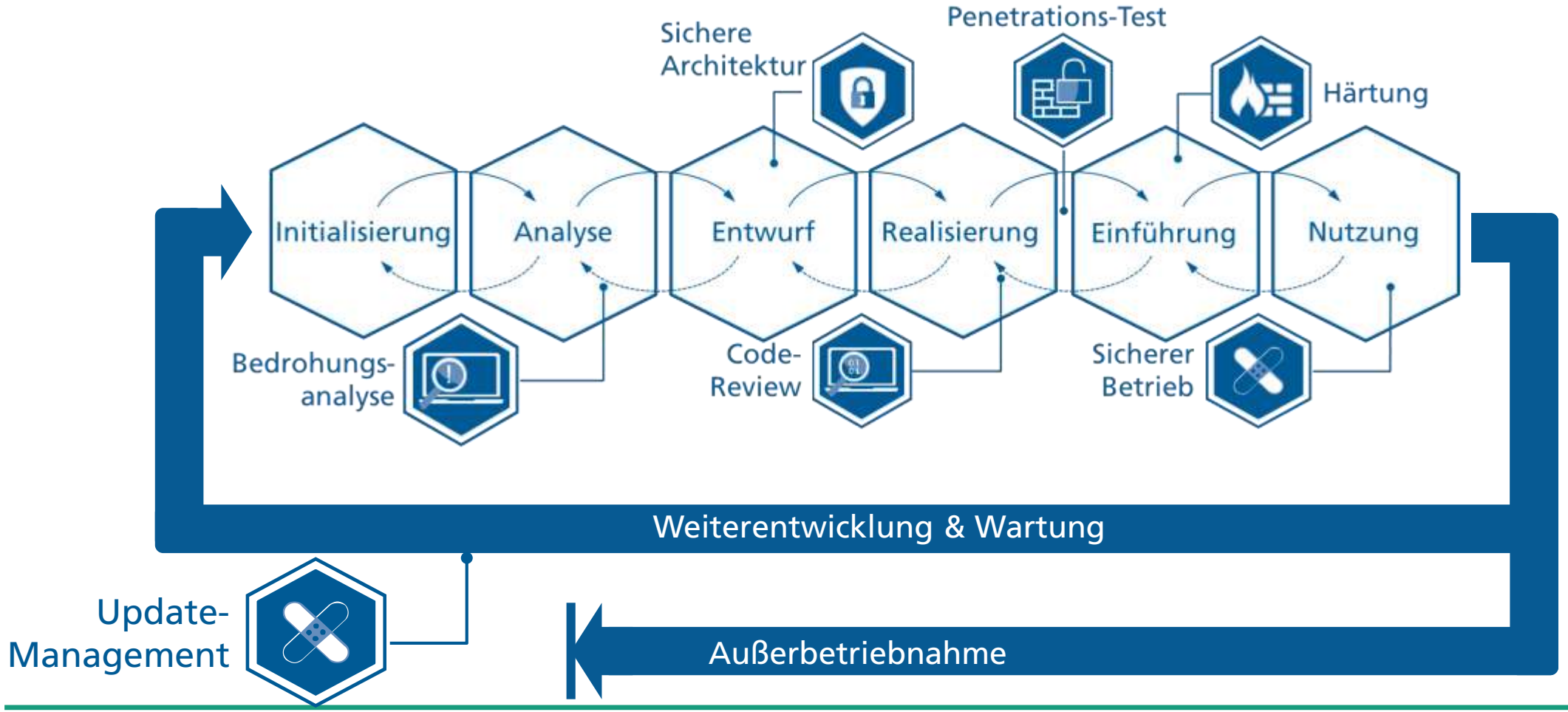
Security-by-Design: Security über den gesamten Prozess berücksichtigen

Ist das jetzt endlich alles?



