



sic[!]sec

Information Security Services



Because your data is priceless.

sic[!]sec

Hacker-Typen und Hacker-Angriffe

„vorsätzlich handelnde Angreifer im Cyberraum“
(vgl. Quelle [BSI 1])

Ralf Reinhardt,
sic[!]sec GmbH

7. Cyber-Sicherheits-Tag
12.11.2014, 15:45 -16:10



Bundesministerium für Umwelt,
Naturschutz, Bau und Reaktorsicherheit, BMUB

Robert-Schuman-Platz 3
53175 Bonn

Ralf Reinhardt

- Principal Consultant und GGF sic[!]sec GmbH, Dipl.-Inf. (FH), CISSP, ITIL Service Manager
- Lehrbeauftragter „Web Application Security“, TH N
- „OWASP“ Project Leader, „ISSECO“ Mitglied
- Mitglied Expertengruppe „Nationale Wirtschaftsschutzstrategie 2015“ für den DIHK-Tag
- 24 Jahre Mitglied im CCC, 28 Jahre IT-Erfahrung, darunter Client-, Server- und Datenbank-Prog., Administration, Rollout, Betrieb, Wartung, usw.

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

3

sic[!]sec GmbH, Information Security Services („Hacker-Zeugs“)

- Penetrationstests
- Reverse Engineering
- Source Code Analysen
- Web Application Firewalls
- Digitale Forensik
- Physical Security
- Social Engineering
- Guidelines und Policies
- Workshops, Trainings und Schulungen
- Reviews und Audits



Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

4

Hinweise zum Vortrag

- Dieser Vortrag ist die **Privatmeinung** von **Ralf Reinhardt**. Die Fakten wurden willkürlich ausgewählt und subjektiv interpretiert.
- der „*Hacker*“, die „*Haeckse*“ (auch „*Häckse*“), unbestimmt: „queer hacker“

Über „Hacking“ (*Tech Model Railroad Club, 50er / 60er Jahre*)

*>> [...] "hacker" [...] in its original meaning, someone who **applies ingenuity to create a clever result, called a "hack"**. The essence of a "hack" is that it is done quickly, and is usually inelegant. [...]*

*Despite often being at odds with the design of the larger system, a **hack is generally quite clever and effective** << [TMRC 1]*

TMRC - Hackers

tmrc.mit.edu/hackers-ref.html

Home | Store | About | Progress | TNP | Videos | Visit | Links

tmrc Hackers



We at TMRC use the term "hacker" only in its original meaning, someone who applies ingenuity to create a clever result, called a "hack". The essence of a "hack" is that it is done quickly, and is usually inelegant. It accomplishes the desired goal without changing the design of the system it is embedded in. Despite often being at odds with the design of the larger system, a hack is generally quite clever and effective.



Also see the [definition of "hacker" in the on-line version of the New Hacker's Dictionary](#).

Reference info related to TMRC



This section lists books and other major publications that reference TMRC.

The [Tech Model Railroad Club](#) is featured as the first chapter of *Hackers*, by Steven Levy (New York: Anchor Press/Doubleday, 1984). It is credited as one (possibly the primary) source of the Hacker Culture the book describes.



Several entries in *The New Hacker's Dictionary*, (Second Edition, edited by Eric S. Raymond (MIT Press, 1993); ISBN 0-262-68079-3) are derived from [Abridged Dictionary of the TMRC Language](#). There is also an [online version](#) of the book's content.

The cover article in *Railroad Model Craftsman*, July 1986 was a preview of the club for the 1986 NMRA convention held in Boston. A converted copy of the [text we submitted](#) is available online.

[Tech Model Railroad Club of MIT](#)
 MIT Room N52-118
 265 Massachusetts Avenue
 Cambridge, MA 02139

+1 617 253-3269
 x3-3269 (on campus)
 Email: tmrc-web@mit.edu
 Generated Fri Jul 25 07:19:57 2014
 in 0.048 secs

sic[!]sec

<http://de.wikipedia.org/wiki/Hacker>

>> [...] Wau Holland [...]: „**Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann**“.[...]

[...] um das Experimentelle, den Versuch, **die Grenzen des Machbaren zu erkunden**. Die Durchführung [...] wird *Hacken* genannt;[...]

[...] mit einem besonderen Sinn für Kreativität und Originalität („hack value“). Das Ergebnis ist **ein Hack**. [...] <<

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe
 © 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

Über „Hacking“ (Hackerethik, Steven Levy 1984, CCC später)

- „Die ethischen Grundsätze des Hackens – Motivation und Grenzen:
 - Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
 - Alle Informationen müssen frei sein.
 - Mißtraue Autoritäten – fördere Dezentralisierung.
 - Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung.
 - Man kann mit einem Computer Kunst und Schönheit schaffen.
 - Computer können dein Leben zum Besseren verändern.
 - [Ende der 80er:] Müsse nicht in den Daten anderer Leute.*
 - [Anfang der 90er:] Öffentliche Daten nützen, private Daten schützen.“*
- Quelle: [CCC 1]

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

9

Über die Hutfarbe von Hackern

- White Hat**
 - Handelt „ethisch“ innerhalb der Gesetze
 - Black Hat**
 - Achtet nicht auf Gesetze, oft mit kriminellen Absichten
 - Gray Hat**
 - Eine „Mischung“, der zur Erreichung eines „höheren Ziels“ Gesetzesverstöße (bewusst) in Kauf nimmt
- 

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

10

Der Sicherheitsforscher



- **Wissenschaftler, Studenten und Hobbyisten**
- **Akademisches Interesse** an der Entdeckung und Analyse von Sicherheitslücken; Drang, ein **White-Paper**, einen **Vortrag** oder einen **PoC** zu veröffentlichen

