APT Lifecycle

Von der Kompromittierung zum gezielten Datenabfluss

Digicomp Hacking Day 2015

Referenten: Yves Kraft, Immanuel Willi

www.oneconsult.com

Agenda

- Einführung
- Phasen einer APT-Attacke
- Gegenmassnahmen
- APT Fallbeispiel
- Fazit

Einführung

Über uns

Yves Kraft

Senior Penetration Tester &
Security Consultant

- BSc FH CS, ISO 27001 Lead Auditor, LPIC, OPST, OPSA, OPSE, OSSTMM Trainer
- Kursleiter bei Digicomp
  [Kurscodes PSI, PSO, PST, SWO, TSA]
- Technische Security Audits
- Konzeptionelles Consulting
- Schulung & Coaching
- Security Officer

Immanuel Willi

Senior Security Consultant &
Penetration Tester

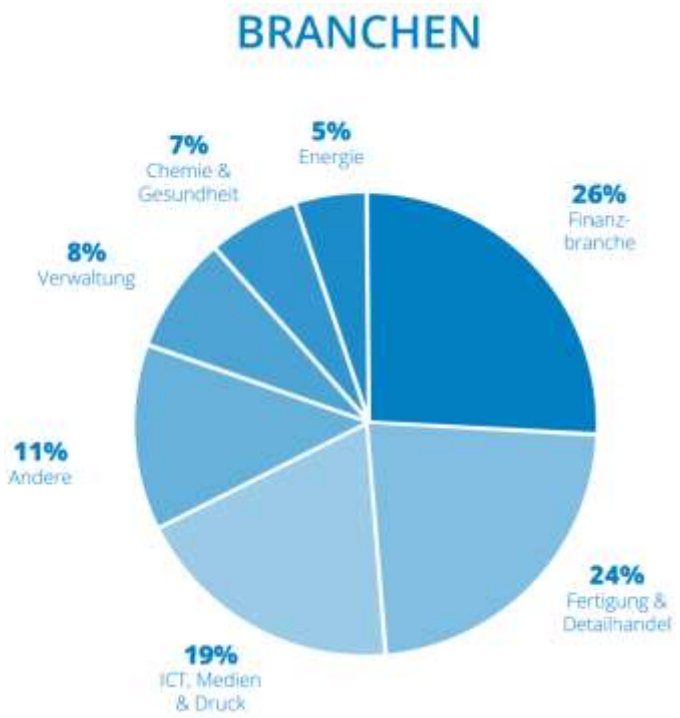
- BSc FH CS, CISSP, OSWP, ITIL Foundation, OPST
- Technische Security Audits
- Konzeptionelles Consulting
- Security Officer

Oneconsult AG

- Holistic Cyber Security Consultancy
- Produkt- und herstellerunabhängig
- in Privatbesitz seit 2003
- Büros in der Schweiz und in Deutschland
- 250+ internationale Kunden
- 1000+ Security-Projekte

Zahlen und Fakten

- 20+ Mitarbeitende, keine Freelancer
- Zertifizierte Security-Experten mit neusten Hacking-Techniken
- Eines der grössten Penetration Tester Teams in der Schweiz
- Research Team entdeckt 40+ Zero-Day Schwachstellen/Jahr
- Mitglied von OWASP, ISECOM, ISSS, SCE



Unser Angebot

Schutz vor externen und internen Cyber-Bedrohungen: APT, Hacker-Angriffe, Malware-Befall, digitaler Betrug, Datendiebstahl etc.

APT Angriffe in den Medien

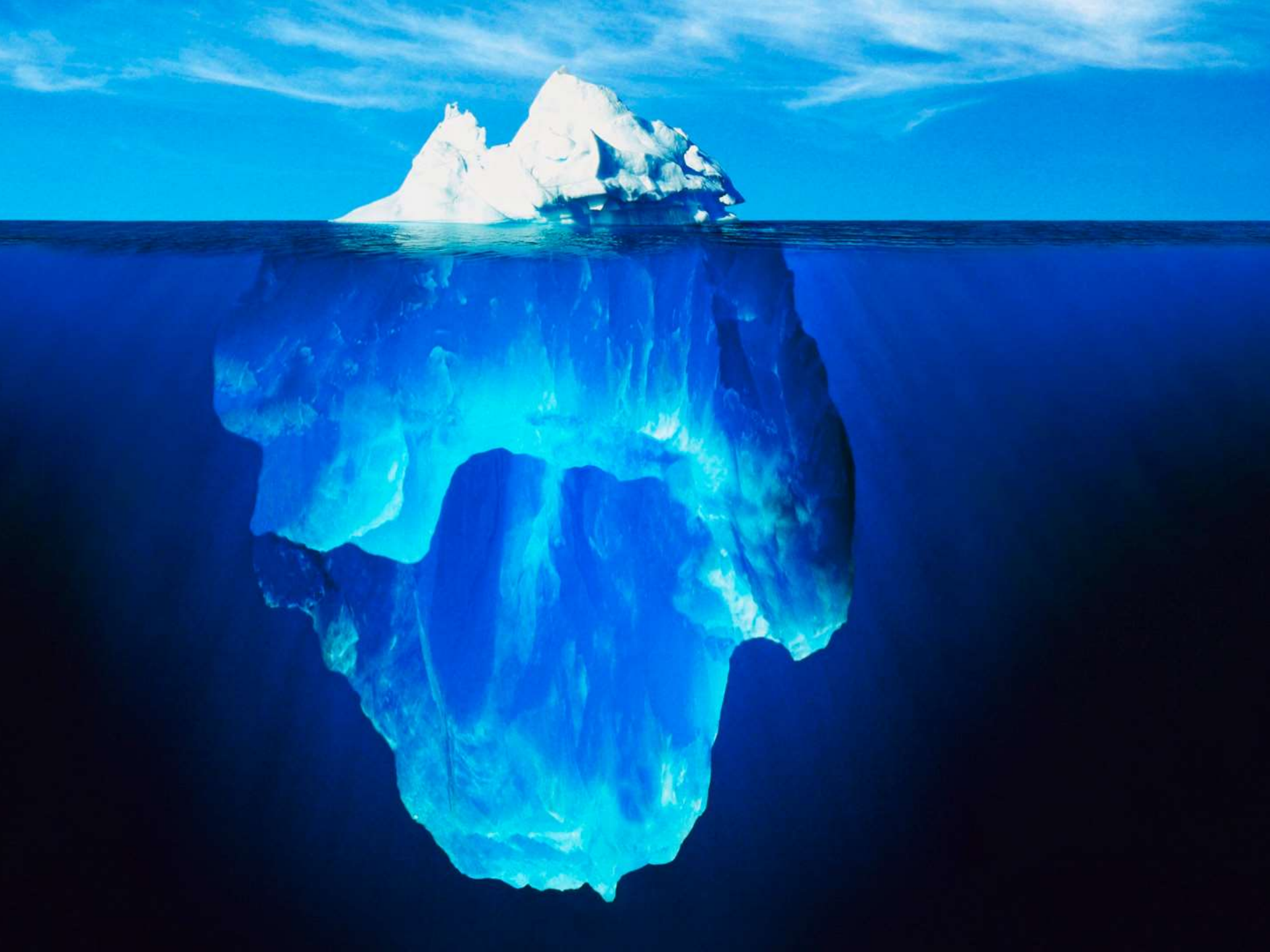
1987:	The Cuckoo's Egg
2003:	Titan Rain
2006:	Sykipot
2009	GhostNet
2009:	Operation Aurora
2007:	Gozi
2007:	Zeus
2009:	SpyEye
2010:	**Stuxnet**
2011:	Duqu
	RSA Attacke
2012:	Flame
	Red October
	Eurograbber
2014:	Sony
	Karbanak
2015:	Kaspersky/Duqu 2.0
	Ashley Madison

Quelle: http://www.itbusinessedge.com/slideshows/the-most-famous-advanced-persistent-threats-in-history.html

