



Internet Sicherheit

Hacken und Schutz von Informationen

Gesamtüberblick

- Überblick Internetsicherheit
- Sicherheitsbenchmarks
- Typische Netzstrukturen und Sicherheitsmaßnahmen
- Sicherheit von Webapplikationen
- Sicherheitsaudits
- Websites / Resources
- Zusammenfassung / Fragen

lessus

Sicherheit im Internet

Angriffziele

- **Verfügbarkeit der Information**
Komme ich an die Informationen dran?
- **Integrität der Information**
Wurde die Information verändert?
- **Vertraulichkeit der Information**
Ist der Inhalt geheim geblieben?
- **Verbindlichkeit der Information**
Ist die Information wirklich von diesem Absender geschickt worden?

lessus

Sicherheit im Internet

Angriffsarten

- Denial of service
- Man in the middle
- Spamming
- Viren / Würmer / Trojanische Pferde
- Ping of death
- Land attack
- Arp spoofing
- Dns spoofing
- Ip address spoofing
- ...

Sicherheit im Internet

Technische Schutzmechanismen

- Verschlüsselung
- Paketfilter
- Firewalls
- virtual private network
- Application-Firewall (proxy)
- Intrusion Detection
- Sichere Konfiguration
 - Schließen aller unbenutzten Ports
 - Beenden aller unbenutzten Prozesse
 - Logging einschalten
 - Gute Passworte
 - Patchen, patchen, patchen...

Sicherheit im Internet

Ursachen

- Protokoll- und Systemdesignmängel
- Implementierungsfehler
- Administrationsfehler
- Ungeschulte Anwender

- Featurerism (z.B. Internet Information Server: Internet Printing Protokoll)
- Immer kürzere Produkt-Haltbarkeit
 - Mit neuen Versionen Geld verdienen
- Schneller sein müssen als die Konkurrenz

