COMPUTERVIREN UND IHR EINSATZ

CHRISTOPH SÜSENS

GRUNDLAGEN DER WIRTSCHAFTSINFORMATIK
FH-FLENSBURG

Agenda

- Computerviren
- Hacker, Cracker …
- Gründe für die Entwicklung
- Verbreitungswege
- Zielgruppen
- Schutzmaßnahmen
- Unternehmen gefährdet, denkbare Angriffsszenarien
- Folgen/Schäden
- Schutzmaßnahmen für Unternehmen
- Viren als politisches Druckmittel
- Viren als unternehmenstechnisches Druckmittel
- Gesetzliche Hürden
- Zukunftsfantasien

Definition

Schadprogramm, das seinen schädlichen Code in fremde Programme einfügt ohne zunächst die Funktionalität zu beeinträchtigen, erst durch einen späteren Zeitpunkt wird der durch das Schadprogramm festgelegte Schaden angerichtet.

Das Computervirus verbreitet sich durch Selbstreplikation und Kopiervorgänge

Quelle: H.R.Hansen Arbeitsbuch Wirtschaftsinformatik

Virenarten

- **Makroviren**: Schädliches Programm (Makro) in einer MS Office Anwendung. Führt zu Beschädigungen der Anwendung, Dateien, Restsystem.
- **Bootsektorvirus**: Angriff auf Bootsektor der Festplatte oder Bios, Partitionssektoren werden befallen und beschädigt
- **Dateivirus**: Greift ausführbare Dateien an, Verbreitet sich durch Ausführen der Datei und ist speicherresistent

Virenarten II

- **Skriptviren**: Virenarten die auf im Internet üblichen Skriptsprachen (JavaScript oder Visual Basic Script) basieren und durch aufrufen von HTML Seiten mit Skriptelementen verbreiten

- **Hoaxes**: Scherzprogramme, welche den User erschrecken oder verwirren sollen, kein Virus, kann aber einen Enthalten als E-Mail Anhang

Virenarten III

- **Trojanisches Pferd**: Gutartiges Programm mit bösen Absichten, zählt nicht zu den Viren, Verbreitung durch Weitergabe, Absicht ausspähen von Daten und ggf. Manipulation

- **Würmer**: Schädliches Programm, welches ohne Wirt-Programm auskommt, Ziel: Verbrauch von Ressourcen (Rechenzeit, Arbeitsspeicher), kann auch Schaden anrichten, Verbreitung durch Reproduktion als Primärziel

Wer produziert Viren

- **Hacker**: Unterscheidung Gute/Böse, Sicherheitslücken sollen aufgedeckt werden um die Internetsicherheit zu erhöhen
- **Cracker**: Absichten meist krimineller Natur, Ziel: Programmcode der Zielsoftware zu manipulieren
- **Script-Kiddies**: Erstellen von Viren, Trojanern, Würmern mit Ziel Chaos zu verbreiten. Tragweite des Handeln oft unbekannt

Gründe der Entwicklung

- Antrieb als Reiz des Verbotenen
- Bosheit
- Schadenfreude
- Jugendlicher Übermut
- Aufmerksamkeit in der Öffentlichkeit
- Finanzielle Absichten
- Imageschaden

Verbreitungswege / Träger

- Datenträger
  (USB-Stick, Diskette, CD/DVD)
- Internet
- E-Mail-Anhänge
- Downloads

- Schädliche Programme:

BAT, COM, EXE, SCR, CMD, PIF, VBS, VXD, CHM

- Schädliche Dokumente:

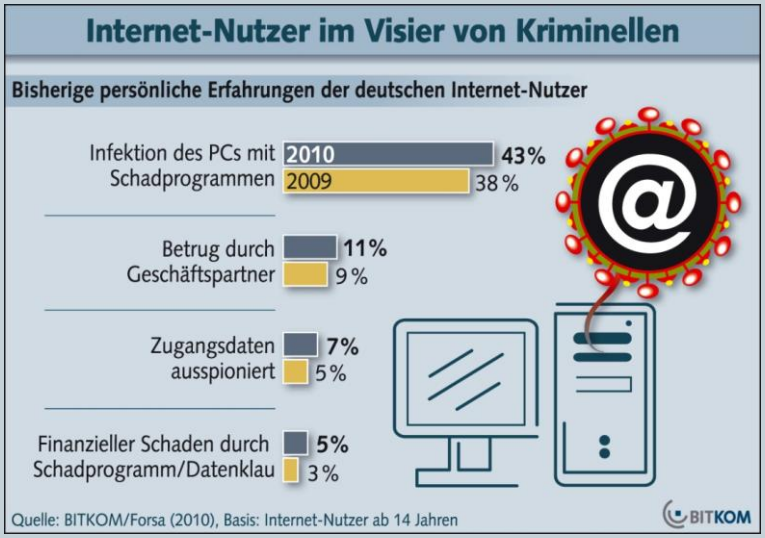
DOC, PPT, XLS, RTF, PDF, MID

- Ungefährliche Dateitypen

JPG, GIF, PNG, BMP, TXT, WIR, ZIP, MP3

Zielpersonen

- Privatpersonen



- Unternehmer
  - Globales Sicherheitsrisiko durch das Internet
  - Totale Vernetzung von Lieferanten und Abnehmer
  - Risiko intern, sowie extern steigt

Schutzmaßnahmen

- Spezielle Betriebssysteme:
  Jedes OS ist angreifbar!

