Bedrohungen der IT-Sicherheit aus wirtschaftlicher Sicht

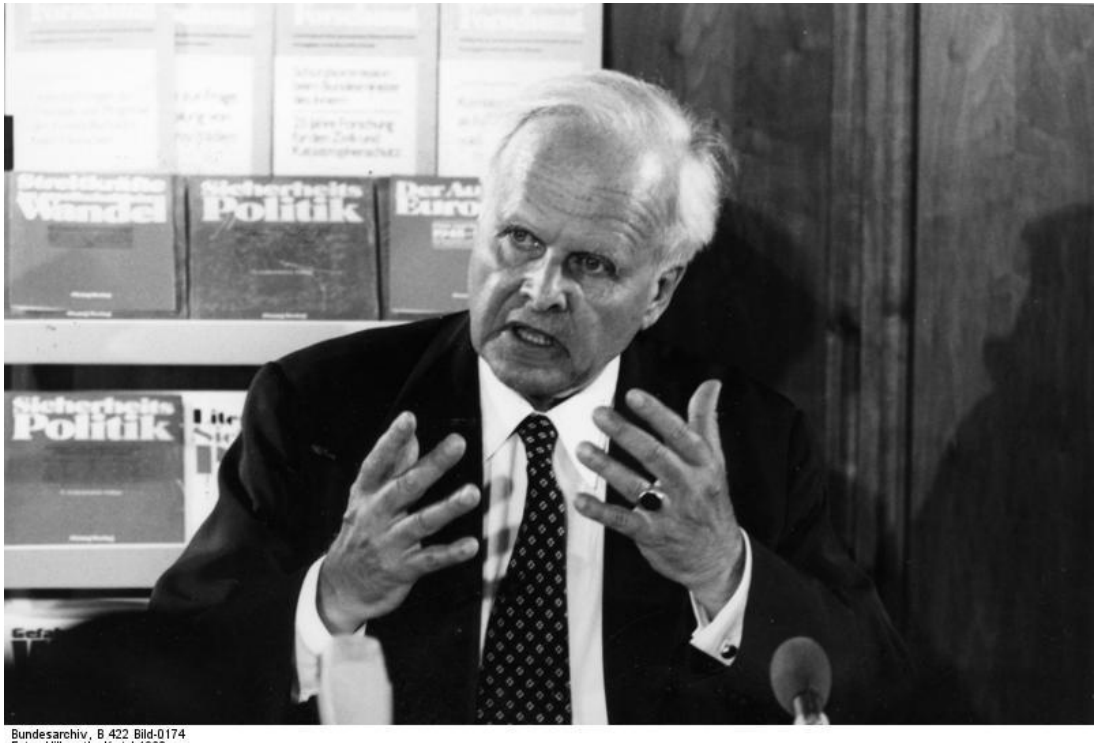
Hamburg, 23. Oktober 2013

Professor Bernhard Esslinger

UNIVERSITÄT SIEGEN

Carl Friedrich von Weizsäcker

- * 1912 in Kiel; † 2007 in Söcking
- Physiker, Philosoph und Friedensforscher
- 1964 bis 1970 Leitung der Forschungsstelle der „Vereinigung Deutscher Wissenschaftler“ (VDW) in Hamburg



Bundesarchiv, B 422 Bild-0174
Foto: Hilberath, Kurt | 1983

Carl Friedrich von Weizsäcker, 1983

Agenda

1	Die IT-Welt heute / Reale Vorfälle	5
2	Mögliche Schadenshöhe – Perspektiven und Szenarien	20
3	Risiko-Management	31
4	Ausblick	42
5	Anhang: Quellen / Modern Education for Cryptology	46

Agenda

1	Die IT-Welt heute / Reale Vorfälle	5
2	Mögliche Schadenshöhe – Perspektiven und Szenarien	20
3	Risiko-Management	31
4	Ausblick	42
5	Anhang: Quellen / Modern Education for Cryptology	46

Sicherheitsziele (1)

- Authentifizierung *(Authentication)*

Identitätsbeweis des Senders einer Nachricht gegenüber dem Empfänger

Das Internet ermöglicht die Verteilung von Daten – von selbst ist keine Authentisierung enthalten.

Peter Steiner,
The New Yorker,
5.7.1993

Sicherheitsziele (2)

- **Authentifizierung (Authentication)**

Identitätsbeweis des Senders einer Nachricht gegenüber dem Empfänger

- **Vertraulichkeit (Confidentiality)**

Das Lesen des eigentlichen Inhalts ist für Unbefugte „praktisch“ unmöglich.

- **Integrität *(Integrity)***

Eigenschaft, dass die Nachricht nicht verändert wurde

- **Verbindlichkeit *(Non-Repudiation)***

Der Empfänger kann den Nachweis erbringen, dass der Sender die Nachricht mit identischem Inhalt abgeschickt hat (Leugnen zwecklos).

- **Verfügbarkeit *(Availability)***

Die Systeme stehen wie definiert zur Verfügung.

Auswirkungen auf die IT-Sicherheit

Entwicklung der IT und deren Auswirkungen auf die IT-Sicherheit

Mainframe

"Ein Rechner, viele Benutzer"

System-zentriert

- Wenige Angriffsziele / isolierte Systeme
- Direkte Angriffe (System als Ziel)
- Angriffe sind kompliziert und aufwändig

Risiken und Maßnahmen der IT-Sicherheit

- IT-Sicherheitsrisiken sind überschaubar
  (primäres Ziel Ausfallsicherheit, Zugangskontrollen)
- Einfache Kontrolle
  (redundante Rechenzentren mit physischen Zugangskontrollen)

PC, Mobile Clients

"Viele Rechner, ein Benutzer"

Anwender-zentriert

- Viele Angriffsziele / vernetzte Systeme
- Indirekte Angriffe (Benutzer als Ziel)
- Angriffe sind oftmals einfach

Risiken und Maßnahmen der IT-Sicherheit

- IT-Sicherheitsrisiken sind vielschichtig
  (nicht autorisierte Zugriffe, Viren und Würmer, Phishing, Denial of Service, Identitätsdiebstahl, etc.)
- Komplexe / virtuelle Kontrolle
  (Virenscanner, Firewalls, Software-Aktualisierung, Verschlüsselung, Awareness-Trainings, etc.)

Attacks on the User

Why is he/she at the focus of the attacks?

- Relatively small efforts necessary
  - e.g. phishing e-mails
- There is a mass of inter-connected Internet applications
  - Web browser, e-mail clients, media player, instant messenger, applications with automated Internet update, file viewer; common libraries, Java, etc.
  - Using exploits in existing applications (especially „Zero Day threats“)
- “Human factor”
  - Unskilled or careless employees with low IT security know-how
  - Simple scalability of attacks because of the big number of users
  - Distribution of work (globalization, outsourcing) simplified social engineering
  - Open periphery, outsourcing, mix of internals and externals
- Complex controls
  - Heterogeneous IT landscapes
  - Continuous update of installations and distribution of security patches
- Additional attack vectors
  - WLAN, Bluetooth, Infra red, USB sticks, CD/DVD, BYOD, etc.

Attacks on the Infrastructure
Why has this changed?

