Intrusion Detection Systems, Zensurinfrastruktur

Sebastian Claus
claus@informatik.hu-berlin.de

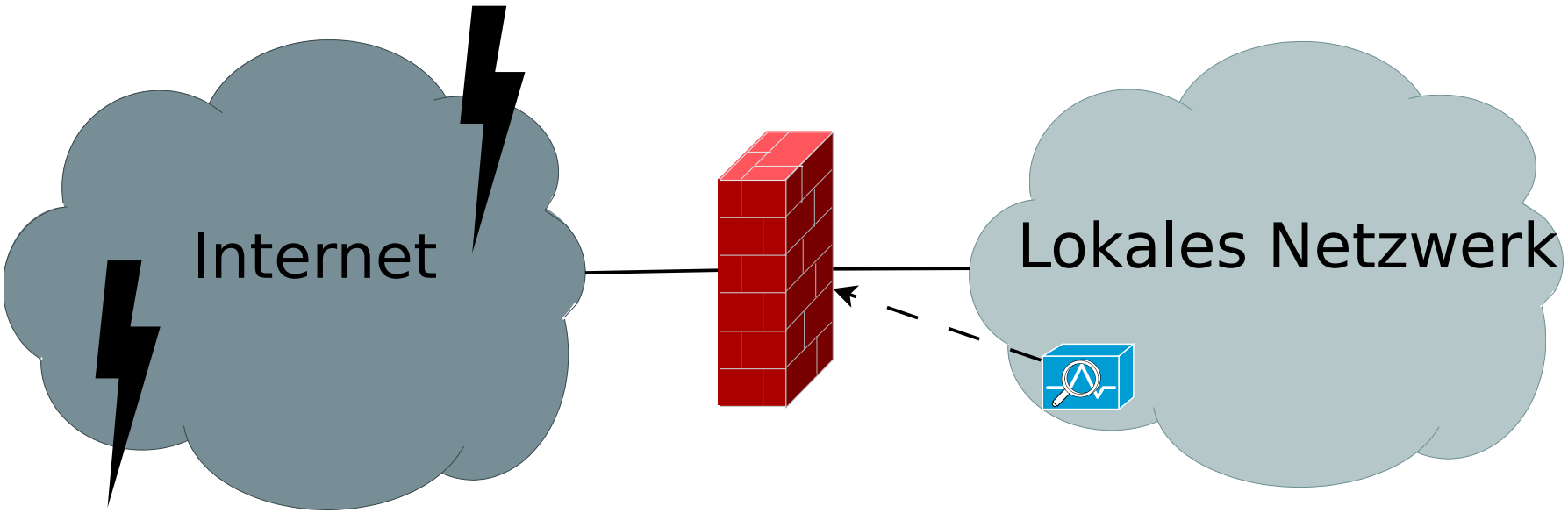
Seminar: Dystopien in der Informatik III,
Dozent: Jörg Pohle,
Institut für Informatik,
Humboldt-Universität zu Berlin

21. November 2012

Inhalt

Inhalt

Schaubild



IDS-Schema

Begriffe I

Intrusion

(Bace und Mell 2001)

- Versuch Vertrauenswürdigkeit, Integrität oder Verfügbarkeit (***C****onfidentiality*, ***I****ntegrity*, ***A****vailability*) eines Informationssystems zu gefährden
- Versuch Sicherheitsmechanismen eines Computers oder Netzwerkes zu umgehen

Begriffe II

Intrusion Detection (ID)

(Bace und Mell 2001)

- Beobachten eines Computersystems oder eines Netzwerkes
- Erkennen von Eingriffen

Begriffe III

Intrusion Detection System (IDS)

(Bace und Mell 2001)

- Soft- oder Hardware zum Automatisieren von ID

Begriffe IV

Intrusion Prevention System (IPS)

(Bace und Mell 2001)

