Angriffe auf Sicherheitsinfrastrukturen

Angriffsmöglichkeiten
und aktuelle Angriffe auf
Sicherheitsinfrastrukturen der IT

Dr. Michael David
T-Mobil
Michael.M.David@T-Mobil.de

Angriffe auf Sicherheitsinfrastrukturen

Themenübersicht:

- Web-Anwendungen
- Firewalls und der Desktop
- Distributed Denial-of-Service Angriffe
- Angriffe auf Crypto-Hardware

Angriffe auf Web-Anwendungen

Besonderheit von Web-Anwendungen bzgl. Sicherheit:

- Offene Standards
- Vielfalt an möglichen Client-Systemen
- Schwierige Identifizierung des Clients und des Benutzers
- Offene Kommunikation, nichtlinearer Kommunikationsablauf
- Angriffsmöglichkeiten bestehen schon für nicht-autorisierte Nutzer
- „Populäre“ Systeme sind Zielsysteme von Angriffen

Angriffe auf Web-Anwendungen

Kerngedanken der Sicherheit von Web-Anwendungen:

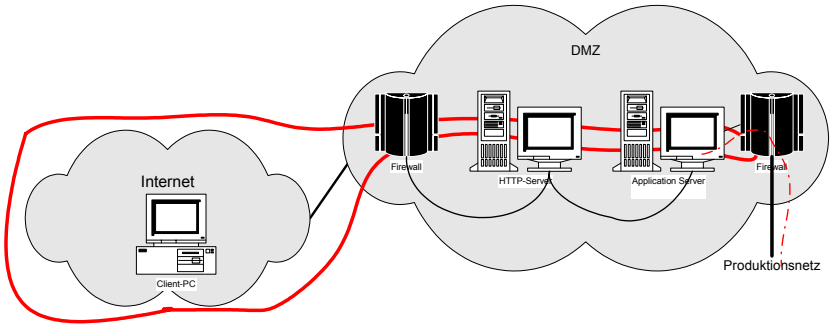
Nutzeridentifikation und Plausibilitätsprüfungen

Bei jeder Kommunikation ist zu prüfen:

- Wer ist das?
- Was will er?
- Darf der das?

Angriffe auf Web-Anwendungen

Nutzeridentifikation: Nicht autorisierte Nutzer können bereits Auswirkungen bis tief in wichtige Systeme verursachen!



Angriffe auf Web-Anwendungen

Angriffsmöglichkeiten für nicht autorisierte Benutzer

- Anwendungsunabhängig: Middleware, Web-Server, Firewall
  - Ausnutzung dokumentierter Sicherheitslücken
  - Ausnutzung dokumentierter Zugänge zur Middleware
  - Unsichere „Standard-Installation“ der Systeme
  - Zugriff auf Datenflüsse (ungenügende SSL-Verschlüsselung, ...)
- Anwendungsbezogen: Öffentlich zugängliche Seiten (Login, FAQ, Hilfe, ...)
  - Passworte erraten
  - Zugänge mit bekannter Kennung sperren
  - Rückschlüsse auf Strukturen durch Auslesen des HTML-Quelltextes oder durch die Analyse von Fehlermeldungen

Diese Angriffsmöglichkeiten stehen WELTWEIT zur Verfügung

Angriffe auf Web-Anwendungen

Angriffsmöglichkeiten für nicht autorisierte Benutzer

Beispiele für Ansatzpunkte:

```
java.io.FileNotFoundException: no resource '/*.gif/login/login.jsp' in servlet context root
'/appl/local/templates‘
```

- `java.net.UnknownHostException: www.bigbox.com`

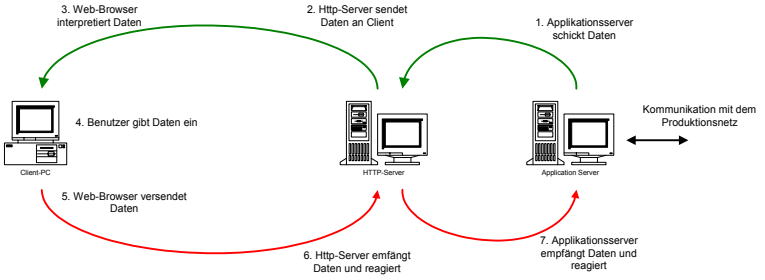
- `javax.servlet.ServletException: Servlet class: examples.servlets.PhoneServlet could not be loaded - the requested class wasn't found in the classpath /appl/local/classes/frontend/servlet:/appl/local/classes/jsp`

