Datensicherheit und Datenschutz

Wie schützt man den eigenen Computer und die eigenen Daten vor Angriffen?

nr-Jahrestreffen 2011 – Hamburg – 01./02. Juni 2011

Ziele dieses Workshops

Nach diesem Seminar kennen Sie:

1. Die Problematik der Rechner- und Kommunikationssicherheit
2. Methoden, um Sicherheit zu erhöhen
3. Werkzeuge, um Sicherheitslücken zu schließen

Sicherheit ist nicht bequem!

Ausgangslage

Schutz der eigenen Daten

ist eine Aufgabe, die nicht delegiert werden kann,

da dies bereits einen Bruch der Vertraulichkeit bedeutete.

Die Bedrohungslage

Was kann passieren?

- ✓ Datenverlust durch Schäden (z.B. Festplattencrash)
- ✓ Kompletter Verlust des Computers / Speichermediums durch Brand / Diebstahl / Beschlagnahme
- ✓ Krimineller Angriff aus dem Netz / Online-Durchsuchung

Mögliches Angriffs-Szenario (1)

alt (2000)

Keystoke-Logger (physikalisch)

neu (2008)

Keystoke-Logger (virtuell)

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

1. Erstellung von Verzeichnisübersichten, Durchsuchen von Verzeichnissen nach bestimmten Dateinamen, Volltextsuche nach Stichworten

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

2. Durchsuchen angeschlossener Datenspeicher (USB-Sticks, CDs/DVDs, Flash-Memory, externe Festplatten, zugängliche Netzwerk-Laufwerke/Server-Laufwerke)

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

3. Herunterladen von ausgewählten Dokumenten (Texte, Bilder, ...)

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

4. Tastatur-Logger (Protokollierung aller Tastaturanschläge)

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

5. Protokollierung von Internetzugriffen (URL, Datentransfers, Verweildauer, ...)

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

6. Passwort-Protokollierung (Web-Dienste, Entschlüsselung von Daten etc.)

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

7. Übermittlung des vollständigen Bildschirminhalts ("Screen-Shots")

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

8. Abfangen von gesendeten und empfangenen elektronischen Nachrichten (nach Angaben des BMI Teil einer "Quellen-Telekommunikationsüberwachung")

Mögliches Angriffs-Szenario (2)

Geplant im Rahmen der "Online-Durchsuchung" (BKA-Gesetz):

9. Raumüberwachung (Aktivierung des Rechnermikrofons, Aktivierung einer angeschlossenen Web-Kamera; nach Angaben des BMI nicht geplant)

Methoden und Ziele von Angriffen

- ✓E-Mails - Viren, Schadsoftware, Botnetze
- ✓Webseiten - Schadsoftware, Botnetze
- ✓infizierte PDFs

- ✓Überwachung
- ✓Nutzung des eigenen PC (Spam-Versand / Speicherung)
- ✓Ausspähen verwertbarer Daten (Kontoinformationen)
- ✓Erpressung (Verschlüsselung, Entschlüsselung gegen Geld)
- ✓Ausspähung (Gegenrecherche)

Mögliches Angriffs-Szenario (3, ot)

Moderne Kopierer

- haben Festplatten
- haben Netzwerkanschlüsse
- Bringen Codierungen auf jedem Farbausdruck an

Moderne Drucker

- sind via E-Mail ansprechbar
- haben Netzwerkanschlüsse
- Bringen Codierungen auf jedem Farbausdruck an

http://www.eff.org/Privacy/printers/docucolor/index.php

Das Schutz-Paradox

Der Staat will unsere Daten, muss aber Datensicherheit garantieren.

Eine gute Richtschnur bietet die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), z.B. der G 5 Gefährdungskatalog "Vorsätzliche Handlungen".

