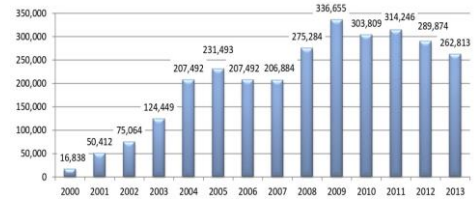
openHPI – Sicherheit im Internet
Risiken im Internet

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Steigende Internetkriminalität erhöht Risiken im Internet

Kommerzielle Nutzung des Internets führt zu einer signifikanten Erhöhung der Anzahl von Computer-Angriffen und kriminellen Aktivitäten

In den USA wurden beim FBI seit dem Jahr 2000 über **3 Millionen** Klagen eingereicht („Internet Crime Complaint Center")



Quelle: FBI IC3 Annual „Internet Crime Report 2013"
http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

Risiken resultieren nicht nur aus der Internet-Nutzung …

Risiken in der digitalen Welt betreffen:

- Computer und Endsysteme selbst
- Verbindung der Computersysteme über das Internet
- Nutzung der Internet-Technologie in Unternehmensnetzwerken - Intranets

Risiken bei Computersystemen …

… bei der **Verarbeitung von elektronischen Informationen** auch ohne jede Verbindung zum Internet:

- Nicht-Verfügbarkeit der Computersysteme oder Datenbanken
- Verlust von Daten, Missbrauch von Daten, Datendiebstahl, ...
- Menschlicher Faktor (meist unbeabsichtigt):
  - falsche oder unvollständige Systemkonfiguration
  - fehlende oder fehlerhafte Datensicherung – „Backup"
  - Schadsoftware über Email-Anhänge oder externe Datenträger
  - fehlerhafte Bedienung, z.B. unbeabsichtigtes Löschen von Dateien
- ...

Risiken bei der Anbindung von Computersystemen ans Internet

- Infiltration von Malware: Viren, Würmer, Trojaner, ...
- Datenverlust: Datendiebstahl, Löschen, Fälschungen, …
- Verlust der Vertraulichkeit: Wettbewerb, Werbung, ...
- Beschädigung des Images in der Öffentlichkeit:
  - Verfälschung der Inhalte von Webseiten
  - Falsche Verwendung von Internet-Adressen durch Dritte
- Sabotage des Systembetriebs und Betriebsstörungen
  - Gezielte Überlastung der Dienste – „Denial of Service"
- …

Risiken im Intranet

Ein vom Internet abgeschottetes Netz, das mit Internet-Technologie betrieben wird, heißt **Intranet**

Sicherheitsrisiken bei Intranets:

- Unberechtigter und unerwünschter Zugriff auf vertrauliche Informationen
  - Leitungsentscheide, Gehaltsinformationen, Personalakten, ….
  - 80% des Missbrauchs von IT-Systemen erfolgt durch eigene Mitarbeiter!
- Zunehmend liegen alle Informationen in elektronischer Form vor
  - Migration der Papier-Form
  - Archivierung, Messaging-Systeme, Voicemail-Systeme, Newsgroups, Videos, ...

Kann man Risiken messen?

Begriffsbestimmung nach ISO 31000:

- Risiken werden in zwei verschiedenen Dimensionen betrachtet:
  - Schadenshöhe und
  - erwartete Häufigkeit
- Risiken bei der Nutzung von Computersystemen und Internet haben sich im Laufe der Jahre in beiden Dimensionen drastisch erhöht

Risikoanalyse erfolgt in 4 Phasen

Phase 1:

- Definition der Analysedomäne
  → Eingrenzung spezifischer Bereiche

Phase 2:

- Beschreibung der Risiken in der Analysedomäne
  → Szenario-basiert, Simulations-basiert

Phase 3:

- Bewertung dieser Risiken
  → Einordnung nach Schadenshöhe und Eintrittswahrscheinlichkeit

Phase 4:

- Interpretation der Ergebnisse

Weitere Risiken bei Nutzung des Internets (1/2)

Risiken, die mit der Datenübertragung in offenen Netzen wie dem Internet verbunden sind:

- Verlust von Nachrichten
- Verfälschung von Nachrichten
- Fälschung des Absenders
- Manipulation und Betrug bei Online-Shopping / Banking
- Illegale oder schädliche Online-Geschäftspraktiken
- Verletzung des Datenschutzes
- Unbestimmtheit der Rechte im Cyberspace
- …

Weitere Risiken bei Nutzung des Internets (2/2)

Fälschung von Nachrichten / Absender

- Ohne besondere Schutzsysteme ist
  - Abfangen,
  - Änderung und
  - Weiterleitung von Emails und Nachrichten mit falscher Adresse im Internet (für Fachmann) leicht möglich
- **Integrität** (Unverfälschtheit) und **Authentizität** (unverfälschter Absender) kann mithilfe der Verschlüsselung und mit geeigneten kryptographischen Verfahren gewährleistet werden

Risiken beim Online-Shopping / Banking

Online-Shopping und -Banking ist heutzutage sehr beliebt

- Transaktionen sind in den meisten Fällen gesichert (verschlüsselte Verbindung, Chipkarte usw.)
- Unzureichende Absicherung der verwendeten PCs bzw. der dort gespeicherten Daten führen zu folgenden Risiken:
  - Diebstahl von Passwörtern
  - Offenlegung der Transaktionen
  - Verwendung von versteckten Programmen, um unbeabsichtigte Transaktionen vorzubereiten
  - …
- Phishing, Pharming (Angriffe mittels gefälschter Emails/Websites) öffnen Angreifer die Tür

Risiken durch illegale/schädliche Online-Geschäftspraktiken

Illegale und schädliche Online-Geschäftspraktiken

- Immer mehr Kriminelle nutzen das Internet wegen seiner Anonymität und breiten Erreichbarkeit
- Bundeskriminalamt beziffert die Zahl der kriminellen Web-Seiten mit mehr als 5 Mio.
  - Illegale Angebote von (gefälschten) Medikamenten und Drogen
  - Online-Casinos – Jahresumsatz wird auf mehr als 2 Milliarden US-Dollar geschätzt
  - Betrügerische Schneeballsysteme
  - Kinder-Pornographie
  - …

Datenschutz

Viele Online-Dienste sammeln persönliche Daten (Adresse, Alter, ...) ihrer Nutzer und erstellen daraus z.B. Interessensprofile, z.B.

- durch Gewinnspiele, kostenlose Angebote und Downloads mithilfe von Registrierungen, Cookie-Mechanismus, usw.
- Oft werden die erhobenen Daten offen gelegt bzw. anderen Anbietern (z.B. Direktmarketing-Agenturen) verkauft ohne ausdrückliche Zustimmung des Betroffenen

Internet-Provider werten Internet-Datenstrom aus. Sie können/ müssen

- alle Verbindungsdaten speichern, inklusive unverschlüsselter Emails, usw.
- sich Informationen über den Verbindungsaufbau für die Versendung der verschlüsselten Datenströme merken

Nationale Rechtsprechung (1/2)

IuKDG - Informations– und Kommunikationsdienstgesetz – schafft Rechtssicherheit im Internet in Deutschland:

- Paragraph 1 der IuKDG definiert Nutzung der elektronischen Informationen und Kommunikationsdienste
- Online-Verträge (Bestellungen, Letter of Intent, etc.) sind rechtsverbindlich
- Paragraph 3 IuKDG bestimmt Voraussetzungen für Anerkennung digitaler Signaturen
- …

Nationale Rechtsprechung (2/2)

§202c StGB ("Hackerparagraph") stellt Nutzung und Entwicklung von möglichen Angriffswerkzeugen unter Strafe

- Problem: Sicherheitsüberprüfungen und Bildung (Lehre und Ausbildung) nutzen auch solche Werkzeuge!

Aber grundlegendes Problem:

- Globale Kommunikation – nationale Rechtsvorschriften …

Nationale Rechtsprechung (2/2)

§202c StGB ("Hackerparagraph") stellt Nutzung und Entwicklung von möglichen Angriffswerkzeugen unter Strafe

- Problem: Sicherheitsüberprüfungen und Bildung (Lehre und Ausbildung) nutzen auch solche Werkzeuge!

Aber grundlegendes Problem:

- Globale Kommunikation – nationale Rechtsvorschriften …

Risiken im Internet | Sicherheit im Internet | Prof. Dr. Christoph Meinel 15