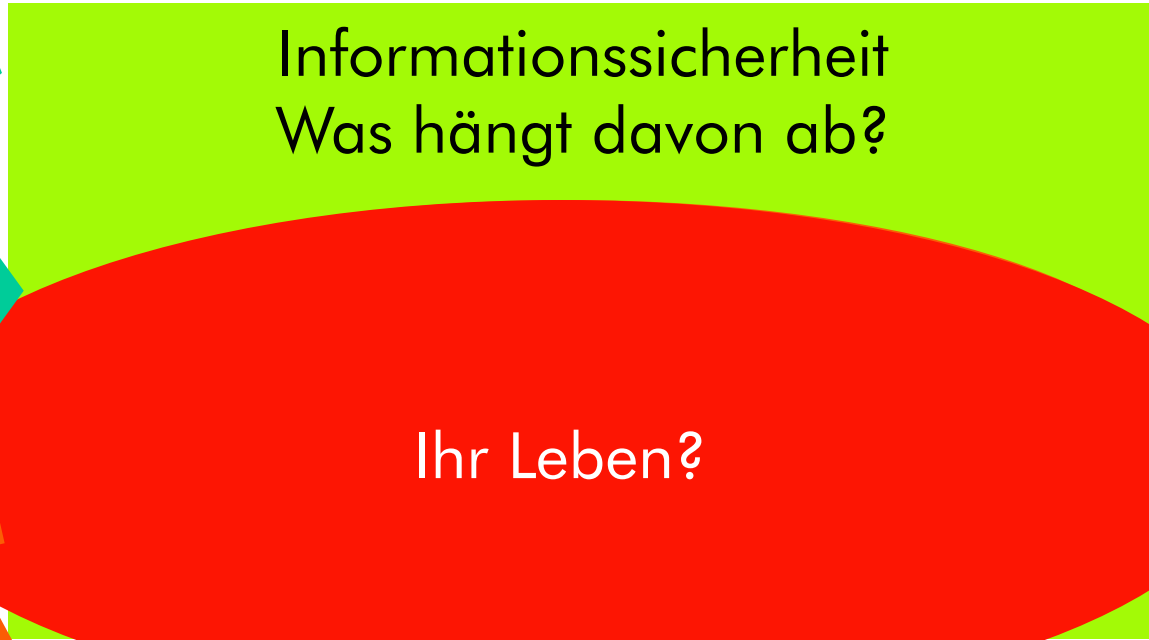
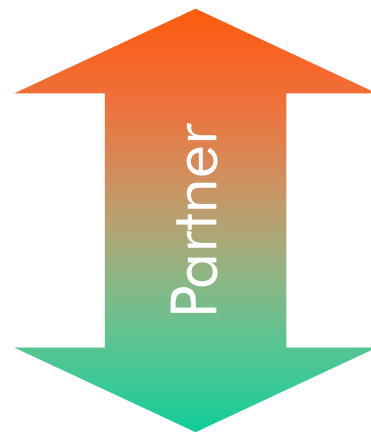


Risikomanagement bzgl. Sicherheit und Datenschutz

SPOL Social Event 2009
Dr. Marcus Holthaus, IMSEC,
Geschäftsführer

Faktoren und Prioritäten



Schlagzeilen

16.03.2009

<http://www.csoonline.com/article/print/484418>



From: www.csoonline.com

Researchers Sniff Keystrokes from Thin Air

by Robert McMillan, IDG News Service

March 13, 2009

SAN FRANCISCO (03/12/2009) - That PC keyboard you're using may be giving away your passwords. Researchers say they've discovered new ways to read what you're typing by aiming a special wireless or laser equipment at the keyboard or by simply plugging into a nearby electrical socket.

Two separate research teams, from the Ecole Polytechnique Federale de Lausanne and security consultancy Inverse Path, have taken a close look at the electromagnetic radiation that is generated every time a computer keyboard is tapped. It turns out that this keystroke radiation is actually pretty easy to capture and decode -- if you're a computer hacker-type, that is.

