Hacking Day 2012 – Future Security

Incident Response – so reagieren Sie richtig

Christoph Baumgartner - CEO & Inhaber - OneConsult GmbH

oneconsult®
IT Security & Strategic Consulting

Agenda

- → Vorstellung
- → Der Fall DigiNotar
- → Situativ richtig reagieren
- → Massnahmen
- → Fazit

Über mich

- Christoph Baumgartner
- Studium der Wirtschaftsinformatik 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
- → Kompetenz
  - Mehr als 500 technische Security Audits (davon 450 OSSTMM konform)
  - Dutzende konzeptionelle Projekte
- → Standorte
  - Schweiz: Hauptsitz in Thalwil
  - Deutschland: Büro in München
  - Österreich: Büro in Wien

Unsere Dienstleistungen

→ Security Audits
- Security Scan
- Penetration Test
- Application Security Audit
- Ethical Hacking
- Social Engineering
- Conceptual Security Audit

→ Consulting
- Strategy & Organisation
- Policies & Guidelines
- Processes & Documentation
- Business Continuity & Disaster Recovery
- Engineering & Project Management

→ Incident Response
- Emergency Response
- Computer Forensics

→ Training & Coaching
- OSSTMM Zertifizierungskurse
- Practical Security Scanning
- Secure Software Development
- Coaching

→ Security as a Service

Agenda

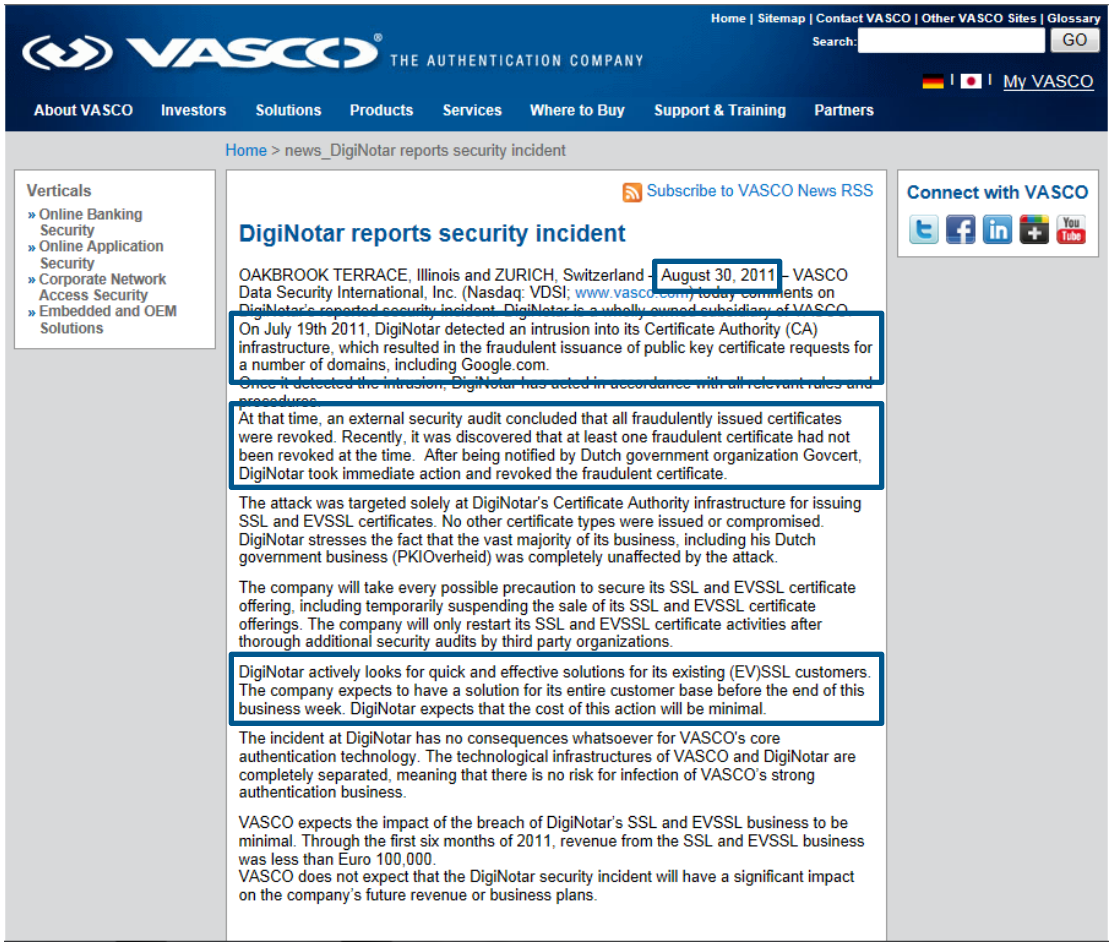
- → Vorstellung
- → Der Fall DigiNotar
- → Situativ richtig reagieren
- → Massnahmen
- → Fazit