- More potential players
  - e.g. Stuxnet, Duqu, Flame
  - Information war in ESTLAND 2007, in GEORGIEN 2008
- Better knowledge about the Internet architecture
  - e.g. attack against DNS and registries

Angriffs-Beispiele (1)

- Datendiebstahl bei RSA Inc.
  - 40 Mio. Security Tokens bei Kunden betroffen
- Sicherheitsleck bei Bundesfinanzagentur
  - Angebote von außen änderbar
- Zugangsdaten zum Kauf angeboten
  - Amazon, eBay, Packstation, PayPal, Mailkonten
- Virus sabotiert Krankenhaus-IT
  - Geplante Operationen ausgesetzt
- 100.000 Namen, Adressen und Bankverbindungen gestohlen
  - Unverschlüsselt bei einem Callcenter
- Versehentlich Spione enttarnt
- Spanner beobachtet Schülerinnen per Webcam
- Gezielter Angriff auf US-Firmen mit PDFs
- Phishing, Skimming, …

Angriffs-Beispiele (2)

- Drogen-Schmuggler spionieren mit Hilfe von Hackern Computersysteme im Antwerpener Hafen aus (Interpol, 18.10.13) http://www.heise.de/newsticker/meldung/Europol-sieht-Gefahr-in-Teams-aus-Hackern-und-Schmugglern-1981456.html
- Stuxnet
  - 2010 entdeckt , Schadprogramm zur Überwachung und Steuerung technischer Prozesse (SCADA-System) der Firma Siemens
  - Störte die Urananreicherungsanlage im Iran
  - Gebaut aus bisher unbekannten Sicherheitslücken (0-day exploits)
  - Tarnung mit gestohlenen digitalen Unterschriften
  - Genaue Kenntnis des Ziels
  - Infektionsweg über USB und Druckernetzwerk, da die Steuerung nicht mit dem Internet verbunden war. Diese beiden Schwachstellen waren schon bekannt.
- …

Vorgehen zur Gewährleistung von IT-Sicherheit

Ganzheitlich innerhalb und zwischen Organisationen

- CERT (Austausch von Informationen zwischen Organisationen)
- Ganzheitlich:
  - Risiko-Management
  - Multi-Layer-Security
  - Kombination von technischen und organisatorischen Maßnahmen

Technische Lösungen (1)
Woher kommen die Schwächen?

http://de.wikipedia.org/wiki/Turmbau_zu_Babel

Technische Lösungen (2)
Woher kommen die Schwächen?

- Systeme sind komplex, frei programmierbar
- Sicherheit ist nicht spürbar, ständig gibt es neue Features, Unternehmen (Apple, Google, Samsung) wollen Ihre Daten
- Sicherheit ist nicht intuitiv
- Naive Lösungen
- Unvorhergesehene Nutzung (Gewaltvideos mit Handies)
- Komposition (Chip& PIN)
- Fehlen von durchgängigen Prozessen, abschließender Analyse, gemeinsamer Sprache (nicht PPT)
- Und manchmal verstehen auch die Sicherheitsexperten einander nicht: http://www.heise.de/newsticker/meldung/Kommentar-Standardpasswoerter-kein-Sicherheitsrisiko-1981454.html

Agenda

1	Die IT-Welt heute / Reale Vorfälle	5
2	Mögliche Schadenshöhe – Perspektiven und Szenarien	20
3	Risiko-Management	31
4	Ausblick	42
5	Anhang: Quellen / Modern Education for Cryptology	46

Rahmendaten

Für die maximale Risikohöhe

- Bruttoinlandsprodukt (BIP)
  - z.B. Deutschland pro Jahr: 2666 Mrd. € (Stand 2012)
- Gesamtwert aller Aktien eines Unternehmens (Marktkapitalisierung)
  - z.B. Siemens: ca. 80 Mrd. € (Stand 17.10.2013)

Aktuelle Studien: Schäden in Deutschland 2011

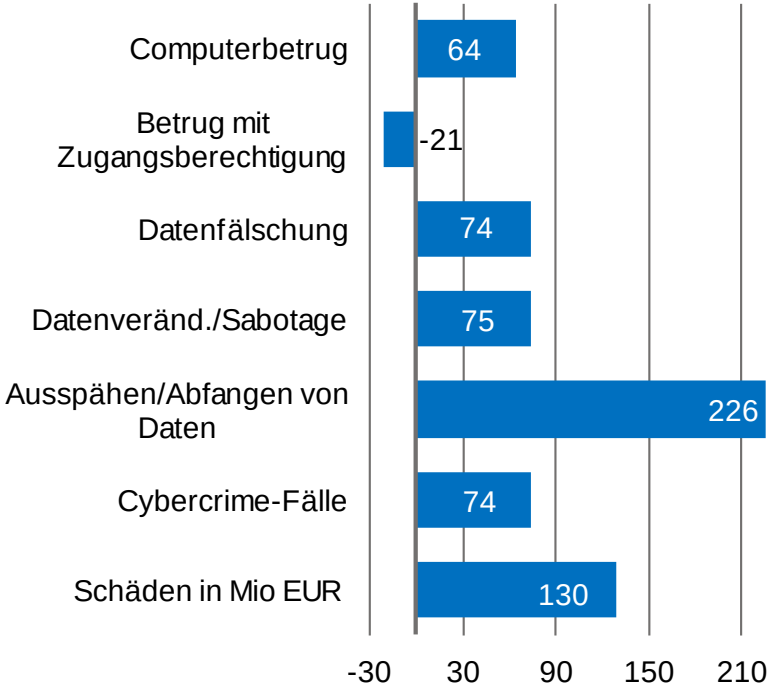
- Durch Hacker-Angriffe und Geheimnisverrat: 4,2 Mrd. Euro *
  (30 % der entdeckten Angriffe aus Russland, 25 % aus den USA, 11 % aus Asien)
- Durch Produktpiraterie: Umsatzverlust: fast 8 Mrd. Euro **
  (d.h. rund 37.000 Arbeitsplätze)

* Industriespionage, Corporate Trust (Münchner Sicherheitsberatung), Studie April 2012
** Verband Deutscher Maschinen- und Anlagenbauer (VDMA), Studie April 2012

BKA – Lagebericht Cyber-Crime 2011

Cyber-Crime in Deutschland

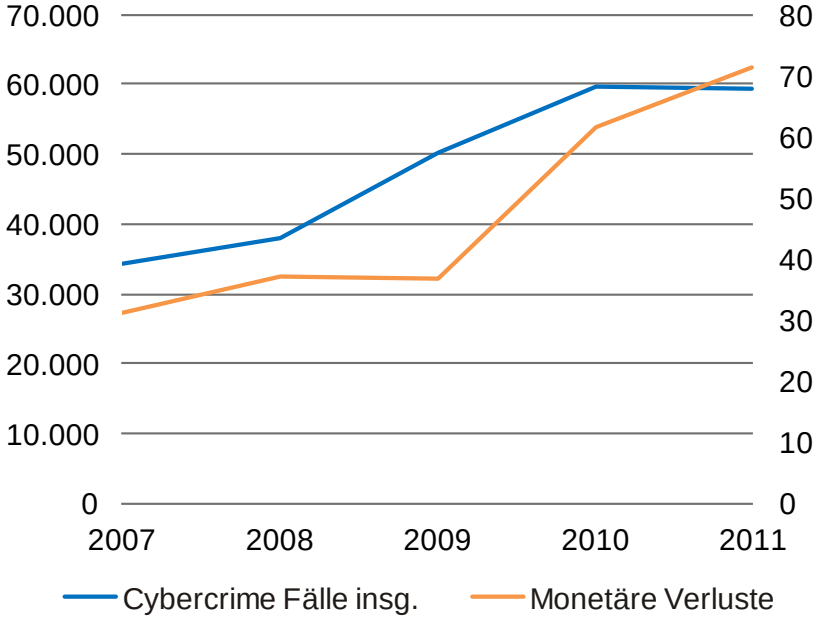
% Veränderung, 2007 - 2011



Quelle: BKA

Volkswirtschaftlicher Schaden durch Cyber-Crime

Einzelfälle nach Straftaten (links),
finanzieller Schaden in Mio. EUR (rechts)



Quelle: BKA

70 Mio. Euro Schaden
(erfasst nur, wenn angezeigt und deutsches Opfer)

BND zu Cyberkriminalität in Deutschland

- Umsätze der Cyberkriminalität übersteigen die des Drogenhandels
- Derzeit liegt der Fokus auf der Verwertung gestohlener „Identitäten“ sowie auf Schutzgelderpressung
- Der technische Engpass ist die Umwandlung von virtuellem in echtes, sauberes Geld
- Hacker/Cracker gehen immer früher dazu über, ihre Fertigkeiten zu vermarkten, Hacking also ökonomisch motiviert zu betreiben
- Die Gefährdung geht vorwiegend von organisierter Kriminalität (OK) und von Staaten aus – Einzeltätern fehlen die nötigen Ressourcen
- Etablierte Geschäftsmodelle:
  - Zerstörende Operationen: Ausschalten eines Konkurrenten, Sabotage einer Kriegspartei
  - Informationshandel: „private Intelligence“, gestohlene digitale Identitäten
- Auch staatliche Akteure betreiben Outsourcing: z.B. bei Info War

Die Haupt-Akteure und ihre Fähigkeiten

Von chaotisch zu organisiert

- Hacker
  - Script Kiddies (geringes Wissen, Nutzen vorhandener Werkzeuge)
  - Hacker, Cracker, etc.
- Terroristen: Cyberterrorismus/Cyberanarchismus
- Unternehmen
  - „Business Intelligence“: Handel mit legalen und illegalen Informationen
  - Kriminelle Organisationen: Computerkriminalität, Verwertungsketten
- Nachrichtendienste und Polizeibehörden
- Staaten

- Und hinzu kommen Innentäter.