11.03.2009

<http://www.heise.de/newsticker/Norton-unter-PIFTS-Verdacht-/meldung/134358>

#1



[heise online](#) > [News](#) > [2009](#) > [KW 11](#) > [Norton unter PIFTS-Verdacht](#)

11.03.2009 10:13

Norton unter PIFTS-Verdacht

Am gestrigen Dienstag kursierten Beschwerden über Alarmmeldungen zu einer mysteriösen Datei namens PIFTS.exe im Netz, die offenbar im Zusammenhang mit Symantec Norton stand; parallel dazu sperrte **Symantec** [<http://www.symantec.com>] Foren-Einträge. Das führte zu Verunsicherung und teilweise haarsträubenden Verschwörungstheorien. Alles ein Missverständnis, das auf einem kleinen Fehler beruht, beruhigt nun der Antiviren-Hersteller.

Top Ten Web Hacking Techniques of 2008!

1. [GIFAR](#)

(Billy Rios, Nathan McFeters, Rob Carter, and John Heasman)

2. [Breaking Google Gears' Cross-Origin Communication Model](#)

(Yair Amit)

3. [Safari Carpet Bomb](#)

(Nitesh Dhanjani)

4. [Clickjacking / Videojacking](#)

(Jeremiah Grossman and Robert Hansen)

Schlagzeilen

09.03.2009

<http://www.heise.de/netze/news/meldung/print/134169>

#



News-Meldung vom 07.03.2009 16:23

BND benutzt Online-Durchsuchung zur Spionage

Der Bundesnachrichtendienst (**BND[1]**) hat offenbar in großem Umfang die Online-Durchsuchung zur Spionage benutzt und damit geheime Daten abgefangen, wie das Nachrichtenmagazin *Der Spiegel* in der kommenden Ausgabe 11/2009 unter Berufung auf BND-interne Quellen berichtet. In den vergangenen Jahren seien in mindestens 2500 Fällen Computer im Ausland infiltriert und Festplatteninhalte nach Pullach übermittelt worden. In weiteren Operationen installierten die BND-Mitarbeiter Keylogger, mit denen sie Tastatureingaben und damit Passwörter zum Beispiel für E-Mailfächer abgriffen.

16.03.2009

<http://www.networkworld.com/cgi-bin/ma...ks-change-security.html&site=printpage>

#1

Sponsored by:

NETWORKWORLD

This story appeared on Network World at

<http://www.networkworld.com/news/2009/031309-foreign-web-attacks-change-security.html>

Foreign Web attacks change security paradigm

By Fred O'connor , IDG News Service , 03/13/2009

Traditional security systems may be ineffective and become obsolete in warding off Web attacks launched by countries, according to Val Smith, founder of Attack Research. New attack trends include blog spam and SQL injections from Russia and China, Smith said during his talk at the Source Boston Security Showcase on Friday.

Sponsored by:



"Client-side attacks are where the paradigm is going," Smith said. "Monolithic security systems no longer work."

Schlagzeilen

11.03.2009

<http://www.networkworld.com/cgi-bin/ma...-theft-trojans-are.html&site=printpage>

#1

Sponsored by:

NETWORKWORLD

This story appeared on Network World at

<http://www.networkworld.com/news/2009/030909-panda-id-theft-trojans-are.html>

Panda: ID theft Trojans are on 1 in 100 PCs we scan

By [Robert McMillan](#) , IDG News Service , 03/09/2009

Perhaps as many as ten million PCs are infected with sneaky programs designed to steal sensitive financial information, antivirus vendor Panda Security reports. Sponsored by:

The company found that just over one percent of the 67 million people who tried out its free [ActiveScan](#) test site last year were infected with malicious software designed to help thieves steal sensitive information about victims. If one percent of the world's 1 billion computers are infected, that would mean that this kind of software is on 10 million PCs worldwide

