13tes EntwicklerCamp

Hotel Maritim, Gelsenkirchen

17. - 19. März 2014

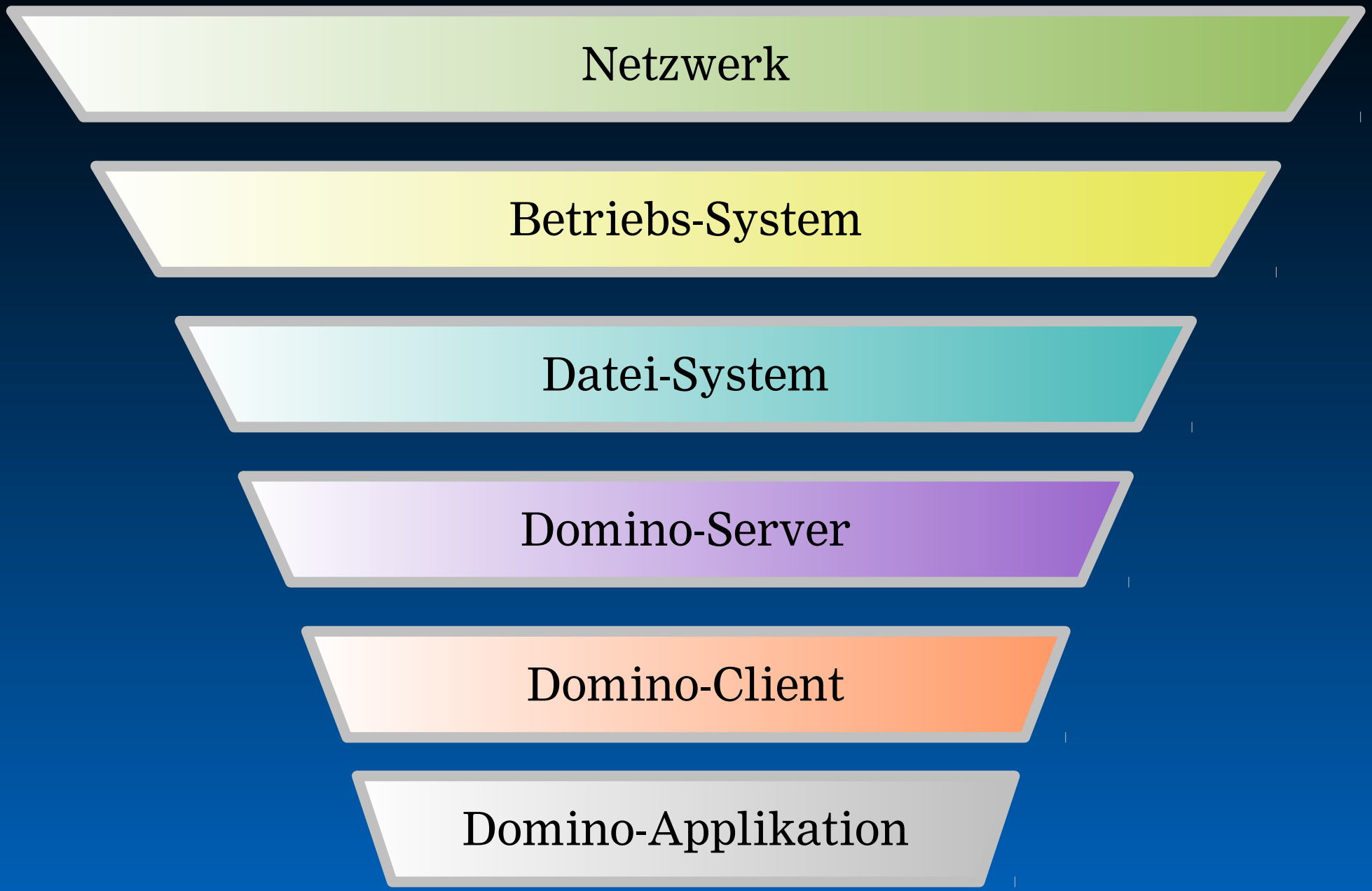
IBM Domino Notes Database Security

Analyse, Konzept und Techniken

C. Habermueller

http://chabermu.wordpress.com

Sicherheitsmodell


Netzwerk
Betriebs-System
Datei-System
Domino-Server
Domino-Client
Domino-Applikation

Unterschiede in der Sicherheitsbetrachtung

Domino-Administrator

Verwendet ein vorgegebenes Zugriffskonzept !

Domino-Entwickler

Entwickelt pro Applikation
ein individuelles Zugriffskonzept !

Schematischer Aufbau einer Domino-Datei


Gestaltung
Dokumente
Zugriff

Was kann wie zugriffsberechtigt werden ?