Der Sicherheitsforscher

- **Forschung ist oft langwierig** (über Wochen und Monate)
- Das **Angriffsziel** sind eher Hersteller und ihre „**sicheren**“ **Produkte**.
- Klassische Untersuchungen „**im Labor**“: Reverse Engineering, Source Code Analysen, Protokoll Analysen, Seitenkanal-Angriffe, Debugging, usw.
- **Durchführung eines PoC** gelegentlich „In The Wild“ zu „Awarness-Zwecken“ → „Medien-S.“

Der Sicherheitsforscher

- Sicherheitsforscher will, dass eine Schwachstelle gefixt und er als Entdecker bekannt wird
→ „**Wettlauf**“ um die „**Entdeckung**“
- **Gefahren und Risiken sind indirekter Natur**
(wenn Sie kein unfähiger und / oder unwilliger Hersteller sind) durch **full disclosure**:
 - **Zero-Day** wird „über Nacht“ zur **kown vulnerability** / public knowledge, ohne dass ein Fix existiert
 - **Zigtausend produktive Systeme** betroffen und ggf. für Tage bis Wochen „**exploitable**“
 - **Black-Hats** → Windhundrennen um „**juicy targets**“

Das Skriptkiddie



Analogie: Mittelmäßig begabtes Kind findet eine **geladene Waffe** („weaponized exploit“) für eine **bestimmte Art von Ziel, sucht ein solches (x-beliebiges) Ziel willkürlich aus und drückt ab**, um mal zu sehen, was passiert.

Das Skriptkiddie, „Skiddie“

- **Anwender**, der **ein Programm** („Skript“) abtippen oder herunterladen und **starten** kann.
- **Kein tiefes KnowHow** vorhanden.
- Warum: **Skiddies wollen** einfach mal „in the wild“ **ausprobieren, ob „das Skript“ funktioniert**.
- Kein finanzielles Interesse, evtl. **Geltungssucht** oder ein **Zugehörigkeitswunsch** zu einer Gruppe.

Das Skriptkiddie, „Skiddie“

- Wie: Skiddie sucht gezielt nach einer **bestimmten Vulnerability** (z.B. mit einem Scanner), für die sein „Skript“ geschrieben wurde. **Opfer-Auswahl zufällig / unspezifisch**.
- Gefahren und Risiken: **Abhängig von** der jeweiligen **Schwachstelle** → Alles von **DoS bis** hin zur **vollständigen Kompromittierung** des betroffenen Systems und seiner Daten
- „**Known vulnerabilities**“ und „**low hanging fruits**“ werden ausgenutzt.

Der Hacktivist

- **"Cyber-Aktivisten:**
Angreifer, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen" [BSI 1]
- 21.01.2008, **Anonymous** veröffentlicht „Message to Scientology“ [ANON 1]

Der Hacktivist



- Einige, **wenige Köpfe mit hohen Skills**
 - **Aktives, bewusstes Hacken**, meist gerechtfertigt durch moralische Überlegenheit und / oder ein höheres Ziel.
- Bei großen „Organisationen“ wie Anonymous
 - **Viele Mitläufer** mit Skriptkiddie-Fähigkeiten

DDoS durch „LOIC“ und Skiddies



Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

19

Lulz Security

- Beispiel: LulzSec / Lulz Security (vgl. LOL, LULZ)
- Warum: „**4 da LULZ**“, „Weil es uns Spaß macht (und Ihr es verdient habt)“, Presse: „Spaßguerilla“
- Bei den Zielen war immer ein gesellschaftspolitischer und kein pekuniären Hintergrund gegeben.
- **50 Tage LulzSec** ab Mai 2011 in Beispielen: FOX (Fernsehsender), InfraGuard (BotNetz-Überwachung), US-Senat, CIA, Public Broadcasting Service, Sony, The Sun, ...

„Set sail for fail“ → Sony im Visier von Anonymous, LulzSec u.a.

- Ursprünglich unterstützte die **PS3** alternative Betriebssysteme wie z.B. **Linux**, daher gab es **keine „Homebrew“-Szene**, da nicht notwendig
- Ab **Firmware-Version 3.21** ging das nicht mehr, man hatte keine vollständige, „echte“ Kontrolle mehr über das eigene Gerät, „**Other OS functionality**“ wurde **deaktiviert**
- „**Sicherheitsforschung**“ an der PS3 **begann...**

27C3, 29.12.2010 und danach

- „*2010 saw the first hacks for the Playstation 3, soon after Sony removed Other OS functionality. We will detail the operation of current PS3 exploits, show a few new ones and explain where and how Sony went wrong when designing its security system, and show how these holes can be used to gain control over the system and bring Linux back to the PS3.*“
- → **Security Keys / Private Keys** wurden veröffentlicht, damit kann die PS3 geöffnet werden!
- **11.01.2011**
Sony verklagt Georg „geohot“ Hotz, fail0verflow u.a.

The screenshot shows the homepage of the Pwnie Awards 2011 website. At the top, there's a large, stylized title "the PWNIE AWARDS" with a golden gradient. To the right of the title is a cartoon illustration of a blue pony with a white mane and tail, wearing a small crown and a purple vest with patches. Below the title, there's a dark background with some abstract blue and white patterns. At the bottom of the page, there's a navigation bar with links for "News", "About", "Nominations", "Winners", and "Archive". On the far right of the navigation bar is a "Site search" input field with a magnifying glass icon. A blue banner at the bottom right corner says "Deadline for nominations." with a date "Jul 6".

the PWNIE AWARDS

News About Nominations Winners Archive

Site search

Deadline for nominations.

Jul 6

The screenshot shows a specific section of the Pwnie Awards 2011 website. The title of the section is "Pwnie for Most Epic FAIL". Below the title, there's a short explanatory text: "Sometimes giving 110% just makes your FAIL that much more epic. And what use would the Internet be if it wasn't there to document this FAIL for all time?". Then, there's a list of nominees, each preceded by a bullet point and the word "Sony":

- Sony

For each nominee, there's a brief description:

- After FailOverflow and GeoHot published how to jailbreak the PS3, Sony got a bit miffed. Apparently unfamiliar with how the Internet works and how difficult it is to remove the piss from a swimming pool, Sony proceeded to try erase the information from the Internet and sue GeoHot et al. into oblivion. Needless to say, this was about as successful as the MiniDisc.
- Speaking of piss in a swimming pool, that just happened to be how well Sony protected their Sony Online Entertainment (SOE) users' account info and roughly 25 to 77 million account details were stolen by unknown hackers. That metaphor makes just about no sense at all, but you get the point: FAIL.
- Sony is definitely good at one thing: keeping the hits coming and their fans entertained. Oh wait, did we say Sony? We meant LulzSec. I guess that counts as another FAIL for Sony.
- After learning the hard way that their PlayStation Network was about as porous as air, Sony had to shut it down for over two months to rebuild it from scratch. In doing so, they made everyone from your 8-year old cousin to your barber learn about the importance of security. Hooray for us, sorry Sony shareholders.
- Noticing a pattern here? But wait, it gets better. Sony might have been able to better repel the multitude of attacks if they hadn't just recently laid off a significant number of their network security team. Great timing, guys.

Absolute Sownage

attrition.org/security/rant/sony_aka_sownage.html

Incident	Date	Site	Stock	Who (allegedly)	Observation
	2011-04-04	Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit	31.45		The group Anonymous declares Sony an enemy and begins a DDoS attack against PSN over the 'GeoHot' lawsuit filed earlier in the year.
	2011-04-20	Sony PSN Offline	30.14		PSN taken offline by Sony due to hack. Network World has a timeline of events related to PSN .
	2011-04-26	PSN Outage caused by Rebug Firmware	29.79		Sony drops PSN Network due to problems with the 'REBUG' firmware allowing developer access, and rumors of widespread piracy. Initial speculation said the outage was the result of a second DDoS attack by Anonymous. They denied it in a press release saying "for once we didn't do it".
1	2011-04-26	PlayStation Network (PSN) Hacked	29.79	Anonymous (?)	Sony admits attack took place between April 17 and 19, but did not disclose until around the 26th. Anonymous blamed by Sony initially, but denies involvement in hack. Records breached: 77 million names, addresses, email addresses, birthdays, PlayStation Network/Qriocity passwords and logins, handle/PSN online ID, profile data, purchase history and possibly credit cards obtained (DatalossDB Entry)
	2011-04-27	Ars readers report credit card fraud, blame Sony	29.03		
	2011-04-28	Sony PSN hack triggers lawsuit Sony says SOE Customer Data Safe	28.39		
2	2011-05-	Sony Online Entertainment (SOE) hacked	28.80	(unknown)	Sony Press Release. Records breached: 24.6 million customer dates of birth, email addresses and phone numbers, including

Absolute Sownage

attrition.org/security/rant/sony_aka_sownage.html

19	2011-06-08	Spooing lead to fraud via shopping coupons at Sonisutoa / My Sony Club (Google Translation)	25.25	unknown	Through spooing, an attacker used 95 accounts to exchange online shopping coupons worth 278,000 points at Sonisutoa (My Sony Club), defrauding Sony of ~ 280,000 yen (~ US\$3,500). Sony cannot confirm if e-mail addresses or passwords were leaked.
	2011-06-11	Spain Arrests 3 Suspects in Sony Hacking Case			From the article: "According to a police statement , the suspects are part of Anonymous."
20	2011-06-20	SQLI on sonypictures.fr	24.28	Idahc and Authgntiq	SQL injection reveals hashed passwords and e-mail addresses. Idahc announced the day before that the site was vulnerable. Records Breached: 177,172 e-mail addresses (DatalossDB Entry)
	2011-06-23	Class Action Lawsuit Filed Against Sony/SCEA			Suit alleges Sony fired employees in network security weeks before breach
	2011-06-28	Sony CEO asked to step down on heels of hacking fiasco	25.42		".. the CEO sidestepped the request and instead pointed out that Sony is hardly the only company to face this kind of cyber assault."
21	2011-07-06	Hackers posts fake celebrity stories on Sony site	26.93		sonymusic.ie (Ireland) defaced to include the fake stories.
	2011-10-12	Sony Press Release: 93,000 PSN Account Passwords Compromised	20.06		Note: The attack was performed using brute force guessing of accounts. The problem was due to customers using weak passwords. It could be argued that Sony should enforce a stronger password policy.

Note:

- This table does not count any Denial of Service (DoS) attacks against Sony as an incident.
- Several sources including news outlets and blogs consider the first DoS attack by Anonymous against Sony as the first attack.
- Stock has been on a steady decline for a long time before these events.

Der „Cyber“-Terrorist

W Cyber-Terrorismus – Wikipedia Sicherheit.

In anderen Sprachen

- [العربية](#)
- [English](#)
- [Español](#)
- [فارسی](#)
- [Français](#)
- [עברית](#)
- [हिन्दी](#)
- [日本語](#)
- [한국어](#)
- [Bahasa Melayu](#)
- [Polski](#)
- [Português](#)
- [Русский](#)
- [Српски / srpski](#)
- [Türkçe](#)

[Links bearbeiten](#)

Während etwa der deutsche [Verfassungsschutz](#) darauf beharrt, das [Internet](#) sei das zentrale Instrument zur Propagandaverbreitung und Nachwuchsrekrutierung von Terroristen, erklärte Stephen Cummings, Chef der britischen Behörde zum Schutz kritischer [Infrastrukturen](#)^[1], auf einer Cyber-Security-Konferenz in [London](#) Mitte April 2008 schlicht und unumwunden: "Cyberterrorismus ist ein [Mythos](#)."^[2]

Siehe auch [Bearbeiten]

- [CERT](#)
- [Cyber](#)
- [Cyberwar](#)
- [Bundesamt für Sicherheit in der Informationstechnik](#)
- [Nationales Cyber-Abwehrzentrum](#)

SHODAN - Computer Search Sicherheit.

www.shodanhq.com

Shodan Exploits Scanhub Maps Blog Anniversary Promotion Register Login ?

