IT-Sicherheit in Unternehmen: Typische Probleme und Lösungsmöglichkeiten

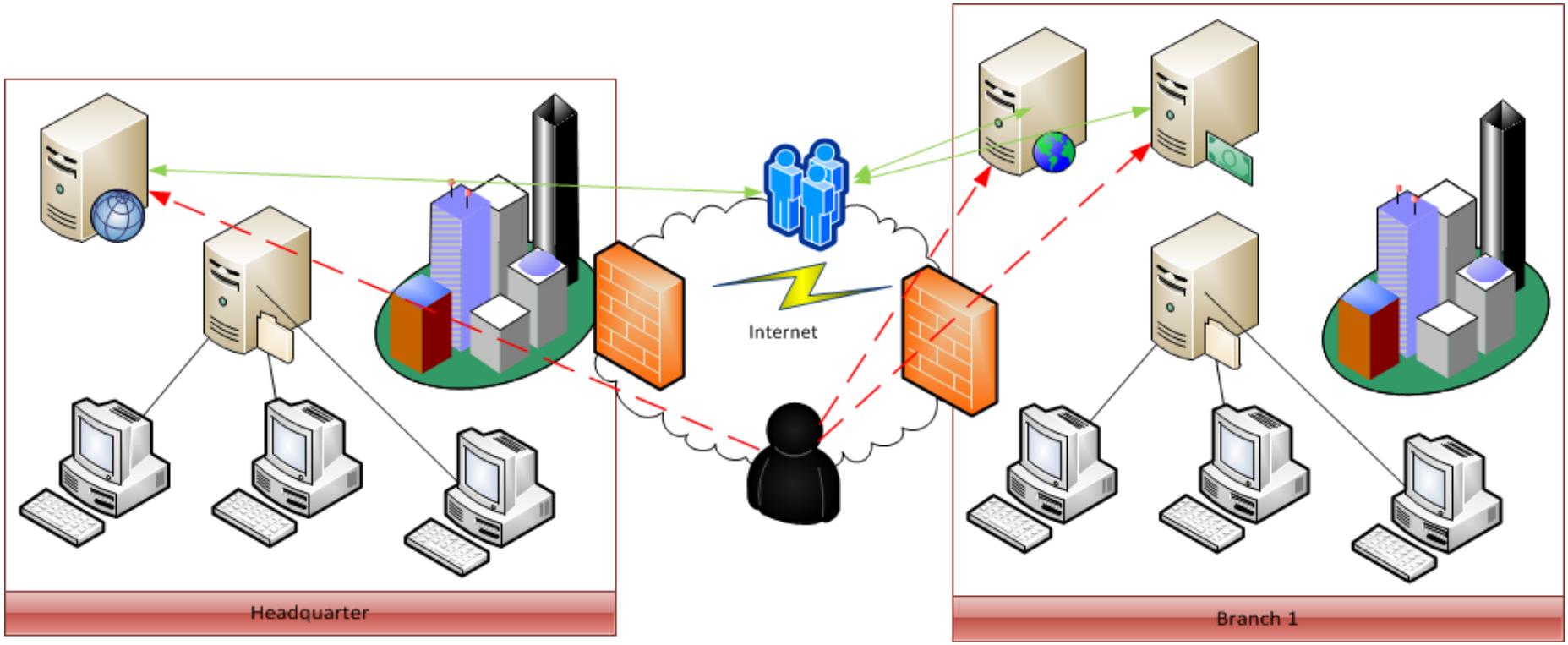
Amir Alsbih

http://www.xing.com/profile/Amir_Alsbih
http://de.linkedin.com/pub/amir-alsbih/1a/19a/b57

OWASP
17.11.2011

INFORMATION SECURITY UND DAS BUSINESS

Firewalls sind nur ein Teil der Lösung



Applikationssicherheit vs. Features

* Deadlines der Projekte
* Implementierungsfortschritt vs. Compliance
* Sicherheit ist eine nicht funktionale Anforderung
* Unterschiedlichstes Know How der Entwickler
* Integration der Lösung in eine (komplexe) Umgebung

Wer Entscheidet und wer zahlt?

Kunden erwarten mehr Sicherheit

* 68% der befragten Unternehmen wurden gebeten ihren Umsetzungsstand hinsichtlich Sicherheitsstandards offenzulegen.
* 61 % der befragten Unternehmen, entdeckten erhebliche Bemühungen in deren Netzwerke einzudringen.

