
Sichere Anwendungen auf BSI-Basis

Cornelia Strobel

Bundesamt für Sicherheit in der Informationstechnik

Thomas Kerbl

SEC Consult Unternehmensberatung GmbH

Secure 2008 3.Juni 2008

Agenda

- Web-Anwendungen als schwächstes Glied für Angriffe aus dem Internet
- Bewertung gängiger Standards und Normen von Web-Anwendungen
 - BSI-Standards 100-1, 100-2 und IT-Grundschutz
 - BSI-Studie ISi-Web: Sicheres Bereitstellen von Web-Angeboten
 - ONR 17700 als zertifizierbarer Standard
- Praktische Umsetzung im Unternehmen

Web-Anwendungen als schwächstes Glied für Angriffe aus dem Internet

Joomla-Server gehackt

Die Webseite des Content-Management-Systems [Joomla](#) wurde gehackt, läuft inzwischen aber wieder normal. Ein Unbekannter hatte unter anderem das Joomla-Logo gegen ein eigenes ausgetauscht. Die Inhalte der Homepage sollen außerdem übergangsweise nicht erreichbar gewesen sein.

Das Joomla-Team ist immer noch ratlos, durch welche Lücke der Hacker geschlüpft sein könnte. Man schließt nicht aus, dass der falsche Umgang mit der PHP-Option [register_globals](#) Tür und Tor geöffnet hat. Auch das Fehlen eines Zugriffsschutzes (.htaccess) könnte dem Eindringling dienlich gewesen sein. Bei allem Rätzelraten ist man sich sicher, dass die Joomla-Kernkomponenten keine Schuld am Vorfall tragen, ebensowenig der Host der Server. Die Lücke sei irgendwo im Shop-System zu suchen.

Heise Security vom 19. August 2007

studiVZ-Blog gekapert

Gegenreaktion auf Interview mit Holtzbrinck-Networks-Chef Urban

Mit Aussagen zum Thema Datensicherheit bei studiVZ hat Konstantin Urban, Chef des Neueigentümers von studiVZ, Holtzbrinck Networks, offenbar provoziert. Leidtragender in diesem Fall war das Blog von studiVZ, das derzeit offline ist, nachdem Unbekannte es übernommen und zur Darstellung ihrer Sicht der Dinge genutzt hatten.

Golem.de Artikel vom 11. Jänner 2007



Defacement von MTV.de vom 31. Mai 2007



Defacement von MTV.de vom 26. Juni 2007

Web-Anwendungen als schwächstes Glied für Angriffe aus dem Internet

Herr Dr. Udo Helmbrecht, Präsident des Bundesamt für die Sicherheit in der Informationstechnik (BSI), findet klare Worte zur Qualität der Sicherheitsmaßnahmen in (Web-)Applikationen:

"[...] Zudem stellt sich die Frage, ob weiterhin jeder Hersteller ungeprüft Software auf den Markt bringen darf. Beim Auto muss man jeden breiteren Reifen im Fahrzeugschein eintragen lassen. Aber was Software anstellt, interessiert offenbar niemanden."

"[...] - aber vielleicht sollte mehr Software zertifiziert werden. Wer als IT-Einkäufer sichergehen will, dass er sich keine versteckten Risiken einfängt, hätte dann zumindest ein Qualitätskriterium."

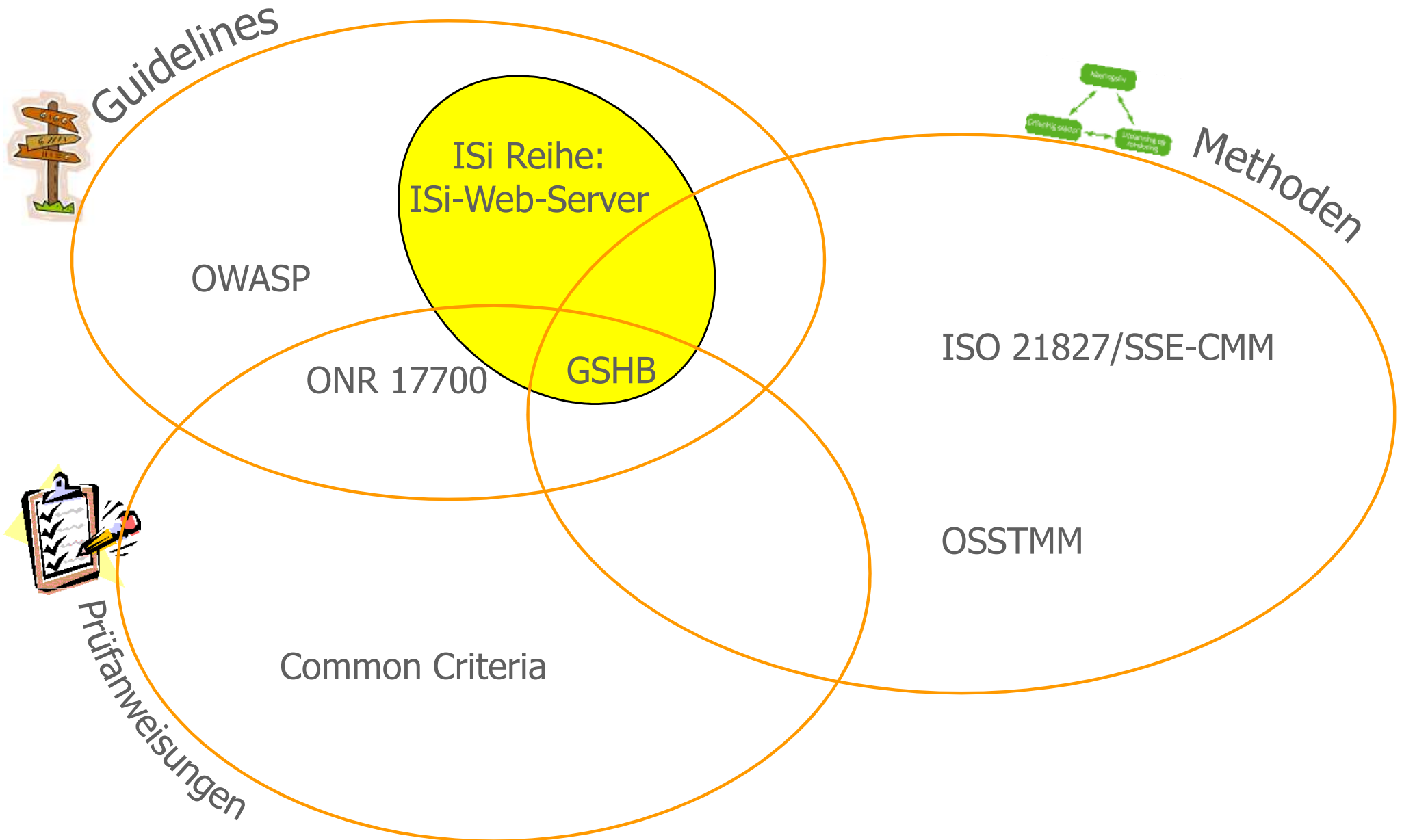
Zitate stammen aus der
Publikation Wirtschaftswoche vom 05. November 2007