Dokumentierte APT Angriffe 2015 (Q1-Q2)

Jan 11 - Hong Kong SWC attack
Jan 12 - Skeleton Key Malware Analysis
Jan 15 - Evolution of Agent.BTZ to ComRAT
Jan 20 - Analysis of Project Cobra
Jan 20 - Reversing the Inception APT malware
Jan 22 - The Waterbug attack group
Jan 22 - Scarab attackers Russian targets | IOCs
Jan 22 - Regin's Hopscotch and Legspin
Jan 27 - Comparing the Regin module 50251 and the "Qwerty" keylogger
Jan 29 - Backdoor.Winnti attackers and Trojan.Skelky
Jan 29 - Analysis of PlugX Variant - P2P PlugX
Feb 02 - Behind the Syrian Conflict's Digital Frontlines
Feb 04 - Pawn Storm Update: iOS Espionage App Found
Feb 10 - CrowdStrike Global Threat Intel Report for 2014
Feb 16 - Equation: The Death Star of Malware Galaxy
Feb 16 - The Carbanak APT
Feb 16 - Operation Arid Viper
Feb 17 - A Fanny Equation: "I am your father, Stuxnet"
Feb 17 - Desert Falcons APT
Feb 18 - Shooting Elephants
Feb 18 - Babar: espionage software finally found and put under the microscope
Feb 25 - PlugX goes to the registry (and India)
Feb 25 - Southeast Asia: An Evolving Cyber Threat Landscape
Feb 27 - The Anthem Hack: All Roads Lead to China
Feb 24 - A deeper look into Scanbox
Mar 05 - Casper Malware: After Babar and Bunny, Another Espionage Cartoon
Mar 06 - Animals in the APT Farm
Mar 06 - Is Babar a Bunny?
Mar 10 - Tibetan Uprising Day Malware Attacks
Mar 11 - Inside the EquationDrug Espionage Platform
Mar 19 - Rocket Kitten Showing Its Claws: Operation Woolen-GoldFish and the GHOLE campaign
Mar 31 - Volatile Cedar – Analysis of a Global Cyber Espionage Campaign
Apr 12 - APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation
Apr 15 - The Chronicles of the Hellsing APT: the Empire Strikes Back
Apr 16 - Operation Pawn Storm Ramps Up its Activities; Targets NATO, White House
Apr 18 - Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack
Apr 20 - Sofacy II – Same Sofacy, Different Day
Apr 21 - The CozyDuke APT
Apr 22 - CozyDuke
Apr 27 - Attacks against Israeli & Palestinian interests
May 07 - Dissecting the Kraken
May 12 - root9B Uncovers Planned Sofacy Cyber Attack Targeting Several International and Domestic Financial Institutions
May 13 - SPEAR: A Threat Actor Resurfaces
May 14 - The Naikon APT
May 14 - Operation Tropic Trooper
May 18 - Cmstar Downloader: Lurid and Enfal's New Cousin
May 19 - Operation 'Oil Tanker'
May 21 - The Naikon APT and the MsnMM Campaigns
May 26 - Dissecting-Linux/Moose
May 27 - Analysis On Apt-To-Be Attack That Focusing On China's Government Agency'
May 28 - Grabit and the RATs
May 29 - OceanLotusReport
Jun 03 - Thamar Reservoir
Jun 04 - Blue Thermite targeting Japan (CloudyOmega)
Jun 10 - Crysys Lab - Duqu 2.0
Jun 10 - The_Mystery_of_Duqu_2_0 IOC Yara
Jun 15 - Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114
Jun 16 - Operation Lotus Bloom
Jun 22 - Winnti targeting pharmaceutical companies
Jun 24 - UnFIN4ished Business (FIN4)
Jun 26 - Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign
Jun 28 - APT on Taiwan - insight into advances of adversary TTPs
Jun 30 - Dino – the latest spying malware from an allegedly French espionage group analyzed

Quelle: https://github.com/kbandla/APTnotes



APT Lifecycle

Phasen einer APT-Attacke

Vorbereitung | Infektion | Verteilung | Persistenz

Vorbereitung | Infektion | Verteilung | Persistenz

Vorgehen

- Zielauswahl für Angriff
  - Personen
  - Systeme
- Suche nach
  - Schwachstellen
  - Informationen zur Organisation
    - Google
    - Firmenwebseite
  - Namen und Funktionen von Mitarbeitenden
    - Social Media (Facebook, LinkedIn, XING, etc.)