lessus

Sicherheit im Internet

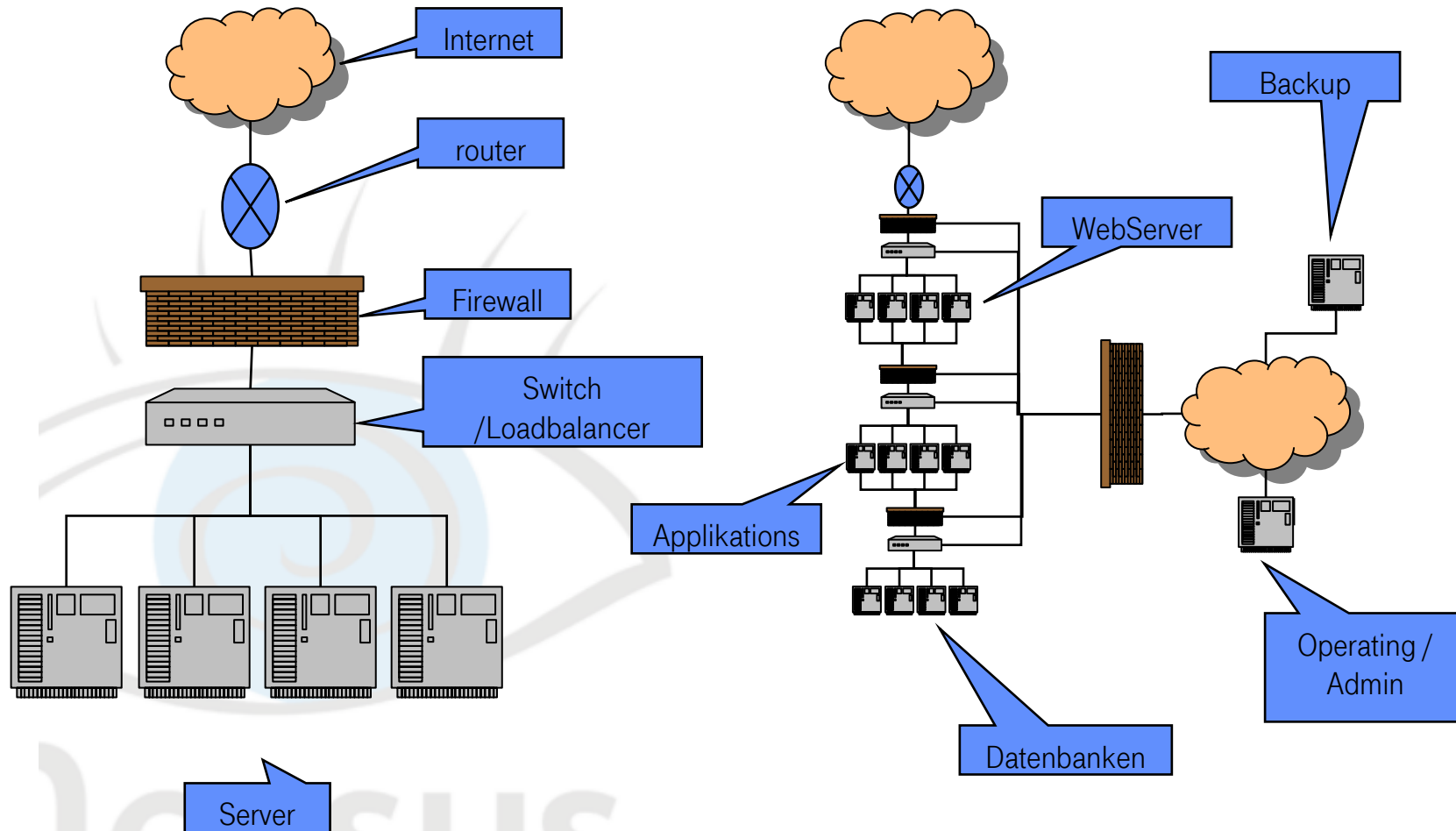
Werkzeuge

- Portscanner: nmap
- Vulnerability-Scanner: nessus
- Session Hijacking: hunt
- rootkit
- Arprouter
- Passwort Cracker: l0phtcrack, crack, cain