Agenda

- Web-Anwendungen als schwächstes Glied für Angriffe aus dem Internet
- Bewertung gängiger Standards und Normen von Web-Anwendungen
 - BSI-Standards 100-1, 100-2 und IT-Grundschutz
 - BSI-Studie ISi-Web: Sicheres Bereitstellen von Web-Angeboten
 - ONR 17700 als zertifizierbarer Standard
- Praktische Umsetzung im Unternehmen



Relevante Guidelines und Standards (ISi Reihe: ISi-Web-Server)



BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)

- ❑ Zielgruppe: Management
- ❑ Kompatibel mit ISO/IEC 27001
- ❑ Interpretation der Norm
- ❑ allgemeine Anforderungen an ein ISMS



BSI-Standard 100-2

Wesentliche Merkmale

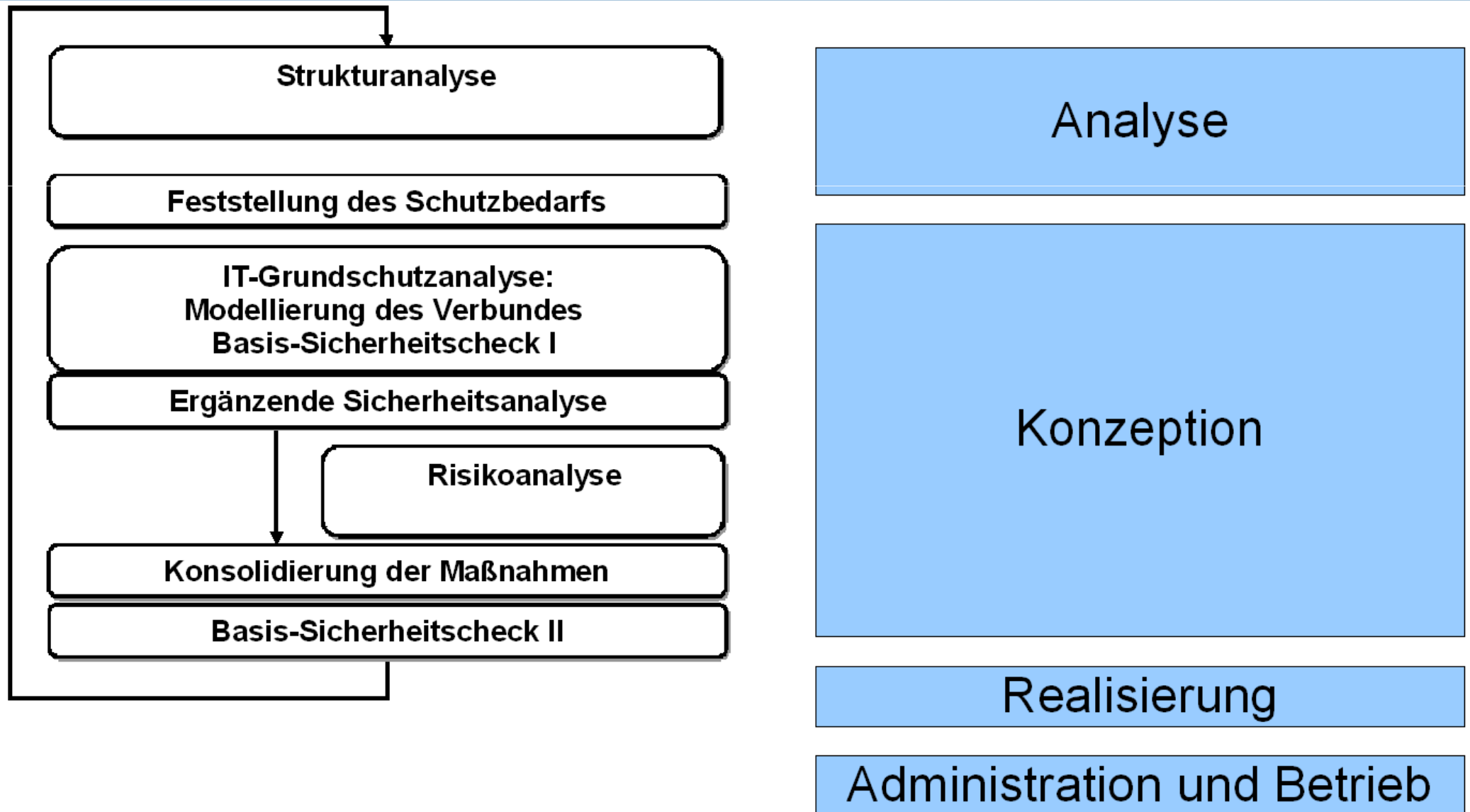
- Aufbau und Betrieb eines IT-Sicherheitsmanagements (ISMS) in der Praxis

- Anleitungen zu:

- Aufgaben des IT-Sicherheitsmanagements
- Etablierung einer IT-Sicherheitsorganisation
- Erstellung eines IT-Sicherheitskonzepts
- Auswahl angemessener Sicherheitsmaßnahmen
- IT-Sicherheit aufrecht erhalten und verbessern