- Antivirensoftware: Software welche über Virensignaturen verfügt und so die Schädlinge ausfindig machen kann. Muss stets aktuell gehalten werden.

- Unbekannte Viren: Antivirensoftware sollte über eine Wahrscheinlichkeitsberechnung verfügen um gleiche Codestrukturen erkennen zu können.

Denkbare Angriffsszenarien auf Unternehmen

- Umleitung von Geldtransaktionen
- Mailzugänge von hunderten Usern blockieren
- Diebstahl von Geschäfts- und Kundendaten (E-Business)
- Verfälschung von Geschäftsdaten ->
- Manipulation der Entscheidungsträger

Folgen durch Virenangriffe

- Zeitverlust
- Kostenanstieg
- Personalkosten Steigung
- Software zur Beseitigung (Lizenzgebühren)
- Wiederherstellung zerstörter Daten bzw. Geräte
- Entgangener Umsatz und verlorene Produktivität durch Systemausfall
- Kosten können in die Millionen gehen
- Jede Virenattake kostet rund 7600 Euro, Beseitigungszeit rund 40 Stunden

Schäden durch Virenangriffe

- Zerstörte Dateien, Festplatten, Hauptplatinen
- Überflutung von Netzwerken, Mailservern (Denail of Service Attake)
- Weiterleitung vertraulicher Daten
- Fälschung der Daten
- Sekundäre Folgen: Vertrauens- und Image-Verlust der betroffenen Organisation

Schutzmaßnahmen f. Unternehmen

- Ausbau von VPN um die Vertraulichkeit, Unverfälschtheit bei Datenübertragungen zu gewährleisten
- Einsatz digitaler Zertifikate / Signaturen
- Benutzerrechte optimal konfigurieren, Stichwort Datenschmuggel, illegale Downloads
- Einsatz von Proxy-Servern, Firewalls
- Datenschutzschulungen Mitarbeiter
- Uptodate bleiben (Hard-/Software)
- Katastrophenpläne anlegen / testen
- Risikoanalyse durchführen

Viren als politisches Druckmittel

- Alle großen kriegsführenden Nationen arbeiten an militärischen Computerviren (Gerüchte)
- Experten sehen Cyberkrieg als eine neue Art der Kriegsführung
- Cyberwar umfasst: Spionage, Defacement, Social Engineering, kompromittierte Hardware, Denail-of-Service Attaken
- Der gläserne Bürger, Vernetzung der Daten, der Staat als Spitzel
- Hacker können Daten klauen und missbrauchen z. B. Erpressung Politiker

Viren als wirtschaftliches Druckmittel

- Trojaner zur Industriespionage
- Mitschnitt von Konferenzen
- Anzapfen der Telefonleitungen
- Video-Kameras
- Abhören des Netzwerkverkehrs
- Wlans besonders gefährdet
- Dienste zeitlich blockieren als Druckmittel für Erpressungsversuche
- Trend geht weg von Massenwürmern, hinzu spezialisierte Schädlinge für gezielte Angriffe

Gesetzliche Hürden

- StGB § 303 Datenveränderung
- UrhG § 95a Schutz technischer Maßnahmen
- StGB § 202c Vorbereiten des Ausspähens und Abfangen von Daten
- StGB § 303b Computersabotage
- StGB § 263a Computerbetrug

Zukunftsfantasien

- Handy/Smartphones werden Zukunftziele der Hacker
- Antivirensoftwarehersteller als das virtuelle Gesundheitswesen von Morgen
- Der Cyberterrorismus im Unternehmensbereich wird stark ansteigen
- Computerviren als Gefährdung des Menschen

  (Google: Erster Mensch mit Computervirus infiziert)

Quellen

- Kampf dem Virus, Wilfred Lindo, Buch Verlag Markt+Technik
- Internet sicher nutzen, Buch Verlag Konsument
- Viren, Würmer & Trojanische Pferde Buch Verlag Data Becker
- Sicherheitsrisiko Internet Buch Verlag dtv
- Internet Spionage Verlag Sybex
- Sicherheit im Internet Verlag bhv
- Arbeitsbuch Wirtschaftsinformatik Aufl. 7 Buch Verlag UTB
- Wirtschaftsinformatik - eine Einführung Buch Pearson Studium
- https://www.sicher-im-netz.de/files/documents/unternehmen/03_01_03_02_Virenmail_Dateitypen.pdf
- Artikel Online-Kriminelle gehen immer raffinierter vor http://www.bitkom.org/65019_65010.aspx
- Artikel Was sagt das Gesetz? http://www.computerviren-info.de/Gesetz.html
- Artikel Stuxnet N-TV http://www.n-tv.de/politik/Stuxnet-wuetet-im-Iran-article1604216.html
- Artikel Zdnet Stuxnet ist ein Propagandatrick des Westens http://www.zdnet.de/news/wirtschaft_sicherheit_security_iran__stuxnet_ist_ein_propagandatrick_des_westens_story-39001024-41538442-1.htm
- Cyberwar Wikipedia http://de.wikipedia.org/wiki/Cyberwar
- Stern Online Angriff der Cyber-Söldner 2007 http://www.spiegel.de/spiegel/print/d-52417831.html

Ende

Vielen Dank