Sicherheit und Risikomanagement

- Auswahl von Sicherheitsmechanismen: Sicherheit / Kosten / Risiko -

U. Hübner (HIS GmbH) / M. Pattloch (DFN-Verein)

huebner@his.de / pattloch@dfn.de

DFN-Nutzergruppe Hochschulverwaltung

8 . Tagung in Halle, 8. Mai 2007

Sicherheitsmechanismen

- Grundsätzlich breites Spektrum, z.B.
  - Verschlüsselung von Datenbanken
  - Pseudonymisierung
  - Integritätssicherung Hard- und Software

- im Folgenden Konzentration auf

  Authentifizierung von Nutzern

Integration IT-Sicherheit

- Idealfall
  - IT-Sicherheit ohne Zusatzaufwand „integriert“
  - IT-Sicherheit für Nutzer transparent
- Praxis / Realität
  - differenzierte Sensibilitätsniveaus
  - Kompetenz für Konzepte und Betrieb erforderlich
  - (immer) zusätzlicher Aufwand
  - Kriterien für die Auswahl von Lösungselementen oft nicht transparent (PINs, TANs, Passwörter, zusätzliche Software, etc.)

Nutzer Authentifizierung

- Einige Mechanismen sind "Stand der Technik“ und stehen selten zur Disposition, z.B.
  - SSL/TLS zwischen Klient und Server (mit Serverzertifikat)
- Optionen für die Authentifizierung von Nutzern
  - Wissen (Passwort/Phrase)
  - Besitz (TAN-Liste, Hardware-, Software-Token)
  - Sein/Können (Biometrie)

Wie absichern?

- Wissen (Passwort/Phrase)
  - sehr variable Sicherheit, aber
  - wie und wo sind Vergleichsmuster abgelegt?
- Besitz (TAN-Liste, iTANs)
  - wenig technische Anforderungen, aber
  - Zusatzaufwand für Handling
- Besitz (Hardware-, Software-Token)
  - gut geeignet für Klientenzertifikate, aber
  - hohe technische Anforderungen
- Sein/Können (Biometrie)
  - *Ernüchterung durch „Gummibärchen-Gelatine“*

Gummibärchen-Gelatine

http://crypto.csail.mit.edu/classes/6.857/papers/gummy-slides.pdf

Mehrfaktor-Verfahren

- Kombination mehrerer Schutzmechanismen
  - gegen breites Risikospektrum
  - größere Sicherheit
  - höherer Aufwand
- Beispiele:
  - Passwort + TAN
  - Passwort + Klientenzertifikat

Single Sign-On

- *pro*: kommt mit wenigen Merkmalen pro Person aus
- *kontra*: es gibt “besonders wertvolle” Merkmale
- Aktionen unterschiedlicher Sensibilität ggf. unterschiedlich absichern
  - nach Art der Authentifizierung kann Zutritt zu / Zugriff auf Bereiche unterschiedlicher Sensibilität gewährt / verweigert werden

Anwendung

- Typische sensible Prozesse an Hochschulen
  - Student meldet sich zur Prüfung an
  - Prüfer registriert Leistungen
  - Student ruft Prüfungsergebnisse ab
  - Administrator stellt Prozessparameter ein
  - Verwaltungsmitarbeiter erstellt Zeugnisse

Was bedeutet „Risiko“?

- Risiko enthält viele monetär schwierig zu bewertende Komponenten:
  - Rufschädigung / entgangenes "Geschäft"
  - Verlust von Zuwendungsgebern / Studenten
  - Rechtsstreit
  - Beeinträchtigung der Effizienz des Handelns (Papierprozess neben IT ...)
  - gesetzliche Konsequenzen

Angriffsszenarien

- Manipulation auf der Serverseite
  - Software-Anfälligkeiten oder Administratoren
- Manipulation netzseitig
  - MitM, Verbindung mit Fake-Server, "Abhören"
- Manipulation eines Klientenrechners
  - Keylogger ...
- "Social Engineering“
  - “Schicken Sie bitte mal schnell ...”

Risiken

- Person kann Status einer anderen manipulieren
  - "Fake-Anmeldung" zu irgendetwas
- Person kann eigenen Status manipulieren
  - Leistungsstand ...
- Person kann Falschinformation einbringen
  - “Prüfung fällt aus” ...
- Person sieht unbefugt Informationen ein
  - Noten
- Person kann Verfügbarkeit beeinflussen
  - Verteilung knapper Ressourcen
- .....

Risiken

- mindern
  - Auditierung der serverseitigen Soft- und Hardware
  - Komplexität begrenzen
- beseitigen
  - Netz: SSL/TLS mit gutem Zertifikat-Management
- akzeptieren
  - Nutzersensibilisierung
- vermeiden
  - bei Prozessgestaltung berücksichtigen

ROSI ?

“Return on Security Investment”

Gibt es so etwas wie ROSI?

- *kontra*: IT-Sicherheit ist vergleichbar mit Versicherung: Risiken sind identifiziert und „abgefedert“
- *pro*: erst durch die Einführung von IT-Sicherheitsmaßnahmen werden manche Anwendungen und Workflows ermöglicht

Kosten (1)

- Versuch einer Kalkulation der Kosten
- wir bitten um Rückkopplung/Korrektur zu unseren Annahmen/Zahlen!
- Annahmen
  - alle einmaligen Kosten werden über 4 Jahre verteilt (Nutzungsdauer ohne größere Änderungsaufwendungen)
  - Nutzerzahl: 20.000
  - Kosten pro Personentag (PT): 600 EUR

Kosten (2)

- Passwortadministration
  - Parametrisierung 100 PT einmalig
  - Helpdesk (für vergessene/vertippte Passworte): jeder 20. Student verursacht 10 min/Jahr, d.h. 200 PT für 20.000 Studenten
  - ergibt 135.000 EUR/Jahr

- TAN Administration
  - vergleichbar mit Passwortadministation, d.h. zusätzlich 135.000 EUR/Jahr (bei TANs für alle)

Kosten (3)

- Klientenzertifikate
  - Parametrisierung 200 PT einmalig
  - Helpdesk (für verlorengegangene Zertifikate: Handhabungsprobleme, ...): jeder 20. Student verursacht 20 min/Jahr, d.h. 400 PT für 20.000 Studenten
  - ergibt 270.000 EUR/Jahr
  - Hardware Token 30 EUR, d.h. 600.000 EUR für 20.000 Studenten (evtl. vom Studenten zu tragen?)

Zusammenfassung

- Risikoanalyse ist Bestandteil des IT-Sicherheitskonzepts
  - "Lösung sucht Problem" vermeiden
- realistische Risiko-Behandlung einplanen und implementieren
  - Menschen und Prozesse vor "Geräten"
  - Differenzierung
- Kosten realistisch ermitteln und einplanen
  - Hauptkostenfaktor: Behandlung von "Sonder- und anderen Störfällen"