Zugriffs-kontrollliste

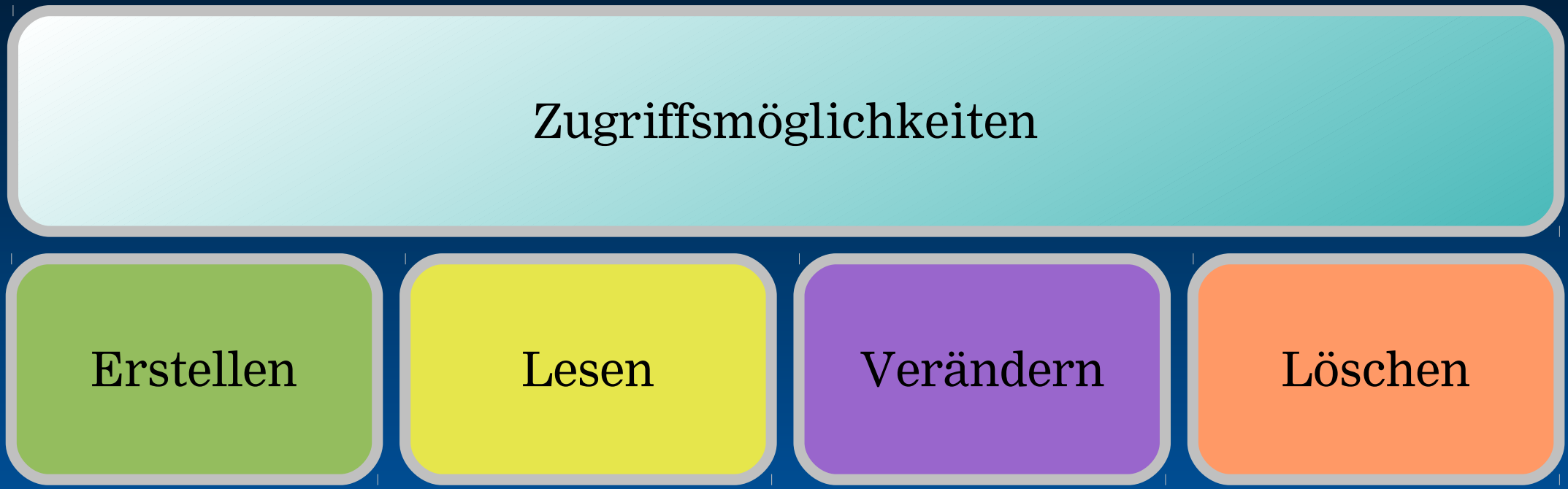
Gestaltung verbergen

Leserfeld

Autorfeld

Zugriffs-kontrollliste

Unterteilung der Zugriffsmöglichkeiten


Zugriffsmöglichkeiten
Erstellen
Lesen
Verändern
Löschen

Neue Dokumente erstellen

Neue Dokumente erstellen

Einschränkung über Zugriffskontrollliste

Alle anderen Techniken sind unsicher

Ein neues Dokument kann z. B. mit der Kopierfunktion der Zwischenablage erstellt werden

Regeln: Neue Dokumente erstellen

Zugriffsstufe *Leser* darf **nur** lesen aber **nichts** erstellen

Erstellberechtigung lediglich für die Zugriffsstufe *Autor* entziehbar

Editor sowie jede höhere Zugriffsstufe kann **uneingeschränkt** neue Dokumente erstellen

Vorhandene Dokumente lesen

Vorhandene Dokumente lesen

Einschränkung über **Leserfeld**

Alle anderen Techniken sind unsicher

Dokument kann z. B. über eine persönliche Ansicht gelesen werden

Regeln: Vorhandene Dokumente lesen

Jedes Dokument

__ohne__ Leserfeld bzw.

mit Leserfeld __ohne Inhalt__

ist für **jede** Zugriffsstufe ab *Leser* sichtbar

Leserfelder **ergänzen** sich gegenseitig

Im Leserfeld stets **Rollenbezeichnungen** verwenden

niemals: Einzelnamen oder Gruppenbezeichnungen !

Sichtbares Dokument verändern

Sichtbares Dokument verändern

Einschränkung über **Autorfeld**

Alle anderen Techniken sind unsicher

Dokument kann z. B. mittels eines Agenten verändert werden

Regeln: Sichtbares Dokument verändern

Jede höhere Zugriffsstufe als *Autor* kann **alle** sichtbaren Dokumente verändern

Autorenfelder **ergänzen** sich gegenseitig

Autorfeld erteilt auch **Lesezugriff** !!!

Im Autorenfeld stets **Rollenbezeichnungen** verwenden

niemals: Einzelname / Gruppenbezeichnungen !

Wichtiger Hinweis

Ein Ersteller kann seine eigenen Dokumente nicht mehr verändern, wenn ...