DigiNotar BV

- 1997 gegründet und im Januar 2011 von VASCO Data Security International übernommen
- Dienstleistungen für Notare und Betrieb zweier CAs
  - Sub-CA der offiziellen PKI der holländischen Regierung
  - Kommerzielle CA
- Historie
  - 19. Juli 2011: DigiNotar erkennt Hackerattacke
  - 30. August 2011: VASCO verfasst Pressemitteilung
  - 20. September 2011: Insolvenz von DigiNotar
- Ausmass
  - Mehr als 500 gefälschte Zertifikate ausgestellt
  - Darunter weltbekannte Organisationen wie Facebook, Google, Microsoft, Mozilla, Skype, Thawte, die CIA und der Mossad
  - Gefälschte Zertifikate nachweislich zum Ausspionieren der iranischen Bevölkerung missbraucht (Mittels Man-in-the-Middle Attacke)

Datum	Aktienkurs USD VASCO (Close)
19.07.2011	13.44
30.08.2011	7.01
20.09.2011	5.10
12.06.2012	7.09

DigiNotar BV



Home | Sitemap | Contact VASCO | Other VASCO Sites | Glossary

Search: GO

VASCO THE AUTHENTICATION COMPANY

My VASCO

About VASCO | Investors | Solutions | Products | Services | Where to Buy | Support & Training | Partners

Home > news_DigiNotar reports security incident

Verticals

- Online Banking Security
- Online Application Security
- Corporate Network Access Security
- Embedded and OEM Solutions

Subscribe to VASCO News RSS

DigiNotar reports security incident

OAKBROOK TERRACE, Illinois and ZURICH, Switzerland – August 30, 2011 – VASCO Data Security International, Inc. (Nasdaq: VDSI; www.vasco.com) today comments on DigiNotar's reported security incident. DigiNotar is a wholly owned subsidiary of VASCO.

On July 19th 2011, DigiNotar detected an intrusion into its Certificate Authority (CA) infrastructure, which resulted in the fraudulent issuance of public key certificate requests for a number of domains, including Google.com.
Once it detected the intrusion, DigiNotar has acted in accordance with all relevant rules and procedures.

At that time, an external security audit concluded that all fraudulently issued certificates were revoked. Recently, it was discovered that at least one fraudulent certificate had not been revoked at the time. After being notified by Dutch government organization Govcert, DigiNotar took immediate action and revoked the fraudulent certificate.

The attack was targeted solely at DigiNotar's Certificate Authority infrastructure for issuing SSL and EVSSL certificates. No other certificate types were issued or compromised. DigiNotar stresses the fact that the vast majority of its business, including his Dutch government business (PKIOverheid) was completely unaffected by the attack.

The company will take every possible precaution to secure its SSL and EVSSL certificate offering, including temporarily suspending the sale of its SSL and EVSSL certificate offerings. The company will only restart its SSL and EVSSL certificate activities after thorough additional security audits by third party organizations.

