HanseCom InformationsTechnologie

Sicherheit in der Notes Entwicklung?

Oder … wie werde ich Revisors Liebling!

Ulf.Duvigneau@HanseCom.com

SOLUTIONS
Führende IT-Lösungen im ÖPV

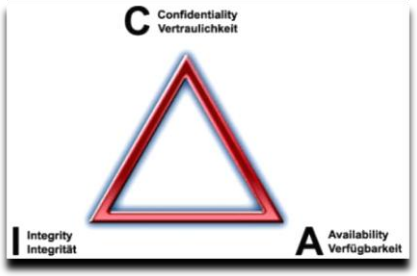
CONSULT
Individuelle IT-Prozessberatung

OPERATE
IT-Betrieb für den Mittelstand

Agenda

- Informationssicherheit
- Domino Sicherheitsebenen
- Agentensicherheit
- Worauf sollten Entwickler achten?
- Zusammenfassung

Informationssicherheit

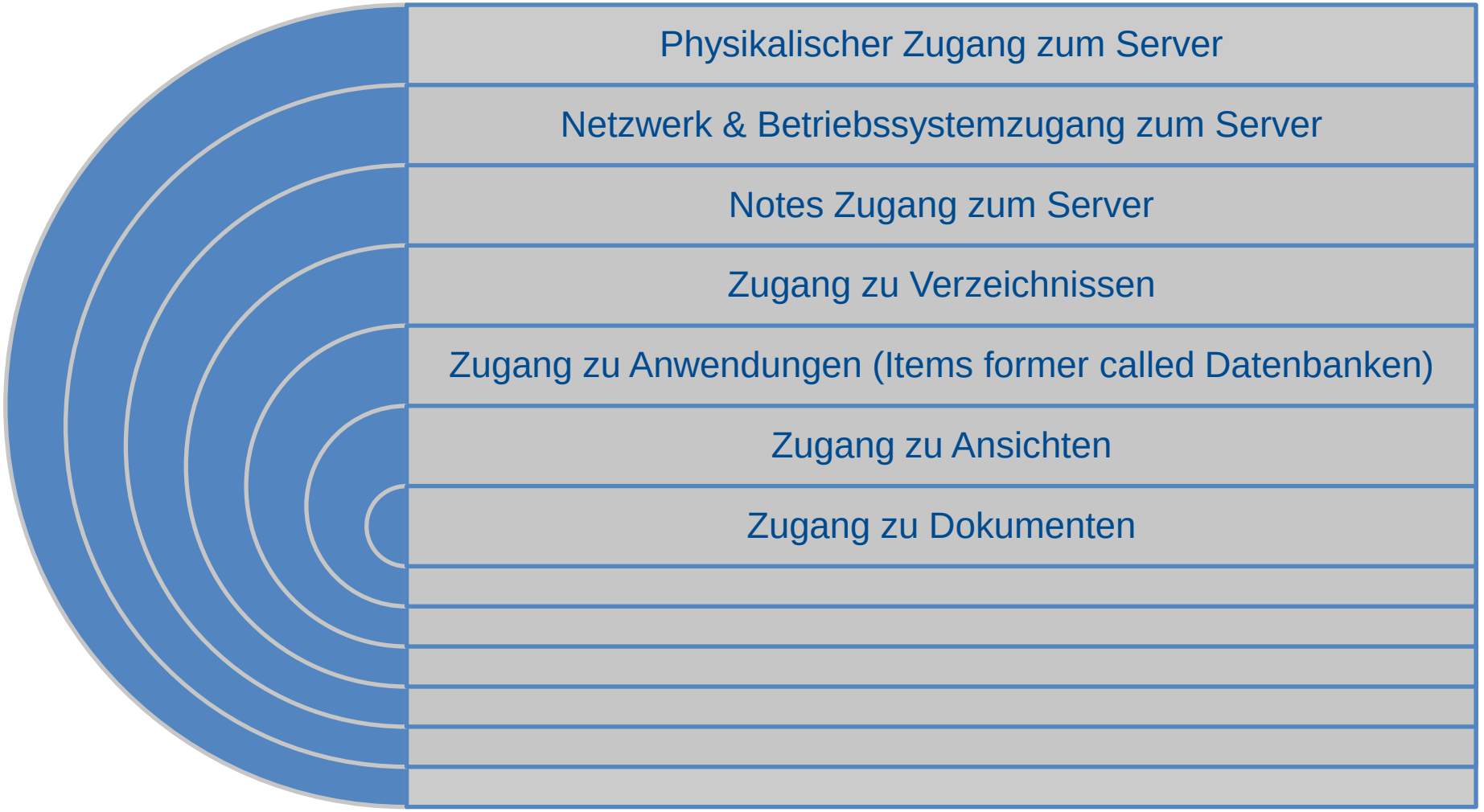


- **Vertraulichkeit**
  „Vertraulichkeit ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein. Weitergabe und Veröffentlichung sind nicht erwünscht. Vertraulichkeit wird durch Rechtsnormen geschützt, sie kann auch durch technische Mittel gefördert oder erzwungen werden. “
- Verfügbarkeit
  „Die Verfügbarkeit eines technischen Systems ist die Wahrscheinlichkeit oder das Maß, dass das System bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllt. Sie ist ein Qualitätskriterium und eine Kennzahl eines Systems. “
- **Integrität**
  „Integrität ist die Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen .“

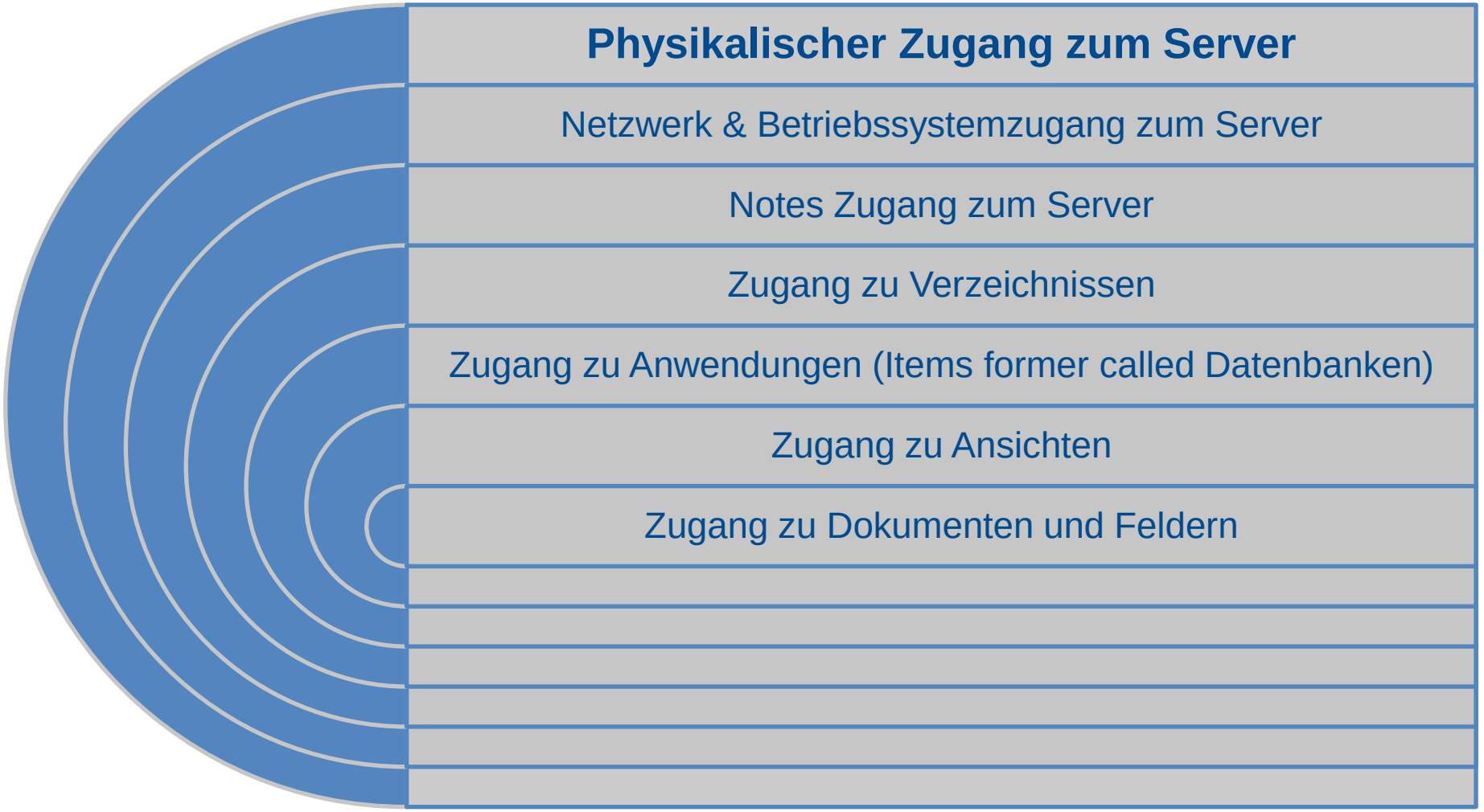
Gefährdung der Informationssicherheit

Bedrohung	Countermeasure
Deny of service Attacken	Firewalls Internet-Lockout Agentsicherheit Ausführungskontrollliste ECL
Abhören	Verschlüsselung
Vertraulichkeit	Verschlüsselung Dokumentenrechte
Authentifizierung	Ids, Benutzernamen & Kennwörter Zertifikate
Verfälschung	Signatur Datensicherung
Unbefugter Zugriff	Zugriffskontrollliste Dokumentenrechte

