Fachhochschule Nordwestschweiz
Hochschule für Technik

Sicherheit in der digitalen Welt

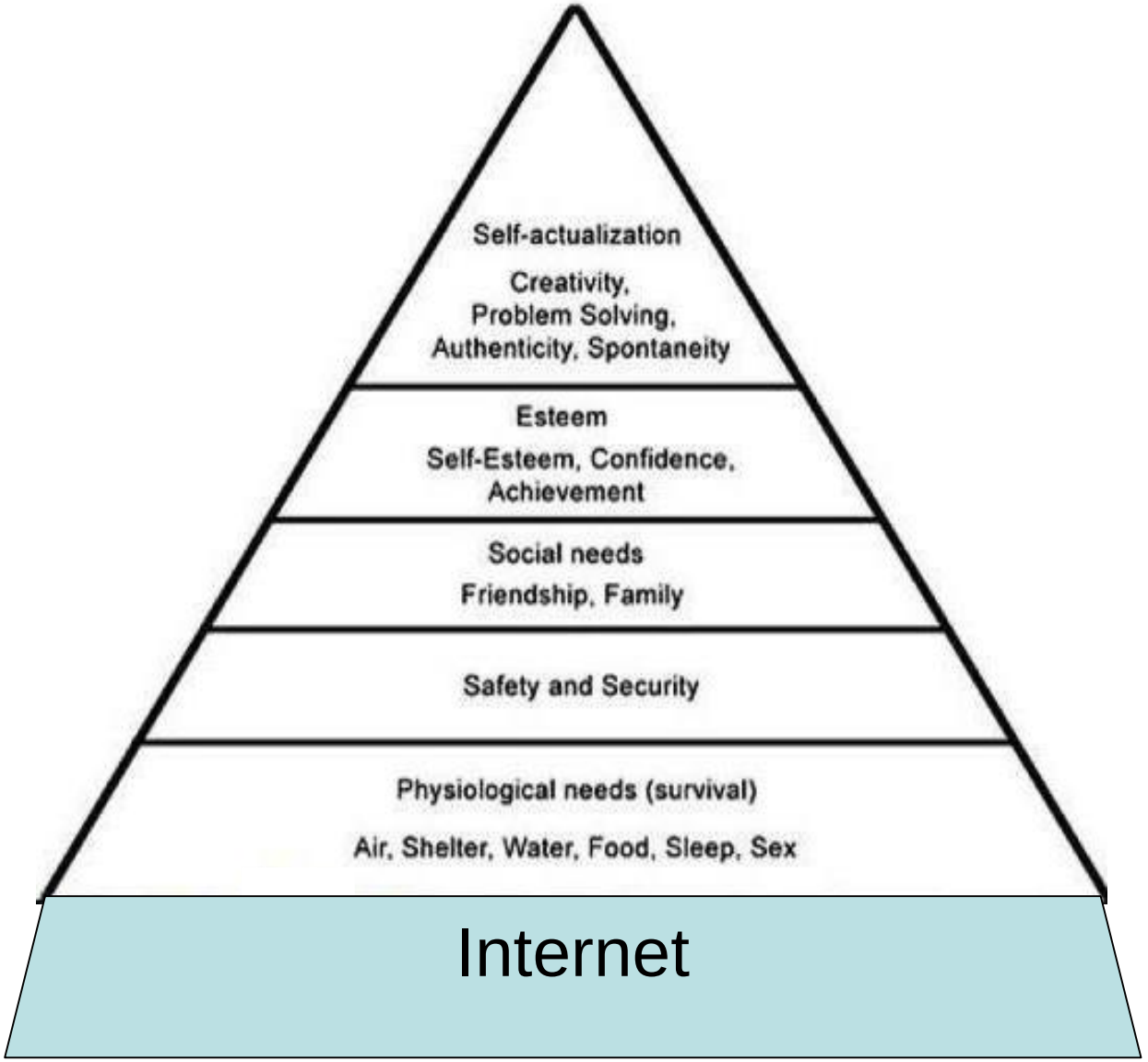
Die Welt ist gefährlich

Schadens
-Ausmass

Eintretens-
Wahrschein
-lichkeit

Das Bedürfnis nach „Sicherheit“

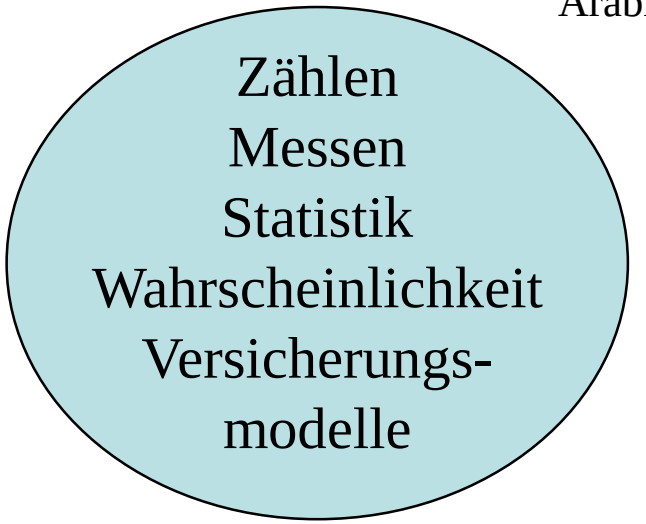
Sicherheit:
das Ausbleiben
unvertretbarer Risiken



Umgang mit Risiken

Antike Gesellschaften — Schicksal durch „die Götter“ vorbestimmt

Mittelalter



Arabische Zahlen (0)
Cardano
da Vinci
Pascal
Fermat
Bernoulli‘s
Leibniz
Gauss
Laplace
Keynes
von Neumann

Neuzeit — aktives, abstraktes Risiko-Management (Vermeidung, Übertragung, Begrenzung, Akzeptanz, Ignoranz)

Zukunft — Vorhersagen, Derivate, Chaos Theorie

Was ist ein “Risiko”?

Ein Risiko ist die *kalkulierte Prognose* eines möglichen *Schadens bzw. Verlustes im negativen Fall (Gefahr)* oder eines möglichen *Nutzens bzw. Gewinns im positiven Fall (Chance)*. Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab.

„Management“ des Risikos durch Vermeidung, Übertragung, Begrenzung, Akzeptanz, Ignoranz

Abhängig von Risikotyp und Risikokultur

Umgang mit Risiken

Umgang mit Risiken