DigiNotar actively looks for quick and effective solutions for its existing (EV)SSL customers. The company expects to have a solution for its entire customer base before the end of this business week. DigiNotar expects that the cost of this action will be minimal.

The incident at DigiNotar has no consequences whatsoever for VASCO's core authentication technology. The technological infrastructures of VASCO and DigiNotar are completely separated, meaning that there is no risk for infection of VASCO's strong authentication business.

VASCO expects the impact of the breach of DigiNotar's SSL and EVSSL business to be minimal. Through the first six months of 2011, revenue from the SSL and EVSSL business was less than Euro 100,000.
VASCO does not expect that the DigiNotar security incident will have a significant impact on the company's future revenue or business plans.

Connect with VASCO

Was lief schief?

- Mangelhafte Sicherheitsmassnahmen (laut Aussage des Auditors)
  - In gleicher Domäne
  - Schwache Passwörter
  - Mangelhafter Schutz vor Malware
  - usw.
- Versuch, die Hackerattacke
  - Zu verschweigen
  - Nach Bekanntwerden deren Folgen zu beschönigen
- Folgen
  - Verlust der Vertrauenswürdigkeit (bei Softwareherstellern & Abstrafung an Börse)
  - Alle von DigiNotar ausgegebene Zertifikate mussten für ungültig erklärt und von Software erkannt werden -> diverse Patches und Software-Updates
  - Gesamte Zertifizierungsbranche betroffen:
    - Aufwand
    - Image-Schäden

Richtige Reaktion

→ Sofortmassnahmen
- Zertifikatsausstellung unterbrechen
- Hackerattacke stoppen/verhindern (z.B. Systemzugriff via Internet verunmöglichen)
- Geschäftsleitung und Inhaber informieren
- Untersuchung des Vorfalls initiieren
  - Vorkommnis
  - Schadensausmass und Auswirkungen
  - Kontakt mit Behörden und evtl. mit Spezialisten aufnehmen

→ Innert 12 h
- Andere CAs und Kunden informieren
- Medienmitteilung veröffentlichen und laufend aktualisieren (mit Erkenntnissen und News)

