Cyberterror

Reale Bedrohung oder Mythos?

Stefan Schumacher

Magdeburger Institut für Sicherheitsforschung

4. Sicherheitspolitische Aufbauakademie
Königswinter 25. - 28. Oktober 2013



Über Mich

- Geschäftsführender Direktor des Magdeburger Instituts für Sicherheitsforschung
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`
- Hacker seit >20 Jahren
- Berater Unternehmenssicherheit
- Berater für diverse Finanzinsitute, Strafverfolgungsbehörden und Regierungen



Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- Consciousness of a Hacker



Informationstechnologie und Sicherheitspolitik

Sambleben, J. und Schumacher, S. (Herausgeber)



http://www.sicherheitsforschung-magdeburg.de/buecher.html

Inhaltsverzeichnis

1 Terrorismus

2 Angriffsvektoren

3 Gruppen



Disclaimer

- Forschungslage bisher sehr dünn
- meist eher technische Diskussion
- oder komplett ohne technisches Verständnis ;-)
- keine umfassende Beantwortung der Fragestellung möglich



Was ist Terror? Was ist Terrorismus?

Definition (Terrorismus)

systematisch vorbereitete Planung und Durchführung illegaler Gewaltakte durch temporär oder dauerhaft zusammengesetzte Gruppen die in der Regel konspirativ und subversiv, national oder international mit der Zielsetzung kooperieren, eigene oder im Auftrag zu erfüllende politische Ziele zu erreichen.



Cyber Cyber

- abgeleitet von Kybernetik: Regelungstechnik, Regierung
- Cyberspace: geprägt von William Gibson in den 1980ern
- technische und soziale Dimension
- Technik: Rechner, Betriebssysteme, Protokolle, Dienste ...
- Soziale: Leben im Internet, 2nd Life, Facebook, Mobbing, Propaganda ...



Cyberterrorismus

- systematisch vorbereitete Planung und Durchführung illegaler Gewaltakte *im Internet bzw. Cyberspace*
- durch temporär oder dauerhaft zusammengesetzte Gruppen, die in der Regel konspirativ und subversiv, national oder international mit der
- Zielsetzung kooperieren, eigene oder im Auftrag zu erfüllende politische Ziele zu erreichen,

folgende Ziele erreicht werden können:

- Abschaffung bestehender Herrschaftsverhältnisse
- Beseitigung bestehender Herrschaftseliten
- Etablierung radikaler Alternativen unter Zuhilfenahme von Gewalt, Schrecken und Terror.
- Zugleich soll aber auch in Teilen der Bevölkerung Sympathie und Unterstützungsbereitschaft erzielt werden.



Abgrenzung Cybercrime

Organisierte Kriminalität ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig

- a) unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,
- b) unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder
- c) unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaf

zusammenwirken. Der Begriff umfasst nicht Straftaten des Terrorismus.



Cyberwar

- Krieg ist ein Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen. Clausewitz
- Im Internet nicht möglich!
- Wichtig: Akteur ist staatliche Organisation oder handelt im staatlichen Auftrag (Militär, Geheimdienst, etc.)
- Schumacher, S.: Vom Cyber-Kriege
  Schumacher, S.: Vom Cyber-Frieden



Abgrenzung der Akteure

- aus politikwissenschaftlicher, juristischer Sicht: Cybercrime - Cyberwar - Cyberterrorismus
- technische Sicht: irrelevant; stattdessen Handlungskompetenz
- Einschätzung der Handlungskompetenz notwendig
- Abschätzung der Fähigkeiten
- Abschätzung der Aufwuchsmöglichkeiten/Nachwuchsgewinnung
- Einteilung in der IT-Sicherheitsszene

Abgrenzung der Akteure

- aus politikwissenschaftlicher, juristischer Sicht: Cybercrime - Cyberwar - Cyberterrorismus
- technische Sicht: irrelevant; stattdessen Handlungskompetenz
- Einschätzung der Handlungskompetenz notwendig
- Abschätzung der Fähigkeiten
- Abschätzung der Aufwuchsmöglichkeiten/Nachwuchsgewinnung
- Einteilung in der IT-Sicherheitsszene



Hacker, Cracker Bauernfänger

- Script Kiddies: the lowest form of crackers, use scripts but don't understand them
- Problem: Scripte werden besser, z.B. Metasploit, Armitage, Saint
- höheres Schadenspotenzial möglich
- Hacker: A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular.
- sehr hohes technisches Verständnis/hohe Kompetenz
- aber: Hackerethik!, starke Politisierung in Deutschland



Ausbildung

- formale Ausbildung existiert, aber ein Dipl.-Inf. ist kein Hacker!
- formale Ausbildung im Bereich IT-Sicherheit dauert
- non-formale Ausbildung dauert noch länger (20 Jahre and still counting ...)
- Hacker haben eine Kultur und bestimmte Persönlichkeit (Openness, Neuroticism, Extraversion)
- Stipendien möglich, aber sinnvoll?
- Kann ein Terrorist Hacker werden?



Inhaltsverzeichnis

1 Terrorismus

2 Angriffsvektoren

3 Gruppen

Cyber?-Terror?

Ziele:

- Abschaffung bestehender Herrschaftsverhältnisse
- Beseitigung bestehender Herrschaftseliten
- Etablierung radikaler Alternativen unter Zuhilfenahme von Gewalt, Schrecken und Terror.
- Zugleich soll aber auch in Teilen der Bevölkerung Sympathie und Unterstützungsbereitschaft erzielt werden.