Umgang mit Risiken

Gefahren im Internet (gezielt und ungezielt)

Privatpersonen

- Digitaler Identitätsdiebstahl, dann Verwendung zum Kauf von Software, Services, Altersnachweis etc.
- Preisgabe sensitiver Informationen, Bilder in Social Media Plattformen, dann Erpressung, Mobbing, Stalking etc.
- Nutzung fremder Rechner /Netze für sensitive Tätigkeiten (E-banking, Bewerbungen)
- Missbrauch des eigenen PC / Notebook / Tablet / Handy (Daten, Kamera, Speicher, Rechenleistung etc. via Netzwerk oder direkt)
- Betrieb ungeschützter (W)LANs und Systeme (keine Patches, keine Security-Software etc.)

Firmen

- Diebstahl von geistigem Eigentum oder Erlangung eines wirtschaftlichen Vorteils / Vorsprungs durch den Auftraggeber
- Verlangsamung / Beschädigung der IT-Umgebung, dadurch Wettbewerbsnachteile, Produktionsausfall, Haftungsschäden, Auftragsverluste, Lizenzentzug, etc.
- Missbrauch der Firmen-Infrastruktur durch Fremddienste (Verteilung raubkopierter Daten, Musik, Software, Zugriffe auf illegale Inhalte)
- Nutzung der Firmen-IT als Plattform für weitere Angriffe
- Schäden durch Erpressung von Mitarbeitenden

