TRALIOS
Linux Server Management

Einfallstore in Webanwendungen und deren Folgen

Dipl.-Inform. Dominik Vallendor ▪ 14.07.2012

Über mich

TRALIOS
Linux Server Management

- Dominik Vallendor
- Studium der Informatik in Karlsruhe
- Ca. 17 Jahre Linux-Erfahrung
- Seit 2002 selbständig
- Seit 2010: Tralios IT GmbH: Betrieb von Linuxbasierten Web/Mailservern

Einführung

TRALIOS
Linux Server Management

- Warum werde gerade ich gehackt?
- Typische Einfallstore
- Beispiel
- Gegenmaßnahmen
- Fragen & Diskussion

Warum werde gerade ich gehackt?

TRALIOS
Linux Server Management

Äusserst selten:

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

Regelfall:

- Angriff auf die breite Masse
- Zufallstreffer
- Seite bei Google gefunden

Typische Einfallstore

TRALIOS
Linux Server Management

In der Praxis gibt es nur wenige Einfallstore:

- Sicherheitslücken in PHP-Skripten:

  Ermöglichen es, Fremdcode nachzuladen

  Falsche Serverkonfiguration (Bsp. *bild.php.jpg*)

  SQL-Injections

  $\Rightarrow$ Kinderleicht auszunutzen, siehe Demo!

- Erlangen von FTP-Passwörtern durch Trojaner auf Windows-PCs

Warum macht der Hacker das?

TRALIOS
Linux Server Management

- Geltungsbedürfnis: Webseiten-Defacement
- Verteilung von Schadcode per JavaScript, iFrames

  $\Rightarrow$Botnetze, Banking-Trojaner
- Spam-Versand

Andere Einfallstore

TRALIOS
Linux Server Management

Alle anderen oft genannten Einfallstore sind in der Praxis quasi irrelevant:

- Probleme lassen sich durch gute Serveradministration unterbinden:
  - Ausprobieren von Passwörtern
  - Sicherheitslücken in Serverdiensten (Apache, SSH, etc.)
- Selten genutzt oder nur indirekt nutzbar:
  - Cross-Site-Scripting (XSS)
  - Social engineering

  Trotzdem nicht zu unterschätzende Gefahr, da sehr wirkungsvoll

Beispiel eines Server-Einbruchs

TRALIOS
Linux Server Management

- Initialer Einbruch durch PHP-Sicherheitslücke
- Ablage einer PHP-Shell

  $\Rightarrow$Komplette Rechte im Kontext des Webservers/Webbenutzers, Demo!
- Ablage von Hintertüren, weiteren PHP-Shells für den späteren Zugriff
- Ausprobieren von Kernel-Exploits

  $\Rightarrow$im Idealfall hat der Hacker danach Root-Rechte
- Veränderung der Originalwebseiten, Spamversand, etc.

Gegenmaßnahmen

TRALIOS
Linux Server Management

- Software aktuell halten, insb. CMS-Systeme, Shops, etc.
- Bei Individualsoftware: gute Programmierer beauftragen!
- Bei eigenem Server:
  - Konfiguration absichern, insb. PHP-Einstellungen/Userrechte
  - Zugriffe blockieren, z.B. per SSHGuard
  - System überwachen und so Auffälligkeiten früh erkennen

Fazit

TRALIOS
Linux Server Management

- Einbruch in Webseiten ist kinderleicht
- Meist keine gezielten Angriffe
- Gegenmaßnahmen erforden viel Zeit & Aufwand

  Fertige Sicherheitstools sind nur ein Teil der Lösung

Fragen & Diskussion

TRALIOS
Linux Server Management

???

Danke

TRALIOS
Linux Server Management

Danke für die Aufmerksamkeit

Kontakt

TRALIOS
Linux Server Management

- Dipl.-Inform. Dominik Vallendor

- Tralios IT GmbH

  Pfinztalstr. 90

  76227 Karlsruhe

  Telefon: 0721 - 94269660

  Telefax: 0721 - 94269666

  E-Mail/Jabber: vallendor@tralios.de