TRALIOS
Linux Server Management

CyberCircle IT Professionals: Wie schütze ich meine Webseite vor Bedrohungen durch Hacker?

Dipl.-Inform. Dominik Vallendor ▪ 14. November 2013

Über mich

TRALIOS
Linux Server Management

Dipl.-Inform. Dominik Vallendor

- Studium der Informatik in Karlsruhe
- Seit 1995: Internet/Linux-Erfahrung
- Seit 2002: Selbständig im Bereich Internetdienstleistungen
- Seit 2010: Geschäftsführer der Tralios IT GmbH:
  Betrieb von Linuxbasierten Web/Mailservern

Einführung

TRALIOS
Linux Server Management

- Warum werden Server “gehackt“?
- Wieso macht der Angreifer das?
- **Einfallstore**
- Welche Nachteile entstehen?
- **Gegenmaßnahmen**
- Diskussionsrunde

Warum werden Server “gehackt“?

TRALIOS
Linux Server Management

Selten:

- Hacker möchte persönlichen Schaden zufügen
- Erlangung von (Firmen-)Geheimnissen

Warum werden Server “gehackt“?

TRALIOS
Linux Server Management

Selten:

- Hacker möchte persönlichen Schaden zufügen
- Erlangung von (Firmen-)Geheimnissen

Regelfall:

Angriff auf die breite Masse

- Zufallstreffer
- Seite mit Sicherheitslücke über Google gefunden

Wieso macht der Angreifer das?

TRALIOS
Linux Server Management

Nicht-wirtschaftliche Interessen:

- Geltungsbedürfnis: Webseiten-Defacement
- Ablage von illegalen Inhalten, Filetausch

Wieso macht der Angreifer das?

TRALIOS
Linux Server Management

Nicht-wirtschaftliche Interessen:

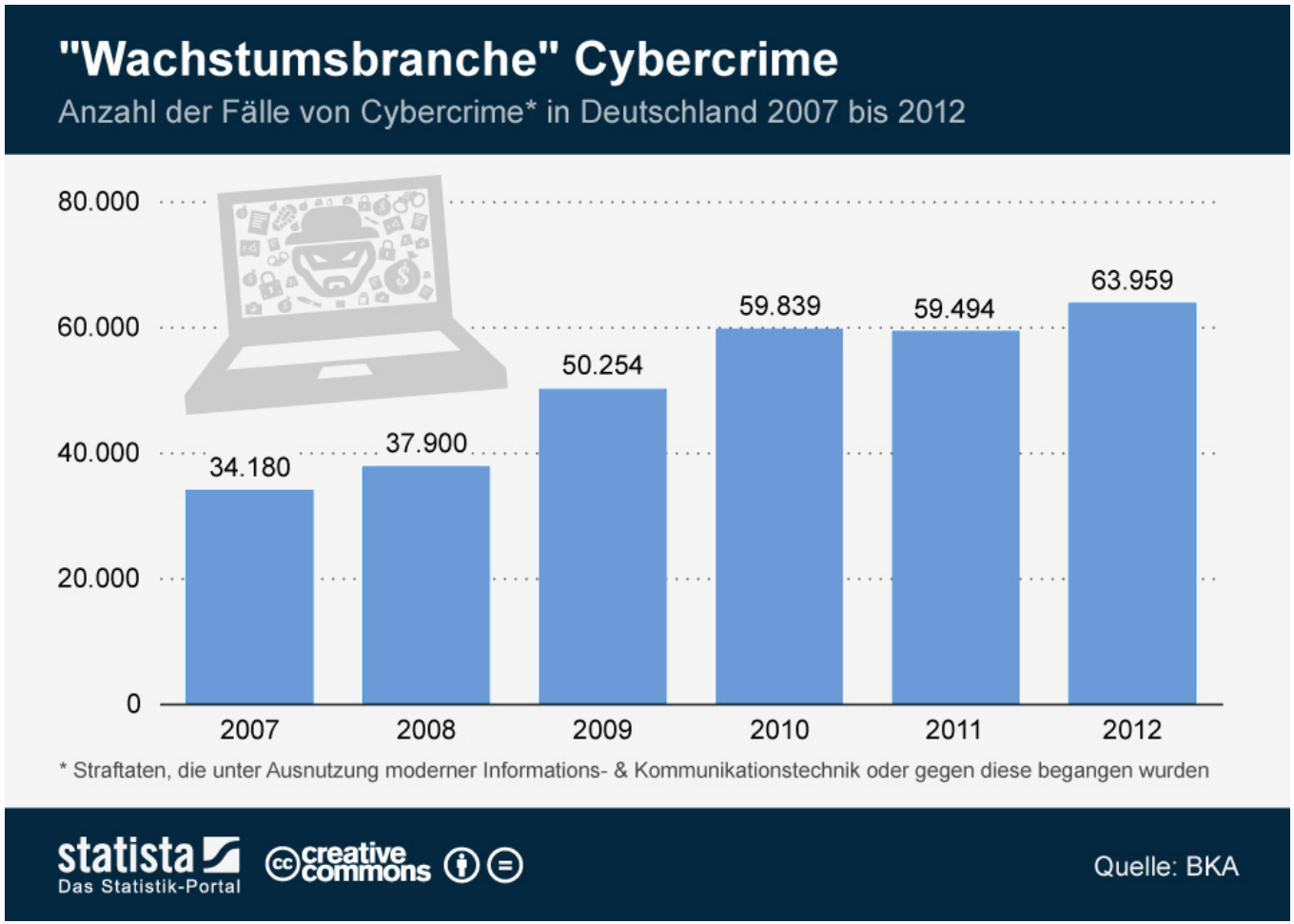
- Geltungsbedürfnis: Webseiten-Defacement
- Ablage von illegalen Inhalten, Filetausch

