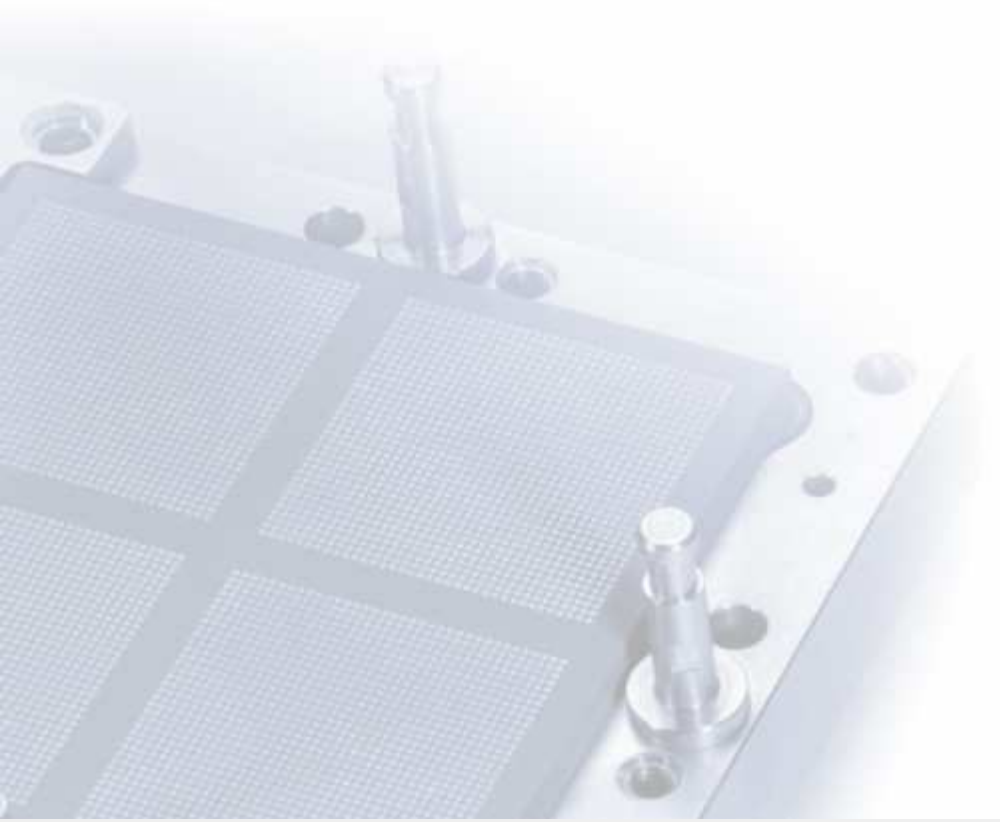
Leibniz Universität Hannover

Begrüßung & zur Sicherheitslage

Hergen Harnisch
harnisch@rrzn.uni-hannover.de



Programm

Montag 19.11.12

09:15-10:00 Sicherheitslage
10:00-11:00 Webanwendungen
11:00-11:30 *Pause*
11:30-12:15 FileVault 2
12:15-13:00 Sophos

Dienstag 20.11.12

09:15-10:30 Physische IT-Sicherheit
10:30-11:00 mobile Apps
11:00-11:30 *Pause*
11:30-12:15 Spam- & Virenabwehr
12:15-13:00 Abschlussdiskussion & Fragen

"Traditionelles":

Mobile IT

Cloud:

technische Probleme

organisatorische Probleme

Desktops/Notebooks

eigentlich keine wirklich neue Entwicklung:

- Drive-By-Downloads dominieren
- Spam wird zunehmend malicous
- direkte Angriffe kaum noch
- Malware installiert Rootkit, PC wird zum Bot
- Updates von OS *und* Applikationen wichtig

Trends & Veränderungen:

- Zweck ist weniger Bot, mehr Abgriff von Passwörtern / IDs
- rausgehenden Traffic an Firewall zu filtern & loggen ist wichtig
- mehr Filterung auf Applikationsebene (z.B. Proxy)

Server

Angriffe erfolgen über

- die angebotenen Applikationen (insbesondere Web-Server)
- Remote-Zugänge (z.B. ssh-Bruteforce)
- Server-Management-Zugänge (KVM over IP, IPMI)

Gegenmaßnahmen:

- Applikation absichern …
- Zugriff auf Applikation einschränken
- Teile der Applikation (z.B. Konfig-Seite) im Zugriff einschränken
- Abschotten der Managementzugänge

Social Engenieering

- zunehmend sowas wie „malicous spam“:
  Virus ist nicht in Mail sondern in verlinkter Webseite
- Phishing-Attacken auf LUH-Nutzer: einige wenige antworten

Fake-AV

- teilweise als zu kaufendes Produkt
- mit Handbuch, Support-Hotline …
- der Rechner wird sogar schneller

Smartphone & Tablets

Malware schon da, Security-Suites etablieren sich erst:

- meist ganze Management-Systeme für mobile Endgeräte
- Funktionen:
  - Malware-Scans
  - Lock-Down (Funktionseinschränkung, App-Auswahl)
  - Verschlüsselung
  - Fernlöschung

  Je nach Produkt und Endgerät unterschiedlich verlässlich.