- `Client Certificate for srv1@abx0abmg`
- `Client Certificate for srv2@abx0abmg`

Angriffe auf Web-Anwendungen

Probleme durch den Ablauf der Kommunikation:

- Ausgangssituation II: Zugriffsmöglichkeiten für autorisierte Benutzer

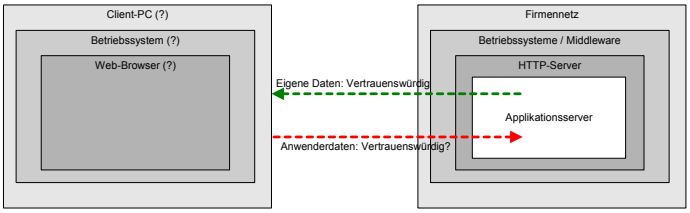


Problem 1: Ein autorisierter Benutzer bewirkt Aktionen, deren Auswirkungen tief in eigene Systeme hinein wirken.

Angriffe auf Web-Anwendungen

Angriffsmöglichkeiten für Web-Anwendungen

- Was wissen wir über den Anwender?



Problem 2: Wir können keine Aussagen über die Entstehung der Daten auf Anwenderseite geben:

- Manipulation von Eingaben (Umgehung von Plausibilitäten etc.)
- Eingabe „böswilliger“ Daten

Angriffe auf Web-Anwendungen

Angriffsmöglichkeiten für autorisierte Benutzer

- Manipulation der URL

Beispiel: „Setzen“ von Daten durch die URL durch Anfügen von Informationen

http://www.server.de/Abfrage?show=Kontostand

wird zu

http://www.server.de/Abfrage?show=Kontostand&customer=Hans.Eichel

Mögliche Konsequenz: Es werden die Daten eines Dritten angezeigt.

Variationen davon: Ausführen von eigentlich hier nicht zugänglichen Funktionen, deren Existenz bekannt ist oder sich etwa aus dem HTML-Quelltext ergibt

Angriffe auf Web-Anwendungen

Angriffsmöglichkeiten für autorisierte Benutzer

- Manipulation des HTML-Quelltextes (1)
  - Beispiel: Umgehen von Eingabebeschränkungen
    - <input type=text maxlength=30 ... >
    - <form action=javascript:testeEingabevorSubmit() ...>
    - <select <option value=1>hallo</option> ...>
  - Mögliche Auswirkungen:
    - Es werden zu viele Daten angeliefert (type = file...)
    - Es werden keine Plausibilitätsprüfungen durchgeführt
    - Es werden „out of index“-Werte weitergegeben (0, 1000, -1, ...)

Angriffe auf Web-Anwendungen

Angriffsmöglichkeiten für autorisierte Benutzer

- Manipulation des HTML-Quelltextes (2)
  - Beispiel: Nicht konsequent umgesetzte Rechte, Umgehen der Anwendungslogik
    - <form action=abfrage ...>
      <input name=kontonummer ...>
      <input type=hidden name=nextPage value=„Kontoübersicht“ ...>

      Ersetzen durch
      <input type=hidden name=nextPage value=„Kontostand“ ...>
  - Mögliche Konsequenz:
    - Abfragen eines Kontostands, wenn die Rechteüberprüfung nur bei der Abfrage der Kontoübersicht durchgeführt wird *(„... auf die Kontostandsseite kommt man nur von der Kontoübersicht, und das nur über die Abfrage, das ist sicher!“)*

Angriffe auf Web-Anwendungen

Angriffsmöglichkeiten für autorisierte Benutzer

- Manipulation der Session-ID
  - Das zustandslose (S)HTTP-Protokoll benötigt die „Hilfe“ des Browsers, um einen Anwender für mehrere aufeinanderfolgende Abfragen identifizieren zu können. Dies wird durch sog. Session-IDs durchgeführt, d.h. Zeichenketten, die eigentlich eindeutig unter allen Benutzern sein sollen.
  - Probleme:
    - Leicht zu erratende Zeichenketten, Doubletten (zu kurze Session-IDs bei vielen Benutzern, ...)
    - Weitergehende Informationen über den Benutzer in der Session-ID
  - Mögliche Auswirkungen:
    - beabsichtigte oder unbeabsichtigte Kenntnisnahme von Daten Dritter
    - Umgehung interner Authentifizierungsmechanismen

