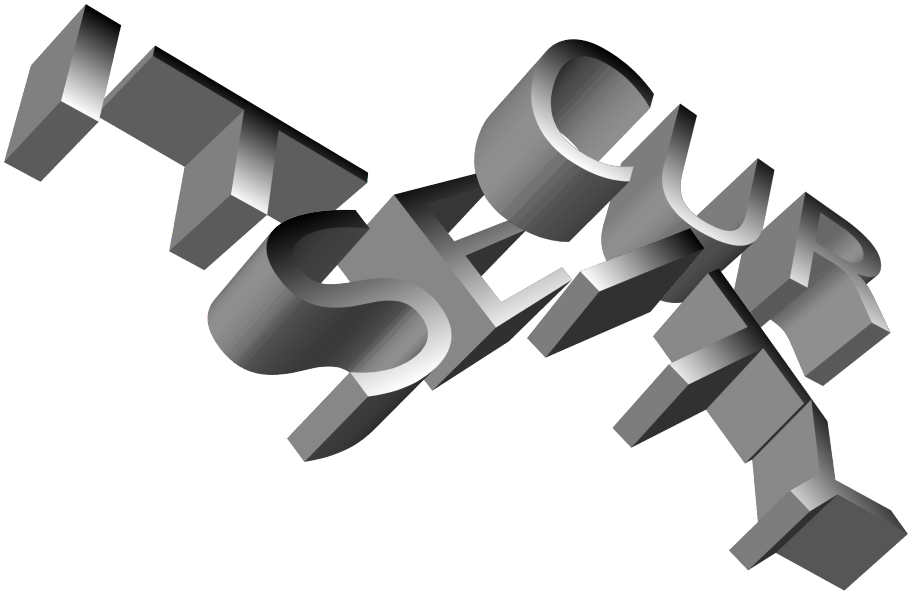
Let's Clear up the Debris



What the Snowden Leaks Mean for Your IT Security Strategies

Sylvia Johnigk and Kai Nothdurft

Who We Are

Sylvia Johnigk Dipl. Inform

- Studied computer science with focus on it-sec and privacy
- 5 years it sec researcher at GMD
- 8 years ISO at big bank institute
- Self employed it-security consultant at secucat Informationssicherheit
- Board member of FIfF

Kai Nothdurft Dipl. Inform,CISSP

- Studied computer science with focus on it-sec and privacy
- 6 years self employed training and consulting privacy and it-sec
- 7 years ISO at Allianz Health insurance (APKV)
- Since 2006 ISO Allianz Deutschland AG
- Board member of FIfF

cyberpeace eine Kampagne des FIfF

Disclaimer and Legal Stuff

- copyright protected logos:

- Copyleft


- Content and opinions are personal views of Sylvia Johnigk and Kai Nothdurft
- Kai Nothdurft is not officially speaking for Allianz.
- Our opinion is public domain - anyone can join and adopt it ;-)
- Rest of the Contents of these slides are published under creative commons


TOP SECRET//COMINT//X1
NSA Strategic Partnerships
Alliances with over 80 Major Global Corporations Supporting both Missions
• Telecommunications & Network Service Providers
• Network Infrastructure
• Hardware Platforms Desktops/Servers
• Operating Systems
• Applications Software
• Security Hardware & Software
• System Integrators
AT&T
Qwest
EDS
H-P
Motorola
CISCO
Qualcomm
Oracle
IBM
Intel
Microsoft
Verizon
TOP SECRET//COMINT//X1