Domino Sicherheits-Ebenen



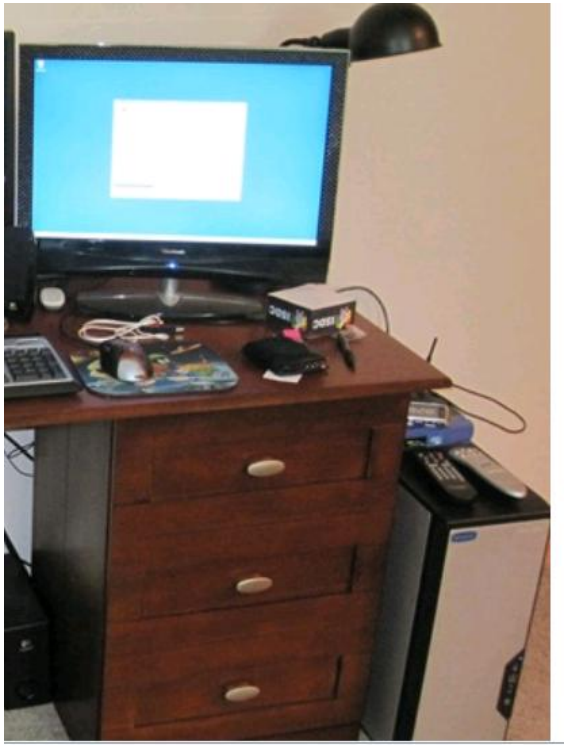
Domino Sicherheits-Ebenen



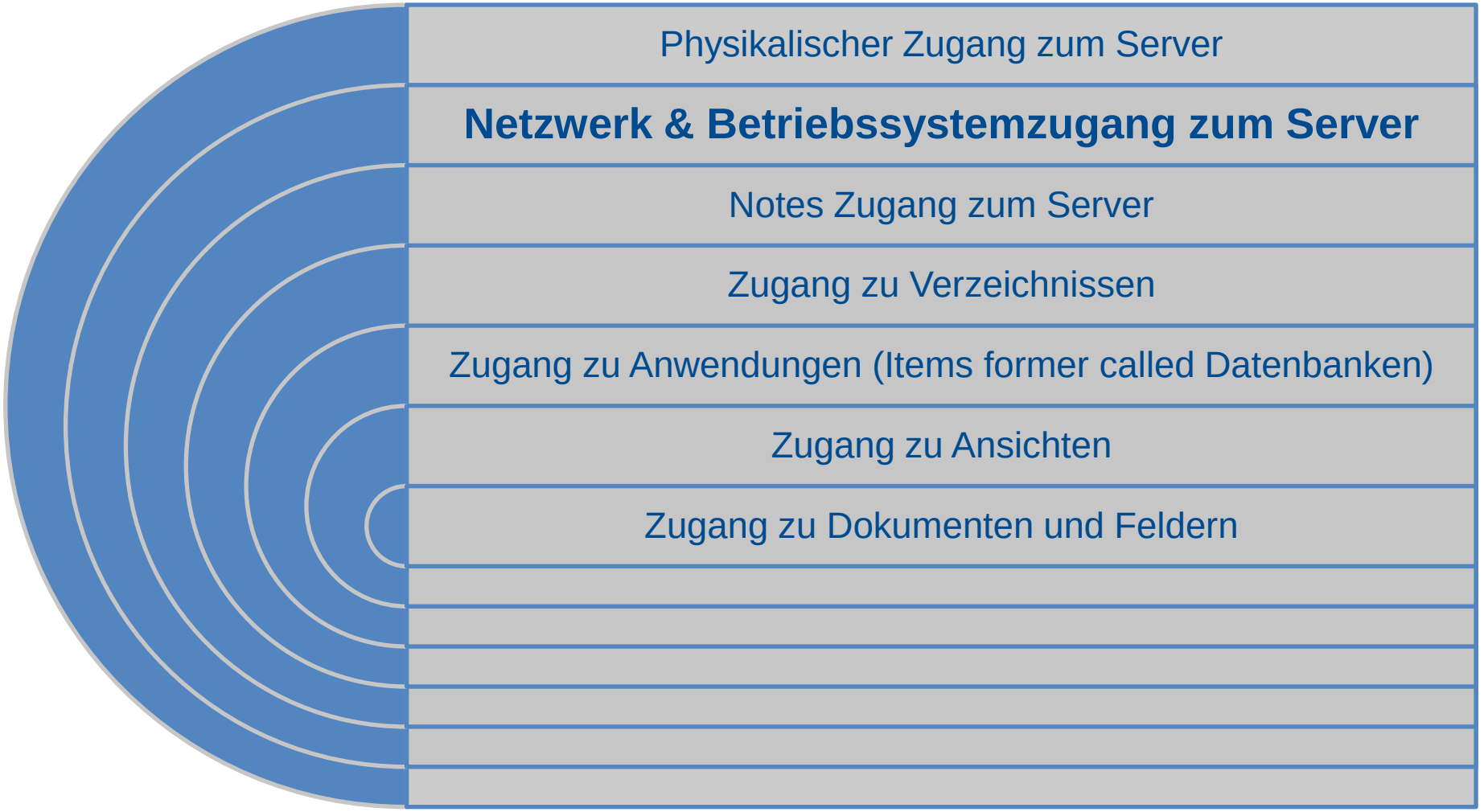
Physikalischer Zugang zum Domino Server

Lieber so …

… als so

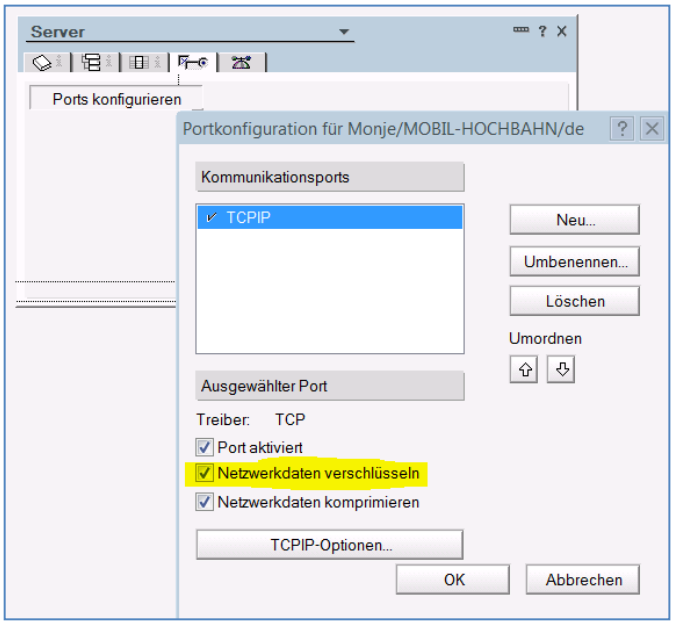


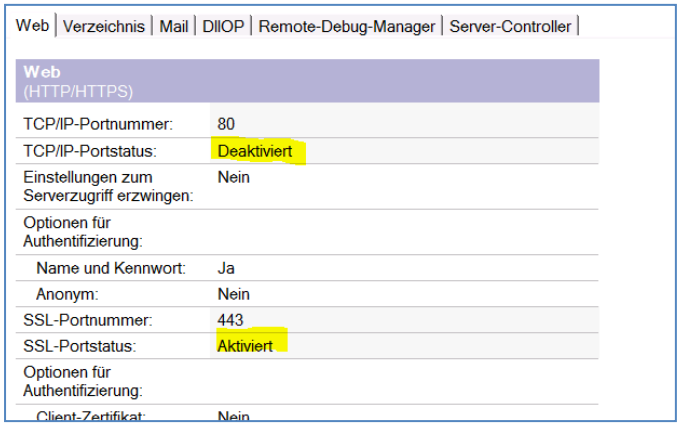
Domino Sicherheits-Ebenen



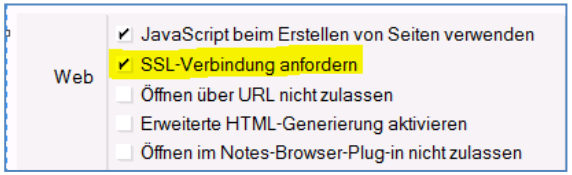
Netzwerk Zugang zum Server

- Der Netzwerkverkehr zwischen Notes Client und Domino Server lässt sich verschlüsseln.
  (Admin-Client – Server–Eigenschaft)
- Auch für den Browserzugang http > https
  (x.509 Zertifikat wird benötigt, Server-Dok. > Ports > InternetPorts)



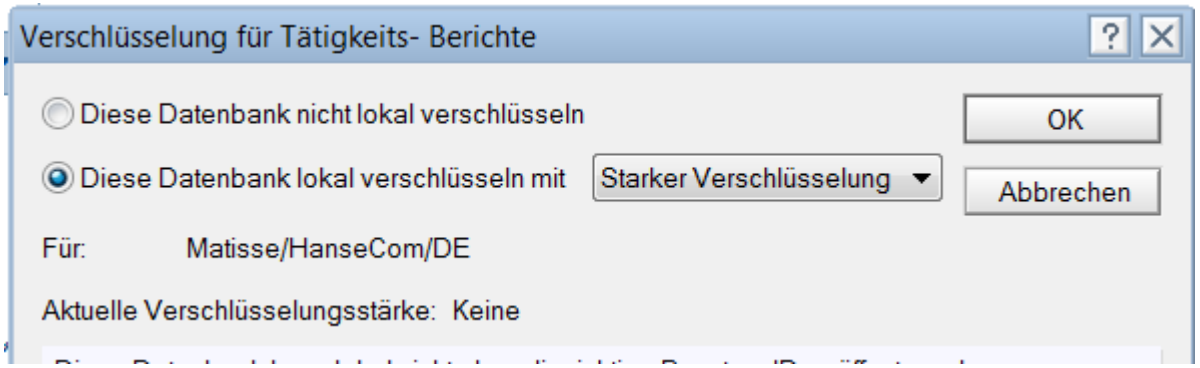


- Zusätzlich noch in den Eigenschaften der Anwendung



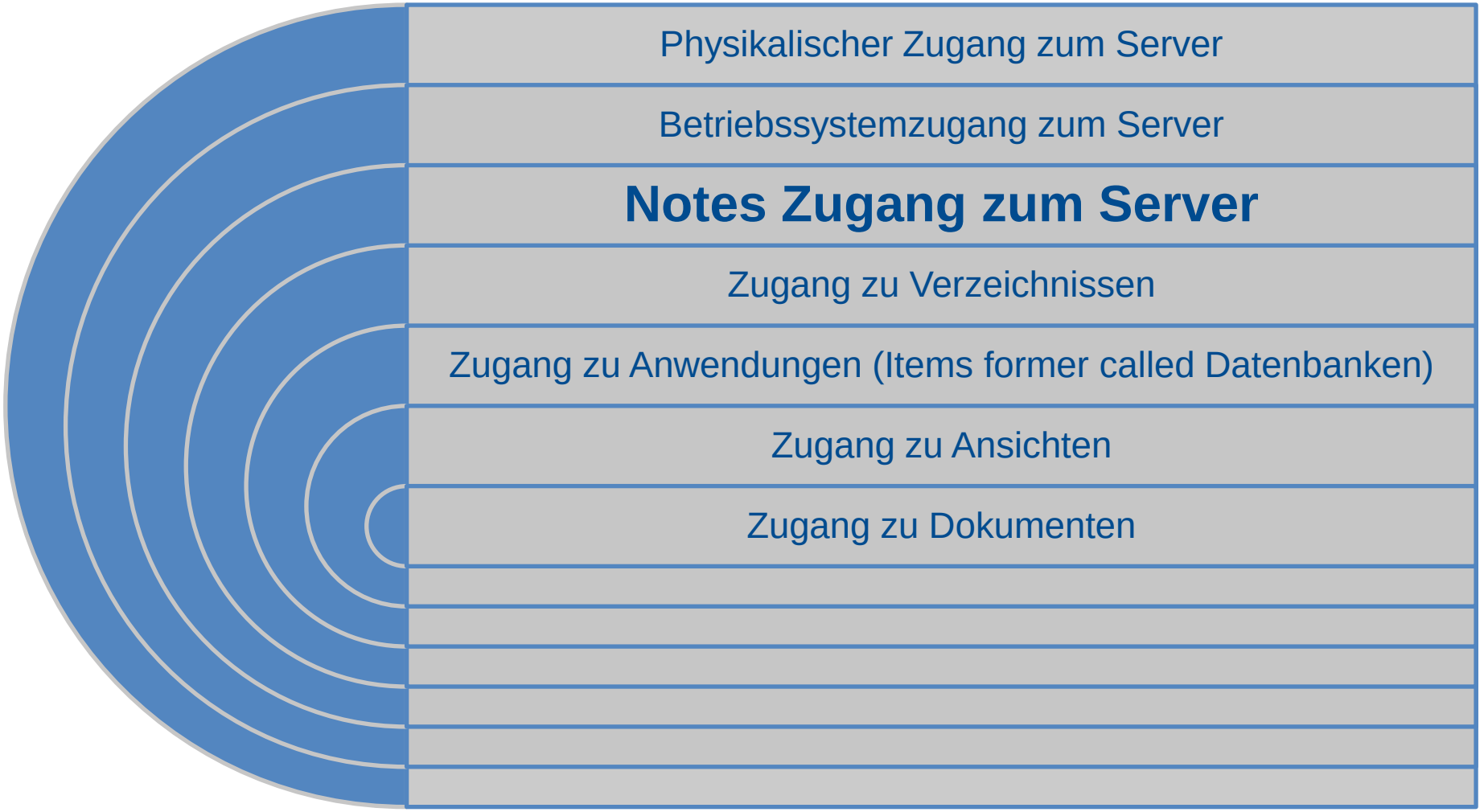
Betriebssystem Zugang zum Server

- Warum muss ein Domino Server in einer (Windows) Domäne stehen?
- Damit sich alle daran anmelden können … Genau!
- Domänen Policys erleichtern die OS Administration des Servers. (WSUS, Zeit etc…)
- Countermeasures:
  - Verschlüsselung der Anwendungen mit Server ID



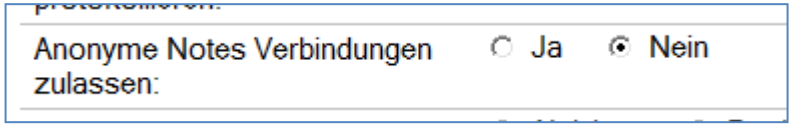
  - Server ID mit Kennwort versehen
    (Auch gut für Entwickler Server, die in einer VM auf einer externen Platte betrieben werden)

Domino Sicherheits-Ebenen

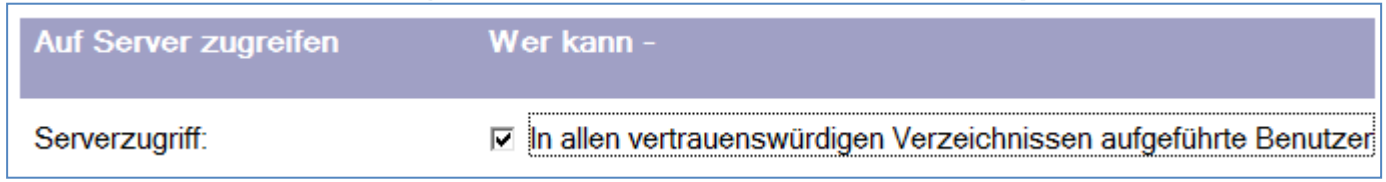


Notes Zugang zum Server
(Serverdokument Register Sicherheit)