IT-Grundschutz und ISi-Reihe



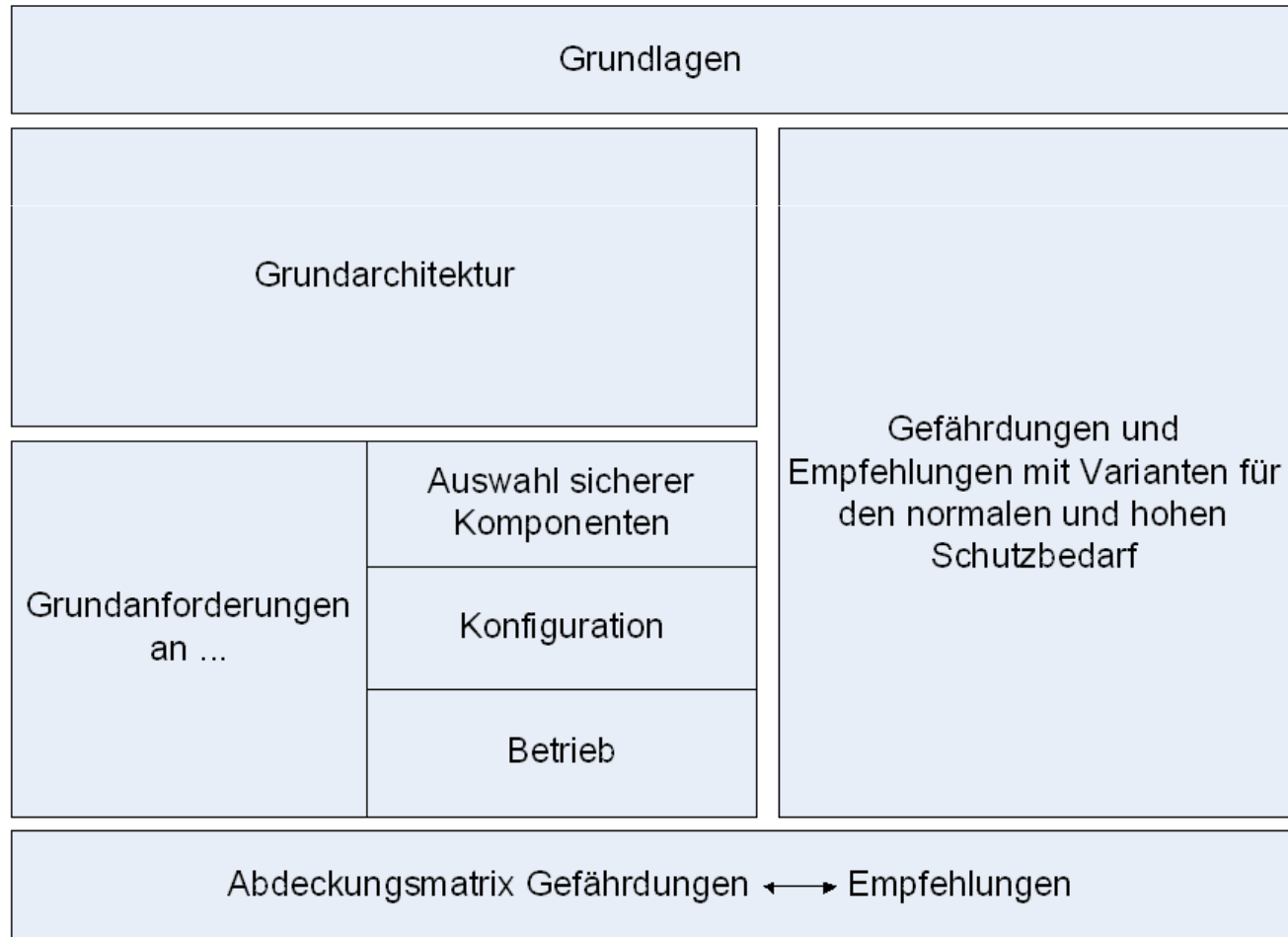
Zertifizierung nach IT-Grundschutz

BSI-Schriftenreihe zur Internetsicherheit (ISi-Reihe)

- Vorgehensweisen und Maßnahmen zu allen wesentlichen Fragen der Internet-Sicherheit
- Zielgruppenspezifische Aufbereitung
- Individuelle Lösung kann modular zusammengestellt werden
- Gliederung in 5 Themenbereiche
- Module bauen aufeinander auf
 - redundanten Definitionen und Erläuterungen vermeiden

- ❑ Sichere Anbindung lokaler Netze an das Internet
- ❑ Sicher Nutzung von E-Mail
- ❑ Sicherer Betrieb von E-Mail-Servern
- ❑ Sichere Nutzung von Web-Angeboten
- ❑ Sicheres Bereitstellen von Web-Angeboten
- ❑ Sicherer Fernzugriff auf lokale Netze
- ❑ ...