UNODC Cyber-Crime-Studie

- In 2011, more than one third of the world's total population had access to the internet.
- Over 60 % of all internet users are in developing countries, with 45 % of all internet users below the age of 25 years.
- It's estimated that mobile broadband subscriptions will approach 70 % of the world's total population by 2017.
- The number of networked devices (the "internet of things") are estimated to outnumber people by six to one, transforming current conceptions of the internet.
- In the future hyper-connected society, it is hard to imagine a "computer crime", and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity.
- Average loss per person: 200 USD (Seite 30, basierend auf Norton).

Comprehensive Study on Cybercrime - United Nations Office on Drugs and Crime
http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Vision Industrie 4.0

Mehr Produktivität und höhere Flexibilität durch dezentrale, hochgradig vernetzte Systeme
Erfordert höhere Sicherheitsstandards

Globales elektronisches Aufklärungssystem

Echelon

Echelon hört ungefiltert den gesamten eMail-, Telefon-, Fax- und Telexverkehr ab, der weltweit über Satelliten weitergeleitet wird.

„Natürlich spionieren wir euch aus, weil ihr dauernd bestecht und wir nie.“

Woolsey, ehemaliger CIA Chef in der FAZ vom 04.02.2001

Betreiber	
USA National Security Agency (NSA)	
Großbritannien Government Communications Headquarters (GCHQ)	
Kanada Communications Security Establishment (CSE)	
Australien Defence Signals Directorate (DSD)	
Neuseeland Government Communications Security Bureau	

Menwith Hill Yorkshire	Misawa Japan
Morwenstow Cornwall	Waihopai Neuseeland
Bad Aibling Bayern	Yakima Firing Center 200 km sw von Seattle
Geraldton Station Westaustralien	Leitrim Kanada
Shoal Bay Nordaustralien	Sugar Grove 250 km sw von Washington D.C.

Waihopai

Kommunikationssatelliten

Kommunikationssatelliten

Abhörstation

Grafik: Landesamt für Verfassungsschutz Baden-Württemberg

Literaten haben es zumindest schon lange geahnt …

- http://de.wikipedia.org/wiki/The_Newsroom
  - season 1, episode #8 (2012) nahm Snowden vorweg
- „1984“ (1949) und „Der Staatsfeind Nr. 1“ (1998)
  - nahmen die NSA-Überwachung vorweg
  - http://www.moviepilot.de/movies/der-staatsfeind-nr-1
- Geschichte in c‘t nahm Erpressung per Herzschrittmacher vorweg
- „Stirb langsam 4“ enthält Manipulation von Ampeln und U-Bahnen
- Schneier sammelte mehrere Movie-Plots zu Cyber-Crime
- Der Roman „Blackout“ (2012) zeigt, wie ein Infrastruktur-Angriff (Stromausfall) ein Land verändert.

08.06.12 | **Schnüffelliste**

Diese 377 Worte machen Sie in den USA verdächtig

Ob "Flughafen" oder "Brücke", "Schweine" oder "Vorführung": Nach diesen und ähnlichen Schlagworten durchsucht das US-Heimatschutzministerium Telefonverkehr und Internet. Wem nützt das?

Von Hanns-Georg Rodek

Foto: Ronald Grant Archive / Mary Evan

Will Smith im Netz-Visier der Geheimdienste: Der Film "Staatsfeind Nr. 1" wirkte 1998 noch wie Science-fiction. Heute ist die flächendeckende Kontrolle der Kommunikationsnetze banale Gegenwart

DIE WELT

Zukünftige Anwendungen für Kryptographie

Auto-Sicherheit

- In einem Auto sind heute schon mehr Chips als in einem PC
- Warnung vor Glatteis, Verhinderung von Fahrfehlern. Ohne Krypto: Staus durch Hacker?

Medizinische Implantate

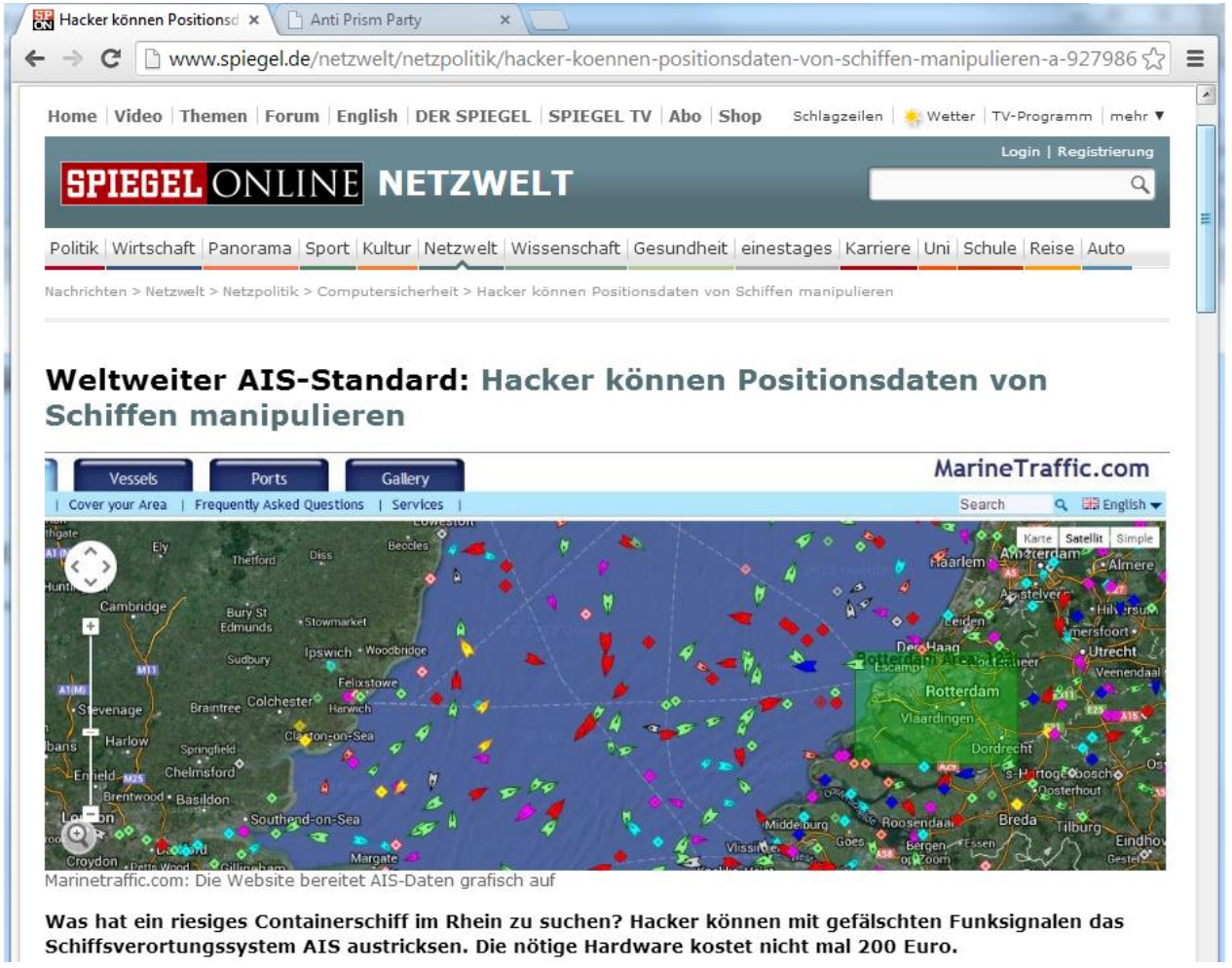
- Herzschrittmacher übertragen die Daten per Funk unverschlüsselt.
- Implantierte Geräte lassen sich vom Arzt via Internet überwachen und steuern.

