Digicomp Hacking Day 2013

IT-Security im Web und Time-to-Market – Chance statt Widerspruch

Coop: **Dirk Schmidt**
OneConsult: **Christoph Baumgartner**
Zürich, 16.05.2013

Agenda

- → Vorstellung
- → Einführung
- → IT-Security bei Coop
- → Erfahrungswerte
- → Q&A
- → Anhang: Methoden und Standards

Über mich

- Dirk Schmidt
- Studium der technischen Betriebswirtschaft an der Fachhochschule Offenburg
- Studium Business Administration RMIT Melbourne
- Seit 2004 bei coop als Leiter eCommerce
  - Seit 2010 Leiter Prozesse Services
    - Internet / Intranet
    - eCommerce
    - CRM
    - HR / Workflow

Über mich

- Christoph Baumgartner
- Studium der Wirtschaftsinformatik an der Universität Zürich (MSc UZH IS)
- Seit 1996 Berater in den Bereichen IT Security und Strategie
- Gründer der OneConsult GmbH im Jahr 2003
- Seither CEO und Inhaber
- ISECOM Board Member

OneConsult GmbH

- IT Security Consulting & strategische Beratung (kein Verkauf von Hard- und Software)
- Kunden
  - Hunderte Unternehmen und Konzerne in Europa und Übersee
  - Tätig in allen Branchen
- Security Audit Kompetenz: seit 2003 mehr als
  - **650 technische Security Audit Projekte**, davon über **550 nach OSSTMM** – Nr. 1 für OSSTMM-konforme Security Audits in Europa
  - **200 Web Application Security Audits** (Internetbanking-Lösungen und Onlineshops) und **Dutzende Mobile Application Security Audits**
  - **100 konzeptionelle Security Audits**
- 9-köpfiges, festangestelltes und zertifiziertes **Penetration Tester Team**
- Standorte
  - Schweiz: Hauptsitz in Thalwil
  - Deutschland: Büro in München
  - Österreich: Büro in Wien

Agenda

- → Vorstellung
- → Einführung
- → IT-Security bei Coop
- → Erfahrungswerte
- → Q&A
- → Anhang: Methoden und Standards

"There are only two types of companies, those that have been hacked and those that will be."

Robert Mueller, head of the Federal Bureau of Investigation, www.nytimes.com, 4 March 2012

Vorfälle

Vorfälle

Zeitpunkt	Betroffene	Vorfall
Juli 2011	**Rewe/Penny**	- Hacker stellen 52'000 gestohlene Datensätze (E-Mail-Adressen und Passwörter) ins Internet - Passwörter unverschlüsselt gespeichert - Entwendete Administratordaten
Juni 2012	**LinkedIn**	- Passwort-Hashes von mehr als 6,4 Millionen Nutzern im Internet veröffentlicht - Mit Hilfe schneller Grafikkarten stellen Sicherheitsexperten ca. 85 Prozent der Original-Passwörter wieder her
Juli 2012	**Dropbox**	- Hacker verschaffen sich über das Dropbox-Konto eines Mitarbeiters Zugriff auf zahlreiche E-Mail-Adressen - Nutzung für Versand von Spam
April 2013	**Wordpress**	- Botnet Angriffswelle gegen die Blog-Plattform - Brute-force Attacke nutzt verbreitete Usernamen und schwache Passwörter aus

Application Security Audit

Gründliche, *technische*, *unprivilegierte* und *privilegierte* Sicherheitsüberprüfung einer Applikation und der zugehörigen Systeme aus der Perspektive eines versierten Angreifers.

Mögliche Untersuchungsbereiche

- IT Infrastruktur und Basisdienste: fehlende Security Patches und Konfigurationsmängel
- Applikationen: Schwerpunkte
  - Authentisierung
  - Autorisierung / Vertrauensstellungen
  - Validierung
  - Datenkommunikation
  - Datenhaltung
- Ansätze
  - Laufende Systeme (= mittels Application Security Audit / Penetration Test)
  - Source Code (= mittels Code Review)
  - Binaries (= mittels Reverse Engineering)
  - Application Architektur (= mittels Design- und Configuration Review)

Stichwörter

→ Applikationen
- Online-Shops
- Interbanking-Portale
- Mailserver
- Datenbanken
- Branchenlösungen
- Mobile Apps
- etc.

