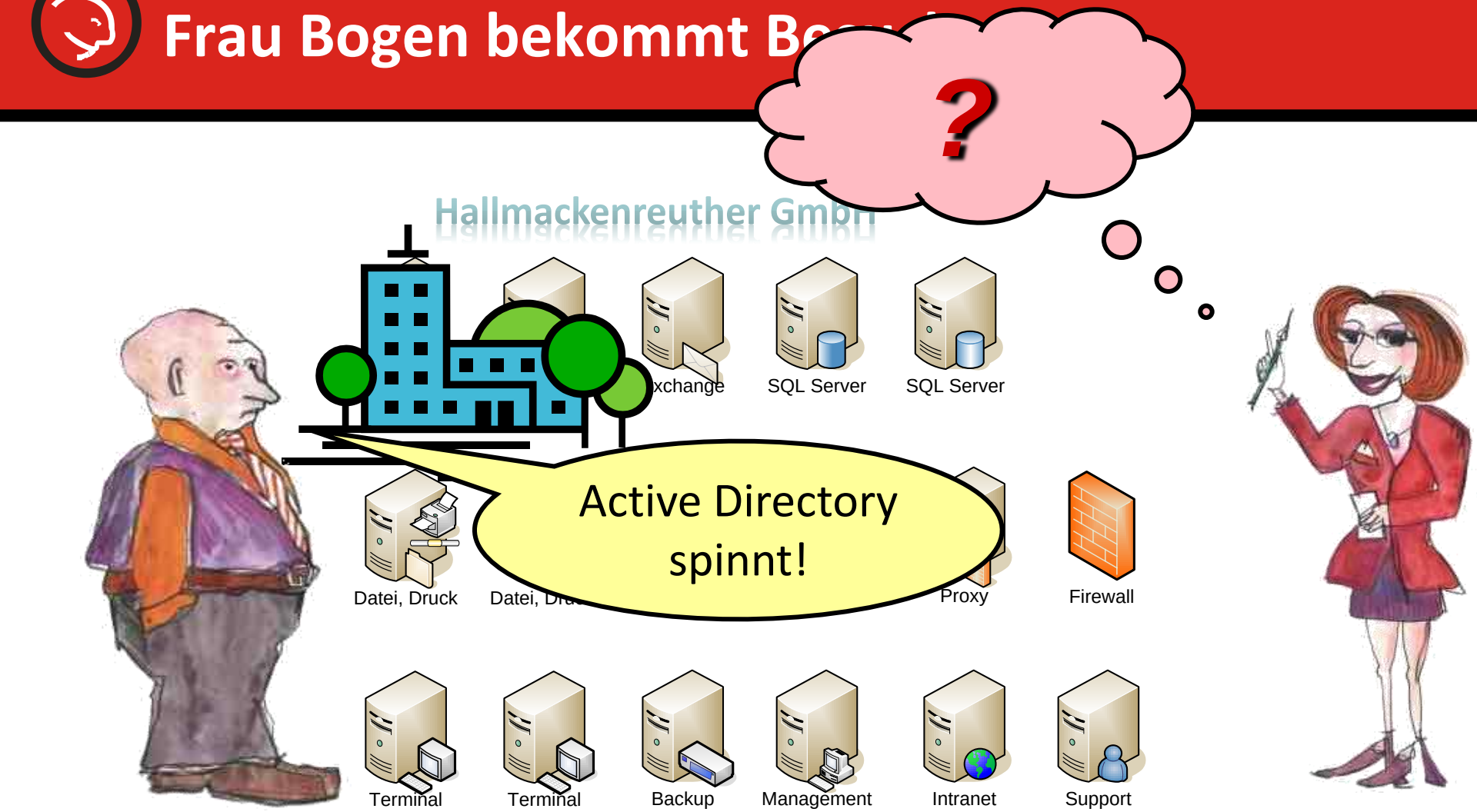
Das Active-Directory-Kuriositätenkabinett