BSI: IT-Grundschutz-Kataloge:

www.bsi.bund.de/gshb/index.htm

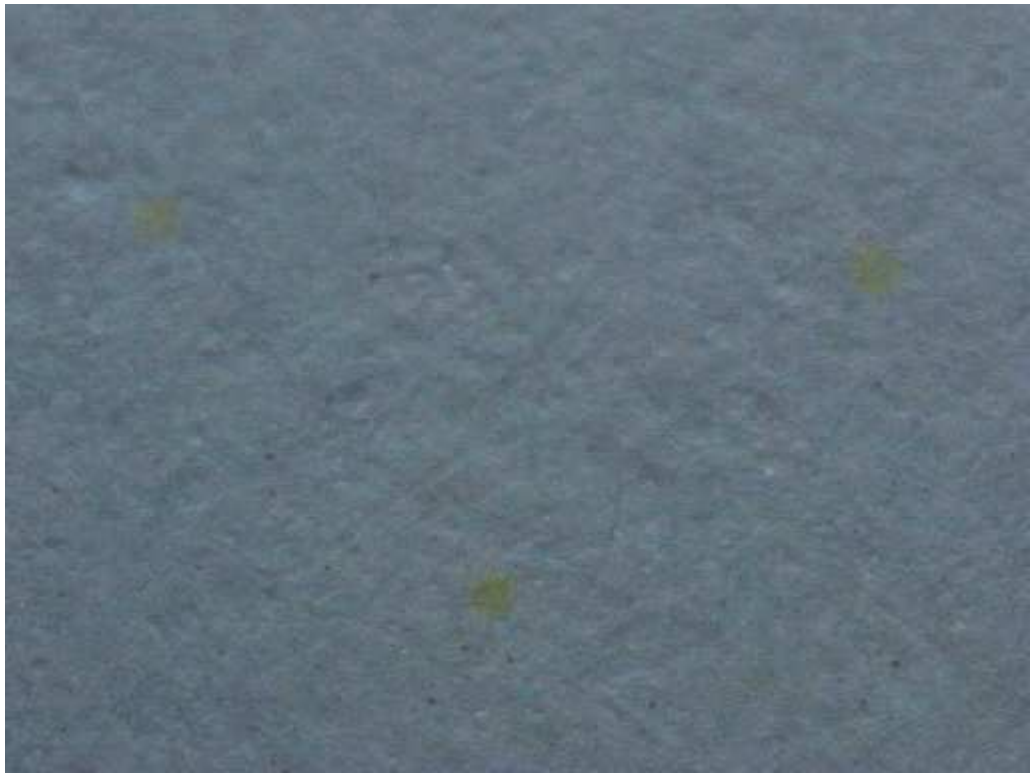
BSI: G 5 – Gefährdungskatalog Vorsätzliche Handlungen:

www.bsi.bund.de/gshb/deutsch/g/g05.htm

Versteckte Codierungen auf Farbausdrucken / -kopien

Originalansicht

Versteckte Codierungen auf Farbausdrucken / -kopien

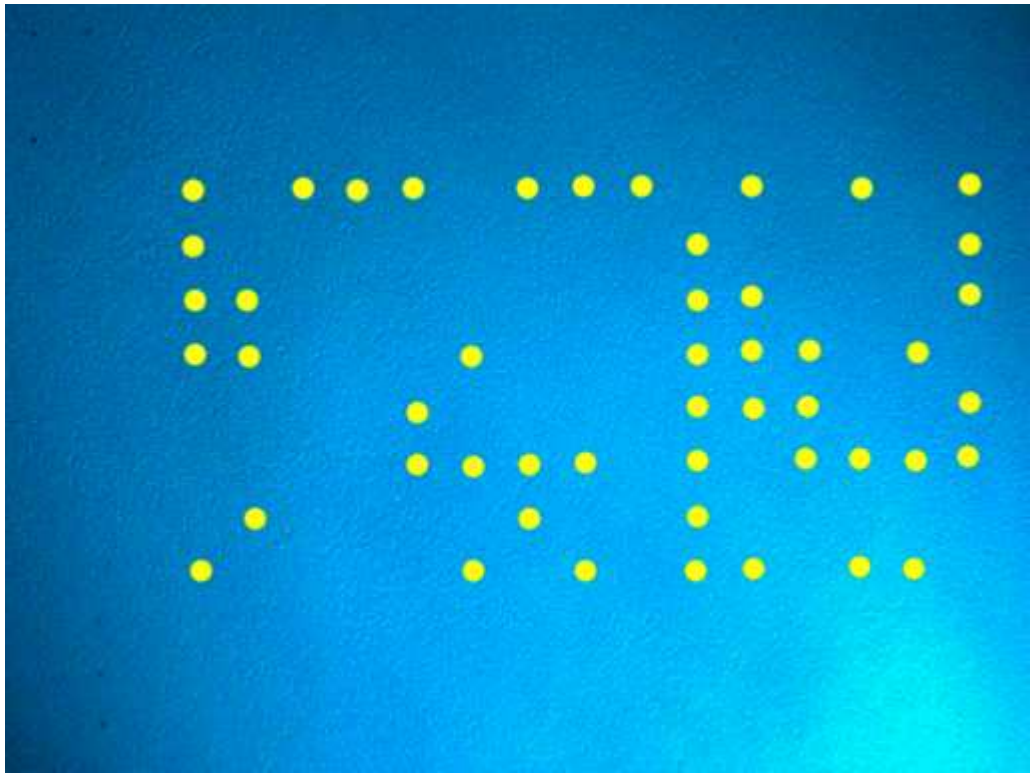


Vergrößerung: gelbe Punkte

Versteckte Codierungen auf Farbausdrucken / -kopien

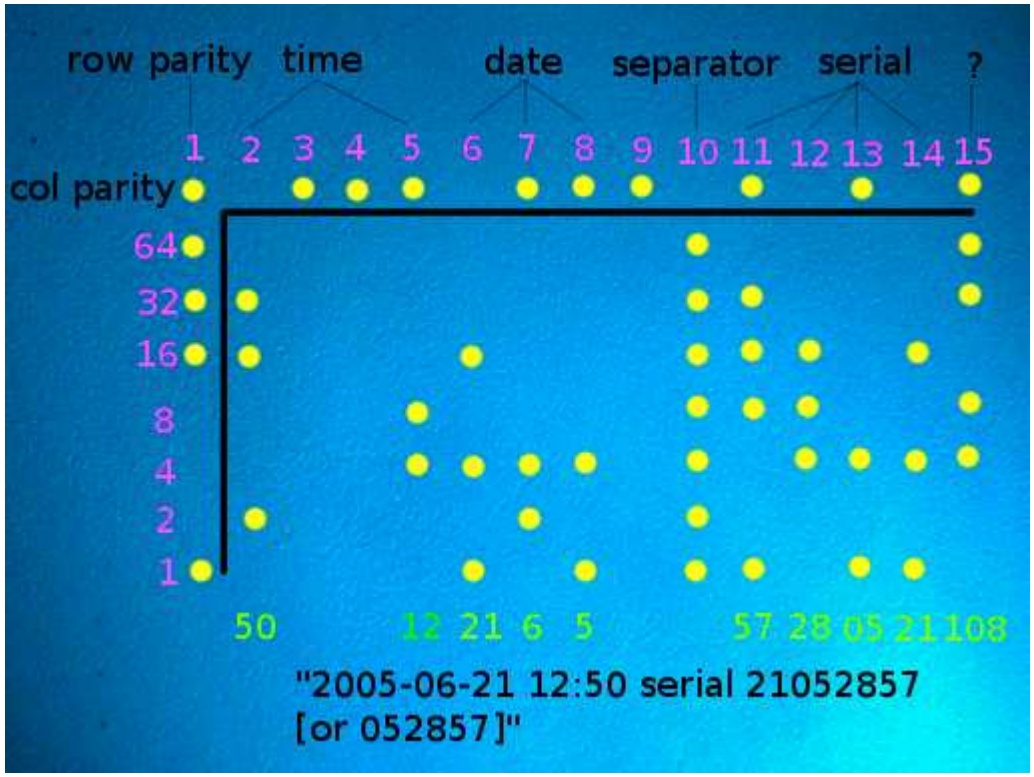
Ansicht in anderer Belichtung

Versteckte Codierungen auf Farbausdrucken / -kopien



Die Punkte ergeben ein Muster

Versteckte Codierungen auf Farbausdrucken / -kopien



Dieses Raster enthält Seriennummer des Gerätes

und Timestamp des Ausdruckes

Was tun?

Organisationsebene:

- ✓ Schutz der Netze, Wecken von Sicherheitsbewußtsein
- ✓ Roter Ordner, Whitepapers

Was tun?

Organisationsebene:

- ✓ Schutz der Netze, Wecken von Sicherheitsbewußtsein
- ✓ Roter Ordner, Whitepapers

Individuelle Ebene:

- ✓ Schutz der Computer und der Daten
- ✓ ... und der Kommunikation / Kontakte

Was tun?

Organisationsebene:

- ✓ Schutz der Netze, Wecken von Sicherheitsbewußtsein
- ✓ Roter Ordner, Whitepapers

Individuelle Ebene:

- ✓ Schutz der Computer und der Daten
- ✓ ... und der Kommunikation / Kontakte

Datensicherung, Verschlüsselung, Anonymisierung, Pseudonymisierung

... und nicht immer die ganze Wahrheit sagen!

Grundlegende Ziele

Rechnersicherheit

1.) Jederzeit eine saubere Installation
2.) Jederzeit unkorrumpierter Zugriff auf die eigenen Daten
3.) Jederzeit ein arbeitsfähiges System

Datensicherheit und Kommunikationssicherheit

Die eigenen Daten und die eigene Kommunikation sind

1.) unverändert
2.) unbeobachtet
3.) jederzeit verfügbar

1.) Eigenen Rechner sichern

Schutz vor Zugriff via Netz (z.B.Online-Durchsuchung)

"Tatsächlich sind keine Möglichkeiten bekannt, eine Online-Durchsuchung so zu gestalten, dass ein Zielsystem nicht wirksam davor geschützt werden kann."

1.) Eigenen Rechner sichern

Schutz vor Zugriff via Netz (z.B.Online-Durchsuchung)

"Tatsächlich sind keine Möglichkeiten bekannt, eine Online-Durchsuchung so zu gestalten, dass ein Zielsystem nicht wirksam davor geschützt werden kann."

Stellungnahme zur "Online-Durchsuchung" - Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07 / von Dirk Fox, Secorvo Security Consulting GmbH

Version 1.1, Stand 29. September 2007

http://www.secorvo.de/publikationen/stellungnahme-secorvo-bverfg-online-durchsuchung.pdf

1.) Eigenen Rechner sichern

Empfehlungen von
Dirk Fox, BVerfG-Stellungnahme, 4.2 :

Verhinderung der Installation der Durchsuchungssoftware

1.) Patchen des Betriebssystems
2.) Restriktive Konfiguration des Systems
3.) Restriktive Konfiguration des Browsers
4.) Nutzung eines Virenscanners
5.) Sicherheitssensibler Umgang mit E-Mails
6.) Nutzung einer Personal Firewall
7.) Einsatz "Virtueller Maschinen"

1.) Eigenen Rechner sichern

Weitere Empfehlungen von mir

8.) Regelmäßige Backups
9.) Image-Programme
10.) Speichermedien verschlüsseln
11.) Informiert bleiben

1.) Eigenen Rechner sichern

1.) Patchen des Betriebssystems

Sicherheitsupdates ("Patches", Flicken) werden von den Herstellern bereitgestellt.

Installieren Sie diese regelmäßig.

(entweder automatisch oder nach Benachrichtigung)

1.) Eigenen Rechner sichern

Gleiches gilt für alle eingesetzen Programme:

Jedes Programm hat Fehler und Lücken

Werden Lücken ("expolits") bekannt ("zero day"), sollten die Hersteller zeitnah die Lücken stopfen ("patches").

Patches und Updates regelmäßig einspielen

Mindestens für automatische Benachrichtigung sorgen!

1.) Eigenen Rechner sichern

Tipp zur Aufteilung der internen Festplatte:

Aufteilung der eigenen Festplatte in mehrere Partitionen:

1.) für Betriebssystem und Programme (Sicherung mit Image)
2.) für Daten (Sicherung mit Backup, Mirror)
3.) ggfs. Archiv

1.) Eigenen Rechner sichern

2.) Restriktive Konfiguration des Systems

Richten Sie mehrere Accounts ein.

Nutzen Sie den Administator-Account (höchste Berechtigungsstufe) nur offline für Installationsarbeiten.

Gehen Sie nur mit einem Nutzer-Account (der keine Programme installieren darf) ins Netz.

1.) Eigenen Rechner sichern

3.) Restriktive Konfiguration des Browsers

Empfehlung:
Firefox und die Firefox Addons
http://www.mozilla-europe.org/de/firefox/
https://addons.mozilla.org/de/firefox/

Dieser Webbrowser hat - gut konfiguriert - das höchste Sicherheitsniveau

1.) Eigenen Rechner sichern

3.) Restriktive Konfiguration des Browsers

Firefox-Erweiterungen für sicheres und ungestörtes Surfen

- ✓ z.B. NoScript : Konfiguration der Javascripts für die jeweilige Website

  Sehr guter Schutz gegen "Cross-Site Scripting" und "Drive-by Downloads", also infizierte Webseiten!
- ✓ z.B. HistoryBlock : Gegen Tracking (unbemerktes Auslesen) der History.

... es gibt noch mehr davon - s. Linkliste.

1.) Eigenen Rechner sichern

4.) Nutzung eines Virenscanners

Setzen Sie stets ein Antivirenprogramm ein und aktualisieren Sie es regelmäßig. Ein Antivirenprogramm, dessen Signaturdatei (anhand derer es Viren erkennt) über einen Monat alt ist, bietet keinen ausreichenden Schutz mehr.

Da auch Virenscanner Lücken haben können, sollten Sie gelegentlich das Programm wechseln. Verwenden Sie auch ein Programm gegen Spionageprogamme ("Spyware").

Software-Archiv des Heise-Verlages

http://www.heise.de/software/default.shtml?kat=176

1.) Eigenen Rechner sichern

5.) Sicherheitssensibler Umgang mit E-Mails

Unterbinden Sie den Empfang von E-Mails im HTML-, im DOC- oder im RTF-Format.

Lesen Sie E-Mails (zunächst) nur im Textformat.

Damit verhindern Sie das Ausführen von Schadcode und Spionage durch das Nachladen von Dateien .

Wo möglich, lesen Sie E-Mails nur offline, so dass keine Dateien unbemerkt aus dem Netz geladen werden können.

1.) Eigenen Rechner sichern

5.) Sicherheitssensibler Umgang mit E-Mails

Gehen Sie besonders vorsichtig mit Downloads und Dateianhängen von Mails (Attachments) um. Löschen Sie unverlangte oder nicht beschriebene Anhänge unverzüglich (ggfs. beim Absender nachfragen)

Öffnen Sie Dateien mit Viewern (die keine Makros ausführen können) statt mit den Programmen (Word, Acrobat) selbst.

http://www.microsoft.com/downloads/details.aspx?familyid=3657CE88-7CFA-457A-9AEC-F4F827F20CAC&displaylang=de

http://pdfreaders.org/

1.) Eigenen Rechner sichern

5.) Sicherheitssensibler Umgang mit E-Mails

Online Sicherheitscheck des Heise-Verlages
http://www.heise.de/security/dienste/emailcheck

1.) Eigenen Rechner sichern

5.) Sicherheitssensibler Umgang mit E-Mails

Empfehlung:

Thunderbird und die Thunderbird-Addons

http://www.mozillamessaging.com/de/thunderbird/

https://addons.mozilla.org/de/thunderbird/

Dies Mailprogramm ermöglicht die Einbindung von sicherheitsrelavanten Programmen und Verschlüsselungswerkzeugen.