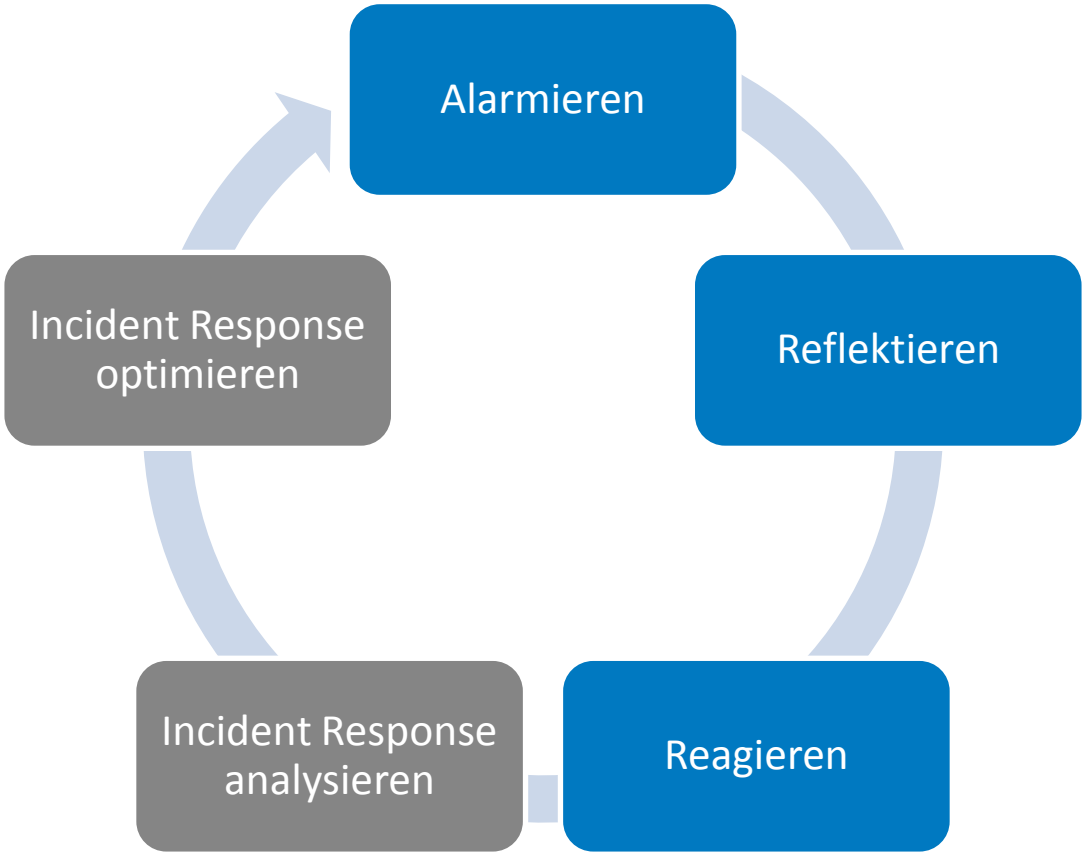
Agenda

- → Vorstellung
- → Der Fall DigiNotar
- → Situativ richtig reagieren
- → Massnahmen
- → Fazit

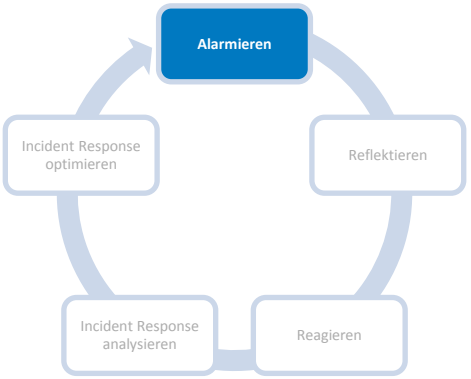
Grundsätze

- → **Keine Organisation** ist vor Security Incidents **gefeit**
- → Je **grösser**, **erfolgreicher** und/oder **bekannter** eine Organisation, desto **höher** die **Eintrittswahrscheinlichkeit** von Security Incidents
- → Es gibt bei Hacker- und Malware-Attacken oder Datendiebstahl nicht **das eine richtige Vorgehen**, sondern es geht darum, die Strategie **mit den geringsten** (potenziell) unerwünschten **Nebenwirkungen** zu erkennen und konsequent **umzusetzen**.

Incident Response-Prozess



Phase 1: Alarmieren



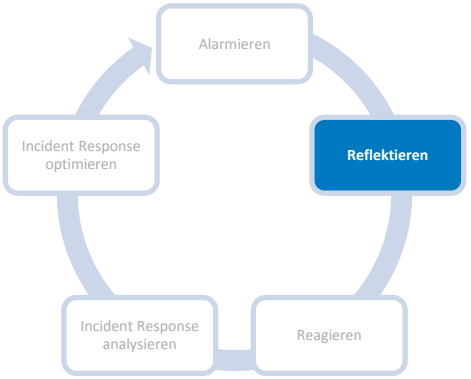
→ Wen informieren?