nessus

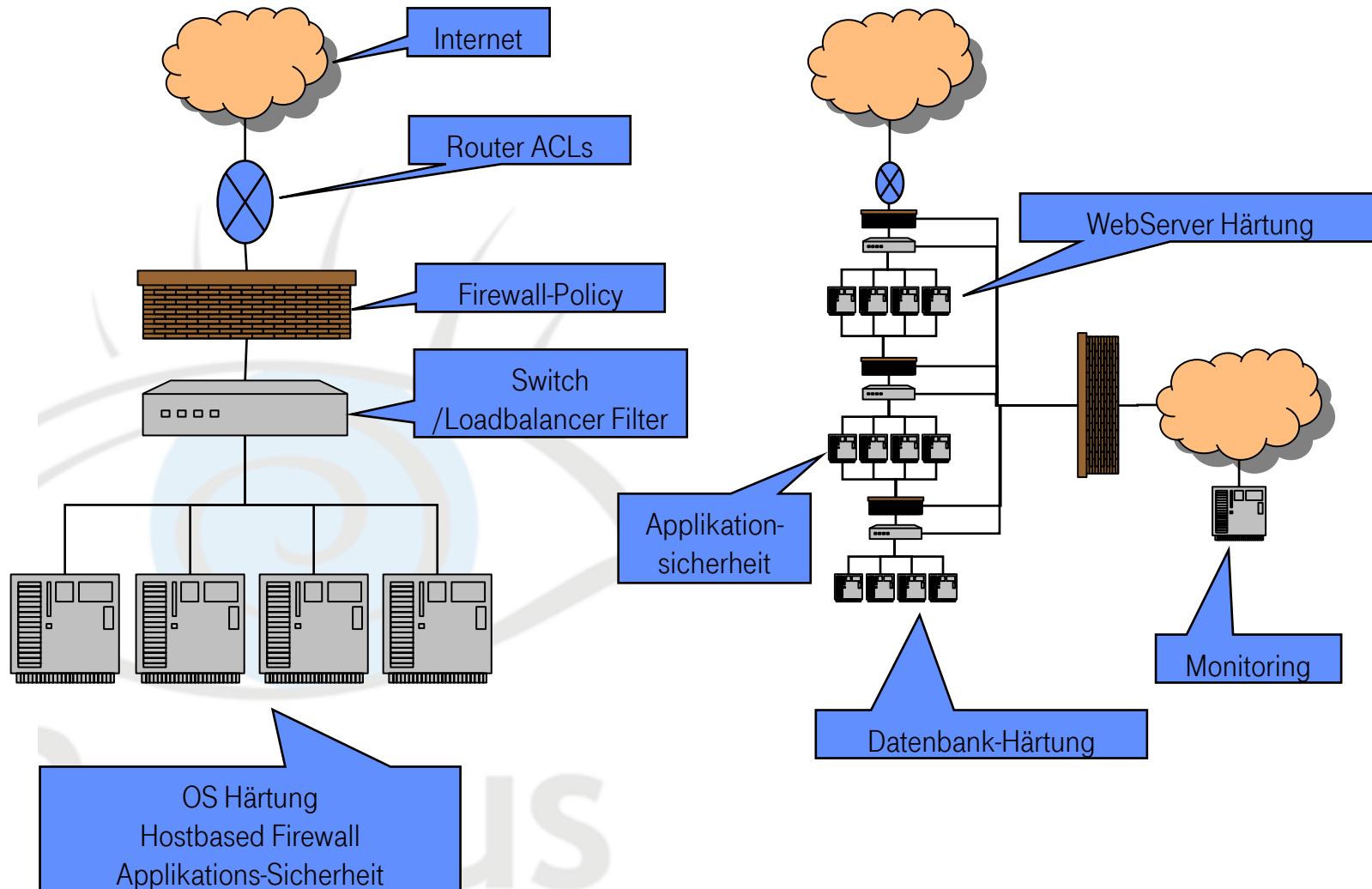
Hacken und Schutz von Informationen

Netzstrukturen



Hacken und Schutz von Informationen

sichere Strukturen



Sicherheit in Webapplikationen

Anforderungen

- Ids sollen nicht leicht ratbar sein

http://www.marktplatz.demo/katalog/edit.jsp?org_id=11

<http://www.email-umsonst.demo/lesen/user=1234>

Nicht durchzählen, sondern per Zufall aus einer großen Menge wählen oder Hashes, z.B. des Userobjects, verwenden.

- Typ der Parameter soll leicht verifizierbar sein.

Am Besten alles Integers oder Zeichenketten fester Länge und Struktur z.B.: AbxZ-018A-F0FF-0A01-AA0b
Das erschwert das Einfügen von z.B. SQL statements oder OS Befehlen

- Cookies sollen verschlüsselt sein und in sich auch ihr Gültigkeitsdatum enthalten

- Sowenig wie möglich "versteckte" Parameter.

Am Besten nur einen, der verschlüsselt ist und alle anderen enthält

- Alle Nutzereingaben müssen gefiltert werden (tainted mode) und in ihrer Länge auf der Serverseite beschränkt sein (Client side javascript zählt nicht)

Sicherheit in Webapplikationen

Anforderungen

- Kommunikation verschlüsseln

Verhindert "man in the middle" Angriff

Verhindert Abhören und Manipulation der Kommunikation

- Betriebssystemhärtungsmaßnahmen festlegen

Der Applikationsprogrammierer muss wissen, was sein Programm erwartet.

Am Besten testet der Entwickler auf einem gehärteten System.



HAW

Sicherheit in Webapplikationen

Anforderungen

- Applikation muss als Nicht-Administrator lauffähig sein

Benutzer "sa" unbedingt vermeiden

Stored Procedures anstatt SQL verwenden

- Zugriff auf "stored procedures" einschränken

xp_cmd_shell

- "Stored Procedures" verwenden

- SQL Bindvariables verwenden

- Fehlermeldungen nicht an Nutzer weiterleiten

Stattdessen Standardfehlerseite anzeigen

- JSP Kommentare "`<%/* ... */%>` statt HTML Kommentare

Kommentare liefern dem Angreifer zu viel Information

Jesus

Fallen in Webapplikationen

Ursachen: Warum sind die Applikationen schlecht?

Hauptursache:

Schlechte Beispiele aus Büchern,
von Demo-Applikationen oder aus dem Internet

Weiter:

- „geht doch!“ schnell mal was zusammengehackt
- Keine Zeit für Codereview
- Eigentlich bin ich „Datenbankadministrator“ / „Webdesigner“ / ...
- Keine Zeit! (sowieso)

Hersteller versprechen tolle Features. Alles ist ganz einfach!

Chef sagt: Warum kriegt Ihr das nicht hin?

Sicherheitskonzept: Was ist das?

Wir wissen selbst am Besten, wie wir unsere Maschinen zu sichern haben!

Sicherheit ist in den meisten Programmier-, Datenbank- und Betriebssystemkursen kein Thema. -> DoItYourself-"Sicherheitsexperte"

Webapplikationssicherheit

Was ist zu tun?

- Klare Vorgaben in klare Verträge schreiben!
- Realistische Projektpläne erkämpfen!!! (Tom DeMarco)
- Least Privilege Regel verwenden
 - Das gilt für Administratoren und Nutzer
 - Das gilt für Applikationen
 - Niemals den "sa" account verwenden (außer wenn der Server brennt)
 - Views verwenden und minimale "Sicht" erlauben
- OS härten und Applikationen patchen
- Sicherheitsschulungen sind notwendig!
- KISS (keep it simple stupid) !!! (Bruce Schneier)
- Code Review durch Experten
- Audits der Betriebsumgebung
- Intrusion Detection

Webapplikationssicherheit

Was muss der Programmierer tun?

-Niemals den Nutzereingaben trauen!

