Protect7

Software Schwachstellen

am Beispiel - SQL Injection

Inhalt

Einführung

- Warum ist Sicherheit ein Software Thema?
- Sicherheit in heutigen Softwareprodukten & Trends
- OWASP Top 10 Kategorien

Hacking Demo

- SQL Injection: der Weg zu den Daten oder dem System

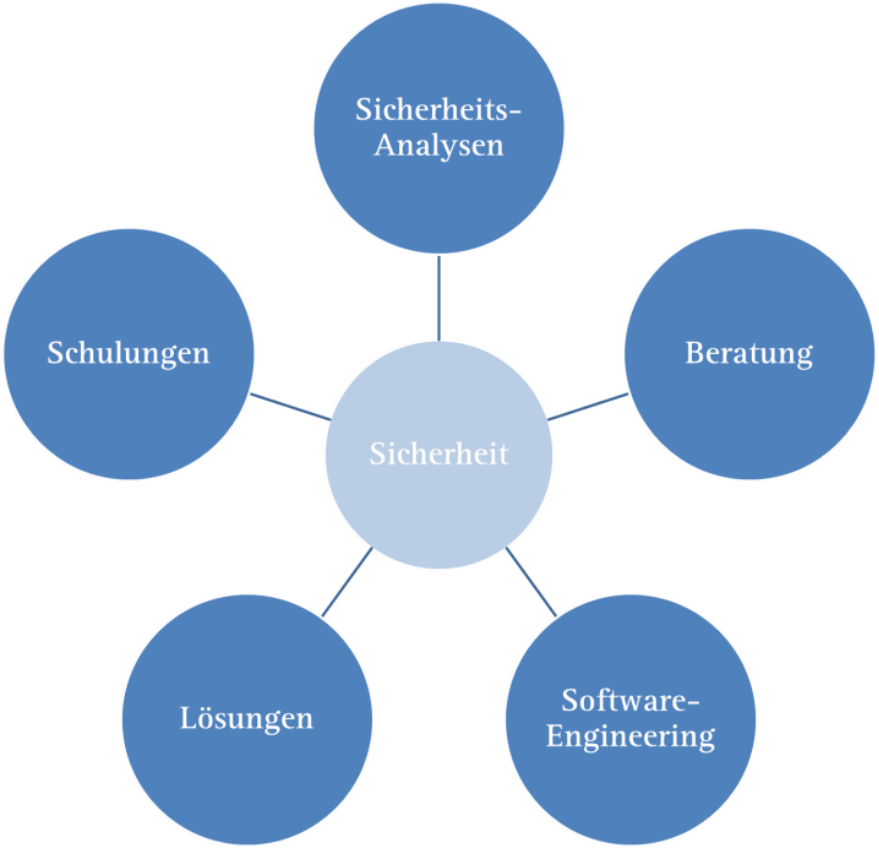
Massnahmen zur Förderung der Sicherheit in Software

- Sicherheit im Software Lifecycle
- Web Application Firewall
- Penetration Test

Über Protect7

Protect7 ist spezialisiert auf Sicherheitsanalysen, Beratung für die Absicherung von Applikationen, sowie sicheres Software-Engineering.

Wir unterstützen unsere Kunden bei der Entwicklung und Implementierung von Applikationen (Lösungen) und sorgen für einen zuverlässigen Schutz vor Missbrauch und Datendiebstahl.



Einführung

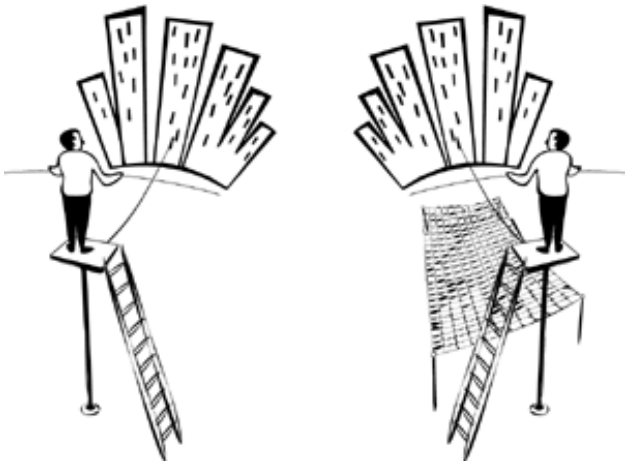
- Warum braucht es sichere Software?

Warum brauchen wir sichere Software

Oft ist es gar nicht möglich, “Business” zu tätigen ohne Software. Software würde wiederum nicht existieren ohne Business.