SHODAN Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

[TAKE A TOUR](#) [FREE SIGN UP](#)

Popular Search Queries: Snom VOIP phones with no authentication - A list of Snom phone management interface without authentication

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.

IN THE PRESS

<p>The Register <i>Shodan pinpoints shoddy industrial controls.</i></p>	<p>threatpost <i>It greatly lowers the technical bar needed to canvas the Internet...</i></p>	<p>DEF CON <i>'Shodan for Penetration Testers'</i> <i>presented at DEF CON 18</i></p>	<p>dark READING <i>It's a reminder to many to know what's on your network...</i></p>
<p>ZDNet <i>Shodan is the Google for hackers.</i></p>	<p>heise online <i>Shodan vereinfacht die Suche nach SCADA-Systeme erheblich...</i></p>	<p>CIO <i>Firmen öffnen Stuxnet und Co. selbst die Tür.</i></p>	<p>AARGAUER ZEITUNG <i>Computerangriffe werden einfacher. Zumindest für die Nutzer von Shodan.</i></p>

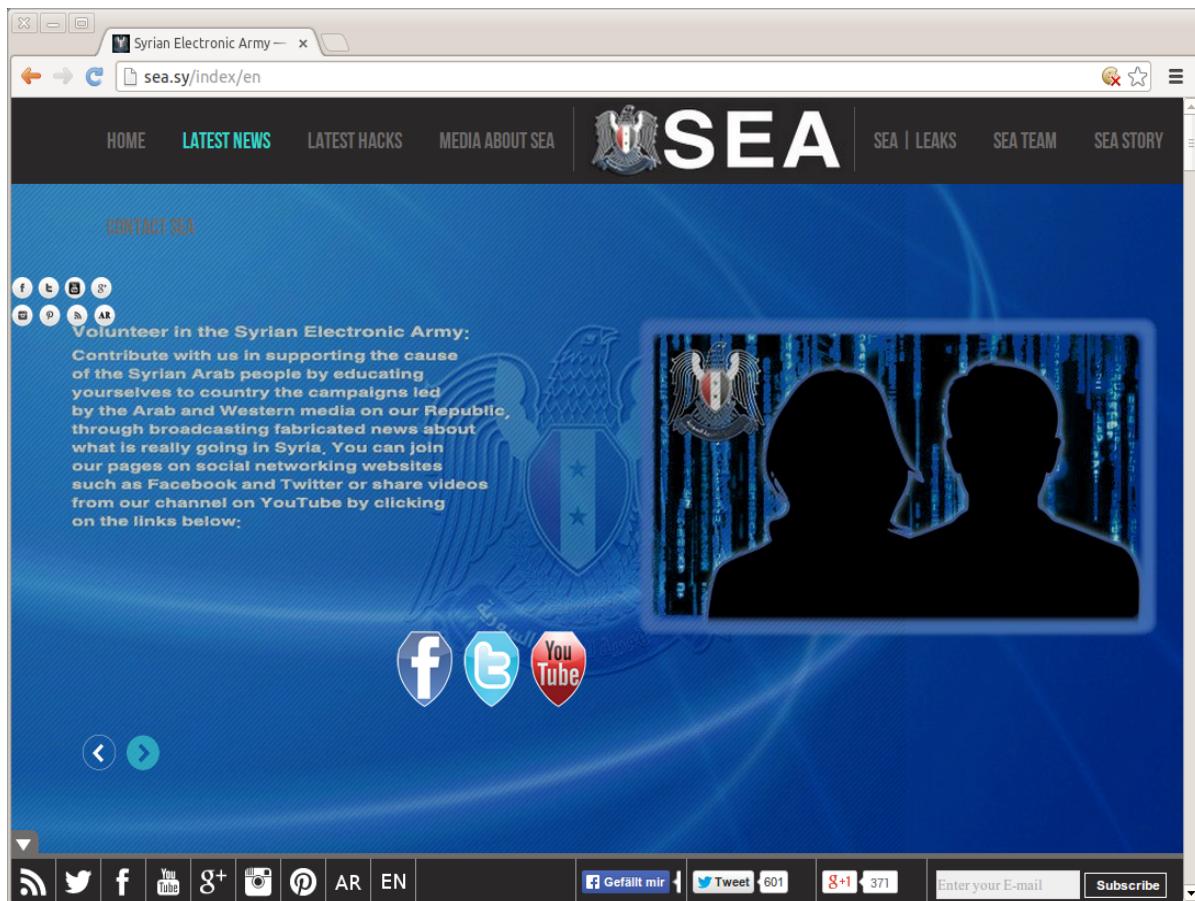
www.shodanhq.com/anniversary

Der „Cyber“-Terrorist

- **Angriffe auf „Kritische Infrastruktur“ wie Versorgungsunternehmen, usw. sind möglich**
- **Skiddie** ist dabei genau so gefährlich wie ein „Elektromudschaheddin“ → Honeypot-Tests
- **Nadelstiche** vs. „Konzertierte Aktion“
- Auch hier: **InfoSec Hausaufgaben machen!**
 - Warum sollten SPSen frei im Internet stehen?

Der „Cyber“-Terrorist

- Echtes Problem: „**Paramilitärische**“ Einheiten
 - **Internetangriffe (DoS)** auf Estlands Infrastruktur ab 27. April 2007 nach Aufruhr russischer Esten
 - **Syrian Electronic Army** greift systematisch Assad-Gegner an: **RSA conference website**, Reuters, Forbes, BBC News, the Associated Press, National Public Radio, Al Jazeera, Financial Times, The Daily Telegraph, The Washington Post, Syrian satellite broadcaster Orient TV, al-Arabia TV, Human Rights Watch, usw.