- Informationssicherheitsverantwortlichen (CISO, SSO, Leiter IT, CIO, etc.) oder Vorgesetzten
- Nicht Geschäftsleitung (weil anderer Fokus, wird anschliessend vom Informationssicherheitsverantwortlichen informiert)

→ Information über

- Typ des Vorfalls
- Zeitpunkt (Vorfall bzw. Entdeckung)
- Auswirkungen / Schaden bisher (soweit abschätzbar)

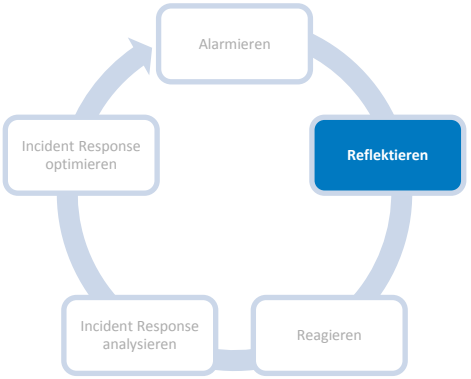
Phase 2: Reflektieren (1)



- → Nachdenken!
- → Folgende Punkte klären
  - Höhe Schadensausmass in zeitlicher Abhängigkeit?
  - Nur direkte Schadensbegrenzung oder rechtliche Schritte gegen Verursacher offenhalten?
  - Höhe des Risikos von Kollateralschäden?
  - Mögliche Lösungsansätze
    - technische,
    - organisatorische,
    - oder rechtliche

    und deren direkte und indirekte Konsequenzen
    - rechtliche,
    - finanzielle,
    - und Firmen-Image-relevant
  - Lösung mit Bordmitteln möglich oder externe Hilfe benötigt?

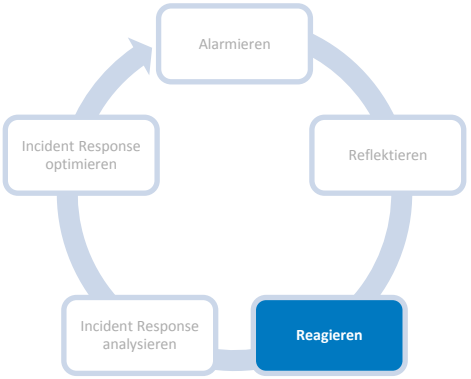
Phase 2: Reflektieren (2)



→ Juristische Stolpersteine
- Rechtsabteilung/Juristen nach Möglichkeit in Entscheidungsfindung einbeziehen
- Spezialisten für forensische Analysen beiziehen

→ Informationspolitik: Vorfall kommunizieren oder verheimlichen?

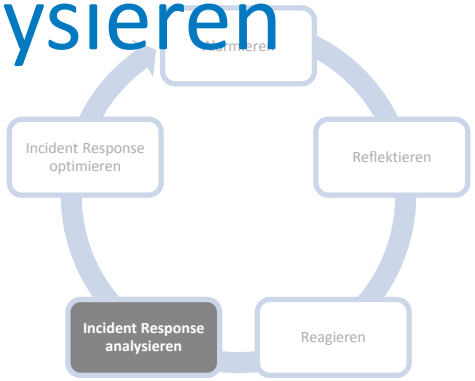
Phase 3: Reagieren



→ Sobald Entscheid gefallen ist, Massnahme(n)
- kommunizieren (intern und evtl. extern),
- umsetzen,
- und dokumentieren

→ Zeit messen

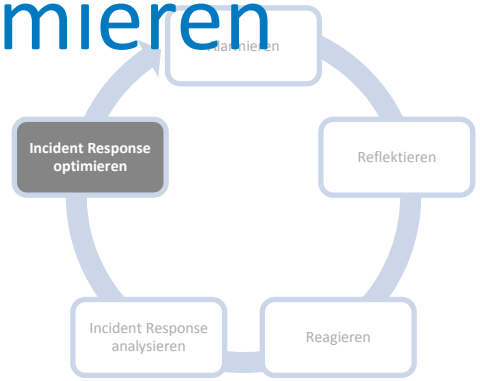
Phase 4: Incident Response analysieren



→ Erwartungen erfüllt?
- Qualität der Massnahme(n)
- Aufwand und Kosten
- Dauer
- Auswirkungen

→ Verbesserungspotential?
- Alarmierungsprozess
- Ausbildung
- Ressourcenplanung
- Kommunikation
- etc.