Agenda

1	Die IT-Welt heute / Reale Vorfälle	5
2	Mögliche Schadenshöhe – Perspektiven und Szenarien	20
3	Risiko-Management	31
4	Ausblick	42
5	Anhang: Quellen / Modern Education for Cryptology	46

Gesunder Menschenverstand (Meldungen vom 16.10.13)

- http://www.heise.de/newsticker/meldung/Manipulation-von-Funkdaten-Schiffe-versenken-mit-AIS-Hacks-1980065.html
- http://www.spiegel.de/netzwelt/netzpolitik/hacker-koennen-positionsdaten-von-schiffen-manipulieren-a-927986.html



Einschätzung von Risiko und Reaktion

Badesee: Plötzensee in Berlin (Wikimedia)

- Wann nehmen wir Risiken als solche wahr?
- Was ist gesellschaftlich akzeptiert?
- Kann man die Zahl der Toten aufrechnen?
- Governance: Allokieren wir gesellschaftliche Ressourcen adäquat?
- Gehen wir reaktiv oder präventiv (langfristig) vor?

100 % geht nicht !

- IT-Sicherheit dient der Sicherung des Standortes und der Innovation
- Adäquate Risikovorsorge
- IT-Gesamtausgaben laut Bitkom: ca. 60 Mrd. €
  - Adäquat wären davon ca. 5 % für IT-Sicherheit = 3 Mrd. € (branchenabhängig)
- Externe Effekte internalisieren
  - Regulierung gegen Marktversagen

Empfehlungen (1)

- Was findet man in den Computerzeitschriften?
  - Wer ist die gefährlichste Frau / Prominente der Welt?
  - Updates, gesunder Menschenverstand, Misstrauen, Hinterfragen
- Was sagen
  - unsere Behörden (LfV, BSI, …),
  - entsprechenden Verbände (Bitcom, DsiN, …),
  - internationale Einrichtungen (NIST, OWASP, …) ?

  Beispiele:
  - Identifizieren der wichtigsten Daten im Unternehmen?
  - Verschlüsseln aller wichtigen Daten (at rest & in transit)
  - Awareness
  - Die Konzentration auf die wichtigsten Daten und auf die Zu- und Ausgänge ist kosteneffizient.

Lesen Sie DIE WELT auf allen digitalen Kanälen. Jetzt mit ePaper testen. Nur 0,99 € im 1. Monat.

25.08.09 | Kriminalität

Jessica Biel ist die gefährlichste Frau im Internet

Jessica Biel ist Hollywoods Nummer eins – wenn es nach Internet-Kriminellen geht. Denn wer online nach der schönen Schauspielerin sucht, landet am häufigsten auf einer betrügerischen Webseite. Kollege Brad Pitt, im vergangenen Jahr noch vorne, hat bei den Banditen dagegen abgewirtschaftet.

ARTIK

E-Mail

Komm

EIGE

Empfehlungen (3)

http://www.heise.de/security/meldung/BSI-Sicherheitskompass-Zehn-Regeln-fuer-mehr-Sicherheit-im-Netz-1968203.html

27.09.2013 14:33 « Vorige | Nächste »

BSI Sicherheitskompass: Zehn Regeln für mehr Sicherheit im Netz

vorlesen / MP3-Download

Das BSI beteiligt sich mit der Aktion "BSI Sicherheitskompass" am diesjährigen europäischen Cybersicherheitsmonat, der im Oktober stattfindet. Zehn Faustregeln hat das Bundesamt für Sicherheit in der Informationstechnik in Zusammenarbeit mit der Polizeilichen Kriminalprävention der Länder aufgestellt:

1. Verwenden Sie sichere Passwörter.
2. Schränken Sie Rechte von PC-Mitbenutzern ein.
3. Halten Sie Ihre Software immer auf dem aktuellen Stand.
4. Verwenden Sie eine Firewall.
5. Gehen Sie mit E-Mails und deren Anhängen sowie mit Nachrichten in Sozialen Netzwerken sorgsam um.
6. Erhöhen Sie die Sicherheit Ihres Internet-Browsers.
7. Vorsicht beim Download von Software aus dem Internet.
8. Sichern Sie Ihre drahtlose (Funk-)Netzwerkverbindung.
9. Seien Sie zurückhaltend mit der Angabe persönlicher Daten im Internet.
10. Schützen Sie Ihre Hardware gegen Diebstahl und unbefugten Zugriff.

Der interaktive Kompass klärt über die zehn Regeln auf.

Bild: Polizeiliche Kriminalprävention der Länder und des Bundes

Empfehlungen (4)

http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass/sichere-passwoerter.html

Empfehlungen (5)

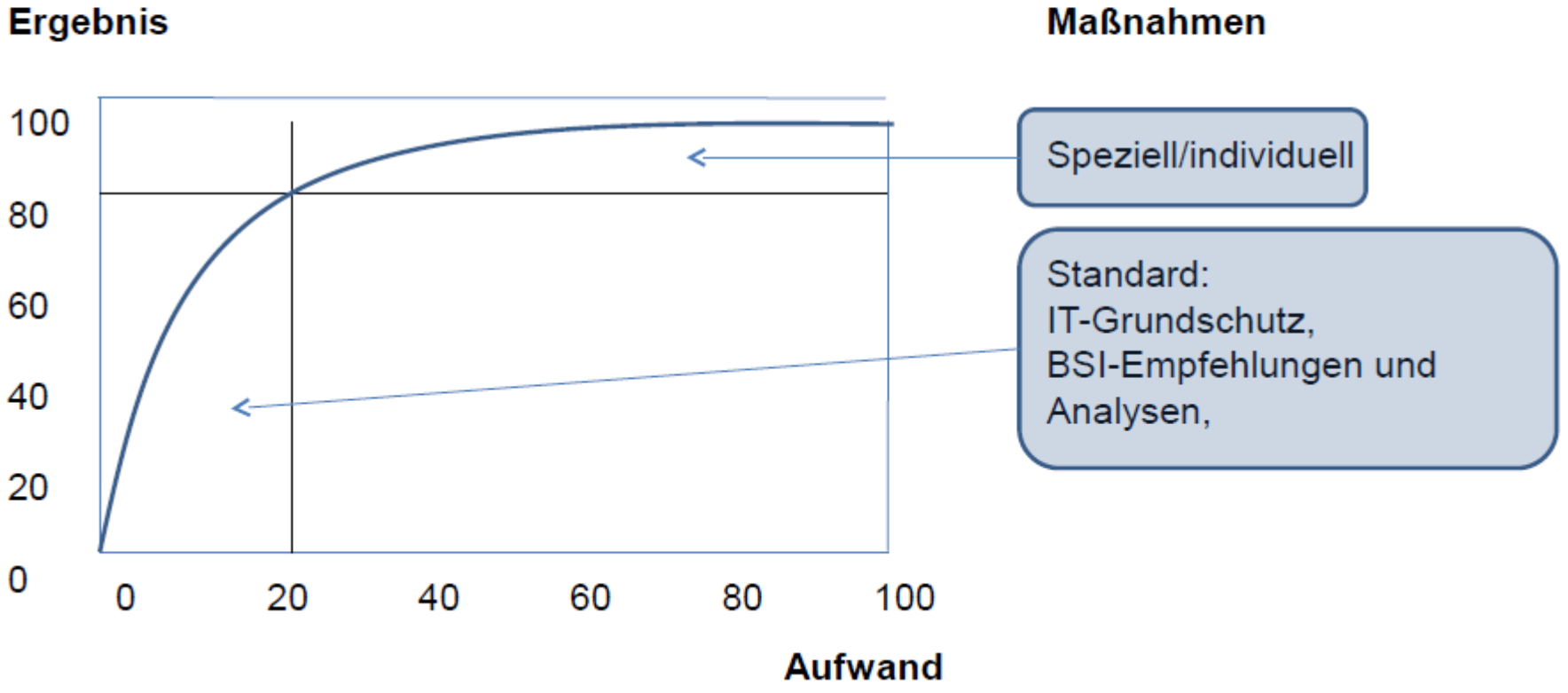
- https://www.sicher-im-netz.de/unternehmen/DsiN-Sicherheitscheck.aspx
- https://www.sicher-im-netz.de/files/documents/unternehmen/studie-mittelstand_2013_web.pdf
- https://www.sicher-im-netz.de/files/documents/Pocketquide_IT_Sicherheit.pdf