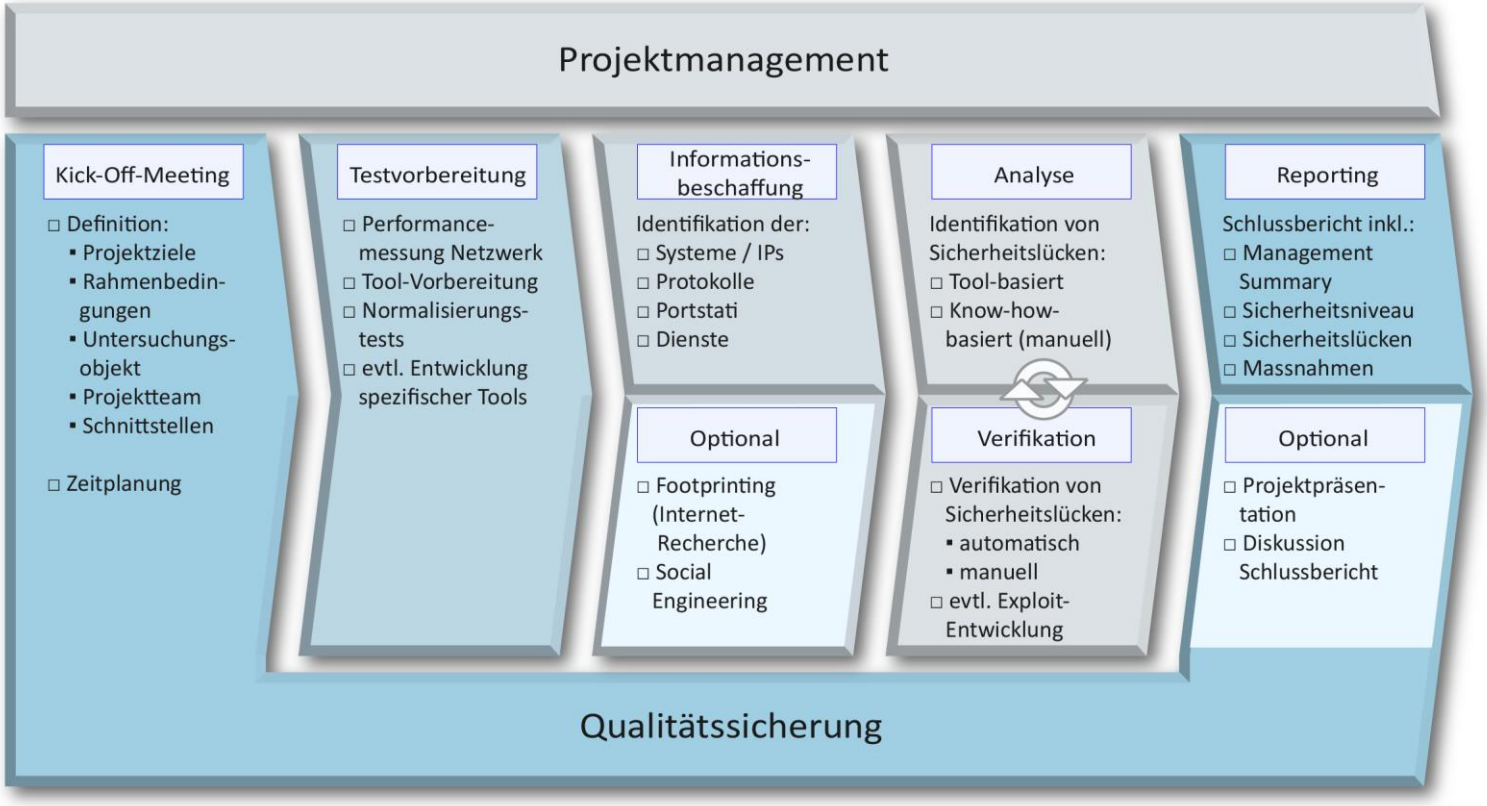
→ Ansätze
- Client und Server
- Dediziert vs. virtualisiert (Cloud)
- Mobile Client
- Web Application vs. Web Service
- etc.

