

# Hacking Day 2014 – Datenschutz



## Defense in Depth und Security Prozesse am Beispiel von Heartbleed

Yves Kraft – Senior Security Consultant – OneConsult GmbH

# Agenda

- Vorstellung
- Einleitung
- Beispiele/Demo
- Gegenmassnahmen
- Fazit

# Über mich



- Yves Kraft
- Senior Security Consultant
- BSc FH CS, OPST, OPSA, OSSTMM Trainer
- Kursleiter bei Digicom [Kurscodes [PSI](#), [PSO](#), [PST](#), [SWO](#), [TSA](#)]
- Technische Security Audits
- Konzeptionelles Consulting
- Schulung & Coaching
- Security Officer



# Unternehmen

## → Kunden

- Mehr als 200 Unternehmen in der Schweiz, Europa und Übersee (inklusive ein Dutzend der «Fortune Global 500 Corporations»)
- Kunden gleichmässig auf alle Branchen verteilt (Finanz-, Pharma-, Industrie-Branche sowie öffentliche Verwaltungen (Bund, Kantone und Städte))

## → Projekterfahrung, über

- 750 technische Security Audit Projekte / Penetration Test Projekte (650 davon nach OSSTMM)
- 350 Application Security Audits von Banking Lösungen und Online Shops
- 45 Mobile App Security Audits
- 50 Code Reviews
- 35 Digitale Forensik und Notfalleinsätze, rund ein Projekt pro Monat
- 120 konzeptionelle Security Audits
- Weitere anonymisierte Informationen: <http://www.oneconsult.com/de/references>

# Einleitung

- Was ist Heartbleed?
- Was ist schief gelaufen?
- Der Angriff?

«Catastrophic is the right word. On the scale of 1 to 10, this is an 11.»

Bruce Schneier, [www.schneier.com](http://www.schneier.com)

# Was ist Heartbleed?



- Schwachstelle der Heartbeat-Erweiterung des TLS-Protokolls in OpenSSL
- OpenSSL-Versionen 1.0.1 bis 1.0.1f sind verwundbar
- Wurde von Codenomicon Defensics am 3. April 2014 entdeckt
- Bug mit Version 1.0.1g am 7. April 2014 behoben
- CVE-2014-0160:

[https://www.openssl.org/news/secadv\\_20140407.txt](https://www.openssl.org/news/secadv_20140407.txt)

# Was ist schief gelaufen?

## → Heartbeat-Funktion

- Kommunikationspartner A sendet zufälligen Inhalten
- Kommunikationspartner B sendet exakt die selben Daten zurück

## → Länge der Daten wird nicht geprüft

## → Feld `payload_length` kann mit beliebigen Werten überschrieben werden



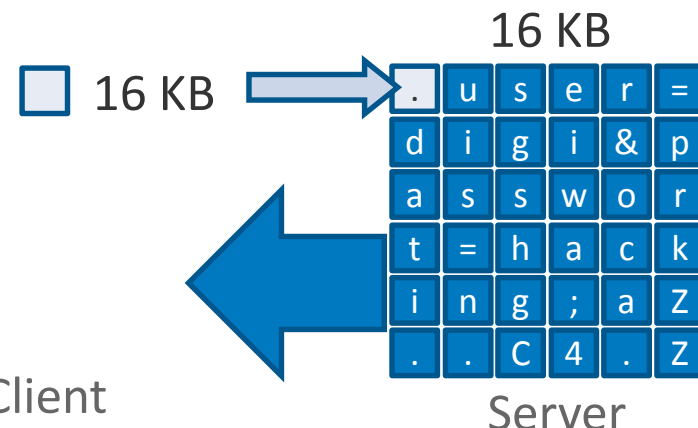


# Der Angriff

→ Angreifer sendet Heartbeat-Payload

- Grösse: 1 Byte
- Länge: 16KByte

→ Server sendet die angeforderten Daten zurück



```
buffer = OPENSSL_malloc(1 + 2 + payload + padding);
bp = buffer;
memcpy(bp, pl, payload);
```



→ RFC6520 «The total length of a HeartbeatMessage MUST NOT exceed  $2^{14}$ »

→ Mit Payload `0xFFFF` sind theoretisch 64 Kbyte möglich

# Demo

- Wie wird der Heartbleed-Bug ausgenutzt?
- An welche Informationen kann man gelangen?
- Bekanntgewordene Fälle

# Heartbleed-Bug (CVE-2014-0160)

→ OpenSSL-Versionen 1.0.1 bis 1.0.1f sind verwundbar

→ Vorgehen:

