B-K H

Lotus Notes EntwicklerCamp '06

Planung und Umsetzung von Sicherheitsebenen

Rudi Knegt
RKJ-Soft

B-KH

Lotus Notes EntwicklerCamp '06

Planung und Umsetzung von Sicherheitsebenen

Welche Optionen gibt es, wie kann ich diese umsetzen, und welche der Einstellungen vermitteln nur eine scheinbare Sicherheit

Rudi Knegt, RKJ-Soft

B-K H

Lotus Notes EntwicklerCamp '06

Agenda

- Einführung
  - Was ist Security
  - Wo sind die verschiedenen Möglichkeiten
- Ziel
- Einiges im Detail => Beispiele & Demos
- Zusammenfassung, und wie geht es weiter ?
- Q & A

B-KH

Lotus Notes EntwicklerCamp '06

Über mich

- Wer bin ich: Rudi Knegt
- Was bin ich: Holländer
- Was mache ich: Entwicklen & Administrieren und und und
- Wo mache ich das: Wo immer es notwendig ist.

- Beschäftigt mit Lotus Notes seit 1993
- Zertifiziert seit 1995, CLI seit 1996
- Solo von 1999 bis 2005
- Eigene GmbH mittlerweile.. Geschäftfuhrer und Putzmann

B-KH

Lotus Notes EntwicklerCamp '06

Zertifizierungen:

- CLE App-Dev & Admin R3,
- Dual Principal-CLP App-Dev & Admin R4,
- Principal-CLI Level-2 App-Dev & Admin R4, Principal-CLP App-Dev & Admin R5,
- Principal-CLI Level-2 App-Dev & Admin R5,
- Principal-CLP App-Dev N6 & CLP Admin ND6,
- CLS - Colaborative Solutions Administrator
- CLI App-Dev & Admin ND6

Was ist Sicherheit ?

- Physicalische Sicherheit
- Plattform sicherheit
- ID File & Passwort
- Configuration
- Anwendungsentwicklung
- Denk an den SuperAdmin in ND6

B-KH

Lotus Notes EntwicklerCamp '06

Grundkenntnisse der Sicherkeit

- Was du nicht sehen kannst, kannst du nicht bearbeiten
- Strukturen ins Chaos bringen
- Wissen was geht
  (oder wo es steht wie es geht)

- Learning by doing...

Wie viel Sicherheit kann mann kaufen ?

- Es gibt kein kostenlimit nach oben...
- Es gibt ein Limit an erreichbare Sicherheit
- Je sicherer die Anwendung je benutzer unfreudlicher er wird
- Welche bedrohungen sind da ?
  - Hackers
  - Spionen
  - Gut gelaunte Admins (und schlecht gelaunte)
  - Informations "klau" oder vernichtung