- IDS mit Fähigkeit der Gegenmaßnahmen

Signaturerkennung

Signaturerkennung

(Liao et al. 2012)

- wissensbasiert
- Vergleich von Mustern mit erfassten Ereignissen

Pro

- einfachste Methode
- effektiv gegen bekannte Angriffe
- detaillierte Kontextanalyse

Con

- ineffizient gegen unbekannte, ausweichende, variierte Angriffe
- keine Zustände und Protokolle
- Aktualisierung der Wissensbasis

Anomalieerkennung I

Anomalieerkennung

(Liao et al. 2012)

- verhaltensbasiert
- Profile repräsentieren normales Verhalten
- statische und dynamische Profile mit vielen Attributen
- Vergleich von Profilen mit beobachteten Ereignissen

Anomalieerkennung II

Pro

- effektiv gegen unbekannte Angriffe, Schwachstellen
- weniger Abhängigkeit vom Betriebssystem
- erleichtert Erkennen von Privilegienmissbrauch

Con

- Ungenauigkeit von Profilen durch ständige Veränderung der Beobachtung
- nicht verfügbar während Neuberechnung der Verhaltensprofile

Stateful protocol analysis I

Stateful protocol analysis

(Liao et al. 2012)

- spezifikationsbasiert
- IDS kennt Protokollzustände
- Gegensatz zu Anomalieerkennung: allgemeine Profile von Entwicklern bereitgestellt
- im Allgemeinen: Protokollstandards von internationalen Institutionen (z. B. IETF)

Stateful protocol analysis II

Pro

- kennt und verfolgt Protokollzustände
- erkennt unerwartete Befehlsfolgen

Con

- hoher Ressourcenverbrauch zur Analyse von Protokollen
- erkennt keine Angriffe, die legitim erscheinen

Inhalt

Definition

Zensur

Karl-Dieter Bünting (1996). *Deutsches Wörterbuch*. Isis-Verlag AG

> *behördliche Prüfung von Büchern, Theaterstücken, Filmen, od. Ä. [insb. Internetseiten], bei der bestimmt wird, ob Teile eines Werkes od. das Gesamtwerk aus moralischen, sittlichen, politischen, religiösen od. ä. Gründen gestrichen od. verboten werden*

Vor- und Nachzensur

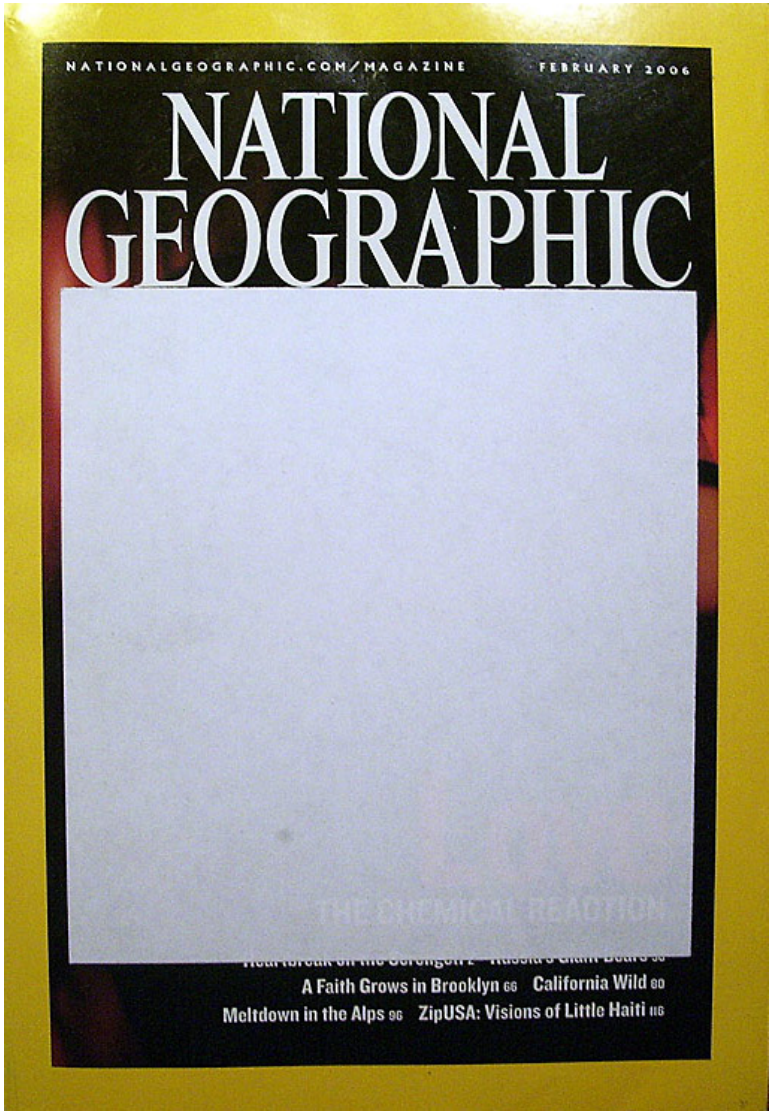
Vorzensur Prüfung und Verbot vor Veröffentlichung