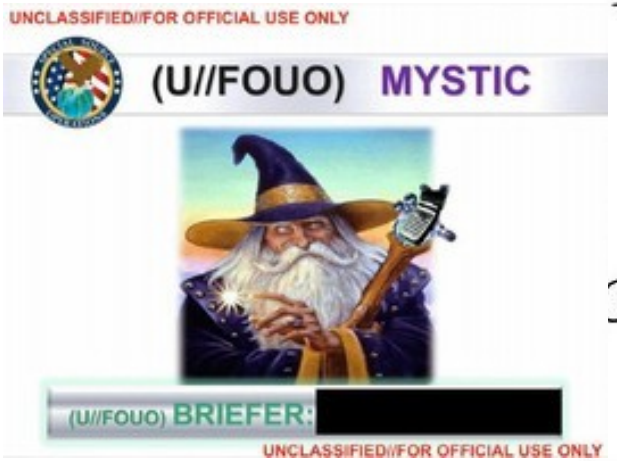
Content

- The Snowden leaks: a brief overview
- Threat analysis and assessment
- Consequences for IT sec strategies
- Q&A - discussion!

Information from the Snowden Documents

- Mass surveillance and spying
- Company as an accessory and sharer, compromise of IT products
- Military use of the Internet
- Objectives, priorities, approach and motivation of the NSA
- Info-warfare, propaganda, disinformation, falsification of Information

Mass Surveillance and Spying



PRISM/US-984XN
Overview

OR

*GAD Used **Most** in NSA Reporting*
Overview

[redacted]

April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901
TOP SECRET//SI//ORCON//NOFORN

- Tempora
- Tracfin
- ...

Mass Surveillance - Dimensions and Numbers

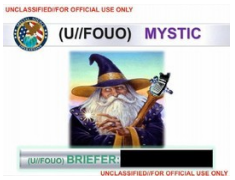
- Tempora: 3 day Internet full take, (metadata 30 days)

  Capacity in 2012 46 lines each with 10GBit/s

  finds the needles in the haystack

- Tracfin: credit card, money transfer- also Swift?
- Dishfire 194 Million SMS / day
- Fascia DB: 5 billion geolocation datasets in a few days
- Mystic retro: 30 day telephony full take amongst others of Iraq and Panama



Companies as Subsidiaries, Suspects, Indirect Perpetrators

- Internet- Cloud service Provider collaboration
  - RSA and Yahoo got paid for their “efforts”
- Subproviders
  - Booz Allen Hamilton, CSC and Stratfor
- Strategic Partners
  - IBM, HP, CISCO, Microsoft, Intel, Oracle, EDS, Qualcom, AT&T, Verizon und Qwest
- Telecos cooperate directly
  - Voluntarily or forced by law(-ful interception)

Telcos Cooperating with the NSA Directly

- Verizon
- AT&T
- QWEST
- British Telecom
- Global Crossing
- Interoute
- Level 3
- Viatel
- Vodafone

SZ 2.8.2013 http://www.webcitation.org/6JFs622aR

Compromised IT Products

unknown vulnerabilities or intentional weaknesses and back doors
➔ plausible deniability

- ANT (Advanced/Access Network Technology)
- manipulate IT Products during shipment (delivery)
- NIST intentionally introduced weak crypto systems
- RSA was paid for an insecure random number generator
- “Bullrun” is the NSAs program dealing with the breaking of encryption. Weak crypto (e.g. RC4 and MD5) do not resist Bullrun crypto analysis attacks.
- US IT products and services?

  Remember the 80+ strategic partners, cooperating with the NSA!

  Historical excursion: Win NT Variable: _NSAKEY

  https://en.wikipedia.org/wiki/NSAKEY

Dropoutjeep

Attribution: Matthew Yohe at en.wikipedia

Compromised IT Products

Horror show from the ANT Catalog (Advanced/Access Network Technology)

- Hardware sniffer in Chassis and covers, WLAN Routers, keyboards, storage devices
- Hard disks: Seagate (Maxtor), Samsung, Western digital
- Network equipment: Cisco, Dell, Hewlett-Packard, Huawei, Juniper Networks

Products of these companies are vulnerable to NSA exploits that are mentioned in the catalog. There is no evidence of active cooperation from these companies with the NSA as far as we know (but from some others as mentioned before).