Wirtschaftliche Interessen:

- **Versand von SPAM** (z.B. über PHP)
- **Einschleusen von Schadcode** (JavaScript, iFrames) $\Rightarrow$ Banking-Trojaner
- Abgreifen von Daten: Passwörter, Kreditkartendaten, ...
- Nutzung des Servers als Sprungbrett für weitere Angriffe
- Ablage von Phishing-Seiten (Nachgebaute Bank-Homepages)

Anzahl der Fälle von Cybercrime

TRALIOS
Linux Server Management



Typische Einfallstore

TRALIOS
Linux Server Management

- Sicherheitslücken in (PHP-)Skripten, SQL-Injections
  - Veraltete Standard-Software: bekannte Sicherheitslücken werden ausgenutzt
  - Programmierfehler in Individualsoftware, schlechte Programmierer
- Erlangen von Passwörtern durch Trojaner auf Windows-PCs
- SPAM-Versand durch nicht abgesicherte Webformulare (Kontaktformular), Gästebuch-Spam

Problem: Sicherheitslücken lassen sich schnell und **automatisiert** finden.

Fertige Tools erleichtern den Angriff.

Der typische Hacker?

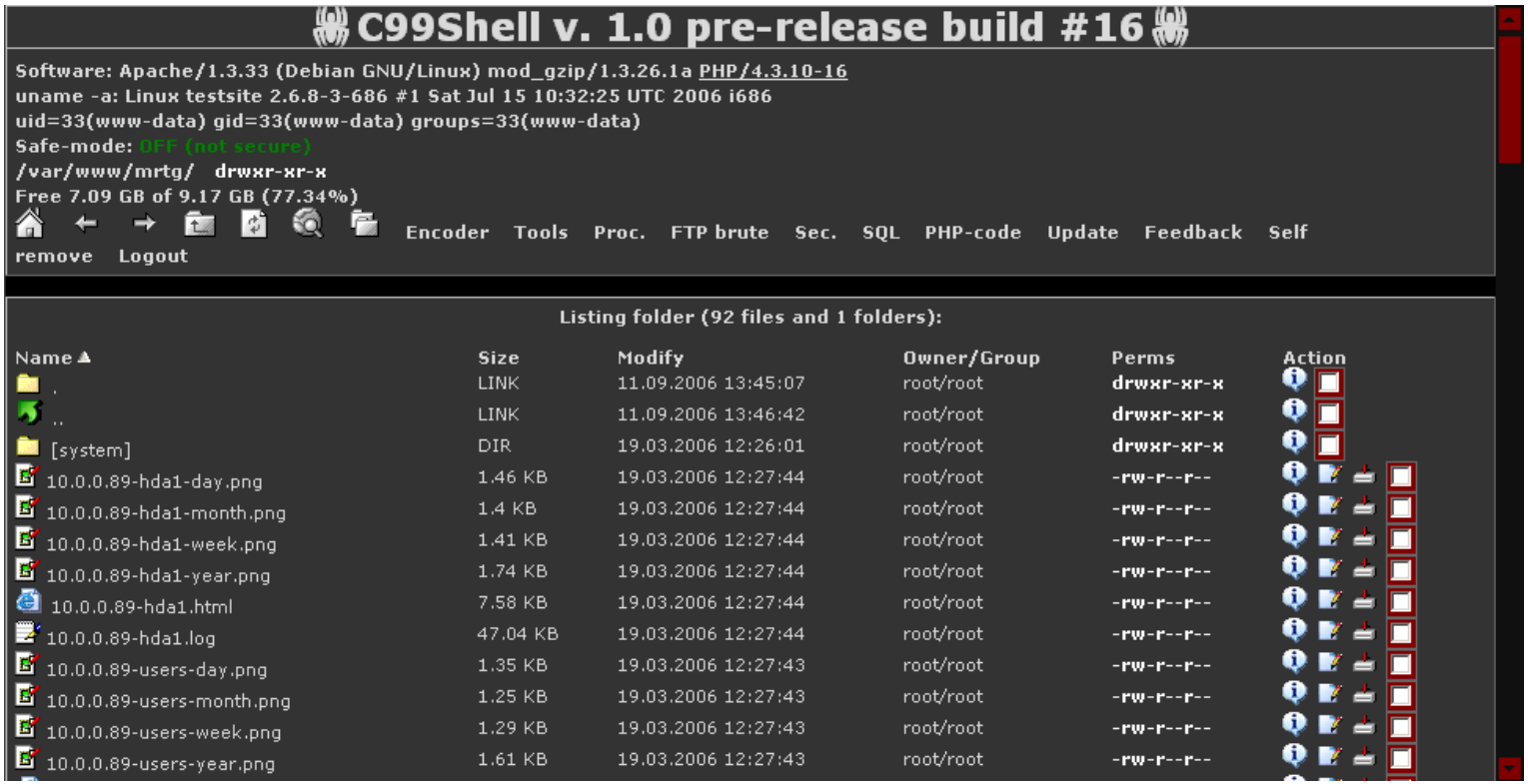
TRALIOS
Linux Server Management

Der typische Hacker?

TRALIOS
Linux Server Management

Beispiel einer PHP-Shell

TRALIOS
Linux Server Management



Weitere Einfallstore & Probleme

TRALIOS
Linux Server Management

- Ausprobieren von Passwörtern
- Falsche Serverkonfiguration
- Sicherheitslücken in Serverdiensten (Apache, SSH, etc.)

Weitere Einfallstore & Probleme

TRALIOS
Linux Server Management

- Ausprobieren von Passwörtern
- Falsche Serverkonfiguration
- Sicherheitslücken in Serverdiensten (Apache, SSH, etc.)

- Mithören/Belauschen der Kommunikation Anwender/Server
- Angriffe auf die Verfügbarkeit, DDOS-Attacken
- Cross-Site-Scripting (XSS)

Konkretes Beispiel eines Server-Einbruchs

TRALIOS
Linux Server Management

- Portal mit öffentlichen Einrichtungen für Kinder & Senioren
- Initialer Einbruch durch SQL-Injection
- Diebstahl der Einträge aus der Datenbank
- $\Rightarrow$ Zugang zum Administrations-Bereich