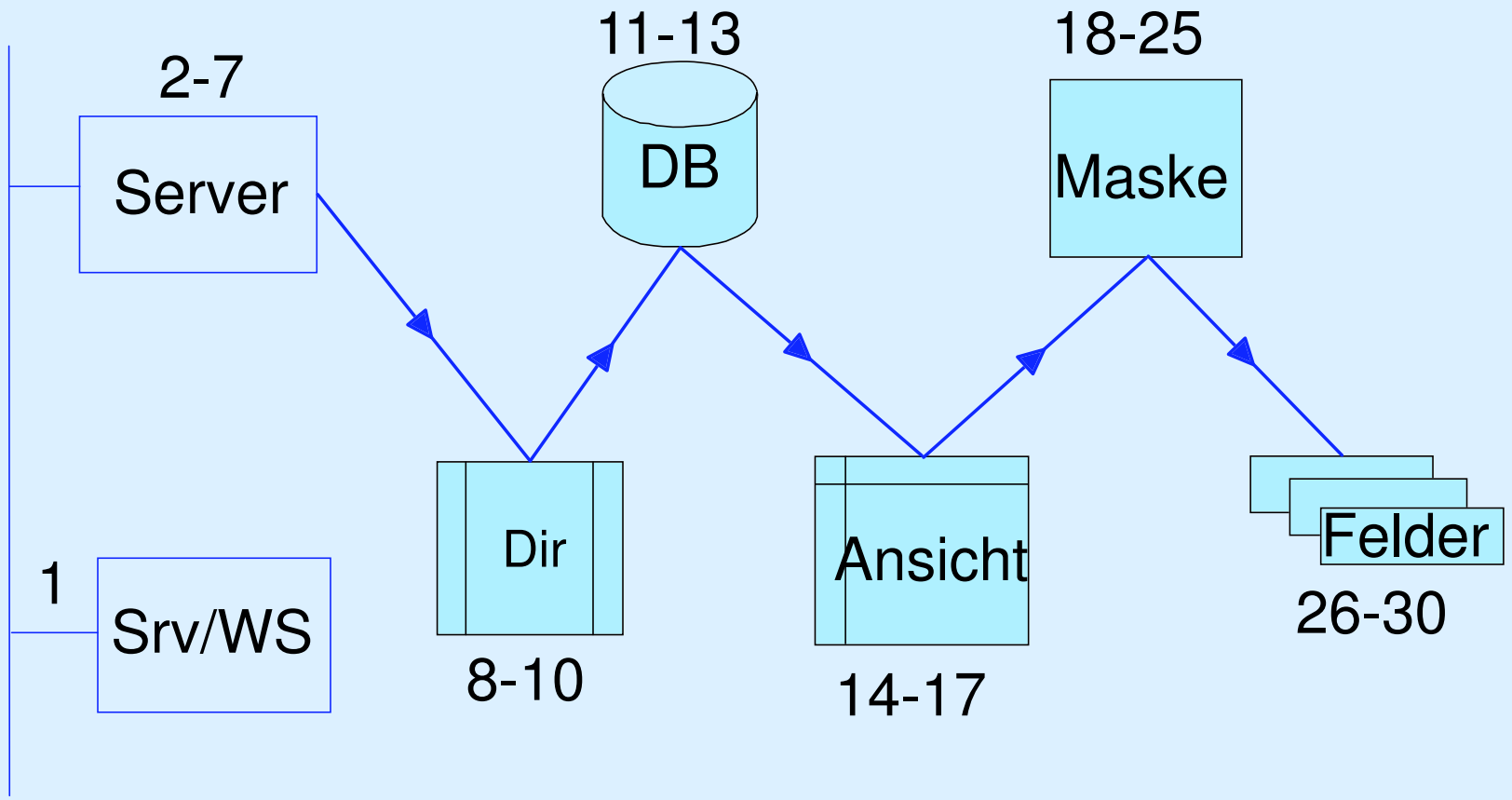
Defensiv masnahmen

- Kryptography
- Verschlüsselung
- ACL
- ECL
- Public/Private Key
- Server Konfiguration
- Client Konfiguration
- Trojaner

Der Super Administrator von ND6

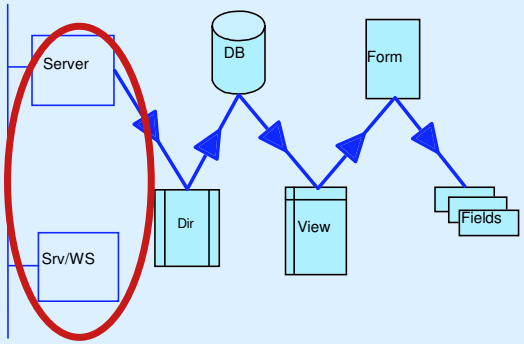
- Den neuen Super Administrator kann . . .
  - Jeder DB ACL Ändern
  - Jeder Rolle hinzufügen
  - alle Dokumente sehen und bearbeiten !
  - Verschlüsselung ist einzige schutz !
- Es hinterläßt Spuren
  - Eintrag im Log (erneuten änderung von Log zum löschen)
  - Eintrag im ACL-Log (kann nicht entfernt werden)
  - Löschstubs oder $Modified im Dokument