Security-by-Design: Security über den gesamten Prozess berücksichtigen

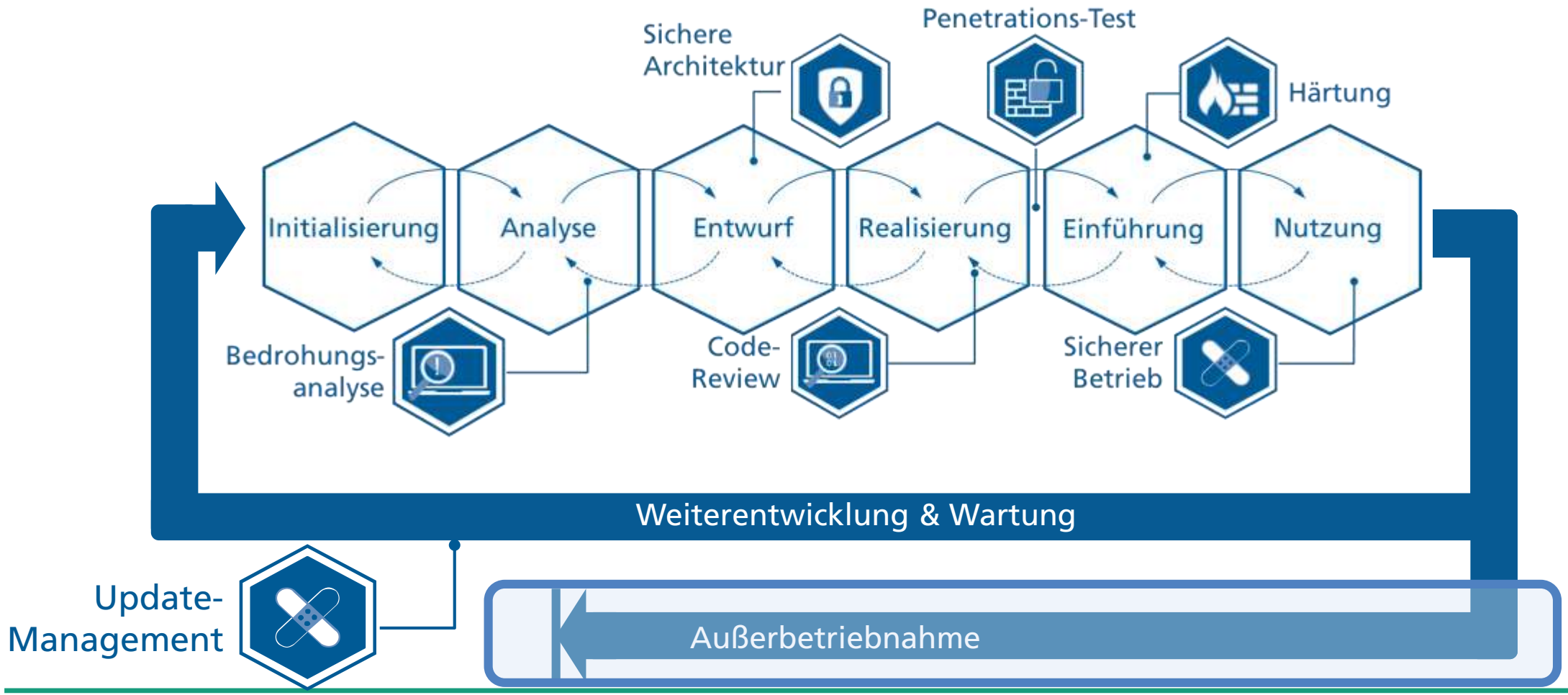
Fast geschafft…



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Security-by-Design: Security über den gesamten Prozess berücksichtigen

Außerbetriebnahme



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Außerbetriebnahme
Was kann hier schon schief gehen?

GARMIN

Navigon-Apps werden eingestellt

Garmin zieht sich fast komplett aus dem Geschäft mit Navigations-Apps zurück. Die Navigon-Apps werden fast ausnahmslos eingestellt. Offenbar war die Konkurrenz kostenloser Navigationslösungen einfach zu groß.

18. April 2018, 13:50 Uhr, Ingo Pakalski

Quelle: https://www.golem.de/news/garmin-navigon-apps-werden-eingestellt-1804-133920.html

Quelle: https://www.amazon.de/Garmin-Wuerzburg-GmbH-NAVIGON-Europe/dp/B019C5LZX4

Außerbetriebnahme
Was kann hier schon schief gehen?