Quelle: Information Security Breaches Survey 2010 Pricewaterhouse Coopers

Aussagen zum Thema Sicherheit

*„[…] wir haben Firewalls […]“

*„[…] wir verwenden SSL […]“

*„[…] unsere Leute sind clever, die machen keine Fehler […]“

*„[…] ich habe eine D&O Versicherung […]“

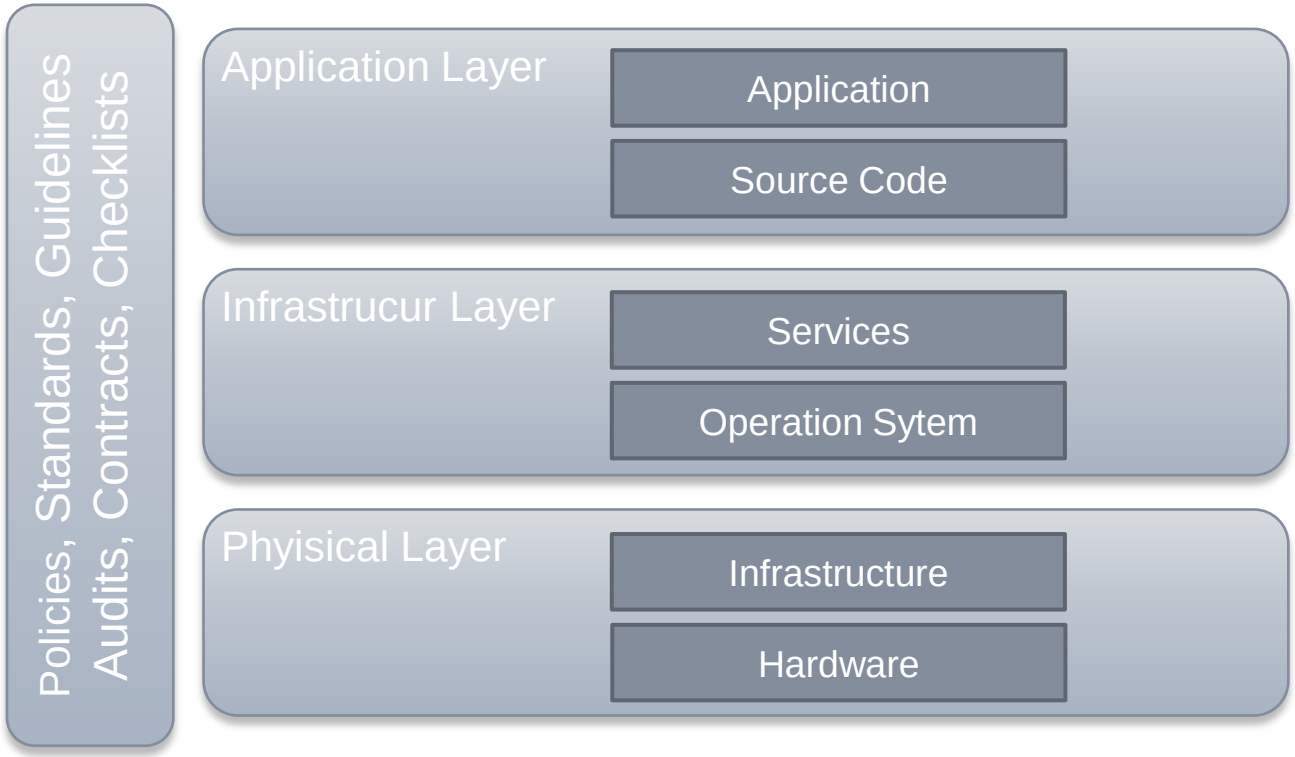
Die Geschäftsführung haftet, sofern ein Schaden aufgrund nicht eingehaltener Best-Practices auftritt.