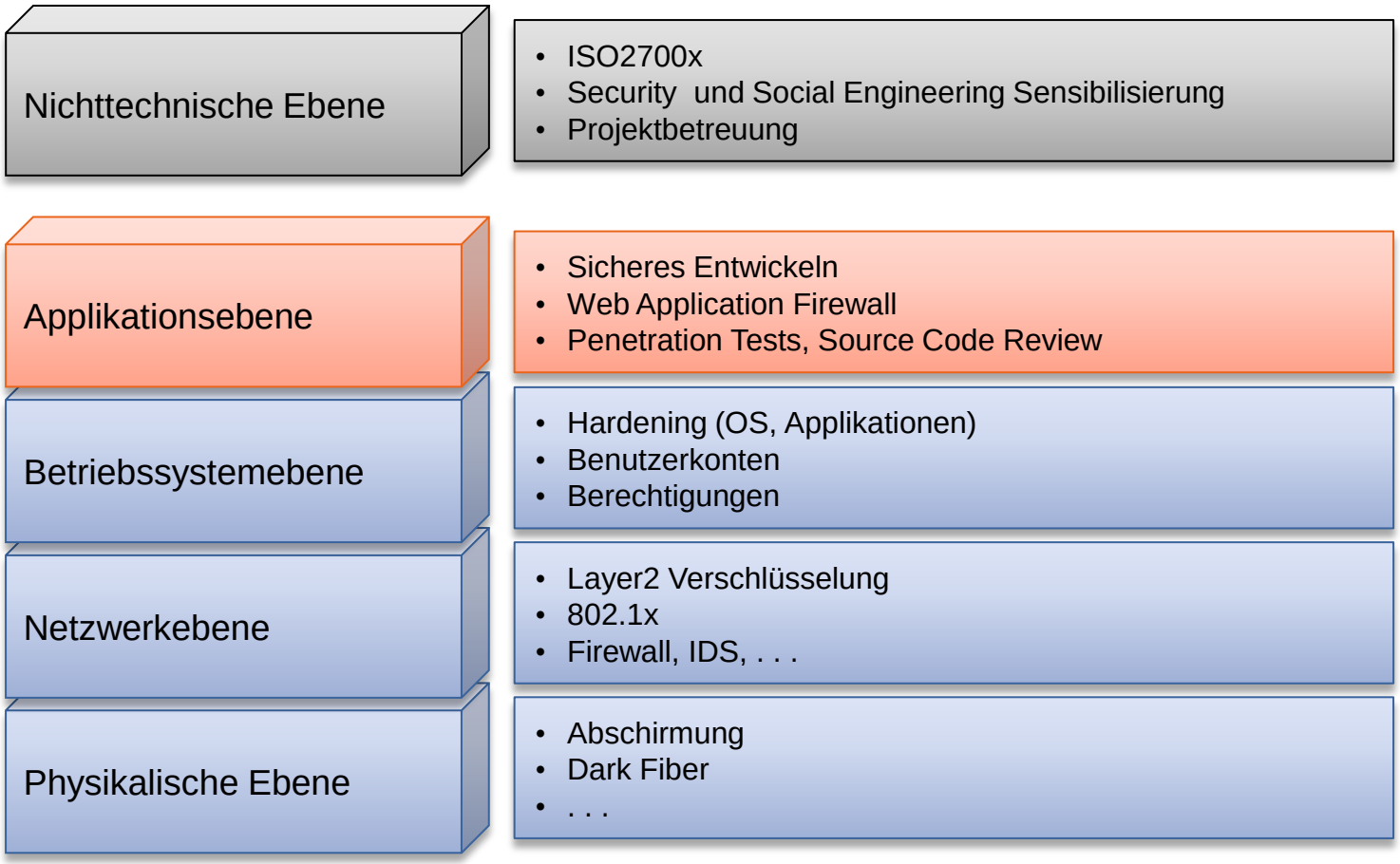
- Das Unternehmen lebt von seinen Geschäften
- Software unterstützt das Geschäft oder macht es erst möglich
- Software zeichnet sich grundsätzlich durch seine Funktionalität aus
- Korrekt funktionierende Software ist für ein Unternehmen sehr wichtig

«Software ist ein Bestandteil vom Business Risiko»



Security Layers

Viele Schwachstellen und die Angriffe um diese auszunutzen, sind auf dem Application Layer. Heutige Massnahmen wirken jedoch nicht auf diesem Layer.



Sicherheit in heutigen Software Produkten

Sicherheitsvorfälle und Trends

Cyberdelikte – bekannt aus der Presse

« Vorige | Nächste »

06.01.2014 12:20

Alert! Yahoo als Virenschleuder: Yahoo.com griff europäische Besucher an

vorlesen / MP3-Download

Yahoo.com wurde von Online-Kriminellen als Virenschleuder missbraucht. Die IT-Sicherheitsfirma Fox-IT hat auf dem Portal speziell präparierte Werbeanzeigen entdeckt, welche die Besucher auf Angriffsseiten des Exploit-Kits umleiteten. Dort wurden die Rechner der Besucher durch Sicherheitslücken in älteren Java-Versionen attackiert. Hat das Exploit-Kit ein Schädlinge wie etwa den Onlin gefunden, hat es laut Fox-IT diverse platziert. ZeuS auf dem Opferrechner

Hacker dringen in Schengen-Datenbank ein

Hackern ist es gelungen, die Schengen-Datenbank zu knacken und 1,2 Millionen Datensätze zu kopieren. Die Angreifer sind mittlerweile gefasst.

« Vorige | Nächste »

13.04.2014 12:56

Heartbleed-Worstcase: Server-Schlüssel kann ausgelesen werden

vorlesen / MP3-Download

Bisher war nicht ganz klar, ob der geheime Schlüssel eines Servers tatsächlich real gefährdet ist. Das US-Unternehmen CloudFlare setzte deshalb einen verwundbaren Server auf und forderte die Community auf, den privaten Schlüssel zu stehlen.

Hacker erbeuten 70 Millionen Kundendaten

Beim Hacker-Angriff auf die US-Kaufhauskette Target wurden mehr Daten geklaut, als bisher vermutet. Laut Angaben von Target griffen die Unbekannten bis zu 70 Millionen Kundendaten ab.

« Vorige | Nächste »