Military Use of the Internet

- Increasing offensive military activities
  - Quantum Insert 0dayExploits for application are designed or shopped.
  - Fox Acid targeted attacks against individuals
  - Tailored Access Operations (TAO) is dedicated to prepare and conduct attacks
  - 69.000 Bots (compromised systems) back in 2011

Objectives, Priorities, Approach and Motivation of the NSA

- National Intelligence Priority Framework (NIPF), authorized by President Obama
  - 35% of the budget serves the fight against terrorism
  - international financial institutions are identified with the second highest priority intelligence
  - foreign leaders from government, opposition as well as NGOs, international organizations of the UN (WTO, WHO) and the EU are intercepted and their IT systems are compromised to read along encrypted communication
  - *Loveint – the abuse for private purposes*
  - A judge of the FISA court has complained about multiple constitutionally prohibited interception activities against US citizens (illegal activities even according to US law)

Info Warfare, Propaganda, Disinformation, Falsification of Information

- Intelligence's daily business: systematic disinformation and propaganda
  - Information about threats or vulnerabilities influenced by intelligence sources can be biassed colored, falsified or misleading, defined down or exaggerated (a different perspective on Mandiant Report, Symantic Regin Report, ...)
  - Because of their lack of transparency intelligence are difficult to control
  - Democratic control boards are misinformed or lied to
  - NSA has manipulated financial transactions

What Does this Mean for Threatened Companies?

- General threats
- Military usage of the Internet
- Legal aspects
- Can we trust the (German) state
- Lack of transparency, smoke grenades and cover-up

General Problems and Threats

Any company (also yours) can become a target:

- SMEs with innovative products
- Manufacturers of security products and communication technology
- Even supplier or subcontractors of a primary target

Risk: Reputational loss, loss of customer trust, damage claims and the termination of contracts and partnerships, legal fines

General Problems and Threats

- Widespread spying and surveillance makes it easier,
  - to identify people with special knowledge and rights in a targeted company
  - to gain (with tightly focused search) specific useful information about these individuals
  - to perform advanced social-engineering and spearphishing attacks
- Use reputational damage to blackmail individuals or entire organizations into collaboration
  - to handover corporate or government secrets or to force or influence decision-makers to cooperate
  - particularly interesting: hosting provider, cloud service providers, hardware manufacturers, software vendors, admins with privileged access rights

General Problems and Threats

The Challenge:

Each piece of information must be protected

...but there is no secure communication channels left to do so

General Problems and Threats

Each (harmless?) piece of information is screened and analyzed and therefore contains a potential risk and has to be protected

- Internal or confidential business communication is at risk because of economical or military motivated espionage
- Even private content information of employees is indirectly misused for targeted attacks, social engineering, blackmail
- Meta data, connections, geolocation data, PIM data (personal contact and calendars) can reveal interesting informations since they allow conclusions on the intensity and nature of existing business relations e.g. a confidential meeting on the development of business, upcoming merger, ...

General Problems and Threats

There is no secure communication channel left:

- Every (public) channel (fixed-line and mobile phones, satellite, VoIP, SMS, email, chat, social networks, ...) is under observation
- Corporate networks use leased lines for internal data communication (MPLS-connects) from collaborating Telcos
- Compromised end user devices, backdoors and not published weaknesses in operating systems, application software ➞ no trusted platform / base for encryption
- Manipulation of hardware in transit on the delivery route
- Partially compromised encryption techniques or weak crypto systems
- Even Virtual Private Networks have the risk of back doors (most use closed source products)
- Strong encryption is rarely used in just a minimum part of communication
- There are just a few rarely used exceptions like GnuPG, OTR, TOR encrypted communication

The Threat of Military Usage

The military (mis-) use of the Internet, cyber warfare and the botnets of the NSA

- even without tangible acts of cyberwarfare -

pose a serious threat for all IT Security objectives:

confidentiality, integrity, availability and even to non repudiation

Undisclosed Vulnerabilities

- Cyberweappons need undisclosed vulnerabilities in IT products.
- Built-in or undisclosed vulnerabilities in IT Products:
  - Can lead to infrastructure simply being switched off or destroyed
  - can be discovered and exploited by everyone who finds them

    so they also can be exploited by other (non-governmental) criminals
  - Private service providers support the NSA even in sovereign functions
  - Employees in intelligence or private service providers acan be tempted to sell their knowledge of vulnerabilities to organized crime
  - STUXNET worm broke out due to a programming error in the 'wilderness'

Military or intelligence service knowledge does not remain exclusive and limited with government agencies for eternity!

