



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung

Neue Risiken in der Informations- und Kommunikationstechnologie für Firmen und Märkte im 21. Jahrhundert

Dr. Ruedi Rytz
13. Mai 2011



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung

Problemstellung



Kritische Infrastrukturen

Systeme, die für das **Funktionieren der Gesellschaft kritisch** sind:

- Energieversorgung
- Telekommunikation
- Transport und Logistik
- Finanz- und Versicherungswesen
- Notfall- und Rettungswesen
- Gesundheitswesen (inkl. Wasserversorgung)
- Regierung und öffentliche Verwaltungen



Im **Informationszeitalter** hängen diese zunehmend von den **IKT**, d.h. auch vom **Internet** ab.





Davis-Besse Kernkraftwerk, Ohio, U.S.A



- Am 25. Januar 2003 dringt der **Slammer-Wurm** ins **LAN** des **KKW** ein.
- **Sicherheitsüberwachungssystem fällt** für 5 Stunden **aus**.



Wasserversorgung von Maroochy Shire in Queensland, Australien



- Im Jahr 2000 **hackt sich** ein Ex-Angestellter 46mal in die **Wasserversorgung**.
- Er **lässt Millionen Liter Abwasser** in Parks, Flüsse und die Anlage eines Erstklasshotels **ausfließen**.



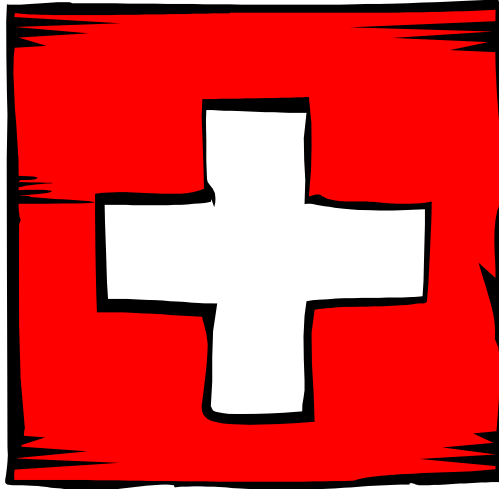
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung

Lösungsansatz



Partnerschaft zwischen Wirtschaft und Verwaltung

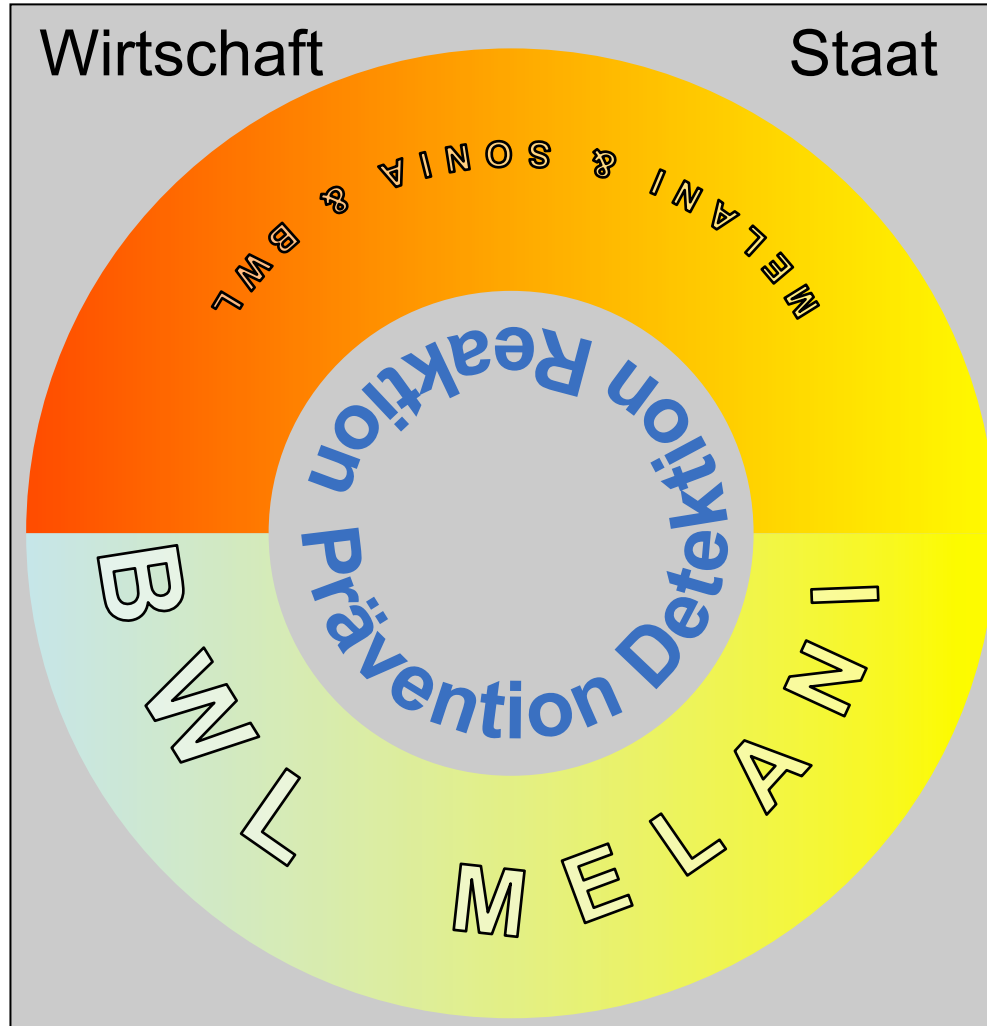


- Staatsaufgabe: Artikel 2, Absatz 2 der Bundesverfassung „[...] die gemeinsame Wohlfahrt“
 - Artikel 102 „Landesversorgung“

 - Kritische Infrastrukturen sind heute zum grossen Teil von der Privatwirtschaft betrieben
- Mitverantwortung (gewichtiger) Vertreter aus der Wirtschaft



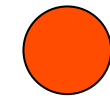
CH-System zum Schutz der IKT-Infrastrukturen



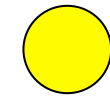
BWL: Bundesamt für wirtschaftliche Landesversorgung

