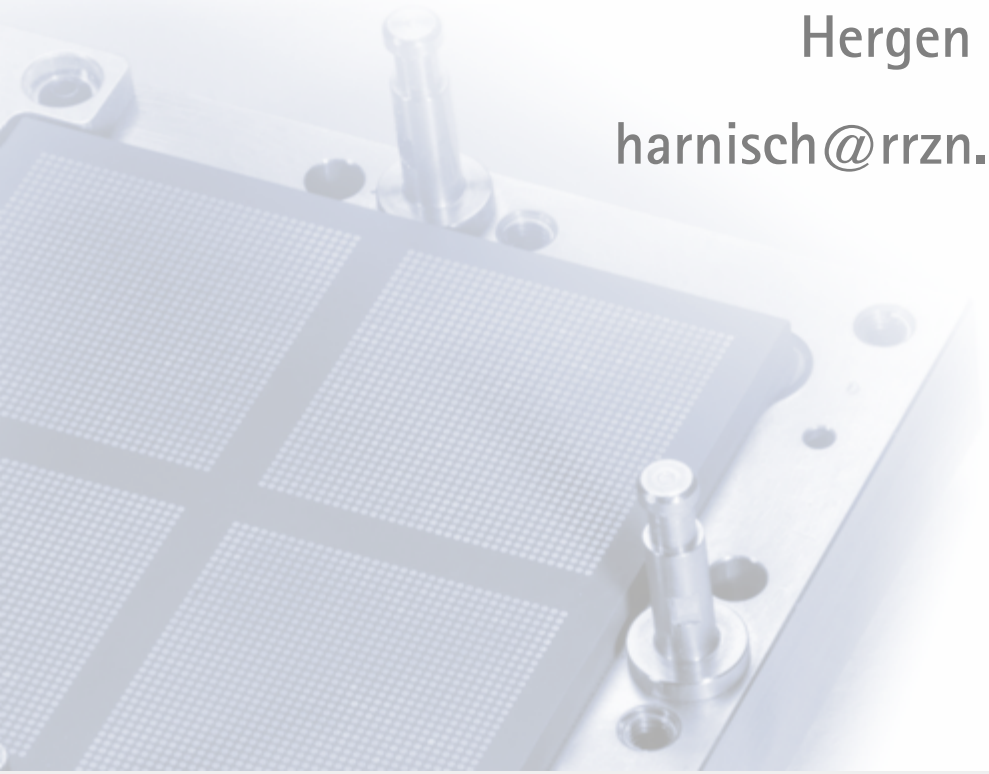
Umgang mit Infektionen



Hergen Harnisch

harnisch@rrzn.uni-hannover.de

1 Feststellung

2 Sofortmaßnahmen

3 Aufräumen

- Maßnahmenentscheidung
- Datenrettung
- Abschluss

4 Tools

- Bootbare Anti-Viren
- Rescue-Systeme

Wie erfährt das RRZN davon?

- durch Hinweise anderer, meist über das DFN-CERT
- durch IDS-Maßnahmen (z.B. DNS-Überwachung bei Conficker)
- durch Überwachung aggregierter Trafficdaten (nicht Inhalte)
  - Zahl der Flows, z.B. viel Verbindungen Zielport TCP-25 (Spammer)
  - ungewöhnlich hohes Traffic-Volumen
- durch Hinweise / Anzeigen von Ihnen
  - Teilen Sie uns mit, wenn Ihnen etwas komisch vorkommt.
  - Melden Sie uns Sicherheits-Vorfälle.

Wie erfahren OU-Admins davon?

- durchs RRZN (über `sec-*@ou.uni-hannover.de`-Adressen)
- durch eigenes Monitoring
- durch Nutzer

wichtig

Achten Sie auf Ihre `sec-*@ou`-Adresse:

- Haben Sie eine eingerichtet, sind die Admins im Verteiler?
- Infektionen, Sperrungen etc. werden darüber bekannt gegeben.
- Übergeben Sie die Adresse an Andere bei Urlaub & Ausscheiden, sonst sind Infektionen nur plötzliche Sperrungen …

vgl. http://www.rrzn.uni-hannover.de/fileadmin/it_sicherheit/pdf/Rundschr_B-42-2005_SecAdr.pdf

Sofortmaßnahmen
durchs RRZN

In den allermeisten Fällen sperrt das RRZN den Netzzugang:

- Die Infektion soll sich nicht im Netz ausbreiten.
- Das System soll nicht von Außen gesteuert und für Innenangriffe genutzt werden.
- (Weitere) Daten sollen nicht nach Außen abfließen.
- *leider auch:* Nutzer oder Admin muss reagieren.

Sperrung erfolgt irgendwo zwischen Switchport und Internetgateway, basierend auf IP- oder MAC-Adressen (betriebliche Gründe, entscheidet das RRZN).

Sofortmaßnahmen

durchs Institut / Einrichtung

… wenn es keine Falschmeldung ist

- umgehende Trennung des Systems vom Netzwerk
- ggf. Unterrichtung des zuständigen Admins & des RRZNs
- Unterrichtung des Nutzers:
  - Er soll das System nicht mehr nutzen & muss das wissen.
  - Seine Daten sind evt. an Dritte gelangt.
  - *Er muss alle seine Passwörter (Uni und privat) ändern, die sind wahrscheinlich „geleakt".*
    Wenn Nutzer nicht vor Ort ist, Kontaktaufnahme trotzdem versuchen; es eilt und ist im Interesse von Uni und Nutzer.