Vorbereitung | Infektion | Verteilung | Persistenz

Vorgehen

- Direkter Angriff exponierter Systeme
- Social Engineering
  - Phishing E-Mail
  - Rouge Access Point
  - Evil Maid
  - Bad-USB
- Drive-by-Infections
  - Bsp. Adobe Flash
- Infektion privater Rechner
  - BYOD
  - Telearbeitsplätze

Vorbereitung | Infektion | **Verteilung** | Persistenz

Vorgehen

- Kommunikation zu Angreifer
  - Herstellen
  - Persistenz der Sitzung herstellen
- Ausweitung der Rechte
  - Benutzer zu Administrator
  - Lokal zu Domäne
- «Interessante» Daten sammeln
  - Keylogger
  - Dateisystem
  - SSH Schlüssel
  - …

Vorbereitung | Infektion | Verteilung | **Persistenz**

Vorbereitung | Infektion | Verteilung | **Persistenz**

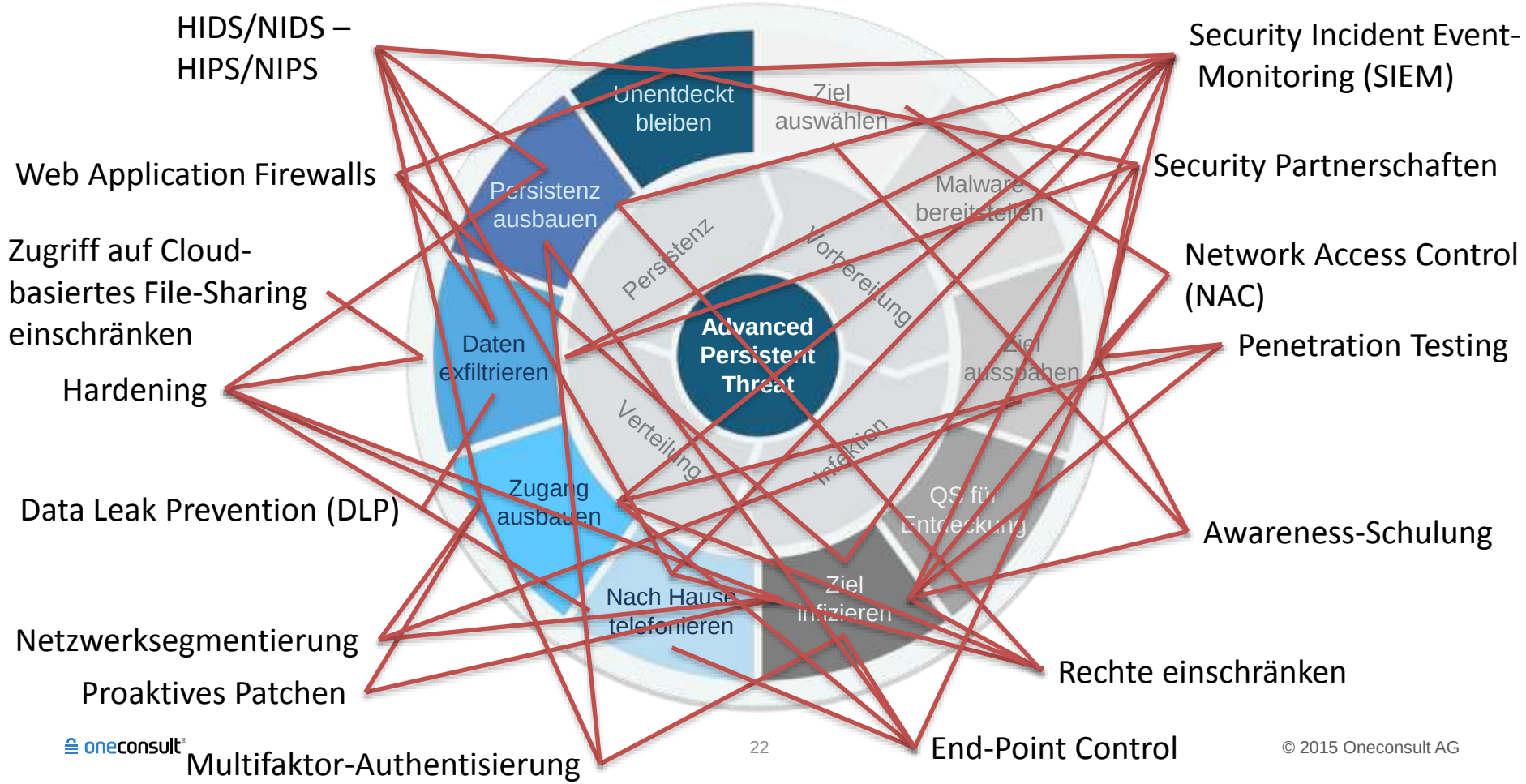
Vorgehen

- Daten-Exfiltration
  - Anti «Data-Leakage-Prevention» Massnahmen
  - Automatisierung
- Langfristige Persistenz sicherstellen
  - Regelmässige Verbindungsherstellung zum Angreifer
  - Neue Benutzer erstellen
  - Rootkit Funktionalität implementieren
- Spuren verwischen
  - Log-Daten/Zeitstempel löschen oder fälschen
  - Malware aus Infektionsphase löschen

Gegenmassnahmen

Gibt es ein Patentrezept?

Wirkung im APT Lifecycle



APT Fallbeispiel

APT Fallbeispiel

Vorbereitung

Informationen sammeln
Ziel auswählen

Infektion

Bad-USB Angriff
Anti AV Mechanismen

Verteilung

Rechte ausweiten
Key Logger

Persistenz

Persistenz via Scheduler

