Proseminar „Ethische Aspekte der Informationsverarbeitung“

Thema: Cyber-Terrorismus

Susanne Schölzel

Gliederung

1. Definition

2. Cyberattacken allgemein

3. Gründe für die vielen Cyberattacken

4. Cyberproteste

5. Nutzung des Internets durch Terroristen

6. Cyberattacken durch Terroristen

7. Möglichkeiten zum Schutz vor Cyberattacken

8. Fazit

1. Definition

- US-Verteidigungsministerium definiert Terrorismus als:
  „Den kalkulierten Einsatz gesetzwidriger Gewalt oder die Drohung mit gesetzwidriger Gewalt, um Angst zu erzeugen, mit der Absicht Regierungen oder Gesellschaften zu nötigen oder einzuschüchtern zur Verfolgung von Zielen, die im Allgemeinen politisch, religiös oder ideologisch sind."
- Cyber-Terrorismus: Methode bezieht Art Internetattacke gegen Computer, Netzwerke oder Informationen, die auf bzw. in ihnen gespeichert sind, ein
- Beispiele für Cyber-Terrorismus:
  - Attacken, die zu Explosionen, Flugzeugabstürzen, Verseuchung von Trinkwasser, Tod oder physischer Verletzung führen
  - je nach Grad der Beeinträchtigung Angriffe auf wichtige Infrastrukturen
- nicht unter Begriff des Cyber-Terrorismus gefasst: Angriffe, die lediglich nicht lebensnotwendige Dienste stören und hauptsächlich kostspieliges Ärgernis darstellen

2. Cyberattacken allgemein

- Studie der US-Sicherheitsorganisation CERT (Computer Emergency Response Team):
  - Anzahl der Attacken im Internet in letzten paar Jahren drastisch zugenommen
  - 2000: CERT registrierte 21.756 Cyber-Attacken
  - 2001: 52.658 Attacken
  - 2002: 82.094 Attacken
  - 2003: 137.529 Attacken
  - jeder einzelne dieser Vorfälle kann Attacke entsprechen, die tausende oder hunderttausende Computer infiziert hat
  - nicht alle Vorfälle werden CERT gemeldet
    → wahrscheinlich nur kleiner Bruchteil aller Attacken
- Firma Riptech Daten gesammelt für ihre Kunden:

    - fast 40% der Attacken zielten auf konkrete Organisation oder konkretes Firmennetzwerk
      → viele Leute versuchen sehr spezifische Stellen anzugreifen
    - Intensität der Attacken nimmt zu
    - Intensität der Attacken, entgegengesetzt zu einigen Berichten, nicht gesunken nach dem 11. September
    - Notfälle, bei denen Sicherheitsverletzung stattgefunden hat und jemand ins Netzwerk eingedrungen ist bei etwa 12% der Firmen
    - alle Firmen: Informationsattacken gegen sich
    - fast alle: Warnungen, in denen Attacke Firewall umging, aber System nicht schadete
    - Mehrheit der Attacken von Personen in den USA, gefolgt von Südkorea, China, Deutschland und Frankreich
    - hinsichtlich Ursprüngen von Attacken pro Einwohner: Israel Hauptquelle, gefolgt von Hong Kong, Thailand, Südkorea, Frankreich und Türkei
- viel Besorgtheit über ernsthafte Attacken gegen kritische Infrastrukturen
- Riptech berichtete:
    - ernste Attacken hauptsächlich auf Strom- und Energieindustrien und Finanzdienstleistungsindustrien (beides kritische Infrastrukturen) gerichtet
    - Hightechindustrie folgt danach
- Rate der Virusinfektionen von e-mails steigt
- Daten einer Anti-Virus Firma, die e-mails ihrer Kunden geprüft hat:
    - 1999: eine in 1400 e-mails mit Virus infiziert
    - 2001: eine in 300 e-mails
    - 2015: 3 von 4 e-mails werden Virus haben
- 2007: im Durchschnitt eine von 117,7 e-mails mit Virus infiziert
- Rate der Virusinfektionen von Computern steigt ebenfalls
    - 1996: rund 1% der Computer infiziert
    - 2001: rund 10%
- benötigt nicht viele Fähigkeiten, um Virusattacken durchzuführen
- kann freie Softwareprogramme aus Internet herunterladen, die Virus erschaffen:
    - startet Programm, füllt ein paar Kästchen aus und hat Virus erzeugt