Empfehlungen (6)

- Awareness / Aufklärung und klare Regeln am wichtigsten:
  - Mitarbeiter ansprechen, Betriebsvereinbarung unterschreiben lassen
  - IT nur für die Arbeit (auch aus rechtlichen Gründen)
- Ausreichend Zeit und Schulung der Administratoren
- Gutes Betriebsklima, ethisches Verhalten
- IT Security-Experten einkaufen, regelmäßige Penetrationstests
- Der Einkauf: zentralisiert, setzt auch Produktvorgaben durch
  - z.B. Richtung Datenkonsistenz, GoldenSource, wofür welche Zertifikate
  - Pragmatisch, kein 100+-seitiges Rahmenwerk, das vor allem Juristen und Projektmanager beschäftigt
- Einsatz von Open Source aus Kosten- und Anpassbarkeitsgründen
- Security by Design
  - z.B. vor Einsatz neuer Technologien wie „Industrie 4.0“

Empfehlungen (7)

- Standard-Sicherheitsmaßnahmen für 80 Prozent der Cyber-Angriffe,
- Individuelle Maßnahmen für 20 Prozent der Cyber-Angriffe



Agenda

1	Die IT-Welt heute / Reale Vorfälle	5
2	Mögliche Schadenshöhe – Perspektiven und Szenarien	20
3	Risiko-Management	31
4	Ausblick	42
5	Anhang: Quellen / Modern Education for Cryptology	46

Ausblick (1): Ein ewiger Wettlauf
Wirtschaftliche Aspekte für Unternehmen und Infrastruktur

- Ausgaben für IT-Sicherheit weniger als 3 Mrd. €.
- Adäquate Risikovorsorge bedeutet
  - Balance zwischen Sparen und Totalverlust
  - **Kritische IT-Infrastrukturen** dürfen nicht allein mit den Maßstäben der Budgetminimierung bemessen werden
    → Hier hat der Staat eine wichtige Aufgabe
  - Kritisches Know-How muss tatsächlich und rechtlich im Hause (bzw. bei Behörden in nationaler Hoheit) verbleiben (Auflage auch der BaFin)
- Externe Effekte internalisieren
  - Regulierung gegen Marktversagen
  - Primat der Wirtschaftlichkeit schafft Sicherheitsprobleme
  - Sicherheit ist kein Designkriterium bei COTS-Produkten
  - Es gibt keine breite, zivile und qualifizierte Wertediskussion über den Umgang mit dem Cyber-Space
- Die Balance kann gehalten werden

COTS: commercial off-the-shelf (englisch für Kommerzielle Produkte aus dem Regal / von der Stange)

Ausblick (2): Eine politische Entscheidung

Wer wesentliche Freiheit

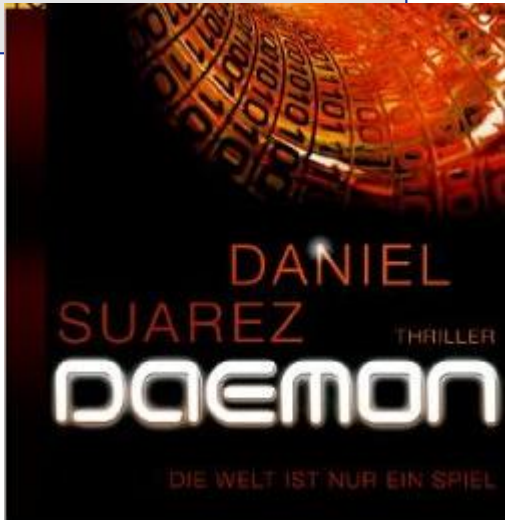
Wir in der Regierung müssen uns vor unbefugtem Einfluss … durch den militärisch-industriellen Komplex schützen … Wir dürfen es nie zulassen, dass die Macht dieser Kombination unsere Freiheiten oder

Die Snowden-Affäre hat uns allen gezeigt, dass wir endlich aufwachen müssen …

Wenn ihr Schiss habt vor der Freiheit, geht zurück in euren Stinkstall und lasst Euch verwursten!

F. K. Waechters (1937-2005)

— Oder muss man wieder die Literatur bemühen, um Hoffnung – in einem schizophrenen Spieler – zu finden? (Suarez; Daemon und Darknet)