Legal Threats and Issues

- US Companies are under pressure of national law
  - National Court decisions (e.g. Twitter)
  - National Court decisions obligate EU subsidiaries of US companies (e.g. Microsoft Ireland) to handover data
  - Patriot Act / National Security Letter (means issuing a gag order)

Legal Issues

- Privacy contracts under the Safe Harbor agreements are still valid
- Non-Disclosure Agreements (civil contractual confidentiality obligations) with US companies must be doubted and revised in the light of the revelations
- US court claim against Microsoft in April 2014 US companies are even obliged to surrender the data if the data is stored on servers outside the United States, even if a request contradicts local laws

Can We Trust the (German) State?

Help from governmental side will fall short - Companies should not expect too much.

- After 9/11 most governments tended to a restrictive security doctrine / strategy - also Germany
- Priority is on strengthening governmental security authorities (BKA, intelligence services) with expanded legal authorizations towards surveillance while weakening cilvil rights and privacy but also security interests of private economy.
- Governments' security interests are different from security interest of the economy (and both are different from those of private persons e.g. privacy and anonymity aspects)

Can We Trust the (German) State?

Reactions from government on the Snowden Leaks

- No asylum granted for Snowden (cause of higher interest in foreign relations with the US)
- Investigation committee of German parliament was hindered (censored, mostly blackened dossiers) and threatened with consequences based on US law !
- Federal prosecutor did not see probable cause of criminal activities in the leaked material - until Merkel-phone surveillance was published (sec of gov is not sec of economy or citizens)
- No spy agreement approach was the only try from governmental side to react on the Snowden Leaks

State Security versus Business Security

Cooperation between Intelligence Services - BND is part of the problem

- Log term cooperation with the Allys secret services starting after World war II, surveillance and espionage
- SWIFT, passenger record exchange:Access of US intelligence services
- BND cooperates with NSA
  - bi-directional data exchange
  - handover of DE-CIX sniffed data
  - BND-NSA Joint venture surveillance bases e.g in Bad Aibling
  - NSA Dagger Complex at Darmstadt co-financed with German tax money
- BND uses XKeyscore (and Verfassunsgschutz runs a pilot test)
- German government wants to become sixth of the “five eyes“
- Subcontractors and consultants of NSA also used by German Government executives e.g. CSC

State Security versus Business Security

- Malware for lawfull interception of encrypted traffic, aka “Staatstrojaner” (governmental Trojan Horse) illegal and a risk since vulnerabilities have to be disclosed instead of publishing and fixing them
- Cyberweapons for intelligence services (BND, Verfassungsschutz) and German armed forces
- eGovernment, DE-Mail (interceptable) transport layer encryption instead of strong e2e encryption
- Latest example: Resurrection of Cryptowars debate, the demand of installing backdoors in encryption for (so-called) “lawfull” interception aka as governmental key escrow procedures

State Security versus Business Security

BSI (Bundesamt für Sicherheit in der Informationstechnik, German Federal Authority for Information Systems Security) as an advisor? BSI fails to protect economy

- Not independent, conflict of interests as it has to follow orders of Ministry of Interior and acts also for the interests of intelligence services
- Some members from the crypto department are former BND people
- BSI bought vulnerabilities from VUPEN – for what reasons?
- How far can we trust BSI Certifications on Services and product e.g. CAs ?