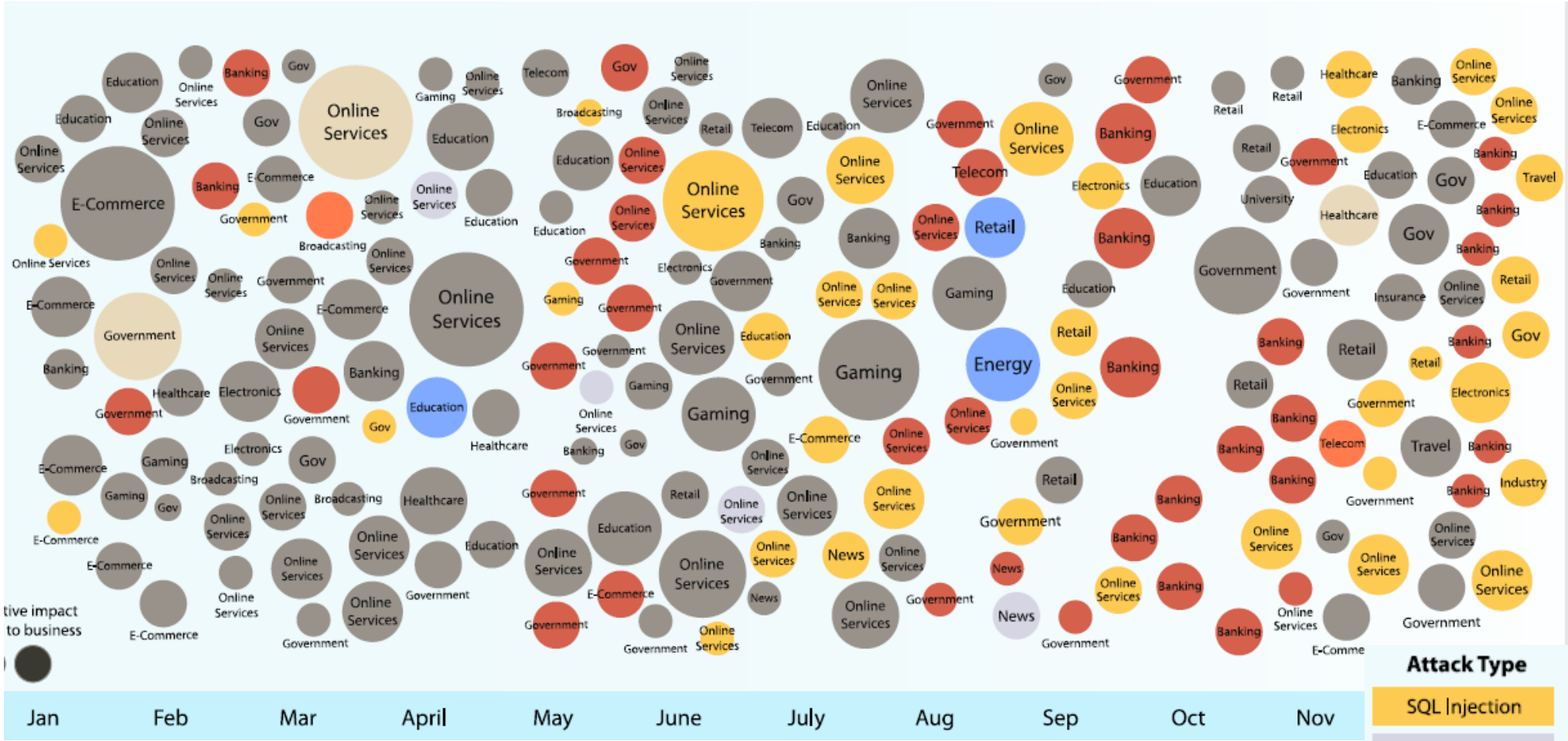
03.01.2014 00:07

Mysteriöse Backdoor in diversen Router-Modellen

vorlesen / MP3-Download

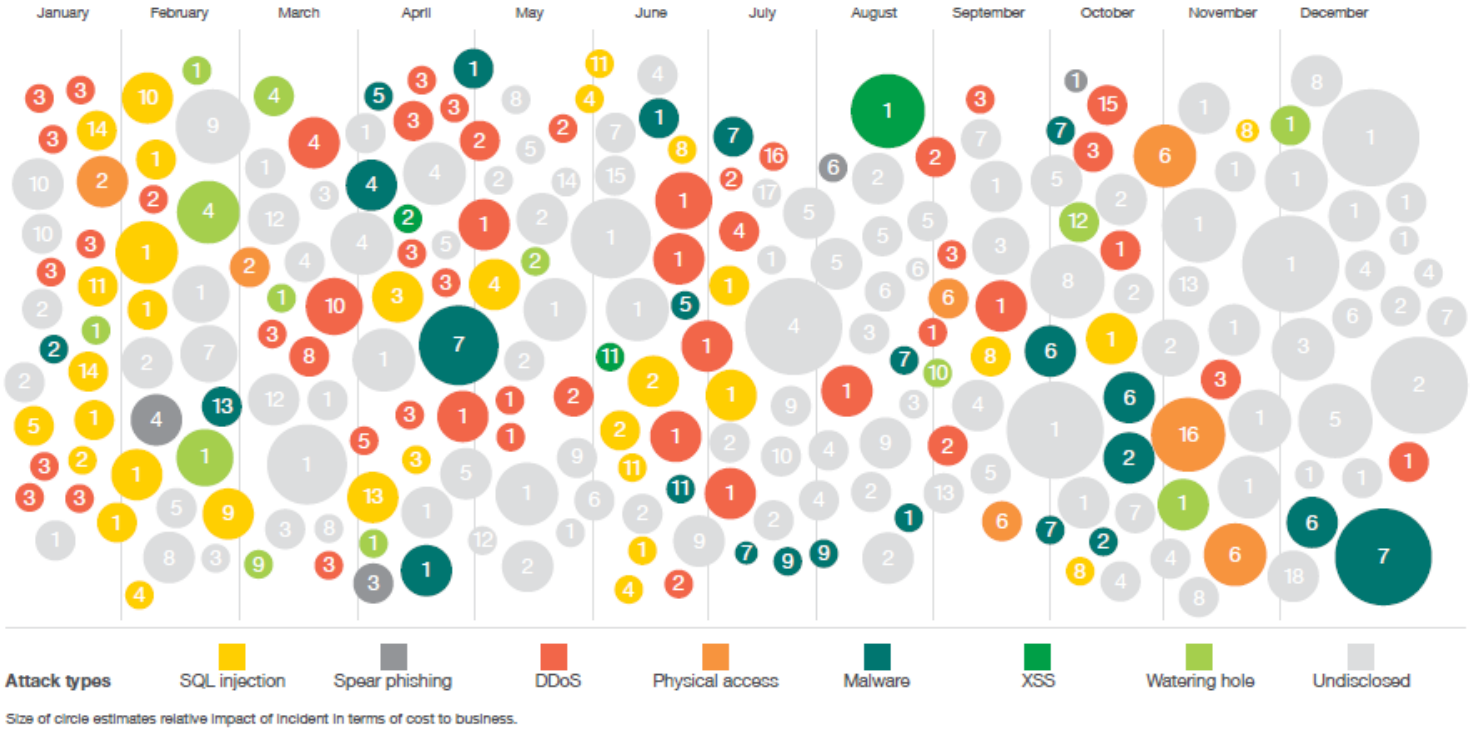
Auf einige Routern von Linksys und Netgear läuft offenbar ein undokumentierter Dienst, über den man unter anderem die Konfiguration einschließlich der Klartext-Passwörter auslesen und auch manipulieren kann. Es besteht die Möglichkeit, dass auch Geräte anderer Hersteller betroffen sind.