Alles weitere hat Zeit,
Forensik ist meist nur bei Server-Hacks erforderlich.

R|R|Z|N

Nicht-Technisches

- Gefahr ist nicht im Verzuge, Sie haben Zeit.
- Es ist nicht Ihr Rechner, fragen Sie vorher den Nutzer um Erlaubnis.
- Es sind nicht Ihre Daten, der Nutzer sollte nach Möglichkeit dabei sein oder wissen, was Sie tun.
- Dateneinsicht sollte so wenig wie möglich erfolgen, sie dient nur dem Zweck der Beseitigung des Sicherheitsproblems.
- Klären Sie den Nutzer auf, wo seine Daten bleiben und was los war.

Infektionsfeststellung

Scannen Sie mit einem separaten Boot-Medium den Rechner, gucken Sie in die Logs. Keine ausführliche Analyse, nur Verdachtserhärtung.

Säuberung oder Neuinstallation?

Die Neuinstallation ist der sicherste Weg, häufig auch der schnellste. Entfernen von Malware geht nur bei bekannter Malware (z.B. Conficker) einfach und recht zuverlässig.

Aufräumen Datenrettung

Sichern Sie die Daten des Nutzers:

- Kopieren Sie mit einem sauberen Live-System die Daten auf eine USB-Platte o.Ä.
- Kopieren Sie nicht das Profil, dort sitzt z.T. die Malware (z.B. Aktivierungs-Hooks in Registry-Einträgen)
  Denken Sie aber an die Mail, Bookmarks etc.
- Kopieren Sie Mail am Besten auf den imap-Server
  (z.B. RRZN-Mail-Archiv)
- Scannen Sie diese Daten nach Malware:
  - auf der USB-Platte *alle* Dateien, nicht nur einige Typen
  - zusätzlich haben Sie auf dem Zielsystem einen On-Access-Scanner[1]

[1] Denken Sie an Conficker und die `Autorun.Inf`

R|R|Z|N

nach dem Aufräumen wieder Aufräumen

Entsperrung

Beantragen Sie die Entsperrung beim RRZN per Mail, am Besten als Antwort auf die Sperrungsmail (zumindest IP im Betreff).

Datenvernichtung

Löschen Sie nicht mehr benötigte Daten des betroffenen Nutzers und zum Vorfall, ggf. zeitversetzt aber nicht vergessen.

Warum separates Booten?

Malware schützt sich gegen Entdeckung und Entfernung

- Anti-Virus-Updates werden unterbunden
- MSRT und ähnlich Tools sind nicht installierbar
- Stealth-Viren gab es schon zu DOS-Zeiten,
  heute sind es eher die Rootkits

Torpig/Mebroot ist z.B. derzeit kaum zu finden — aus einem infizierten System heraus.

R|R|Z|N

Knoppicillin

c't-Projekt

- abgespeckte Knoppix-Version mit Menü-Führung zum Virenscannen
- liegt ca. jährlich einer c't-Zeitschrift bei
- enthält mehrere Virenscanner mit Möglichkeit zum Live-Update

RRZN-Variante

- basiert (derzeit) auf Knoppicillin 7, aber nur Sophos-AV
- gerade erst fertig geworden, demnächst als ISO-Image auf
  `ftp://ftp.rrzn.uni-hannover.de/pub/uni-intern/Sicherheit/`

R|R|Z|N

vom AV-Hersteller

Viele Antiviren-Hersteller bieten CDs zur kostenfreien Nutzung zum Download:

Avira bietet ein Exe zum Download, das CD-Brennprogramm enthält:
`http://www.free-av.de/de/tools/12/avira_antivir_rescue_system.html`
Iso: `http://dl.antivir.de/down/vdf/rescuecd/rescuecd.iso`

F-Secure `http://www.f-secure.com/en_EMEA/security/security-lab/tools-and-services/rescue-cd/index.html`

Kaspersky `http://ftp.kaspersky.com/devbuilds/RescueDisk/`

Sophos leider nicht (aber in unserer Knoppicillin-Version)

(ausprobiert hat das RRZN bisher nur die Avira-CD)

Live-Linux

Eine Live-CD wie Ubuntu hat zwar keinen Virenscanner, aber

- „Forensik“ ohne Änderung und ohne aktive Malware
  - Suche nach Dateien auf dem System
  - Unix-Tools mächtiger bei händischer Suche
- Rettung von Daten
- Wiederherstellung von MBR, Partiontstabellen

Spezielle Rescue-Systeme haben beides, z.B. der RRZN-Bootstick
(ISO folgt, dann auch auf dem RRZN-ftp-Server)

Live-Windows

Es gibt auch bootbare Windows-CDs, z.B. Windows-PE oder Bart-PE.

aber diese greifen meist nicht nur r/o auf die Platte zu (z.B. Änderung der Access-Time) und könnten dort unbemerkt infizierte Dateien öffnen (z.B. Vorschau, Icons)