Server 2012 – Gruppenrichtlinie Softwareeinschränkungen

Mit der **Richtlinie für Softwareeinschränkungen**, lässt sich festlegen, welche Programme der User ausführen darf und welche nicht.

https://technet.microsoft.com/en-us/library/bb457006.aspx

Die Softwareeinschränkung erlaubt uns den Einsatz von 4 Indikatoren zur Identifizierung von Software:

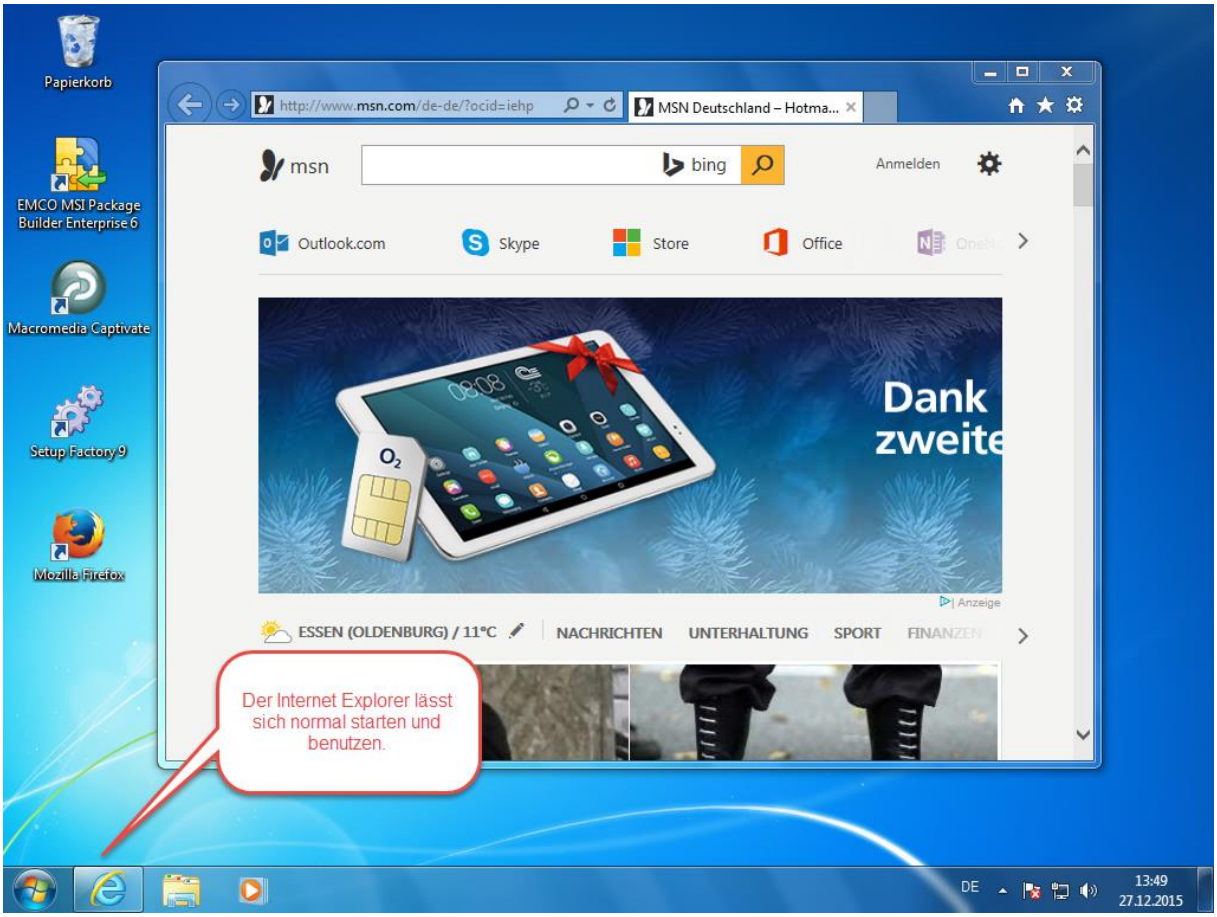
- Zertifikatsregeln (verwendete Zertifikate zum Signieren einer Datei seitens des Softwareherstellers)
- Hashregeln (der kryptografische Fingerprint einer Datei – z.B. MD5 oder SHA1)
- Netzwerkzonenregeln (Internet Zone)
- Pfadregeln (lokaler oder UNC Pfad zu einer Anwendung)

Wie man sieht ist die Palette an Möglichkeiten recht vielfältig und es eröffnet einem neue Wege zur Einschränkung des Anwendungsspielraums von Benutzern an einem Netzwerkcomputer.

Über diese Methode lassen sich auch portable Programme verbieten, komplette Pfade mit Unterverzeichnissen ausschließen, die Ausführung von Viren, Skripten usw. verhindern.