Der „Cyber“-Kleinkriminelle

- **Ziel:** Erschleichen von **Leistungen oder Geld**
- Konkret: Kreditkarteninformationen, Credentials von PayPal und alternativen Bezahlsystemen, Wallets von Cyber-Währungen wie Bitcoin, Credentials zu Handelsplattformen wie eBay oder Warenhäuser wie amazon, kopierte Geld- oder Kreditkarten, Prepaid Credit von Telefonkarten, Gutscheine, Voucher, MITM beim Online-Banking, Vorschuss-Betrug („Nigeria-Connection“), usw.
- **Meist klassischer Betrug**, wenig echtes „Hacking“

sic[!]sec

Der „Cyber“-Kleinkriminelle

- **Angriff auf Dienstleister** (meist Bezahltdienste)
 - SQL-Injection, Datenbankdump
 - XSS, Session-Diebstahl
 - Implementierung / Geschäftslogik fehlerhaft
 - Klonen von Seiten
- **Angriff auf Endkunde**
 - Technischer Angriff auf den Client (Trojaner, MITM)
 - Social Engineering, „klassische Maschen“
 - Klonen von Seiten / Token

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

33

Wichtige Information zu Ihrem Kundenkonto

Von: newsletter@zigarrenschachtel.de + 22.05.2014 um

Sehr geehrter Kunde,

an 17.5.2014 haben wir bemerkt, daß Betrüger in unserem Namen Zahlungsaufforderungen per Email verschickten. Vielleicht haben Sie auch eine dieser Emails erhalten. Ignorieren Sie bitte diese Email und bezahlen Sie nichts.

Nach aktuellem Erkenntnisstand sind wir Opfer eines Hacker Angriffs geworden. Im Zuge des Angriffs konnten sich die Kriminellen Zugang auf einen Teil der Kundendaten unseres Online Shops verschaffen.

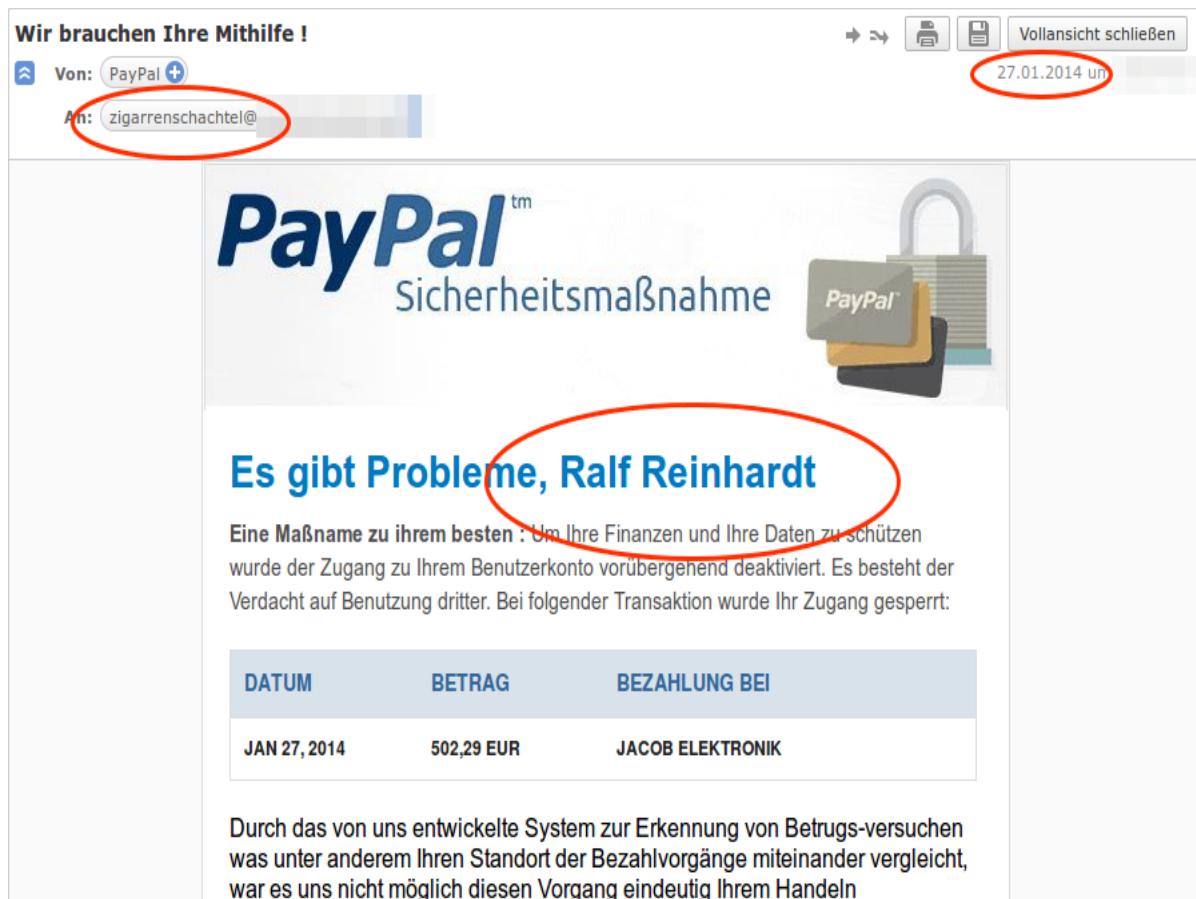
Diese Daten werden nun benutzt, um die dubiosen Zahlungsaufforderungen an Kunden, aber auch andere Empfänger zu versenden. Kreditkartendaten konnten sich die Kriminellen nicht verschaffen, da diese nicht in unserem Online-Shop gespeichert werden.

Wir halten es für sehr unwahrscheinlich, es ist aber nicht auszuschließen, daß neben den Emailadressen auch Adressdaten entwendet wurden. Sollten Sie bei uns schon einmal per Lastschrift bezahlt haben, könnten auch Ihre Bankkontodaten davon betroffen sein.