- in Deutschland keine Zensur (*Art. 5 Abs. (1) GG*)

Nachzensur Prüfung und Verbot nach Veröffentlichung (**Indizierung**)

- praktisch in jedem Rechtsstaat
- beschränkt durch allgemeine Gesetze, Jugendschutz, Recht der persönlichen Ehre (*Art. 5 Abs. (2) GG*)
- in Deutschland bspw.: Bundesprüfstelle für jugendgefährdende Medien (BPjM)

Zensiertes Titelfoto



http://de.wikipedia.org/wiki/Datei:Natgeo_censorship.jpg

Das Bild

http://ngm.nationalgeographic.com/2006/02/true-love/slater-text

Inhalt

Geschichte der Netzsperren
(CCC 2012b)

Sommer 1996 Sperrung der Webseite der Zeitschrift „Radikal“

Herbst 2000 Hans Bernhard (AT) wird die Domain *vote-auction.com* entzogen

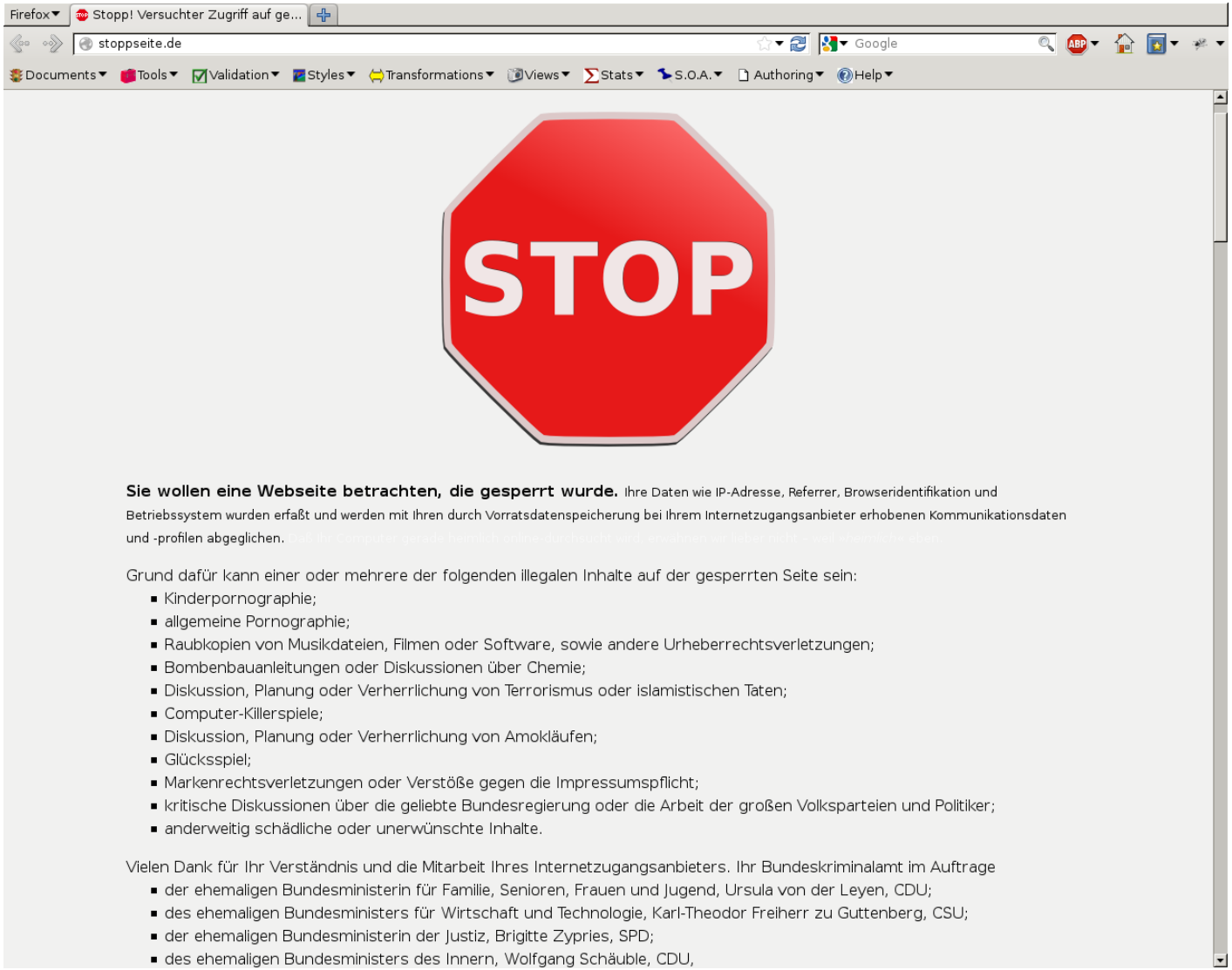
Frühjahr 2002 Scientology bewirkt: Cignal (USA) kappt Internet von Xtendend Internet (NL).

Herbst 2002 Schweizer Provider müssen zwei Internetseiten sperren wegen Ehrverletzung.

DNS-Spoofing

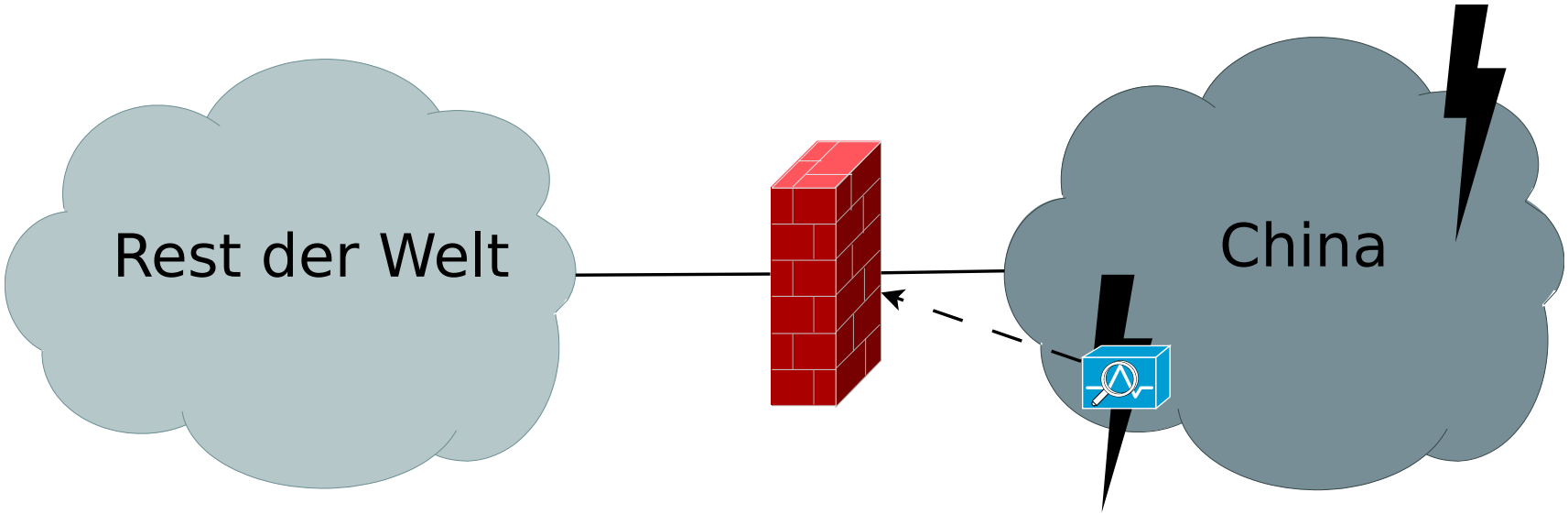
- Manipulation der Auflösung von Domänen
- signaturerkennendes IDS/IPS
- Beispiele
  - Unterbinden von Werbung im Web
  - Sperren von Internetseiten