→ Environment
- Betriebssystem
- Programmiersprache
- Framework
- etc.

Zweck und Nutzen

- Qualitätssicherung dank (unabhängiger) IT Security-Analyse
- Compliance: Nachweis bezüglich gesetzlicher Rahmenbedingungen und Vorgaben
- Prävention: Ermöglicht (in der Zukunft) direkte und indirekte Kosteneinsparungen
- Awareness auf allen Stufen
- Know-how Transfer
- Argumentationsgrundlage für zukünftige
  - IT Security-Investitionen
  - Aktivitäten

Generischer Ablauf Application Security Audit



OneConsult Testansatz

Mischung aus zwei bekannten und verbreiteten Methoden

→ Open Source Security Testing Methodology Manual (OSSTMM)

→ Open Web Application Security Project (OWASP)

→ Weitere Informationen: siehe Anhang

Typische Szenarien

- → Bestehende Lösung
- → Neuentwicklung
- → Neuer Release

Typische Zeitpunkte

- → Frühe Entwicklung: Eher Konzept-Review
- → In der Entwicklung: Eher Code-Review
- → Gegen Ende der Entwicklung:
  - Häufig noch nicht alles fertig oder nicht funktionierend (-)
  - Nicht finales Umfeld (-)
- → In der Test-Phase:
  - Nicht finales Umfeld (-)
  - Teilweise noch nicht alles fertig / komplett funktionierend (-)

Typische Zeitpunkte

→ In Produktiv-Umgebung vor Go-Live: optimal
- Funktionalität komplett (+)
- In Zielumgebung (+)
- Noch nicht produktiv (+)
- Meistens dedizierte Testingzeit nötig (-)

→ Live:
- Funktionalität komplett (+)
- In Zielumgebung (+)
- Produktiv (evtl. Ausfälle) (-)

Agenda

- → Vorstellung
- → Einführung
- → IT-Security bei Coop
- → Erfahrungswerte
- → Q&A
- → Anhang: Methoden und Standards