1.) Eigenen Rechner sichern

6.) Nutzung einer Personal Firewall

Eine Firewall überwacht alle Außenkontakte Ihres Rechners. Konfigurieren Sie die Firewall scharf:

Kein Außenkontakt ist erlaubt, außer jenen, die Sie explizit gestatten (z.B. Webbrowser und Mailprogramm).

Umfangreicher Eintrag zu Firewalls im Wiki des Hackerboard:

http://wiki.hackerboard.de/index.php/Firewall

1.) Eigenen Rechner sichern

7.) Einsatz "Virtueller Maschinen"

Wird das Zielsystem als „Virtuelle Maschine“, gewissermaßen auf einem „simulierten Rechner im Rechner“ betrieben, und wird die ursprüngliche virtuelle Maschine täglich neu gestartet, ist damit auch eine erfolgreich installierte Durchsuchungssoftware spätestens beim nächsten Neustart entfernt.

(aus Dirk Fox: Stellungnahme zur "Online-Durchsuchung")

http://de.wikipedia.org/wiki/Virtuelle_Maschine

1.) Eigenen Rechner sichern

8.) Regelmäßige Backups

Legen Sie regelmäßig - am Ende jedes Arbeitstages - Sicherheitskopien an. Speichern Sie diese nicht nur auf Ihrer Festplatte, sondern auch auf einem externen Medium, z.B. auf einer externen Festplatte.

Es ist sinnvoll, Backups an einem anderen Ort aufzubewahren als dort, wo sich Ihr Computer befindet. Externe Festplatten bieten sich auch an, um Images, Backups und sensible Dateien in einem Bankschließfach oder an einem anderen sicheren Ort zu verwahren.

http://de.wikipedia.org/wiki/Backup

1.) Eigenen Rechner sichern

8.) Regelmäßige Backups

Neben Backups lohnen

- ✓ Klarkopien der eigenen Daten auf externem Medium
- ✓ Mirrors der eigenen Festplatte auf externem Medium

1.) Eigenen Rechner sichern

9.) Image-Programme

Image-Programme ermöglichen es, alle Dateien eines Mediums (also hier: einer Festplatte bzw. Partition) in einer einzigen Datei zu speichern und zu komprimieren - das Image ist also kleiner als das so gesicherte Medium.

Images sind de facto eine Zeitmaschine. Wenn Sie neue Programme probehalber installieren, erstellen Sie vorher ein Image. Wenn die Programme nicht gefallen, wird nicht deinstalliert (was oft nur mangelhaft funktioniert), sondern das Image eingespielt. Das ist wie ein Zeitsprung, als hätten Sie das Programm nie installiert.

http://de.wikipedia.org/wiki/Image_(Informatik)

1.) Eigenen Rechner sichern

10.) Speichermedien verschlüsseln

Nutzen Sie das Open-Source-Programm Truecrypt,
um die gesamte Festplatte und externe Festplatten zu verschlüsseln.
http://www.truecrypt.org/

1.) Eigenen Rechner sichern

11.) Informiert bleiben

Egal, welche Programme Sie einsetzen: Informieren Sie sich regelmäßig über neue Versionen, insbesondere über so genannte Patches, mit denen Sicherheitslücken geschlossen werden.

Newsletter "Heise Security Summary"

http://www.heise.de/newsletter

http://www.heise.de/bin/newsletter/listinfo/heisec-summary

Newsletter "Sicher Informiert" des BSI für Bürger

http://www.bsi-fuer-buerger.de/newsletter/index.htm

1.) Eigenen Rechner sichern

11.) Informiert bleiben

Das Infoportal des Bundesamtes für Sicherheit in der Informationstechnik für "normale" Nutzer

http://www.bsi-fuer-buerger.de/

heise Security – News, Dienste und Foren zum Thema Computer-Sicherheit

http://www.heise.de/security/

Das Software-Verzeichnis des Heise-Verlages

http://www.heise.de/software/

Vielen Dank für die Aufmerksamkeit

Albrecht Ude
albrecht@ude.de
www.ude.de
https://privacybox.de/aude.msg