- erklärt enorme Anzahl an Computerviren
- häufiger Virustyp: Wurm
  - als Anhang einer e-mail gesendet
  - schickt sich selbst an jeden im Outlook e-mail Adressbuch, wenn man Anhang öffnet
- Code Red Wurm:
  - einer der kostspieligsten Viren (kostspieligste: I Love You Virus)
  - durch Code Red Wurm verursachte Verluste auf 2,4 Millionen $ geschätzt
  - verbreitete sich schnell quer übers Internet
  - endete mit 359.000 infizierten Computern innerhalb von 13 Stunden
  - breitet sich nicht per e-mail aus
  - attackiert Computer nur, kopiert und automatisiert das, was Hacker tun würde
  - wenn infizierter Computer läuft, sucht er Internet nach ungeschützten Computern ab
  - wenn er einen findet, kopiert er sich selbst auf diesen Computer und sucht dann wieder nach ungeschützten Computern
- mit etwas mehr Geschick und krimineller Energie lassen sich noch ganz andere Computerviren entwickeln, die sich noch schneller verbreiten und noch größeren Schaden anrichten können
- Verunstaltung von Webseiten:
  - auch darin dramatischer Anstieg in letzten Jahren
- Denial-of-Service(DoS)-Attacken (Dienstverweigerung):
  - Benutzergruppen schließen sich zusammen, um einen Server zu bestimmtem Zeitpunkt mit Anfragen zu überhäufen
  - speziell geschriebene Computerprogramme simulieren tausende von Anfragen pro Sekunde
  - überlastet früher oder später auch leistungsstarke Server → Dienste des Servers werden arbeitsunfähig gemacht
  - DoS-Attacken steigen ebenfalls an
  - San Diego Supercomputing Center schätzt: rund 4000 DoS-Attacken pro Woche
  - meisten davon dauern weniger als eine Stunde, ein paar Prozent gehen mehr als einen Tag weiter

3. Gründe für die vielen Cyberattacken

- Ziele: z.B. Datendiebstahl, Datenlöschung, finanzielle Bereicherung
- Internet gewachsen → mehr Leute da draußen zum attackieren und mehr Seiten, die potentielle Opfer sind
- Angreifer bekommen immer mächtigere Tools
- Attacken leicht auszuführen und haben geringes Risiko
    - wenn man nur Webseite verunstaltet, sind Risiken, dass jemand versucht einen ausfindig zu machen und festnehmen zu lassen beinahe Null, da Schäden meist nicht so hoch
- Hauptgrund: Anzahl der Schwachstellen in Systemen
    - Software hat bekannte Schwachstellen
    - werden immer wieder weitere Schwachstellen entdeckt
    - Microsoft am meisten genutzt → Hacker stärker geneigt in dieses System einzudringen
    - Schwachstellen können auch auftreten durch Art und Weise, in der Systemadministratoren Software installieren und betreiben
    - Benutzergewohnheiten erzeugen Schwachstellen:
        - schlechte Passwörter immer noch Hauptplage im Internet
        - erstaunliche Anzahl von Leuten noch nicht einmal default Passwort geändert, das sie anfänglich erteilt bekommen haben → Hacker kennt default Passwort
    - meisten Attacken nutzen bekannte Schwachstellen aus, die durch Anwender behoben werden könnten
    - Anzahl der Schwachstellen, die CERT berichtet wurden:
        - in letzten paar Jahren dramatisch gestiegen
        - 2001: 2437 pro Jahr (rund 7 pro Tag)
        - 2007: 7236 pro Jahr erreicht (rund 20 pro Tag)
- Vielzahl der Attacken, die im Internet stattfinden, nicht von Aktivisten oder Terroristen durchgeführt, sondern von:
    - Leuten, die Spaß haben wollen
    - organisierten kriminellen Gruppen, die Kreditkartennummern stehlen, sich Zugriff zu Bank- und Finanzsystemen verschaffen und falsche finanzielle Transaktionen ausführen

- Erpressung auch immer häufiger, insbesondere gegen Finanzinstitutionen:
    - Angreifer gelangen hinein, erhalten Zugriff zu Kreditkartennummern oder anderen Finanzdaten
      → drohen Firmen bloßzustellen oder sensible Daten ins Internet zu stellen, falls Firma nicht bezahlt