Angriffe auf Sicherheitsinfrastrukturen

Themenübersicht:

- Web-Anwendungen
- **Firewalls und der Desktop**
- Distributed Denial-of-Service Angriffe
- Angriffe auf Crypto-Hardware

Firewalls und der Desktop

Die Standardkonfiguration in vielen Anwendungsfällen der Bürokommunikation erlaubt einen Datenverkehr über den Port 80 (Standardport für Http). Diese Daten werden i.a. untersucht auf

- Viren
- Unerwünschte Inhalte (z.B. anhand der URL)

Verschlüsselte Verbindungen werden i.a. direkt (Proxy-Connect) und ungefiltert zugelassen

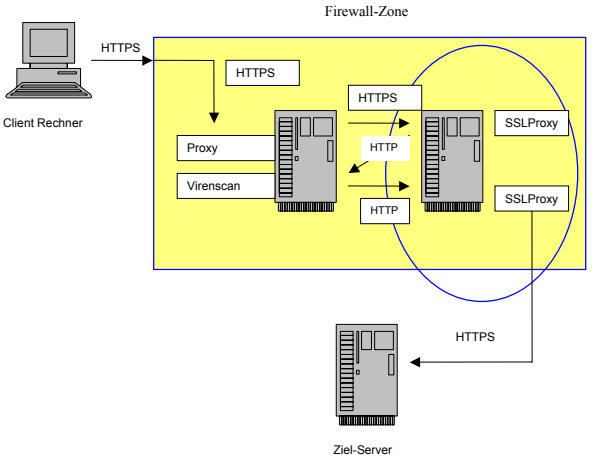
Firewalls und der Desktop

Sicherheitsprobleme:

- Umgehen der Sicherheitsrestriktionen durch SSL-Proxies im Internet
- Tunneln der Firewall durch das Routen eines zweiten Protokolls über die Proxy-Connect-Methode (i.w. durch Fehlkonfiguration; zusätzliche Software erforderlich)
- Tunneln der Firewall durch Kapselung eines zweiten Protokolls innerhalb von Http (Gegenstelle im Internet sowie zusätzliche Software erforderlich)

Firewalls und der Desktop

Eingeschränkte Lösungsmöglichkeit: Filtern von SSL-Verkehr



Firewalls und der Desktop

Bestehende Problematiken beim Filtern von SSL-Verkehr

- Vertraulichkeit von z.B. E-Banking ist nicht gewährleistet
- „Schnüffelsoftware“
- Tunneln der Protokolle bleibt unentdeckt

„Technische Lösungen helfen nicht bei
Problemen der sozialen Ebene“

Angriffe auf Sicherheitsinfrastrukturen

Themenübersicht:

- Web-Anwendungen
- Firewalls und der Desktop
- **Distributed Denial-of-Service Angriffe**
- Angriffe auf Crypto-Hardware

DDOS: Distributed Denial of Service

Beschreibung und Analyse eines DDOS-Angriffs auf www.grc.com ist im Internet verfügbar. Die Highlights sind:

- Koordinierte Erzeugung von Last auf dem Server durch einen Angriff von 417 „Zombies“
- Zusammenbruch der Connectivity: Die gesamte Bandbreite wurde von den Angriffen genutzt
- Auslöser war eine vermeintlich abfällige Bemerkung des Besitzers von grc.com über „Script-Kiddies“
- Initiator war ein nach Eigenauskunft ein 13-jähriger

DDOS: Distributed Denial of Service

Konsequenz des Betreibers:

I surrender.

I surrender right now, completely and unconditionally.

And I'm not kidding.

...