Die grössten Sicherheitsvorfälle 2012



Quelle: IBM Internet Security Systems X-Force® 2012 Trend und Risk Report

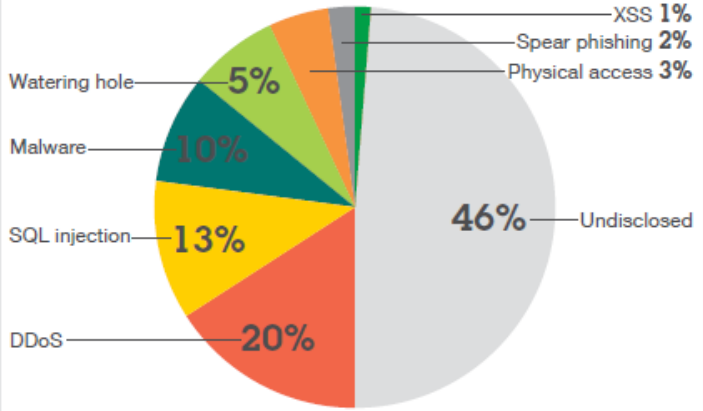
Die grössten Sicherheitsvorfälle 2014



Most-commonly attacked industries

28%	Computer Services (1)
15%	Government (2)
12%	Financial Markets (3)
9%	Media & Entertainment (4)
7%	Education (5)
5%	Healthcare (6), Retail (7), Telecommunications (8)
3%	Consumer Products (9)
2%	Non-Profit (10), Automotive (11), Energy & Utilities (12), Professional Services (13)
1%	Industrial Products (14), Travel & Transportation (15), Wholesale Distribution & Services (16)
<1%	Aerospace & Defense (17), Insurance (18)

Most-common attack types



Quelle: IBM Internet Security Systems X-Force® 2014 Trend und Risk Report

Wirtschaftsspionage – klein bis gross

Hacker steigen bei Lockheed Martin ein

vorlesen / MP3-Download

Bislang unbekannten Hackern soll es laut der Nachrichtenage… sein, in das Netzwerk von Lockheed Martin sowie einigen anderen … beauftragten Firmen einzubrechen. Ermöglicht haben dies angeblich die … Hackerangriff im März erbeuteten Informationen über die SecurID -Produkte des … Spezialisten RSA. Bislang ist unklar, ob die Hacker an wertvolle Informationen gelange… konnten. Die Tatsache, dass in allen Netzwerken Unterlagen zu aktuell eingesetzten … sowie in der Entwicklung befindlichen Waffensysteme gespeichert sind, lässt aber nichts … Gutes erahnen. Weder das Militär noch RS… erten sich bislang zu den Vorfällen.

24.02.2013 14:47

Berichte: Hacker griffen Firmen und Behörden an

« Vorige | Nächste »

vorlesen / MP3-Download

Verfassungsschützer haben im vergangenen Jahr mehr als 1000 Angriffe chinesischer Hacker auf Computer deutscher Bundesbehörden registriert. Das berichtet das Nachrichtenmagazin *Focus* unter Berufung auf den Inlands-Geheimdienst. Auch der *Spiegel* meldet, der Verfassungsschutz habe 2012 fast 1100 digitale Angriffe ausländischer Nachrichtendienste registriert. Hinzu kämen Ausspähaktionen in deutschen Unternehmen.

Weiteres Beispiel:
Mehrjährige nicht-öffentliche Entwicklung eines Produktes aus dem Bereich des Maschinenbaus steht vor dem Abschluss. Noch bevor das Produkt der Öffentlichkeit vorgestellt wird, stellt ein Mitbewerber ein offensichtlich baugleiches Produkt auf einer deutschen Fachmesse aus.