Sicherheitsebenen - Überblick



Sicherheitsebene - Ausgearbeitet I / 8

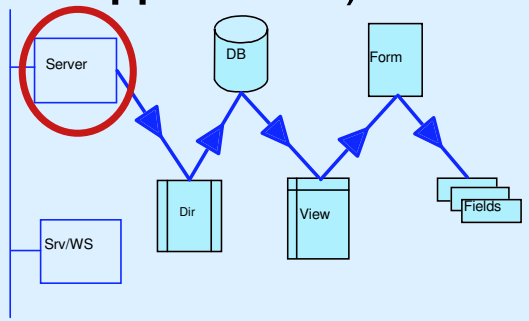
- 1. Netzwerkzugang
  - NUR TCPIP kann (bedingt) ohne Authentification ins Netzwerk
  - Alle anderen Protokolle brauchen Zugangsrechte
- 2. Authentification
  - Wer bist du, und beweise mir das.
  - Server- & Clientseitig
  - Web User Einstellungen



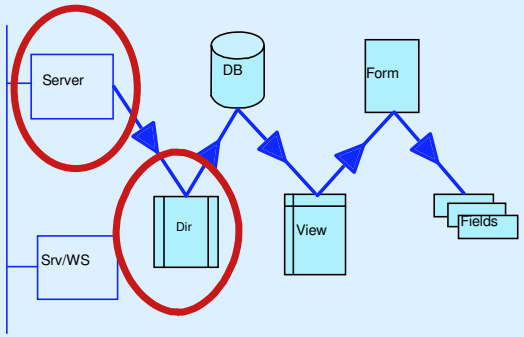
- 3. Anonymer Zugriff
  - Wenn Userauthentification nicht erfolgreich war (Notes+Web)

Sicherheitsebene - Ausgearbeitet 2 / 8

- 4. Wer darf NICHT auf den Server zugreifen
  - Einstellungen im Serverdokument
  - Notes.ini Variable (Deny_Access_Portname=Gruppe,Person)
- 5. Wer darf auf den Server zugreifen
  - Einstellungen im Serverdokument
  - Notes.ini Variable (Allow_Access_Portname=Gruppe,Person)



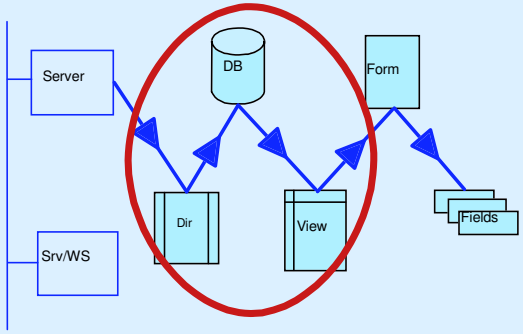
Sicherheitsebene - Ausgearbeitet 3 / 8



- 6. Notes Public-Key vergleichen
  - Serverdokument Security
- 7. Kennwort vergleichen
  - Serverdokument oder Personendokument
- 8. Virtuelles Verzeichnis
  - text.dir Text file auf Betriebsystemebene, mit Verweis und Zugangsberechtigung
- 9. Virtuelle Datenbank
  - db.nsf Text file mit Verweis und Zugangsberechtigung

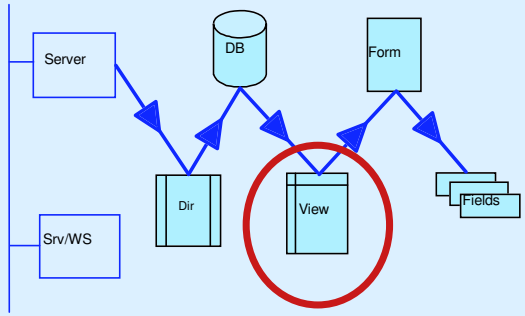
Sicherheitsebene - Ausgearbeitet 4 / 8

- 10. Verzeichnisse/Datenbanken durchsuchen
  - Webeinstellung "HTTP-Clients zum Suchen von Datenbanken zulassen:"
- 11. Datenbank ACL
  - nicht nur die Einträge sondern Rollen / Optionen nicht vergessen...
- 12. Datenbank Verschlüsselung
  - Nur auf Personenebene mittels Private-Key
- 13. Agenten
  - Run on behalf of / Run as Webuser