Nils Kaczenski
MVP Directory Services
faq-o-matic.net

Fotos von stock.xchng

\\ice:lingen
intelligent communities for europe

Frau Bogen bekommt Be



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

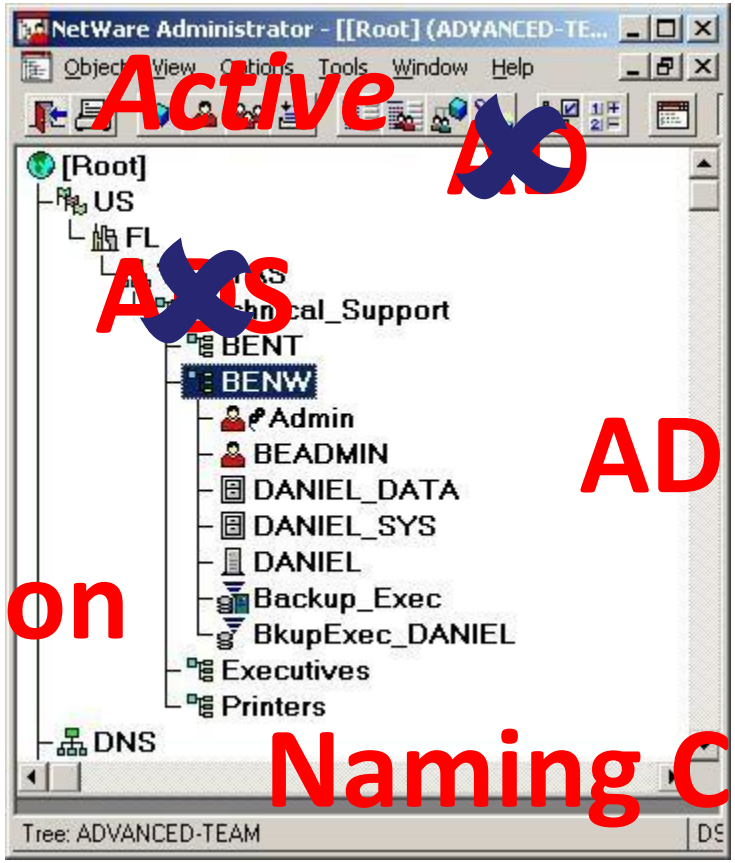

Wer bin ich eigentlich?

Wer bin ich eigentlich?

- *Active* Directory
- Das verschwiegene Vorbild

FAQ-O-MATIC.net

Wer bin ich eigentlich?



~~NDS~~ ~~Active~~ ~~AD~~ ~~AXS~~

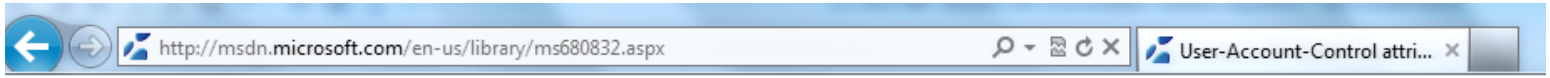
AD DS

~~Partition~~

Naming Context

FAQ-O-MATIC.NET

ADS: Nicht mehr verwendet (?)



Remarks

This attribute value can be zero or a combination of one or more of the following values.

Hexadecimal value	Identifier (defined in iads.h)	Description
0x00000001	ADS_UF_SCRIPT	The logon script is executed.
0x00000002	ADS_UF_ACCOUNTDISABLE	The user account is disabled.
0x00000008	ADS_UF_HOMEDIR_REQUIRED	The home directory is required.
0x00000010	ADS_UF_LOCKOUT	The account is currently locked out.
0x00000020	ADS_UF_PASSWD_NOTREQD	No password is required.
0x00000040	ADS_UF_PASSWD_CANT_CHANGE	The user cannot change the password. **Note** You cannot assign the permission settings of PASSWD_CANT_CHANGE information and a code example that shows how to prevent a user from chang :
0x00000080	ADS_UF_ENCRYPTED_TEXT_PASSWORD_ALLOWED	The user can send an encrypted password.
0x00000100	ADS_UF_TEMP_DUPLICATE_ACCOUNT	This is an account for users whose primary account is in another domain. This that trusts this domain. Also known as a local user account.
0x00000200	ADS_UF_NORMAL_ACCOUNT	This is a default account type that represents a typical user.
0x00000800	ADS_UF_INTERDOMAIN_TRUST_ACCOUNT	This is a permit to trust account for a system domain that trusts other domains
0x00001000	ADS_UF_WORKSTATION_TRUST_ACCOUNT	This is a computer account for a computer that is a member of this domain.
0x00002000	ADS_UF_SERVER_TRUST_ACCOUNT	This is a computer account for a system backup domain controller that is a me


Und was seid ihr für welche?

