PRISM und TEMPORA

- was wissen wir bisher?

Mark Neis

07. 09. 2013

Vorstellung

Mark Neis

- Mail: neismark@gmx.de
- Key-ID: 0xE68C47B7

- Beruf: Systemadministrator
- Chaos Computer Club seit über zehn Jahren
- Pirat seit 2009

1984 – Der große Bruder

Krieg ist Frieden

Freiheit ist Sklaverei

Unwissenheit ist Stärke

Überwachung ist Sicherheit

Agenda

1. Eine Chronologie
2. Wie läuft das alles?
3. Die deutsche Sicht
4. Die Auswirkungen

PRISM: Chronologie

6. Juni: The Guardian (UK)

Verizon liefert Telefon-Verbindungsdaten an die NSA

Das Weiße Haus verteidigt das Vorgehen als „entscheidendes Instrument“ gegen Terrorismus

Quellen:
http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

PRISM: Chronologie

6./7. Juni: The Guardian, Washington Post

NSA hat Zugriff auf die Daten von 9 Internet-Firmen:

- **Microsoft (2007)**
- **Yahoo (2008)**
- **Google, Facebook, PalTalk (2009)**
- **YouTube (2010)**
- **Skype, AOL (2011)**
- **Apple (2012)**

Quellen: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

PRISM: Chronologie

9. Juni, The Guardian (UK)

Snowden enttarnt sich in einem Interview selbst.

Zuvor war er nach Honkong geflohen.

„Ich bin bereit, alles zu opfern, weil ich nicht guten Gewissens der US-Regierung erlauben kann, die Privatsphäre, die Freiheit des Internets und die Grundrechte von Menschen rund um die Welt einer umfassenden Überwachungsmaschinerie zu opfern, die sie im Geheimen bauen“

Quellen:
http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video
http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

PRISM: Chronologie

11. Juni, Tagesschau

Die deutsche Regierung und die Geheimdienste haben angeblich nichts von PRISM gewusst.

IM Friedrich: *US-Geheimdienste gaben Hinweise zur Verhinderung von Terroranschlägen in Deutschland*

Kanada hört ebenfalls Internet- und Telefonverkehr im Ausland ab

Quelle:http://www.tagesschau.de/ausland/prism-nsa108.html

PRISM: Chronologie

16. Juni, The Guardian (UK)

Der britische Geheimdienst GCHQ hat internationale Treffen in Großbritannien ausspioniert

Z. B. das G20-Treffen im Jahr 2009

Quelle: http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

PRISM: Chronologie

21. Juni, The Guardian

Bericht über massive Internetüberwachung durch den britischen Geheimdienst GCHQ: Tempora

Mehr als 200 Glasfaserverbindungen würden überwacht

Volker Kauder (CDU):
Wenn das zuträfe, wäre das „*nicht akzeptabel*“

Quelle: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

PRISM: Chronologie

29. Juni, Der Spiegel

Die NSA habe die EU-Vertretungen in Washington und bei den Vereinten Nationen verwanzt

Quelle: http://www.spiegel.de/netzwelt/netzpolitik/nsa-hat-wanzen-in-eu-gebaeuden-installiert-a-908515.html

„EU-Politiker äußern sich empört“

PRISM: Chronologie

30. Juni, Der Spiegel

Die NSA erhebt in Deutschland wesentlich mehr Daten als in jedem anderen Land:

<u>500 Millionen</u> Kommunikationsdaten pro Monat

Die US-Geheimdienste forschen gezielt die Bundesregierung aus bis hinauf zur Kanzlerin

Die Bundesregierung: Das sei „*inakzeptabel*“

Quellen:
http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html
http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining#

PRISM: Chronologie

01. Juli, The Guardian

Die NSA habe Dutzende Botschaften in Washington verwanzt

Regierungssprecher Seibert: Das sei „*inakzeptabel*“

Quelle: http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies

PRISM: Chronologie

02. Juli, Wien / Berlin

Notlandung des bolivianischen Präsident Evo Morales in Wien, nachdem mehrere europäische Länder den Überflug verweigern.

Vermutung: Snowden sei an Bord.

Snowden beantragt in 21 Ländern Asyl

Deutschland lehnt den Antrag noch am gleichen Tag ab

Quelle:
http://www.spiegel.de/politik/ausland/snowden-geruechte-boliviens-praesidentenmaschine-muss-in-wien-landen-a-909108.html

PRISM: Chronologie

03. Juli, Berlin

Die deutschen Sicherheitsbehörden und die Bundesregierung:

„*Keine Kenntnis*“ über die Überwachung des deutschen Internetverkehrs durch US-Geheimdienste.

PRISM: Chronologie

04. Juli, Le Monde

Der französische Geheimdienst DGSE sammelt systematisch Metadaten von Telefonaten, E-Mails und sozialen Netzwerken.

Quelle:
http://www.lemonde.fr/societe/infographie/2013/07/04/comment-la-dgse-collecte-et-stocke-l-ensemble-des-communications-electromagne

PRISM: Chronologie

05. Juli

Asylangebote mehrerer lateinamerikanischer Länder an Snowden

NZZ: http://www.nzz.ch/aktuell/startseite/asylangebote-aus-lateinamerika-1.18112647

PRISM: Chronologie

12. Juli, Moskau

Snowden nimmt das Asylangebot Russlands an

Quelle: http://www.dw.de/snowden-nimmt-asylangebot-russlands-an/a-16948687

The Guardian

Microsoft habe mit der NSA und dem FBI zusammengearbeitet, um Verschlüsselungen offenzulegen

Quelle: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

PRISM: Chronologie

16. Juli, USA

Yahoo: Freigabe von Dokumenten

Belege der Abwehrversuche des Unternehmens gegen die NSA

Quelle: http://www.nbcnews.com/technology/court-sides-yahoo-nsa-prism-data-collection-case-6C10651458

PRISM: Chronologie

17. Juli, Berlin

Bundesregierung dementiert, dass die Bundeswehr in Afghanistan auf die Daten von PRISM zugreifen könne.

Das sei ein völlig anderes Programm, das zufällig gleich heiße.

Quelle: http://www.n24.de/n24/Nachrichten/Politik/d/3203654/ploetzlich-gibt-es-zwei-prism-programme.html

PRISM: Chronologie

20. Juli, Berlin

Deutsche Geheimdienste verwenden die NSA-Software XKeyscore

BND und Verfassungsschutz:

„Wir testen das nur“

Quellen:
http://www.heise.de/tp/artikel/39/39555/1.html
http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
http://www.welt.de/politik/deutschland/article118593621/So-funktioniert-das-XKeyscore-Programm-der-NSA.html

PRISM: Chronologie

24. Juli, USA

US-Behörden verlangen von Unternehmen die Herausgabe von SSL-Keys

Quelle: http://news.cnet.com/8301-13578_3-57595202-38/feds-put-heat-on-web-firms-for-master-encryption-keys/

PRISM: Chronologie

25. Juli, Tagesschau

NSA war auch an "Euro Hawk" beteiligt:

„Beim Start, Streckenflug und bei der Landung werden Kryptoschlüssel benötigt, die vom Operator gesendet und von der Drohne bestätigt werden müssen. Die Generierung dieser Schlüssel liegt bei der NSA.“

(Quelle: http://www.heise.de/newsticker/meldung/Euro-Hawk-und-NSA-Eine-verwirrende-Geschichte-1924145.html)

Quelle:http://www.tagesschau.de/inland/nsa166.html

PRISM: Chronologie

18. August, The Guardian

David Miranda, der Partner von Glenn Greenwald, wird 9 Stunden am Flughafen festgehalten und verhört

Notebook beschlagnahmt

Herausgabe von Passwörtern unter Haftandrohung

Quellen:

http://www.theguardian.com/world/2013/aug/18/glenn-greenwald-guardian-partner-detained-heathrow

http://www.bbc.co.uk/news/uk-23776243

PRISM: Chronologie

19. August, The Guardian

Britische Geheimdienstler zwingen Guardian, Festplatten mit Daten zu vernichten

Wie sich herausstellt, geht das von Premier Cameron aus

(Quellen:

http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters

http://www.belfasttelegraph.co.uk/news/local-national/uk/snowden-affair-pm-david-cameron-told-heywood-to-warn-guardian-of

PRISM: Chronologie

25. August, Der Spiegel

Die NSA hört die UN-Zentrale ab

- Eindringen in die interne Videokonferenz-Anlage

(Quelle: http://ml.spiegel.de/article.do?id=918421)

PRISM: Chronologie

29. August, The Age

Australien zapft ebenfalls Unterseekabel an

- Australien Signals Diretorate

- In Partnerschaft mit Briten, Amis und Singapur

(Quelle: http://www.theage.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58)

Agenda

1. Eine Chronologie
2. Wie läuft das alles?
3. Die deutsche Sicht
4. Die Auswirkungen

Früher: Echelon

Ein weltweites Abhörnetzwerk seit den 70er Jahren

Quelle: http://cryptome.org/echelon-ep.htm

PRISM: Wie?

- Erste Erwähnung: 2005 („Sunchart“)
- Ab 2007 massiver Ausbau

„STELLARWIND“:

- MAINWAY: Speicherung von Telefon-Metadaten
- MARINA: Speicherung von Internet-Metadaten
- NUCLEON: Speicherung von Gesprächsinhalten
- PRISM: Kommunikationsinhalte von den großen Internet-Firmen

PRISM: Wie?

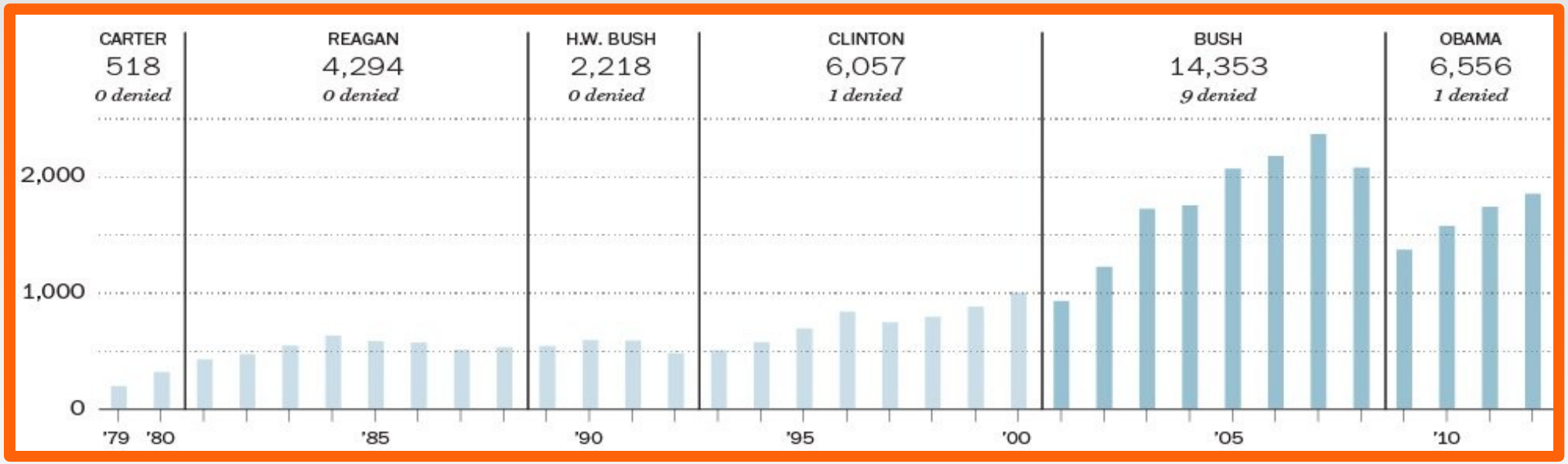
Rechtsgrundlage:

- ***Foreign Intelligence Surveillance Act*** **(FISA)**
- ***Protect America Act (2007)***

- **Weit reichende „Warrants“ werden ausgestell durch den *Foreign Intelligence Surveillance Court* (FISC)**
- **Das FISC tagt nur im Geheimen**
- **Warrants werden für ein Jahr ausgestellt**
- **Seit 2001: 10 von 20. 000 Anfragen abgelehnt**

PRISM: Wie?

Übersicht über die Anfragen an das FISC:



Quelle:
http://www.washingtonpost.com/politics/the-foreign-intelligence-surveillance-court/2013/06/07/4700b382-cfec-11e2-8845-d970ccb04497_graph

PRISM: Wie?

Kritik im Kongress „verhindert“

- 2012: Versuch einiger Abgeordneter, FISA zu ändern

- Abgeordnete mit Kenntnis von PRISM dürfen nicht offen sprechen (Geheimhaltung)

PRISM: Wie?

Sen. Ron Wyden:

Wie viele amerikanische Bürger sind von der Überwachung betroffen?

NSA (Inspector General McCullough III):

Können wir nicht sagen. Wenn wir versuchen, das rauszukriegen, verletzen wir deren Privatsphäre

PRISM: Wie?

Vorgehensweise:

- NSA-Analyst tippt Suchbegriffe ein („Selektoren“)
- NSA-Analyst füllt Formular mit Begründung aus

- FBI: Direkter Zugang zu Systemen der großen Firmen
- Übermittlung der Suchanfragen („tasking“)

Quelle: http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/

PRISM: Wie?

Vorgehensweise:

- **Daten fließen zurück: Audio- und Video-Chats, Bilder, E-Mails, Dokumente, Logs von Verbindungen, Adressbuchinhalte, Kalender, Files aus der Cloud, …**

- **98% der Inhalte von Yahoo, Google und Microsoft**

Quelle: http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/

PRISM: Wie?

Vorgehensweise:

Daten landen in PRINTAURA (ein Sortiersystem), werden weiter verarbeitet.

Hinzu kommen Metadaten aus anderen Quellen

Innerhalb von Minuten bis wenige Stunden hat der Analyst die Daten

Quelle: http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/

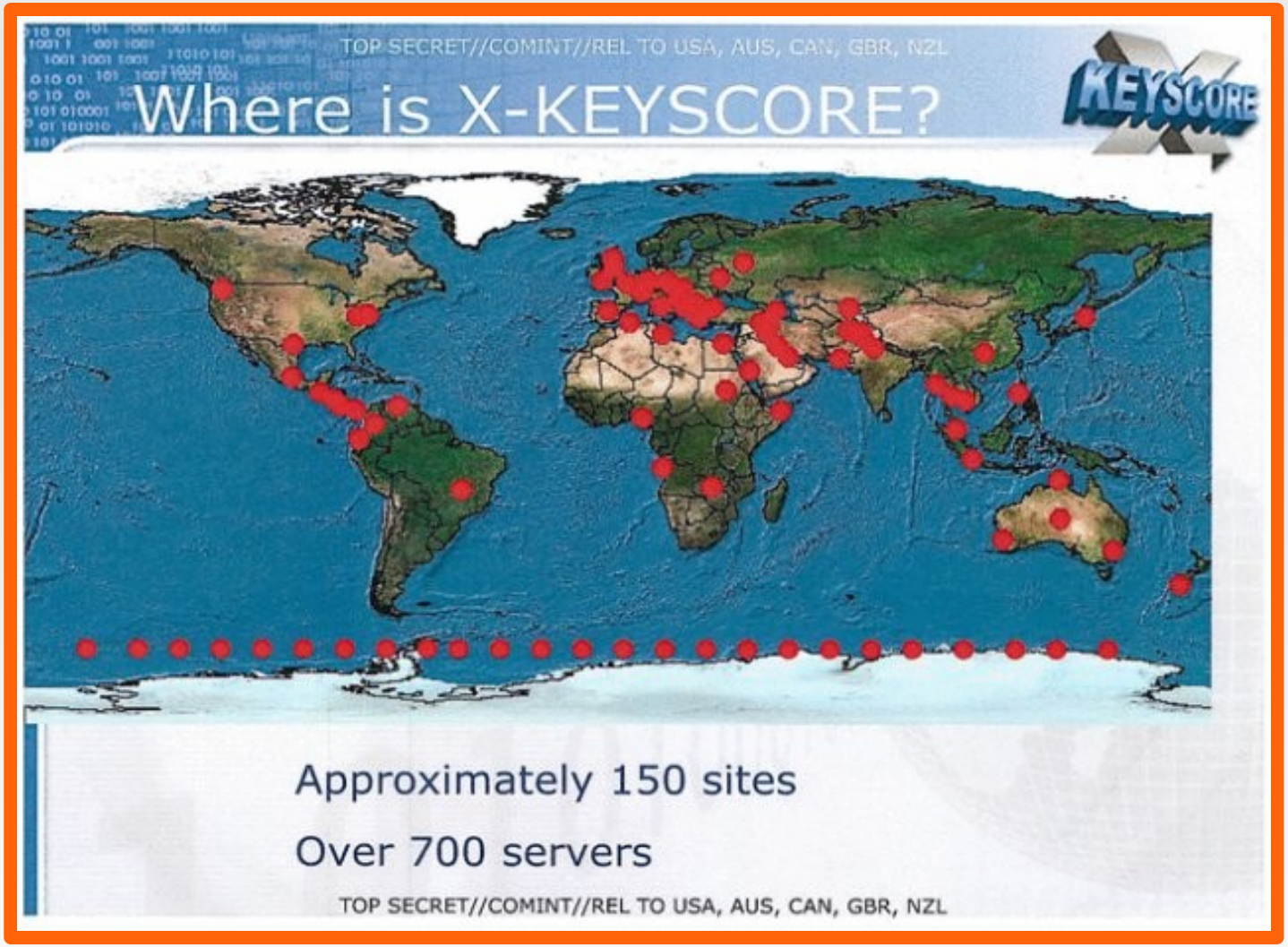
XKeyscore

XKeyscore

- Digital Network Intelligence / Analytic Framework
- 3 Tage Vorhaltezeit für alle Daten
- Cluster von 500 Linux-Servern weltweit verteilt
- XKS kann auf sehr großen Datenmengen suchen
- XKS braucht dabei keine einschränkenden Kriterien
- Integration mit MARINA (Internet-Metadaten)

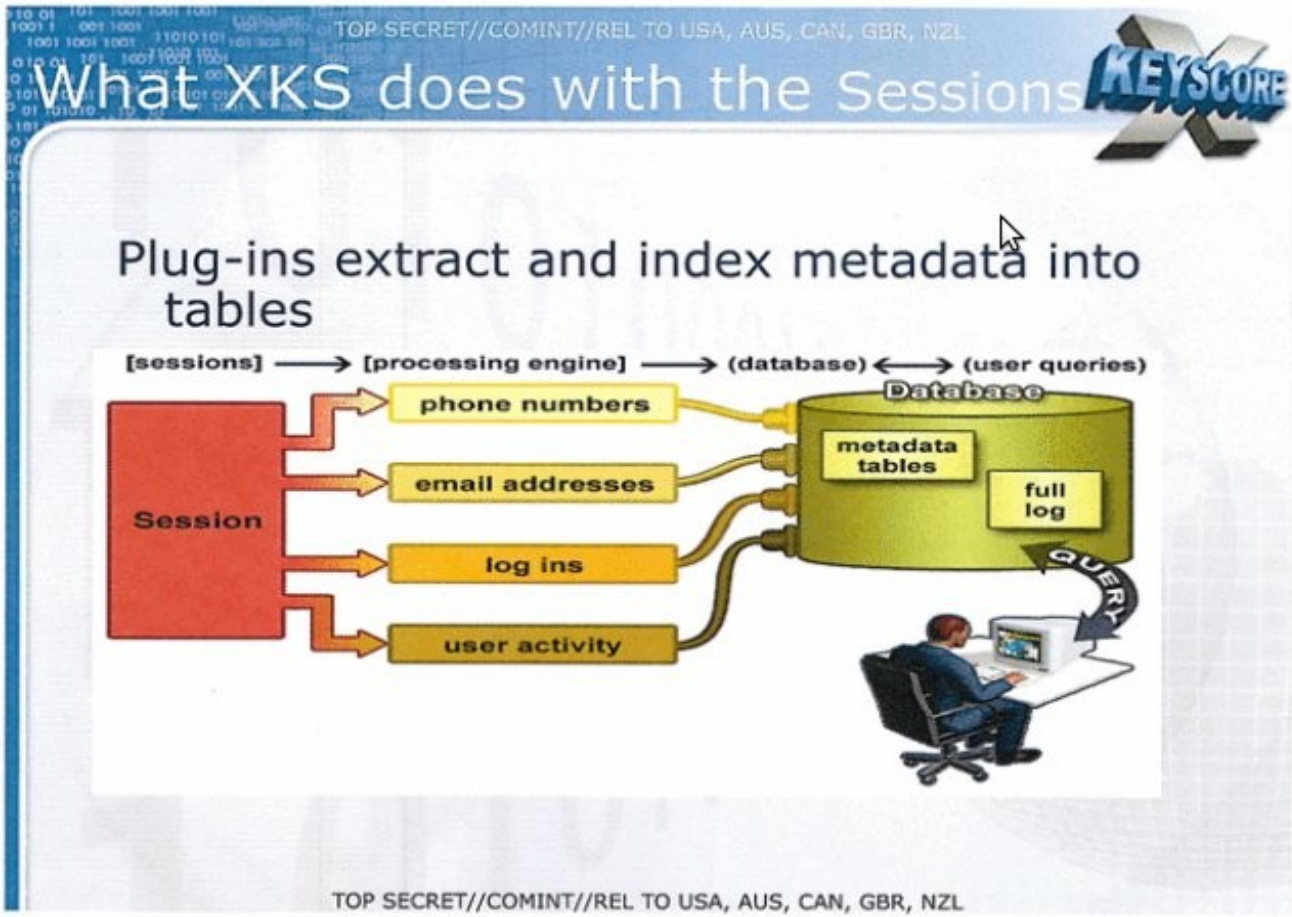
Quelle:http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

XKeyscore



Quelle:http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

XKeyscore



Quelle:http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

XKeyscore

Nach was kann gesucht werden

- E-Mail (Metadaten UND Inhalte)
- Facebook-Chats, Twitter-Nachrichten
- Browsen im Netz
- Websuchen
- IP-Adressen der Besucher einer Webseite
- Telefonate (Metadaten UND z. T. Inhalte)

Quelle:http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

XKeyscore

Nutzungsbeispiele:

- **Sprache passt nicht zur Umgebung**
- **Nutzung von Verschlüsselung**
- **'verdächtige' Suchen im Netz**
- **„*Show me all PGP usage in Iran*“**
- **„*My target speaks German but is in Pakistan – how to find him?*“**
- **„*Show me all Excel sheets containing MAC addresses from Iraq*“**

Quelle:http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

Tempora: Wie?

Ein Abhörprogramm des GCHQ

In Betrieb seit 2009 / 2011

Zwei Komponenten:

- **„*Mastering the Internet*“**
- **„*Global Telecoms Exploitations*“**

Tempora: Wie?

Anzapfen von 200 Glasfaserkabeln

Unternehmen müssen kooperieren

Daten werden kopiert, Speicherung für 30 Tage

Datenmenge in den Kabeln: 21 Petabytes pro Tag

21 000 000 000 000 000 Zeichen.

(fast 200 Mal der komplette Inhalt der British Library)

Agenda

1. Eine Chronologie
2. Wie läuft das alles?
3. Die deutsche Sicht
4. Die Auswirkungen

Deutschland

Die Regierung weiß offiziell von nichts

„inakzeptabel“

Die Dienste bestreiten zunächst ebenfalls jedes Wissen

BND:

Entweder sie lügen, oder sie haben ihren Job nicht gemacht

Deutschland

Situation des BND

Es stellt sich heraus, dass

- BND und Verfassungsschutz XKeyscore nutzen

- BND nutzte seit 1999 „Thin Thread“

- BND Daten an die NSA weitergibt

Sie haben also gelogen.

Deutschland

DE-CIX

Level 3 soll die Daten des DE-CIX an die NSA weitergegeben haben

Agenda

1. Eine Chronologie
2. Wie läuft das alles?
3. Die deutsche Sicht
4. Die Auswirkungen

Auswirkungen

Abschaffung der Unschuldsvermutung

Jeder ist verdächtig. Immer.

Oder weshalb sollte man sonst seine Daten speichern?

Auswirkungen

Software bestimmt zunehmend unser Leben

- **(Such)-Algorithmen beruhen auf Annahmen**
- **Daten können falsch/unvollständig sein**
- **Entscheidungen aufgrund von statistischen Auswertungen**

Auswirkungen

Etablierung einer neuen Sicht- und Denkweise

- **Menschen als Sammlung klassifizierbarer Einzelaspekte**
- **Einordnung in Schubladen, z. B.:**
  - **Über drei Ecken bekannt mit einem Verdächtigen?**
  - **„Gefährder“?**

➔ **Was ist unser Gefahrenpotential?**

Auswirkungen

Mainstreaming

„Du sollst nicht rauchen. Du sollst keine Geheimnisse haben. Du sollst tun, was alle tun. Und denk daran: Du wirst beobachtet!“

(Quelle: Harald Martenstein: http://www.zeit.de/2012/24/DOS-Tugend/komplettansicht)

Sein und Schein sollen sich nicht mehr unterscheiden.

Alle sollen einer angenommenen „Norm“ entsprechen.

Auswirkungen

Automatisierung sozialer Kontrolle

- **Kameras in Mailand**
  (http://www.heise.de/tp/artikel/32/32673/1.html)
- **Project INDECT**
  (http://www.heise.de/tp/artikel/36/36821/1.html)
- **MUNI in San Francisco: Pendler**
  (http://www.fastcompany.com/1839052/big-brother-is-coding-you)
- **ADIS**
  (Fraunhofer: Videoanalyse-Tool erkennt Gefahrensituationen)

Auswirkungen

Geheimdienste sitzen am Hebel

Sammlung von Kompromat?

Beeinflussung von Entscheidungen?

Auswirkungen: Konkret

Beispiel 1: Leigh van Bryan

- „@MellissaxWalton free this week for a quick gossip/prep before I go and **destroy America**?"
- „3 weeks today, we're totally in LA pissing people off on Hollywood Blvd and **digging Marily Monroe up**“

Auswirkungen: Konkret

Beispiel 2: Justin Carter

- **„You're fucked up in the head“**
- **„Oh yeah, I'm real fucked up in the head. I'm going to shoot up a school full of kids and eat their still beating hearts. LOL. JK.“**

Auswirkungen: Konkret

Beispiel 3: Andrej Holm

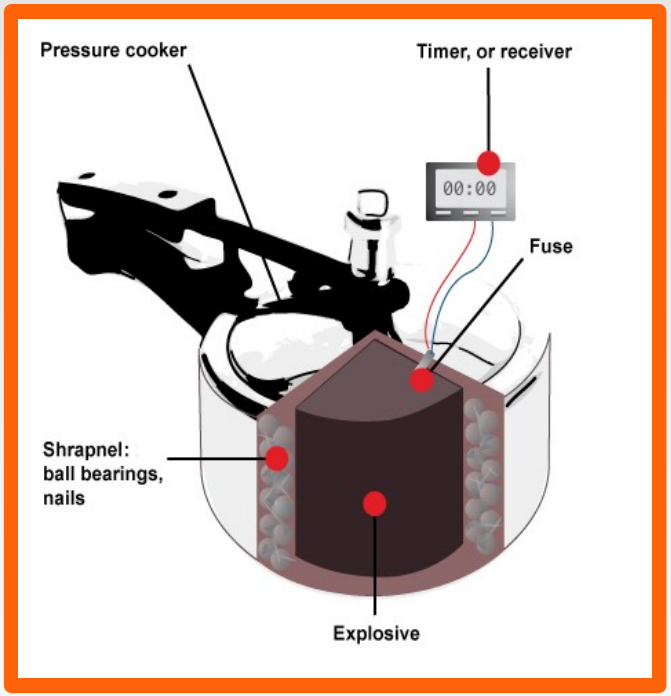
- **Gentrification**
  beschreibt spezifische sozioökonomische Umstrukturierungsprozesse in städtischen Wohngebieten als ein Phänomen der sozialen Ungleichheit.
- **Prekarisierung**
  bezeichnet die Zunahme von Arbeitsplätzen mit geringer Arbeitsplatzsicherheit, niedrigem Lohn, Teilzeitbeschäftigung, befristeten Verträgen...