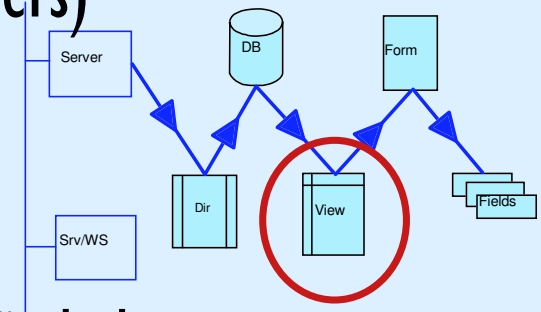
Sicherheitsebene - Ausgearbeitet 5 / 8

- 14. Ansicht Restriktionen
  - Notes oder Web Verwendung
  - Wer darf diese Ansicht verwenden (Personen/Gruppen/Rollen)
- 15. Form Formel
- 16. Frameset oder Outlines verwenden
  - Durch Vorgaben beim Datenbank-öffnen
- 17. LotusScript Kontrollen beim DB öffnen
  - Z.B. Post open, und DB schließen...



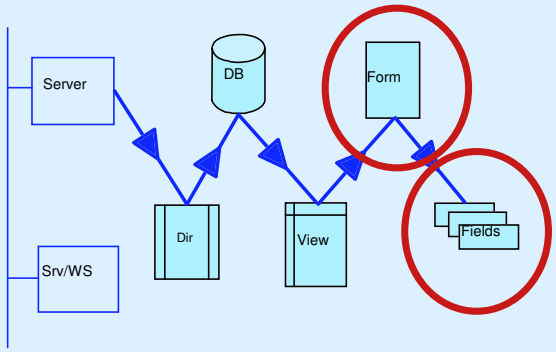
Sicherheitsebene - Ausgearbeitet 6 / 8

- 18. Maskenerstellung Einschränken
- 19. Maskenverwendung Einschränken ($Readers)
- 20. für Notes und/oder Web verfügbar
- 21. Lesernamenfelder
  - Programmierte Vorgaben und vom Benutzer änderbar
- 22. Lesernameschutz auf Dokument
  - $Reader im Dokument (Benutzer änderbar vom Ansicht)



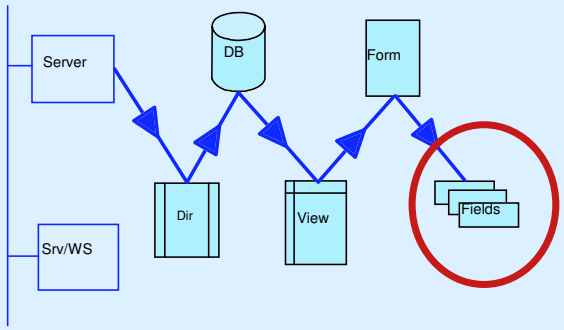
Sicherheitsebene - Ausgearbeitet 7 / 8

- 23. Autorenfelder
  - Programmierte Vorgaben und vom Benutzer änderbar
- 24. Verbergen-beim Formeln
  - Notes und/oder Web Einstellungen
- 25. Abschnitte mit Beschränkungen
  - Editor berechtigung für Feld bearbeitung
- 26. Verschlüsselung mit Publik/Private key
  - nur in Emails