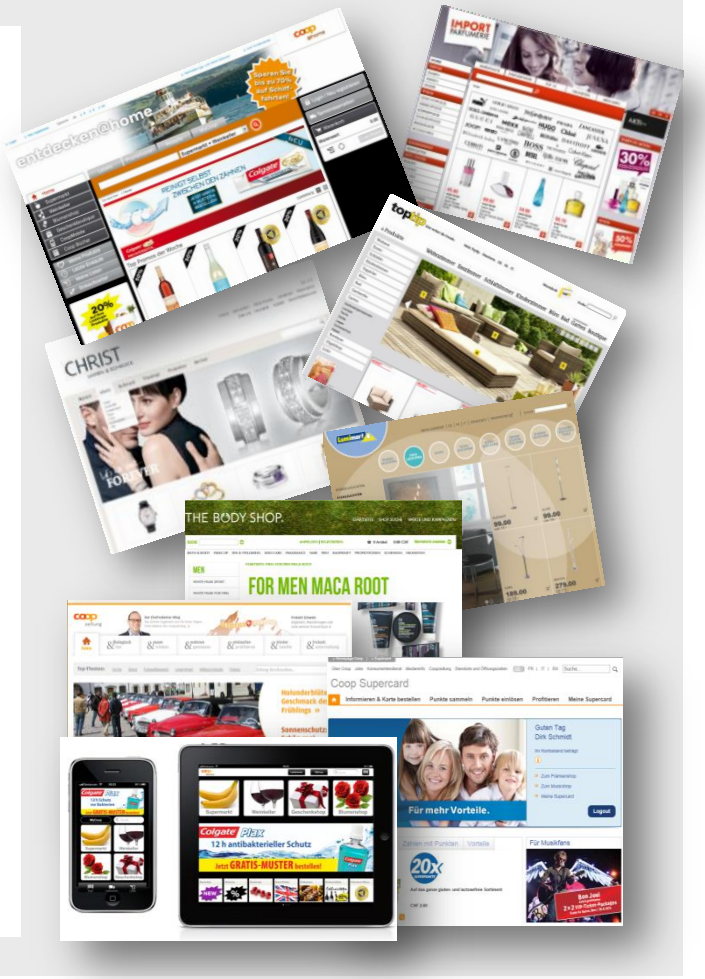
Coop und IT-Security

Fakten coop-Internet

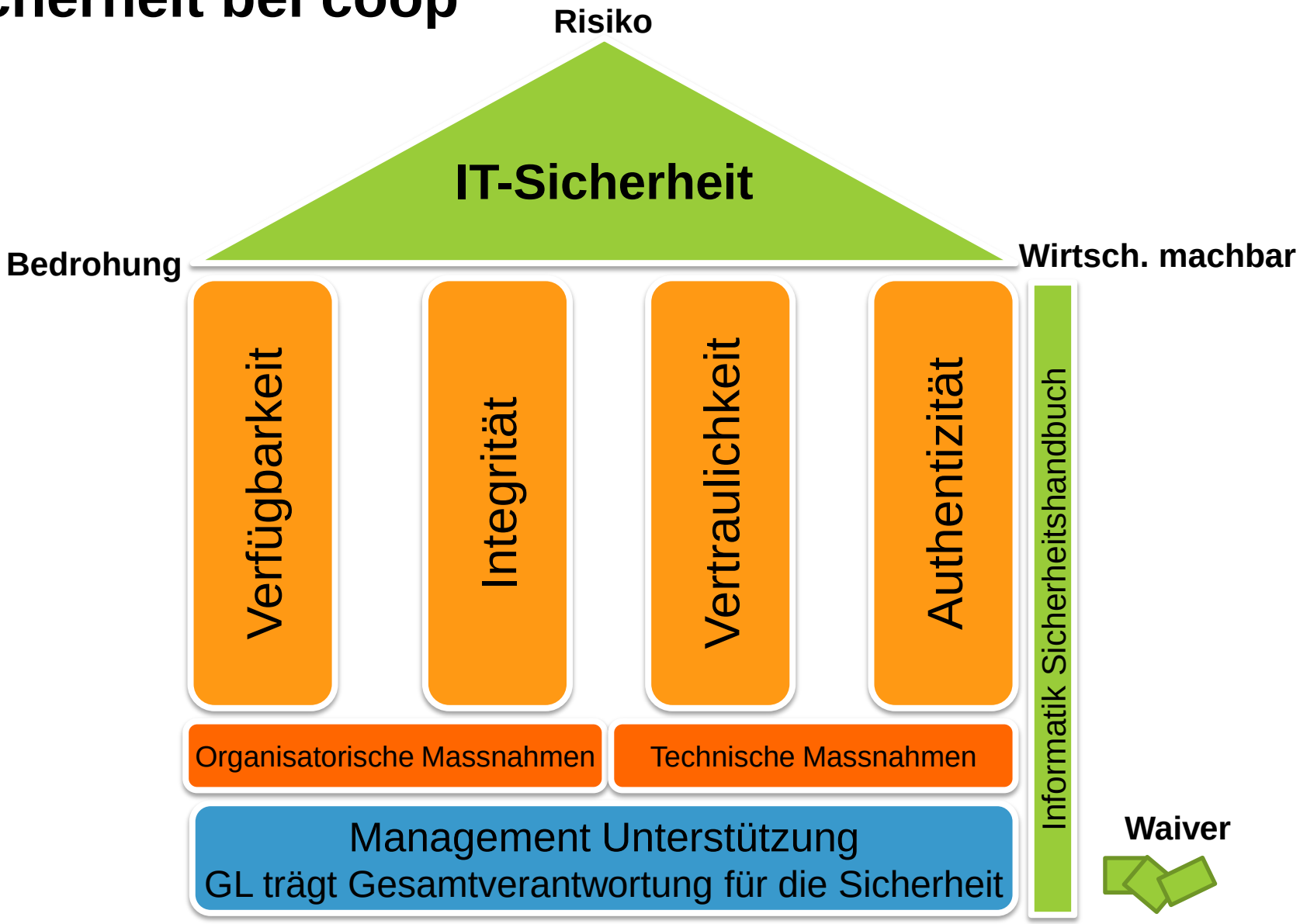
- **coop.ch**
  - wurde in den letzten Jahren ein bedeutendes Kommunikationsmedium von Coop
  - Nahezu jede "Offline"-Kampagne wird Online begleitet
  - Jede grosse Marketing-Kampagne (z.B. BigWin, Simsalawin etc.) hat Kernelemente auf der Webseite, die wesentlich für den Erfolg der Kampagne sind.
  - Stark steigende Besucherraten – November 2012: > 5.4 Mio Besucher (143% z.V.) // sonst **2.2 Mio Besuche / Monat**
  - coop.ch belegte Rang # **10** (!) der Top 50 Schweizer Internet-Seiten (Migros # 19; Amazon # 21)
  - Suchanfragen bei Google (Zeitgeist 2012): Rang #3