Wirtschaftsspionage

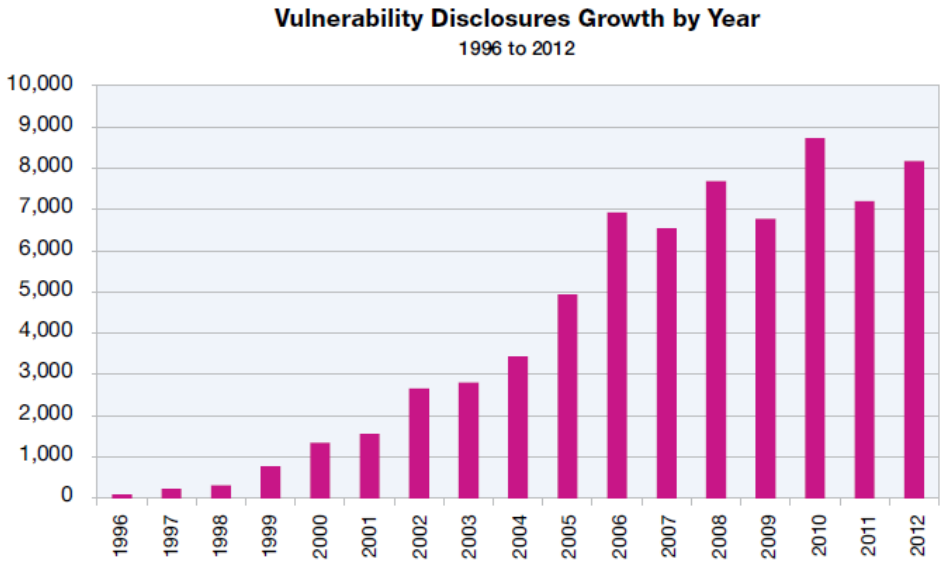
Lockheed USAF F22

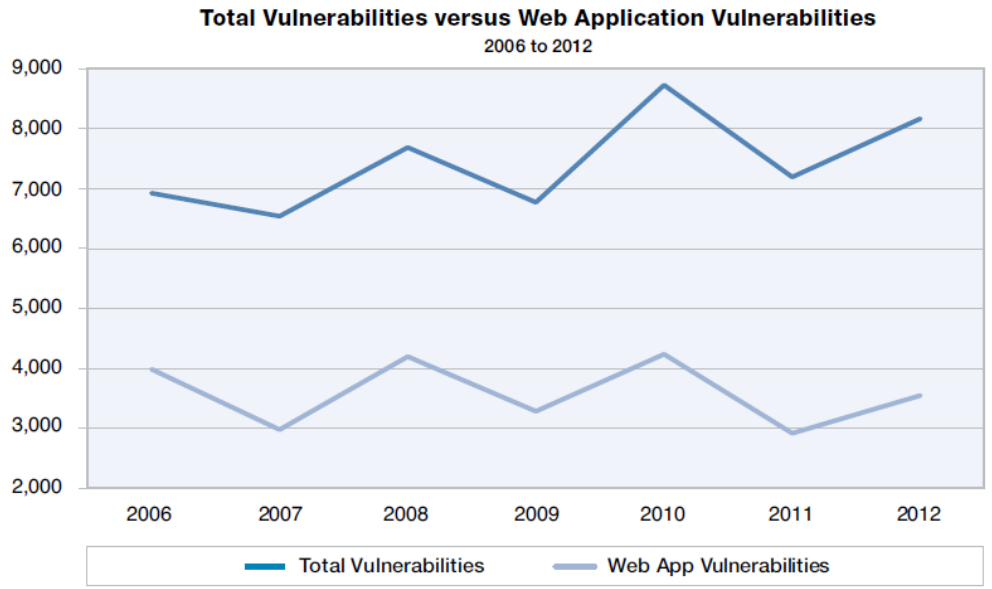
China’s J20

Sicherheits – Trends

Zunahme der Schwachstellen, sowie der Verteilung der Schwachstellen auf (Web-)Applikationen und andere Bereiche (ohne Custom-Applikationen).

Im Schnitt 150 neue Schwachstellen pro Woche.

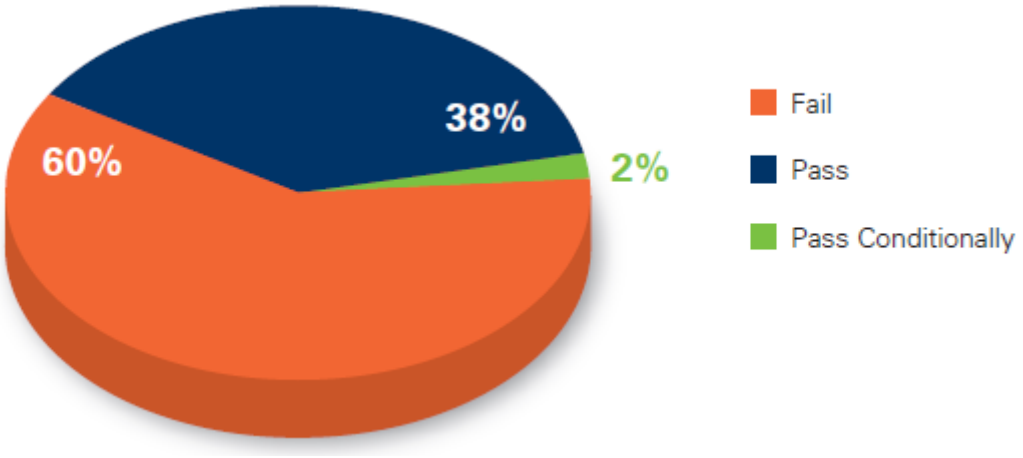




Quelle: IBM Internet Security Systems X-Force® 2012 Trend und Risk Report

Benchmark gegen OWASP Top10

Die meisten Applikationen, welche gegen die OWASP Top 10 geprüft werden, bestehen die Prüfung nicht