Fazit

Fazit

- Momentane APT-Attacken werden vorwiegend von Regierungen durchgeführt
  - Ziel/Motiv: klassische Spionage, Sabotage
- Cyber-Kriminelle greifen in der Regel bei finanziell lohnenswerten Zielen auf APTs zurück
  - Ziel/Motiv: Wirtschaftsspionage, E-Banking
- APT-Attacken erfolgen in mehreren Phasen, die meist über längere Zeit andauern
- APT ist nächster Evolutionsschritt der Internetkriminalität
- Die Frage ist nicht ob, sondern wann ein Angreifer sein Ziel erreicht!
- Gezielte Abwehrstrategien und technische Tools einsetzen, die für jede Phase eines APT-Angriffs am effektivsten wirken

Vielen Dank für Ihre Aufmerksamkeit!

Yves Kraft
BSc FH CS, ISO 27001 Lead Auditor,
OPST, OPSA & OPSE, OSSTMM Trainer

Team Leader Bern
Senior Penetration Tester & Security Consultant

yves.kraft@oneconsult.com
T +41 31 327 15 16
M +41 79 308 15 15

Immanuel Willi
BSc FH CS, CISSP, OSWP, ITIL Foundation,
OPST

Senior Security Consultant & Penetration Tester

immanuel.willi@oneconsult.com
T +41 31 327 15 55
M +41 79 135 25 25

Hauptsitz
Oneconsult AG
Schützenstrasse 1
8800 Thalwil
Schweiz

Tel +41 43 377 22 22
Fax +41 43 377 22 77
info@oneconsult.com

Oneconsult AG
Bärenplatz 7
3011 Bern
Schweiz

Tel +41 31 327 15 15
Fax +41 31 327 15 25
info@oneconsult.com

Deutschland
Niederlassung der Oneconsult AG
Karlstraße 35
80333 München

Tel +49 89 452 35 25 25
Fax +49 89 452 35 21 10
info@oneconsult.de