Fakten coop-Internet

- **Online-Shops → 2.7 Mio Besuche / Monat**
  - microspot / Interdiscount / Fust
  - coop@home
  - Trading (Toptip, Lumimart, Import Parfumerie, Christ, The Body Shop)
- **coopzeitung.ch → 400'000 Besuche / Monat**
- **supercard.ch → 300'000-600'000 Besuche / Monat**
- Mobile Applikationen haben ein starkes Wachstum



IT-Sicherheit bei coop



Ziel

Das langfristige Sicherstellen der korrekten Informationsverarbeitung im Interesse des Gesamtunternehmens. Dabei müssen in jedem Fall auch die rechtlichen Aspekte (z.B. Datenschutzgesetz) abgedeckt werden.

Grundsätze

- Verantwortung übernehmen
- Fortbestand des Unternehmens sichern
- Daten schützen
- Netze schützen
- Funktionen trennen
- Dritte einbinden

Überprüfung durch die in- und externe Revision

Zusätzliche Awareness im Bereich Internet geschaffen:

Ausgangslage

- Coop investiert(e) seit langem viel in die Datensicherheit – sowohl für technische, als auch organisatorische Massnahmen

- Aufgrund der Datenpannen bei REWE, PENNY und Marktkauf in Deutschland wurden und werden bei Coop alle relevanten Webseiten/Applikationen (inkl. mobile Apps) von einem externen Spezialisten (OneConsult) auf Sicherheitslücken untersucht:

- Im Speziellen die folgenden Seiten/Auftritte:
  - Hello Family-Seiten
  - Memofit (extern gehostet)
  - Ernährungscoach (extern gehostet)
  - Coop-Verantwortung.ch
  - Publikationen bestellen
  - Mobile Applikationen
  - Online-Shops

http://www.spiegel.de/netzwelt/web/0,1518,775354,00.html

Meistbesuchte Seiten | Erste Schritte | Aktuelle Nachrichten | Google Analytics

Schlagzeilen | Hilfe | RSS | Newsletter | Mobil | Wetter | TV-Programm

SPIEGEL ONLINE NETZWELT

NACHRICHTEN | VIDEO | THEMEN | FORUM | ENGLISH | DER SPIEGEL | SPIEGEL TV | ABO | SHOP

Home | Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | einestages | Karriere | Uni | Schule | Reise | Auto

Nachrichten > Netzwelt > Web > Hacker

Login | Registrierung

THEMA

Hacker

Alle Artikel und Hintergründe

Feedback | Merken

Zum Glück nicht geschehen … aber es wäre durchaus möglich gewesen

VERWANDTE THEMEN

Computer

Rewe

…SEITEN

FOTOSTRECKE

Begriffsfindung: Wer sind eigentlich Hacker?