4. Cyberproteste

- Cyberproteste zunehmend alltäglich geworden
- ebenso wie Konflikte in realer Welt stattfinden, z.B. die im Nahen Osten, Kosovo oder Kashmir, der Spionageflugzeugvorfall mit China usw., starten Hacker eigene Formen des Protests, indem sie Regierungsseiten in anderen Ländern, E-Commerce-Seiten oder irgendeine Seite, zu der sie Zugriff bekommen können, attackieren
- Institute for Security Studies in Dartmouth:
    - schaute sich Konflikte an, die in physischer Welt stattfanden, um zu sehen, wie diese in Beziehung zu Cyberattacken standen
    - fanden gute Übereinstimmung mit einigen Ereignissen
- Oktober 2001: Nahost-Cyber-Krieg ausgebrochen:
    - pro-palästinensische Angreifer zielten hauptsächlich auf kommerzielle Seiten in Israel
    - pro-israelische Angreifer zielten hauptsächlich auf Webseiten, die Terroristenorganisationen, insbesondere Hamas und Hisbollah, unterstützten
    - pro-palästinensische Hacker schlossen die in London ansässige Gruppe al-Muhajiroun mit Verbindungen zu al-Qaida ein
- Elektrohippies:
    - in Großbritannien ansässige Hackergruppe
    - in letzten paar Jahren verschiedene Arten von Cyberprotestereignissen organisiert
    - April 2002: Aktion gegen israelische Regierung gestartet wegen politischen Maßnahmen und Aktionen des israelischen Ministerpräsidenten Sharon

    - war Art Denial-of-Service-Attacke
    - klickten sich durch mehrere Teile der israelischen Regierungsseiten, um eine Menge Traffic gegen diese Webseiten zu erzeugen und sie zu blockieren → legitimer Traffic konnte nicht auf Webseite gelangen
    - legte Webseiten nicht wirklich still, aber verlangsamte sie so sehr, dass sie nicht mehr nützlich waren
- nach 11. September haben Leute im Cyberspace entweder versucht ihre Unterstützung für bin Laden auszudrücken oder Leute, die wütend waren wegen Ereignissen des 11. September, haben alles mögliche in Afghanistan oder Nachbargebieten angegriffen:
    - pro-bin Laden Gruppen wie al-Qaida Alliance Online tauchten auf
    - G-Force Pakistan (Hackergruppe, die al-Qaida Alliance Online gegründet hat) hat mehrere Webseiten verunstaltet
    - ihre Verunstaltungen legten dar, dass sie Ereignisse des 11. September verurteilen, aber gleichzeitig bin Laden und das, wofür er steht, unterstützen
    - Hacker haben ihre Forderungen aufgeführt
    - auf Anti-Terroristen-Seite auch mehrere Gruppen erschienen
    - Gruppe Young Intelligent Hackers Against Terrorism (YIHAT) sagt: darauf aus Geldressourcen des Terrorismus zu unterbrechen
    - behaupteten in zwei Banken im Nahen Osten, die Konten für bin Laden hatten, eingebrochen zu sein (Banken bestreiten das)
    - YIHAT Webseite forderte vereinigtes Amerika auf ihre Computer den Hackern zu spenden, damit sie diese für das Cyberattacken-Training nutzen könnten
    - andere Anti-Terroristen-Hacker verunstalteten Webseiten, die die Taliban unterstützten
    - Hacker „Fluffi Bunny“ stellte Bild eines kleinen ausgestopften Hasen auf seine Webverunstaltung
    - eine Verunstaltung lautete: „Wenn ihr das Internet wieder sehen wollt, gebt uns Mr. bin Laden und 5 Millionen $ in einer braunen Papiertüte. In Liebe, Fluffi B.“

- ziemlich große Gruppe, geleitet von Hacker „Hacka Jak“ aus Ohio, auch Webseiten angegriffen, die eng mit Terroristen verbunden waren
- Sicherheitsgemeinschaft bat sie inständig, das nicht zu tun → Gruppe stoppte danach Webseiten zu verunstalten