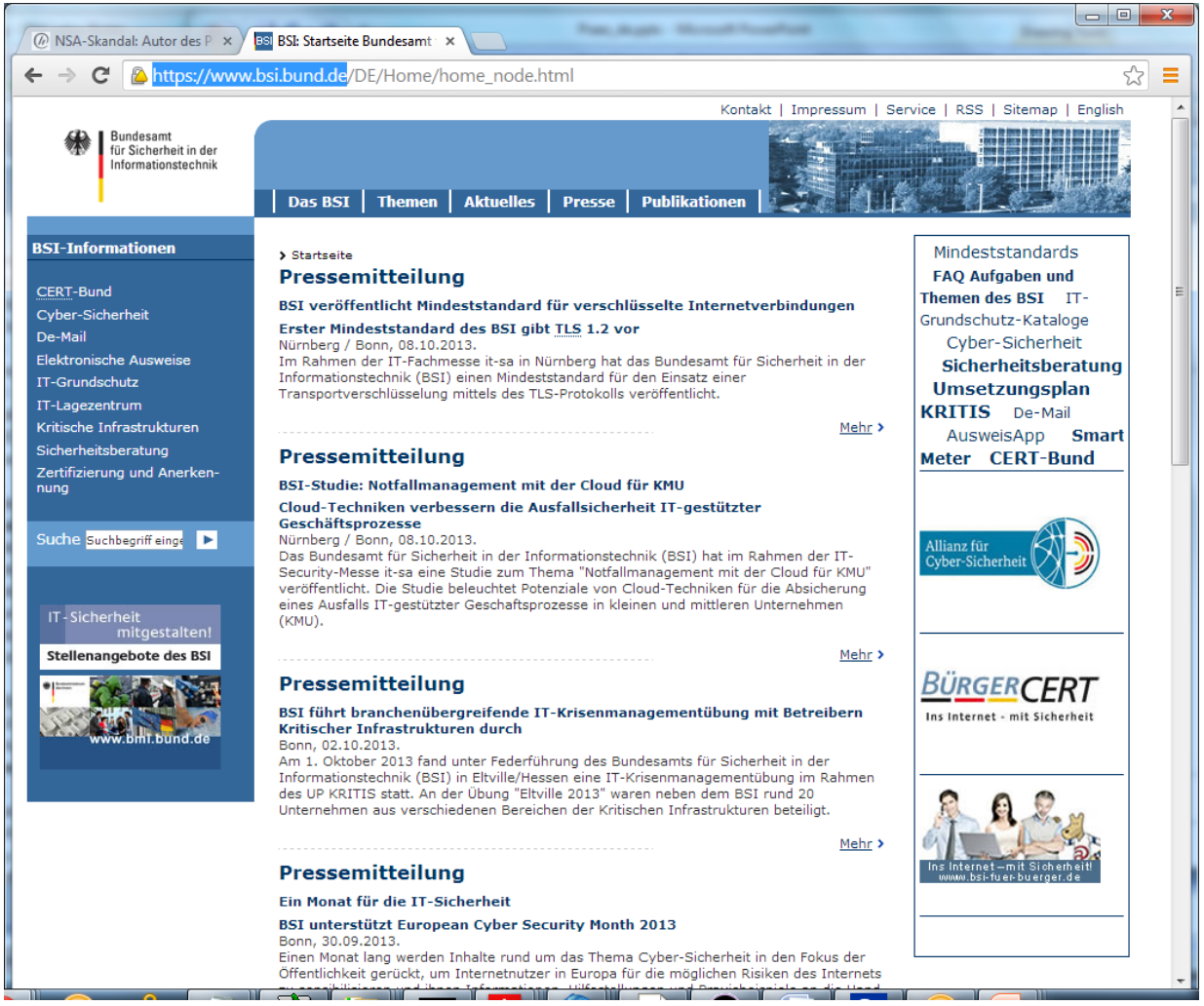


Agenda

1	Die IT-Welt heute / Reale Vorfälle	5
2	Mögliche Schadenshöhe – Perspektiven und Szenarien	20
3	Risiko-Management	31
4	Ausblick	42
5	Anhang: Quellen / Modern Education for Cryptology	46

Quellen (1)

— https://www.bsi.bund.de



Quellen (2)

- https://www.bsi-fuer-buerger.de
- https://www.buerger-cert.de/
- https://www.sicher-im-netz.de/

- http://www.verfassungsschutz.hessen.de/irj/LfV_Internethttp://www.heise.de/thema/NSA
- https://www.owasp.org/index.php/Top_10_2013 (Open Web Application Security Project)
- http://csrc.nist.gov/
- http://www.heise.de/thema/NSA
- http://www.spiegel.de/thema/nsa_ueberwachung/

Quellen (3)

- http://www.mik.nrw.de/verfassungsschutz/spionageabwehr/abwehr-von-wirtschaftsspionage.html
- www.im.nrw.de/wirtschaftsspionage

Quellen (4)

http://www.handelsblatt.com/politik/international/wikileaks-will-us-grossbank-blossstellen/3651782.html

http://www.express.de/news/politik-wirtschaft/ex-banker-gibt-steuer-cd-an- wikileaks/-/2184/5752846/-/index.html

http://www.heise.de/newsticker/meldung/Schwarzmarktpreise-fuer-gestohlene-Online-Banking-Daten-ermittelt-1183524.html

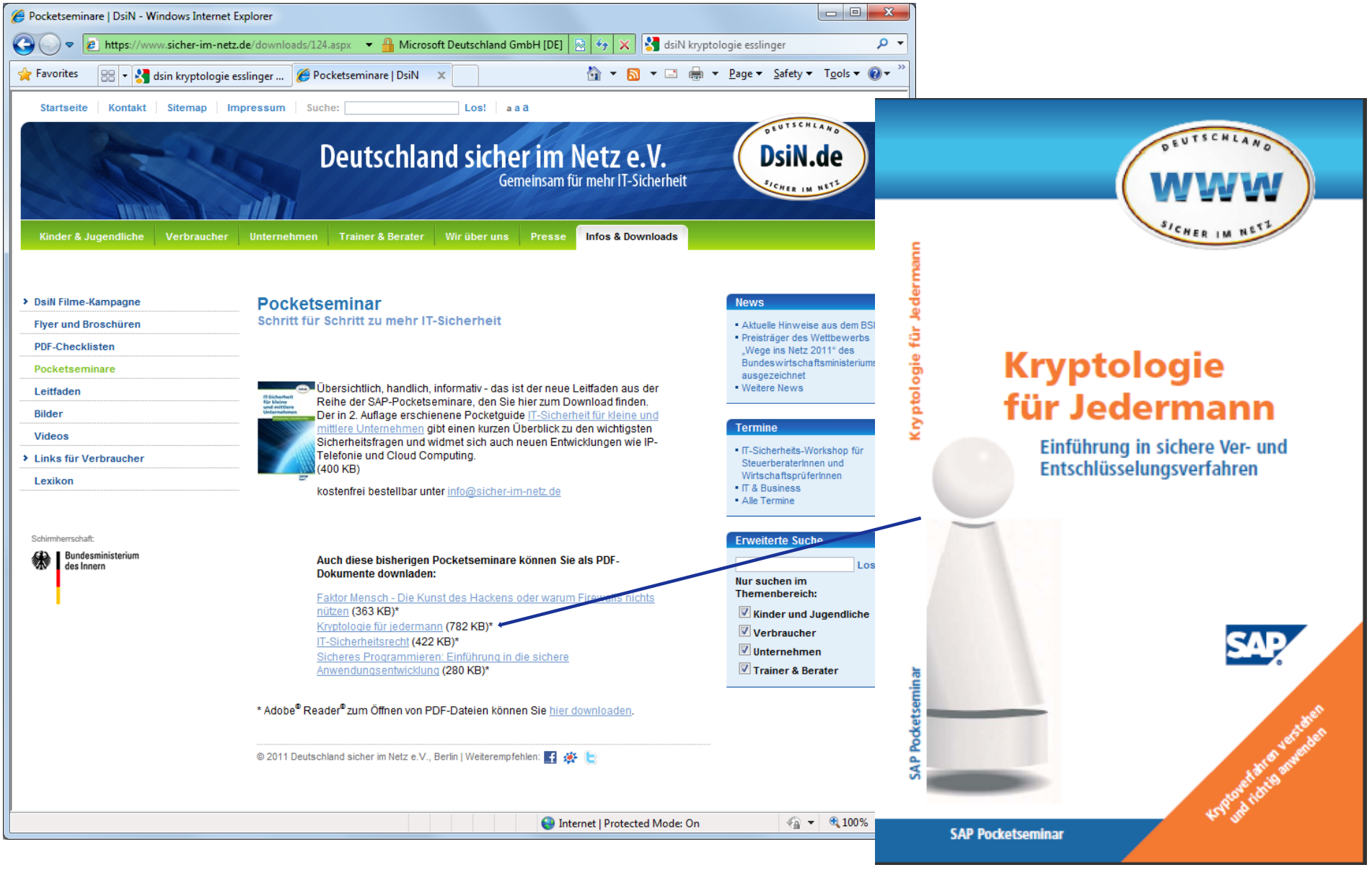
Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder. Orientierungshilfe. Datensicherheit bei USB-Geräten. Stand: 27. November 2003. Abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Orientierungshilfen/DatensicherheitBeiUSBGeraeten.pdf?__blob=publicationFile

http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

http://www.personalausweisportal.de

Kryptologie für jedermann
https://www.sicher-im-netz.de/files/documents/06_02_Kryptologie_fuer_Jedermann.pdf

Siehe Quelle (4)



Quellen (5)

http://www.heise.de/newsticker/meldung/Online-Banking-Trojaner-attackiert-Smartphones-mit-Windows-Mobile-1195455.html

http://www.heise.de/security/meldung/chipTAN-Verfahren-der-Sparkassen-ausgetrickst-866115.html

http://www.h-online.com/open/news/item/SSL-meltdown-forces-browser-developers-to-update-1213358.html

http://www.h-online.com/security/news/item/SSL-meltdown-a-cyber-war-attack-1214104.html

ftp://ftp.rfc-editor.org/in-notes/rfc5246.txt

http://www.internet-sicherheit.de/fileadmin/docs/publikationen/Reale-Nutzung-kryptographischer-Verfahren-in-TLS-SSL-CeBIT-2009-03-06.pdf

http://www.handelsblatt.com/politik/international/wikileaks-will-us-grossbank-blossstellen/3651782.html

http://www.express.de/news/politik-wirtschaft/ex-banker-gibt-steuer-cd-an-wikileaks/-/2184/5752846/-/index.html