STEVEN LEVYS HACKER-ETHIK

1. Zugang zu Computern - und sonst allem, was einem etwas über das Funktionieren der Welt beibringen könnte - sollte unbegrenzt und vollständig sein.
2. Eigenhändiger Zugang soll stets den Vorrang haben.
3. Alle Information sollte frei sein.
4. Misstraue Autorität - fördere Dezentralisierung.
5. Hacker sollten nach ihren Hacks beurteilt werden, nicht aufgrund von Scheinkriterien wie Abschlüssen, Alter, Rasse oder Position.
6. Man kann mit einem Computer Kunst und Schönheit schaffen.
7. Computer können dein Leben zum Besseren verändern.

MEHR AUF SPIEGEL ONLINE

…und Mail-Adressen von Coop-Kunden …ehen im Web

DPA

Gedächtnistrainer vergisst die Sicherheit: Mehr als 10'000 Kundendaten mit Passwörter im Netz

Unbekannte haben gut 14.000 Datensätze mit E-Mail-Adressen und Passwörtern veröffentlicht. Offenbar wurden sie von Websites des Einzelhändlers Coop kopiert. Das Unternehmen bestätigt den Datenklau - die Passwörter wurden unverschlüsselt gespeichert.

Empfehlen 260 | Tweet 88

Basel - Der Datenklau bei Coop wird für Zehntausende Kunden zum ernsten Problem: Am Dienstag veröffentlichten Unbekannte im Web ein Textdokument mit gut 14.000 Datensätzen, die E-Mail-Adresse und zugehörige Passwörter von Verbrauchern enthalten.

Massnahmen

- Kritische Findings (Prio1): Sofortige Information der Lieferanten / Betreiber der externen Applikationen die detektierten Schwachstellen unverzüglich zu schliessen / vom Netz zu nehmen.

- Wichtige Findings (Prio2 und geringer): detektierte Schwachstellen wurden aufgezeigt und bzgl. Umsetzung eng terminiert und überwacht.

- Neugestaltung der Rahmenverträge mit externen Lieferanten

- Aufnahme von Web-Sicherheits-Standards in die Entwicklungsrichtlinien

➢ Von Seiten des Managements wurde der Grundsatz erlassen, dass bei allen Web-Präsenzen und mobilen Applikationen, welche Kundendaten speichern und verwalten (unabhängig ob in- oder extern gehostet), ein externes Sicherheitsaudit vor GoLive durchgeführt werden muss. Dies ist in den jeweiligen Projektplänen und –budgets zu berücksichtigen. Verantwortlich für die Umsetzung ist die Projektleitung. Der Informatik Security-Officer unterstützt die Projektleitung.

Konsequente Umsetzung

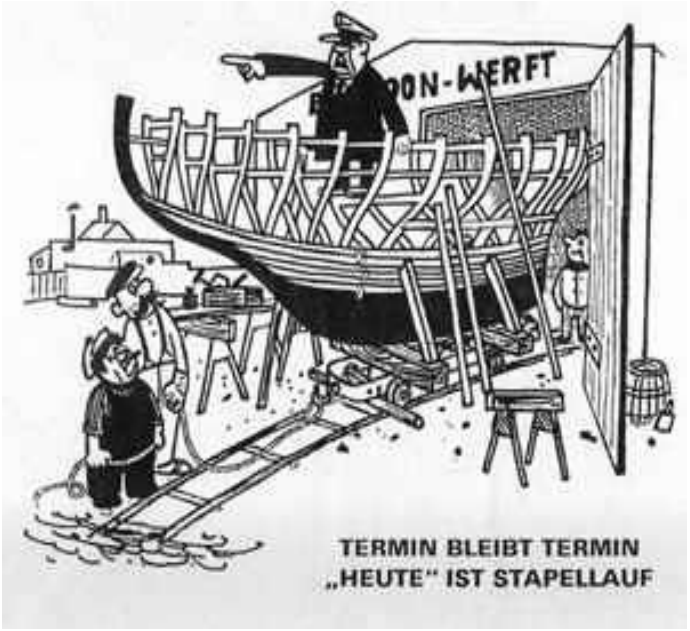
- Einbeziehen der Sicherheitsüberlegungen in Architektur und Entwicklung von Anfang an
- Alle neuen Gewinnspiele boten bisher keine Angriffsfläche
- Sämtliche neue Apps wurden bisher nicht kompromittiert
- Alle neuen Shops wurden einem Audit unterworfen und zeigten bisher keine nennenswerten Sicherheitsprobleme
- Konsequente Überprüfung ca. 3-4 Wochen vor einem GoLive auf möglichst produktiver / produktionsnaher Umgebung