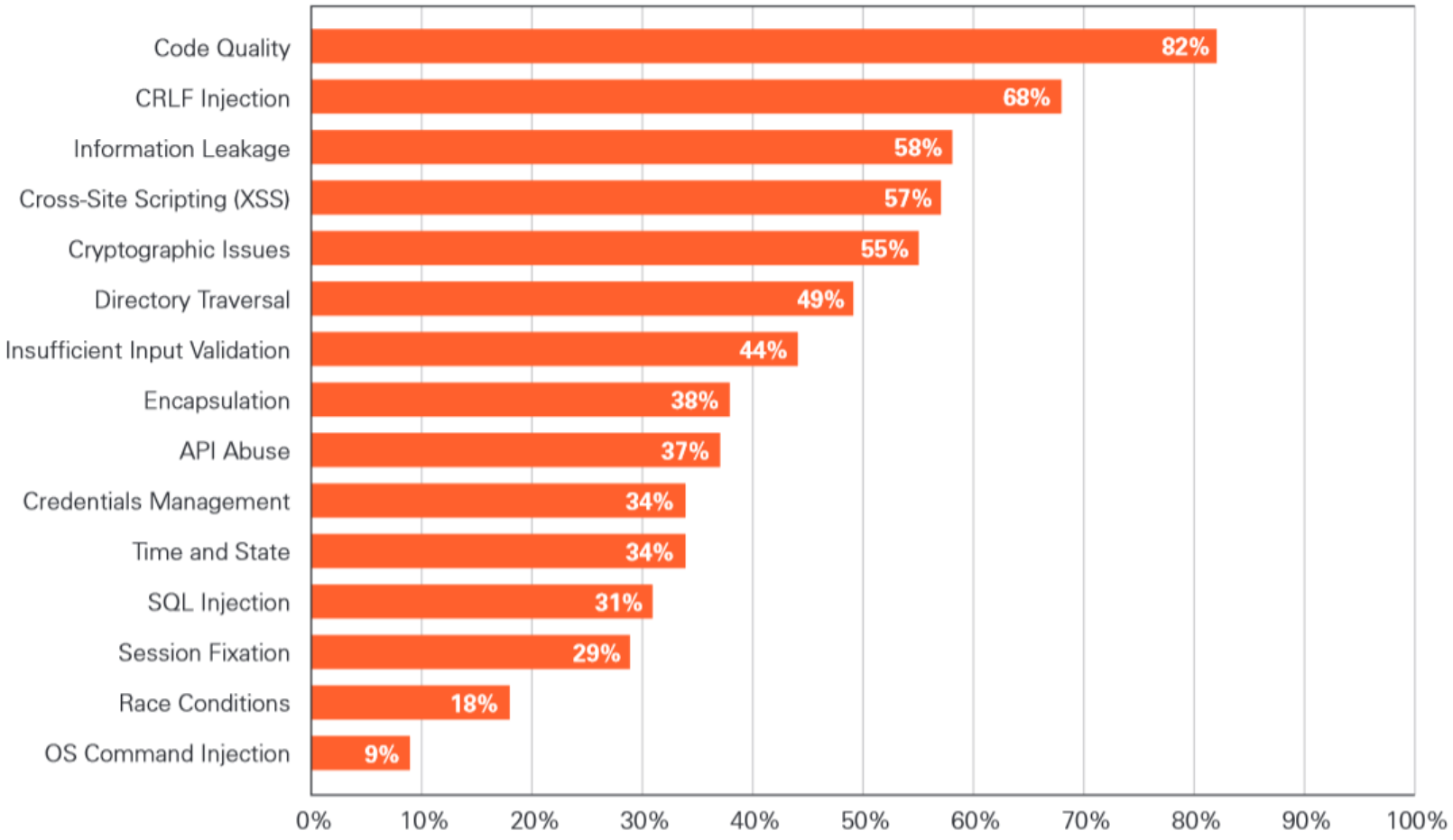


Viele der Applikationen fallen auch im zweiten Versuch durch

Quelle: Veracode

Technologie – Java

Schwachstellen in Prozent der geprüften Applikationen



Quelle: Veracode – state-of-software-security-report-volume5.pdf

Typische Software Schwachstellen

- OWASP Top 10

Kategorisierung von Web-App Schwachstellen

A1: Injection	• SQL- und SSI Injection • Format String Attack • LDAP Injection	• OS Commanding • XPATH Injection
A2: Cross-Site Scripting (XSS)	• Cross-site Scripting • Content Spoofing • Cross-site Request Forgery	
A3: Broken Authentication and Session Management	• Insufficient Authorization • Credential/Session Prediction • Insufficient Session Expiration	
A4: Insecure Direct Object References	• Direct without access control check to • object references • File, directory, or database key	
A5: Cross-Site Request Forgery (CSRF)	• Directory Indexing • Information Leakage • Path Traversal	

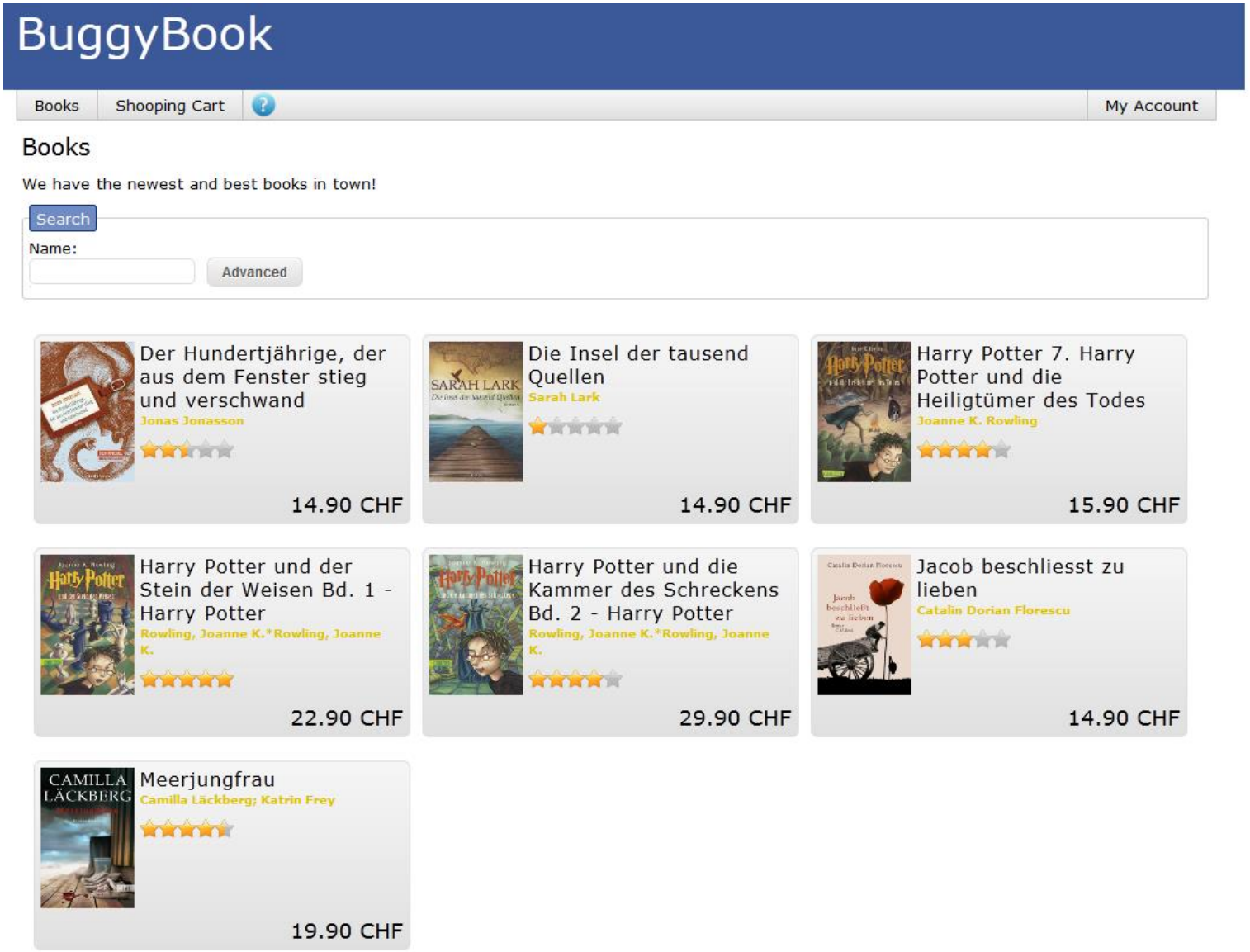
Kategorisierung von Web-App Schwachstellen

A6: Security Misconfiguration	• Secure configuration for frameworks, application and webserver defined and deployed • Frequently update the software
A7: Insecure Cryptographic Storage	• Protect sensitive data, such as credit cards, access information with sufficient encryption
A8: Failure to Restrict URL Access	• Forceful browsing • URL guessing • Access control for every requst
A9: Insufficient Transport Layer Protection	• Insecure encryption • Correct server certificate
A10: Unvalidated Redirects and Forwards	• Manipulated redirects and forwards