Identitätsverwirrung

- Benutzerkonten sind … Benutzerkonten?
- Der geheimnisvolle Wald
- Anmeldenamen sind eindeutig … ziemlich


Trinken. Cruisen. Rumlungern.

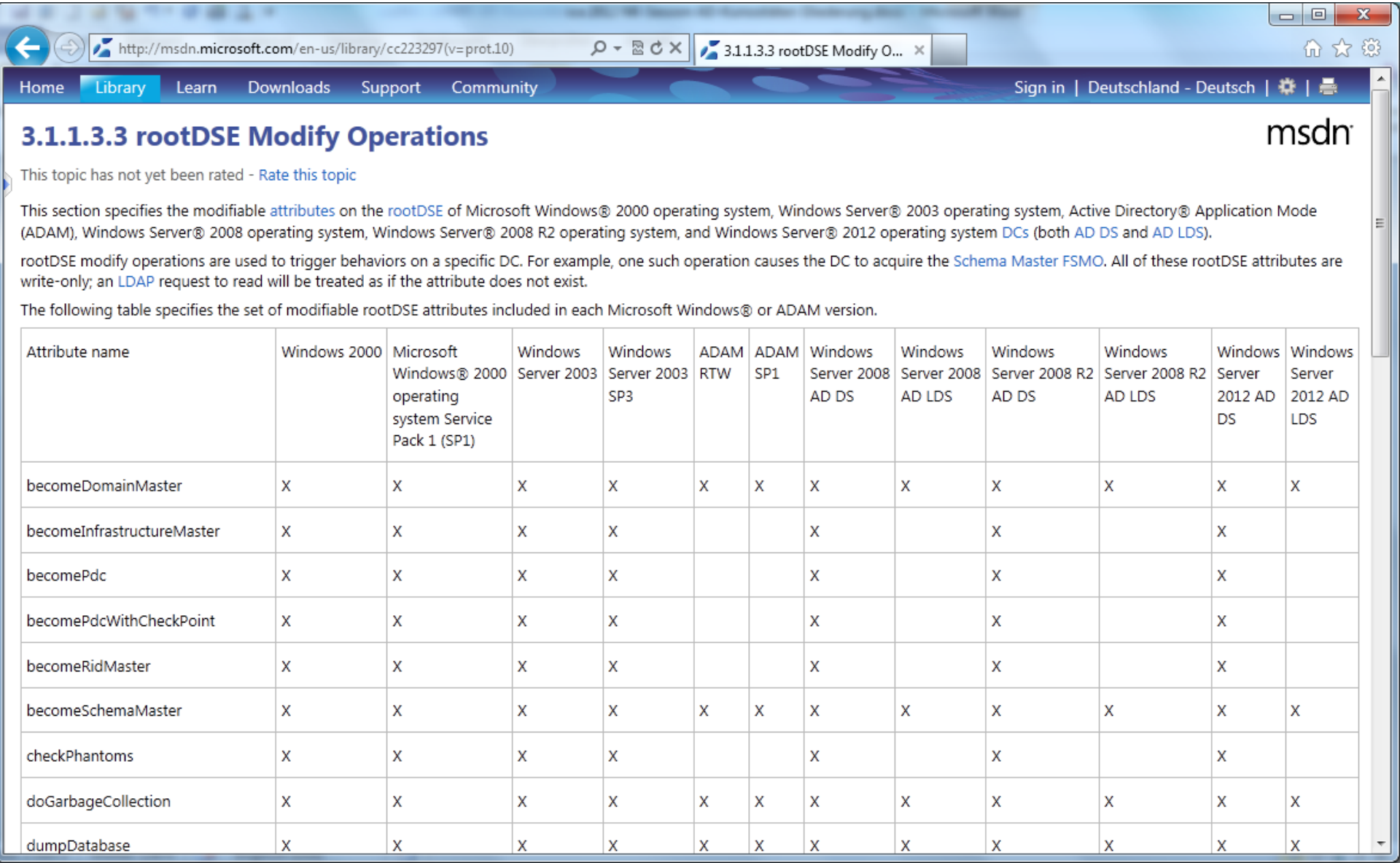
Folgt alles einem Schema

- Aufschlussreiche Attribute
- Wir nutzen genau dieses Attribut
- Name ist Schall und Rauch
- Feste Partnerschaften
- Die Klasse von 88
- Verwirrung auf dem Friedhof
- Attribut-Auslöser

Verwirrung auf dem Friedhof

- TSL original: 60 Tage
- TSL seit Windows Server 2003 SP1: 180 Tage
- Entscheidend: *Erster* DC im Forest
- Datei-Bug in Windows Server 2003 R2:
  - Installation 1. CD/dcpromo: 180 Tage
  - Installation 2. CD/dcpromo: 60 Tage …

Attribut-Auslöser



http://msdn.microsoft.com/en-us/library/cc223297(v=prot.10)

3.1.1.3.3 rootDSE Modify O...