5. Nutzung des Internets durch Terroristen

- Terroristen nutzen wie jeder andere Informationstechnologie, insbesondere Internet
- seit 11. September haben wir gesehen, wie die Flugzeugentführer e-mail und instant messaging genutzt haben und sich im Web nach Informationen umgesehen haben
- nutzten auch einige Informationsverbergungstools → schwerer aufzuspüren im Internet
- kanadische Regierung berichtete: al-Qaida hat Web genutzt, um Informationen über kritische Infrastrukturen zu suchen
- Aum Shinryko Gruppe:
  - Giftgasattacke auf U-Bahn in Tokio durchgeführt
  - gründete Softwarezweig
  - japanische Polizei entdeckte, dass diese Gruppe die Software geschrieben hat, die die Polizei genutzt hat
  - war unter Vertrag, um Systeme für 10 Regierungsbüros und etwa 80 Handelsfirmen zu entwickeln
- Hisbollah Webseite hat englische Version ihrer Webseite, aber viele Seiten von Terroristengruppen nicht auf Englisch → muss Originalsprache, in der sie sind, lesen können
- manche haben Bereiche auf ihren Webseiten, die unzugänglich für Gelegenheitsnutzer sind
- Guido Rudolphi:
  - Computerspezialist in der Schweiz
  - hat nachgeforscht, wie al-Qaida Internet genutzt hat
  - fand Webseite, die von Mann namens Ould Slahi betrieben wurde (mit Millenium-Bomben-Anschlag gegen Flughafen von Los Angeles und 11. September verbunden)

    - Webseite hat Gästebuch, das von al-Qaida zur internen Kommunikation genutzt wurde
    - Rudolphi verfolgte Aktivität auf dieser Webseite
    - offenbar stieg Anzahl der Personen, die auf diese Webseite gingen und Nachrichten posteten, dramatisch kurz vor 11. September
- über einige Fälle berichtet, in denen Verschlüsselung genutzt wurde, um Mitteilungen zu verbergen
- Regierungsbeamte konnten Verschlüsselung in vielen Terroristenfällen entschlüsseln, weil Qualität nicht so gut war, im Grunde aus USA exportierte Verschlüsselung
- gab Spekulationen, dass Terroristen Mitteilungen in Bildern, die im Internet gepostet wurden, versteckt haben:
    - Computerwissenschaftler hat Webseite, die bin Laden unterstützte, genau beobachtet
    - untersuchte Bilder
    - hat herausgefunden, dass Bilder von einem zum anderen Tag gleich aussahen, aber wenn man sich binären Code angeschaut hat, sich die Bits, aus denen die Bilddateien zusammengesetzt waren, von Tag zu Tag geändert haben

6. Cyberattacken durch Terroristen

- sehr wenige Cyberattacken von Leuten begangen, die bekannte Terroristen sind
- Fall eines Terroristen:
    - wandte sich 1998 an Hacker, um Software zu kaufen, die von Computersystem des Verteidigungsministeriums entwendet wurde
    - Hacker behauptete, dass sie benutzt werden könnte, um Netzwerke des Verteidigungsministeriums zu kontrollieren
    - war Übertreibung dessen, was Software tun konnte
    - trotzdem interessant, dass jemand versuchte, dieses Programm zu kaufen
- anderer Fall:

    - IRA Hacker in Computer der britischen Regierung eingebrochen
    - Ziel nicht, Zerstörung zu verursachen, sondern Informationen zu sammeln, um diese in physischen Attacken zu nutzen
- gab Berichte darüber, dass al-Qaida Cyberdrohungen gemacht hat:
    - al-Qaida-Mitglied behauptete, dass sie Programmierer hatten, die für Microsoft gearbeitet haben, und trojanische Pferde in Microsoftcode eingebaut haben
    - sehr unwahrscheinlich, dass das geschehen ist
    - deutet an, dass al-Qaida sich des Potentials einer Cyberattacke bewusst ist
- beste Arbeit über Cyberterrorismus vom Center for the Study of Terrorism and Irregular Warfare (CSTIW) gemacht:
    - 1999 Bericht über Perspektiven, dass Terroristengruppen Cybermethoden einsetzen werden
    - Schlussfolgerung: Barriere für Eintritt ziemlich hoch
    - Terroristen fehlen im Allgemeinen die erforderlichen Mittel, einschließlich menschlichem Kapital
- Studie hat ergeben:
    - religiöse Gruppen suchen am wahrscheinlichsten nach fortschrittlichen Möglichkeiten, gefolgt von Ethno-Nationalisten, separatistischen und revolutionären Gruppen
- einer der ernsthaftesten Vorfälle vor einigen Jahren in Australien:
    - gelang Mann, sich in Abwasserkontrollsystem zu hacken und Abwasserströme umzukehren → schädigte Umwelt und vernichtete Tierwelt
    - hatte keinerlei soziale oder politische Absichten
    - war sauer, weil er abgelehnt wurde für Job bei Landkreis, der Abwassersystem betrieb → war seine Rache
    - konnte das durchführen, weil er für Firma gearbeitet hat, die die Software geschrieben hat, und diese mit nach Hause genommen hatte, als er Firma verließ
    - hatte Wissen und Tools, die kein anderer hätte erlangen können
    - 46 Versuche gebraucht das hinzubekommen
    - nicht so einfach, in System einzugreifen, sogar für jemanden, der die Software hatte und wusste, was zu tun war