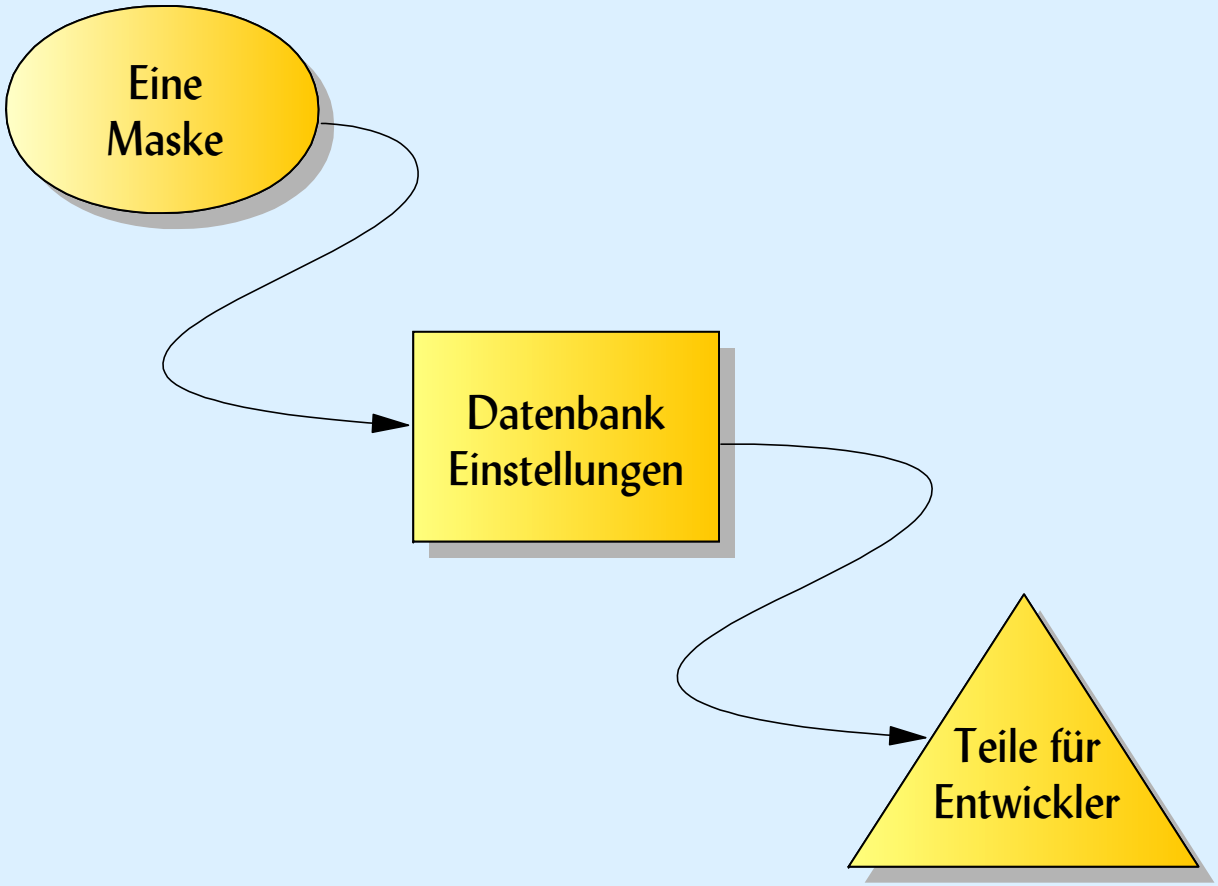


Sicherheitsebene - Ausgearbeitet 8 / 8

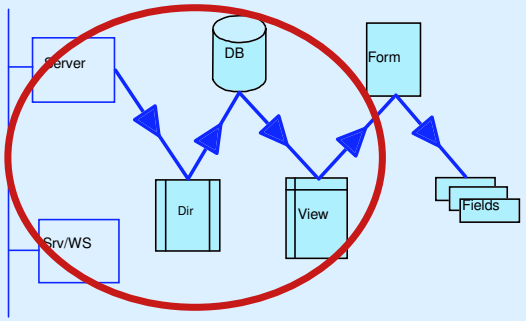
- 27. Verschlüsselung mit erstellten Keys
  - Encryption key nicht in Emails
  - Encryption keys in SecretEncryptionKeys Feld
- 28. Editorrechte für Felder
  - nur für Autorenberechtigung
- 29. Elektronische Unterschrift
  - Für die Wiedererkennung des Erstellers
- 30. SMime und Externe Verschlüsselung
  - Entwerder mit PHP oder andere Tools