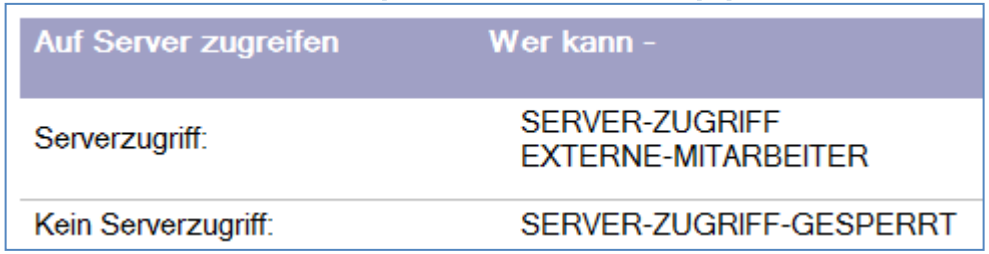
- Generell: Anwender, die mit derselben ID zugelassen wurden wie der Server, sonst Querzulassung.
- Oder Anwender, dessen Personendokument im Directory (names.nsf) des Servers ist



- Oder Anwender, die in vertrauenswürdigen Verzeichnissen sind (Stichwort: Directory Assistance)



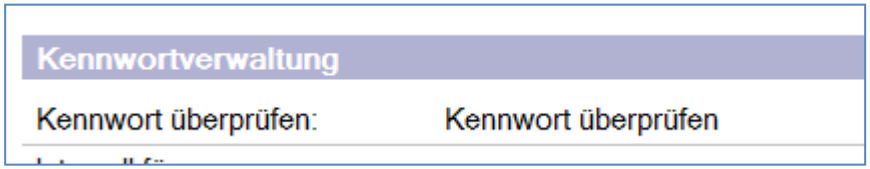
- Oder Anwender, die in speziellen Gruppen stehen



Notes Zugang zum Server
(Serverdokument Register Sicherheit)

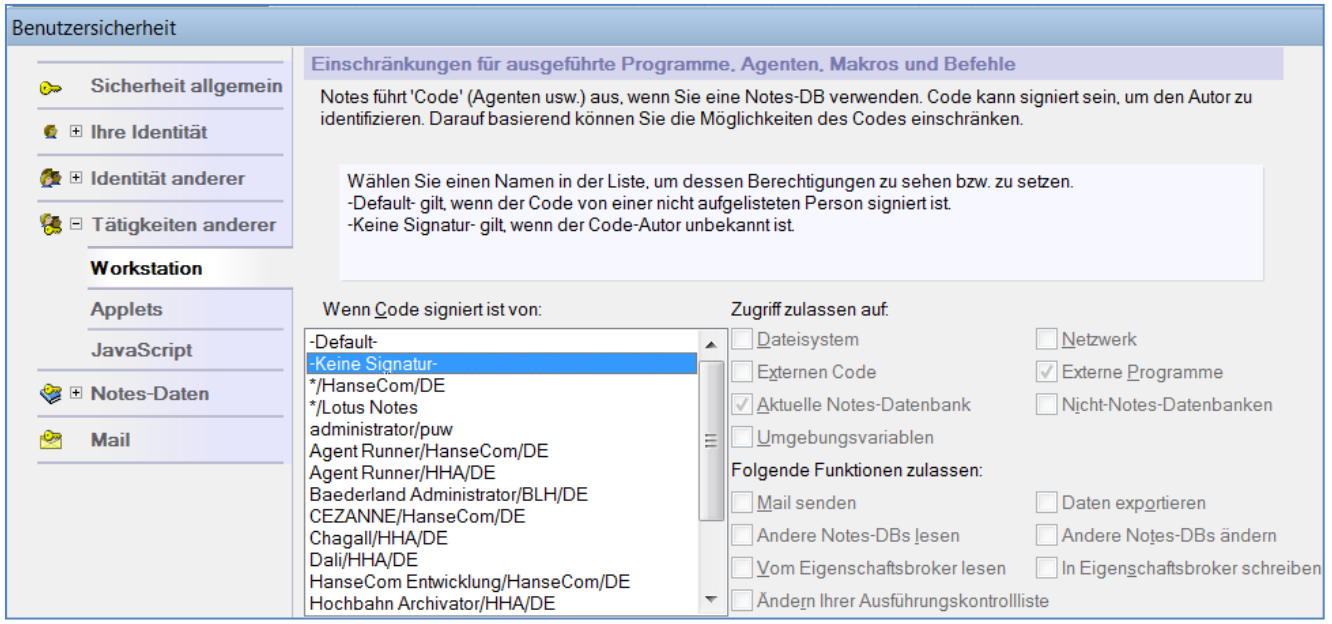
- Zusätzlicher Schutz vor alten Ids mit alten Kennwörtern:

- Zusätzlich in den Personendokumenten die Kennwortüberprüfung im Register Administration aktivieren



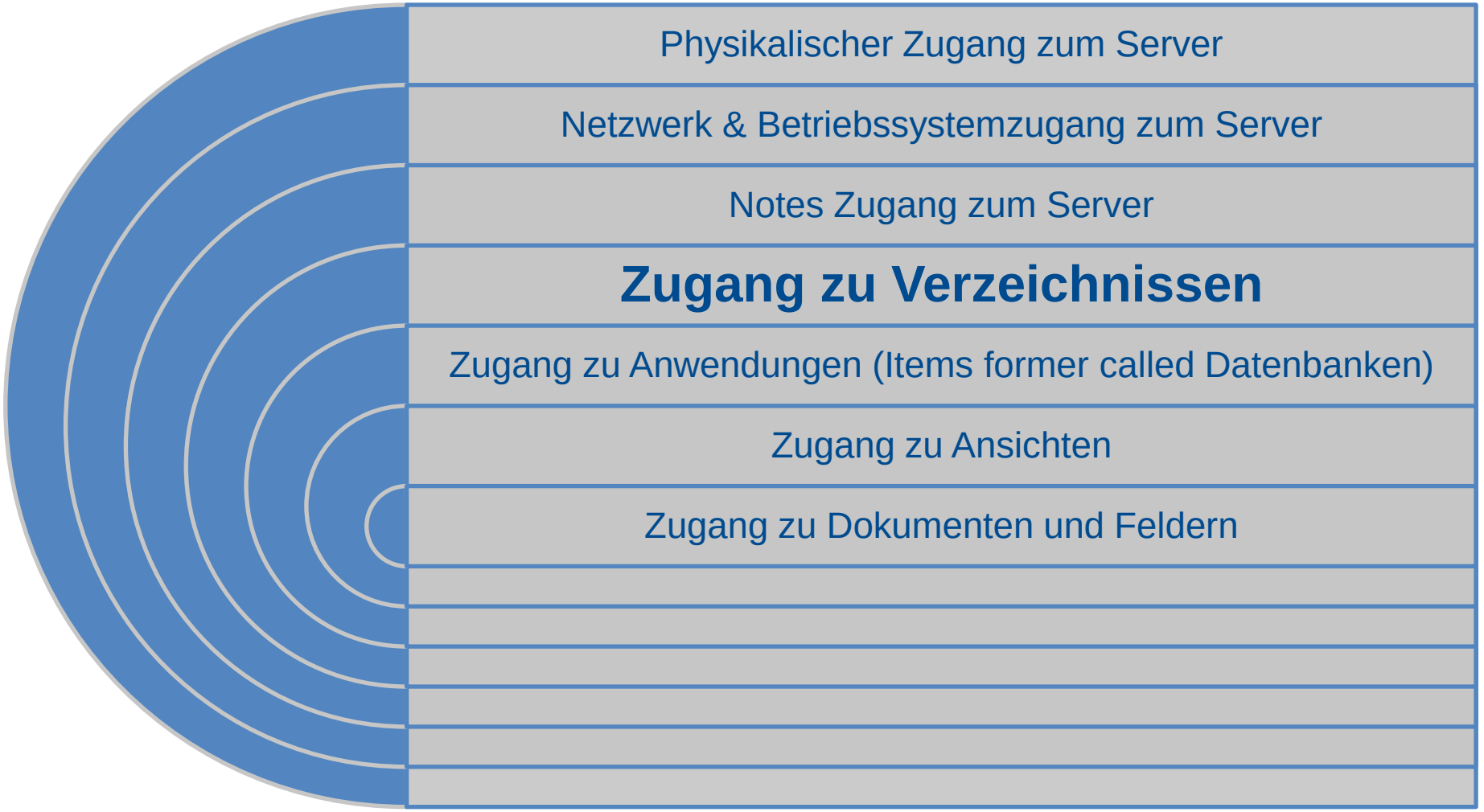
Notes Zugang zum Server

- Ausführungskontrollliste – ECL Execution Controll List
- Verhindert, das nicht autorisierte Entwickler, Schadcode im Notes Client zur Ausführung bringen
- Aufgabe der Administratoren!
- Menü Datei > Sicherheit > Benutzersicherheit



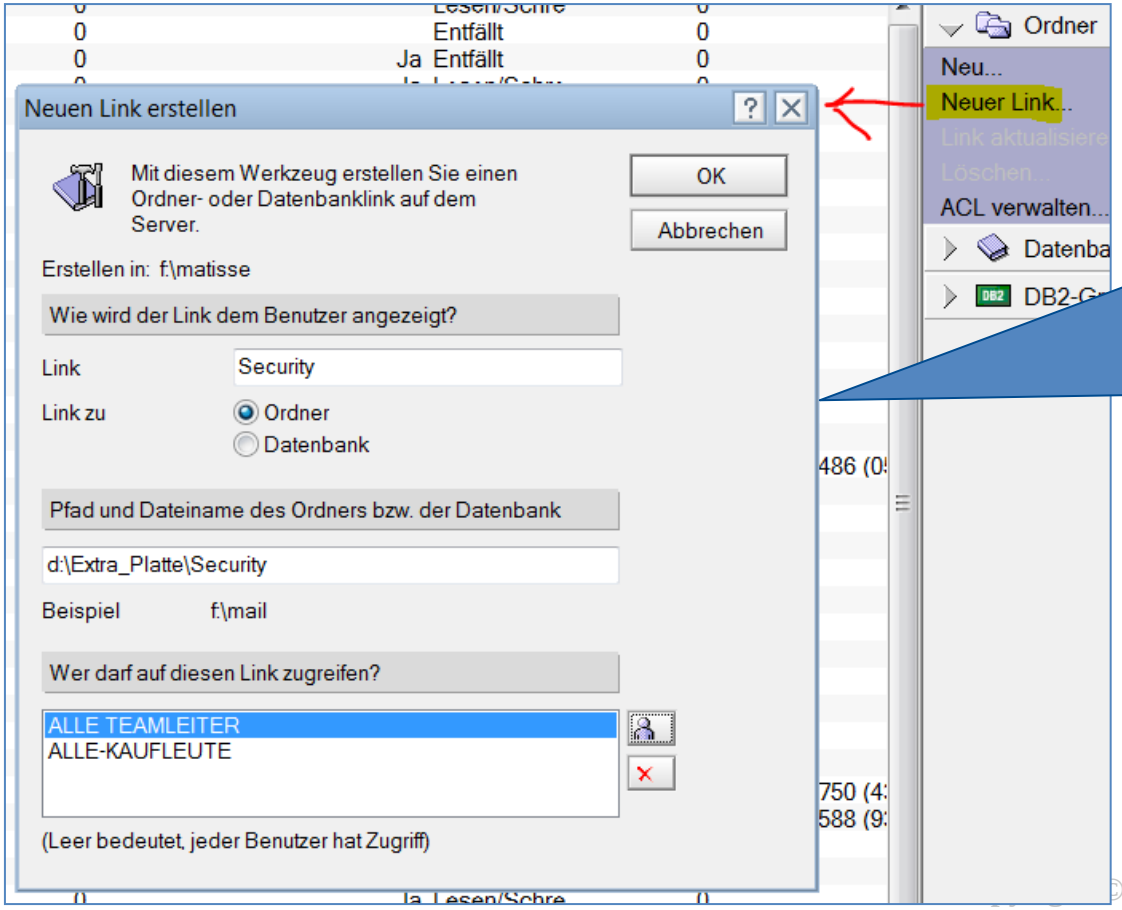
Der Admin setzt dies im Directory unter Aktionen >Administrations ECL bearbeiten.
Ein netter Admin kann den Entwickler seines Vertrauens mit einer besonderen ECL ausstatten, mit der er leichter entwickeln kann.

