
CYBERCRIME COORDINATION
KOBIK
SCOCI
CYCO
fedpol

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol
Bundeskriminalpolizei
KOBIK

Bekämpfung der Kriminalität im Netz und in der Wolke

Tobias Bolliger, Kommissariatsleiter a.i. KOBIK

25.11.2015, GovCloud Day, Olten

Iran bestätigt Cyber-Angriff durch Stuxnet

Der Iran hat erstmals eine Cyber- Attacke auf seine Industrieanlagen durch den mysteriösen Computer- Schädling Stuxnet bestätigt.

1085 Fälle von Kinder-Pornografie

1206 Meldungen über harte Pornografie untersuchten die Ermittler des Bundes im vergangenen Jahr. Zu 90 Prozent waren Kinder die Opfer. Doch die Arbeit der Ermittler wird immer schwieriger.

Doch was genau ist CYBERCRIME ist kaum zu ignorieren

Internetkriminalität verursacht bei Firmen Milliardenschäden

Sie breitet sich aus wie ein Krebsgeschwür: Internetkriminalität wird von Interpol auf dieselbe Stufe gestellt wie den Drogenhandel.

Schweiz

Internetkriminalität nimmt zu

Freitag, 4. Mai 2012, 13:01 Uhr

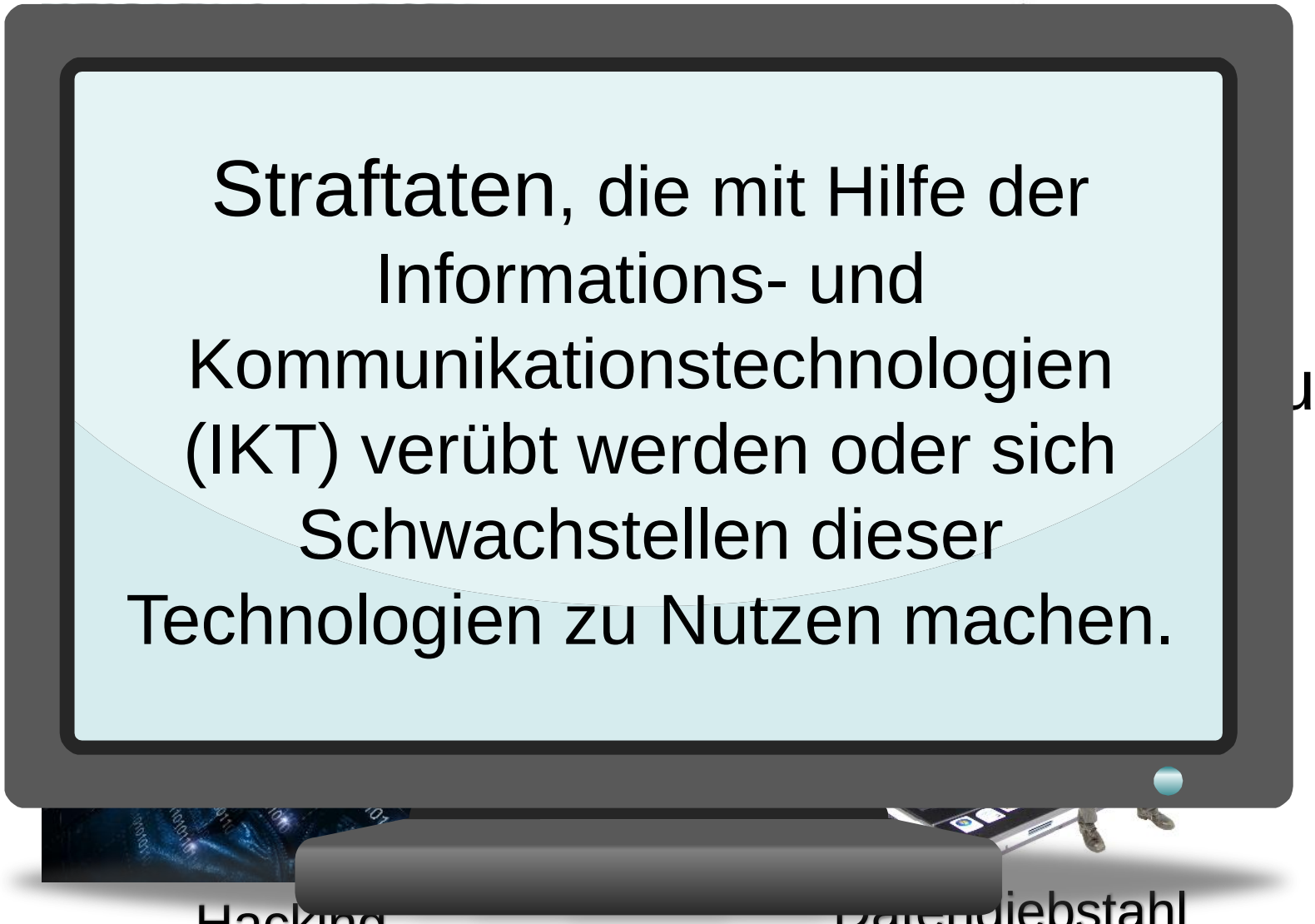
Angriffe aus dem Cyberspace werden technisch immer raffinierter. Dies stellt die Melde- und Analysestelle Informationssicherung (MELANI) des Bundes fest. Sie mahnt zur Vorsicht im Internet. Grösster Risikofaktor bleibe der Mensch.