Quellen (6)

http://www.heise.de/newsticker/meldung/Schwarzmarktpreise-fuer-gestohlene-Online-Banking-Daten-ermittelt-1183524.html

http://www.h-online.com/security/news/item/RSA-hack-could-endanger-the-security-of-SecurID-tokens-1210393.html

http://www.h-online.com/security/news/item/RSA-break-in-it-was-the-Flash-Player-s-fault-1221057.html

http://www.anti-prism-party.de/cms/downloads/sichere-email-smime-thunderbird-anleitung.pdf

Quellen (7)

http://www.heise.de/newsticker/meldung/Studie-Nur-8-5-Prozent-der-Internet-Kriminalitaet-wird-angezeigt-1982889.html

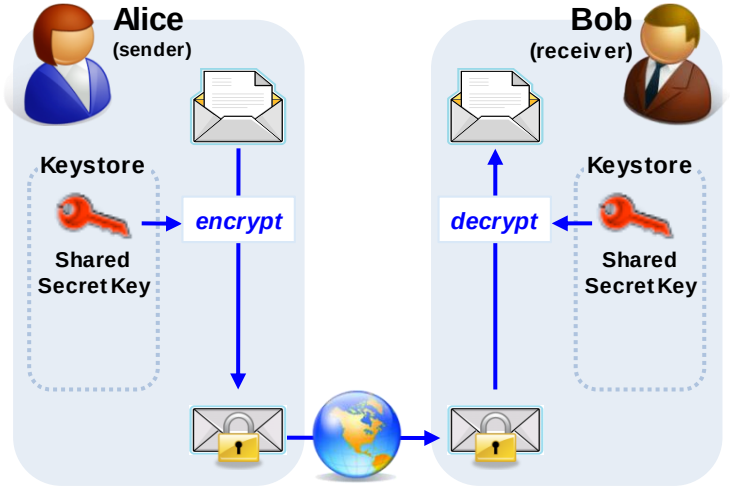
21.10.2013: Ergebnis der Studie, die der niedersächsische Innenminister Boris Pistorius vorlegte: **Nur 8,5 Prozent der Internet-Kriminalität wird angezeigt**

Nach der Studie lag der **Internet-Betrug** 2012 beim Vierfachen aller gemeldeten Fälle, das Abfischen vertraulicher Daten ("**Phishing**") übers Internet beim Zehnfachen und die **finanziellen Einbußen und der Datenverlust** durch Computer-Viren oder Trojaner beim Zwanzigfachen der gemeldeten Fälle.

Cryptography knowledge
Symmetric Key, Public Key and Hybrid Encryption

Symmetric Key Encryption

The same key for encryption and decryption, shared by sender and receiver.

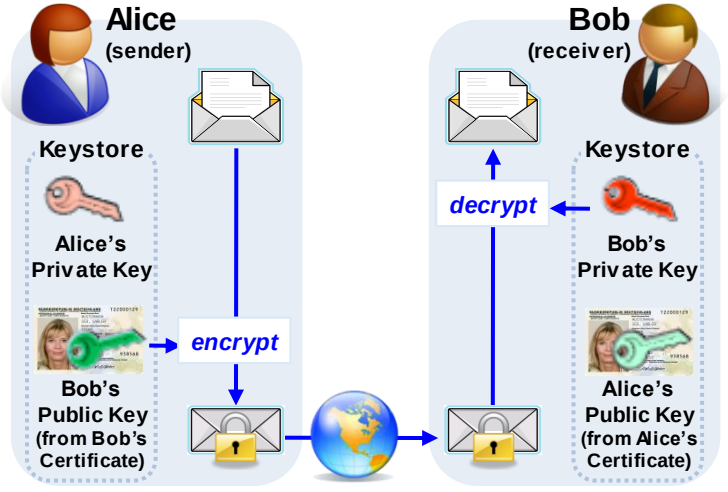


The sender needs to know the shared secret key which must be exchanged securely first.

Public Key Encryption

Different keys for encryption and decryption, each person has a key pair (public and private key).

The association of a public key and an identity can be assured with a public key certificate.



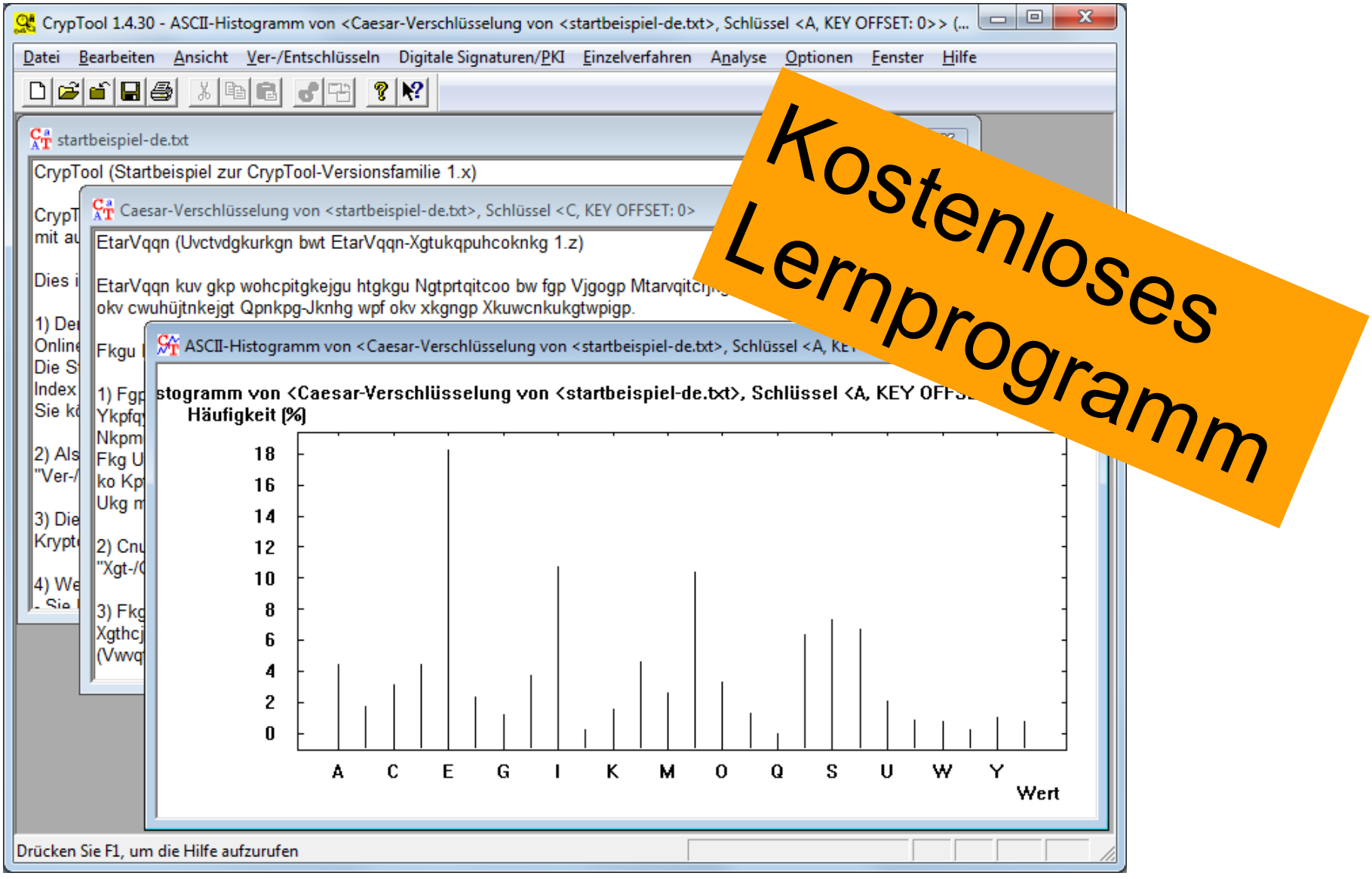
The sender does not need any secret information, the certificates are public and can be exchanged unencrypted. However, the private key must not leave its owner's key store.

In practice it's mostly a combination of both (Hybrid Encryption):
Public-key encryption to exchange symmetric keys securely which are then used to encrypt the data.

