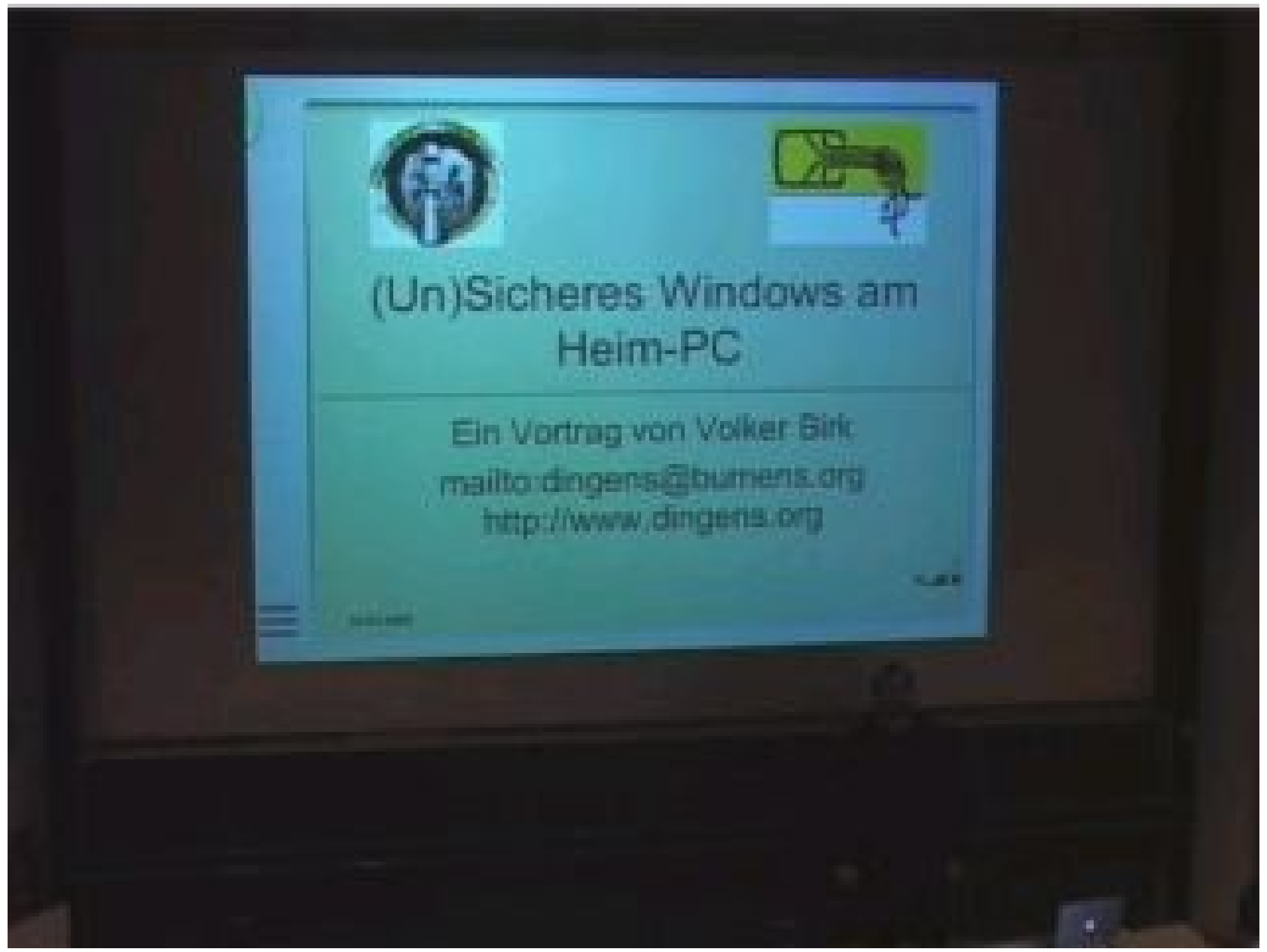
(Un)Sicheres Windows am Heim-PC
Ein Vortrag von Volker Sirk
mailto:dingens@bumens.org
http://www.dingens.org

W-insecure - das Problem.

- Viren, Würmer, Mailwürmer
- Dialer
- Scriptkiddies, Cracker, „böse" Firmen
- Spyware, trojanische Pferde, Fernsteuerungssoftware

- Was wollen die alle auf meinem PC?

Ich will doch bloß...

- „Surfen“
- Mailen
- Internet Banking
- Spielen
- ...

Die Werbung sagt:

- „Personal Firewalls“
- Virenscanner
- Spyware Removal Tools
- „Sicherheitspakete“
- Ein Milliardenmarkt!

- Machen die mich sicher?

„Personal Firewalls“

- Manche „Personal Firewalls“ machen den PC von außen sicherer.
- Keine „Personal Firewall“ macht den PC von innen sicherer.
- Viele „Personal Firewalls“ machen den PC aber unsicherer.
- Alle „Personal Firewalls“ machen den PC potentiell unsicherer.

Virenscanner

- Virenscanner erkennen viele Viren, bevor diese zuschlagen.
- Kein Virenscanner erkennt alle Viren, bevor sie zuschlagen.
- Kein Online-Virenscanner ist zuverlässig, sobald ein Virus zugeschlagen hat.
- Kein Offline-Virenscan erkennt alle Viren.
- Virenscanner bieten keine Garantie zur Virenfreiheit.