Smoke Grenades, Disinformation and Propaganda

...are intelligence services' daily business - but what about consultants, vendors and partners?

- Studies and research might be financed or ordered by intelligence services. How independent are research results and studies from security consulting companies?
- Consultants of collaboration companies oder even subsidiaries of the NSA
- NIST standards compromised
- Mandiant Report (template - Howto blame the Chinese)

Threat Summary

Intelligence services in general and particularly the NSA are an extreme IT security threat for companies

- Near zero ethical, political or jurisdictional boundaries / limitations for attacks: no consideration of diplomatic problem with Allys, loss of US companies global reputation interests, customer confidence, violating even US constitution, lying to US Senate, Loveint
- They want it all approach: No secure communication channels, any information is potentially sensitive and has to be protected
- Everyone is a potential target (because he is interesting or can be misused as a nice bot)
- Most existing IT products and technologies are compromised
- Vendors and Service Providers cooperate
- No or low protection and assistance from governmental side
- Consultants, research and studies from companies are an insecure source for defender knowledge
- Consider also the high-hanging fruits. Anything what they can do- they will do if not now maybe in the future Paranoic scenarios have already become reality and there will probably be more upcoming. Theoretical weaknesses, even resource-consuming, obscure and tricky attacks will be developed and used (if there is no easier way to break your security).

Consequences for Companies

- Changing the overall IT security strategy
- Legal consequences
- A national approach?
- Quick wins, short term activities
- Free Software
- Encryption
- Reducing risk and attack vectors
- Advanced paranoia procedures
- Politics

Consequences for the Overall IT Strategy

Isn't it hopeless, do we have to give up the fight?

- Huge Challenge, there is no easy way with a silver bullet solution
- … but we should and need to react according to the risks and legal demands!
- What we need is a mid- / long-term, holistic and big invest approach
- Stop now running on the road to ruin
- Radical reroute of former (and todays?) strategies based on closed source products and a somehow nice and free Internet with cloud services and fancy end user gadgets for i-junkies.
  - Decades of investment in products of collaborative NSA partners have to be written off in value and replaced (as soon as possible and affordable)
  - Vendors and suppliers as well as depending processes have to be changed
  - Some current outsourcing contracts have to be terminated
  - Black box and closed source solutions have to be checked and replaced as well

Legal Consequences

Privacy law §11 BDSG: Mandatory check of reliability of subcontractors processing person related data:

- The reliability of companies that willingly coorperate with the NSA in mass surveillance is similar to the antipode of what privacy law demands.
- Therefore any outsourcing contracts with these companies in which they handle personal data have to be reviewed and probably terminated.
- New contracts are risky as well, since customers or partners might start a lawsuit or inform the data protection authorities (if these do not act on their own account). Bad reputation comes along with non reliable partners.

Legal Consequences

- Privacy law: Safe Harbor is still officially valid but a weak basis for future outsourcing contracts with US companies processing personal data, EU parliament already plans to cancel Safe Harbor, Swift and PFR Treaty, customers' trust is already almost lost
- Microsoft Ireland Datacenter law suite might extend problem to EU-based services of US companies. There is a Dilemma between either the violation of US - or of European law, companies might be forced to end contracts of data processing without consent of each single customer. The legal base according to §11BDSG erodes that formerly allowed it .

Legal Consequences

Liability of choosing a non reliable partner

- Beside privacy issues, just from a strategic perspective, cooperation with non reliable, collaborating NSA partners brings company secrets at risk. This may cause direct strategic weakening of the company, financial losses, liability claims, reputational loss and loss of customer and partner trust.
- Stock corporations might face financial losses due to law suits from shareholders and investors
- Special management liability risks for mistakes and failures in Risk- and Emergency Management (§14 StGB, §91, §93 KontraG) when ignoring risks of economic / industrial espionage and cyberattack caused outages of IT
- Liability for disturbance when operating critical infrastructures

A National Security Strategy?