Stopp!



http://stoppseite.de

Die chinesische Mauer des 21. Jahrhunderts I
(Qiu 2000)



Zensurinfrastruktur in China

Die chinesische Mauer des 21. Jahrhunderts II
(Qiu 2000)

rechtliche Basis:

- keine direkten Verbindungen außerhalb von China
  - jede Verbindung muss durch *ChinaNet*, *GBNet*, *CERNet*, *CSTNet*
- BBS nur für akademische Zwecke
  - Operatoren müssen politische Inhalte umgehend löschen
  - Im Notfall: alle HTTP-/Telnet-Verbindungen blockieren

technische Umsetzung:

- Internet-Knoten (IXP) sperren Zugriff auf Webseiten mit „schädliche Informationen“
- protokollieren Zugriffe mit gewissen Inhalten (z.B. „June Fourth“)
- Polizei kann jede Verbindung innerhalb des Netzes überwachen
- *China Wide Web* umgesetzt von viele amerikanischen Firmen (Sun Microsystems, bay networks of California, uvm.)

Quellen I

Bace, Rebecca und Peter Mell (2001). *Special report on intrusion detection systems*. Techn. Ber. National Institute for Standards und Technologie (NIST).

Bünting, Karl-Dieter (1996). *Deutsches Wörterbuch*. Isis-Verlag AG.

CCC (2012a). *China - Privacy Emergency Response Team*. Chaos Computer Club. URL: http://chinesewall.ccc.de.

— (2012b). *Internet-Zensur*. Chaos Computer Club. URL: http://www.ccc.de/censorship.

Liao, Hung-Jen et al. (2012). „Intrusion detection system: A comprehensive review“. In: *Journal of Network and Computer Applications* 0, S. –. ISSN: 1084-8045. DOI: 10.1016/j.jnca.2012.09.004. URL: http://www.sciencedirect.com/science/article/pii/S1084804512001944.

Quellen II

MacKinnon, Rebecca (2008). „Flatter world and thicker walls? Blogs, censorship andcivic discourse in China“. In: *Public Choice* 134 (1). 10.1007/s11127-007-9199-0, S. 31–46. ISSN: 0048-5829. URL: http://dx.doi.org/10.1007/s11127-007-9199-0.

Qiu, Jack Lunchuan (2000). „Virtual Censorship in China: Keeping the gate between the cyberspaces“. In: *Internetation Journal of Communications Law and Policy* (4), S. –. ISSN: 0048-5829.