- ernsthafte Attacke kann nicht einfach von jedem durchgeführt werden
- benötigt wirklich einiges an Insiderwissen
- andererseits: Insider können gekauft werden
- gibt eine Menge Spione, die Informationen an ausländische Regierungen verkauft haben

7. Möglichkeiten zum Schutz vor Cyberattacken

- Sicherheitssysteme, wie Norton Anti-Virus Programm sehr gut, aber muss sie auf neustem Stand halten, weil sich Viren kontinuierlich entwickeln, da Angreifer immer neue Viren schreiben, die Anti-Virus Programm nicht entdeckt
- nicht Outlook für e-mails nutzen
- meisten gewöhnlichen Computernutzer wissen nichts über Firewalls und haben sie nicht
- wenn sie Anti-Virus Programm haben, halten sie es oft nicht auf neustem Stand
- Microsoft und die anderen Firmen können aber nichts ins Betriebssystem einbauen, das in dieser Hinsicht helfen würde, da viele Attacken Anwendungsschicht treffen
- Microsoft in schwieriger Lage: je mehr sie tun, desto mehr Leute sagen, dass sie Markt übernehmen
- jemand hat vorgeschlagen:
    - sollte illegal sein einen Computer zu betreiben ohne seine Anti-Virus Programme auf dem neusten Stand zu halten
    - dass man eines Vergehens für schuldig befunden werden kann, wenn der Computer einen Virus verbreitet und die Anti-Virusprogramme nicht auf dem Laufenden sind
    - sollte man Lizenz wie Führerschein brauchen, um im Internet tätig zu sein, müsste man sie erneuern, nicht einmal aller 3 oder 5 Jahre, sondern aller 2 Wochen oder jeden Monat, um zu zeigen, dass Computer sicher ist
- benötigen immer neuere und bessere Verteidigungsmethoden, weil Hacker neue und bessere Angriffsmethoden erfinden

- brauchen Erfahrungswerte, um gute Schutzpraktiken zu definieren
- Regierung und Industrie sollten aktivere Rolle übernehmen, um Leute zu warnen und sie dazu zu bringen Angriffe der Regierung zu melden, um zu versuchen abgestimmtes Warnsystem zu erhalten
- Industrie selbst hat Information Sharing and Analysis Center (ISACs) errichtet für Meldungen in der Industrie
- braucht Anonymität in den Meldungen, weil sonst Firmen nichts melden würden

8. Fazit

- Cyber-Terrorismus existiert noch nicht
- Amateurhacker bei weitem größte Bedrohung im Internet zur Zeit
- aber: Cyber-Terrorismus wird in Zukunft sicher Bedrohung darstellen

Quellen

- Dorothy E. Denning: Is cyber terrorism coming? http://www.marshall.org/pdf/materials/58.pdf (letzter Zugriff: 26. 3. 2008).

- http://www.kriminologie.uni-hamburg.de/wiki/index.php/Cyber-Terrorismus (letzter Zugriff: 26. 3. 2008).

- Jörg Schieb: Methoden des Cyberterrorismus. http://www.wdr.de/online/computer/cyberterror/terror.phtml (letzter Zugriff: 26. 3. 2008).

- http://de.wikipedia.org/wiki/Denial_of_service (letzter Zugriff: 26. 3. 2008).

- http://www.virenschutz.info/Cyberterrorismus-Techniklexikon-bei-Virenschutz-info_502.html (letzter Zugriff: 26. 3. 2008).

- Statistics on Cyber-Terrorism. http://csciwww.etsu.edu/gotterbarn/stdntppr/stats.htm (letzter Zugriff: 26. 3. 2008).

- http://www.cert.org/stats/fullstats.html (letzter Zugriff: 26. 3. 2008).

- http://www.computerwelt.at/detailArticle.asp?a=113606&n=4 (letzter Zugriff: 26. 3. 2008).