Auswirkungen: Konkret

Beispiel 4: Die Schnellkochtopfbombe

Amerikaner sucht nach

- ***pressure cooker bombs***
- ***backpacks***



Auswirkungen: Konkret

Beispiel 4: Die Schnellkochtopfbombe

- 6-köpfige Anti-Terror-Einheit verhört ihn
- hunderte Fälle jede Woche laut Polizei

Sidenote: Schnellkochtöpfe

Beispiel 4a: Die Schnellkochtopfaufbewahrung

- Französischer Atommüll in Schnellkochtöpfen
- „Zum Transport von atomaren Materialien“

Quelle: http://www.spiegel.de/wissenschaft/technik/frankreich-atom-abfaelle-im-schnellkochtopf-a-916753.html

Auswirkungen: Konkret

Beispiel 5: Name „James Robinson“

- **Terror Watch List**

  - Pilot

  - Anwalt

  - 5-jähriger Junge

⟶ Intensive Untersuchung vor Flügen

Auswirkungen: Konkret

Beispiel 5: Name „Jim Robinson“

- **„kein Problem“**

⟶ Wie verlässlich sind diese Systeme?

⟶ Was schließen wir daraus auf andere Systeme?

Zitat zum Abschluss

„Nun kann ich im Supermarkt zwischen mehr als 20 verschiedenen Ketchup-Sorten wählen. Aber meine digitale Post wird vom Geheimdienst geöffnet. Ist das die Freiheit, die sich meine Eltern für mich gewünscht haben?„

Katharina Nocun
pol. Geschäftsführerin der PIRATEN

1984 – Der große Bruder

1984 war nicht als Anleitung gedacht.

Grußwort an die Überwacher

Ich bin: Mark Neis, Pirat

Ich sage ganz klar:

Ich möchte von euch nicht überwacht werden

Nicht hier. Nicht heute. Nicht morgen. Gar nicht!

Fragen?

Vielen Dank!

Vielen Dank für Ihre Aufmerksamkeit!

Vielen Dank!

Material

- **Video der Piraten: https://www.youtube.com/watch?v=cpQpYVIuImI**
- **Video von manniac: https://www.youtube.com/watch?v=iHIzsURb0WI**
- **Artikel von Katharina Nocun in The European: “Her mit dem Geigerzähler!“**

Lizenz: CC-BY-3.0

Sie dürfen:

- das Werk bzw. den Inhalt vervielfältigen, verbreiten und öffentlich zugänglich machen
- Abwandlungen und Bearbeitungen des Werkes bzw. Inhaltes anfertigen
- das Werk kommerziell nutzen

Zu den folgenden Bedingungen:

- **Namensnennung** — Sie müssen den Namen des Autors/Rechteinhabers nennen.
- **Weitergabe unter gleichen Bedingungen** — Wenn Sie das lizenzierte Werk bzw. den lizenzierten Inhalt bearbeiten oder in anderer Weise erkennbar als Grundlage für eigenes Schaffen verwenden, dürfen Sie die daraufhin neu entstandenen Werke bzw. Inhalte nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch oder vergleichbar sind.

http://creativecommons.org/licenses/by/3.0/