Kann man so etwas im Internet erreichen? - Angriffsvektoren identifizieren



- Stromversorgung
- Versorgung mit Erdöl, Erdgas, Heizöl, Treibstoffen, Kraftstoffen, Schmierstoffen etc.
- nationale Kommunikationsnetze
- Vernetzung der Banken, Geldautomaten
- Smart-Meter in Haushalten
- Steuerungssysteme in intelligenten Häusern
- vernetzte Computersysteme (das ominöse Internet)
- Industriesteuerungsanlagen (SCADA)
- Satelliten
- Geo-Positionssysteme (GPS, Glonass, Galileo)
- Steueranlagen in der Luft- und Raumfahrt, Drohnensteuerung



Inhaltsverzeichnis

1 Terrorismus

2 Angriffsvektoren

3 Gruppen



Relevante Gruppen

- Salafistische/Islamistische Gruppen
- Rechtsterrorismus
- Linksterrorismus
- Anonymous
- Hackergruppe (Antisec, Antiforensics)

Al-Kaida

- kaum technischer Sachverstand im IT-Sicherheitsbereich
- keine IT-Angriffe bekannt
- Quellen zeigen keinerlei sinnvolle Aktionen
- Bastelkryptographie auf Staatstrojaner-Niveau



Tadpole

	Sat	Sun	Mon	Tue	Wed	Thu
08:00	dasdf	dasdf	adsa	asd	asd	assf
08:30	dasdf	dasdf	adsa	asd	asd	assf
09:00	dasdf	dasdf	adsa	asd	asd	assf
09:30	dasdf	dasdf	adsa	asd	asd	assf
10:00	dasdf	dasdf	adsa	asd	asd	assf
10:30	dasdf	dasdf	adsa	asd	asd	assf
11:00	dasdf	dasdf	adsa	asd	asd	assf
11:30	dasdf	dasdf	adsa	asd	asd	assf
12:00	dasdf	dasdf	adsa	asd	asd	assf
12:30	dasdf	dasdf	adsa	asd	asd	assf
13:00	dasdf	dasdf	adsa	asd	asd	assf
13:30	dasdf	dasdf	adsa	asd	asd	assf
14:00	dasdf	dasdf	adsa	asd	asd	assf
14:30	dasdf	dasdf	adsa	asd	asd	assf
15:00	dasdf	dasdf	adsa	asd	asd	assf
15:30	dasdf	dasdf	adsa	asd	asd	assf
16:00	dasdf	dasdf	adsa	asd	asd	assf
16:30	dasdf	dasdf	adsa	asd	asd	assf
17:00	dasdf	dasdf	adsa	asd	asd	assf
17:30	dasdf	dasdf	adsa	asd	asd	assf
18:00	dasdf	dasdf	adsa	asd	asd	assf
18:30	dasdf	dasdf	adsa	asd	asd	assf



Tadpole

JMB Communications Protocol using TADPOLE

1. Use codebook substitutions within cleartext
2. Apply punctuation editing protocol to cleartext
3. Encrypt cleartext file with channel key using TADPOLE
4. Rename cyphertext file deceptively: *DLL, PDF, etc*
5. Upload disguised cyphertext file to a cloud site: *Speedyshare, 2shared*
6. Create short URL for file location and get short code: *Notlong*
7. E-mail the short Notlong file name (only) to recipient

JMB also tried to use TORPark for anonymous uploading.



Aktuelle Vorfälle

- Syria, Iran armed for cyberwar with U.S. - Washington Times
- The Syrian Electronic Army (SEA) are a pro-Assad hacker organisation who claim responsibility for attacks on websites belonging to the Washington Post, Al Jazeera, Human Rights Watch, the Telegraph and the Independent, among others. Most recently, they hacked the BBC Weather Twitter account and flooded it with pro-regime propaganda, which was more hilarious than it was an inspiration to load up, ship out and go to battle with Assad's enemies, but I suppose it's still getting their message out there. (Vice)



Syrien

- diverse Untergrundgruppen
- ziehen anonymisiertes Darknet auf
- versorgen Teile Syriens mit Internet
- GSM-Center gekapert
- von Spezialisten weiterbetrieben u.a. für Rebellen

Rechtsextremisten

- ein bisschen Propaganda, ein paar Foren, Videos
- keine Hacks bekannt
- keine Hacker aktiv
- eher Opfer von Angriffen (Webshops etc.)



Linksextremismus

- höhere intellektuelle Kapazitäten
- engere Verbindung zur Hackerszene
- personelle Überschneidung
- diverse Aktionen gegen Webshops und Webseiten
- effektive (terroristische) Angriffe nicht bekannt

Anonymous

- Spaßguerilla aus 4chan
- u.a. gegen Scientology
- Guy Fawkes-Maske als Statement
- Operation Payback, Operation Blitzkrieg
- dDoS-Attacken, Webseiten gehackt
- politische Bewegung - Verbindungen zu Aktivisten



Chaos Computer Club

- Dezentrale Orga
- lokale Überschneidungen zu linksextremistischen Gruppen
- einige Leute mit viel Ahnung - aber nicht alle ;-)

Stratfor

- Weihnachten 2011 gehackt (Chaos Communication Congress ...)
- Datenbank geleakt
- sämtliche Nutzerdaten und gehashten Passwörter
- 40% der Passwörter in 1 Tag gecrackt
- u.a. StvKdrCalw@Bundeswehr.org



Stratfor

- Weihnachten 2011 gehackt (Chaos Communication Congress ...)
- Datenbank geleakt
- sämtliche Nutzerdaten und gehashten Passwörter
- 40% der Passwörter in 1 Tag gecrackt
- u.a. StvKdrCalw@Bundeswehr.org

- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher