Zürcher Hochschule
für Angewandte Wissenschaften
zh aw School of Engineering
INE Institut für
Nachhaltige Entwicklung

IT-Security-Fallstudien

Ralf Mock, 21. September 2015

Lernziele: Einführung

Die Studierenden ...

- kennen einige IT Security Fallstudien
- können die Ergebnisse einordnen

Hospital

- **Im Hospital:** Ein Botnetz machte sich bemerkbar. Alle IT-Systeme scheinen in Ordnung
- **Komponente**: Eine tagelange Suche durch (externe) IT-Experten identifizierte eine Herz-Lungen-Maschine mit integriertem PC als Quelle.
- **Hintergrund**: Die Hospital-Ausrüstung wurde vernetzt (elektr. Patientenakte ...)
- **Hauptursache**: Die verantwortliche Person wusste nicht, dass hierbei eine Internet-System betrieben wurde

Fallstudien

Wasserwerke

- **Angriffe**
  - Ein Hacker übernimmt die Verantwortung für das Eindringen in das Computersystem eines Wasserwerkes in Texas
  - Ein anderer Eindringling tat das gleiche einige Tage zuvor in Illinois
- **Behörde**
  - Davor haben Vertreter von US-Behörden das Risiko solcher Angriffe heruntergespielt.

Quelle: [5]

Fallstudien

Stuxnet

- **Angepasst**: Beispiel die Bedrohung, eine best. industrielles Steuersystem ins Visier zu nehmen
- Die **Verbreitung** beobachteter Infektionen „...umfasst 40 0000 spezifische IP-Adressen aus über 155 Ländern“
- **Ziel**: Die infizierten Computer „...sind typische Windows-Computer, die aber zum Programmieren genutzt wurden ...(PLCs) “ (Industrielle Notebooks)
- Ursprüngliche **Infektionsquelle**: Wechseldatenträger

Quelle: [6]

IT Security in KMU

UK Survey	UK GFI	German BSI	Canadian survey
▪ Published: 2010 ▪ Online questionnaire ▪ 539 respondents ▪ Main group: M	▪ Published: 2009 ▪ Interviews ▪ 269 participants ▪ Main group: S	▪ Published: 2011 ▪ Interviews ▪ 30 participants ▪ Main group: S, M	▪ Published: 2011 ▪ Interview (telephone) ▪ 502 participants ▪ Main group: S, M
Technical Aspects			
Top rated breach System failure, data corruption ▪ Cause the worst security incident ▪ Most disruptive to business	**Top rated risk** Accidental data corruption	**Critical systems** Redundancy implemented to a 50% level	-

Quellen:

- Zusammenstellung aus [7]
- UK Survey: [3]
- UK GFI: [1]
- German BSI: [4]
- Canadian Survey: [2]

Literaturübersicht: IT Security in KMU

UK Survey	German BSI	Canadian Survey
Business Continuity		
Worse system failures ▪ Rarely experienced ▪ Important to system reliability, operability	**Internet security breach** ▪ Rarely experienced ▪ Affects on business operation	**Internet security breach** ▪ Mainly lost time and productivity ▪ Loss of revenue, profit
Risk Assessment		
Security ▪ Carried out by most organisations ▪ Framework: ISO 27001	**Business processes** ▪ Security measurements, incl. IT education, are implemented in higher than average ▪ Significant weaknesses in hazard assessment	-

Literatur

[1] *The GFI SME software security report (GFI white paper).*
GFI, 2009.
http://www.gfi.nl/documents/articles/SME_UK_survey_results.pdf.

[2] *Canadian SME IT Security Survey.*
Trend Micro, Environics, 2011.
http://ca.trendmicro.com/imperia/md/content/ca/environics_-_trend_micro_it_security_-_final_report_-_jul_18-2011.pdf.

[3] BERR: *Information Security Breaches Survey 2010.*
Technical Report, Commissioned by Infosecurity Europe, London, 2010.

[4] BSI: *Kleine Studie zur IT-Sicherheit in kleineren und mittleren Unternehmen.*
Technical Report, Bundesamt für Sicherheit in der Informaionstechnik, BSI, Bonn, 2011.

[5] E., Mills and Beiersmann S.: *Hacker greift texanisches Wasserwerk an.*
ZDnet, NetMediaInteractive, Nov. 21, 2011,.
http://www.zdnet.de/news/41558114/hacker-greift-texanisches-wasserwerk-an.htm, visited: Jan. 9, 2014.

[6] Falliere, Murchu L O and Chien E: *W32.Stuxnet Dossier.*
Technical Report 1.4, Symantec Corporation, Cupertino, 2011.
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[7] Mock, R., O. Stern, R. Knaack and Kollmann E.: *Higher Education in Informatics: Concepts and Lessons Learnt.*
In *PSAM 11/ESREL 12*, Helsinki, Juni 2012.