Wir raten Ihnen daher, E-Mails von unbekannten Absendern - Werbe-E-Mails (Spam) - nicht zu öffnen und auch Ihr Konto auf verdächtige Abbuchungen zu prüfen.

Da Ihr Passwort bei uns verschlüsselt gespeichert wird - selbst wir kennen es nicht - gehen wir davon aus, daß Ihr Konto sicher ist. Dennoch empfehlen wir Ihnen, umgehend Ihr Passwort in unserem Shop zu ändern.

Sie können dies im Login Fenster auf ZigarrenSchachtel.de tun (siehe Bild).



sic[!]sec

Der Innenräuber

- Motivation: **Geld, Rache, Langeweile, Ethik**
- **Weniger hacking, eher Insiderwissen** und mangelnde Klassifizierung und mangelnder Zugriffsschutz „innerhalb der Familie“
- Beispiele: Nutzung von **Ressourcen oder** tatsächlicher **Geldabfluss**, Verkauf von **Firmengeheimnissen**, bewusste **Sabotage** (Verschlüsselung, unbekannte Credentials, logische Bomben, Löschungen, Änderungen), **Aufdeckung** fragwürdiger Machenschaften, usw.

Wie viel verdient ein DB-Admin?



Bild-Quelle: <http://www.wirtschaftsblatt.at>

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe
© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

37





Der Industriespion

>>**Advanced Persistent Threat (APT)** zu deutsch "**fortgeschrittene, andauernde Bedrohung**" ist ein häufig im Bereich der Cyber Bedrohung (Cyber-Attacke) verwendeter Begriff

für einen **komplexen, zielgerichteten und effektiven Angriff auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen** aller Branchen, welche aufgrund ihres

Technologievorsprungs potenzielle Opfer darstellen oder als Sprungbrett auf solche Opfer dienen können.<< [WIKI 2]

Der Industriespion

*>>Im Zuge eines solchen Angriffes gehen die Angreifer **sehr zielgerichtet** vor und nehmen gegebenenfalls ebenso großen **Aufwand** auf sich, um **nach dem ersten Eindringen** in einen Rechner **weiter in die lokale IT-Infrastruktur des Opfers vorzudringen.***

*Das Ziel eines APT ist es, möglichst **lange unentdeckt** zu bleiben, um über einen längeren Zeitraum **sensible Informationen** auszuspähen (Internet Spionage) oder anderweitig Schaden anzurichten.<< [WIKI 2]*

Der Industriespion

APT Phase	Details	Basis process examples
Reconnaissance	Target determination Evaluate and Define Attack Vectors	Configuration Management User Awareness
Spear-Phishing	Send crafted email with malicious content	User Awareness Anti-Malware Management
Establish Presence	Exploitation of vulnerabilities Installation of backdoors Installation of attack tools Obtaining user credentials	Anti-Malware Management Patch Management Change Management Asset Management Identity Management Configuration Management Audit Management
Exploration and Pivoting	Network exploration Process and resource mapping Extension of control to other systems and applications	Configuration Management Patch Management Anti-Malware Management Software Development
Data Extraction	Obtain, compress, encrypt and transfer information out	Access Management Vulnerability Management
Maintaining Persistence	Analysis of attack data Adapt to the specific environment Infection of further systems Hiding traces	All of the above and for sure in each phase Incident and Response Management

Der Industriespion

- Am Ende geht es um (viel) Geld.
- Sinngemäßes Zitat eines CISOs:

„Sie können es vergessen, dass Sie Ihr Netzwerk so abschotten können, dass Angreifer keinen Erfolg haben werden. Die sind schon da oder schaffen es immer wieder. Die Frage ist:

Wie schnell werden sie entdeckt und können unschädlich gemacht werden?“

- Früher war Prävention das Allerwichtigste, heute ist es Detektion und Reaktion.