Angreifer und Motivationen

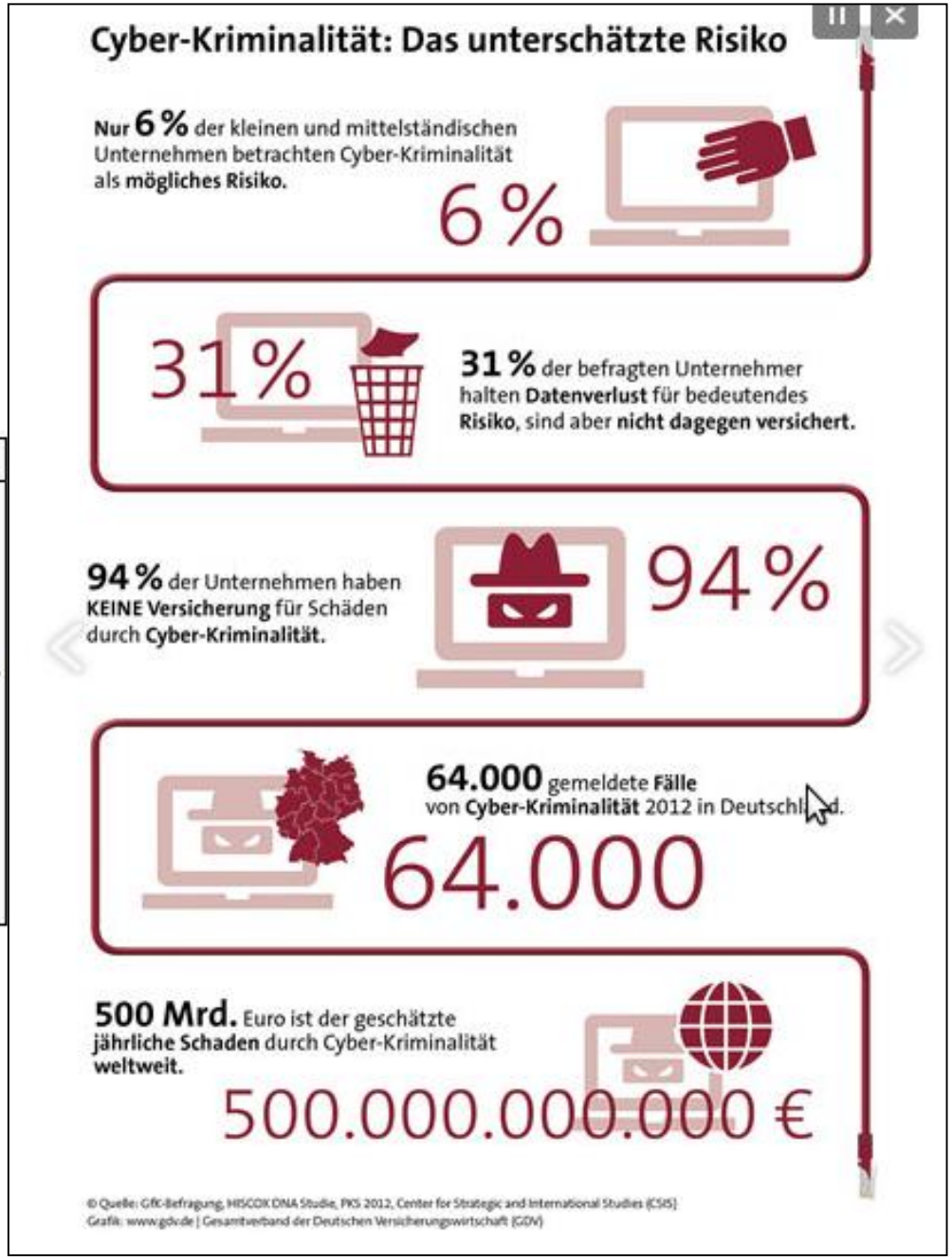
Extern:
- Hacker / Cracker
- Informationssammler
- Kriminelle Personen oder Organisationen
- Aufklärungsdienste
- Partner / Kunden
- Konkurrenten
- Fanatiker / Terroristen
- Militär

Intern:
- Unzufriedene Mitarbeiter
- Lieferanten / Wartung
- System Spezialisten
- Kriminelle
- Unvorsichtige Mitarbeiter

- Reputation (“Community”, Freunde, Öffentlichkeit, …)
- Langeweile (oft mit dem Angreiferalter verknüpft)
- Schaden / Rache (privater Streit, aktuelle / ehemalige Angestellte, …)
- Wettbewerber (Offerten, Kunden, Konditionen, Intentionen patentiertes Material, …)
- Direkter Vorteil (Software, Musik, …)
- Indirekter Vorteil (Lizenzen, Information, Zugang, …)
- Privater Auftrag (Kommerziell / Industriespionage)
- Staatsauftrag (Terrorismusbekämpfung, militärische Aufklärung, Standortstärkung, …)

Lohnt sich das?