1. Information Gathering
2. Footprinting
3. Exploiting

# Szenario 1: Wordpress Blog

## Digicomp Hackingday 2014

*Defense in Depth und Security Prozesse am Beispiel von Heartbleed*

Sample Page



## Hackingday 2014

🕒 June 10, 2014 📁 Uncategorized

### Defense in Depth und Security-Prozesse am Beispiel von Heartbleed

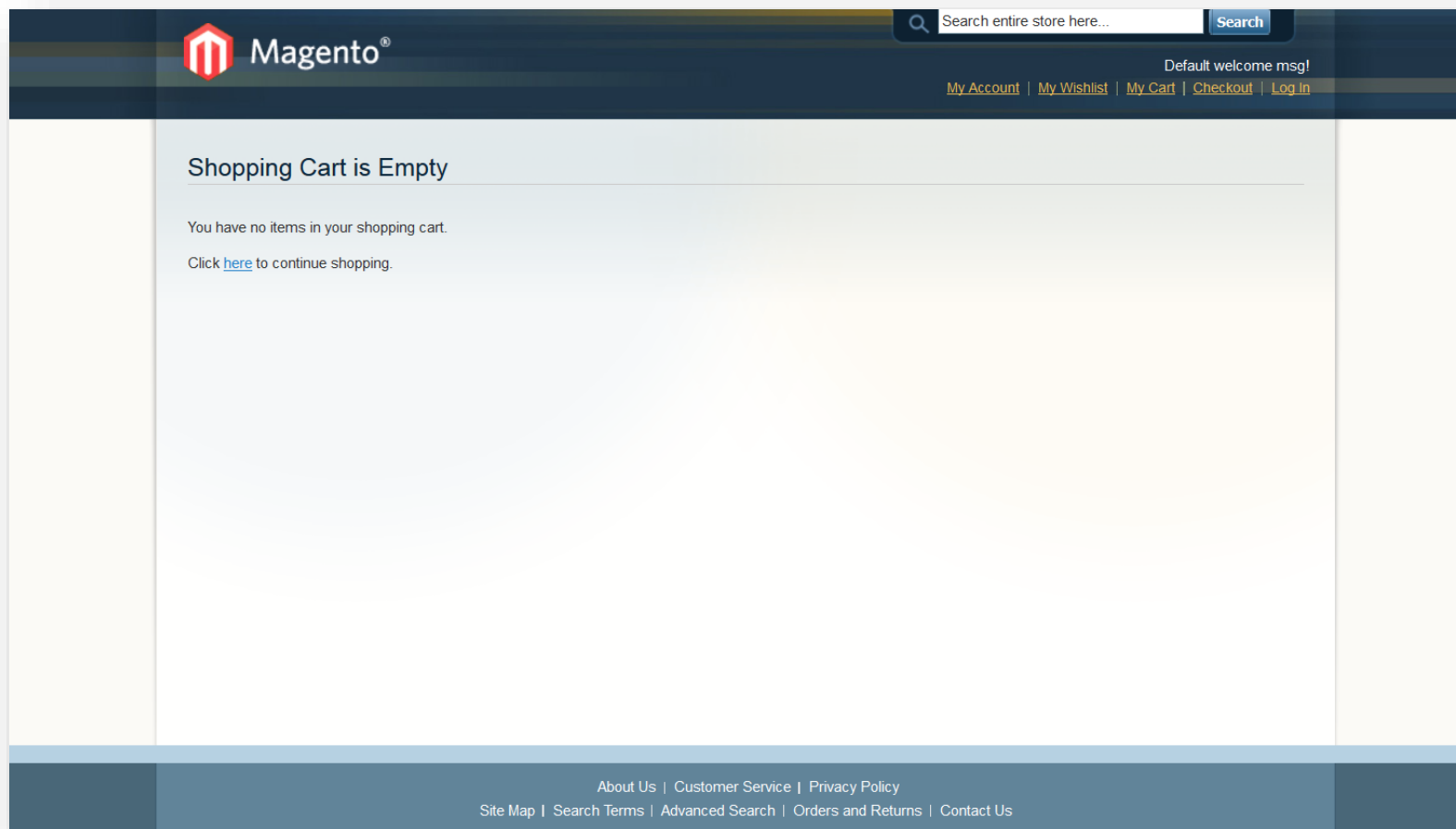
Dieses Referat beschreibt die Situation rund um den Heartbleed-Bug und verdeutlicht dessen Auswirkungen anhand von Live-Demos und Beispielen aus der Praxis. Zudem wird aufgezeigt, wie der potenzielle Schaden mit Verteidigungsmöglichkeiten in Form von gestaffelten Sicherheitsebenen (Defense in Depth) und geregelten Security-Prozessen minimiert werden kann.