03.03.2009

<http://images.zeit.de/text/2009/10/C-Netzkriminalitaet>

#1

DIE ZEIT, 26.02.2009 Nr. 10 [<http://www.zeit.de/2009/10/C-Netzkriminalitaet>]

Computerkriminalität

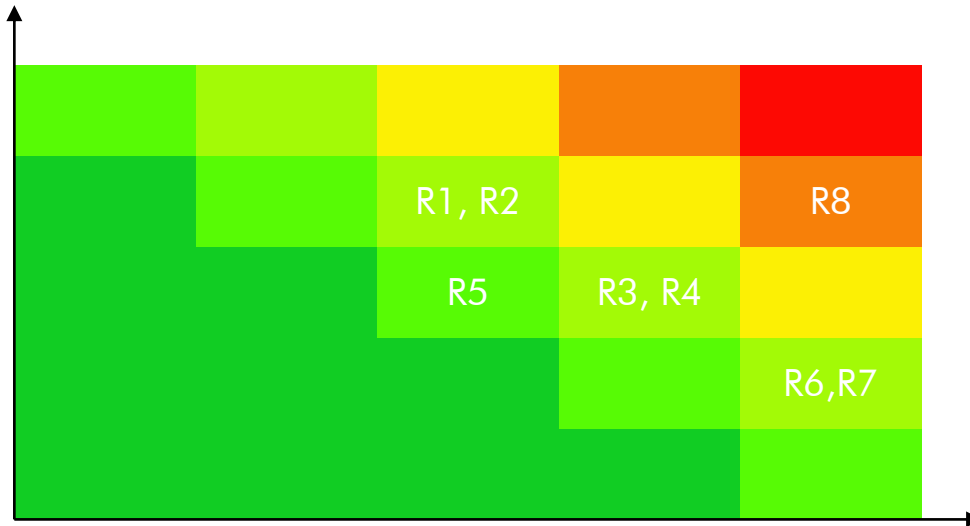
Ihr Rechner ist besetzt!

Von *Lars Reppesgaard*

Cyberkriminelle kapern fremde Computer und schließen sie zusammen. Über diese Schattennetze versenden sie Spam-Mails, manipulieren Internetseiten und plündern Bankkonten

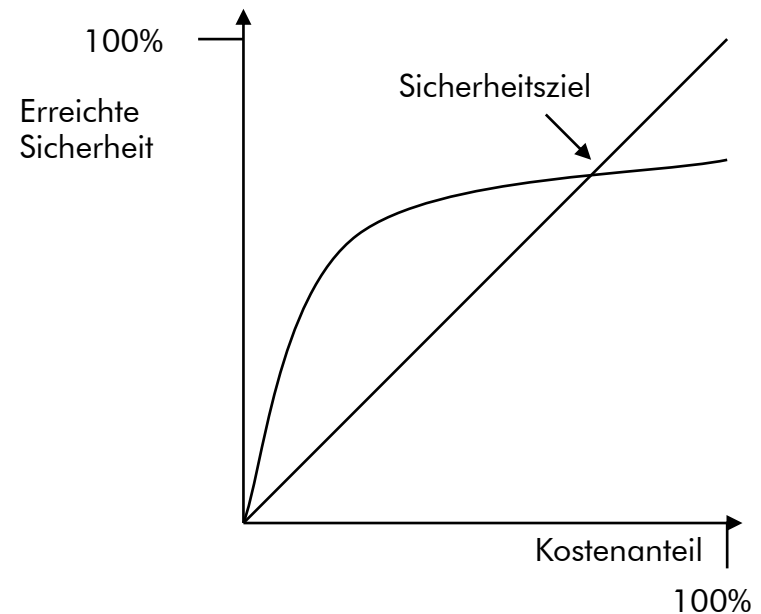
Das Wochenende im Januar, an dem der Computerwurm zuschlug, war für Rainer Harpf, den Chief Information Officer der Kärntner Landeskrankenanstalten (Kabeg), ein Albtraum. Blitzschnell hatte der Schädling, den Sicherheitsfachleute Conficker getauft haben, am Samstagmorgen seine Arbeit aufgenommen, nachdem er irgendwo auf einen Rechner des Klinikverbunds geschlüpft war. Das Hackerprogramm sammelte die Passwörter, die auf dem Rechner zu finden waren, es kopierte Daten und versuchte, all diese Informationen an eine Adresse im Internet zu schicken. Conficker infizierte alle Computer, die er über das Netzwerk des Krankenhauses erreichen konnte. »In unsere medizinischen Systeme, in denen die Patienteninformationen und Röntgenbilder abgelegt sind, konnte der Wurm nicht eindringen«, sagt Harpf. »Aber er hat all unsere Computerarbeitsplätze lahmgelegt.«