GARMIN

zurück.

ngo Pakalski

Quelle: https://www.navigon.com/mobile-app/ - **Stand: 18.09.2018**

NAVIGON Europe
von Garmin Wuerzburg GmbH
Bewertung: Aufsicht empfohlen
5.146 Kundenrezensionen

Preisinformationen nicht verfügbar.

Diese App braucht die Erlaubnis, den Zugang:
- SMS-Nachrichten senden
- Die Kontaktdaten des Benutzers lesen

Alle Applikationsrechte

Entwickler kontaktieren

Quelle: https://www.amazon.de/Garmin-Wuerzburg-GmbH-NAVIGON-Europe/dp/B019C5LZX4

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Außerbetriebnahme
Was kann hier schon schief gehen?

GARMIN

zurück.

ngo Pakalski

Quelle: https://www.navigon.com/mobile-app/ - **Stand: 18.09.2018**

NAVIGON Europe
von Garmin Wuerzburg GmbH
Bewertung: Aufsicht empfohlen
5.146 Kundenrezensionen

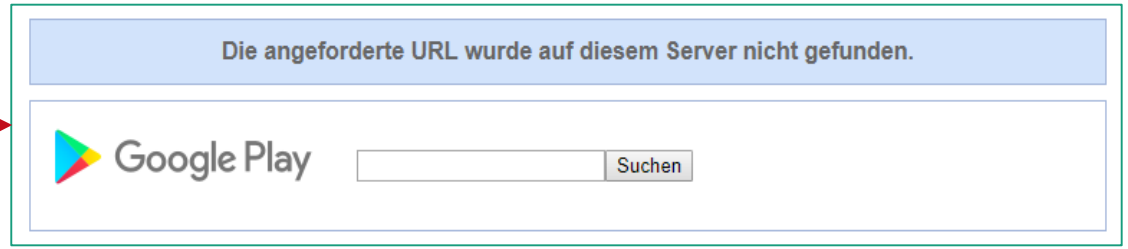
Preisinformationen nicht verfügbar.

Diese App braucht die Erlaubnis, den Zugang:
- SMS-Nachrichten senden
- Die Kontaktdaten des Benutzers lesen