MELANI: Melde- und Analysestelle Informationssicherung

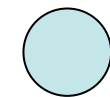
SONIA: Sonderstab Informationssicherung



Krise



Einzelne Vorfälle



Langfristige Massnahmen

Prävention: Strategisches Krisenmanagement

Detektion/Reaktion: Operatives Krisenmanagement



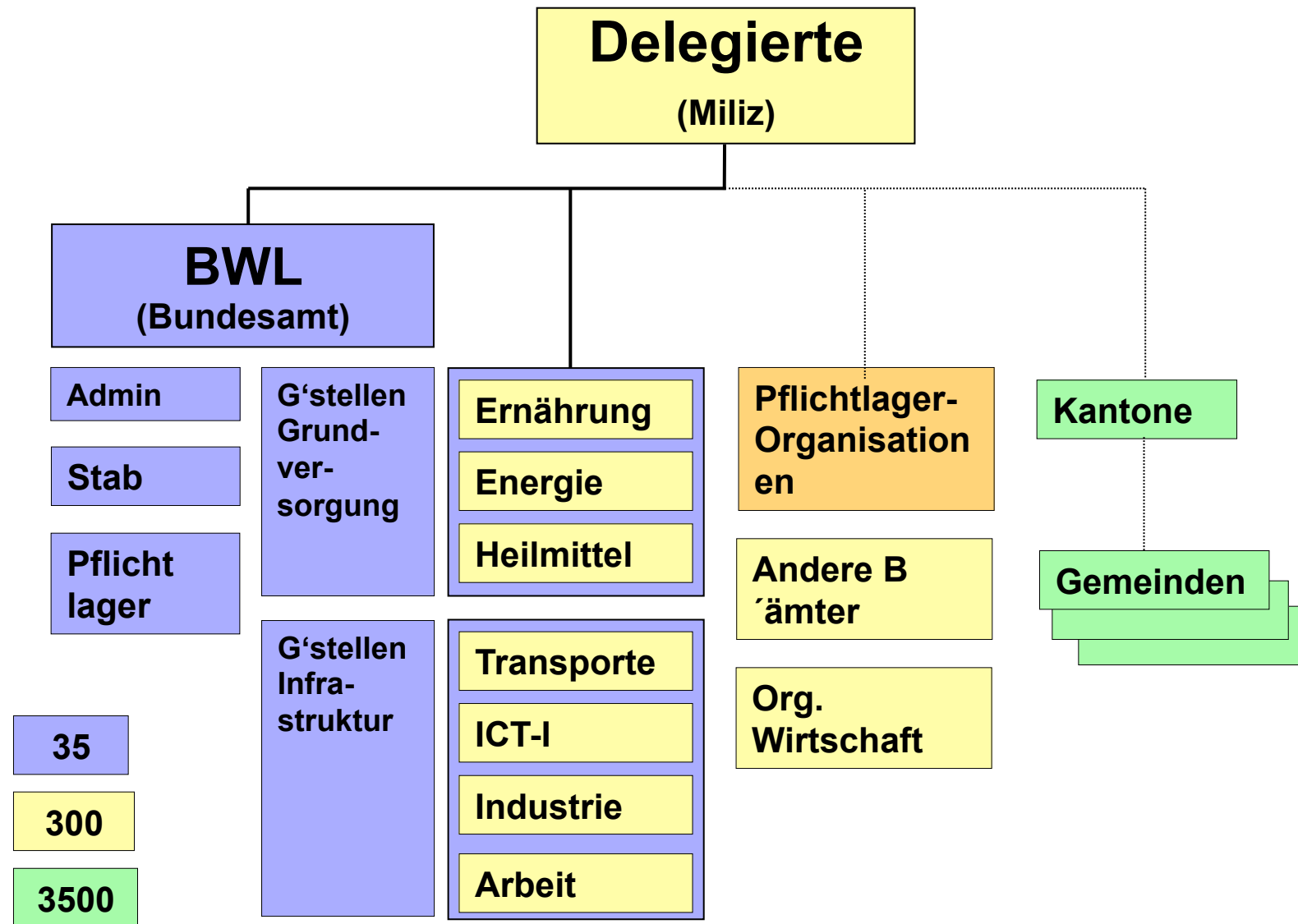
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung

Prävention / Vorsorge



Organisation der WL





Vorsorge durch den WL-Bereich ICT-I





Lösungsbeispiel im Finanzsektor

Massnahmen aus der IKT-Verwundbarkeitsanalyse wurden autonom auf der Basis von BCM-Empfehlungen der Bankiervereinigung umgesetzt. Kernelemente von der finma verbindlich erklärt.

SwissBanking

November 2007
Recommendations for
Business Continuity Management (BCM)

➔



Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Rundschreiben 2008/10
Selbstregulierung als Mindeststandard

Von der Eidg. Finanzmarktaufsicht
als Mindeststandard anerkannte
Selbstregulierung

Referenz: FINMA-RS 08/10 Selbstregulierung als Mindeststandard
Erläss: 20. November 2008
Inkraftsetzung: 1. Januar 2009
Letzte Änderung: 20. November 2008
Konkordanz: vormalis EBK-RS 04/2 Selbstregulierung als Mindeststandard vom 21. April 2004
Rechtliche Grundlagen: FINMAG Art. 7 Abs. 1 Bst. a und Abs. 3
Anhang: Von der FINMA anerkannte Selbstregulierung

		Adressaten							
		BankG	VAG	BEHG	KAG			GwG	Andere
Banken	Finanzgruppen und -kongl.								
x	Andere Intermediäre								
	Versicherer								
	Vers.-Gruppen und -kongl.								
	Vermittler								
	Börsen und Teilnehmer								
	Erfolgsanwärter								
	Fondsstellungen								
	SCAV								
	KVG für KVA								
	SCAF								
	Depotbanken								
	Verwalter von KVA								
	Vermittler								
	Vers. oder ass. KVA								
	Andere Intermediäre								
	SRG								
	DUF								
	SRG-Bewilligte								
	Prüfungsinstitutionen								
	Ratingagenturen								



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung

Detektion / Reaktion



Melde- und Analysestelle Informationssicherung MELANI

- Lage- und Nachrichtenzentrum des Bundes für den **Schutz der kritischen Informationsinfrastrukturen**
- Stellt den **Betreibern** dieser Infrastrukturen (z.B. Energieversorgern, Banken, usw.)

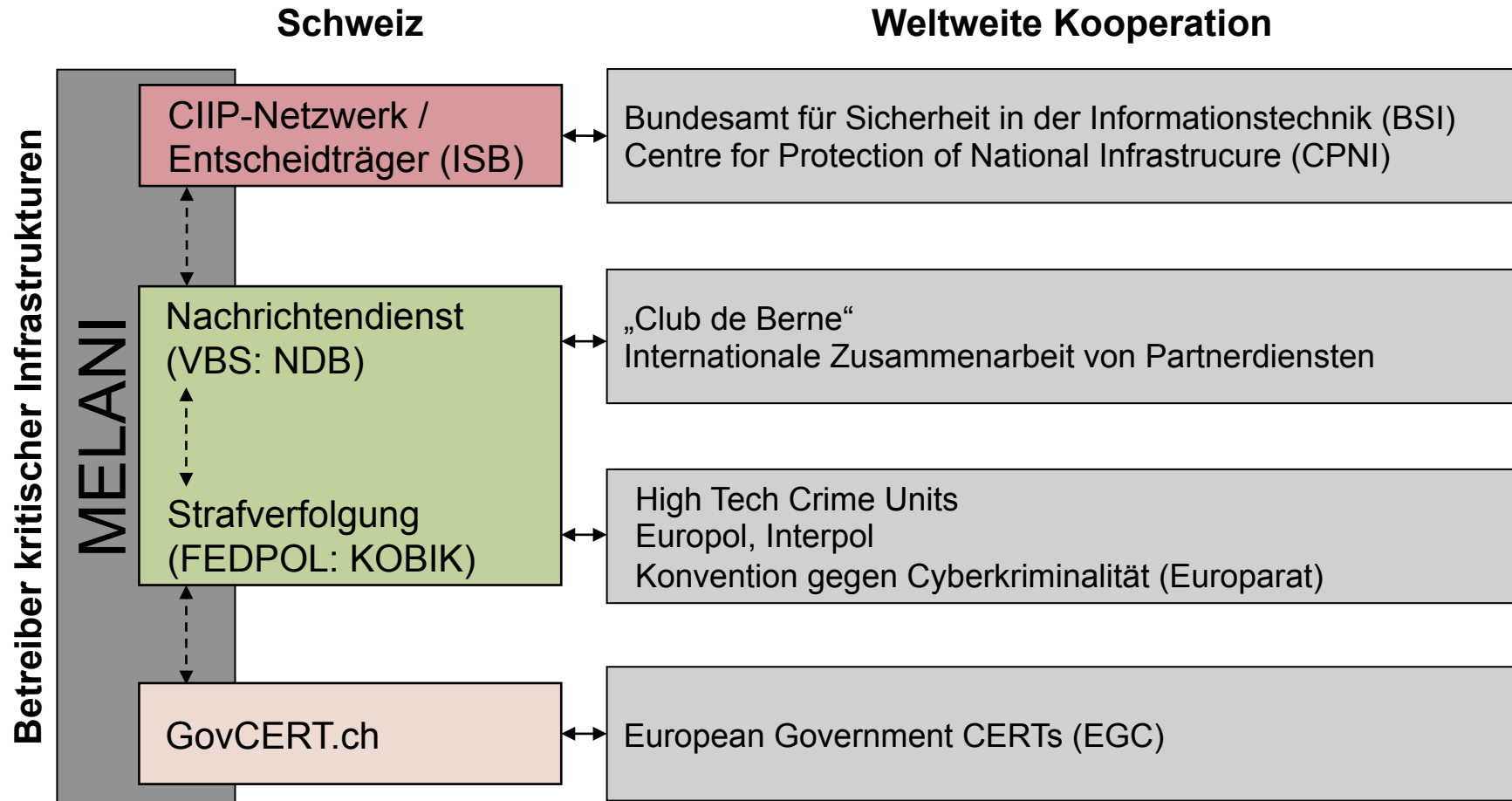
subsidiär Wissen und Mittel aus Quellen

- des **Nachrichtendienstes** → Nachrichtendienst des Bundes
- der **Strafverfolgungsbehörden** → Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK
- der **nationalen** Computer Emergency Response Teams **CERTs**

zur Verfügung.



Das notwendige Netzwerk





MELANI im Internet / Lageberichte

The screenshot shows two overlapping windows. The background window is Microsoft Internet Explorer displaying the MELANI website (http://www.melani.admin.ch). The website header includes the Swiss flag and the text 'Schweizerische Eidgenossenschaft', 'Confédération suisse', 'Confederazione Svizzera', and 'Confederaziun svizra'. Below the header are navigation links: 'Startseite', 'Gefahren im Internet', 'Dokumentation', 'Dienstleistungen', and 'Über MELANI'. The main content area is titled 'Melde- und Analysestelle Informat...' and contains introductory text about the MELANI reporting and analysis center. There are three small images with links: 'Informationen über Gefahren im Internet', 'Lageberichte', and 'Meldeformular'. The foreground window is Adobe Acrobat Professional displaying a PDF document titled 'Informationssicherung - Lage in der Schweiz und international - Halbjahresbericht 2006/II (Juli – Dezember)'. The PDF content features a large, colorful illustration of a person sitting at a desk with a computer, surrounded by various threats like a red devil, a green worm, a yellow lightning bolt, and a red dragon. At the bottom of the PDF, it says 'In Zusammenarbeit mit: KOBIK - Koordinationsstelle zur Bekämpfung der Internetkriminalität' and 'Service de coordination de la lutte contre la criminalité sur Internet'.