The political gimmick of a Germany Net / EU network infrastructure faces

- multinational operating companies
- export orientated German SMEs
- international supply chains (where does your hardware come from, somewhere in the neigborhood? Are Huawei Routers better then CISCO Network equipment
- International collaboration between intelligence services (Tempora is operated by GHCQ, a British (EU member state) intelligence service). The BND is cooperating as well.
- needs state regulated (by law enforcement or freely) collaborating Telcos

  ...and therefore is a stupid - not realistic approach to raise your security against attacks of intelligence services!

Quick Wins, Short-Term Activities

- Check and rework your outsourcing guidelines and contracts
- Include no spy / no collaboration clauses in the contracts, demand them as well for their subcontractors
- Purchasing department guidelines: Positive rating for a code of conduct, mentioning denial / self denegation of collaboration with intelligence services for spying or compromise purposes
- Careful choice of security products and services, especially cloud services

  There can be backdoors and hidden collaboration (and if discovered: plausible deniability). Does a US product (IPS, IDS, Malwareprotection, …) fail just in face of a US attack? Who is the vendor, who are the shareholders? A CIA shareholder investment (like in Facebook) should trigger alarms.
- Test the effectiveness of security solutions against sophisticated attacks and vendor-enabled circumvention wherever possible.
- Avoid black box and closed source solutions for future invest decisions.

Quick Wins, Short-Term Activities

- Employees: There is no strict segregation between private and business world anymore (BYOD, one person has only one Facebook Account for both, private and business purposes, PIM data are shared between private and business calenders (if there still are separate ones)
  - Engage your employees by their own personal / private motivation on privacy and security
  - Raise their awareness on the risks of private insecure behavior and devices. Give consultancy and support for these. The personal private data of your employees and (e.g. in BYOD scenarios also there devices) are a risk for the companies due to spearphishing / Fox Acid attacks
  - Teach them to encrypt, organize crypto parties as part of the companies education program

Free Software or at least Open Source Products

- Free in the meaning of “freedom”, not of “free beer” there is no free lunch:
- Support Free Software projects that develop security relevant components especially if you use them e.g. encryption,
  network applications, drivers, LINUX, Apache…

- Finance code audits and quality reviews
- If you developed closed source software that is security critical release it under public licences and fee bugfinders.
- Allow your company developers to publish their implementations under public licences.
- And replace closed source with free or at least open source products wherever possible

The Heartbleed bug is rather a proof, that open source is a risk but shows that open source security works (only) when there are enough resources for code reviews and quality! Googles bugfinders where enabled to discover the weakness in open ssl because it was open source.

Free Software or at least Open Source Products

Free software replacements for closed source products are still a challenge in some cases but there are light spots in the dark

- GNU LINUX as Server OS, Webarchitectures (LAMP) are widely used and in place 
- Desktop
  - Ubuntu derivates
  - Open Office
  - Firefox, Thunderbird + Enigmail
  - Libreboot (coreboot, an open source BIOS) based Notebooks
- Cyanogenmod for Android devices
- Trusted Hardware? Let's take a closer look to USB armory

Encryption as the “Cure All” Strategy?

- Strong crypto still works (Edward Snowden), that's why the NSA runs Bullrun and tries to compromise vendors and products
- Some weak algorithms and products are known to be compromised (RC4, SHA1, SSLv1..)
- So use strong crypto with maximum key length possible and wherever possible in communication and storage even in low risk scenarios
  - All web applications secured with TLS 1.2 and perfect forward secrecy
  - All company email clients with GnuPG and/or S/mime enabled, encryption and signature activated per default
  - Encrypt all hard drives - on notebooks with 2 factor preboot authentication
  - Have data in rest encryption solutions e.g. Truecrypt, GnuPG supported and installed on all company workstations and notebooks
  - Offer and demand encrypted communication to all partners and customers
- All this makes the “I want it all” approach of the NSA harder to become reality.

  But are the de- and encrypting devices secure?