Goods and services	Percentage	Range of prices
Bank accounts	22%	$10-$1000
Credit cards	13%	$0.40-$20
Full identities	9%	$1-$15
eBay accounts	7%	$1-$8
Scams	7%	$2.5/week - $50/week for hosting. $25 for design
Mailers	6%	$1-$10
Email addresses	5%	$0.83/MB-$10/MB
Email passwords	5%	$4-$30
Drop (request or offer)	5%	10%-50% of total drop amount
Proxies	5%	$1.50-$30



Trends 2016+

- «Advanced Persistent Threats (APT)»
- «Blended Attacks» inkl. «social engineering»
- «Cybercrime as a Service» inkl. «advanced analytics»
- Verschwimmende Grenze Aufklärung / Cybercrime
- Angriffe auf Infrastrukturen & das «Internet der Dinge»
- Internationalisierte, professionelle Wertschöpfungsketten

Trends bis 2030

- Neue Computer Paradigmen (Quantum, Bio, Neuro)
- Zusätzliche Netzwerk-Komplexität (SDN, …)
- «Big Data» Analyse
- Widerstandsfähigkeit (Resilience) & Selbst-Adaptierung

Was können wir tun?

Datenschutz

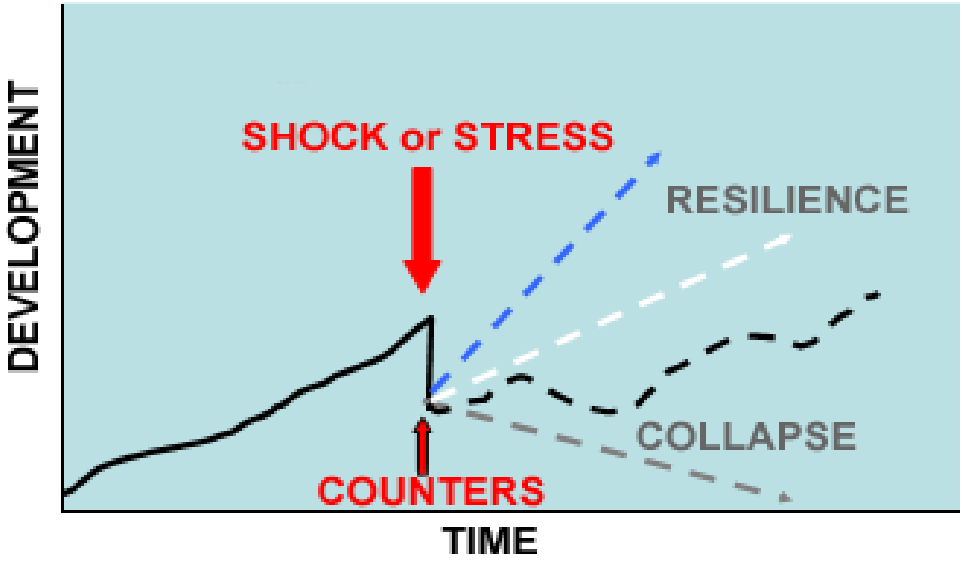
Datensparsamkeit

Pseudonymität

Hinterfragen

Prävention und Widerstandsfähigkeit «by design»

Figure 1 - Concept of resilience



Detektion, Eingrenzung, Wiederherstellung

Antizipieren / Üben des «Ernstfalls»

Fachhochschule Nordwestschweiz
Hochschule für Technik
Institut für Mobile und Verteilte Systeme

Prof. Dr. Hannes P. Lubich
Dozent für ICT System Management
Bahnhofstrasse 6, CH-5210 Windisch

T: +41 56 202 78 21 (direkt)
hannes.lubich@fhnw.ch
http://www.fhnw.ch/personen/hannes.lubich