Domino Sicherheits-Ebenen



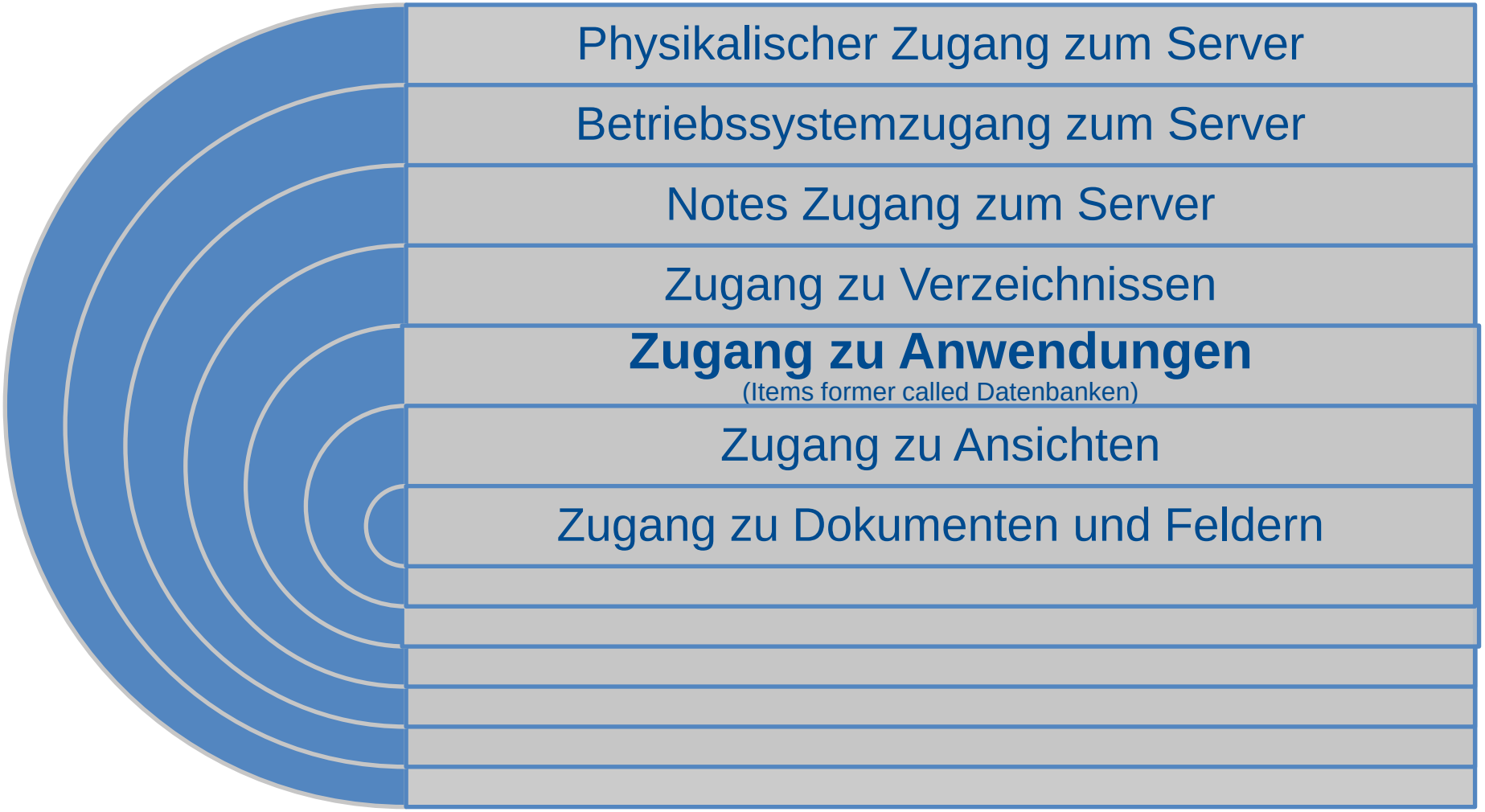
Zugang zu Verzeichnissen

- Auf Domino Servern können Ordner außerhalb des Domino Datenverzeichnisses mit besonderen Zugriffsrechten benutzt werden



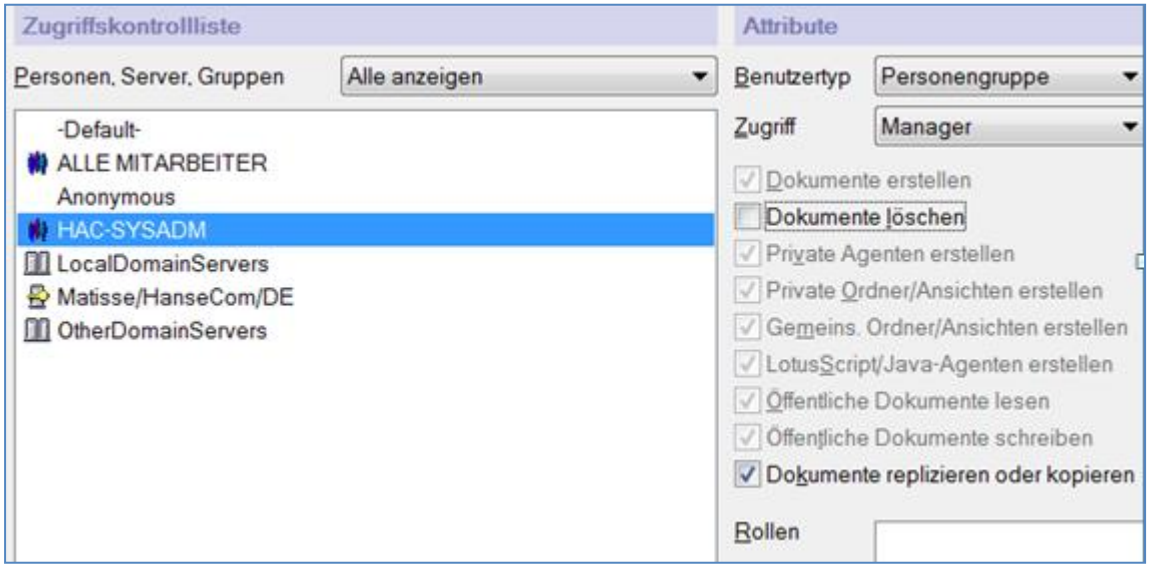
Das Ergebnis ist eine Textdatei Security.dir im Datenverzeichnis mit den Zeilen:
D:\extra_Platte\Security
Alle Teamleiter
Alle-Kaufleute

Domino Sicherheits-Ebenen



Zugang zu Anwendungen

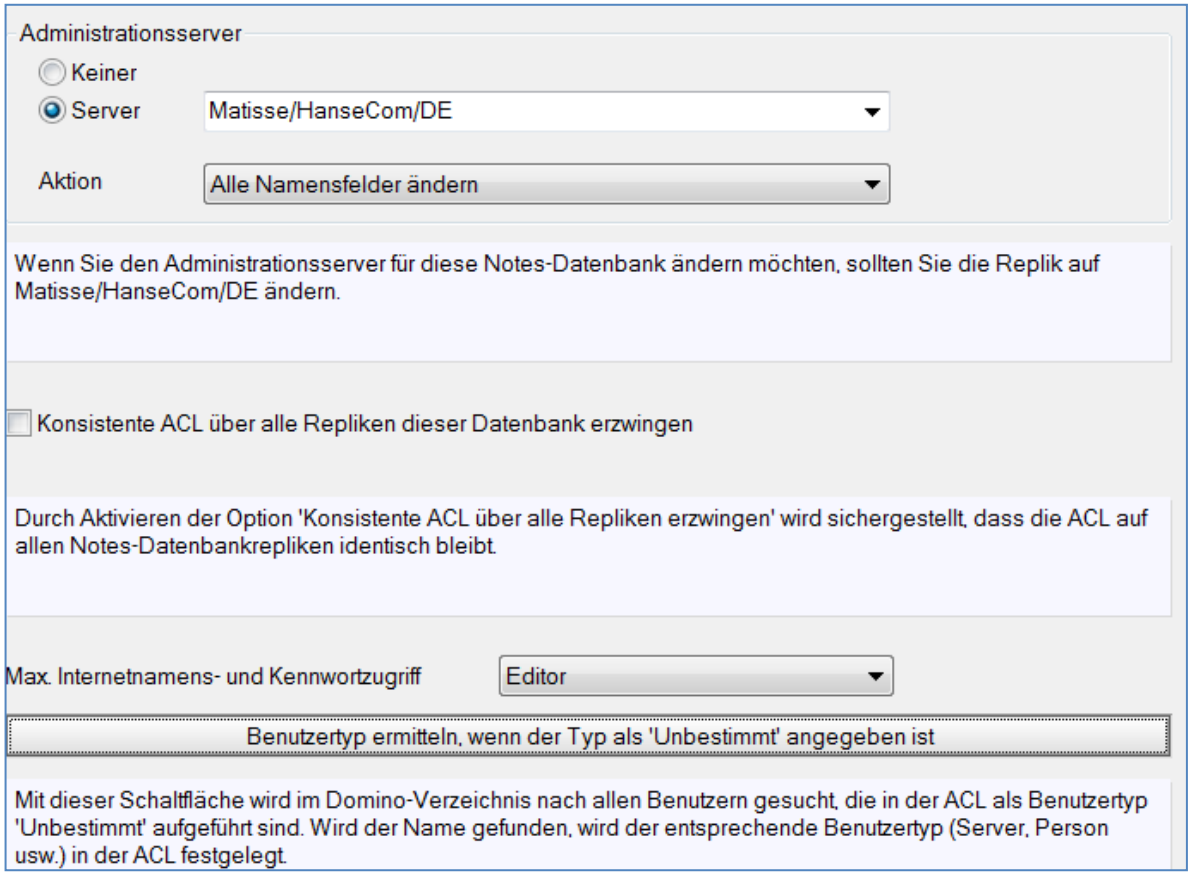
- Jede Anwendung (NSF) hat eine Zugriffskontrollliste (ACL - Access Control List).
- Sieben Rechte-Ebenen
  - Archivar
  - Leser
  - Autor
  - Editor
  - Entwickler
  - Manager



- Rollen (Anzahl beschränkt) , Benutzertyp (zus. Sicherheit)
- Änderungsprotokoll
- Anonymous eintragen und „kein Zugriff“, -Default- auch!
- Gruppen immer besser als Personen,- Änderung delegierbar!