- Ablage einer PHP-Shell und verschiedener Backdoors
- Versuchter Zugriff auf Kernel konnte verhindert werden

Konkretes Beispiel - Maßnahmen

TRALIOS
Linux Server Management

- Recherche durch Tralios IT nach Sicherheitslücke
- Zurückspielen des Backups
- Beseitigung der SQL-Lücken durch neuen Programmierer
- Vergabe neuer Zugangsdaten durch Institution (ca. 1 Woche Arbeit)
- Strafanzeige gegen Unbekannt
- Bericht an Polizeibehörde für weitere Ermittlung

$\Rightarrow$ Hoher Aufwand und Kosten für den Seitenbetreiber

Konkretes Beispiel - Auszug aus dem Logfile

TRALIOS
Linux Server Management

```
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0-- HTTP/1.1" 200 3835 "-" "-"
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878-- HTTP/1.1"
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union+Select+0x787878756E696F6E787878+,0x787878756
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201%20,2,3,4,5,6,7,8,9,10,11,12,
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%200x76697369626C6531323334353637
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201%20,0x76697369626C65313233343
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201%20,0x787878756E696F6E787878,
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201%20,%20UNHEX(HEX(CONCAT(0x5B6
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201,%20UNHEX(HEX(CONCAT(0x5B6B65
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201,%20UNHEX(HEX(CONCAT(0x5B6B65
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201,%20UNHEX(HEX(CONCAT(0x5B6B65
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201%20,%20UNHEX(HEX(concat(0x5B6
"GET /ausgabe.php?seiteID=2&navioben=16+and+1=0+%20Union%20Select%20%201%20,%20UNHEX(HEX(concat(0x5B6
```

Live-Demo

TRALIOS
Linux Server Management

Einbruch durch SQL-Injection in eine Datenbank

Welche Nachteile entstehen dem Seitenbetreiber?