Siehe: <http://www.melani.admin.ch/dokumentation>



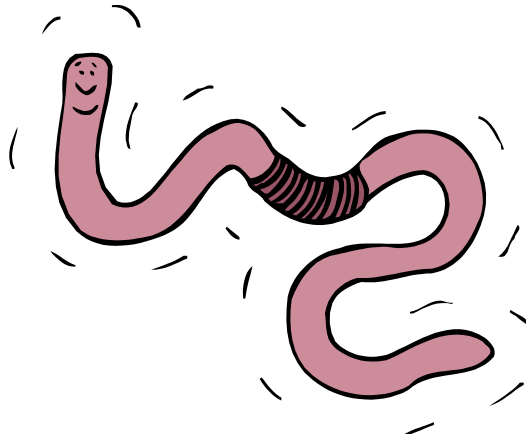
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung

Lektionen aus 20 Jahren Internet



Der Morris Computerwurm 1988 (als alles anfang)



- **Definition:** Computerprogramm, das sich über ein Computernetzwerk verbreitet.
- Robert Morris Jr. programmiert **1988 den ersten Wurm** für das Internet.
- Der Wurm befahl ca. 6000 Rechner (~10% des damaligen Internets).
- Wegen eines Programmierfehlers wurden weite Teile des Netzes (sowie die betroffenen Rechner) lahm gelegt.
- **Keine Auswirkungen auf kritische Infrastrukturen und Unternehmen.**



CSX Eisenbahngesellschaft, Ostküste U.S.A.



- Im August 2003 dringt der **Blaster-Wurm** in das Netzwerk von CSX ein
- Systeme zur Abfertigung des Güterumschlags sowie der **Verkehrs-Signalisation betroffen**
- **Unterbrechung von Zugverbindungen**, inkl. Pendlerverkehr in Washington D.C. für mehrere Stunden



Lektion 1

- Sicherheitslücken werden früher oder später ausgenutzt.
- **Motivation:** Intellektuelle Herausforderung und Anerkennung in der „Szene“
- Schäden entstehen (fast) immer – selbst wenn diese nicht beabsichtigt sind (→ „Murphy’s Law“).
- **Je ähnlicher** die eingesetzten **Technologien** (Entwicklung von 1988 – 2003), **desto wahrscheinlicher** sind **Kolateralschäden für kritische Infrastrukturen** (Energieversorgung, Transport, ...).

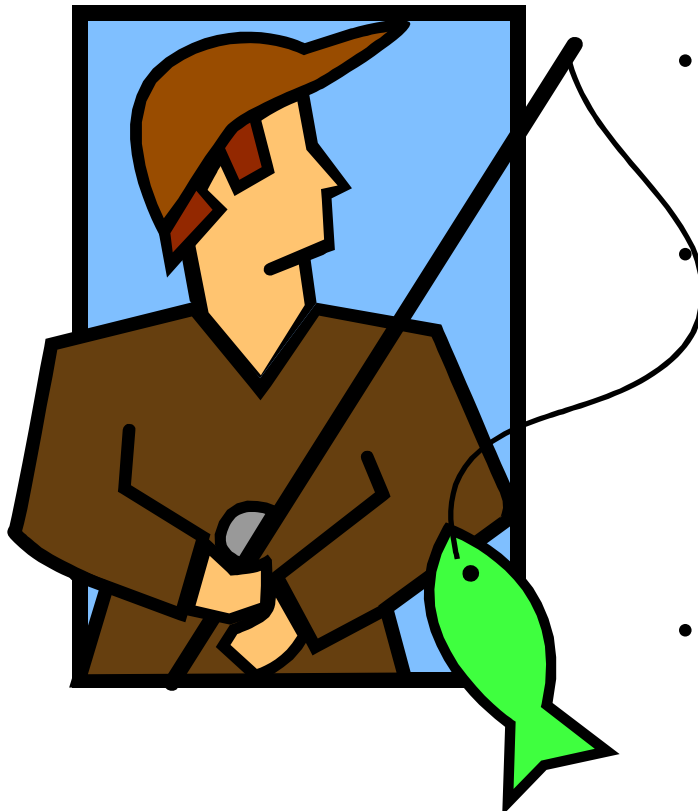


Neue Ausrichtung der „Internet-Unterwelt“

- **2003** erreichte die Verbreitung von Computerwürmern ihren Höhepunkt. **Ein Grund zur Entwarnung?**
- Im Gegenteil: Die **Programmierer** von Schadsoftware („Hacker“) **haben gelernt, ihr Wissen zu Geld zu machen.**
- Die (organisierte) **Kriminalität hält Einzug** im Internet. Sie funktioniert als Auftraggeber.
- Damit existiert ein **lukrativer Arbeitsmarkt für Hacker**, welche (über das Internet) **international zusammenarbeiten.**
- Zunehmend sind auch **staatliche Akteure** (z.B. Nachrichtendienste) mit entsprechend grossen Ressourcen im Internet **aktiv** → Industrie- und Wirtschaftsspionage.



Phishing – so überfällt man Bank(kund)en über das Internet



- **Password, Harvesting & Fishing** (oder vom „Internet-Slang“: f → ph)
- **Phisher** versuchen die Gutgläubigkeit der Leute auszunutzen, um unter anderem an **Zugangsdaten** für das Internet-Banking **zu kommen**.
- Die Daten werden dann benutzt, um **betrügerische Geldüberweisungen** zu tätigen.



Phishing früher – Geld-Diebstahl per eMail

The screenshot shows an email interface with a blue header bar that reads "Für alle Postbank Kunden". Below the header is a menu with options like "Datei", "Bearbeiten", "Ansicht", "Extras", and "Nachricht". A toolbar contains icons for "Antworten", "Allen antw.", "Löschen", "Zurück", "Weiter", and "Adressen". The email header shows "Von: missbrauch@postbank.de", "Datum: Dienstag, 27. Juni 2006 18:20", "An:", and "Betreff: Für alle Postbank Kunden". A magnifying glass icon is positioned over the sender's email address, with a circled "1" next to it. The main body of the email features the Postbank logo and a message in German: "Sehr geehrte Nutzern der Postbank Online-Banking. wir freuen uns Ihnen mitteilen zu dürfen, dass Postbank Online Banking jetzt viel sicherer ist! Weltweit gilt das nummerierte TAN-Verfahren als eines der sichersten Legitimations-Verfahren für Online-Banking und Konten von unseren Kunden bekannt. r neue Schutzmassnahmen entschieden. Um diese Massnahmen einführen zu können, müssen sie 20 iTans aus ihrer aktuellen Tan-liste eingeben. Folgen sie bitte diesen Link, um Ihr Konto bei der Postbank zu authentifizieren - <https://mirror.postbank.de/tan/verification/welcome.do> Wir danken für Ihr Verständnis. Ihre Postbank Achtung! Alle Postbankkonten innerhalb eines Tages authentifiziert werden, sonst gesperrt!" A magnifying glass icon is positioned over the URL, with a circled "2" next to it. At the bottom of the email, there is a footer that reads "© 2006 Deutsche Postbank AG". A circled "3" is placed next to the footer. A large text overlay on the right side of the screenshot reads "Achtung: [...]konten ... werden gesperrt!".