Organisierte „Cyber“-Gangster: sic[!]sec „Krimineller Flashmop“



„Make Money Fast!“

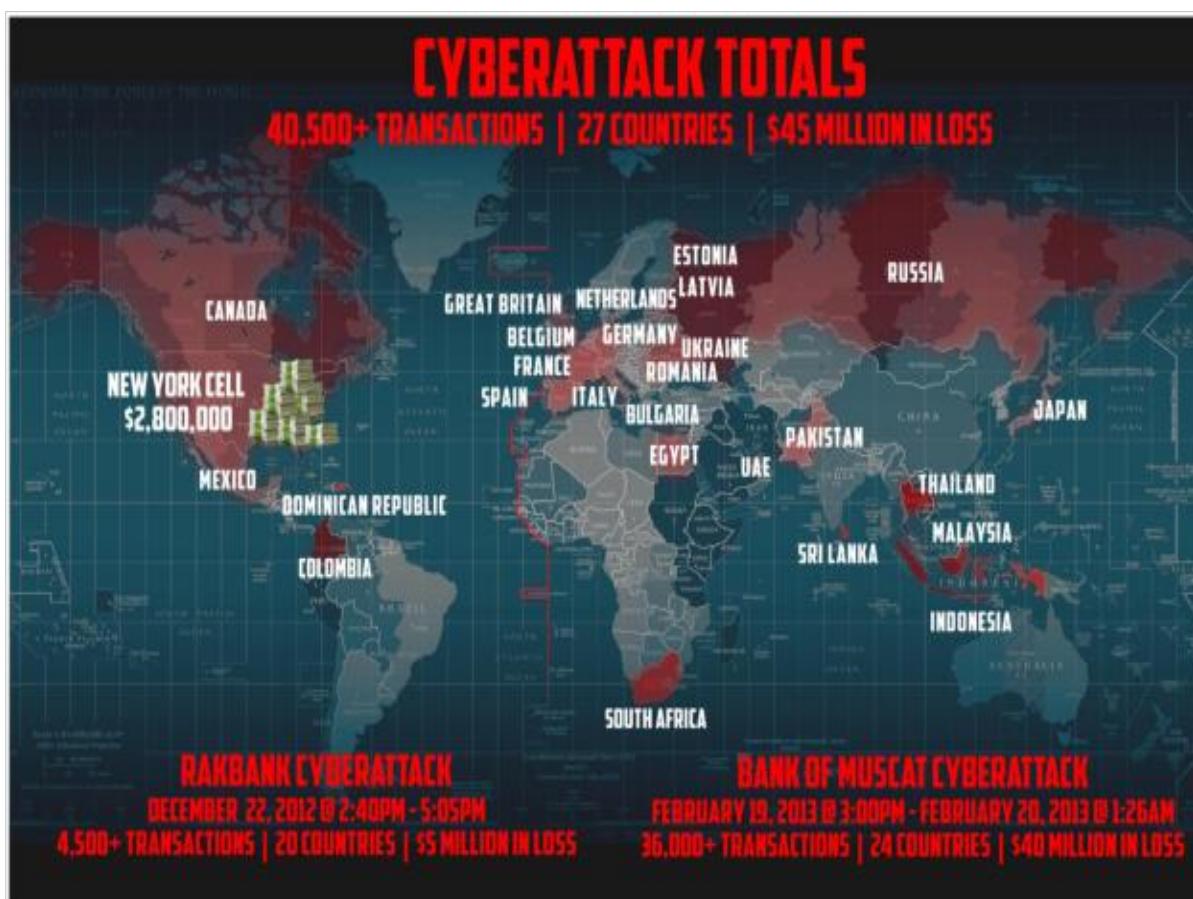
40 Mio. US\$ am 19.02.2013

- „Pilot“ im **Dezember 2012**: 5 Mio. US\$ wurden von der „**Rakbank**“ (VAE) erbeutet
- Im **Februar 2013** wurde dann die „**Bank Muscat**“ (Oman) geplündert, **40 Mio. US\$ Schaden** für die Bank (nicht die Kunden)
- 36.000 Abhebungen innerhalb von 10 Stunden, abgehoben in 24 verschiedenen Ländern
- **Wie geht das?**

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Grobenzell, Germany. - For personal use only. - <http://www.sicsec.de>

45



Bankraub-HowTo im 21. Jahrhundert

- **Kreditkartenprozessor (Dienstleister) hacken** (einen in den USA (unbekannt) für Bank Muscat und einen in Indien (ElectraCard Services) für die Rakbank)
- **Details** zu Mastercard Prepaid Debit Cards (Guthabekarten) und den dazu gehörigen Konten (12 Muskat?, 5 Rakbank?) für die jeweiligen Banken dort **abziehen, bzw. anlegen**, wenn noch nicht ausreichend vorhanden
- **Aufhebung / Manipulation** der relevanten Kartenlimits, speziell **Guthaben / Obergrenzen** (und ggf. Häufigkeits-Zähler)
- Die **Daten** für die Magnetspuren und die jeweilige Pin **an Komplizen schicken**
- Diese Karten der genannten Banken haben keine Sicherheitsmerkmale oder Crypto-Chips, der **Magnetstreifen alleine genügt** völlig
- Beliebige (Blanko-)**Karten** weltweit von den Komplizen **beschreiben lassen**
- **Komplizen zeitgleich losschicken**, um Geld abzuholen, immer und immer wieder
- **Anteil von den Komplizen abkassieren**

Der feindliche Agent

Inhalt

APT1: Years of Espionage	20
APT1: Attack Lifecycle	27
APT1: Infrastructure	39
APT1: Identities	51
Conclusion	59
Appendix A: How Does Mandiant Distinguish Threat Groups?	61
Appendix B: APT and the Attack Lifecycle	63
Appendix C (Digital): The Malware Arsenal	66
Appendix D (Digital): FQDNs	67
Appendix E (Digital): MD5 Hashes	68
Appendix F (Digital): SSL Certificates	69
Appendix G (Digital): IOCs	70
Appendix H (Digital): Video	74

APT1
Exposing One of China's Cyber
Espionage Units

**Egal ob China, Syrien,
Russland, Schurkenstaat XYZ**
→ Methoden sind sehr ähnlich

Der feindliche Agent

Hackerangriff aus China

Washington/Peking – Chinesische Hacker sollen in Computersysteme der US-Regierung eingedrungen sein. Wie die *New York Times* unter Berufung auf Regierungskreise berichtete, hatten sie es auf die Daten Zehntausender Bediensteter abgesehen, die sich um einen Zugang zu hohen Geheimhaltungsstufen beworben hatten. In den Akten werden persönliche Angaben der Antragsteller, darunter auch Fälle von Drogenkonsum gespeichert. Wie weit die Hacker vordringen konnten, sei unklar. Sicherheitsbehörden hätten den Bruch inzwischen entdeckt und den Zugang für Hacker blockiert. DPA

St., 11.07.14

Da es aus Sicht des deutschen Bürgers, Unternehmens oder sonstiger Organisation kaum einen großen Unterschied macht, wird dieser Typus implizit im nächsten Kapitel dargestellt.

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

49

Five Eyes und Edward Snowden

- Was bisher geschah:

<http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html>

- NSA, GHCQ, ASD, CSEC und GCSB kennen weder Freund noch Feind, so wie es aussieht mit freundlicher Unterstützung des BND.