Hat hauptsächlich 3 Aspekte:

- zunehmende Komplexität auf „embedded Devices“
- Nutzung von Cloud-Diensten sowie Apps
- häufig private Endgeräte

private Endgeräte

BYOD

Marketing: „Bring your own device“

Security: „Bring your owned device“

Eigentlich für uns nichts neues

- Studenten kommen mit eigenen Notebooks
- Mitarbeiter arbeiten auch zuhause, nutzen VPN etc.

private Endgeräte

aber:

- Zahl & Heterogenität der Geräte nimmt zu
- Forderungen nach Netz-Öffnungen werden stärker, Verlagerung zu Cloud-Diensten

In den Fokus rücken zunehmend rechtliche Fragen:

- durch stärke Nutzung entsteht stärkere Relevanz
- durch Nutzungsforderungen nun „aktenkundig“

Datenschutz personenbezogene Daten eher unzulässig

Hoheit Daten gehören der Universität

Zugriff kein Zugriff auf Geräte, kaum Vorgaben möglich

Begriff

Der Begriff ist äußerst schwammig …
Marketing nutzt ihn für alte Dinge

- Hosting bei Anbietern oder Providern
- Software-as-a-Service
- Webservice-Anbieter

Cloud ist z.B. neu bei:

- automatischer Verteilung (z.B. Amazon-EC2),
  anders als traditionelles Hosting virtueller Server
- externem Geflecht von Webservices verschiedener Anbieter,
  anders als SOA im Intranet

Trend: Daten liegen bei Anbieter statt Anbieter-Software beim Kunden.

Leibniz Universität Hannover

Schnittstellen

Cloud im eigentlichen Sinne benötigt technische Schnittstellen.

Diese basieren häufig auf

- SSL bzw. Zertifikaten & PKI
- XML (auch mit Signatur)

Beides sind komplexe, nicht immer korrekt implementierte Standards.

SSL

SSL ist komplex, APIs von SSL-Bibliotheken mindestens ebenso.

- Verschlüsslung reicht nicht, Schlüssel muss auch geheim sein
- beide Seiten authentifizieren, häufig wird Server vergessen
- Rückruflisten beachten (CRL, OCSP)
- worauf wird geprüft (DN, CN, Subject-Alternate-Name …)
- wird das Richtige signiert bzw. verschlüsselt?
- gibt es ein unsicheres Kompatibilitäts-Fallback?

aktuelle Probleme im Cloud-/Mobile-Kontext

„The most dangerous code in the world: validating SSL certificates in non-browser software“

vgl. https://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-client-bugs.html

XML-Signing

Wichtig z.B. bei der Security Assertion Markup Language (SAML)

- verwendet bei Webservices, auch bei Singe-Sign-Own im Browser
- Verschlüsselung der Verbindung reicht nicht, da Weiterleitung

XML Signature Wrapping

Angriffe basieren darauf, dass Standard-Bibliotheken fehlerhaft sind oder falsch eingebunden werden:

- fehlende Schema-Validierung
- doppelte ID-Vergabe
- Trennung von XML- & Signatur-Validierung von der Verarbeitung

vgl. z.B. http://www.dfn-cert.de/dokumente/workshop/2012/Folien_Mayer.pdf

Rechtliches

Allen voran Datenschutz:

- Wie der Auskunftspflicht nachkommen, wenn unklar ist, wo die Daten liegen?
- Auftragsdatenverarbeitung
- … und das meist nicht (ausschließlich) in Deutschland oder EU

Insbesondere bei kostenfreien Diensten:

- Wer schließt Vertrag ab, wie sieht der aus?
- evt. nur für private Nutzung zugelassen
- Registrierung auf Personen nicht Einrichtungen
- Wer besitzt Daten oder Nutzungsrechte daran?

Man muss eigentlich wie bei Auftragsdatenverarbeitung vorgehen!

Leibniz Universität Hannover

Vertrauen & Vertrausstellungen

Einräumen von Zugriffsrechten

Webservices zur Nutzung anderer Webservices erfordern AAA als Nutzer

einfach Passwort-Hinterlegung
z.B. zum Abholen von Mails beim fremden Provider

sicherer mit Token, z.B. OAuth

komplex, erfordert Vertrauen, möglichst kleinteilige Rechtestrukturen

Alles im Browser

öffentliche Webseiten & schützenswerte Anwendungen nebeneinander

- XSS & CSRF bedrohen immer wichtigere Dienste

→ Sandboxing von Browseraufrufen statt des Browsers?

Leibniz Universität Hannover

Derzeitige Situation

Herausforderung:

- die meisten Cloud-Dienste nicht für schützenswerte Daten geeignet
- die Funktionalität meist besser als eigene Dienste

nötig:

- Verständnis & Verantwortung des Anwenders
- Schaffung von nutzbaren Cloud-Alternativen
- Verbesserung von Cloud-Angeboten bzgl. Sicherheit & Rechtslage