1. In Sicherheit wiegen
2. „Einfache“ Lösung aufzeigen
3. Druck ausüben

Achtung: [...]konten ... werden gesperrt!



Phishing heute – Geld-Diebstahl per Schadsoftware (Malware)

1. Spam eMail mit Anhang;
2. Installation der Schadsoftware durch Anklicken des Anhangs;
3. Schadsoftware klinkt sich in den **Web-Browser** (z.B. Internet Explorer) ein;
4. nach der Anmeldung an der eBanking-Seite bricht die Verbindung ab, respektive wird sehr langsam und
5. das Geld wird vom Konto des Opfers in Echtzeit auf ein anderes Konto transferiert.



Lektion 2

- Neu: Interessant ist, was Geld bringt.
- Die **Banken investieren viel in die IKT-Sicherheit** und werden trotzdem **erfolgreich angegriffen**.
- Die **Angreifer arbeiten** zusammen (→ Arbeitsteilung), **spezialisieren** sich und **lernen** schnell (→ Professionalität).
- Die **(organisierte) Kriminalität** nutzt die neue Geldquelle.



Spionage – das „klassische“ Verfahren

- **Wissen verschaffen** („Footprinting“)
 - Informationen (Namen, Telefonnummern, usw.) über die Mitarbeiter der Firma beschaffen
- **Social Engineering**
 - Mit diesen Informationen und unter einem Vorwand, Zutritt ins Firmengebäude erlangen
 - Gutgläubigkeit und Hilfsbereitschaft von Mitarbeitern ausnutzen, um an wertvolle Dokumente zu gelangen
- **Abtransport des Wissens**
 - Gebäude mit den gestohlenen Unterlagen verlassen

→ **Beispiel: Der Mann mit dem Drucker**



Spionage: Trojanisches Pferd



- **Definition:** Anscheinend nützliches Programm, das **versteckte Funktionen** enthält.
- Solche Funktionen können zur **Spionage**, Fernsteuerung des PC, Versenden von Spam, usw. genutzt werden.
- Trojanische Pferde gelangen zum Beispiel durch
 - „freiwilliges“ Installieren und
 - Ausnutzen von Sicherheitslücken auf den Computer.