Phase 5: Incident Response optimieren



→ Optimierungen durchführen

- Organisation
  - Aufbau (Organigramm)
  - Ablauf (Prozesse)
  - Vorgaben
- Ressourcen
  - Human Resources
  - Hard- und Software
  - Services

Beispiel 1: Hacker- und Malware-Attacke

→ Prämisse: **Verzicht auf strafrechtliche Verfolgung** zugunsten möglichst rascher Wieder-Verfügbarkeit

→ Vorgehen

1. Betroffenes System temporär vom Netz nehmen (evtl. Ersatzsystem oder Info-Seite aufschalten)
2. Letzte nicht kompromittierte Datensicherung einspielen
3. System härten
4. System mittels eines Security Scan oder Penetration Test auf Sicherheitslücken überprüfen
5. Falls nötig erneut härten und überprüfen
6. System wieder ans Netz anschliessen

Beispiel 2: Datendiebstahl

→ Prämisse: (un)bekannte Person(en) in-Flagranti ertappt

→ Vorgehen

1. Sicherheitsdienst oder den Informationssicherheitsverantwortlichen rufen lassen
2. Betroffene(n) Person(en) nach Möglichkeit verbal an weiteren Manipulationen und am Verlassen des Raumes hindern, ohne handgreiflich zu werden!

→ Vermeintliche Heldentaten sind hier fehl am Platz!

Agenda

- → Vorstellung
- → Der Fall DigiNotar
- → Situativ richtig reagieren
- → Massnahmen
- → Fazit

Technische Massnahmen

- → Systemhärtung
- → Redundante Systeme/Komponenten
- → Ersatzsysteme/-komponenten (vor-Ort/beim Lieferanten)
- → Firewalls (Network- & Data Centric)
- → Netzwerkzonierung
- → Schutz vor Malware
- → Intrusion Detection & Prevention Systeme (Netzwerk- und Host-basiert)
- → Access, Transaction & Network Logging & Monitoring
- → Datenverschlüsselung
- → Backup
- → Load Balancer
- → Kameraüberwachung
- → …

Organisatorisch/konzeptionelle Massnahmen (1)

→ Risikoanalyse und -beurteilung
- Welchen Gefahren ist das Unternehmen ausgesetzt?
- Wie hoch sind Eintrittswahrscheinlichkeit und potenzielle Schadenshöhe?

→ Klassifikation von Informationen/Daten
- Was ist schützenswert?
- Wie hoch ist der Schutzbedarf?

→ Dokumente
- Informations-/IT-Sicherheitsstrategie
- Zielgruppengerechte Reglemente und Handlungsanweisungen
- Setup- und Hardening Guides
- …

Organisatorisch/konzeptionelle Massnahmen (2)

- → Security Awareness
- → Change Management Prozess
  - Was?
  - Wann?
  - Wer?
  - Ausnahmen?
- → Notfallszenarien
  - Detaillierte Notfallpläne
  - Notfallübungen
- → Hilfestellung zu möglichen Massnahmen beispielsweise in
  - ISO/IEC Normenfamilie 2700x
  - BSI-Standards 100-x

Agenda

- → Vorstellung
- → Der Fall DigiNotar
- → Situativ richtig reagieren
- → Massnahmen
- → Fazit

Fazit

- → Jeden kann es treffen
- → Zuerst denken dann handeln
- → Strategie mit den geringsten (potenziell) unerwünschten Nebenwirkungen erkennen und konsequent umsetzen
- → Präventive Massnahmen treffen
- → Übung macht den Meister

Danke für Ihre Aufmerksamkeit! Fragen?

Christoph Baumgartner
MSc UZH IS, OPST
CEO & Owner

christoph.baumgartner@oneconsult.com
+41 79 256 25 25

Hauptsitz
OneConsult GmbH
Schützenstrasse 1
8800 Thalwil
Schweiz

Tel +41 43 377 22 22
Fax +41 43 377 22 77
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

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