Active-Directory-Berechtigungen

oder: Die Tücken der Delegation

Nils Kaczenski, MVP Directory Services
Leiter Consulting & Support, WITstor GmbH

\\ice:lingen

intelligent communities for europe

Bei Frau Bogen klopft es

FAQ-O-MATIC.NET

Wer zu euch spricht

- Nils Kaczenski
- Leiter Consulting & Support WITstor Hannover
  - Windows, Exchange, Virtualisierung
  - Verfügbarkeit, Sicherheit
  - Strategische Beratung
  - Projektleitung
- Fachautor Windows
  - Microsoft Press
  - iX, c't, IT-Administrator
- Nils.Kaczenski@witstor.de

FAQ-O-MATIC.net

MVP Microsoft® Most Valuable Professional

Was euch erwartet

- Wer darf was? Und warum?
- Zahlen und Ausweise: SID und Access Token
- Demo: Adresspflege im Sekretariat
- Demo: Standort-Admins
- Demo: Praktikanten
- Ausblick: Im Sumpf steckt noch mehr

FAQ-O-MATIC.net

FAQ-O-MATIC.net

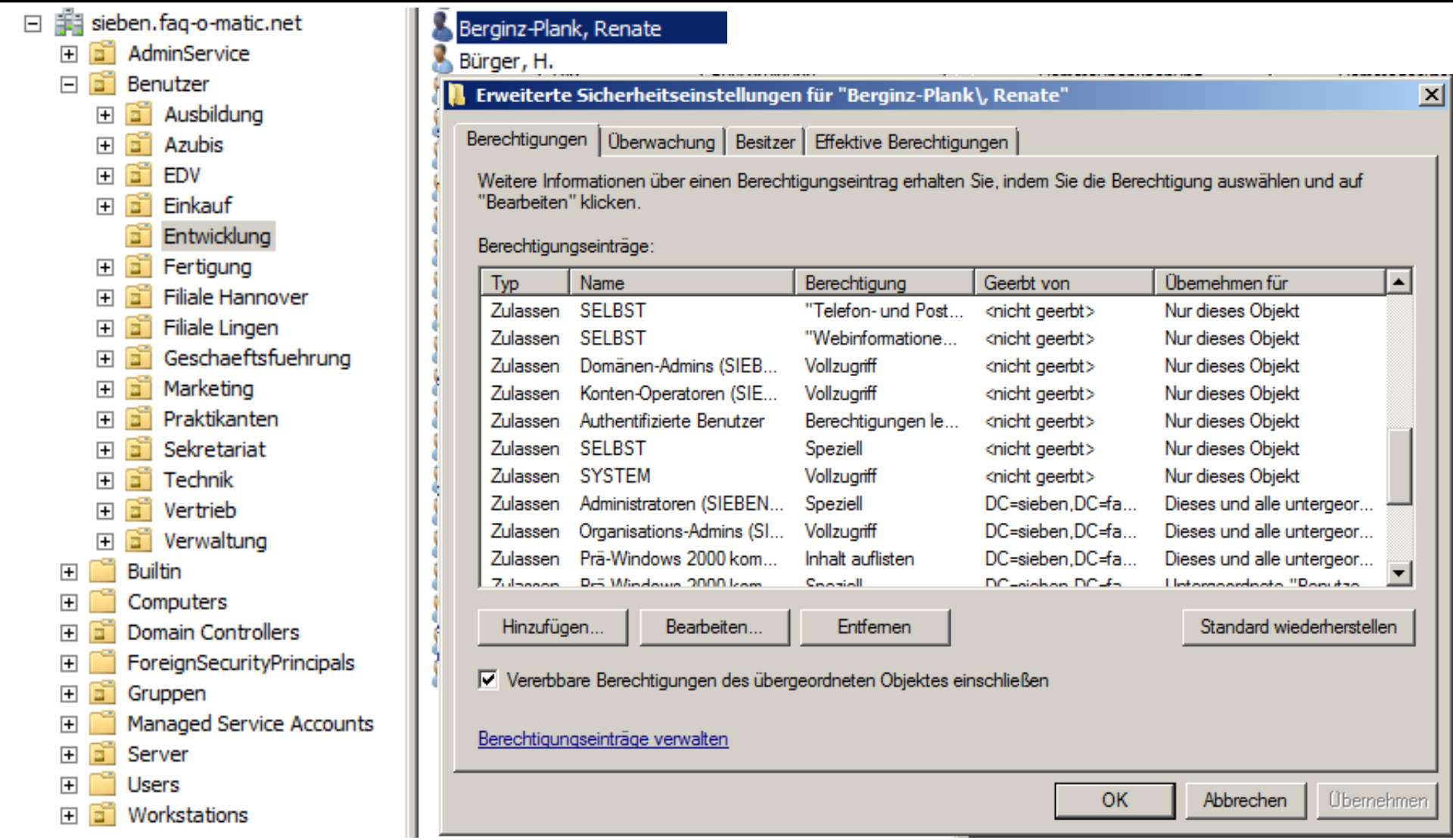
… anfassen!