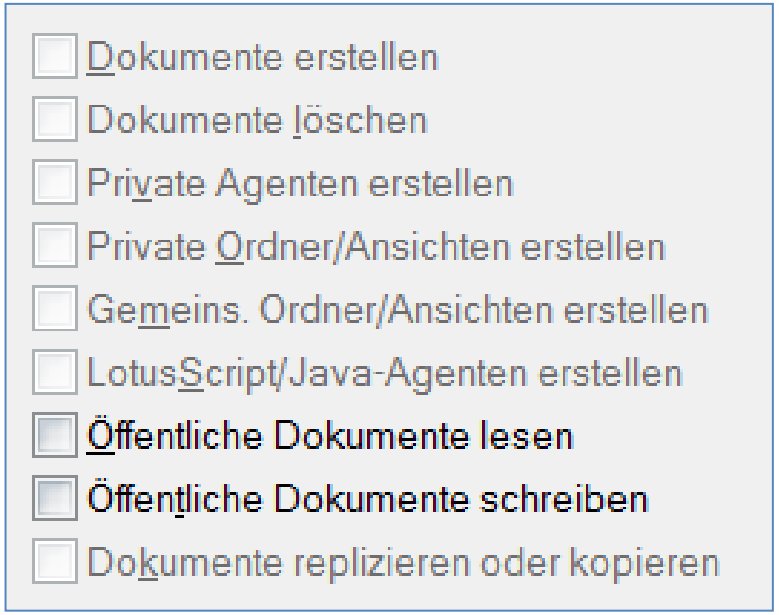
Zugang zu Anwendungen

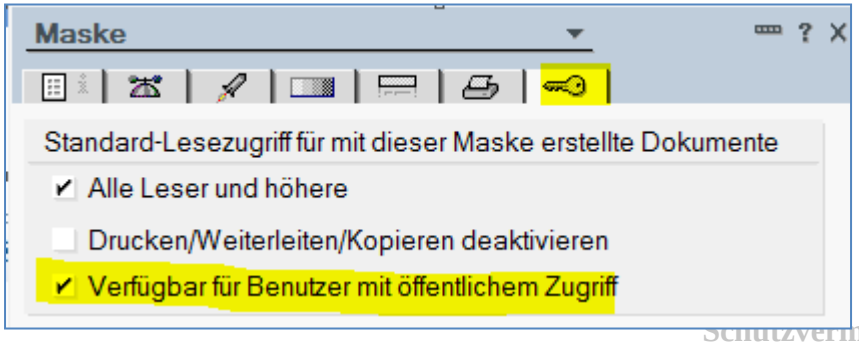
- ERWEITERT:
- AdminServer – wichtig bei Anwender Umbenennung
- Konsistente ACL – Rechte auf allen Repliken (lokal) gleich.
- Max. Internet Zugriff – Wenn nicht geplant „Kein Zugriff“



Zugang zu Anwendungen

- Zusätzliche ACL Optionen – je nach Zugriffsebene wählbar:
- Agenten immer deaktivieren bei Anwendern
- „Dokumente replizieren oder kopieren“ bei vertraulichen Anwendungen, oder solchen die nicht offline funktionieren, deaktivieren
- Mögliche Zweiklassengesellschaft in einer Anwendung: Öffentliche Dokumente in Kombination mit „Kein Zugriff“. Dokument-Arten, die öffentlich und solche, die vertraulich sind. Maskeneigenschaft:



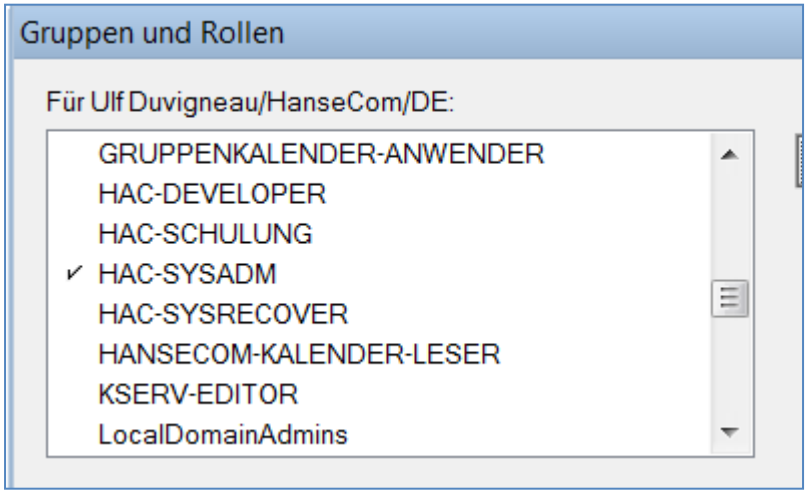


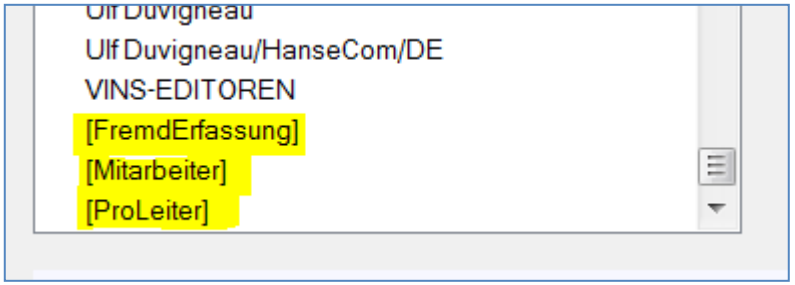
Zugang zu Anwendungen

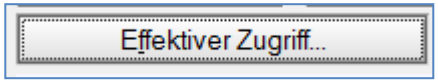
- „**Butter bei die Fische**“ – Wie funktioniert die ACL?

Zugang zu Anwendungen

- Die effektiven Rechte eines Anwenders, lassen sich an seinem Arbeitsplatz über das Symbol und einen Klick darauf erkennen. Die zugriffstärkste Gruppe ist markiert, die vorhandenen Rollen werden unten aufgelistet



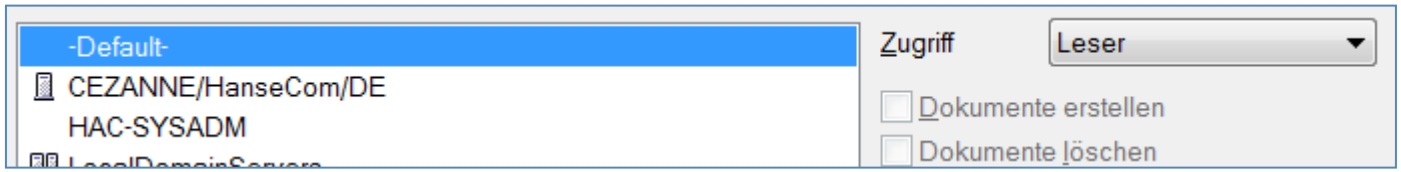


- Damit bei einer lokalen Replik die Rollen greifen, muss die „konsistente ACL“ aktiviert sein
- Aus der Anwendungs-ACL über 

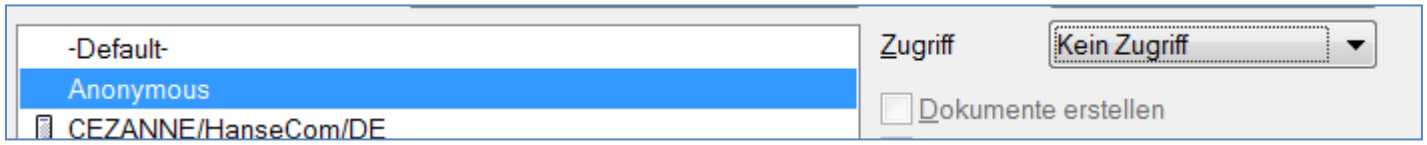
auswertbar.

Zugang zu Anwendungen

- Anwendung mit dieser ACL wird ins Web gestellt. Was passiert?



- Die Anwendung ist ohne Authentifizierung im Web zu öffnen, da bei fehlendem „Anonymous“ für alle nicht angemeldeten Anwender „-Default-“ greift.



Zugang zu Anwendungen

- Anwenderin Claire Cheffin ist Mitglied der Gruppen Geschäftsführung und Kaufmannschaft. Welche Rechte erhält sie bei dieser ACL?

Gruppe	Zugriff	Rolle(n)
Geschäftsführung	Editor	[VETO]
Kaufmannschaft	Autor	[GO] [VERWALTUNG]

- Frau Cheffin hat Editor-Rechte und die Rollen [VETO], [GO] und [VERWALTUNG]
- Gruppen Rechte sind kumulativ.

Zugang zu Anwendungen

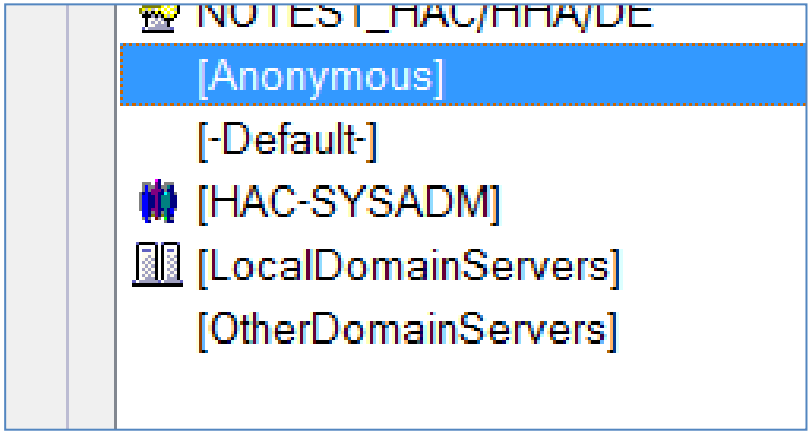
- Der Kaufmann Dennis Depp ist Mitglied der Gruppen Kaufmannschaft. Welche Rechte erhält er bei dieser ACL?

Gruppe	Zugriff	Rolle(n)
Dennis Depp	Kein Zugriff	
Kaufmannschaft	Autor	[GO] [VERWALTUNG]

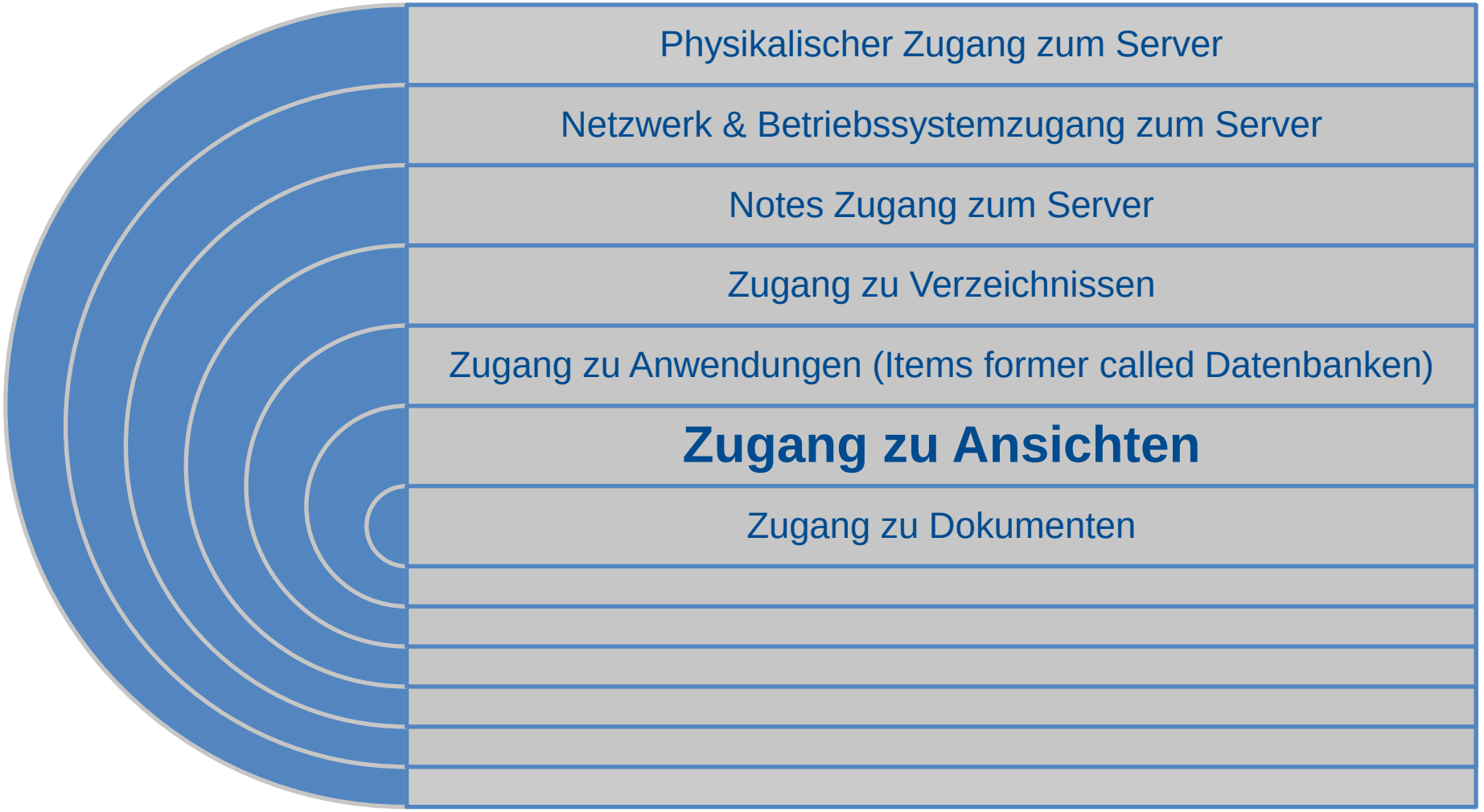
- Herr Depp erhält keinen Zugriff auf die Anwendung. (Auch keine Rollen)
- Personeneinträge stechen Gruppen-Einträge.