TRALIOS
Linux Server Management

- Aufwand zur Beseitigung von Schadcode, illegalen Inhalten, etc.
  Hohe Kosten für Bereinigung, Neuinstallation
- Webseite ist gesperrt, unerreichbar: Umsatzausfall (bsp. Webshop)
- Erzeugt schlechten Eindruck, marketingtechnischer GAU
  Schlechte Reputation/Warnungen bei Google; Gästebuch-Spam
- Im Visier von Strafverfolgungsbehörden: Befragungen, Beschlagnahmungen, ...

Gegenmaßnahmen - Was können Sie tun?

TRALIOS
Linux Server Management

- Software aktuell halten, insb. CMS-Systeme, Shops, etc.
- Bei Individualsoftware: gute Programmierer beauftragen!
- Auf Endbenutzer-Rechnern Virenscanner installieren und aktuell halten
- Für jeden Dienst/Anbieter ein eigenes Passwort verwenden
- Zugangsdaten nur individuell vergeben und spärlich weitergeben
  deaktivieren, falls nicht mehr benötigt
- Verschlüsselte Kommunikation nutzen: IMAP/POP3 mit SSL, SMTPS, FTPS, ...

Gegenmaßnahmen - Was können Sie tun?

TRALIOS
Linux Server Management

- Software aktuell halten, insb. CMS-Systeme, Shops, etc.
- Bei Individualsoftware: gute Programmierer beauftragen!
- Auf Endbenutzer-Rechnern Virenscanner installieren und aktuell halten
- Für jeden Dienst/Anbieter ein eigenes Passwort verwenden
- Zugangsdaten nur individuell vergeben und spärlich weitergeben
  deaktivieren, falls nicht mehr benötigt
- Verschlüsselte Kommunikation nutzen: IMAP/POP3 mit SSL, SMTPS, FTPS, ...

Gegenmaßnahmen - Was können Sie tun?

TRALIOS
Linux Server Management

- Software aktuell halten, insb. CMS-Systeme, Shops, etc.
- Bei Individualsoftware: gute Programmierer beauftragen!
- Auf Endbenutzer-Rechnern Virenscanner installieren und aktuell halten
- Für jeden Dienst/Anbieter ein eigenes Passwort verwenden
- Zugangsdaten nur individuell vergeben und spärlich weitergeben
  deaktivieren, falls nicht mehr benötigt
- Verschlüsselte Kommunikation nutzen: IMAP/POP3 mit SSL, SMTPS, FTPS, ...

Gegenmaßnahmen - Was können Sie tun?

TRALIOS
Linux Server Management

- Software aktuell halten, insb. CMS-Systeme, Shops, etc.
- Bei Individualsoftware: gute Programmierer beauftragen!
- Auf Endbenutzer-Rechnern Virenscanner installieren und aktuell halten
- Für jeden Dienst/Anbieter ein eigenes Passwort verwenden
- Zugangsdaten nur individuell vergeben und spärlich weitergeben
  deaktivieren, falls nicht mehr benötigt
- Verschlüsselte Kommunikation nutzen: IMAP/POP3 mit SSL, SMTPS, FTPS, ...

Gegenmaßnahmen - Was können Sie tun?

TRALIOS
Linux Server Management

- Software aktuell halten, insb. CMS-Systeme, Shops, etc.
- Bei Individualsoftware: gute Programmierer beauftragen!
- Auf Endbenutzer-Rechnern Virenscanner installieren und aktuell halten
- Für jeden Dienst/Anbieter ein eigenes Passwort verwenden
- Zugangsdaten nur individuell vergeben und spärlich weitergeben
  deaktivieren, falls nicht mehr benötigt
- Verschlüsselte Kommunikation nutzen: IMAP/POP3 mit SSL, SMTPS, FTPS, ...

Gegenmaßnahmen - Was können wir tun?

TRALIOS
Linux Server Management

Professionelles Servermanagement

- Verschlüsselung anbieten (Bsp. SSL-Zertifikat)
- Server absichern (Bsp. Firewall)
- Systemsoftware aktuell halten
- Regelmäßige Backups
- Serverüberwachung schützt vor Angreifern und deckt Probleme frühzeitig auf

Fazit

TRALIOS
Linux Server Management

- Einbruch in Webseiten ist kinderleicht
- Meist keine gezielten Angriffe, sondern automatisiert
- Sicherheitslücken werden garantiert ausgenutzt, die Frage ist nur, wann
- Software aktuell halten
- Maßnahmen nach Einbruch erforden viel Zeit & Aufwand
- Auf gute Basis achten (Serveranbieter)

Kontakt

TRALIOS
Linux Server Management

- *Dipl.-Inform. Dominik Vallendor*

  Tralios IT GmbH

  Bannwaldallee 46

  76185 Karlsruhe

  Telefon: 0721 - 94269660

  Telefax: 0721 - 94269666

  E-Mail: vallendor@tralios.de