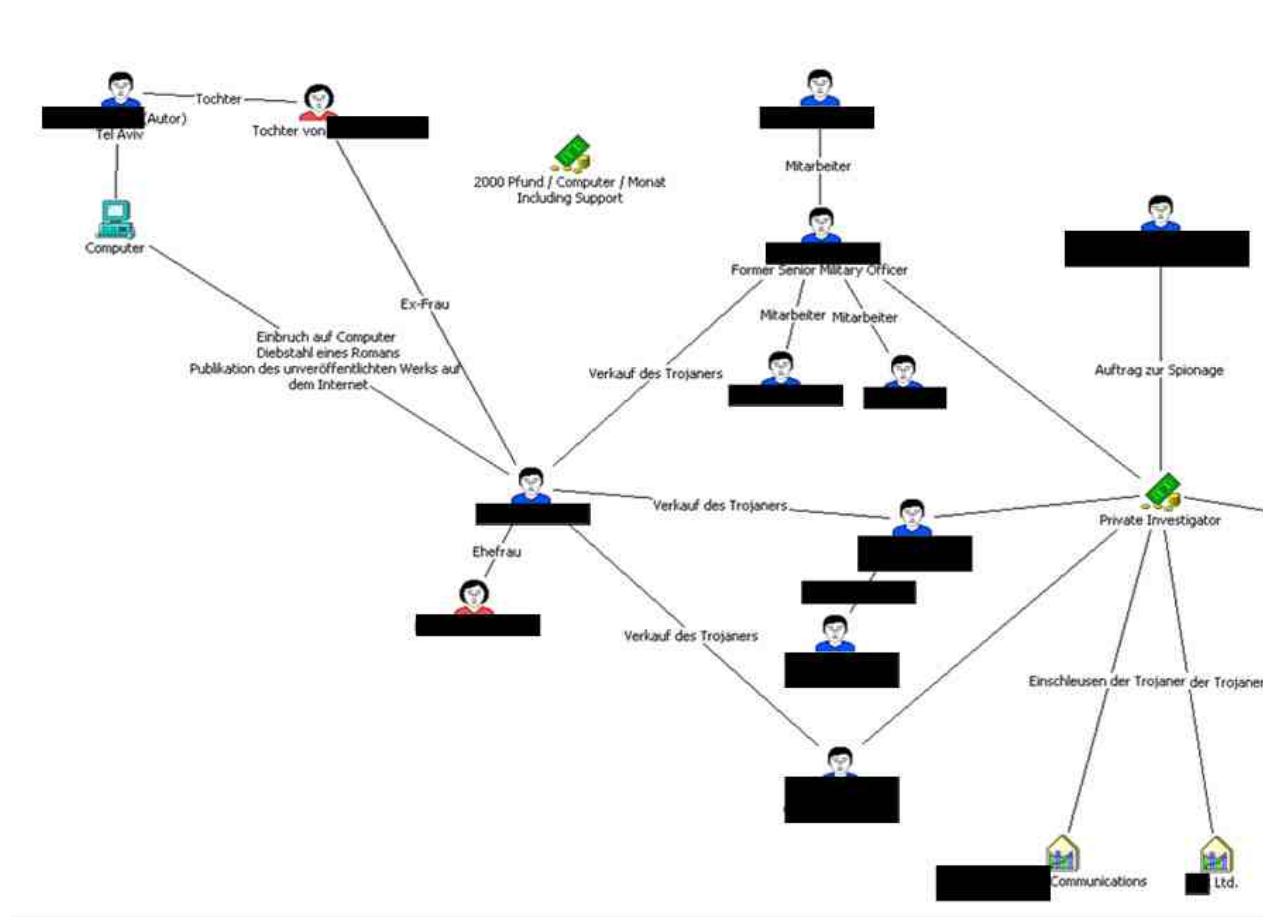


Fallbeispiel: Spionage – Privatdetektei ^{1/2}

- **2005: Spionage mit einem Trojanischen Pferd** in Israel.
- **Faktenlage:**
 - Zwei israelische Staatsbürger wurden als Programmierer und Vertreiber des Trojaners verhaftet.
 - Weiter wurden 7 CEOs und CSOs israelischer Firmen unter dem Verdacht der Spionage verhaftet.
 - Die Trojaner deponierten die gestohlenen Daten auf verschiedenen Rechnern in den USA, Deutschland und Israel.
 - Involviert sind Interpol, British Police (NHTCU), Bundeskriminalamt (BKA) sowie die israelische Polizei.
- **Abklärung ergibt: Der Bezug zur Schweiz beschränkt sich auf einen Scheidungsfall** ohne weitere Implikationen für die kritischen Infrastrukturen.



Fallbeispiel: Spionage – Privatdetektei 2/2





Spionage gegen Verwaltungen – seco (2007) ^{1/2}



Sehr geehrter Herr Max Muster !

Im Rahmen unseres [Programms zur Foerderung des Inlandtourismus](#) wurde ein Amateurfotowettbewerb unter eidgenössischen **Zivilbeamten** durchgeführt. Ziel war ein solches auszuwählen das moeglichst umfassend das Gesamtbild der Naturschoenheiten unseres Landes darstellen wuerde. Unter der Mehrzahl der an unsere Adresse eingegangenen [Bilder](#) hat unsere Jury 6 ausgewaehit. Ihre Meinung ist uns sehr wichtig und wir **moechten** Sie darum bitten uns mit **dem** Wahl der endgueltigen Sieger zu helfen.

Haben Sie kurz Zeit uns zu helfen? Ihre Stimme hilft uns ueber den besten Amateurfotokuenstlerfuer zu entscheiden. Die Wettbewebsbilder sind auf unserer [Web-seite](#) abrufbar. Dort koennen Sie auch Ihre Stimme fuer ein das Ihnen besonders gefallen hat abgeben. Um Ihnen die Ansicht der Fotos benutzerfreundlicher zu machen werden Fotoalben aller Teilnehmer in Form einer Diaschau dargestellt so dass die Panoramabilder mit den Ansichten der Schweiz nacheinander praesentiert werden. Alle Bilder die Ihnen besonders gefallen haben koennen Sie ruhig auf Ihren Arbeits-oder Home PC ohne jegliche Copyrightverletzung herunterladen. Fuer Ihre Stimme danken wir Ihnen im voraus.

[Uebergang zur web-seite zur Stimmabgabe](#)

Diese Mitteilung ist kein Spam, ihre Absendung ist mit der Verwaltung der Domain admin.ch abgestimmt.