TECHNOLOGIE, PROZESSE UND MENSCHEN

Hacken wird immer einfacher

Demo

Absicherung aller Ebenen



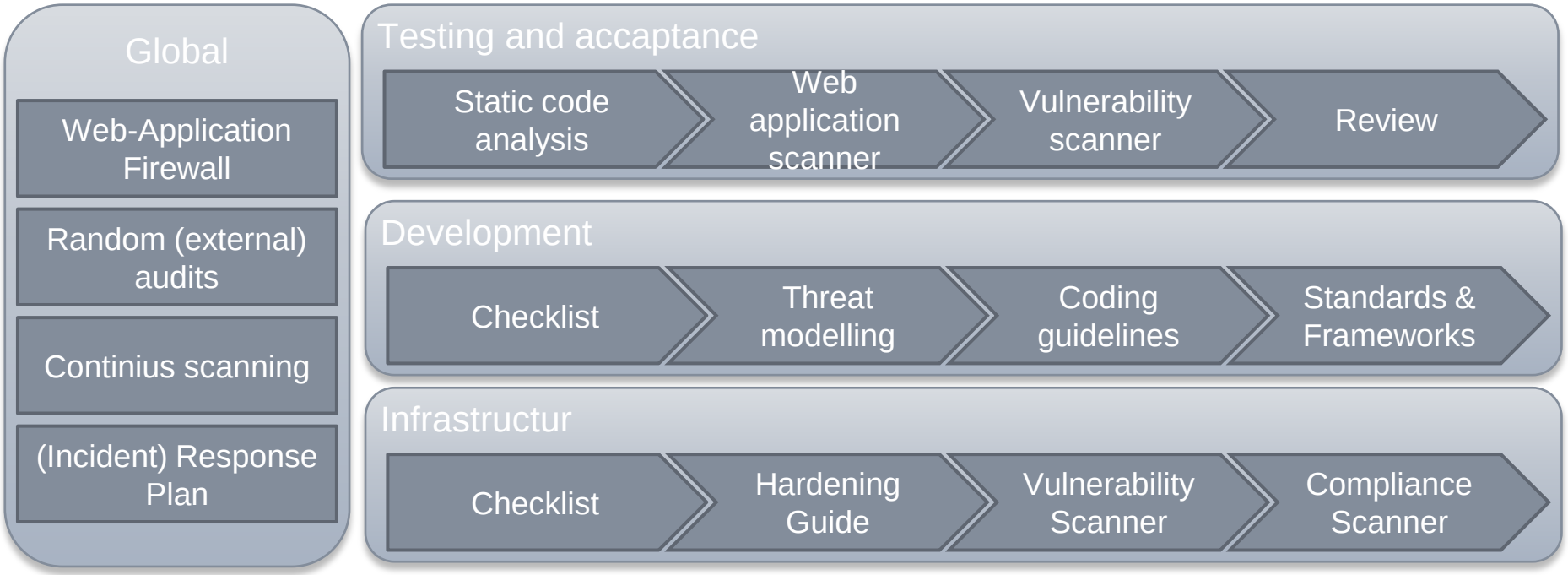
Verfügbare Orientierungshilfen

* Mozilla Secure Coding Guidelines
* ISO 27001, IT-Grundschutz
* Center for Internet Security (CIS)
* OWASP, BSIMM, Microsoft SSDLC

Die Basis für Sicherheit

Nr.	Anforderung	Status	Fachlich Verantwor	SvE	SpE	SnE	N/A	Begründung
REQ 01	Vertrauliche Informationen DÜRFEN NICHT im „localStorage“ oder „sessionStorage“ abgelegt werden.	offen						
REQ 02	Bei der Verwendung von Web SQL MÜSSEN „prepared statements“ verwendet werden.	offen						
REQ 03	Bei der Verwendung von Web SQL MUSS Output encoding vor dem schreiben und lesen von Daten erfolgen.	offen						
REQ 04	Vertrauliche Daten DÜRFEN NICHT in lokalen (Clientseitig) Web SQL Datenbanken abgelegt werden.	offen						
REQ 05	Vor dem Anlegen einer lokalen (Clientseitig) Datenbank MUSS der Benutzer um Erlaubnis gefragt werden.	offen						
REQ 06	Sofern sensible Daten gespeichert werden, MUSS dies über SSL erfolgen.	offen						

Ausschnitte eines möglichen Wegs



Kostenfreie Tools ermöglichen einen Anfang

* OWASP Secure Coding Practices, Mozilla Secure Coding Guidelines
* Open Vulnerability Assessment System (OpenVAS)
* Wikto & Nikto
* W3AF, SkipFish, GrendelScan
* Anti-Cross Site Scripting (Anti-XSS) Library, OWASP AntiSamy, OWASP CSRFGuard
* FindBugs, FxCop, Code Analysis for C/C++
* ModSecurity

Sicherheit muss unabhängig sein

* Funktionsweise der Informationssicherheit analog zu einer Internen Revision, Bauaufsicht, TÜV.
* Einhaltung und Umsetzung der Vorgaben durch die Geschäftsbereiche.
* RACI Matrix für Projekte.
* Aufnahme einer „Ampel“ für Sicherheit in den Projektreports.

Die Sicherheitssteuer

* Information Security Budget 6-9% des IT Budget
  (Source : PWC INFORMATION SECURITY BREACHES SURVEY 2010)
* Sicherheitssteuer 3-20% des Projekt Budget.

Das eigene Budget für die globale Sicherheit, die „Steuer" für die Sicherheit der Projekte.

An die Externen denken

* Entwicklung, Installation, Betrieb und Wartung?
* Einbindung der Infrastruktur in das Vulnerability Management?
* Prozesse und Praktiken um Sicherheitslücken zu vermeiden?
* Prozesse zu Handhabung und Behebung von Sicherheitslücken?
* Information über Sicherheitslücken und wie auf diese reagiert wurde?
* Information über die ungekürzten und ungeschwärzten Prüfberichte von Pentrationstests und Sicherheitsreviews?
* Audit Recht auch von beauftragten Unternehmen, Kunden oder andere berechtigten Stellen?
* Untersagung des Zugangs und der Durchführung von Tätigkeiten mit Ausnahme der notwendigen?
* Pönalen für Mängel?

" Niemand braucht sich auch nur die geringsten Sorgen zu machen. Die wasserdichten Abteilungen der Titanic können das Schiff für unbegrenzte Zeit über Wasser halten."

~ der Zahlmeister des britischen Passagierschiffs RMS Titanic