Home | Library | Learn | Downloads | Support | Community | Sign in | Deutschland - Deutsch

msdn

3.1.1.3.3 rootDSE Modify Operations

This topic has not yet been rated - Rate this topic

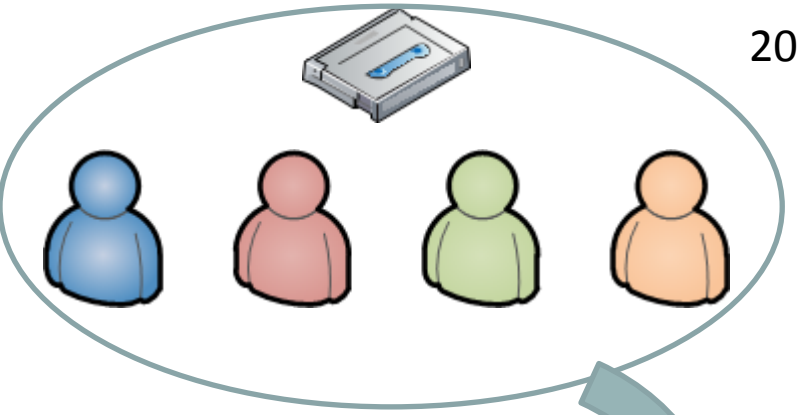
This section specifies the modifiable attributes on the rootDSE of Microsoft Windows® 2000 operating system, Windows Server® 2003 operating system, Active Directory® Application Mode (ADAM), Windows Server® 2008 operating system, Windows Server® 2008 R2 operating system, and Windows Server® 2012 operating system DCs (both AD DS and AD LDS).

rootDSE modify operations are used to trigger behaviors on a specific DC. For example, one such operation causes the DC to acquire the Schema Master FSMO. All of these rootDSE attributes are write-only; an LDAP request to read will be treated as if the attribute does not exist.

The following table specifies the set of modifiable rootDSE attributes included in each Microsoft Windows® or ADAM version.

Attribute name	Windows 2000	Microsoft Windows® 2000 operating system Service Pack 1 (SP1)	Windows Server 2003	Windows Server 2003 SP3	ADAM RTW	ADAM SP1	Windows Server 2008 AD DS	Windows Server 2008 AD LDS	Windows Server 2008 R2 AD DS	Windows Server 2008 R2 AD LDS	Windows Server 2012 AD DS	Windows Server 2012 AD LDS
becomeDomainMaster	X	X	X	X	X	X	X	X	X	X	X	X
becomeInfrastructureMaster	X	X	X	X			X		X		X	
becomePdc	X	X	X	X			X		X		X	
becomePdcWithCheckPoint	X	X	X	X			X		X		X	
becomeRidMaster	X	X	X	X			X		X		X	
becomeSchemaMaster	X	X	X	X	X	X	X	X	X	X	X	X
checkPhantoms	X	X	X	X			X		X		X	
doGarbageCollection	X	X	X	X	X	X	X	X	X	X	X	X
dumpDatabase	X	X	X	X	X	X	X	X	X	X	X	X

Herumlungernde Objekte



20. 06. 2012

User „Blau“
gelöscht am
21. Juni 2012

DC01

DC02

FAQ-O-MATIC.NET

Lingering Objects

- Gelöschte Objekte: Tombstone
- Nach Tombstone Lifetime:
  Jeder DC löscht das Objekt
- Restore eines zu alten Backup …
- … oder Replikationspause länger als
  Tombstone Lifetime …
- … führen zu Lingering Objects
- Abhilfe: repadmin /removelingeringobjects

FAQ-O-MATIC.net


Ignorieren oder umdeuten?