Formelle Betrachtungen

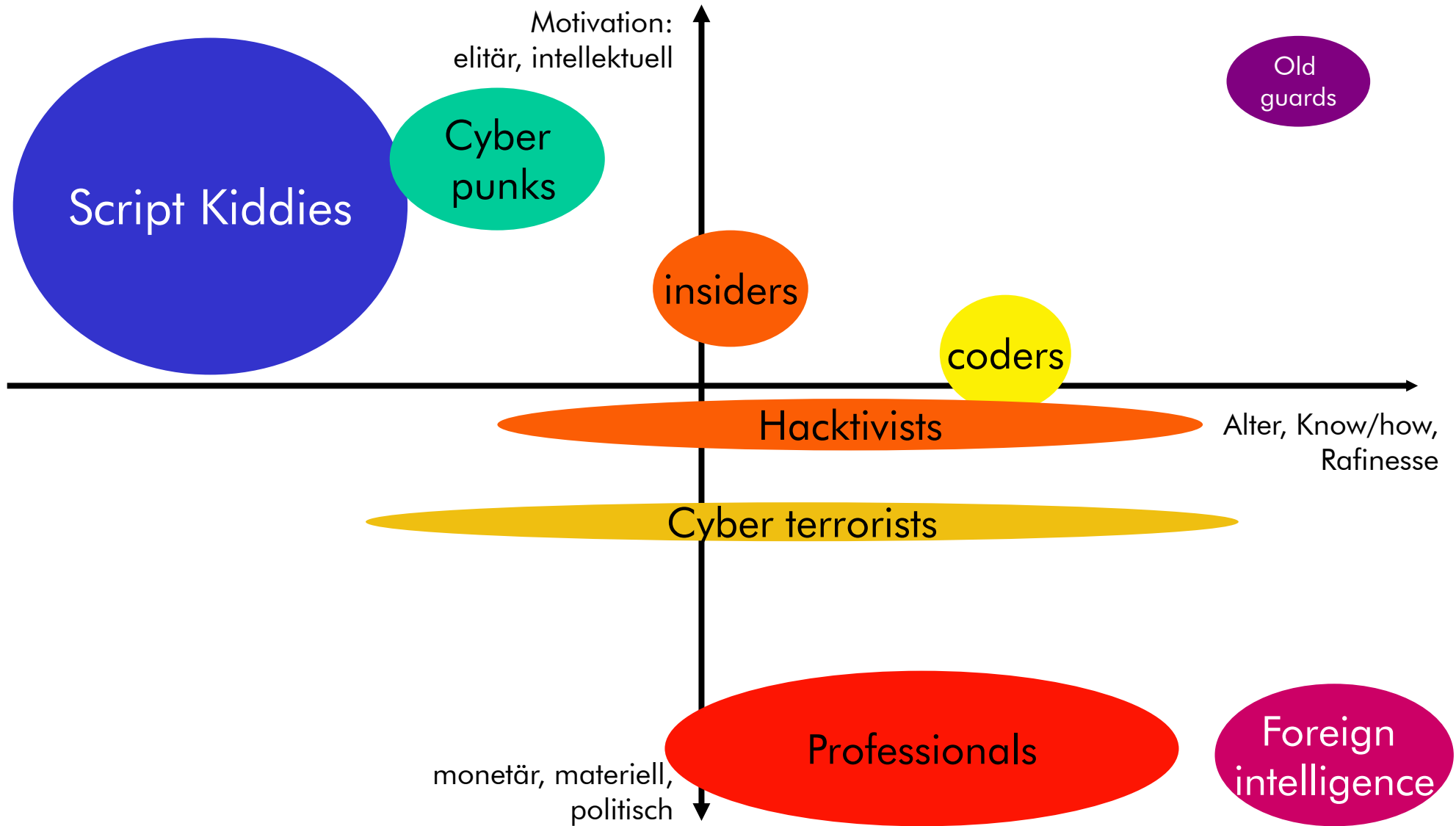


- Formelle Risikoanalysen als Hilfsmittel
 - Gute Übersicht, Eignung als Entscheidungsgrundlage
- Aber:
 - Starke Fluktuation
 - Vielfältige Einflüsse und Kombinationen von Risiken