Staatssekretariat für Wirtschaft SECO und
Schweizer Tourismus-Verband



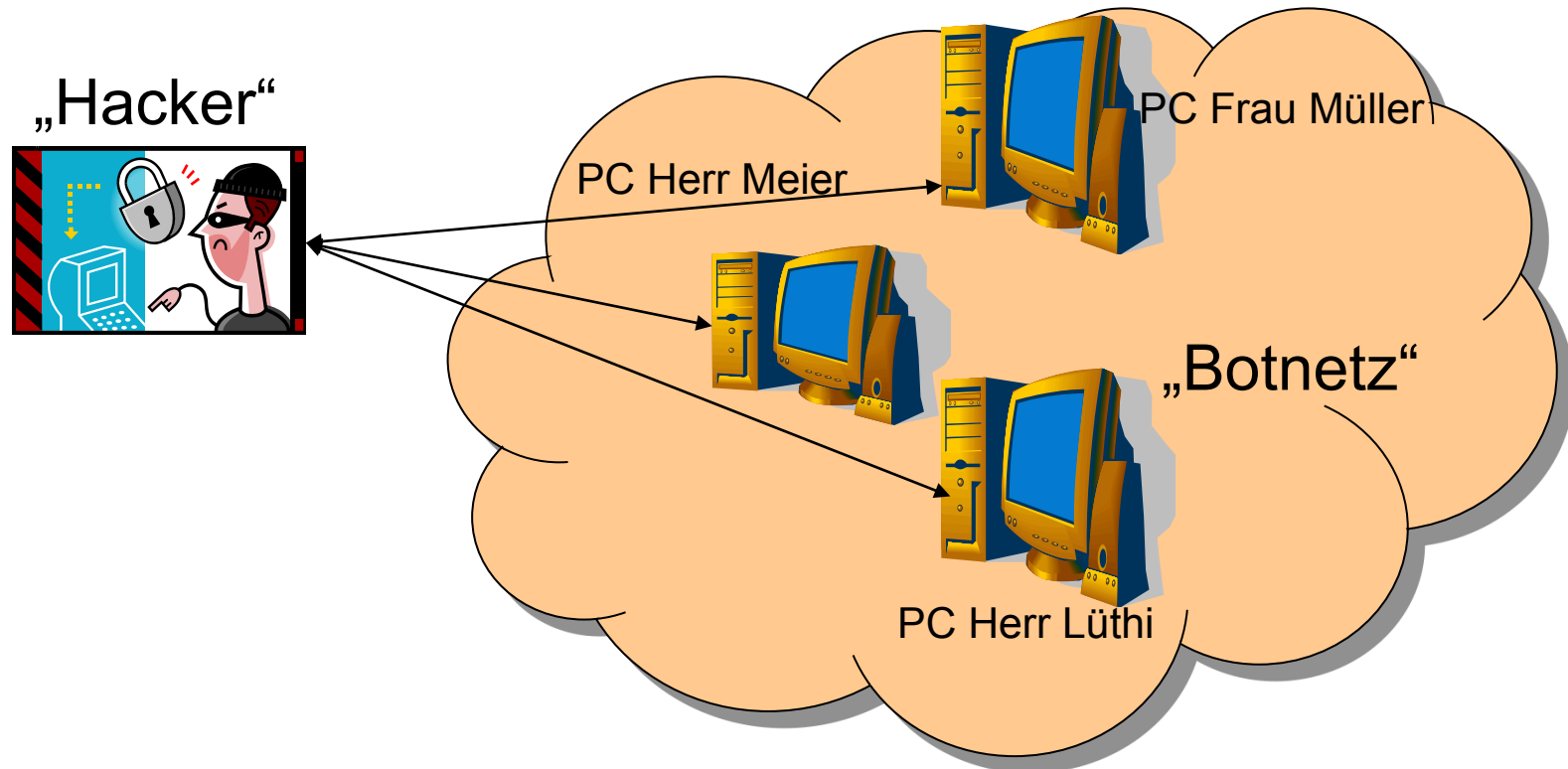
Lektion 3

- Private **und** staatliche Akteure nutzen Schadsoftware (insbesondere Trojanische Pferde) zur Spionage.
- **Staatliche Akteure** verfügen dazu über **enorme Ressourcen** (Computerspezialisten und Geldmittel) und setzen diese auch ein.
- Spionage-Angriffe finden statt – **auch in der Schweiz!**
- Betroffen sind **Verwaltungen**, die **Rüstungsindustrie** aber auch **kleinere innovative Firmen** (mit Handelsbeziehungen in die Länder der Angreifer).



Botnetze

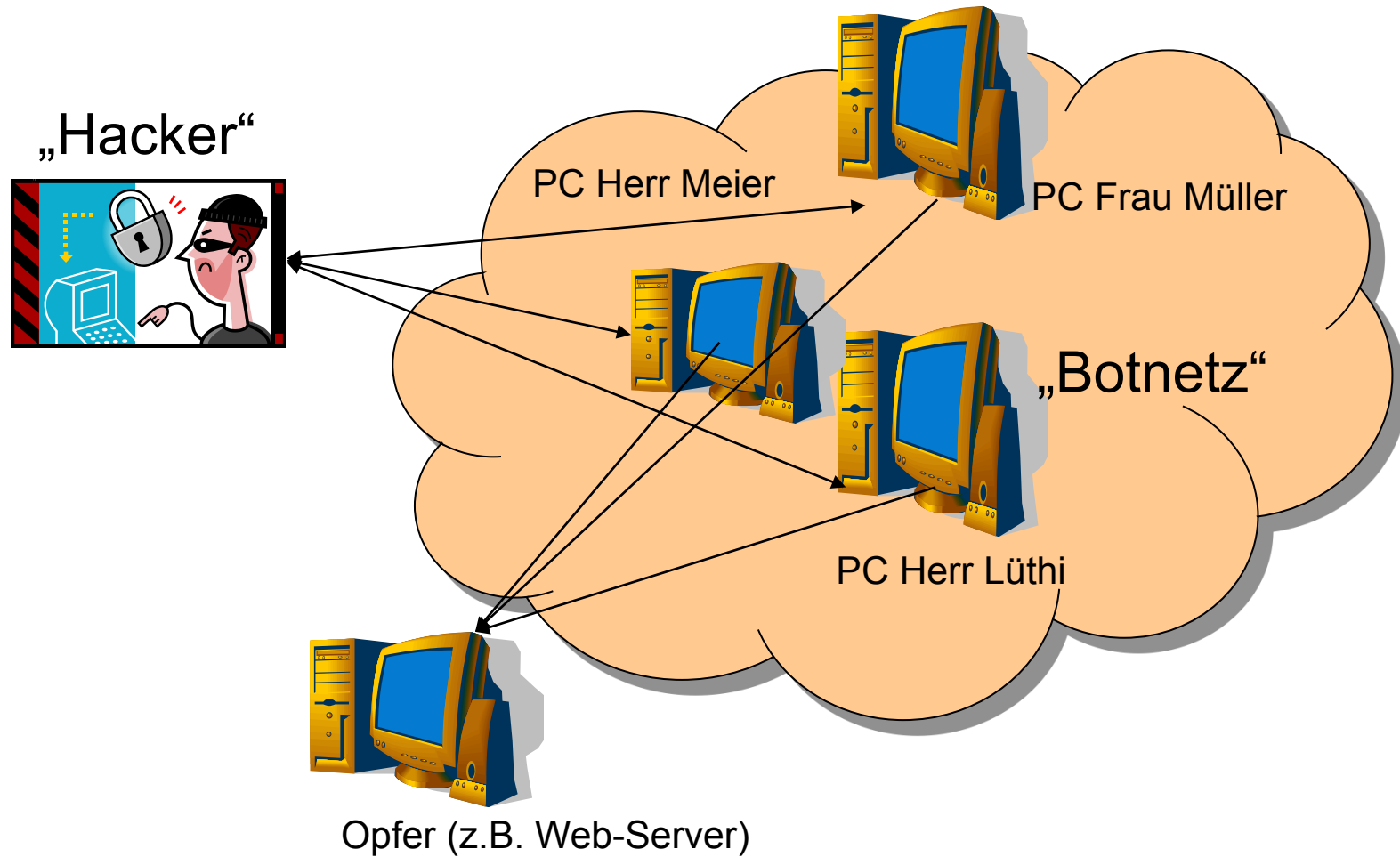
Verbund gehackter Computer, die vom Angreifer („Hacker“) kontrolliert (ferngesteuert) werden.