Demo I



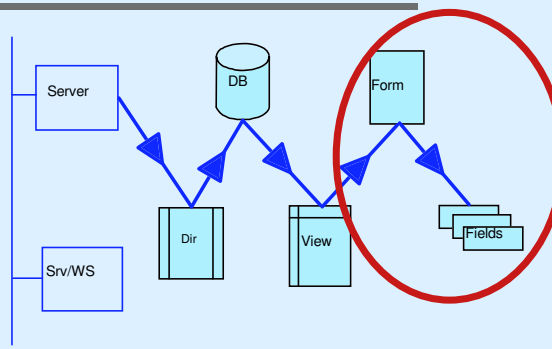
Wem gehört welche Einstellung 1 / 2



- 1 für Netzwerk Admin
  - Netzwerk einstellungen
- 2-11 für Domino Admin
  - ACL Vorgaben aus Projekt oder vom Entwickler
- 12 Domino Admin Vorgaben, Userausführung
- 13-20 Entwickler ausschließlich
- 21-22 Entwicklervorgaben, aber Anwenderänderungen können möglich sein. Auch nachträglich und Lokal

Wem gehört welche Einstellung 2 / 2

- 23 Entwickler möglich - Anwender möglich
- 24 Entwickler ausschließlich
  - Poweruser kommt trotzdem dran
- 25-27 Entwicklervorgaben, aber....
  von Anwender abschaltbar/änderbar
- 28-29 Entwicklervorgaben
- 30 Entwickler / Admin / GF / Kunde / User



Was ist KEINE Sicherheit

- Hide-When
  - Weil ich kann die Felder ansehen & ändern
- Abschnitte
  - Weil ich kann die Felder ansehen & ändern
- Unterschriften
  - Weil die besagen nur wer am letzten dran war
- Editorrechte für felder
  - Weil NUR der UI dieses kontrolliert

weitere ohne Sicherheit...

- Ansicht und Masken restriktionen
  - Weil die erstellung von neue ansichten einfach ist
  - Weil agenten Daten/Dokumente erstellen/ändern können
  - Weil Masken wechsel jederzeit möglich ist
- Framesets und Outlines
  - Weil lokale Replieken es anders tun können
- Postopen Kontrolle
  - Weil die umgangen werden können

Was ist Sicherkeit

- Verschlüsselung
  - Was ich nicht entziffern kann ist nicht da
- Leser und Autorenfelder
  - Weil was nicht da ist, ist nicht zu ändern
  - Was nicht bearbeitet werden kann, ist sicher

Zusammenfassung

- Sicherheit ist nicht trivial
- Ohne Vorbereitung kann viel schief gehen
- Denk nach über die Möglichkeiten

- Sicherheit ist WICHTIG
- Scheinsicherheit ist gefährlich

B-KH

Lotus Notes EntwicklerCamp '06

? Q & A ?

Für Später

- http://www.RKJ-Soft.de/com/info/biz/net mit oder ohne -
- http://www.ExistiertNicht.de
- http://www.NoneExistent.com
- http://www.B-KH.de
- Präsentation ist verfügbar unter:
  http://www.EntwicklerCamp.de - Agenda
- Email: EC2006@NoneExistent.com oder
  EC2006@ExistiertNicht.de

B-KH

EntwicklerCamp '06

Thank You

Danke Schön

Bedankt

Merci

ευχαρισω