- Immer die Länge der Eingaben auf der Serverseite beschränken
- Immer den Datentyp prüfen
- Nur zulässige Zeichen durchlassen
- Sonderzeichen filtern oder abweisen: Apostroph, Semikolon, DashDash, ...
- Alle Eingaben bei SQL in Apostroph hüllen

-Least Privilege Regel verwenden

- Niemals den "sa" account verwenden (außer wenn der Server brennt)
- Views verwenden und minimale "Sicht" erlauben

-Stored Procedures verwenden und Parameter binden

- Unnötige Stored Procedures verbieten (xp_cmdshell, ...)
- OS härten und Applikationen patchen

lessus

Webapplication Security

Security Tools

- AppScan und AppShield von Sanctum Inc
- WebInspect von SPI Dynamics
- WPOISON
- Rats

- Nessus (Freeware von Renaud Deraison)
- Cybercop (Sniffer Technologies)
- Internet Scanner (Internet Security Systems)

nessus

Sicherheitsaudit

Allgemeines

- Vorbereitung
 - Erlaubnis des Rechnerbesitzers einholen
 - Erlaubnis des Netzwerkbesitzers einholen
 - Scan niemals unbeaufsichtigt durchführen
 - Administratoren in Bereitschaft während des Scans
- Durchführung
- Auswertung
 - Falsche Positive eliminieren
 - Statistische Darstellung
 - Anzahl der Rechner
 - Anzahl der Sicherheitslöcher
 - Risiko

nessus

Sicherheits-Schulung

Sicherheitsaudit Ergebnispräsentation

Sicherheit ist ein Prozess

Vorschläge für Prozessverbesserung

Dauerüberwachung

nessus

Sicherheit im Internet

internationale Websites

- <http://www.sans.org/>
- <http://www.astalavista.com/>
- http://www.atstake.com/security_news/
- <http://www.securityfocus.com/>

- <http://www.nessus.org/>
- <http://www.insecure.org/>
- <http://www.foundstone.com/>

nessus

Sicherheit im Internet

Deutsche Sicherheits-Websites

- <http://www.bsi.de/>
 - Bundesamt für Sicherheit in der Informationstechnik
- <http://www.kes.de/>
 - Zeitschrift
- <http://www.telesec.de/>
- <http://www.teletrust.de/>
- <http://www.datenschutz.de/>

nessus

Webapplication Security

Resources

- c't 24/2002 „Schotten dicht“ Daniel Naber
- <http://www.spidynamics.com/whitepapers/WhitepaperSQLInjection.pdf>
- Advanced SQL Injection:
http://www.ngsoftware.com/papers/advanced_sql_injection.pdf
- Sanctum Inc; Developing Secure Web Applications:
http://www.sanctuminc.com/pdf/WhitePaper_DevelopingSecureWebApps.pdf
- SQL Injection: Modes of Attack, Defence, and Why It Matters
Stuart McDonald http://rr.sans.org/appsec/SQL_injection.php
- SQL Injection Walkthrough
<http://www.anticrack.de/modules.php?op=modload&name=News&file=article&sid=2251>
- SQL Injection and Oracle, Part Two by Pete Finnigan
<http://online.securityfocus.com/infocus/1646>
- Hackproofing Oracle Application Servers by David Litchfield
<http://www.nextgenss.com/papers/hpoas.pdf>
- RFPlutonium to fuel your PHP-Nuke by RFP
<http://www.wiretrip.net/rfp/p/doc.asp?id=60&iface=6>

Sicherheit im Internet

Literaturhinweise

- Technische Bücher
 - Maximum Security; Anonymous; 1999
 - Web Security Sourcebook; Rubin, Geer & Ranum; 1997
 - Web Security & Commerce; Garfinkel & Spafford; 1997
 - Firewalls and Internet Security; Cheswick & Bellowin; 1994
 - Building Internet Firewalls; Chapman & Zwicky; 1995
 - Hacking Exposed Fifth Edition 2005
- Fun reading
 - The Cuckoo's Egg; Clifford Stoll; 1989
 - Cyberpunk; Hafner & Markoff; 1991
 - Snow Crash; Neal Stephenson; 1995
 - Secrets and Lies; Bruce Schneier
 - Beyond Fear; Bruce Schneier
 - Der Termin, Tom De Marco

Hacken und Schutz von Informationen

Ansprechpartner

T-Systems International GmbH

SSC ENPS / Technologiezentrum

Axel Nennker

Tel: 030 / 34 97 - 3256

Fax: 030 / 34 97 - 3257

email: axel.nennker@t-systems.com

lessus

Webapplication Security

Fragen



Zusammenfassung

Fragen???

nessus