Was darf ein Benutzer?

Was darf ein Admin?

Und warum?

Berechtigungen: Wer darf was?



Zahlenketten und Ausweise

- Der Security Identifier (SID)
  - S-1-5-21-1539329446-2123584859-1544097757-5023

Präfix — *Sub-Autorität (hier: Domänen-SID)* — *RID*

- Das Access Token
  - Erzeugt bei der Anmeldung ans System
  - Enthält User- und Gruppen-SIDs sowie Privilegien
  - Dient als Berechtigungs-Ausweis für alle Aktionen

FAQ-O-MATIC.net

FaQ-o-maTiC.net

… anfassen!

whoami – das Access Token

Berechtigungen analysieren

Szenario 1: Sekretariat

- Anforderungen
  - Das Sekretariat soll Kontaktdaten der Mitarbeiter aktualisieren
  - Schäden durch zu hohe Berechtigungen vermeiden
  - Sekretärinnen benötigen ein einfaches Werkzeug

FAQ-O-MATIC.net

Don’t try this at home!

- **Warnung!**

  Falsch gesetzte Berechtigungen können die Funktion von Active Directory zerstören!
- **Jede** Änderung genau im **Testlabor** prüfen!
- Änderungen mit einem dsacls-Skript ausführen!
- Keine Gewähr, kein Support von mir!

FaQ-O-MaTiC.net

FaQ-o-maTiC.net

… anfassen!

Sekretariats-Berechtigungen setzen

Ein Werkzeug für die Zielgruppe

dsascls-Syntax

- dsacls <Objekt> /I:[TSP] /G Gruppe:Recht;[Ziel];[Klasse]
  LDAP-Pfad *Vererbung* *Kürzelcode*

- dsacls "CN=Ute,OU=EDV,DC=dom,DC=tld" /G Helpdesk:GR;;
  - *Leserechte für Gruppe „Helpdesk“ auf das Objekt „Ute“*
  - *Keine Vererbung*
- dsacls "OU=EDV,DC=dom,DC=tld" /I:S /G Adr:RPWP;company;user
  - *Lese- und Schreibrechte für Gruppe „Adr“*
  - *auf Attribut „company“*
  - *nur auf User-Objekten in der OU „EDV“*
- dsacls "OU=EDV,DC=dom,DC=tld" /I:T /R Praktikant
  - *Entfernen der direkten Berechtigungen für Gruppe „Praktikant“*
  - *auf OU „EDV“ und allen Unterobjekten*

Szenario: Standort-Admins

- Anforderungen (Szenario 1)
  - Administration aller Ressourcen des Standorts
  - Kein erhöhter Zugriff auf andere Ressourcen
- Anforderungen (Szenario 2)
  - Anlegen und Verwalten von Standort-Benutzern
  - Bei Gruppen nur Mitglieder verwalten
  - Kein Vollzugriff

FAQ-O-MATIC.net

FaQ-o-maTiC.net

… anfassen!

Vollzugriff nur auf Standort-Ressourcen

Eingeschränkte Standort-Administration

Szenario: Praktikanten

- Anforderungen
  - Praktikanten sollen sich an AD anmelden
  - Praktikanten sollen keine anderen Objekte sehen

FAQ-O-MATIC.net

… anfassen!