Alle Applikationsrechte

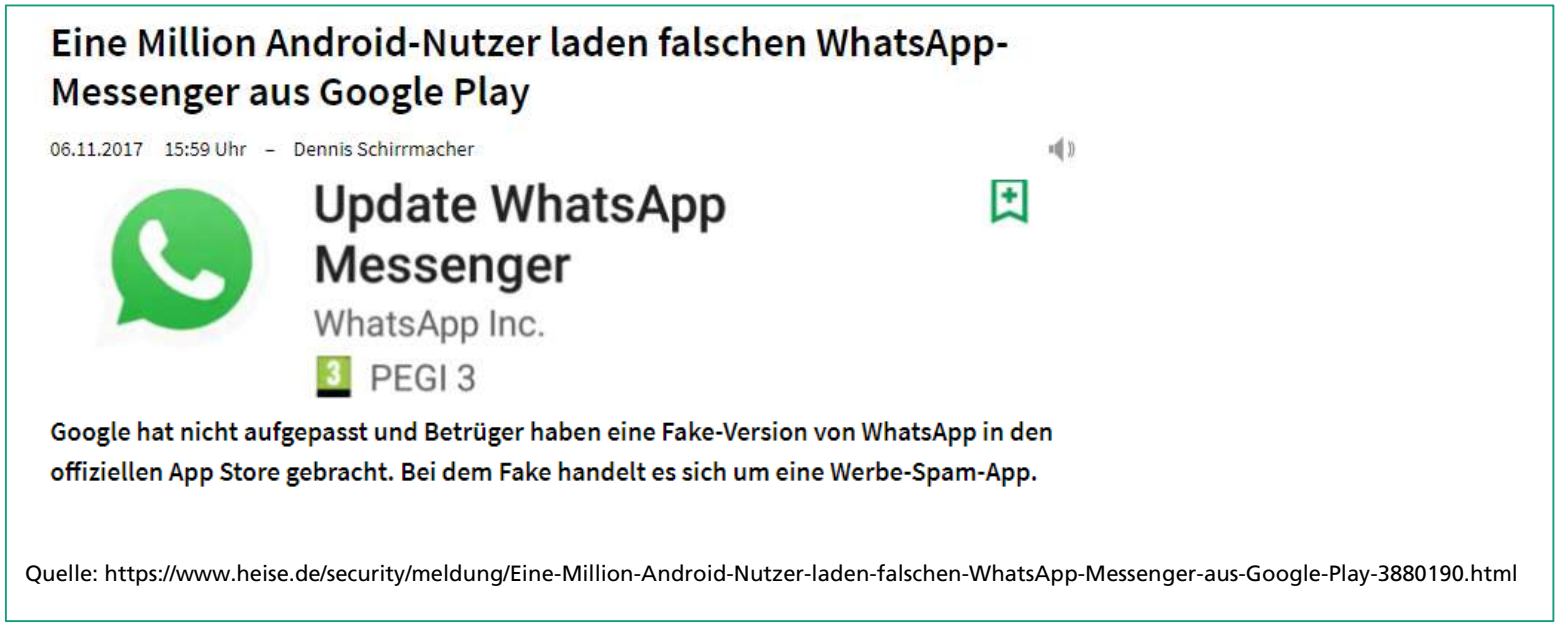
Entwickler kontaktieren

Quelle: https://www.amazon.de/Garmin-Wuerzburg-GmbH-NAVIGON-Europe/dp/B019C5LZX4



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Außerbetriebnahme
Die Gefahr von Fake Apps



Quelle: https://www.heise.de/security/meldung/Eine-Million-Android-Nutzer-laden-falschen-WhatsApp-Messenger-aus-Google-Play-3880190.html

Außerbetriebnahme
Die Gefahr von Fake Apps

Eine Million Android-Nutzer laden falschen WhatsApp-Messenger aus Google Play

06.11.2017 15:59 Uhr – Dennis Schirrmacher

Google hat nicht aufgepasst und Betrüger haben eine Fake-Version von WhatsApp in den offiziellen App Store gebracht. Bei dem Fake handelt es sich um eine Werbe-Spam-App.

Quelle: https://www.heise.de/security/meldung/Eine-Million-Android-Nutzer-laden-falschen-WhatsApp-Messenger-aus-Google-Play-3880190.html

Also:

- Produkt-Abkündigung publik machen
- Produktwebseite aktualisieren ☺
- Apps im Store behalten und als inkompatibel mit allen Geräten markieren