So, I respectfully ask that you leave me alone and allow my site to stay on the net

DDOS: Distributed Denial of Service

Konsequenz aus den Angriffen:

- Brute force-Angriffe machen Probleme
- Ein IDS auf Anwendungsebene kann helfen, die Situation zu erkennen und ein Netz bzw. einen Host „sauber“ zu halten
- Ein DDos-Angriff kann i.a. nicht nur durch den Betreiber eines Servers verhindert werden, sondern auch durch Sicherheitsmassnahmen auf Anwendungsebene
- Personal Firewalls für Clients können helfen, schützen aber nicht immer

Angriffe auf Sicherheitsinfrastrukturen

Themenübersicht:

- Web-Anwendungen
- Firewalls und der Desktop
- Distributed Denial-of-Service Angriffe
- **Angriffe auf Crypto-Hardware**

Angriffe auf Crypto-Hardware

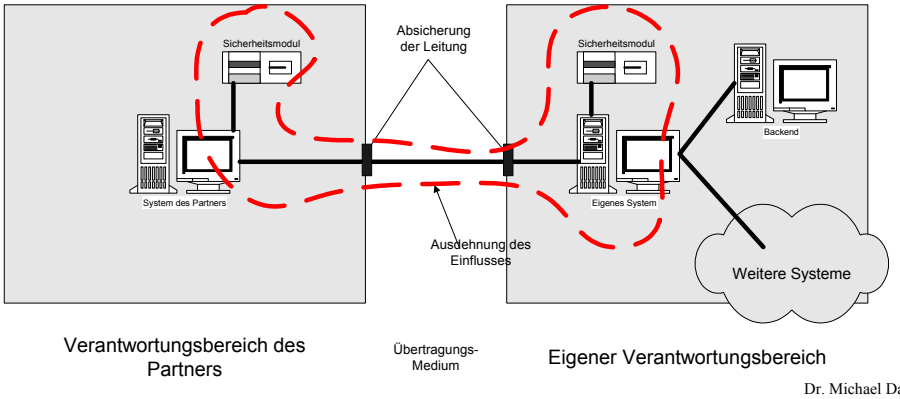
Aktuelle Schreckensmeldung im Internet:

- „Studenten knacken Bankensicherheit“
- „IBM-Verschlüsselung 3DES geknackt“
- „Online-Banking nicht mehr sicher“

... was ist eigentlich passiert, worauf wurde ein Angriff durchgeführt?

Angriffe auf Crypto-Hardware

Crypto-Hardware mit eigenem Schlüsselmanagement wird z.B. bei Bank-Anwendungen (Electronic-Cash) eingesetzt, um den Einflussbereich der eigenen Sicherheitslösungen auf einen Partner auszudehnen:



Dr. Michael David

Angriffe auf Crypto-Hardware

Eigenschaften der Hardware

- Separates Key-Management
- Schlüsseleingabe direkt am Gerät durch Pin-Pad
- Kapselung kryptographischer Funktionen

Vorteile des Einsatzes

- Gültige Transaktionen werden nur vom Besitzer der Hardware generiert
- Der geheime Schlüssel bleibt dem Partner unbekannt
- Nachträgliche Beweisführung der Korrektheit von Transaktionen durch stets nachvollziehbare Prüfsummen
- Fälschung von Transaktionen ist nur möglich, wenn im eigenen Betrieb eine kriminelle Energie bei Zusammenwirken von Entwicklung, Betrieb und Sicherheitsmanagement vorhanden ist.

Dr. Michael David

Angriffe auf Crypto-Hardware

Aktuelles Angriffs-Szenario (10.11.01; Extracting a 3DES-Key ...)

- Angriff auf eine Steckkarte (und keine Box), die aber nach FIPS 140-1, Level 4 zertifiziert war (Hardware, Firmware, OS)
- Schlüsselmanagement ausschliesslich durch API
- Extraktion eines 3DES-Schlüssels war möglich
- Kombinierter Angriff durch Hardware und manipulierter API; nötig ist
  - Zugriff auf die Hardware
  - Zugriff auf einen Account mit entsprechender Berechtigung (den i.a. 3-4 Personen haben)

Fazit

Sicherheitslösungen zeigen ihren Wert erst im wirklichen Einsatz

Systeme erfordern Kreativität in der Absicherung

Ohne Vertrauenswürdigkeit (Personal, RZ, Netz, ...) keine Sicherheit

Blinder Zerstörungswut kann nur schwer begegnet werden

Sensibilität für Sicherheit ist auf allen Ebenen nötig