Attacke auf IAEA: Hacker erbeuten Daten von Atombehörde

Bei der Internationalen Atomenergie-Organisation hat es offenbar eine Sicherheitspanne gegeben. Hacker konnten Informationen von einem abgeschalteten Server sichern - und stellten diese ins Internet. Dabei soll es sich vor allem um Kontaktdaten von Mitarbeitern gehandelt haben.

Cyberkriminalität im engeren Sinn

Straftaten, die mit Hilfe der Informations- und Kommunikationstechnologien (IKT) verübt werden oder sich Schwachstellen dieser Technologien zu Nutzen machen.

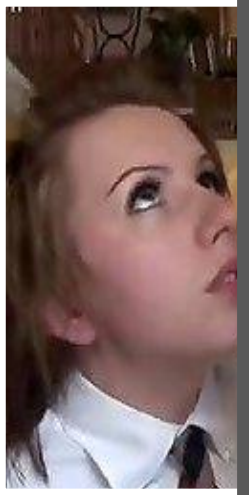


ung,

Hacking

Datendiebstahl

Cyberkriminalität im weiteren Sinn



Verbotene

Nutzt das **Internet als Kommunikationsmittel**, wobei die sich bietenden Möglichkeiten wie bspw. der E-Mail-Verkehr oder der Austausch respektive das Bereitstellen von Dateien für unlautere Zwecke missbraucht werden.

erletzungen

erbindung mit

Internet

Abgrenzungen

CYBERWAR

Einsatz von ICT in einer
kriegerischen Auseinandersetzung
zwischen Staaten

CYBER SECURITY

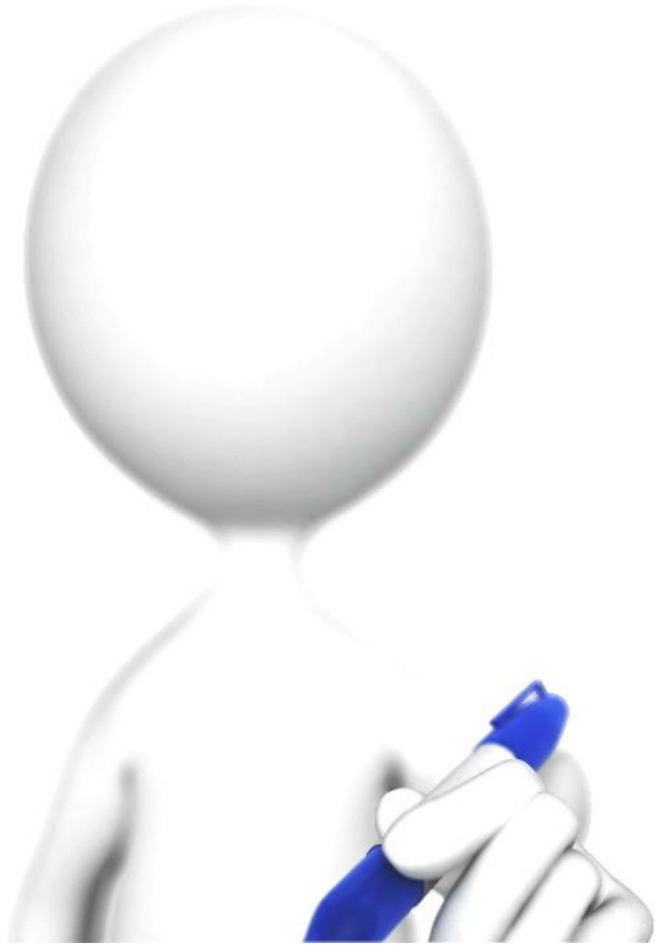
Schutz gegen
Infektionen und
Missbrauch von ICT