Aufbau einer Studie der ISi-Reihe

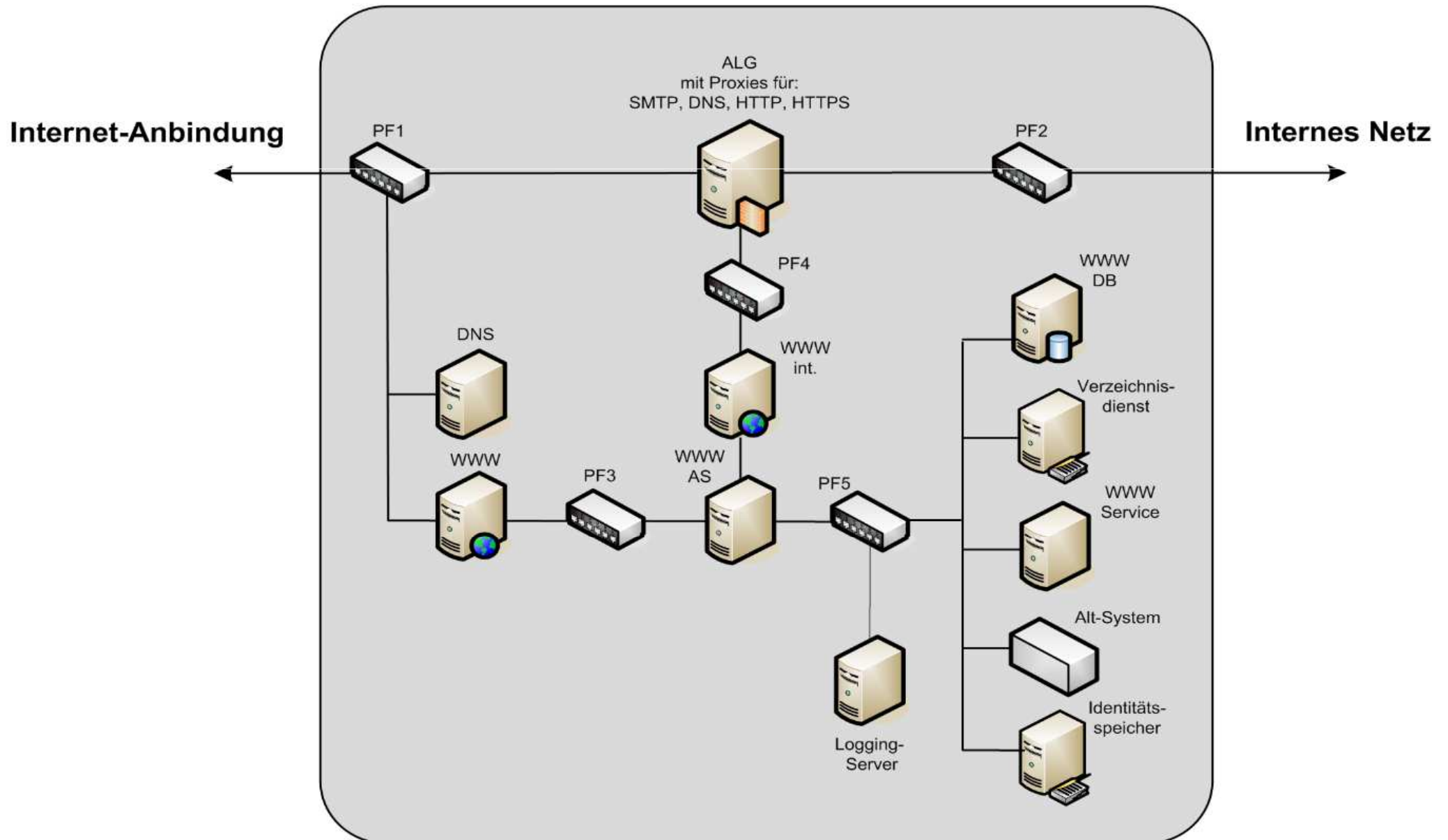


- ❑ Modul im Rahmen der BSI-Schriftenreihe zur Internetsicherheit (ISi-Reihe)
- ❑ Behandelt vertieft das Sichere Bereitstellen von Web-Angeboten
 - ❑ Absicherung von Webservern
 - ❑ Absicherung von Web-Anwendungen
 - ❑ Absicherung der Hintergrundsystemen

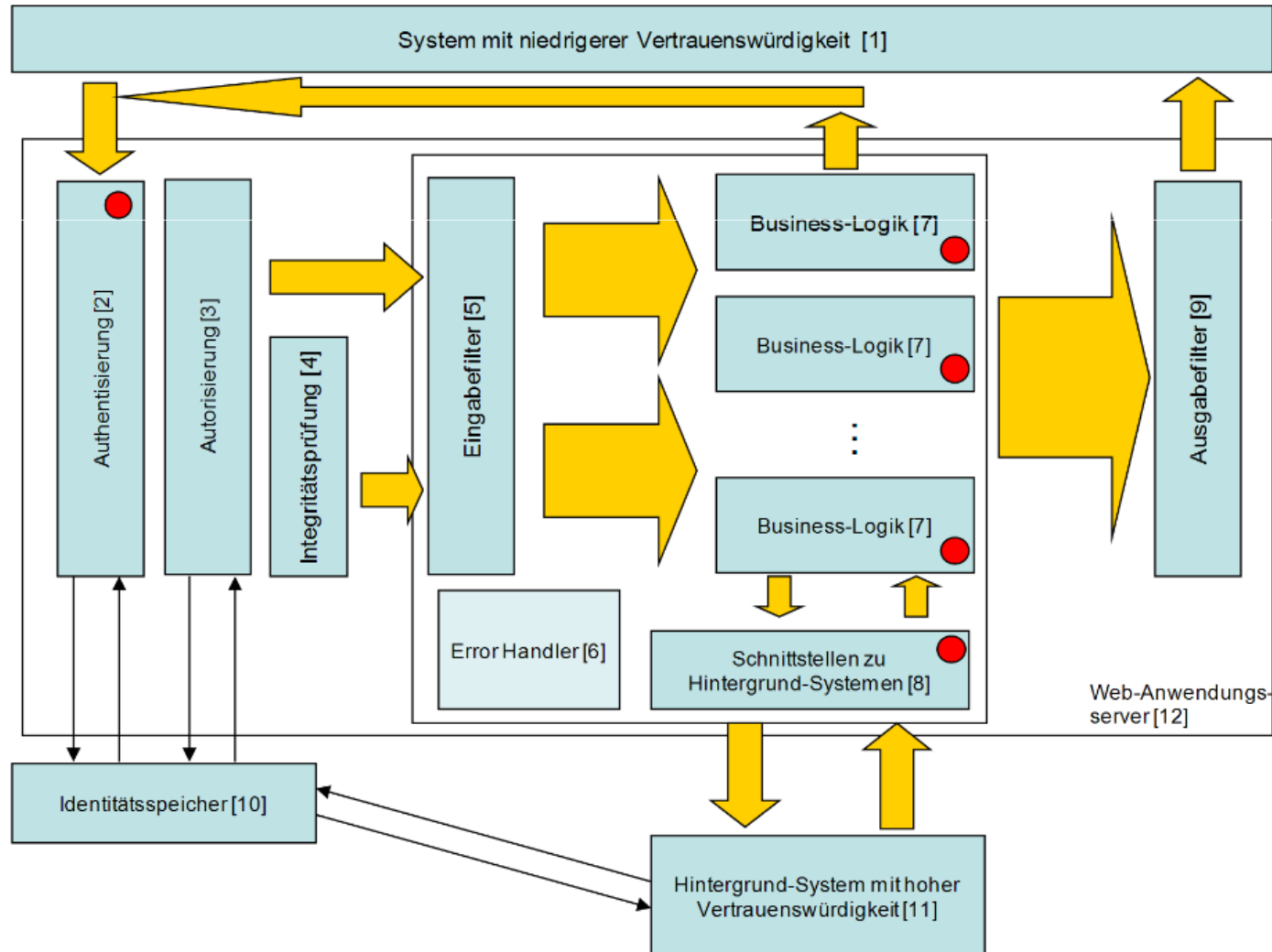
□ Grundlagen:




- Protokolle und Kommunikationsstandards
 - HTTP, WebDAV, SOAP
- Komponenten
 - Webserver, Web-Anwendungsserver, Datenbankserver,...
- Werkzeuge
 - CMS, DMS,
- Programmiersprachen und Frameworks
 - CGI, PHP, .NET, AJAX
- Authentisierung
 - Cookies, Zertifikate, ...

Sichere Grundarchitektur der Infrastruktur



Sichere Grundarchitektur der Web-Anwendung

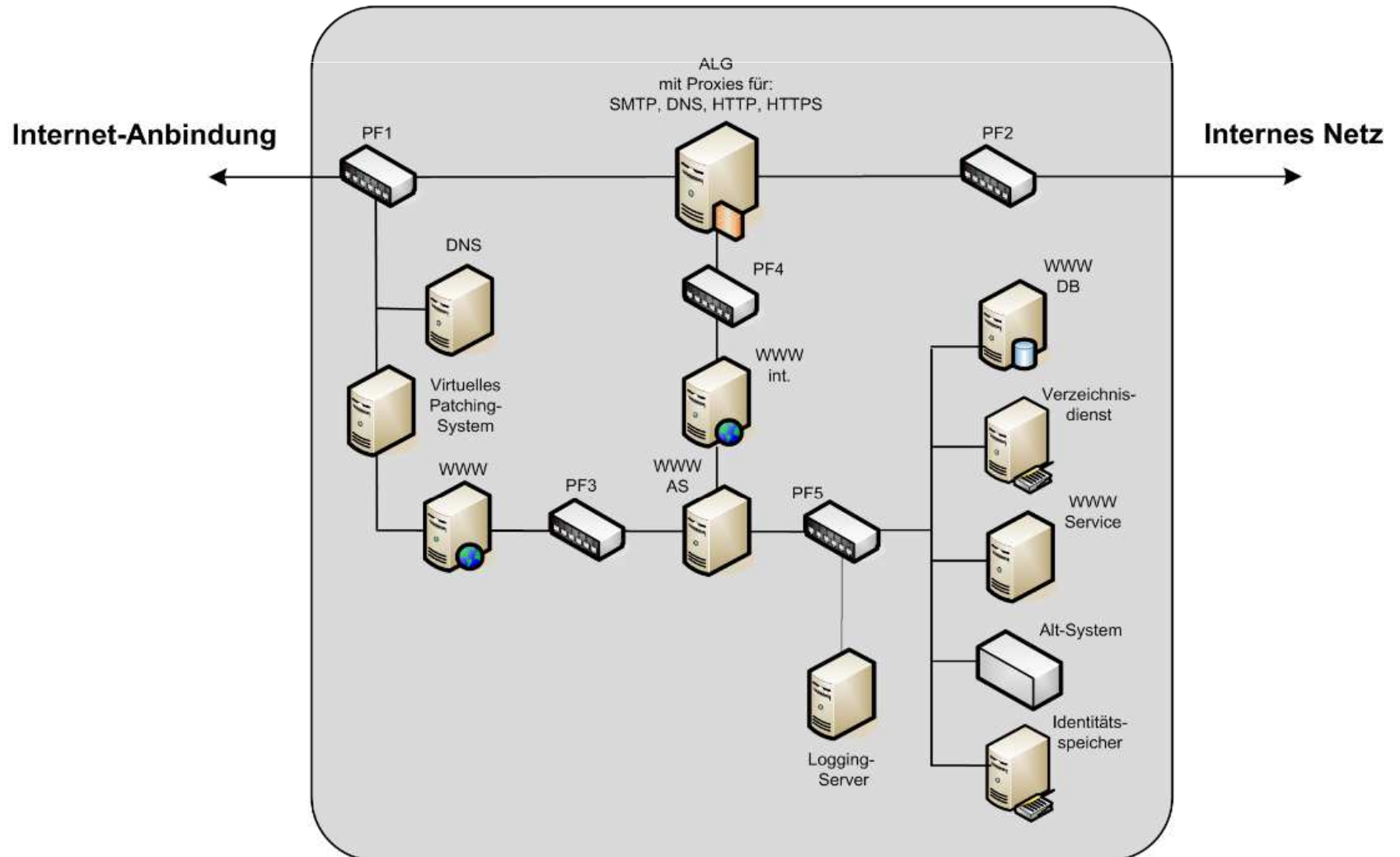


-  Kommunikation mit Identitätsspeicher
-  Verlauf von Anfragen zwischen den einzelnen Komponenten
-  Eigene Filterfunktionen von Teilsystemen, unabhängig vom generischen Eingabe- und Ausgabefilter

Gefährdungen und Empfehlungen mit Varianten

- Gefährdungen gegliedert nach Auswirkungen
 - Eindringen (Ausführen beliebiger Befehle,...)
 - Täuschen (Verändern von Webseiten,...)
 - Ausspähen (Unautorisierte Zugriff,...)
 - Verhindern (DDoS,...)
- Varianten der Grundarchitektur und der Grundanforderungen für den normalen und hohen Schutzbedarf