 - Weitestgehend unbekannte Schadenshöhen und Wahrscheinlichkeiten

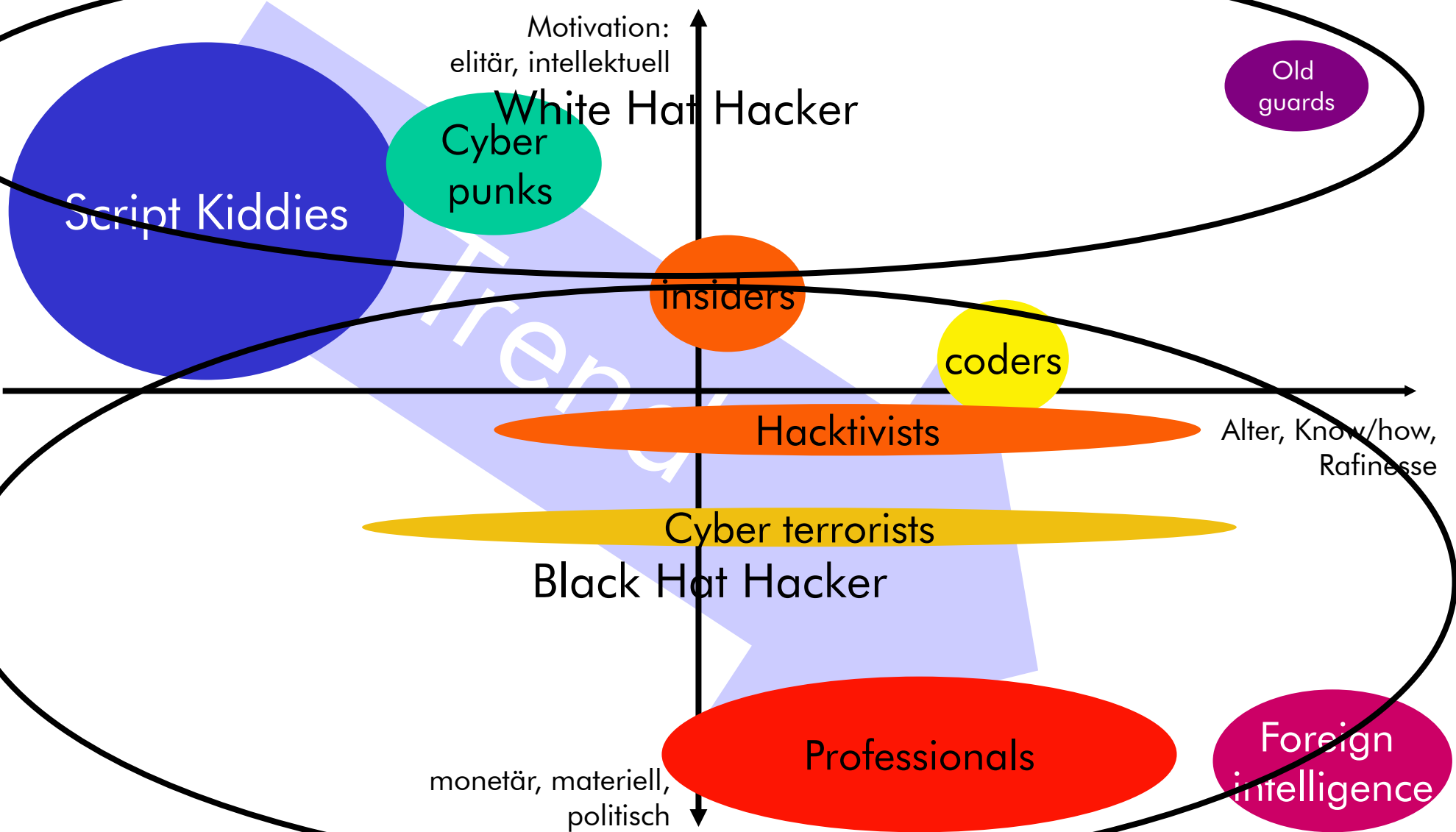
- ROSI als Hilfsmittel
 - Formelle Begründbarkeit von Massnahmen
- Aber:
 - Qualität der Theorie
 - Messbarkeit
 - Korrelation mit verändernden Ansprüchen