Zugang zu Anwendungen

- Best Practices oder „Wie mache ich meinen Administrator glücklich?“
- Schablonen aus denen eine Vielzahl von Anwendungen erstellt werden, sollten Vorgabe-Einstellungen haben. Diese werden beim Erstellen der Anwendung automatisch in der ACL erzeugt.

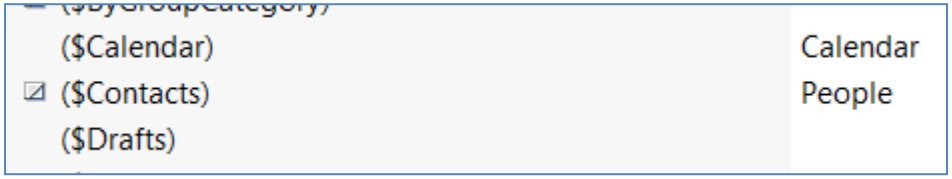


Domino Sicherheits-Ebenen

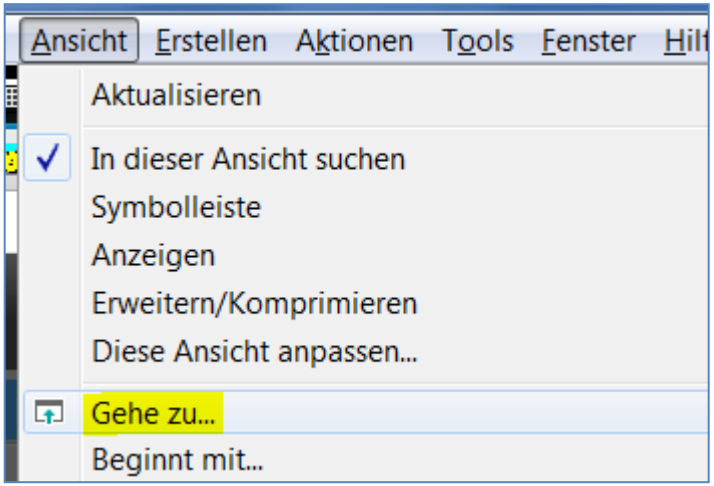


Zugang zu Ansichten

- Wird der Name einer Ansicht in „()“ geschrieben, ist sie in der Navigation der Anwendung nicht zu sehen.

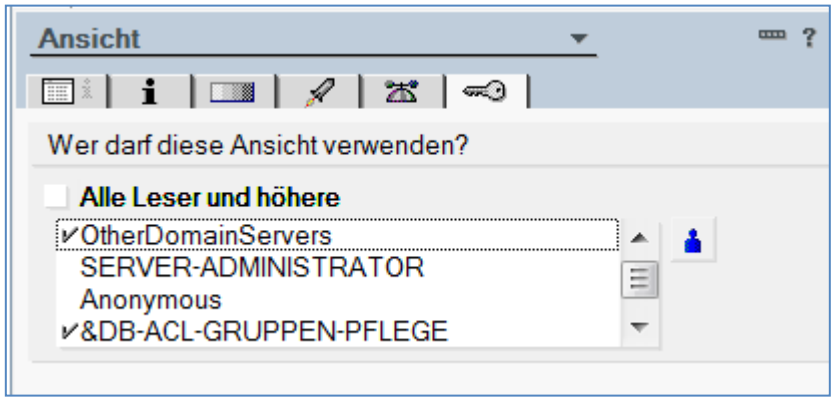


- Ist dies ein Schutz?
- Nein! Über STRG+SHIFT und das Menü Ansicht > Gehe zu sehe ich alles

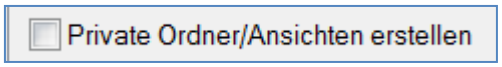


Zugang zu Ansichten

- Ein besserer Schutz ist der Leseschutz einer Ansicht

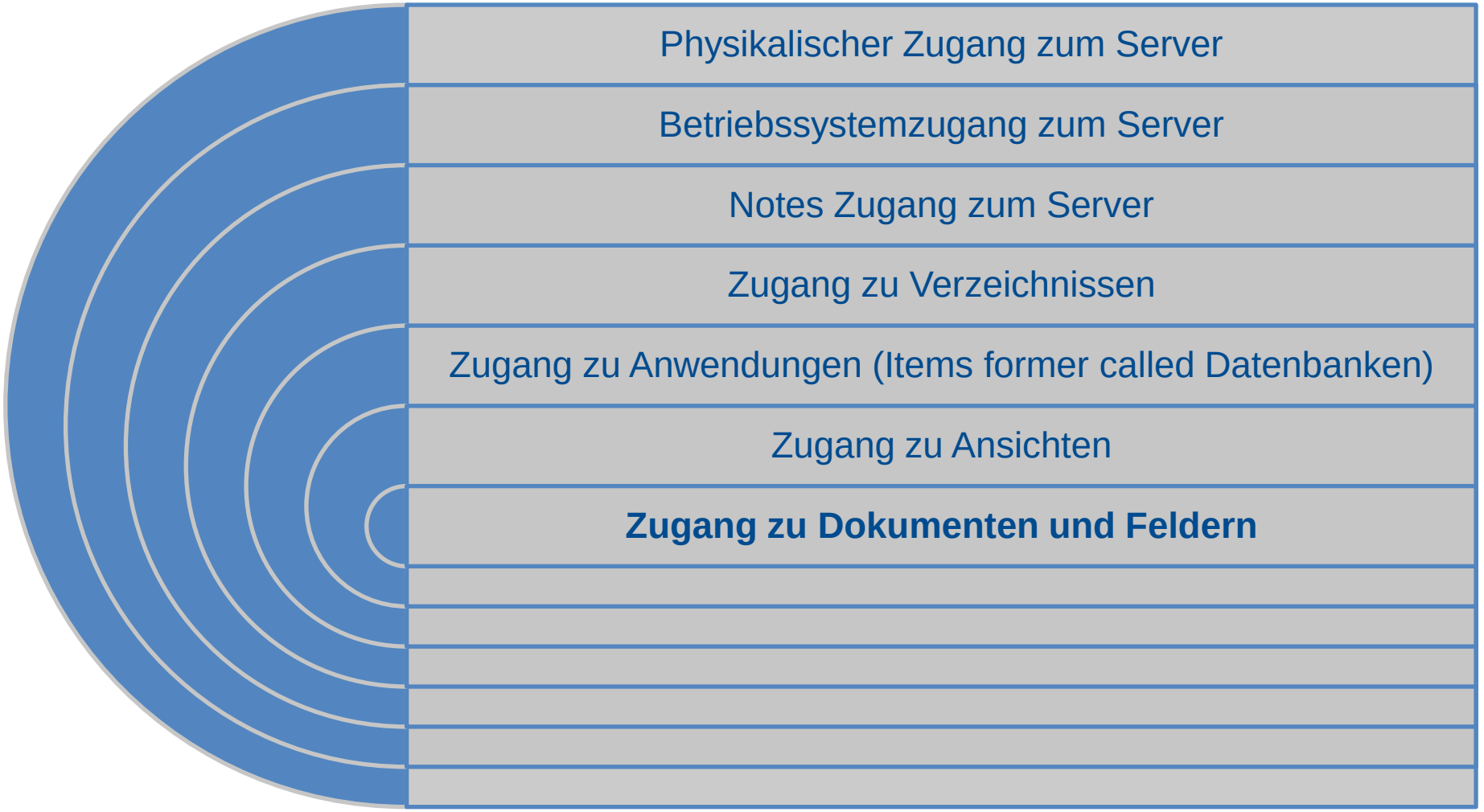


- Besser als Gruppen: Mit Rollen arbeiten und diese vergeben
  (immer an Server und Admin-Gruppen denken!)

- Aber ist das wirklich ein Schutz der Inhalte/Dokumente?
- Nein. Jeder Anwender kann persönliche Ansichten erstellen. Auch ohne Designer oder 

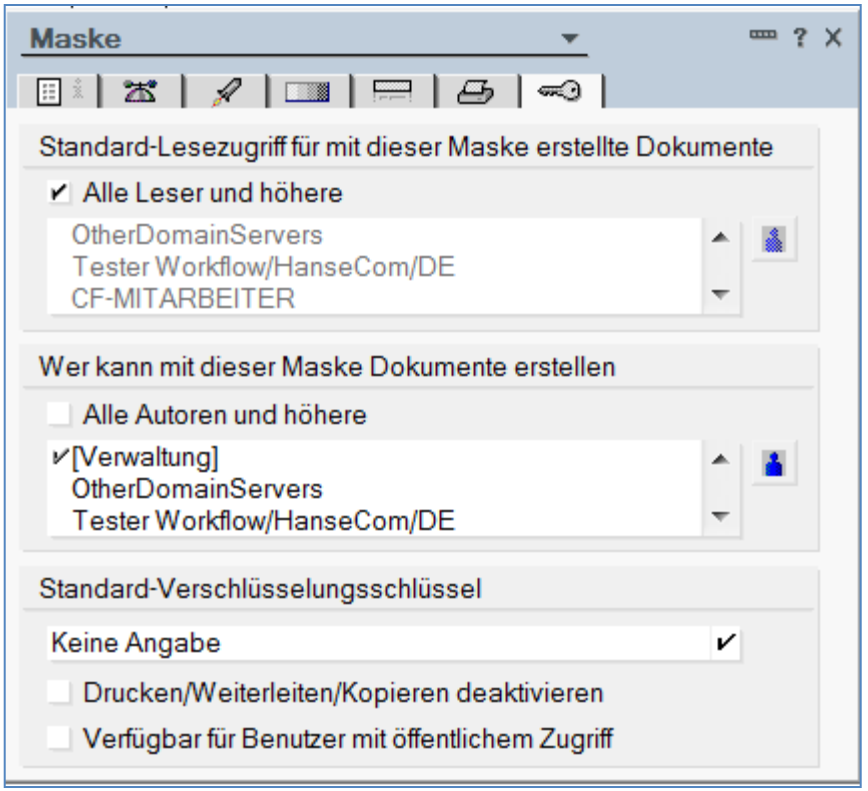
Rechte!

Domino Sicherheits-Ebenen



Zugang zu Dokumenten

- Jeder Anwender mit min. Autor Rechten kann Dokumente in einer Anwendung erstellen
  (öff. Dok. nicht betrachtet)
- In den Maskeneigenschaften lasst sich das Recht zum Erstellen und Lesen der so erstellten Dokumente steuern.
- Öffentlicher Zugriff
- Drucken/Weiterleiten/Kopieren verhindern
- Verschlüsselungsschlüssel?

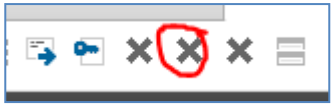


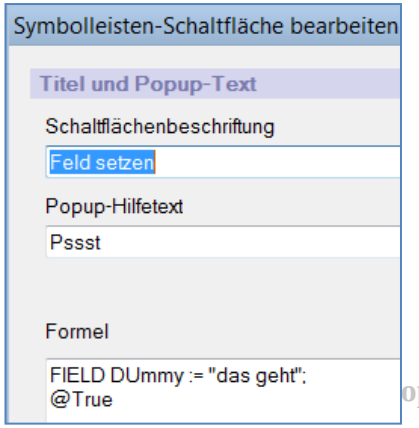
Zugang zu Dokumenten

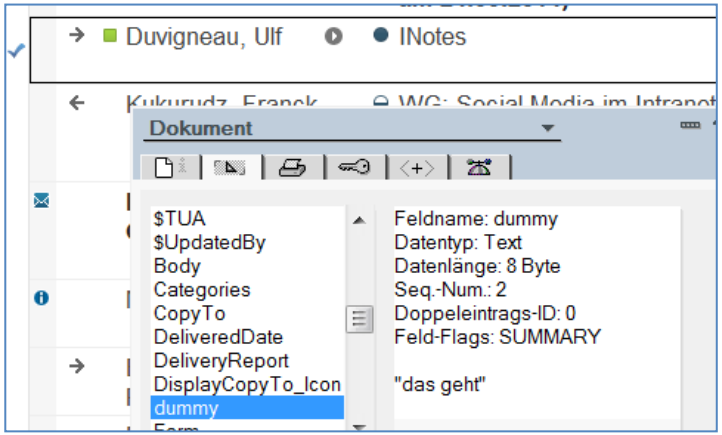
- Ist durch die Maskeneigenschaft „Wer kann mit diese Maske Dokumente erstellen“ die **Integrität** gewahrt?