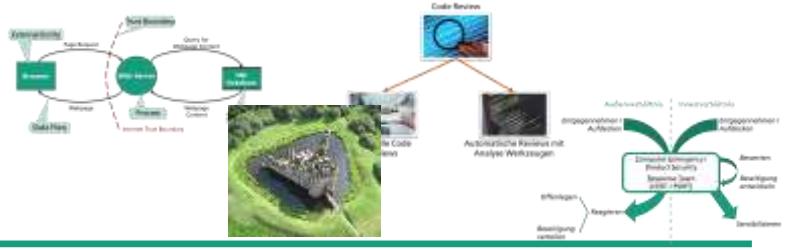
Take Aways

- Security gewinnt zunehmend an Bedeutung…

- … und bleibt eine Herausforderung für viele Unternehmen

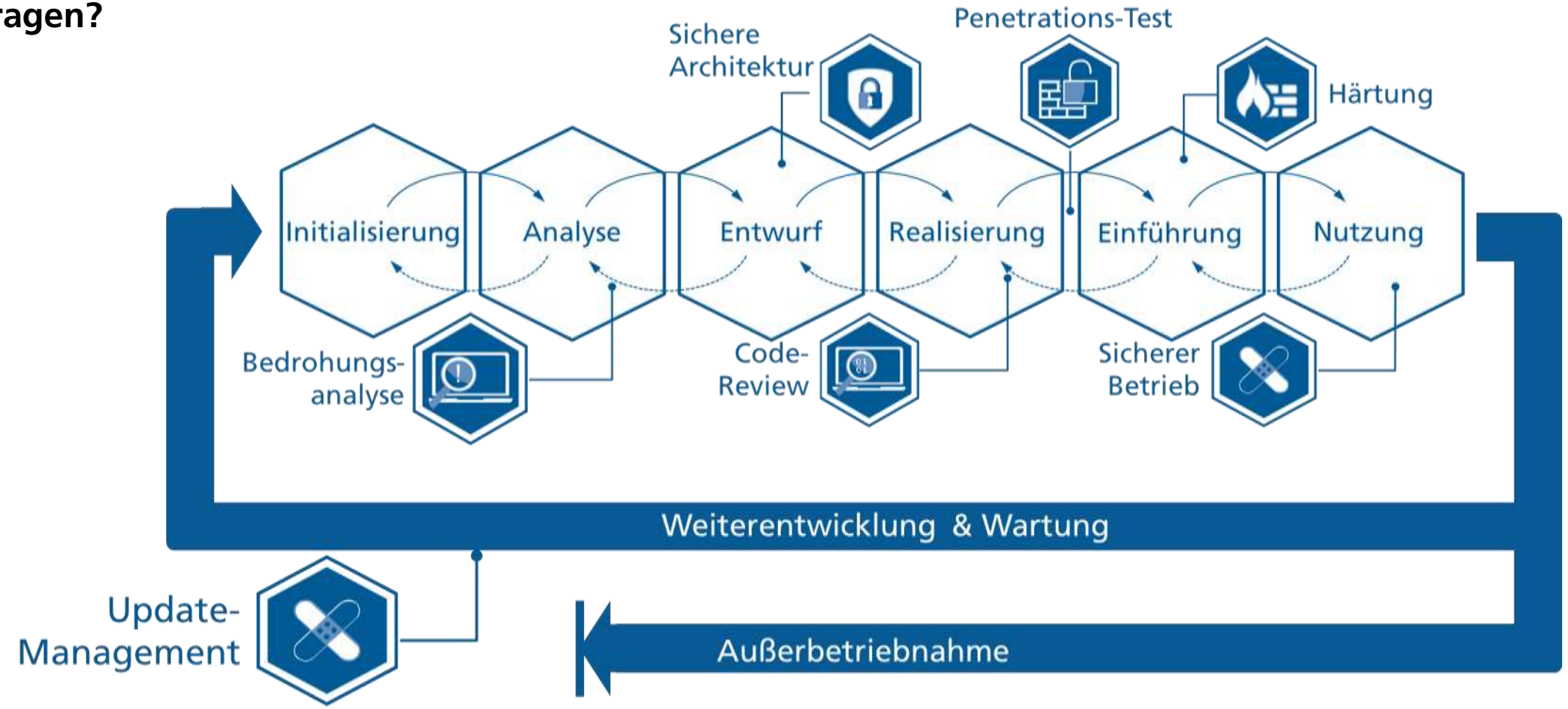
- **Security sollte über den gesamten Prozess berücksichtigt werden**

- Entsprechende Maßnahmen kann jede Organisation durchführen



HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Fragen?



masud.fazal-baqaie@iem.fraunhofer.de
@masudfb

Themenseite: IT-Security am Fraunhofer IEM
https://www.iem.fraunhofer.de/de/forschung/kernkompetenzen/it-security.html

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM

Weiterführende Quellen

Themenseite: IT-Security am Fraunhofer IEM
https://www.iem.fraunhofer.de/de/forschung/kernkompetenzen/it-security.html

Literatur:

Threat Modeling: Designing for Security
Adam Shostack

Software Security: Building Security In
Gary McGraw

Microsoft Security Development Lifecycle (SDL) (for Agile Development) Process Guidance
https://www.microsoft.com/en-us/download/details.aspx?id=29884

PSIRT Services Framework
https://www.first.org/

Werkzeuge:

MS Thread Modeling Tool
*https://www.microsoft.com/en-us/download/details.aspx?id=*49168

CogniCrypt
https://www.cognicrypt.de/

Soot
https://sable.github.io/soot/

FlowDroid
https://github.com/secure-software-engineering/FlowDroid

Phasar
https://phasar.org/

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN
Fraunhofer IEM