

Awareness



Sicherheitslücken live aufgedeckt

Niklas Heibel

heibel (at) internet-sicherheit . de

Markus Linnemann

linnemann (at) internet-sicherheit . de

Institut für Internet-Sicherheit

<https://www.internet-sicherheit.de>

Fachhochschule Gelsenkirchen



- **Internes Hochschulinstitut**
 - Gegründet Mai 2005 mit Herrn Schily
 - Leitender Direktor: Prof. Dr. Norbert Pohlmann
- **Fachbereichsübergreifendes Institut** (als Voraussetzung)
- **Schwerpunkt IT-Sicherheit und verteilte Systeme**
 - Sichere Betriebssysteme (Turaya)
 - Internet-Frühwarnsysteme
 - E-Mail-Sicherheit
- **Mitarbeiter (ca. 35)**
 - Festangestellte Dipl.-Informatiker
 - Hiwi's im Studium
 - Diplomanden (Bachelor, Master)

Wo fängt Sicherheit an...

Die Welt wird nicht bedroht von den Menschen, die böse sind, sondern von denen, die das Böse zulassen.

Albert Einstein
14.03.1879 - 18.04.1955
deutscher Physiker und Nobelpreisträger

- ***Auszug aus suanzeigen.de / BBC:***
 - Biete Botnet inkl. einschlägiger Software stundenweise, 100.000 Rechner angeschlossen, IRC-Zugangsdaten nach Zahlung von 500 Euro auf E-Gold 123456789. Als Memo bitte E-Mail angeben. - Kosten hänge dabei von Größe und Nutzungsdauer ab
 - Nach Auffassung von Vinton Cerf Vice President von Google seien von den 600 Millionen Internet-PCs 100 bis 150 Millionen mit Bots infiziert.

Schutz vor Trojaner-Angriffen

Basissicherheit:

- Betriebssystem immer absolut aktuell halten
- Aktuelle Anti-Virensoftware
- Aktuelle Firewall
- Aktuelle Anti-Spy Software

Fortgeschrittene Sicherheit:

- Virtualisierung beim surfen einsetzen
- Keinen Internet Explorer verwenden, sondern Firefox, Opera, ..

Warum IT-Sicherheits-Schulungen

- **Tausche Passwort gegen Zartbitter**
 - Für Schokolade tun Frauen fast alles. Zumindest ihre Passwörter verraten sie gerne für eine Tafel Ritter-Sport an einen Fremden.
- **Frauen gehen leichtfertiger mit Passwörtern um**
 - 45 Prozent der weiblichen Büroangestellten
 - 10 Prozent der männlichen Büroangestellten
 - Versuch von Infosecurity Europe <http://www.infosec.co.uk> in London

→ **Aber Warum ???**

Passwortraten (1/2)

Passwortlänge	benötigte Zeit	
	68 unterschiedliche Zeichen	94 unterschiedliche Zeichen
1	8.5 Mikrosekunden	11.75 Mikrosekunden
2	0.58 Millisekunden	1.10 Millisekunden
3	0.39 Sekunden	0.10 Sekunden
4	2.67 Sekunden	9.76 Sekunden
5	3.03 Minuten	15.29 Minuten
6	3.43 Stunden	23.95 Stunden
7	9.73 Tage	93.82 Tage
8	1.81 Jahre	24.14 Jahre
9	123.14 Jahre	2260 Jahre
10	8370 Jahre	213350 Jahre
11	569380 Jahre	10.05 Millionen Jahre
12	38.72 Millionen Jahre	1.89 Milliarden Jahre

Mit freundlicher Genehmigung von Tobias Schrödel www.sichere.it

Passwortraten (2/2)

Wie baue ich ein gutes Passwort:

- Lang (mehr als 8 Zeichen)
- Groß und Kleinschreibung
- Ziffern verwenden
- Sonderzeichen verwenden
- Regelmäßig ändern
- Sinnfreie Zusammensetzung

Schlechtes Passwort:

- Geheim

Ein gutes Passwort:

- 3kDmAr8kLkL!



- Aktuelle Handys → Virens Scanner verwenden
- Verbindungen, die NICHT gebraucht werden → **Ausschalten**
- Headsets bei nicht-Gebrauch → **Ausschalten**
- In sicherheitskritischen Umgebungen → Handy **auschalten**
- Bluetooth im Handy unsichtbar schalten

→ Ultimativer Schutz: **Alles Ausschalten**

(scherzhaft gemeint,

neue Technologien sollten genutzt

werden, aber mit gebotener Vorsicht)



- Immer verschlüsseln
- **Sämtliche** nicht verschlüsselte **Informationen** können **einfach mitgelesen** werden (sniffen)
- ***Sichere Verschlüsselung wählen***
 - **Kein** WEP, da es sehr schnell zu knacken ist
 - Bedingt **WPA**
 - Am besten **WPA2** mit AES Verschlüsselung
- ***WLAN ist nicht nur Kurzstrecke***
 - Einfache Richtfunkantennen erzielen **Reichweiten bis 2 km**

Phishing & Pharming (1/2)

→ Wie sieht die Bedrohung aus?

■ **Phishing**

- Angriff durch Täuschung, Umleitung auf gefälschte Inhalte
 - Über Links in E-Mails
 - Java-Skript in Auktion einbauen
 - Einfache Links in Artikelbeschreibung fälschen
 - XSS (Cross Site Scripting) als Phishing-Technik



■ **Pharming**

- DNS (Domain Name Server) – Attacken über
 - Hosts – Datei des Clients
 - Kapern von DNS-Servern
 - DNS Flooding gegen den Client



Phishing & Pharming (2/2)

→ Welche Vorkehrungen gibt es dagegen

- URL per Hand eingeben (bei Pharming nutzlos)
- SSL Zertifikate überprüfen
- Links überprüfen (bei Pharming nutzlos),
- Hosts Datei Schreibschutz aktivieren
- Anbieter überprüfen

→ ***Mit Bedacht am Rechner arbeiten***



Basissicherheit und Datenschutz

- <http://www.internet-sicherheit.de/service/tipps-zur-sicherheit/>
- www.bsi-fuer-buerger.de
- www.sicher-im-netz.de

Grundschutz für die Firma (Angebot der secure IT NRW)

- Basisprüfung IT-Sicherheit
 - (<http://www.secure-it.nrw.de/service/bits.php>)

Wo fängt Sicherheit an...

***Wer die Freiheit aufgibt, um Sicherheit zu gewinnen,
wird am Ende beides verlieren.***

Benjamin Franklin
17.01.1706 - 17.04.1790
US-Staatsmann, Ökonom und Naturforscher

Wir möchten sie sensibilisieren !!!

- Wir zeigen Ihnen alle Vorführungen ausschließlich **um sie zu sensibilisieren!**
- Definitiv wollen wir **niemanden anstiften** eine Straftat zu begehen!
- Alle Informationen und Aktionen dienen dazu, Ihnen die Möglichkeit zu eröffnen, sich **zu schützen!**

Awareness



Vielen Dank für Ihre Aufmerksamkeit

www.internet-sicherheit.de

Fragen ?

Niklas Heibel

heibel (at) internet-sicherheit . de

Markus Linnemann

linnemann (at) internet-sicherheit . de

Institut für Internet-Sicherheit

<https://www.internet-sicherheit.de>

Fachhochschule Gelsenkirchen