*1.) ... seine Zugriffsstufe **Autor** ist und*
2.) ... ein Autorfeld diesen Zugriff verhindert

Sichtbares Dokument löschen

Sichtbares Dokument löschen

Einschränkung über **Zugriffskontrollliste**

Alle anderen Techniken sind unsicher

Dokument kann z. B. mittels eines Agenten gelöscht werden

Regel: Sichtbares Dokument löschen

Löschberechtigung für **jede** Zugriffsstufe ab *Autor* einstellbar

Hinweise zu: *Dokument löschen*

Dokumenteninhalte können auch durch
***überschreiben** der Feldinhalte*
gelöscht werden

Unsichtbare Dokumente können
*von **niemanden***
gelöscht werden

Wichtiger Hinweis

Dabei stets auch an die Replikation denken !

Replikation

Server auf Server

»Server bestimmen die Zugriffssteuerung

Server auf Client

»Client übernimmt nun die Zugriffssteuerung

Unterschiede zwischen
Server & Client
bezüglich Sicherheit

Unterschiede zwischen Server & Client bezüglich Sicherheit

Server

- BIOS- & BS-Zugang geschützt
- Dateisystem geschützt
- Zugriff über Netzwerk
  - Server steuern Berechtigungen

Client

- BIOS- & BS-Zugang meist ungeschützt
- Dateisystem meist ungeschützt
- Zugriff über Dateisystem
  - Client steuert Berechtigungen

Regel: Client steuert Berechtigung

Generell gilt …

*Auf eine Applikation, die über das Dateisystem geöffnet werden kann, hat man **Managerzugriff***

Unabhängig von der Einstellung der Zugriffskontrollliste !!!

… wenn die DB **lokal unverschlüsselt** ist,
… und solange, bis *konstistente Zugriffskontrollliste* markiert ist !

Regeln: Konsistente Zugriffskontrollliste

Client anerkennt Zugriffskontrollliste

»Inkonsistent bedeutet: **stets** *Managerzugriff*

Client anerkennt Rollen

»Inkonsistent bedeutet: Rollen **nicht** auslesenbar

Aber: Nettes Leistungsmerkmal, jedoch kein wirksamer Schutz

»Kann mit Spezialkenntnissen umgangen werden, Zeitaufwand: 30 Sekunden

Zugriffssteuerung bei Web-Applikationen

Unterschied zwischen Intra- & Internet bezüglich Sicherheit

Intranet

»Zugriff kann authentifiziert werden

»Server & Client steuern **gemeinsam** die Berechtigung

User.ID vorhanden

Internet

»Zugriff kann nicht **nicht** authentifiziert werden

»Server steuert **alleinig** die Berechtigung

***Keine** User.ID vorhanden*

Ein Web-Browser verfügt
nicht *über eine User.ID,*
die ein Domino-Server zur Zugriffsberechtigung
verwenden könnte.

Was nun ?

Lösung:

Benutzername und Internet-Kennwort zur Authentifikation

Damit beim Web-Zugriff auf eine DB
der Benutzername und das Internet-Kennwort
abgefragt wird,
muß in der DB-Zugriffskontrollliste der Eintrag

Anonymous = kein Zugriff
Typ = unspezifiziert

eingestellt sein.

Die Zugriffskontrollliste verfügt über eine Web-Zugriffsschranke

Wichtiger Hinweis

Für die Web-Programmierung gelten dokumentierte Einschränkungen.

Bestimmte Eigenschaften, @Funktionen und LotusScript sind ***funktionslos*** *(not supported)*

Ungeeignete Elemente für die Zugriffssicherheit

Diese Aufzählung ist nicht vollständig !

Ungeeignet für die Erstellberechtigung

Manche Gestaltungselementeigenschaften

Ungeeignet für die Leseberechtigung

Ansichtsselektionsformeln
Selektive Replikation
Verberge-Wenn-Eigenschaften
Manche Gestaltungselementeigenschaften

Ungeeignet für Editierberechtigung

Zugriffsgesteuerte Abschnitte ohne Unterschrift
Eingabeberechtigung

Ungeeignet für die Löschberechtigung

Ergebnisse mit programmiertem Abbruch beim Moduswechsel

Diese Präsentation ist ausschließlich für den informativen Einsatzzweck gedacht und wird als diese ohne jegliche Garantie oder Gewährleistung bereitgestellt.

Der Autor ist ausdrücklich nicht haftbar für mögliche Folgen oder mögliche Schäden, die durch die Verwendung des bereitgestellten Materials entstehen können oder könnten.

Hinweise, Verweise oder Verknüpfungen bzw. Links in diesem Material unterliegen ebenfalls diesem Haftungsausschluß und sind Eigentum des jeweiligen Rechteinhabers.

Die Rechte von geschützten Markennamen, Handelsmarken sowie alle weiteren Rechte unterliegen dem jeweiligen Rechteinhaber und bzw. oder des Eigentümers derselben.

Diese Präsentation ist urheberrechtlich geschützt.