Demo

- Hackers choice - SQL Injection

Demo an der Beispiel App “BuggyBook”

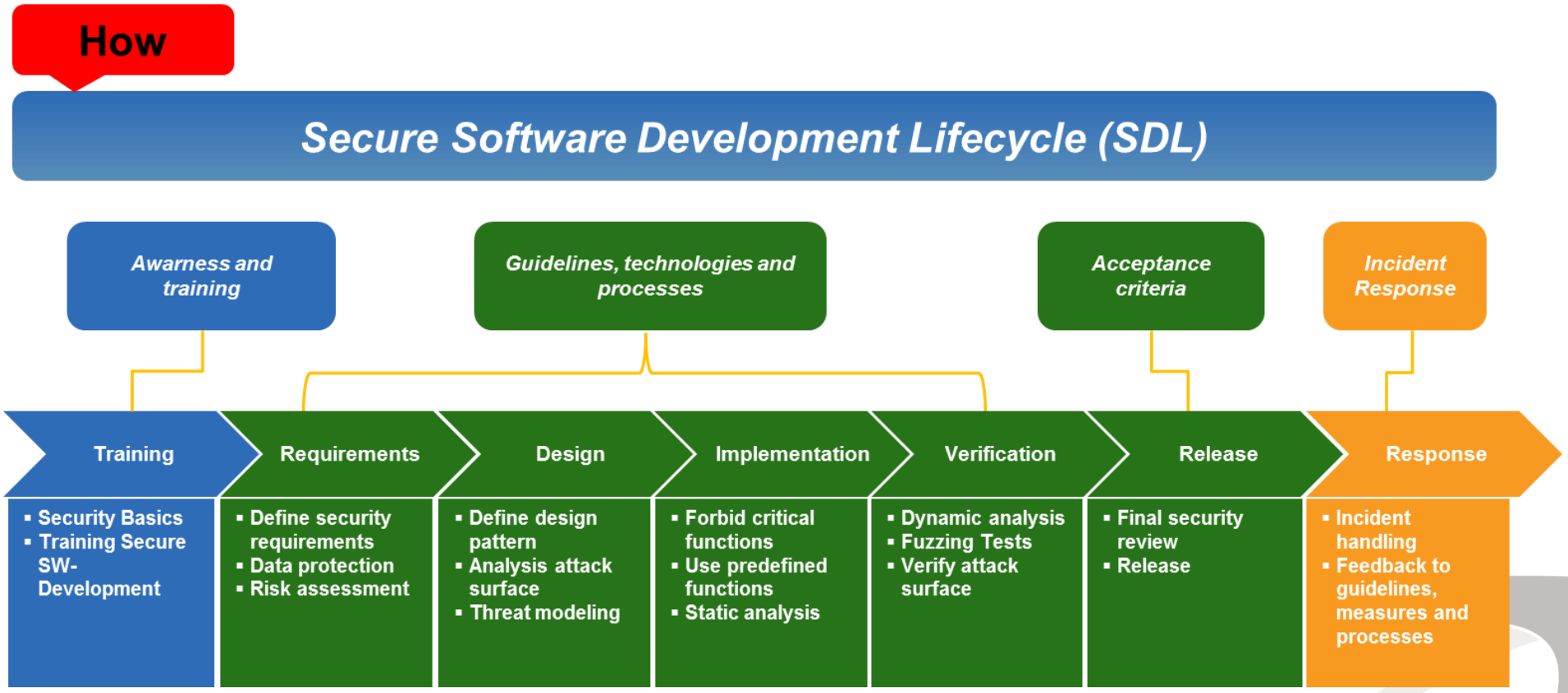


Sicherheit in SW verbessern

- Mögliche Massnahmen

Secure Development Lifecycle (SDL)

Durch die Planung und Umsetzung eines Secure Development Lifecycle (SDL), ist die Sicherheit ein klarer Bestandteil jeder Software Lösung und dient dazu, die Anzahl der Sicherheitsschwachstellen zu reduzieren.