Vorhandene Berechtigungen entfernen

List Object Mode aktivieren

Ausblick: Im Sumpf steckt noch mehr

- Geschützte Konten
  oder: Warum der Admin von Blackberry verschont bleibt
- Exchange Server 2010
  oder: Der Tod der AD-Delegation
- *-Operatoren
  oder: Das böse Erbe der NT-Zeiten
- „Trust“ bedeutet Vertrauen
  oder: Die Domäne ist keine Sicherheitsgrenze

FAQ-O-MATIC.net

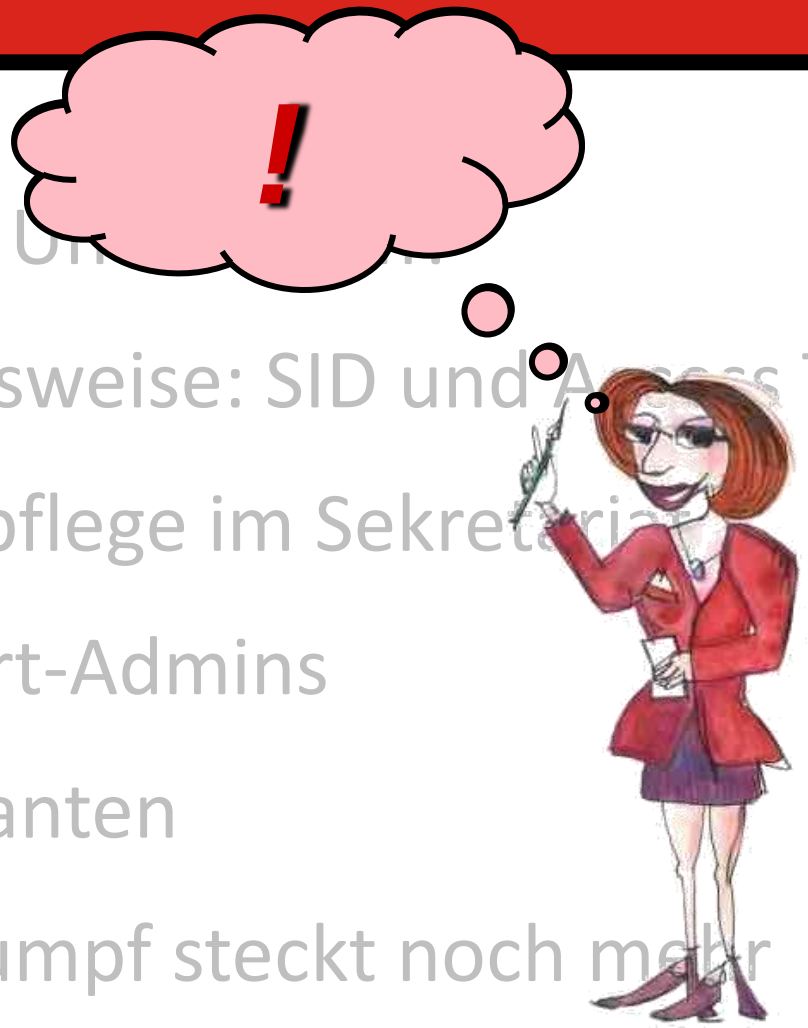
Werkzeugkasten

- LIZA:
  http://www.ldapexplorer.com/en/liza.htm
- name2sid.vbs:
  http://faq-o-matic.net/?p=548
- getNameBySID.vbs:
  http://faq-o-matic.net/?p=531
- Adressbearbeitung.hta:
  http://faq-o-matic.net/?p=834

FAQ-O-MATIC.net

Fragen? Antworten!

- Wer darf was? Un
- Zahlen und Ausweise: SID und Access Token
- Demo: Adresspflege im Sekretariat
- Demo: Standort-Admins
- Demo: Praktikanten
- Ausblick: Im Sumpf steckt noch mehr



FaQ-o-maTic.net

Hört mir zu!

15.9. – 29.9. – 6.10.2010

Hyper-V sicher und sauber

heise-Seminar zu Hyper-V

27. und 28.9.2010

IIR Admin Tech-Talk

Zwei Sessions zu Active Directory

Nils.Kaczenski@witstor.de

twitter.com/Kaczenski

FAQ-O-MATIC.net

Es gibt keine großen Entdeckungen und Fortschritte, solange es noch ein unglückliches Kind auf Erden gibt.

There’s no such thing as a discovery or progress as long as we have bitterly unhappy children on earth.

Er zijn geen grote ontdekkingen en geen vooruitgang, zolang er op deze wereld nog één kind ongelukkig is.

(Albert Einstein)