Warum? „Kampf gegen den Terror!“

- Kosten** dafür in den **USA**: **40 Mrd. EUR**
- Schaden** durch Wirtschaftsspionage in **Deutschland**: **50 Mrd. EUR**

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

50

Kennen Sie das kleine, gelbe Land in Zentraleuropa?

sic[!]sec

TOP SECRET//SI//ORCON//NOFORN REVIVED FROM RSAC 53M 8-57, DATED 09 JAN 2007 DECLASSIFY ON 20320708

BOUNDLESSINFORMANT

OVERVIEW (last 30 days)

TOTAL DNI
97,111,188,358

TOTAL DNR
124,808,692,959

SIGADS
504

CASE NOTATIONS
27,798

PROCESSING SYSTEMS
2,431

map by amMap.com

Global

AGGREGATE DNI DNR

Country View

Top 5 Countries (Last 30 Days)

Country	DNI	DNR
Iran, Islamic Republic of	14,101,066,499	1,733,419,401
Pakistan	13,516,527,385	13,759,417,233
Jordan	12,729,653,438	1,644,602,031
Egypt	7,560,103,072	1,504,519,908
India	6,333,878,580	6,283,036,977

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe

© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

51

TOP SECRET//SI//ORCON//NOFORN

Gmail msn Hotmail Google YAHOO! skype paltalk.com YouTube AOL mail

(TS//SI//NF) PRISM Collection Details

SPECIAL SOURCE OPERATIONS

PRISM

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- Special Requests**

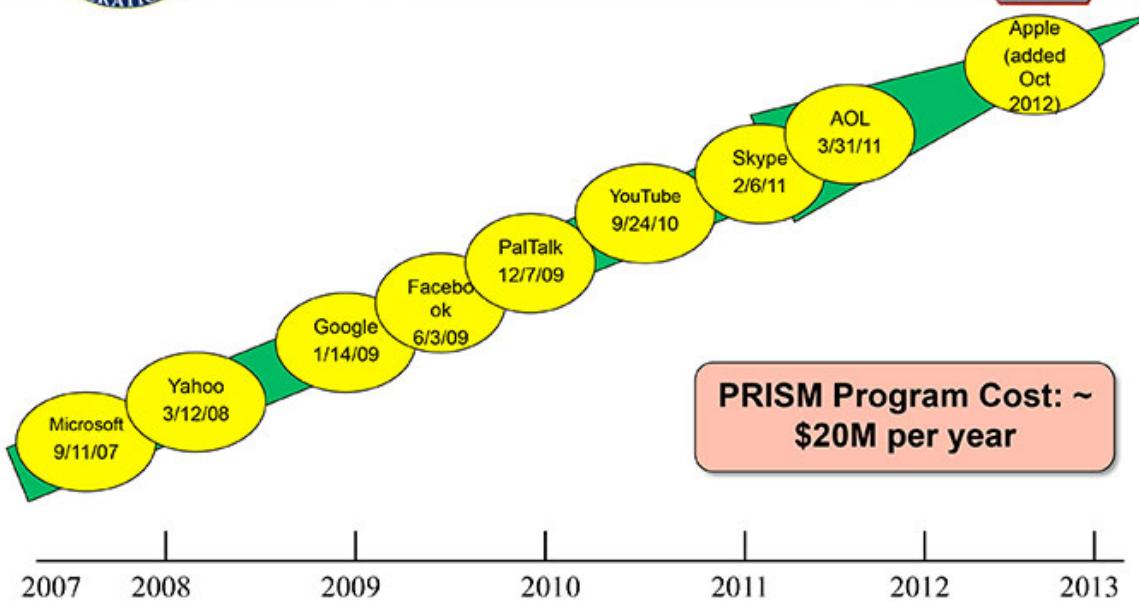
Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF) FAA702 Operations Two Types of Collection



Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.
(FAIRVIEW, ██████████ BLARNEY, ██████████)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

TOP SECRET//SI//ORCON//NOFORN

PRISM ist *nicht* das einzige Programm

[http://en.wikipedia.org/wiki/
Terrorist_Surveillance_Program](http://en.wikipedia.org/wiki/Terrorist_Surveillance_Program)

NSA-Werkzeugkiste:
<file:///home/rr/NSA-Catalogue/>

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Type
© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For perso



National Security Agency surveillance

Programs

[hide]

Pre-2001

ECHELON • Main Core • MINARET •
SHAMROCK • PROMIS

Since 2001

BLARNEY • RAGTIME • Turbulence •
PINWALE • MAINWAY • Upstream

Since 2007

PRISM • Boundless Informant • X-Keyscore
• Dropmire • Fairview •
Surveillance Detection Unit • Bullrun •

MYSTIC

GCHQ collaboration

MUSCULAR • IMP • Tempora
(Mastering the Internet •
Global Telecoms Exploitation)

Discontinued

Trailblazer Project • ThinThread •
President's Surveillance Program
(Terrorist Surveillance Program •
STELLARWIND)

sic[!]sec

Fragen, Anregungen?



ralf.reinhardt@sicsec.de
ralf.reinhardt@owasp.org

sic[!]sec GmbH
Industriestr. 29-31
D-82194 Gröbenzell

Tel.: +49-8142-44250-32
www.sicsec.de

Ralf Reinhardt, sic[!]sec GmbH - Hacker-Typen und Hacker-Angriffe
© 2014 by sic[!]sec GmbH in Groebenzell, Germany. - For personal use only. - <http://www.sicsec.de>

Quellen und weiterführende Infos

- [BSI 1]: BSI, Register aktueller Cyber-Gefährdungen und -Angriffsformen, im Besonderen Anhang A

[https://www.allianz-fuer-cybersicherheit.de/
ACS/DE/_downloads/angriffsmethoden/statistiken/
BSI-CS_026.pdf?__blob=publicationFile](https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/angriffsmethoden/statistiken/BSI-CS_026.pdf?__blob=publicationFile)

- [WIKI 1] - Wikipedia
<http://de.wikipedia.org/wiki/Cyber>
- [TMRC 1] - Tech Model Railroad club
<http://tmrc.mit.edu/hackers-ref.html>

Quellen und weiterführende Infos

- [PHRACK 1] – The Hacker Manifesto
<http://phrack.org/issues/7/3.html>
- [CCC 1]
<http://www.ccc.de/de/hackerethik>
- [ANON 1]: Erste Video-Botschaft von Anonymous
<http://www.youtube.com/watch?v=JCbKv9yiLiQ>
- [WIKI 2]
[http://de.wikipedia.org/wiki/Advanced_Persistent_T
hreat](http://de.wikipedia.org/wiki/Advanced_Persistent_T)