CYBER INTELLIGENCE

Cyber-Risiken für
die Schweiz
Erkennen


KOBIK?
KOORDINATION
ANALYSE
KANTON
BUND

Gemeinsame Koordinationsstelle des Bundes und der Kantone

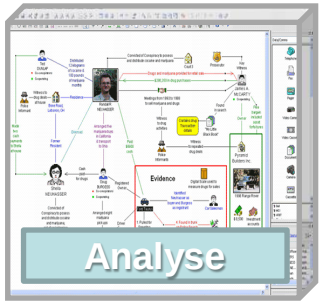


Organisation

- Technische Projekte
- Betrieb NDHS
- Blacklist
- Abklärung der Zuständigkeit
- Zusammenarbeit mit Providern

- Verdachtsunabhängige Recherche
- P2P Monitoring (öffentlich / privat)
- Verdeckte Ermittlungen

- «Operational Center»
- Kriminalpolizeilicher Infoaustausch
- Operative und strategische Kriminalanalyse
- Berichte / Newsletter / Medien



- Rechtsabklärungen
- Behandlung politischer Geschäfte
- Bürgerbriefe
- Berichte / Newsletter / Medien

10 (+6) Mitarbeiter

10 214
Bürger-
meldungen

Sexual-
delikte

58,8%
Abnahme

10,9%
Zunahme

Meldestelle

Vermögens-
delikte

66,9%
der
Meldungen

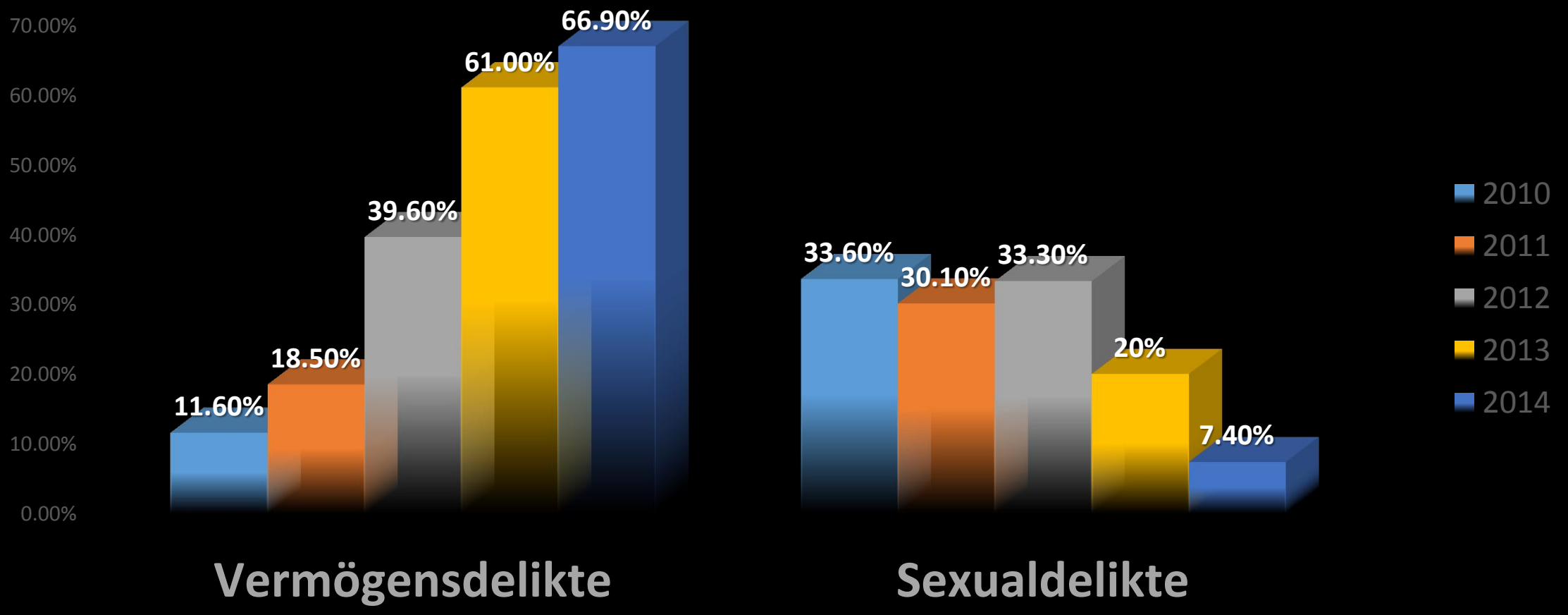
27
Warn-
meldungen

3218
persönliche
Antworten

30,4%
der
Meldungen

SCAM
Betrugsfälle

ENTWICKLUNG DES PROZENTUALEN ANTEILS DER MELDUNGEN NACH DELIKTEN



396 Anzeigen

aus aktiven Recherchen

86
P2P-Scan

27
Verdachts-unabhängige verdeckte Vorermittlungen

283
Verdeckte Ermittlungen nach StPO

Internationale Kooperation

- **FP Cyborg → IT-Crimes**

  Kriminalitätsbekämpfung und Prävention im Bereich Internet und IKT
  Straftaten: Artikel 2-8 der Cybercrime Convention

- **FP Twins → Pädokriminalität**

  Bekämpfung pädokrimineller Netzwerke im Internet
  Straftaten: Produktion, Verkauf und Vertrieb von Kinderpornografie

- **European Union Cybercrime Task Force**

  Heads of National High Tech Crime Units
  Strategisches Gremium und Beirat des EC3

- **Interpol Group of Experts on IT-Crimes**

  Informationsabgleich und Austausch von Best Practices
  Country-Reports / Workshops: eBanking, VPN/TOR und Botnets

- **Virtual Global Taskforce**

  KOBIK ist Mitglied der VGT. Der « Letter of Intent « wurde
  am 13.05.2014 in Brüssel unterzeichnet

OPERATION ONYMOUS

Behörden schließen Drogen-Plattformen im Dark Web

Europol und FBI haben auf einen Schlag zahlreiche Schwarzmarkt-Plattformen im Tor-Netzwerk stillgelegt. Wie sie das geschafft haben, wollen sie für sich behalten.