🗨️ [Leave a comment](#)

# Das Internet blutet

- **Kanadisches Finanzamt** - Sozialversicherungsnummern von 900 Personen entwendet
- **IP-Telefonie** - einige VoIP-Modelle von Cisco betroffen
- **Mobile Geräte** - Google Android in Version 4.1.1 betroffen
- **Netzwerkspeicher** - Hersteller Synology muss Firmwareupdate liefern
- **Internetdienste** – Google-Suche, GMail, YouTube, Play Store, Yahoo, Yahoo Mail, Instagram, Flickr, Tumblr, Amazon Web Services, Dropbox, Pinterest, Last Past, Soundcloud, GitHub, ...

# Szenario 2: Magento Webshop



The screenshot displays the Magento webshop interface. At the top, there is a dark navigation bar with the Magento logo on the left, a search bar with the text "Search entire store here..." and a "Search" button on the right, and a "Default welcome msg!" on the far right. Below the search bar, there are links for "My Account", "My Wishlist", "My Cart", "Checkout", and "Log In". The main content area is white and features the heading "Shopping Cart is Empty" followed by the text "You have no items in your shopping cart." and a link "Click [here](#) to continue shopping." The footer is a dark blue bar containing links for "About Us", "Customer Service", "Privacy Policy", "Site Map", "Search Terms", "Advanced Search", "Orders and Returns", and "Contact Us".

# Gegenmassnahmen

- Was muss ich tun?
- Wie kann ich mich schützen
- Sofortmassnahmen
- Defense in Depth

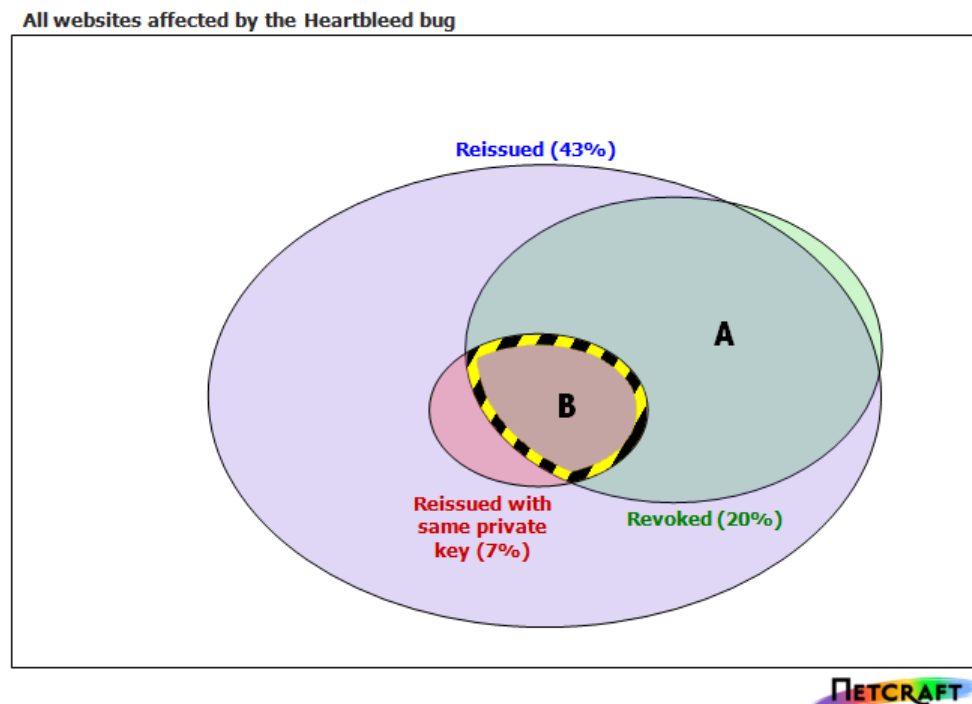
# Gegenmassnahmen - Sofortmassnahmen

- Betroffenes System vom Internet nehmen
- Patch einspielen
- Passwörter wechseln
- Zertifikate erneuern
- Altes Zertifikate revozieren



## ...und in der Realität?

- Studie von Netcraft (vom 9. Mai 2014) zeigt
- Immer noch 300'000 Webseiten verwundbar