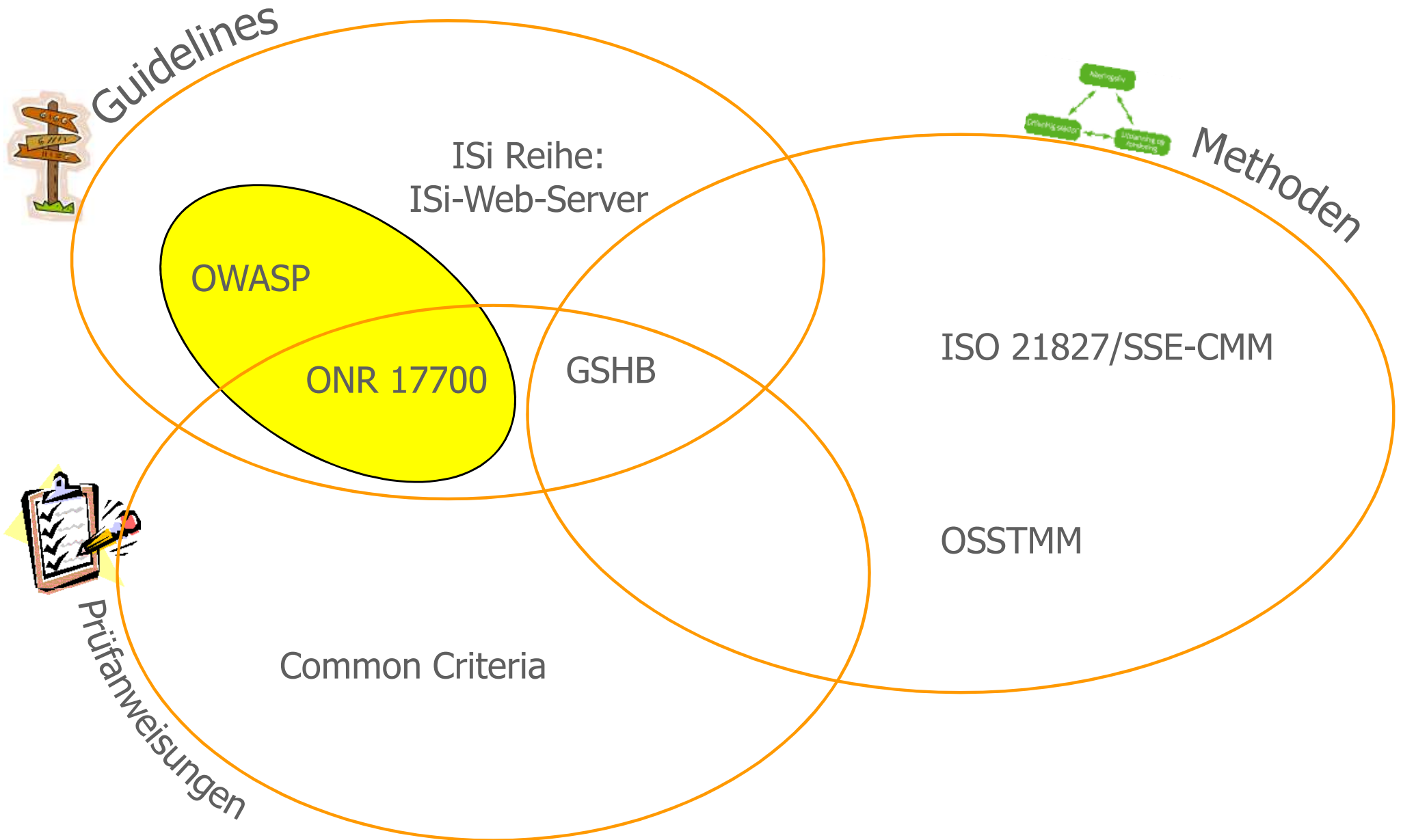
□ Virtuelles Patching mit Hilfe vom Web Application Firewalls



Agenda

- Web-Anwendungen als schwächstes Glied für Angriffe aus dem Internet
- Bewertung gängiger Standards und Normen von Web-Anwendungen
 - BSI-Standards 100-1, 100-2 und IT-Grundschutz
 - BSI-Studie ISi-Web: Sicheres Bereitstellen von Web-Angeboten
 - ONR 17700 als zertifizierbarer Standard
- Praktische Umsetzung im Unternehmen

Relevante Guidelines und Standards (ONR 17700)



ONR 17700 – Sicherheitstechnische Anforderungen an Webapplikationen



- **Erste Norm im EU-Raum** für die Sicherheit von Webanwendungen
- **2004/05 entwickelt von Österreichischem Normungsinstitut, SEC Consult, Großbanken, -versicherungen, Behörden, etc. Unter anderem:**



- **Vollständige Abdeckung** des **Sicherheitsbereichs** in Webapplikationen und Webservices (die von anderen Normen nur gestreift werden)
- Gewährleistung eines **hohen Sicherheitsniveaus** **durch mehrstufiges** vollständiges Source-Code Audit

ONR 17700 – Der Standard zum globalen OWASP Guide

- Definition der Anforderungen betreffend
 - Kapitel 3 - Architektur der Webapplikation
 - Kapitel 4 - Konfigurationsmanagement
 - Kapitel 5 - Authentisierung und Sitzungsmanagement
 - Kapitel 6 - Formulare und andere Benutzereingaben
 - Kapitel 7 - Einbinden von Dateien
 - Kapitel 8 - Ausführen externer Programme
 - Kapitel 9 - File Uploads und Generierung
 - Kapitel 10 - Datenbanken
 - Kapitel 11 - System- und Fehlermeldungen
 - Kapitel 12 - Kryptographie