➔**Security on the internet with many-to-many connections is only feasible with public key / hybrid cryptography.**

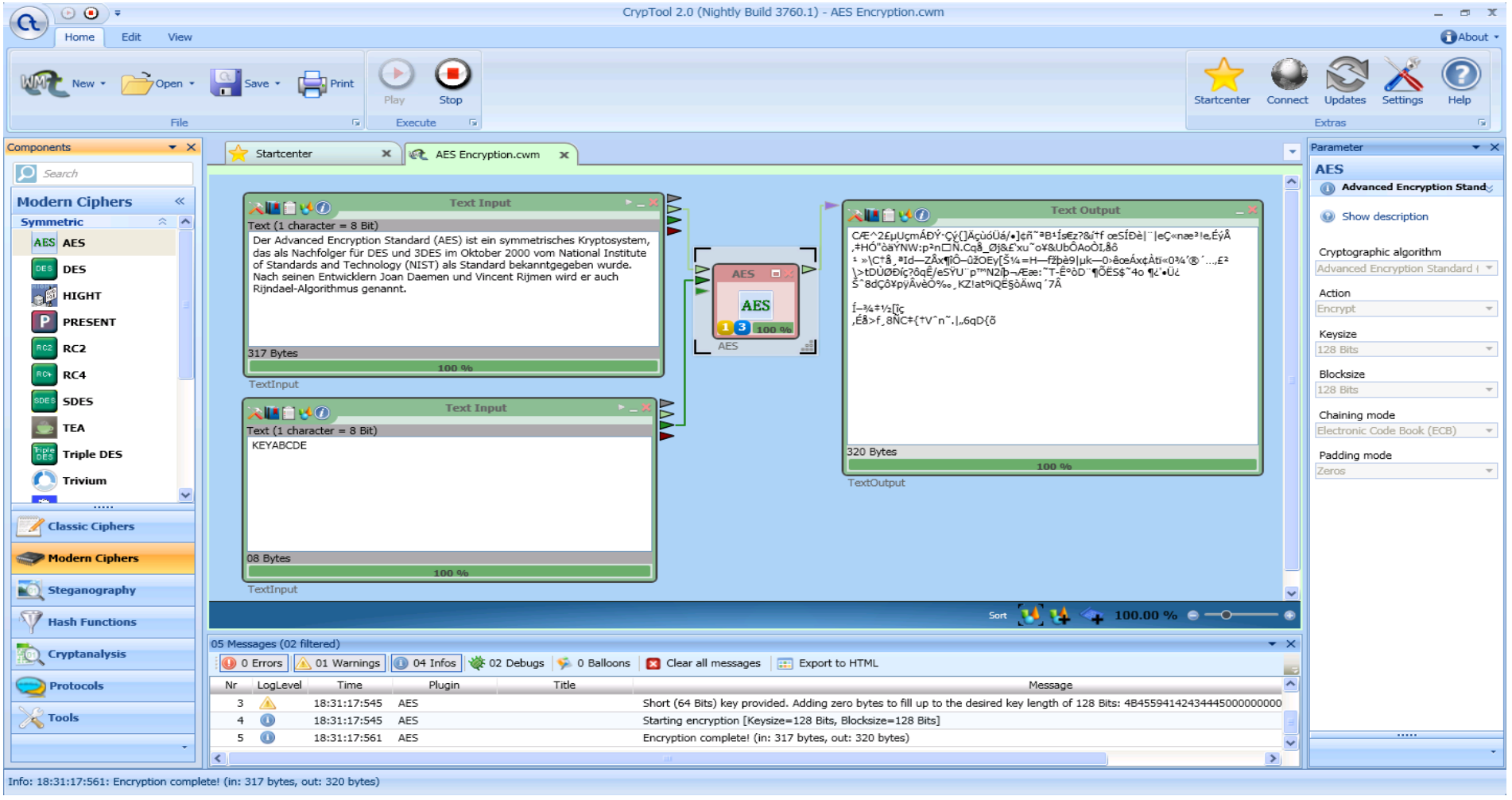
CRYPTOOL www.cryptool.org

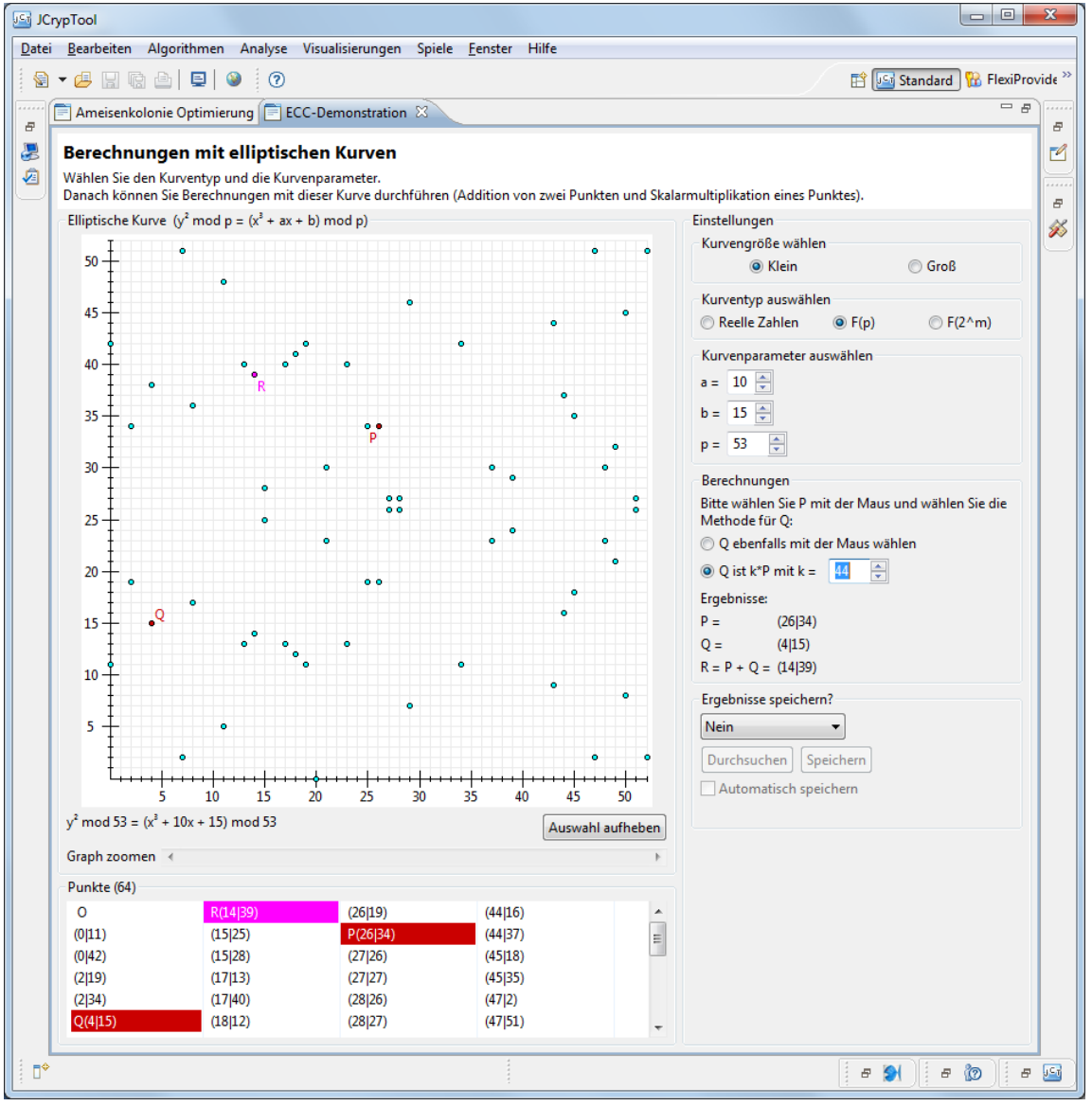
Example of a classic symmetric encryption (Caesar) and its analysis in CT1



CRYPTOOL www.cryptool.org

Example of modern symmetric encryption (AES) in CT2



www.cryptool.org

Example of modern asymmetric encryption (ECC) in JCT