- **Leider Nein**! Warum?

- Anwender mit Editor-Rechten können das Dokument außerhalb der Maske (UI) verändern:
  - Über einen Agenten, wenn jemand bei der ACL nicht aufgepasst hat.
  - Über eine Aktion in einer privaten Ansicht
  - Über ein Smarticon (Symbolleisten-Schaltfläche)





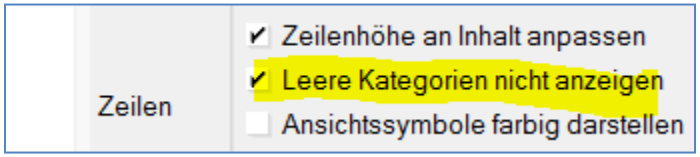


Zugang zu Dokumenten

- Ist durch die Maskeneigenschaft „Standardlesezugriff für mit dieser Maske erstellte Dokumente“ die **Vertraulichkeit** gewahrt?

- **Ja!** Warum?

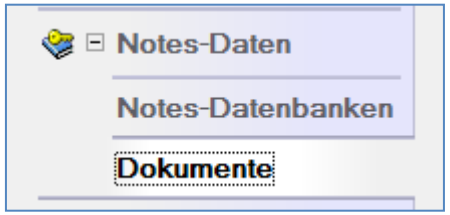
- Anwender, die die entsprechende Rolle (Empfehlung) nicht besitzen, können die Dokumente nicht sehen, kopieren, replizieren oder verändern
- Manchmal ahnen sie nicht einmal, dass es sie gibt.

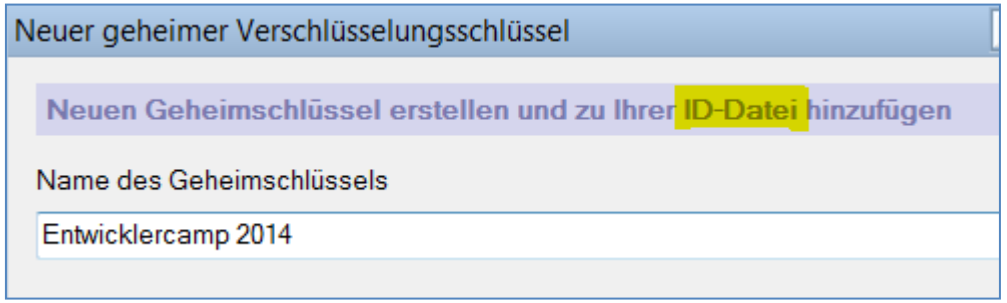


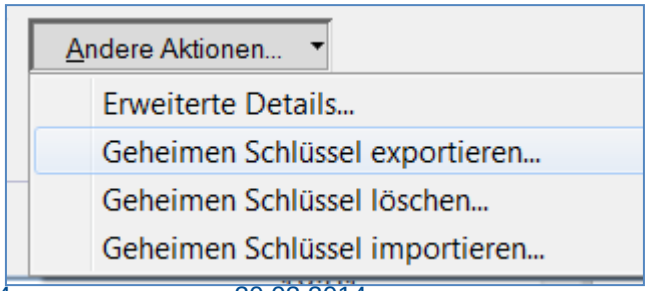
- Achtung „Full Access Admin“ sehen alles! (@Admin: Event mit Mail!)

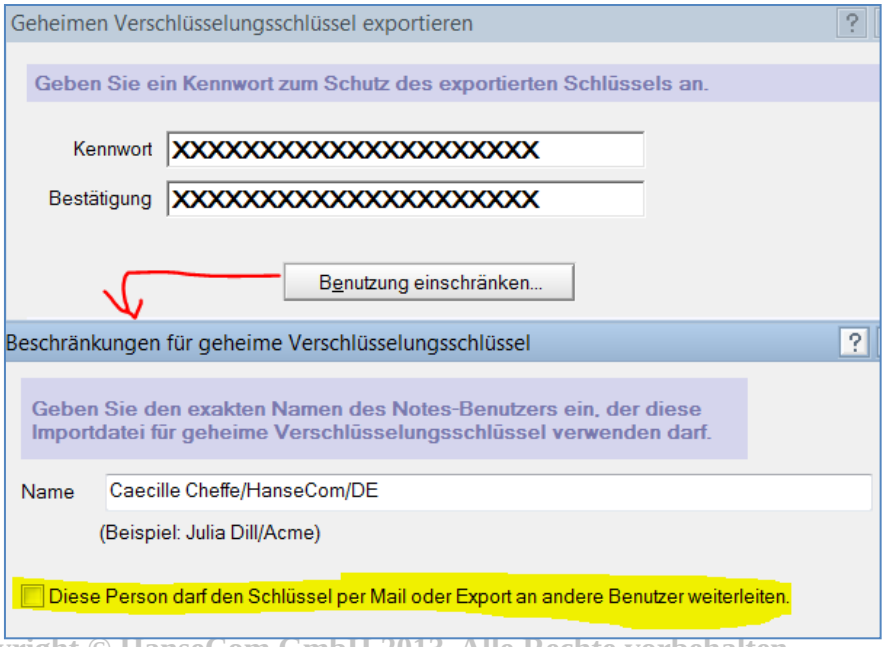
Zugang zu Dokumenten

- Wie werden Verschlüsselungsschlüssel erstellt?
- Wer kennt es? Wer hat es schon einmal benutzt?
- Menü Datei > Sicherheit > Benutzersicherheit







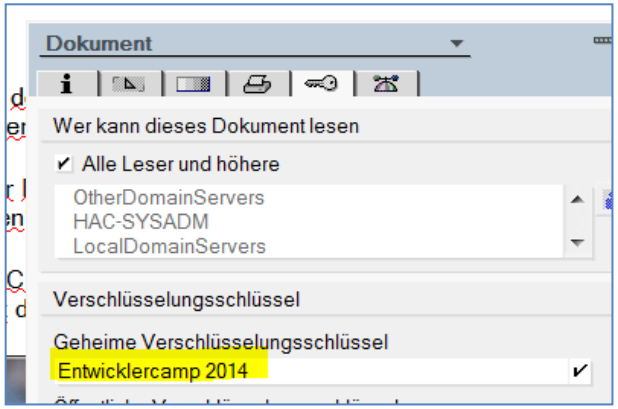


Zugang zu Dokumenten

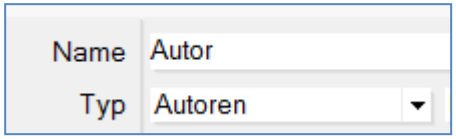
- Ist durch Verschlüsselungsschlüssel die **Vertraulichkeit und Integrität** gewahrt?

- **JA! Mit Sicherheit!**

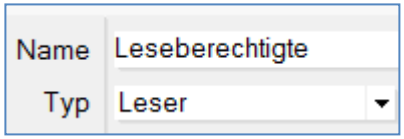
- Auch wenn der Schlüssel nicht im Design der DB hinterlegt ist, lässt auf Ebene einzelner Dokumente verschlüsseln, wenn die entsprechende Feldeigenschaft gesetzt ist.



Zugang zu Dokumenten

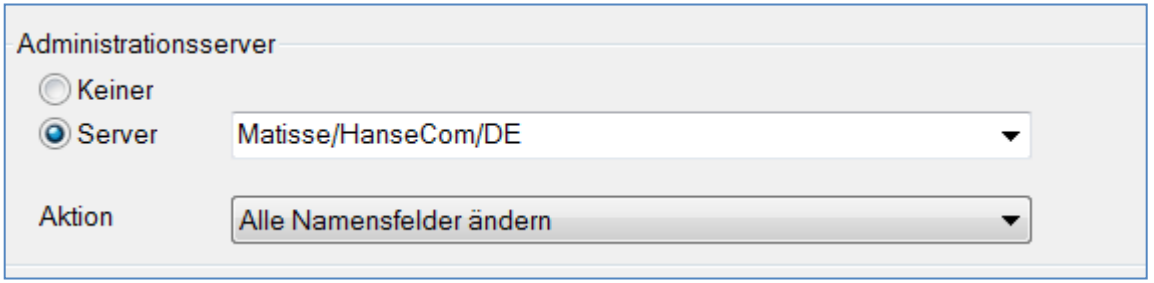


- Autornamenfelder
  - Ohne Autornamenfeld verliert Autor Recht an seinem Dokument
  - Mehrere Autorennamensfelder möglich (berechnet & bearbeitbar)



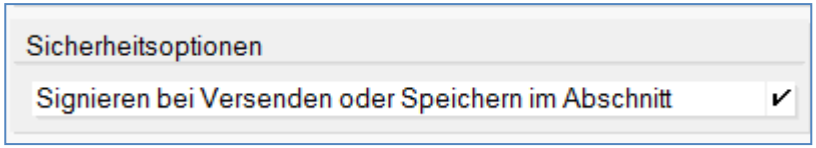
- Lesernamenfelder
  - Auch mehrere
  - Wenn „“ kein Leseschutz, wenn gefüllt immer auch Autoren leseberechtigt
  - Immer an „LocalDomainServers“ ggf. „OtherDomainServers“ und Rolle [AllesLesen]

- Namensfelder für Notes-namen ohne Zugriff, in ACL auf AdminP achten



Zugang zu Dokumenten

- Es gibt eine Feldeigenschaft, die es erlaubt, Felder beim Speichern oder senden zu signieren:



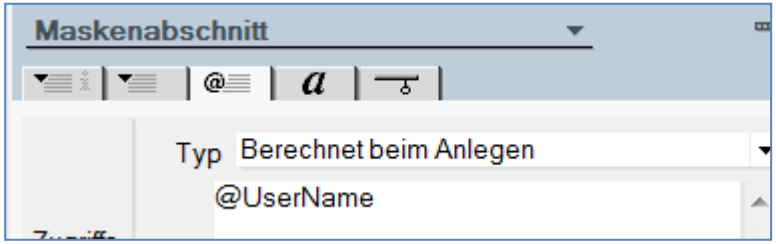
- Ist durch das Signieren von Feldern die **Integrität** gewahrt?

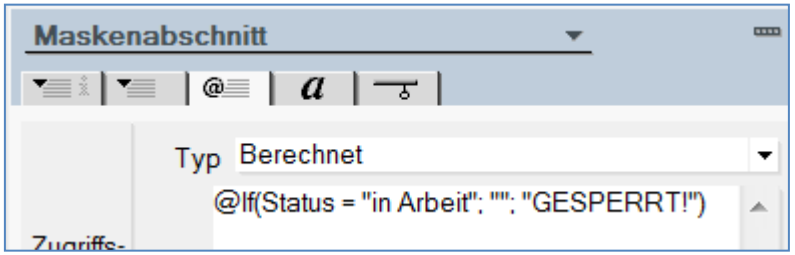
- **Ja!** Weil der Anwender eine Fehlermeldung erhält, wenn signierte Feldinhalte nach dem Speichern manipuliert worden sind.
- Befindet sich das signierbare Feld in einem kontrollierte Abschnitt, so wird der Abschnitt quasi signiert. Hält die Maske mehrere Abschnitte, können mehrere Signaturen enthalten sein.

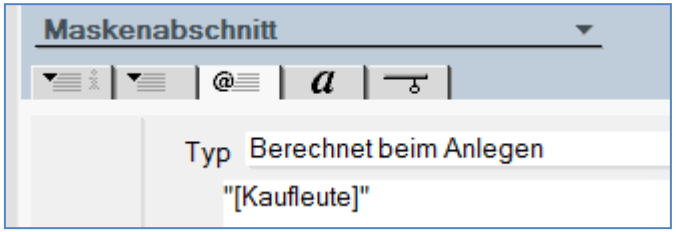
Domino Sicherheits-Ebenen V2

Zugang zu Abschnitten

- Abschnitte schützen einen Bereich von Feldern vor dem nicht autorisierten Zugriff von Editoren im GUI
- Ein Abschnitt wird über mehrere Felder gelegt (im Designer in einer Maske Felder markieren > Menü Erstellen > kontrollierter Zugriff







Zugang zu Abschnitten

- Ist durch kontrollierte Abschnitte die **Integrität** gewahrt?