Spyware Removal Tools

- Kein SRT erkennt Spyware zuverlässig.
- Ist ein Computer erst mal kompromittiert, so hilft nur die Neuinstallation.
  - http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.mspx
- Wie kann ich das verhindern?

Wie machen die das? (1/2)

- Computer führt Programme aus.
- Angriffsmöglichkeit: Programme unterschieben: z.B. Viren, Mailwürmer.
- Computer führt abhängig von Daten andere Programme aus.
- Angriffsmöglichkeit: geeignete Daten unterschieben: z.B. Windows-Nachrichten-Fernsteuerung, wwwshell.

Wie machen die das? (2/2)

- PCs trennen nicht fest zwischen Daten und Programmen.
- Angriffsmöglichkeit: Daten unterschieben und als Programme „umdeklarieren“ und ausführen: Buffer-Overflow-Attacks, Shatter-Attack.

Wie soll ich mich verhalten?

- Führe nur Programme aus, bei denen Du dem Autor und der Quelle vertraust.
- Empfange möglichst Daten, die keine Programme beinhalten können; kein Scripting in Mails, keine Office-Dateien.
- Verwende Programme, die strikt zwischen Daten und Programm trennen; kein Internet Explorer, kein Outlook Express.

Wie soll ich mich verhalten?

- Schalte die „versteckte" Kommunikation Deines Windows-PC ab; http://ntsvcfg.de http://www.dingens.org
- C:\> netstat -ano
- 127.0.0.1 ABHÖREN => OK.
- 0.0.0.0 ABHÖREN => Kommunikation nach außen.
- 123.23.42.23 ABHÖREN => Kommunikation nach außen.

Wie soll ich mich verhalten?

- Schütze Deine Computer vor dem Netz; „Firewalls" in Form von NAT mit Filter auf einem extra Gerät ist sehr sinnvoll!
- Schütze Deine Computer vor dem Nutzer: Arbeite NICHT als Administrator!
- Schütze Dein WLAN: WEP ist total unsicher, nimm WPA oder ein VPN.

Wie soll ich mich verhalten?

- Mehr Sicherheit gibt's durch weniger Programme.
- Mehr Sicherheit gibt's durch weniger Kommunikation; Computer und Telefon trennen. DSL hilft.
- Verwende Formate für Daten, die keine Programme enthalten können.
- Wähle Programme, die eine gute Historie haben in Sachen Umgang mit Fehlern.

Wie soll ich mich verhalten?

- Mißtraue dem Netz.
- Niemand bietet Dir pr0n umsonst per Mail an.
- Niemand fragt Dich per Mail nach Deinem Kennwort oder gibt Dir ein neues.
- Niemand überweist Dir „einfach so" Geld.
- Kostenlose pr0n im Netz ohne Gefahr ist schwer zu finden (mit Ausnahme der Usenet Binary Groups), wenn Du's nicht kannst, kaufe Dir pr0n.

Wie soll ich mich verhalten?

- Halte Deine Arbeitssoftware aktuell!
- Es gibt http://windowsupdate.microsoft.com
- Es gibt http://officeupdate.microsoft.com
- Dafür taugt Internet Explorer.
- Halte auch alle andere Software ständig aktuell, wie z.B. Deinen Browser Mozilla Firefox! ;-)

Ich wurde geknackt!

- Vergiss Removal-Tools.
- Vergiss Computer-Forensik.
- Du hast keine Chance als Otto-Normalbenutzer.

- Halte ein regelmäßiges Backup Deiner Daten bereit.
- Mach die Kiste vollständig platt und spiele Dein Backup zurück.

Passwörter

- Beispiel: bw$EfdSxtv
- Mehr als 8 Zeichen => kein Durchprobieren (brute force).
- Willkürlich. Keine Worte. => kein Wörterbuchangriff.
- Auch kein „Vorwärts/Rückwärts-Trick"!
- Verwende nicht das Beispiel! ;-)
- Speichere alle bis auf ein Kennwort hier: http://truecrypt.sourceforge.net.

Verwende Kryptographie!

- Mozilla Thunderbird + Enigmail + GPG und niemand liest die E-Mail einfach mit.
- SCP und SFTP statt FTP; DSA
- https:// - SSL für HTTP.
- VORSICHT: SSL ist ohne Überprüfung des korrekten Gesprächspartners wirkungslos!

  Niemals einfach „OK" bei SSL!

Muss Windows sein?

- Kauf einen Mac. Für OSX sind bisher 0 (in Worten: „Null") Viren bekannt.
- MacOS X ist nicht absolut sicher!
- Geh zu einer LUG oder einem BSD-Userclub. Freie Software regelt und sieht mit KDE aus wie Windows.
- Linux ist nicht absolut sicher!
- Nimm ein System, das Du beherrscht.

Viel Spass am Gerät!

Volker Birk, Chaostreff Bad Waldsee
CCC ERFA Ulm.

http://fdik.org http://www.dingens.org
http://chaostreff.dingens.org
http://www.ulm.ccc.de
mailto:dingens@bumens.org