IT-Security darf nicht lähmen!

- Eine schnelle IT mit agilen Projekten muss IT-Security bereits von Anfang an berücksichtigen
- Klares Abwägen von Risiko, Bedrohung und wirtschaftlicher Machbarkeit
- Security lähmt nicht – sie gibt die notwendige "Bodenhaftung"

Knappe Ressourcen und dennoch sicher?

- Externe Experten können parallel unterstützen und Testen – diese rechtzeitig planen!
- Externe Experten dürfen die Organisation nur minimal belasten – die langjährige Zusammenarbeit mit OneConsult sorgte hier für ein integriertes Prozesswissen
- Klares Abarbeiten der Findings entlang der Prioritäten
- Eingestehen, wenn noch zu viele Punkte offen sind



DO's und DON'Ts

Do's

- Management Attention schaffen – Sicherheit muss TopDown "verordnet" werden
- Testinfrastruktur sicherstellen: idealerweise Tests auf Pre-Production Plattform, welche identisch mit der zukünftigen produktiven Plattform sein soll
- Security Tracking als Prozess im Projekt etablieren
- Priorisierung und konsequente Umsetzung von Massnahmen
- Alle Zugriffsmöglichkeiten testen: Web Applikationen, Web Services, Mobile Apps, Formulare (z.B. optimiert für Web und/oder Mobile)
- Rechtzeitige Evaluation und Einbindung des (externen) Security Auditors

Don'ts

- Die Do's vernachlässigen
- Wegschauen - "es wird schon nichts passieren" ist grob fahrlässig
- Termintreue vor Sicherheit stellen
- Security-Tests nicht im Projekt- und Finanzplan (Budget) berücksichtigen

Gratislieferung für einen Einkauf ab CHF 200

VISIT13F-X

www.coopathome.ch

Code bis 31.12.2013 einlösbar

Agenda

- → Vorstellung
- → Einführung
- → IT-Security bei Coop
- → Erfahrungswerte
- → Q&A
- → Anhang: Methoden und Standards

Knackpunkte

- → Fach- und Sozialkompetenz der Tester und der am Projekt beteiligten Mitarbeiter
- → Vergleichbarkeit und Nachvollziehbarkeit von
  - Offerten
  - Vorgehen
  - Resultaten und Dokumentationen
- → Compliance zu Gesetzen, Standards und Vorgaben erwünscht, aber:
  - Nur rudimentäre Behandlung von technischen Audits in Standards (z.B. ISO/IEC 2700x)
  - Keine offiziellen Checklisten oder Guidelines verfügbar

Typische Stolpersteine

- → Offerte
  - Kein Geld/Budget eingeplant
  - Offerte zu früh: genauer Scope noch nicht bekannt
  - Offerte zu spät: zu wenig Zeit für Projekt vor Go-Live
- → Kick-off
  - Parteien kommunizieren auf unterschiedlichen Ebenen
  - Zu viele/falsche Personen sind anwesend
  - Änderung des Scopes
- → Audit
  - Verschiebungen
  - Applikation/Umgebung noch nicht fertig
  - Kundenseitige Vorbereitungen nicht abgeschlossen