Vorgaben ignorieren oder umdeuten

- Anzeigenamen sind dynamisch
- Erweiterte Ansicht
- Online-Backup
- Neue Attribute erleichtern vieles

NTDSUtil: SET PATH BACKUP

- set path backup %s
  (where %s identifies a target directory)
- Sets the disk-to-disk backup target to the directory specified by %s. The directory service can be configured to perform an online, disk-to-disk backup at scheduled intervals.
- http://technet.microsoft.com/de-de/library/cc753900(WS.10).aspx

FAQ-O-MATIC.net

Neue Attribute erleichtern vieles

- Früher: Terminalserver-Profile in Binärfeld
  - userParameters
  - Schwer auszuwerten
  - Noch schwerer zu verändern
- Heute: Einzelne TS-Profil-Attribute
  - Leicht auszuwerten
  - Leicht zu bearbeiten
  - … aber …

FAQ-O-MATIC.net


Sicherheit oder Risiko?

Sicherheit? Oder lieber Risiko?

- Willkommen in der Firma!
- Kein Blackberry für die IT … wie schön!
- Geheimnisse für sich behalten

FaQ-o-maTic.net

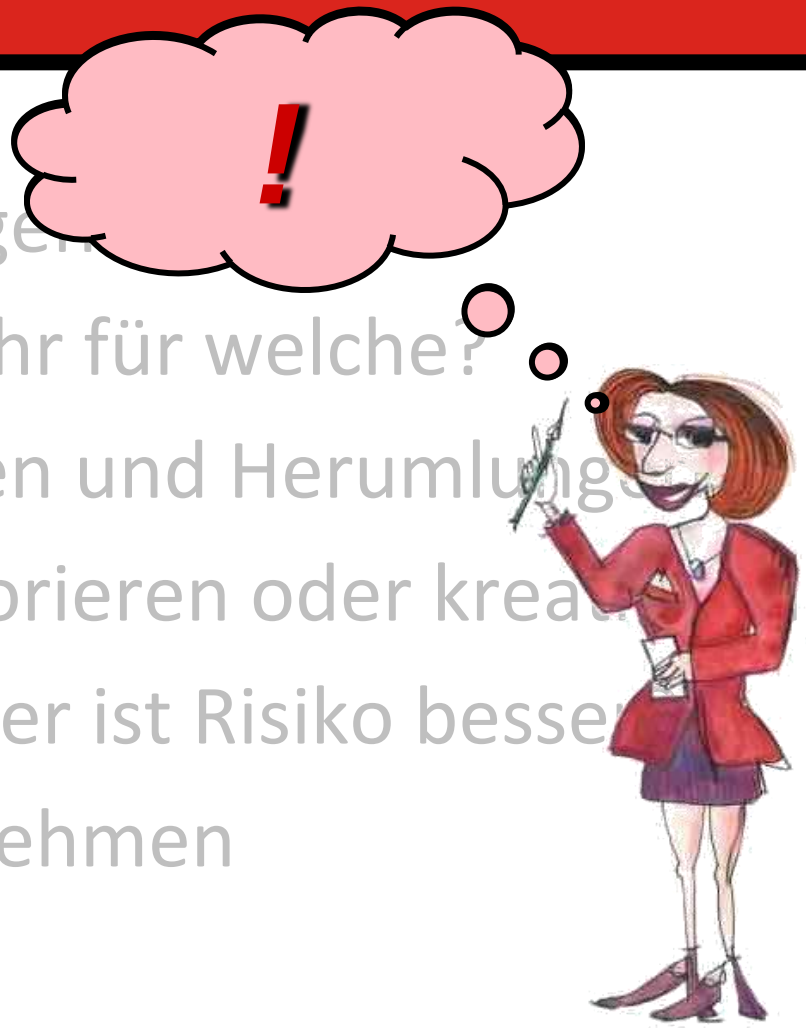

Seltsames Benehmen

Seltsames Benehmen

- Vorsicht? Braucht kein Mensch!
- Dazugehören und Draußenbleiben
- Senf dazugeben
- Möglichst umständlich
- Plötzlich verschwunden

Was euch erwartet

- Wer bin ich eigen
- Und was seid ihr für welche?
- Trinken, Cruisen und Herumlunge
- Vorgaben: Ignorieren oder krea deuten
- Sicherheit? Oder ist Risiko besse
- Seltsames Benehmen



… mehr davon …

12. September 2012

Wirtschaftsmesse Hannover

Windows 8 in aller Munde –
auch auf dem Firmen-PC?

7. bis 29. November 2012

heise Netze Tour

BYOD: Fremde Geräte im Netz

Konferenz-Roadshow

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)