"Hacker-Taxonomie"



"Hacker-Taxonomie"



Betriebsrisiken entstehen in Projekten



Was tun?

In Projekten

- Vermeidung der Monokulturen
- Anforderungen der Kunden berücksichtigen
 - Privatsphäre und Datenschutz
 - Nutzungsmodelle: Wer braucht was wann?
- Sicherheitsabnahme und Revisionen
 - Konsequent, häufige, detailliert
 - Whitebox Tests
- Source Code Hinterlegung und Rekompilation
- Legale Risiken
 - Vermischung von Lizenzmodellen
 - Einhaltung von Verarbeitungsrichtlinien
- Harte Vorgaben für den Betrieb
 - Klassifikationsmodell für die Sicherheitsleistungen
 - Sicherheitsqualifikation der Mitarbeiter
- Planung für
 - Notfalltrennung
 - Offline-Betrieb

Im Betrieb

- Aufbau / Ergänzung ISMS nach ISO 27000
- Sicherheitsarchitekturen und –politiken zu
 - Gesamtarchitektur
 - Qualität der Software-Entwicklung
 - Kooperationen und Datenweitergaben
 - Datenverarbeitung
 - Etc.
- Eigene Exponierung reduzieren
 - Daten löschen!
 - Verarbeitung auslagern
- Verbände bilden, Task Forces
- Frühwarnung ausbauen, eigene Systeme beobachten und alarmieren
- Security Patches schnell anwenden
- Notfallvorsorge
 - Szenario Internet-Ausfall
 - Szenario Massiver Angriff

Was tun?

In Projekten

- Vermeidung der Monokulturen
- Anforderungen der Kunden berücksichtigen
 - Privatsphäre und Datenschutz
 - Nutzungsmodelle: Wer hat Zugriff?
- Sicherheitsabnahme um 27000
 - Konsequent, hören
 - Whitebox Test
- Source Code Review
 - Reduzieren
- Incident Response
 - Übung auslagern
 - Teams bilden, Task Forces
- Hardware
 - Alarm ausbauen, eigene Systeme beobachten und alarmieren
 - Security Patches schnell anwenden
- Notfallvorsorge
 - Szenario Internet-Ausfall
 - Szenario Massiver Angriff
- Planung
 - Notfall
 - Offline

**ISO 27000
umsetzen und
Zertifizierung
durchführen**