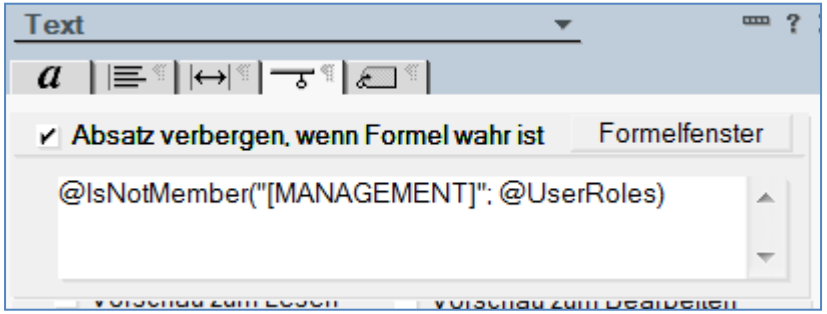
- Leider **Nein**! Warum?

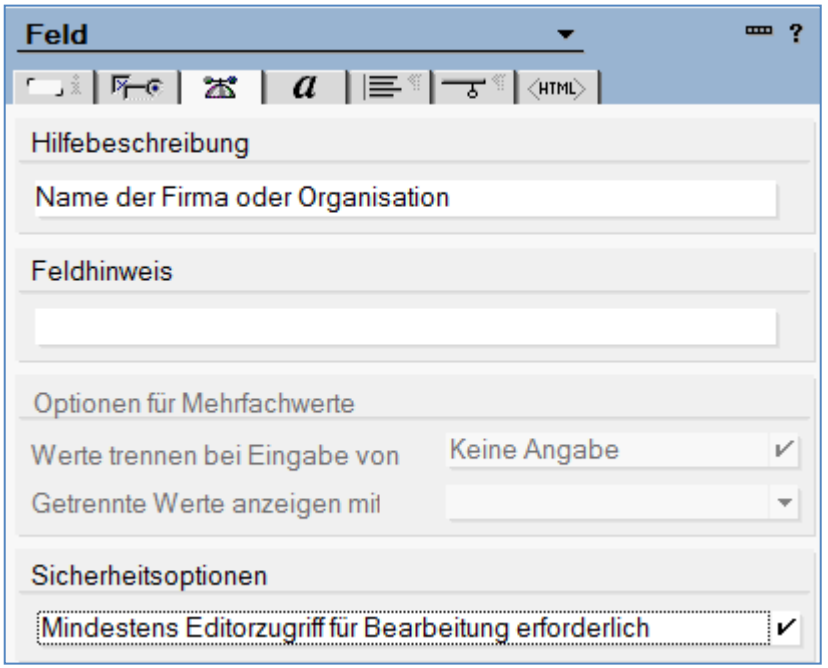
- Anwender mit Editor-Rechten können das Dokument außerhalb der Maske und des Abschnittes (GUI) verändern:
  - Über einen Agenten, wenn jemand bei der ACL nicht aufgepasst hat.
  - Über eine Aktion in einer privaten Ansicht
  - Über ein Smarticon (Symbolleisten-Schaltfläche)

Domino Sicherheits-Ebenen V2

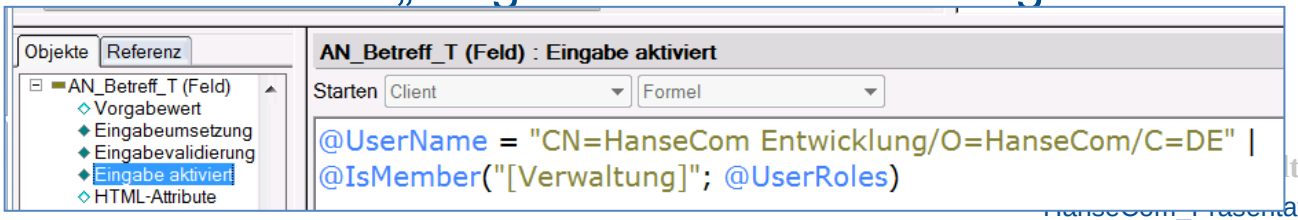
Zugang zu Feldern

- Eine weitere Möglichkeit auf Ebene einzelner Felder die Bearbeitung einzuschränken ist diese:
- Anwender mit Autorenrechten können diese Dokumente nicht bearbeiten. Bsp.: Fullname im Pers.Dok.
- Verbergenformeln in den Textattributen ein oder mehrerer Felder:





- Für einzelne Felder eine Formel für „Eingabe aktiviert“ hinterlegen.



Zugang zu Feldern

- Ist durch das Verbergen von Masken-Inhalten (Feldern) die **Vertraulichkeit** gewahrt?

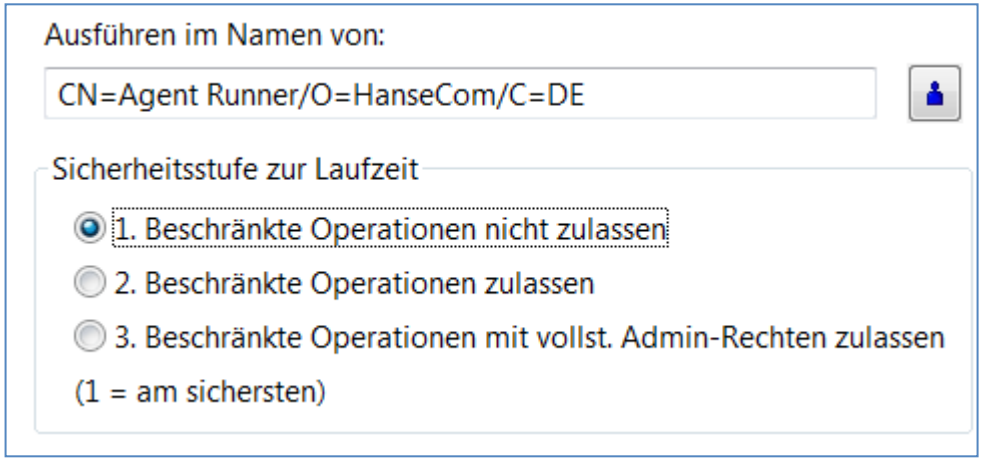
- **Nein! Warum?**

- Über die Eigenschaften des Dokumentes lassen sich die Feldinhalte anzeigen. Selbst Anwendungen mit verborgenem Design helfen da nicht.

Agentensicherheit – Wer das darf, darf alles!

- Serverdokument Register Sicherheit:
- Die Kennung, die den Agenten signiert, muss die entsprechende Agenten-Ausführungsberechtigung haben

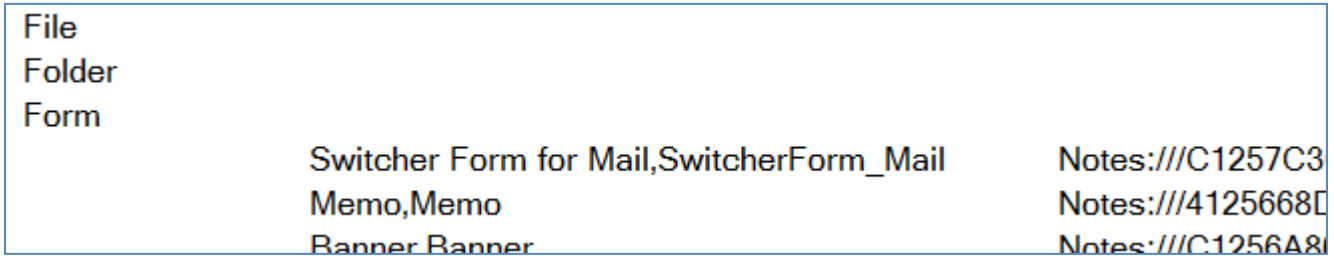
- Die Kennung, unter der der Agent läuft, benötigt Zugriffsrechte an der ACL



Einschränkungen der Programmierbarkeit	Wer kann -
Unbeschränkte Methoden und Operationen signieren oder ausführen:	SERVER-AGENT-UNBEGRENZT
Agenten signieren, die im Namen anderer ausgeführt werden:	
nten oder XPages gnieren, die im Namen des Aufrufers ausgeführt werden:	
Beschränkte LotusScript/Java-Agenten signieren oder ausführen:	SERVER-AGENT-BEGRENZT
Einfache und Formel-Agenten ausführen:	
Scriptbibliotheken signieren, die im Namen anderer ausgeführt werden:	

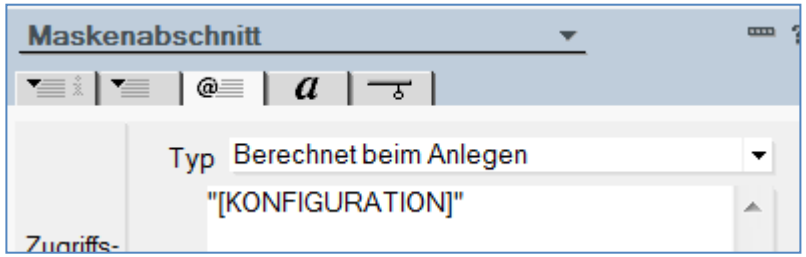
Worauf sollten Entwickler achten?

- Bei der Konfiguration einer Anwendung werden gern Profildokumente benutzt.
  - @Command([EditProfile]; „Anwendungs_Profil")
  - @Command([EditProfile]; „Anwender_Profil" ; @UserName)
- Vorteil: Schneller Zugriff auf Konfigurationsfelder
- Nachteil: Editoren können auch ohne Designer-Client diese Profil-Doks ändern
- **„Dann müssten Sie aber auch wissen, wie die Masken heißen! So einfach ist das nicht.“**
- Ich empfehle einen Blick in die Cache.ndk

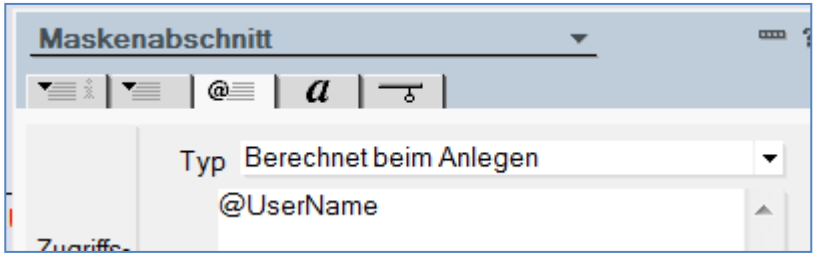


Worauf sollten Entwickler achten?

- Bei der Verwendung von Profildokumenten sollten die Inhalte mindestens mit einem kontrollierten Abschnitt geschützt sein.
  - Bei Anwendungs-Profilen sollte dies über eine Rolle geschützt sein.



  - Bei Anwender-Profilen



- Idealerweise steht die DB-weite Konfiguration in einer extra DB (Leser)

Worauf sollten Entwickler noch achten?

- Verschlüsselungsschlüssel sollten immer bei den Administratoren verwahrt werden. Ein Vier-Augen-Prinzip durch Besitz von Schlüssel und Kennwort ist möglich
- Warum eigentlich?
- Ist der Schlüssel weg, ist die Anwendung tod.

Zusammenfassung Vertraulichkeit und Integrität

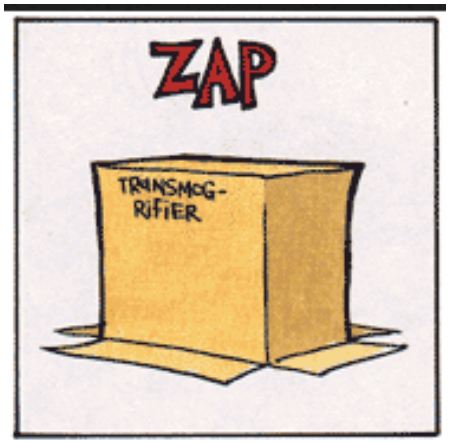
- Vertraulichkeit nur durch
  - Leseschutz
  - Verschlüsselung

- Integrität nur durch
  - Signatur
  - Max. Autor-Rechte für Anwender

Fragen – Diskussionsbedarf?

Vielen Dank für die tollen Berwertungen. Ich habe mich sehr gefreut!

Quellen



- http://de.wikipedia.org/wiki/IT-Sicherheit
- Domino Administrator Hilfe
- Notes Designer Hilfe
- Developerworks: Designer Wiki
- Entwicklercamp 2012: Track 4 Session 1 – Security in Notes Anwendungen
- http://www-10.lotus.com/ldd/ddwiki.nsf
- Developerworks: Notes und Domino Wiki

http://www-10.lotus.com/ldd/dominowiki.nsf

- Wikipedia
- Mein Gehirn