Erfahrungswerte

- → Bei sämtlichen Projekten Schwachstellen gefunden, bei einigen aber nur sogenannte Exposures
- → Sicherheitsniveau in der Finanzbranche und bei grossen Online Shop Betreibern höher als z.B. bei Unternehmen der Fertigungsindustrie
- → Grossteil der Lücken von Web Applikationen und den dazugehörigen Systemen basiert auf schlecht gepflegtem Basisbetriebssystem
  - Zeitnahes Security Patching
  - Umdenken bezüglich Trennung der Verantwortlichkeiten für IT Infrastruktur und darüber liegender Applikationen

Erfahrungswerte

- → Mobile Apps: «Calling Home Syndrom»
- → Spezialentwicklungen für einen einzigen Kunden
  - Tendenziell mehr Sicherheitslücken
  - Schliessung dieser Lücken nimmt mehr Zeit in Anspruch als bei Software von der Stange
- → Sicherheitsüberprüfung in einer frühen Projektphase planen
  - Tendenziell weniger Sicherheitslücken
- → Kommerzielle Software im CMS Bereich
  - Tendenziell weniger Sicherheitslücken als Open Source
  - Schliessung von Lücken erfolgt zeitnaher
- → Altbekannte Sicherheitslücken bei ca. einem Drittel der Projekte wieder gefunden

Agenda

- → Vorstellung
- → Einführung
- → IT-Security bei Coop
- → Erfahrungswerte
- → Q&A
- → Anhang: Methoden und Standards

Danke für Ihre Aufmerksamkeit!

Fragen?

Kontakt Coop:

Dirk Schmidt
Informatik Prozesse Services
+41 61 336 53 03
Dirk.Schmidt@coop.ch

Kontakt OneConsult:

Christoph Baumgartner
CEO & Owner
+41 43 377 22 22
christoph.baumgartner@oneconsult.com

OSSTMM

→ **O**pen **S**ource **S**ecurity **T**esting **M**ethodology **M**anual

→ Entwicklung unter der Leitung von ISECOM,
Institute for **SEC**urity and **O**pen **M**ethodologies,
http://www.osstmm.org

→ Erstausgabe 2001, aktueller offizieller Release OSSTMM 3.0

→ Offene und frei verfügbare Methode zur

- Planung
- Durchführung
- Grobdokumentation

von (technischen) Security Audits

OSSTMM

- Sicherheitsniveau als neutraler Zahlenwert (Risk Assessment Value)
- Umfassender Verhaltenskodex (Rules of Engagement)
- Compliant zu ISO/IEC 17799/27001, ITIL, BSI-Standard-100-1/4, SOX, Basel II etc.
- Optionale Zertifizierung (Projekte, Personen und Organisationen) durch ISECOM
- OneConsult
  - ISECOM Licensed Auditor (Platinum Level)
  - ISECOM Partner (akkreditierter Schulungsanbieter)
  - Aktive Mitarbeit am OSSTMM: 3 Mitarbeiter im ISECOM Core Team
  - Mehr als 550 Projekte nach OSSTMM seit 2003

Open Web Application Security Project (OWASP)

Gratis und offen für jeden, der Sicherheitsaspekte von Applikationen verbessern möchte.

- → OWASP Top 10
- → Tools
- → Dokumente
- → Foren
- → Teilnahme an Meetings der Ortsverbände

OWASP
The Open Web Application Security Project

http://www.owasp.org

Die OWASP Top10 (2013 – RC1)

- → A1 Injection
- → A2 Broken Authentication and Session Management
- → A3 Cross-Site Scripting (XSS)
- → A4 Insecure Direct Object References
- → A5 Security Misconfiguration
- → A6 Sensitive Data Exposure
- → A7 Missing Function Level Access Control
- → A8 Cross-Site Request Forgery (CSRF)
- → A9 Using Known Vulnerable Components
- → A10 Unvalidated Redirects and Forwards

Die OWASP Top10 (2010 - 2013)

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6