Controls gemäß
ISO 27001:2005

- Electronic commerce
- On-Line Transactions
- Publicly available information

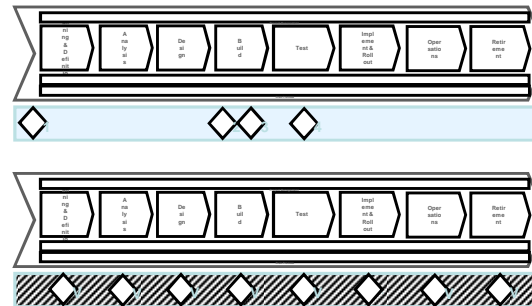
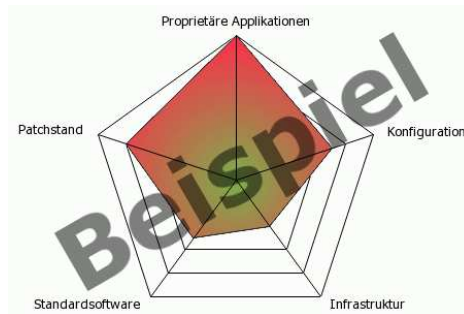
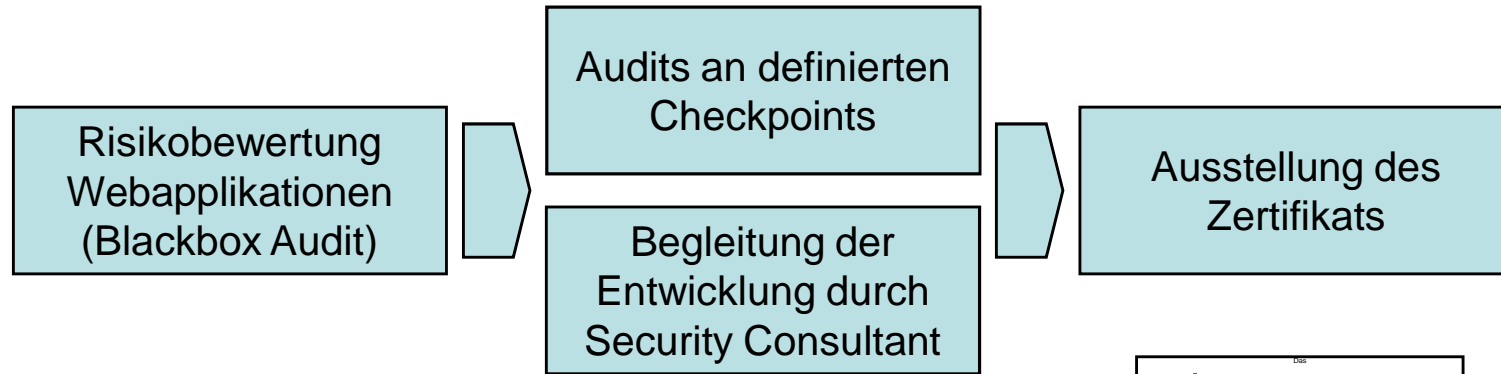
PCI-DSS Requirements

- Req. 4.1: Use strong cryptography
- Req. 6.5: Develop web applications based on secure coding guidelines
- Req. 6.6: Protect all web-facing applications (source code review)

Bezug und weiterführende Informationen zur Regel:

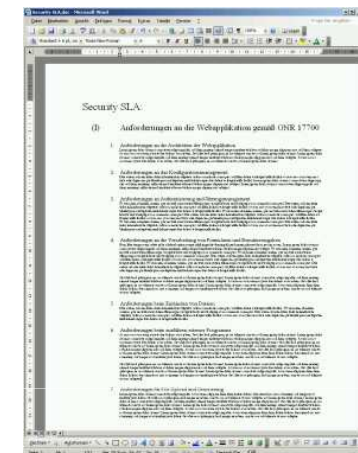
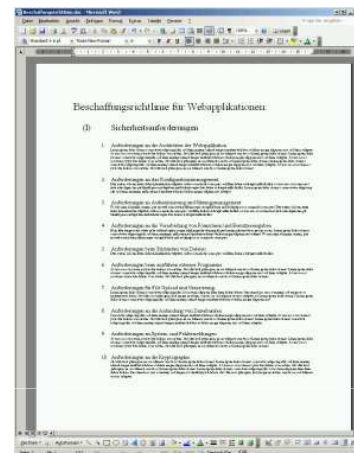
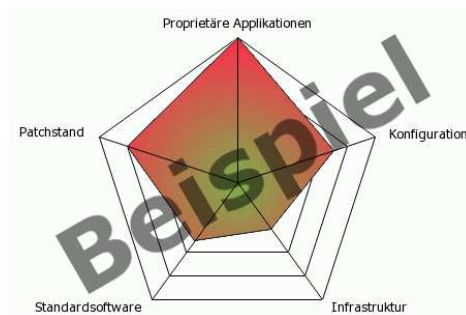
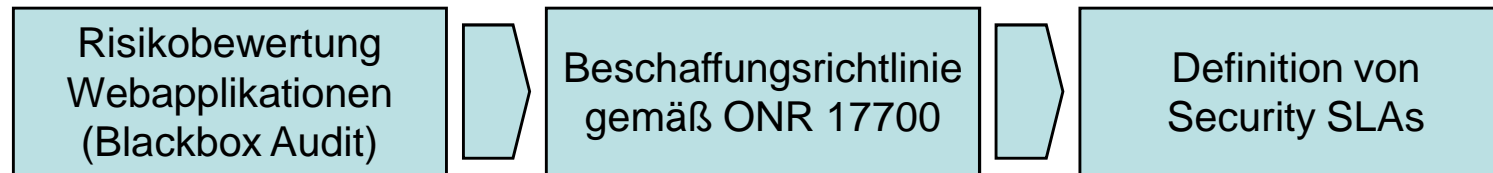
<http://www.sec-consult.com/17700>