VON PATRICK BEUTH

Aktualisiert 7. November 2014 18:12 Uhr

25 Kommentare

THIS HIDDEN SITE HAS BEEN SEIZED

**as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust**

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

By salus

Was erwartet uns in naher Zukunft?

Malware

- Es ist mit einem deutlichen Anstieg von Malware-Vorfälle zu rechnen. Im Zentrum steht weiterhin das Ausspionieren von Bankdaten, Kreditkartennummern und Passwörtern.
- Sekundäre Ziele sind Adressbuchdaten zum Aufbau von Scheinidentitäten für Betrugsversuche und der Aufbau eines Botnetzes für DDoS-Attacken.
- Es ist zudem mit neuen Infektionswegen zu rechnen, beispielsweise Add-Ons für Browser oder Webapps für Social-Media Seiten. Denkbar ist zudem, dass Sicherheitslücken in Cloud-Diensten ausgenutzt werden, um Schadsoftware auf Zielrechnern zu installieren.

Social Engineering / Identitätsmissbrauch

Crime-as-a-service

Die Underground Economy bietet bereits heute kostengünstige und qualitativ hochstehende „Dienstleistungen“ (inkl. Support, SLA etc.) an.

Keine Fachkenntnisse mehr notwendig um die Vorteile der IKT kriminell zu nutzen.

Gefahren für KMUs

- Gezielte Angriffe zwecks Erpressung und Lösegeldforderungen
- Wirtschaftsspionage
- Datendiebstahl oder –sabotage
- Unfriendly Takeover des Online-Geschäfts durch Konkurrenz
- Social Engineering
- .....

Konsequenzen für KMU’s

- Datensicherheit und der Schutz vor Internetkriminalität ist für jedes Unternehmen (egal wie klein) von steigender Wichtigkeit.
- Vorfälle nicht verheimlichen, sondern Anzeige bei Polizei oder KOBIK erstatten.
- Die Thematik gemeinsam angehen und Wissen teilen (Beispiel: BitKom in Deutschland)

- Die Zusammenarbeit zwischen privaten und öffentlichen Institutionen (Public-Private-Partnership) zur Bekämpfung der Internetkriminalität wird eine immer wichtigere Rolle einnehmen.

Vielen Dank für Ihre Aufmerksamkeit!

www.cybercrime.ch

Folgen Sie uns auf Facebook

www.facebook.com/cybercrime.ch

Folgen Sie uns auf Twitter

@KOBIK_Schweiz