Bot: Aus dem slawischen Wort für Arbeit „Robota“ (wie „Roboter“ auch)



Distributed Denial of Service DDoS (Verteilte Verweigerung von Diensten)





Preisliste von Botnetzen

Produkt	Preis
Einfacher Windows Bot	10 Cents / Bot&Tag
Bot mit guter Bandbreite	1\$ / Bot&Tag
Spezialanfertigung	40\$ / Bot

Tauschgeschäfte sind auch möglich:

- 1 GigE Sun gegen 100 Windows Bots
- Kreditkartennummern gegen Bot



Einschlägiges Angebot auf dem Internet

▼ Subject: I offer the DDOS attack service !
From: ddos@safe-mail.net <DDOS Service> 
Date: 3/3/05 10:54
Newsgroups: alt.2600.cardz

HI,

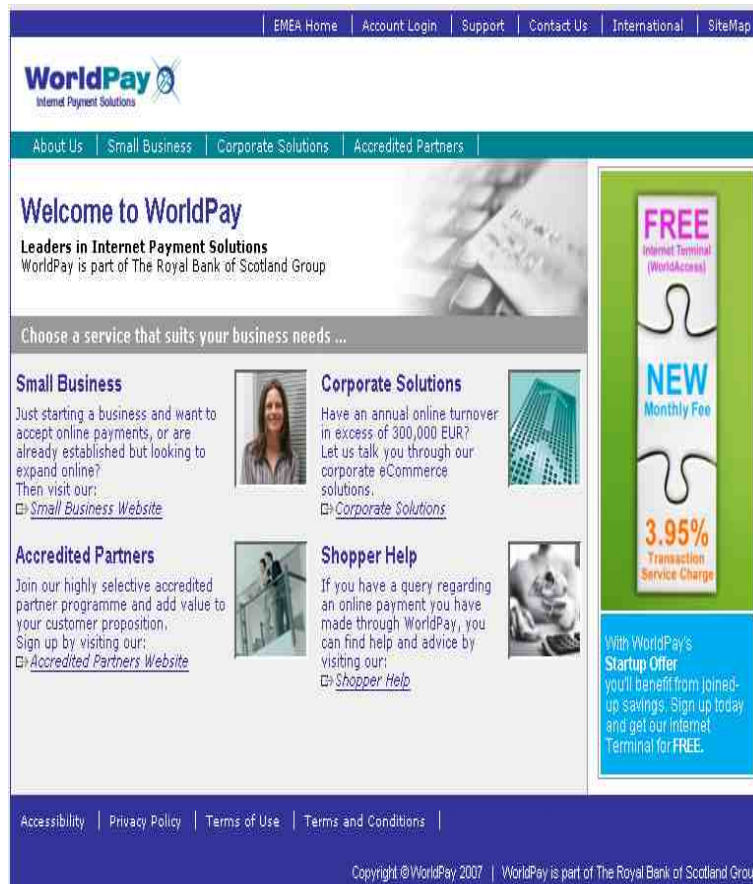
I offer the DDOS attack service, I offer estimate of expense on hour base. Free demonstration (10 minutes).

The price is based on the difficulty to pull down the target website, for the free demonstration or information please contact :

DDOS Service at : ddos@safe-mail.net



DDoS-Attacke auf Worldpay



- DDoS-Attacke führt zum fast **vollständigen Erliegen der Finanztransaktionen.**
- 30'000 Geschäfte in 70 Ländern sind betroffen.
- Einige erleiden **Umsatzeinbußen** zwischen **50 – 80%** während **2 – 3 Tagen.**
- **Beträchtlicher Schaden** für die betroffenen Volkswirtschaften.



Angriff mit Botnetz auf Estland (2007)



- Angriffe im Zusammenhang mit der **Ver-
setzung eines russischen Kriegsdenk-
mals**.
- Ziele:
 - **Internetbanken**
 - **Internet-Medien**
 - **E-Government-Dienstleistungen**
- **Beträchtlicher Schaden für die Volks-
wirtschaft.**
- Zehntausende Rechner aus 73 Ländern
waren an den Angriffen beteiligt.



Lektion 4

- **Was sich zu Geld machen lässt, wird** (früher oder später) **angegriffen.** (Computer samt deren Rechenleistung, Speicherkapazität, Netzwerk-Anbindung, gespeicherte Daten, usw.).
- Wer **Dienstleistungen über das Internet anbietet**
 - eCommerce, (eBanking, usw.),
 - eGovernment,
 - Internet-Medien**ist potentiell Opfer** (z.B. von DDoS-Angriffen).
- Motive: Bereicherung, Durchsetzung politischer Forderungen.
- Täterschaft: (Organisierte) Kriminelle, politische Gruppierungen, Konkurrenten.



Cyberterror / Cyberwar

- *Die Neunzigerjahre waren die Dekade der Cybervandalen, die Zweittausender die der Cyberkriminellen. Ich befürchte, dass nun das Zeitalter des Cyberterrorismus beginnt.*

Eugene Kaspersky

- Aussage bezieht sich auf Stuxnet (Sommer 2010):
 - **Erster Computerwurm**, der explizit dazu entwickelt wurde, **Industrieanlagen zu zerstören.**
 - **Keine finanziellen Interessen**
 - Greift gezielt Kontrollsysteme von Siemens an
 - Angriffsziel: Nuklearanlagen in Natanz und das (sich im Bau befindende) Kernkraftwerk Bushehr (beide im Iran).
 - Folgen des Angriffs: Physische Zerstörung der Ausrüstung (Überdrehen von Zentrifugen, Ausschalten von Schmier- und Kühlsystemen, usw.)



Cyberterror / Cyberwar

- **Entwicklungsaufwand** der Malware war **enorm**:
 - Hohe Komplexität der Software
 - Mind. 5 – 10 Top-Programmierer über **viele Monate**
 - **Braucht Testanlagen** und Originalsoftware von Siemens
- Angreifer: Mit hoher Wahrscheinlichkeit **staatliche Akteure** (Nachrichtendienste, Militär)
- Für Terroristen zur Zeit (vermutlich) technisch zu aufwändig und in dieser Art auch kein Ziel → Medienwirksamkeit, Verbreiten von Angst und Schrecken, Wiederholbarkeit usw. sind nicht gegeben.
- Aber: **Machbarkeit** ist nun **bewiesen!**



Zerstörer der Zivilisation: Von den Goten zu den Computerfreaks...