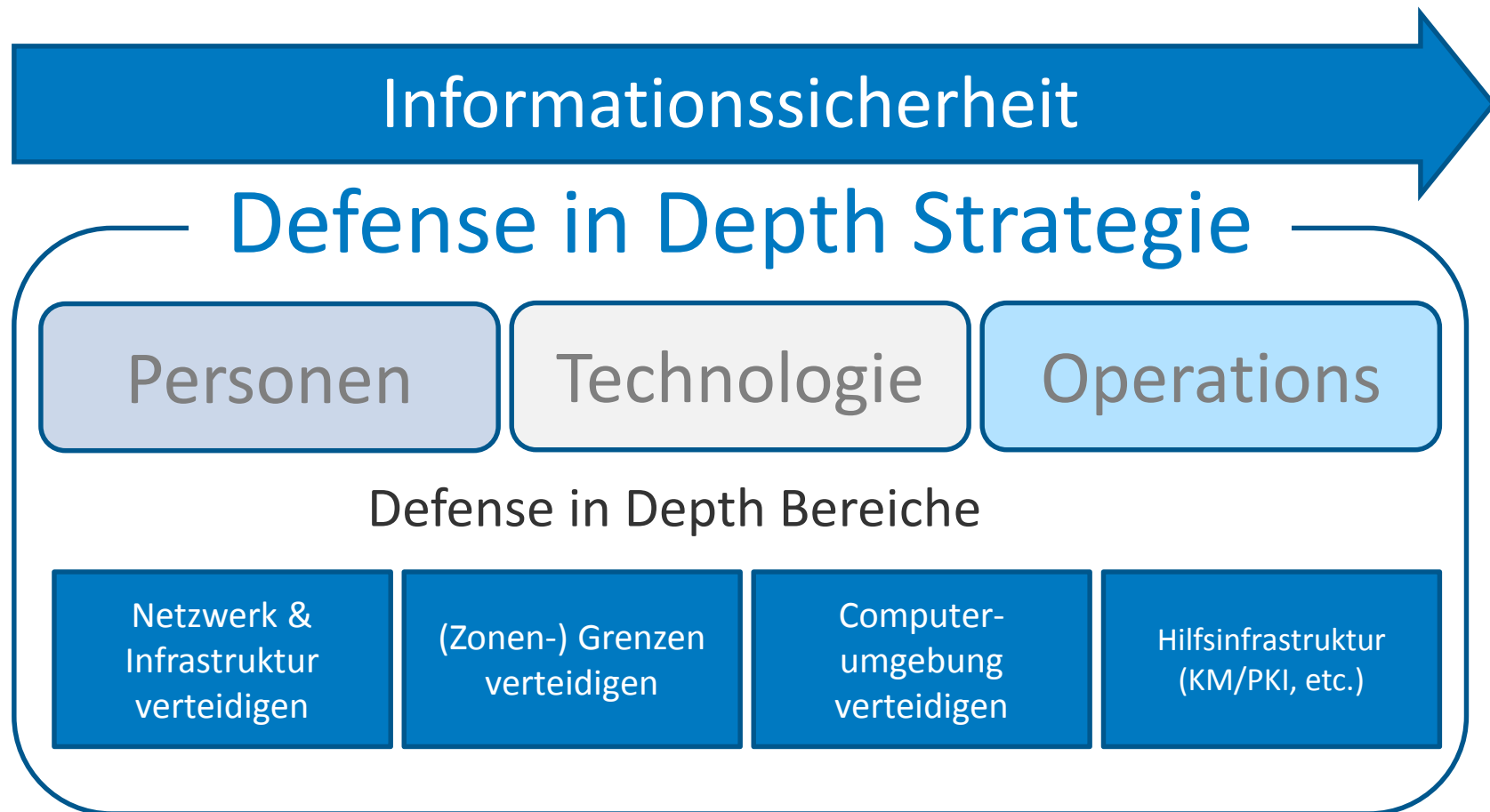


Quelle: <http://news.netcraft.com/archives/2014/05/09/keys-left-unchanged-in-many-heartbleed-replacement-certificates.html>

# Gegenmassnahmen – «Defense in Depth»

- Militärische Strategie: «Verzögerung statt dem Angreifer Raum freigeben»
- Platzierung von Schutzmechanismen, -verfahren und -politik soll Zuverlässigkeit eines IT-Systems erhöhen
- Mehrfache Schichten der Verteidigung sollen Spionage verhindern
- Angriffe gegen kritische Systeme verhindern
- Mehr Zeit zur Erkennung & Reaktion bei Angriffen
- Auswirkungen eines Einbruchs abschwächen