How Secure are Encryption-Processing Devices?

- Microsoft windows?
- Mobile phones? IOS and Android are compromised, Blackberry without enterprise Server was compromised – they succeeded even with Enterprise Server in one case.
- Servers?
- Closed source Hardware Devices? HSM modules for certification storage? Smartcards?

  More questions than answers in the moment, work to be done!
- Suggestion: Use good crpyto as often as possible but have in mind that they still might decrypt it just with bigger effort than cleartext! There are too many ways (side channel attacks) to circumvent the protection good crypto still offers.

Reducing Risks and Attack Vectors

Segregation and decentralization, redundancies

- Network and system segregation help to control and monitor company internal network traffic
- Compromise of segregated network segments must not include the p0wning of the whole company
- Decentralization and redundancies bring more robustness against DoS Attacks performed by military cyberwar units
- Isolation of critical systems or highly sensitive information processing

Advanced Paranoia Procedures

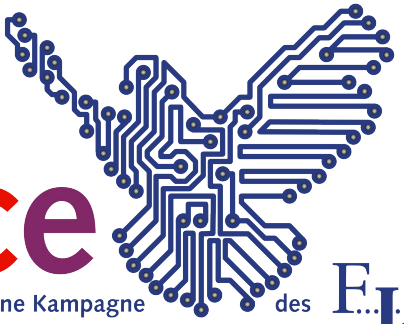
For companies which are high priority targets or for protection of strictly confidential information

- Expect also unexpected, really advanced APTs
- Mask delivery and shipping of hardware by engaging indirect lines over trusted (?) third parties for preventing compromise in transport, avoid payment in advance with e payment, credit card-guarantied orders they can identify with Tracfin
- Conspiratorial business meetings e.g. preparing mergers and acquisitions: Again avoid direct payment in advance e payment and booking and reservation of flights, car rentals, rail, hotels from your business accounts and systems. Use camouflage naming in calenders, hide those business travels behind private aspects e.g. holiday trips. Manage invitations and other organizational aspects with participants from outside your company only via encrypted channel and over TOR (to avoid metadata tracks).

Priorities and Long-Term Approach

- Perform the quick wins, start now to change your IT security strategy..

  ..towards free and open source software only
- Crowd and company sponsored development of secure and trusted systems and platforms
- Apply pressure to politics, ally with associations and the civil society against mass surveillance and cyberwar by intelligence services



cyberpeace

eine Kampagne des FIfF

Those who fight can loose

- those who do not fight have already lost

Thank you for your attention

Q&A, discussion

Sources

- ..
- http://en.wikipedia.org/wiki/Key_escrow
- http://www.zeit.de/digital/datenschutz/2014-06/nsa-bnd-zusammenarbeit-ueberwachung
- Ermittungen durch Bundesstaatsanwalt Range: http://www.tagesschau.de/inland/generalbundesanwalt-nsa100.html
- Foschepoth: „Überwachtes Deutschland“
- http://www.spiegel.de/politik/deutschland/bnd-will-informationen-ueber-software-sicherheitsluecken-einkaufen-a-1001844.html
- EU Parliament votes for cancelation of Swift and Safe habour agreement
  http://www.zeit.de/digital/datenschutz/2014-03/usa-eu-datenschutz-datenaustausch-swift-safe-harbour
- Free Software Foundation https://www.fsf.org/
- http://www.gnu.org/home.en.html
- Open Source coreboot based BIOS and supported Hardware http://libreboot.org/docs/index.html
- Krypto für die Zukunft -Verteidigung gegen die dunklen Künste, Rüdiger Weiß on 31C3

  http://media.ccc.de/browse/congress/2014/31c3_-_6295_-_de_-_saal_2_-_201412281645_-_krypto_fur_die_zukunft_-_ruedi.html#video
- Opensource hardware http://inversepath.com/usbarmory
- Cyberpeace Kampagne des FIfF: cyberpeace.fiff.de
- ..