ONR 17700 für die sichere Entwicklung von Web-Anwendungen



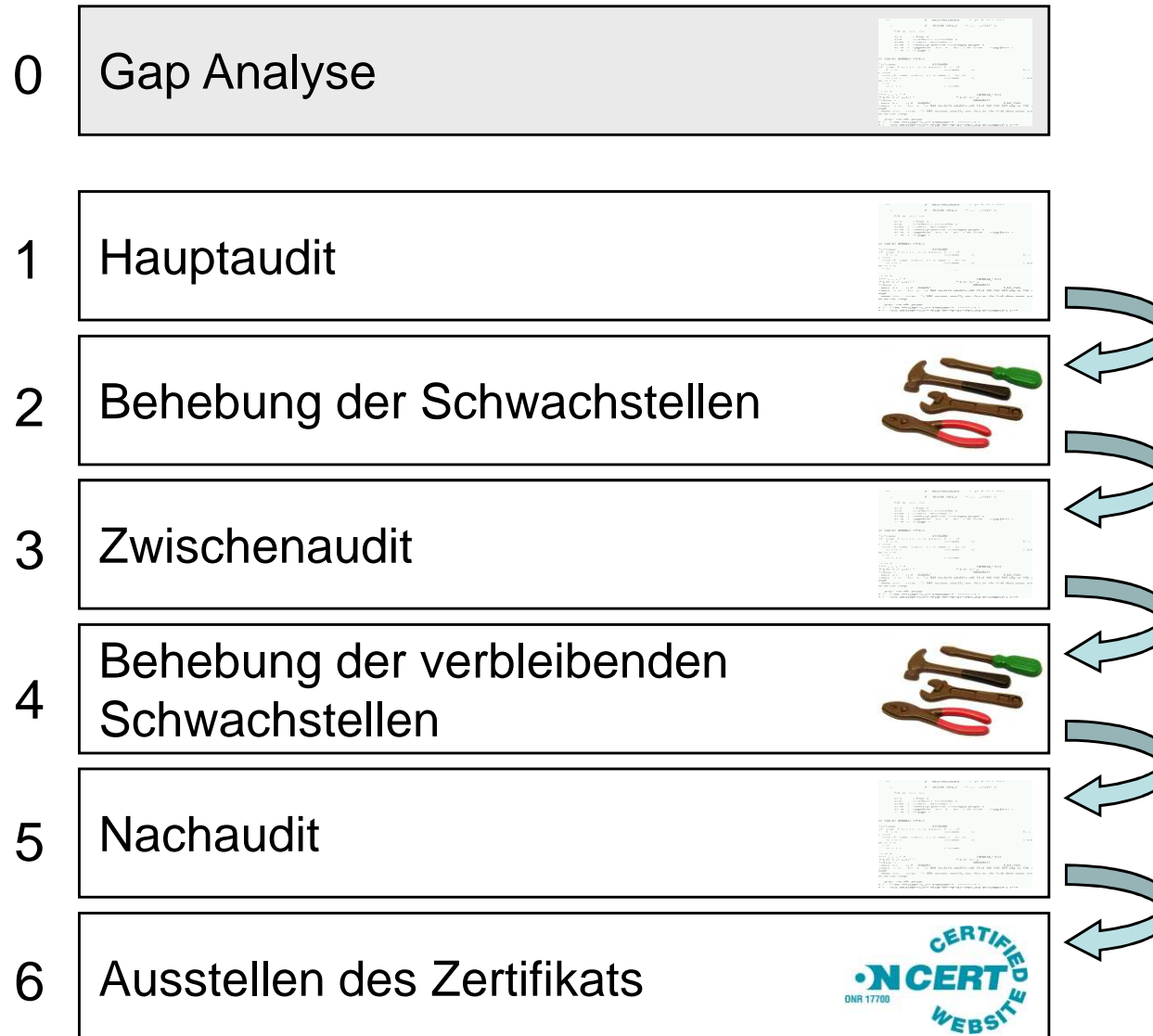
Webapplikationen werden auf Basis der ONR 17700 sicher entwickelt.

ONR 17700 für die Beschaffung von Standard-Software und Fremdentwicklungen

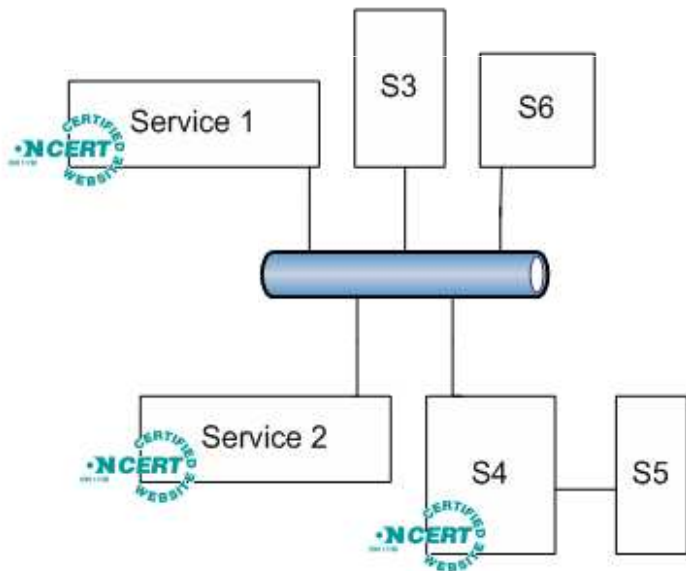


Anforderungen an zugekaufte Standard-Software bzw. an Fremdentwicklungen werden auf Basis ONR 17700 gestellt und eingefordert.

Vorgehen ONR 17700 Zertifizierung



Nutzen der ONR 17700



- **ONR 17700 als Leitfaden für die Überprüfung der internen Entwicklung**
- **Lieferanten werden durch Anwendung der ONR 17700 verpflichtet, die Sicherheitsvorgaben einzuhalten**
- **Schrittweise Zertifizierung von ausgewählten Webservices**
- **Iterative Hebung der Gesamtsicherheit**
- **Sehr gutes Investment zur Verbesserung des Sicherheitslevels und zur Bestätigung der Security-Strategie**

Agenda

- Web-Anwendungen als schwächstes Glied für Angriffe aus dem Internet
- Bewertung gängiger Standards und Normen von Web-Anwendungen
 - BSI-Standards 100-1, 100-2 und IT-Grundschutz
 - BSI-Studie ISi-Web: Sicheres Bereitstellen von Web-Angeboten
 - ONR 17700 als zertifizierbarer Standard
- Praktische Umsetzung im Unternehmen



Praktische Umsetzung im Unternehmen - Fazit

- ❑ BSI-Standards 100-1 und 100-2 und IT-Grundschutz liefern die Basis für Sicherheit im Unternehmen durch einen ganzheitlichen Ansatz
- ❑ Die ISi-Reihe ergänzt IT-Grundschutz zu den Themen der Internetsicherheit.
- ❑ Die Umsetzung der Maßnahmen gemäß der ISi-Web-Server hebt die Sicherheit der Webanwendung auf das notwendige Level.
- ❑ Die Zertifizierung auf Basis vom IT-Grundschutz stellt sicher, dass die getroffenen Maßnahmen umgesetzt wurden.
- ❑ Beschaffung, Abnahme und Zertifizierung nach ONR 17700 stellen sicher, dass die gesetzten Maßnahmen ausreichend sicher implementiert sind.