# «Defense in Depth» Strategie



# Beispiele für «Defense in Depth»

## → Netzwerk

- Demilitarisierten Zonen (DMZ)
- Paket-Filter / Firewalls
- Intrusion Detection Systeme (IDS)
- Intrusion Protection/Prevention Systeme (IPS)

## → Software / Malware

- Antivirus Software
- Sandboxing
- Endpoint Security

## → Vulnerability Scanner

## → Authentisierung und Passwortsicherheit

- Passwortrichtlinien
- Biometrische Sicherheitsmerkmale
- Hashing von Passwörtern
- Timed Access Control

## → Logging und Auditing

## → Physische Sicherheit

## → Awareness / Schulungen

- (Internet Security) Awareness Schulung

# «Defense in Depth» gegen Heartbleed



## → Netzwerk

- Demilitarisierten Zonen (DMZ)
- Paket-Filter / Firewalls
- Intrusion Detection Systeme (IDS)
- Intrusion Protection/Prevention Systeme (IPS)

## → Software / Malware

- Antivirus Software
- Sandboxing
- Endpoint Security

## → Vulnerability Scanner

## → Authentisierung und Passwortsicherheit

- Passwortrichtlinien
- Biometrische Sicherheitsmerkmale
- Hasing von Passwörtern
- Timed Access Control

## → Logging und Auditing

## → Physische Sicherheit

## → Awareness / Schulungen

- (Internet Security) Awareness Schulung

# Gegenmassnahmen – IT-Security Prozesse

- Rollen und Verantwortlichkeiten
- IT-Security als Teil des Projektmanagements
- Risiko Analyse
- Incident Response
- Verträge

# Fazit

- Ein wenig Statistik zum Schluss
- Erkenntnisse aus Heartbleed

# Ein wenig Statistik zum Schluss

→ <http://pacemaker.chokepointproject.net>



# 3933

websites from the Alexa Top 1 Million are still [heartbleeding](#).  
If you want, [this is the full list or urls, by rank](#).

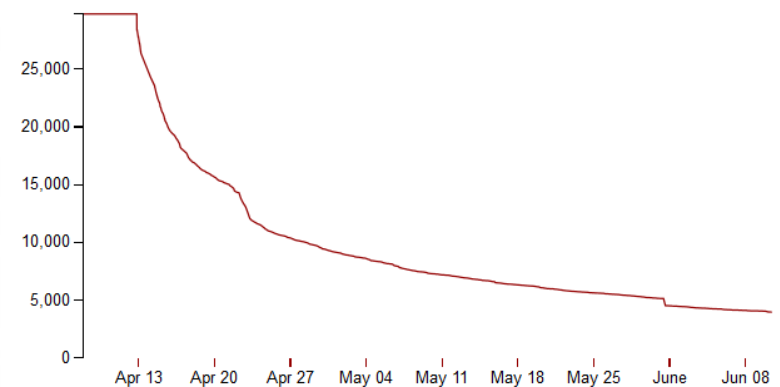
The last scan occurred at 2014-06-11 06:18:38.

 [Show patching rate graph](#)

We are using [this](#) to determine whether the url is still vulnerable.

Made by [Chokepoint Project](#)

Total URLs vulnerable to Heartbleed. [Back to counter](#)





# Erkenntnisse aus Fällen wie Heartbleed

- 100% sichere Software gibt es nicht!
- Grosse Verbreitung bedeutet auch grosse Verantwortung
- Open Source Software braucht Unterstützung
- Protokoll ist zu kompliziert
- Incident Handling vs. Defense in Depth
- Kennwörter sind von gestern

# Danke für Ihre Aufmerksamkeit! Fragen?



**Yves Kraft**

BSc FH CS, OPST&OPSA  
Senior Security Consultant

[yves.kraft@oneconsult.com](mailto:yves.kraft@oneconsult.com)  
+41 79 308 15 15

## **Hauptsitz**

OneConsult GmbH  
Schützenstrasse 1  
8800 Thalwil  
Schweiz  
Tel +41 43 377 22 22  
Fax +41 43 377 22 77  
[info@oneconsult.com](mailto:info@oneconsult.com)

## **Büro Deutschland**

Niederlassung der OneConsult GmbH  
Karlstraße 35  
80333 München  
Deutschland  
Tel +49 89 452 35 25 25  
Fax +49 89 452 35 21 10  
[info@oneconsult.de](mailto:info@oneconsult.de)

## **Büro Österreich**

Niederlassung der OneConsult GmbH  
Wienerbergstraße 11/12A  
1100 Wien  
Österreich  
Tel +43 1 99460 64 69  
Fax +43 1 99460 50 00  
[info@oneconsult.at](mailto:info@oneconsult.at)