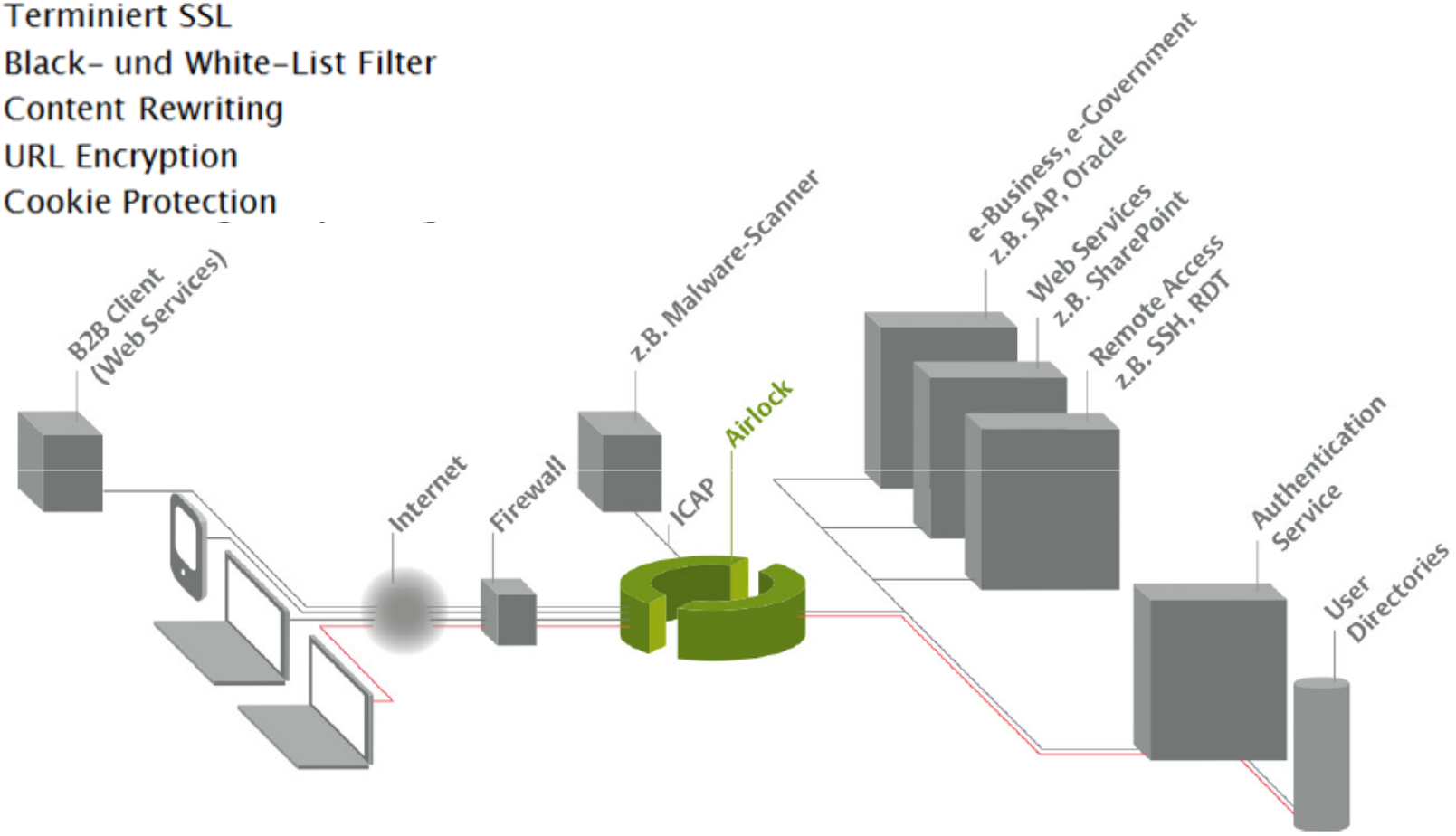


Quelle: Microsoft SDL

Web Application Firewalls (WAF)

Strategic Web Entry Solution

Grundprinzip ist ein intelligenter Reverse Proxy
Terminiert SSL
Black- und White-List Filter
Content Rewriting
URL Encryption
Cookie Protection

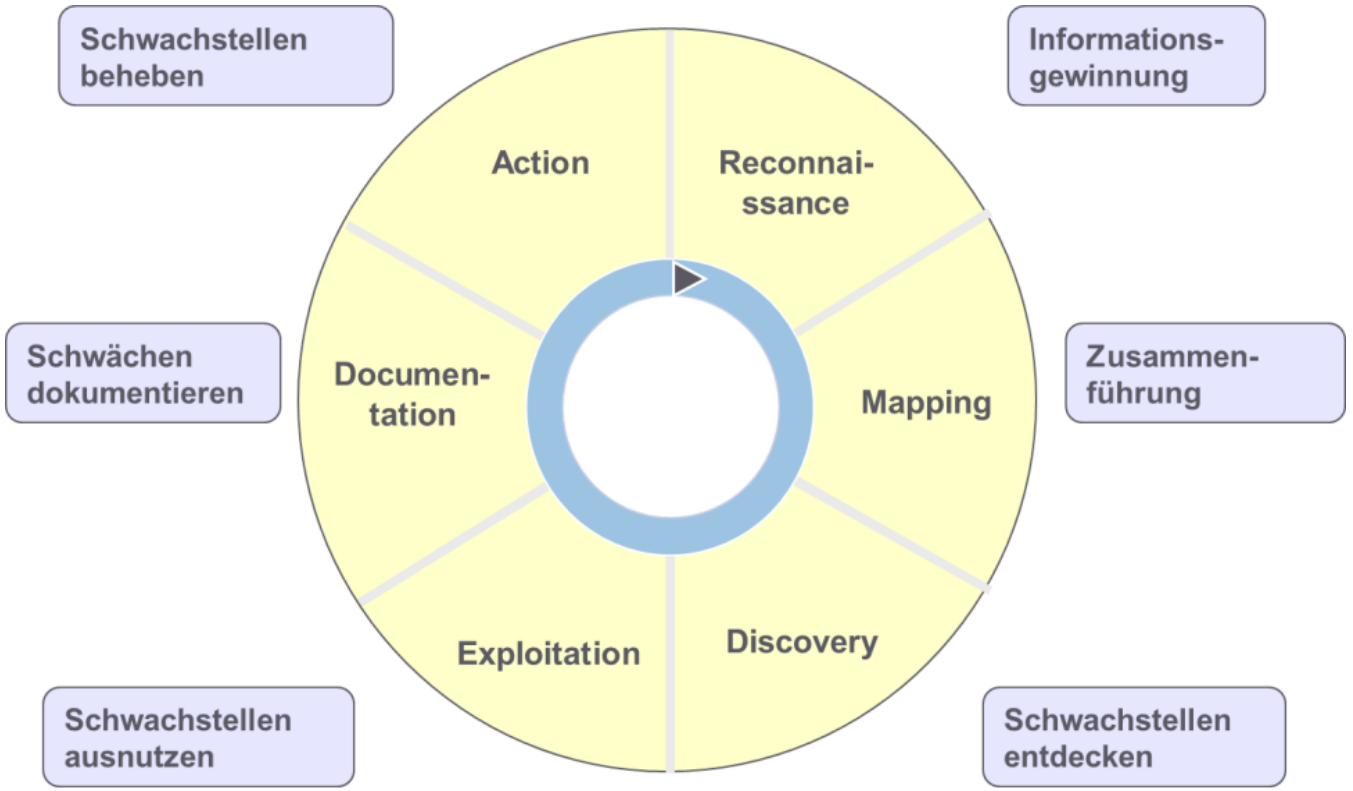


Quelle: Ergon

Penetration Testing

Bei einem Penetration Test wird ein realistischer Angriff eines Hackers simuliert.

Manuelles Application Penetration Testing



Questions & Answers

Besten Dank für Ihre Aufmerksamkeit

Protect7

your application security experts

Bei Fragen kontaktieren Sie bitte:

Roger Caspar
E-Mail: roger.caspar@protect7.com oder
Telefon: +41 44 515 68 68

Herzlichen Dank für Ihre Aufmerksamkeit!

Protect7 GmbH | Franklinstrasse 7 | CH-8050 Zürich | www.protect7.com