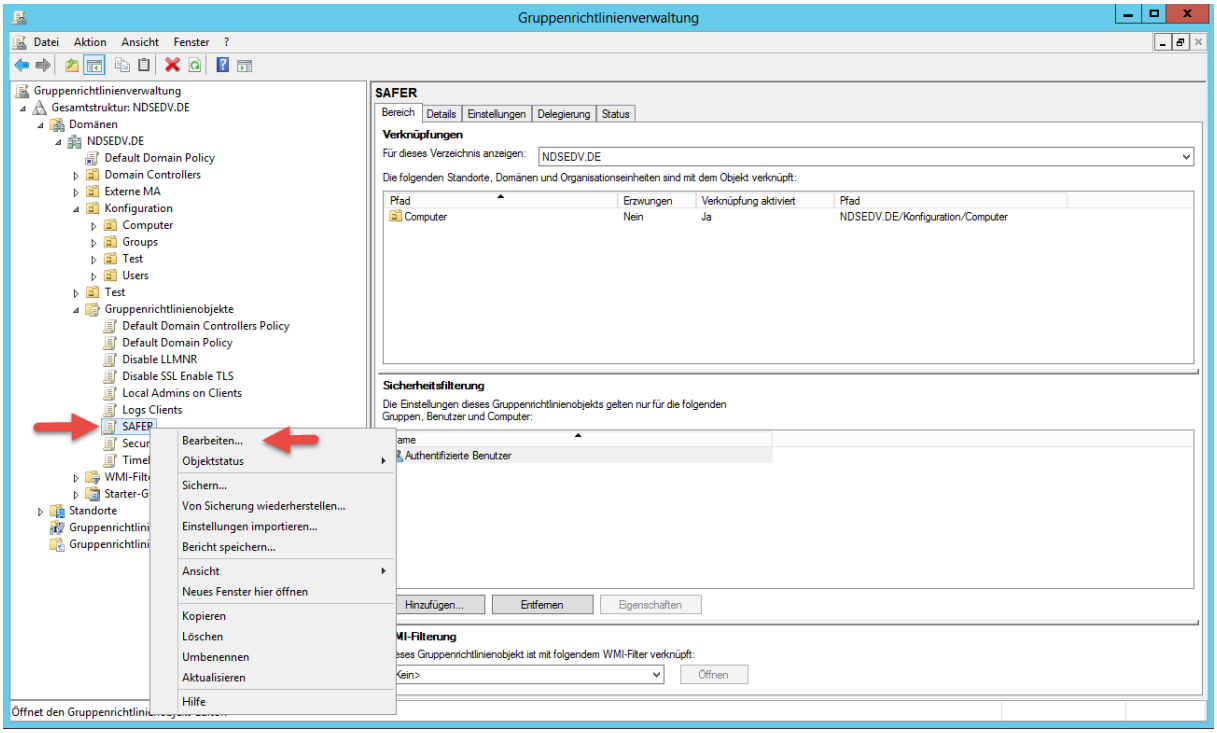
Ausgangssituation:

Der Internet Explorer lässt sich ganz normal starten.

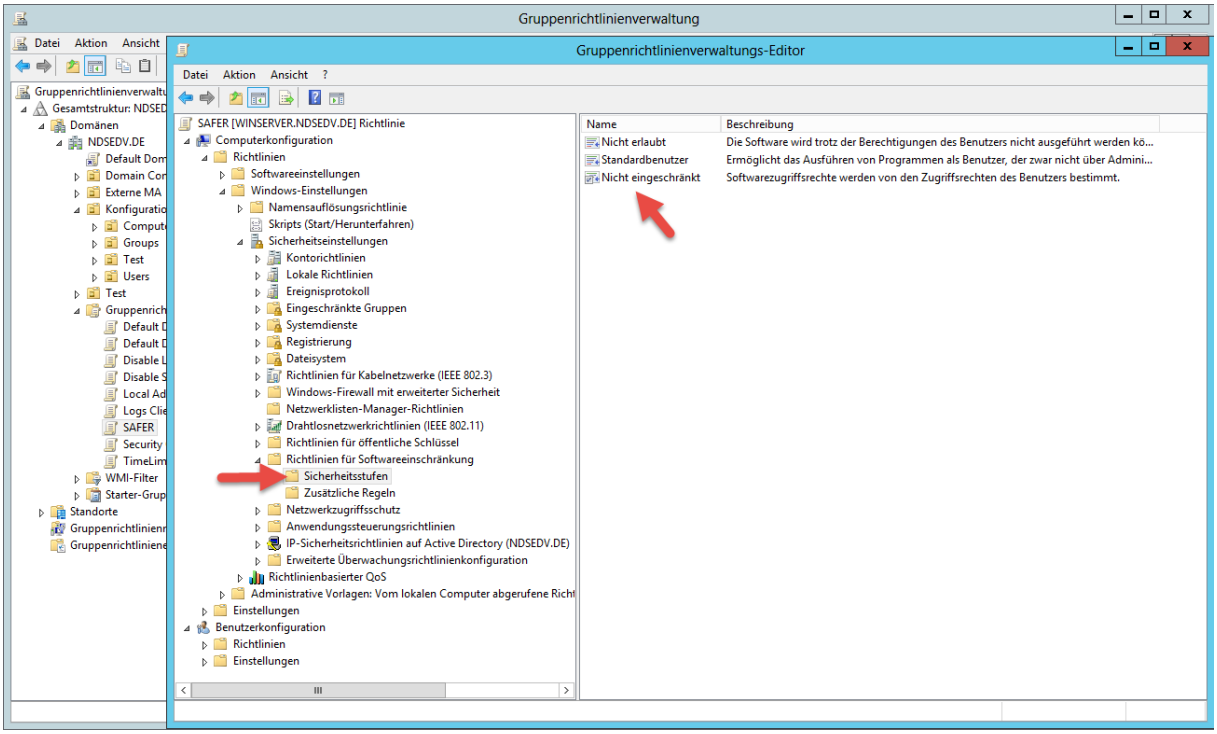


Server 2012 – Gruppenrichtlinie Softwareeinschränkungen

Wir erstellen zur Einschränkung ein neues GPO (Group Policy Object) und nennen es SAFER.

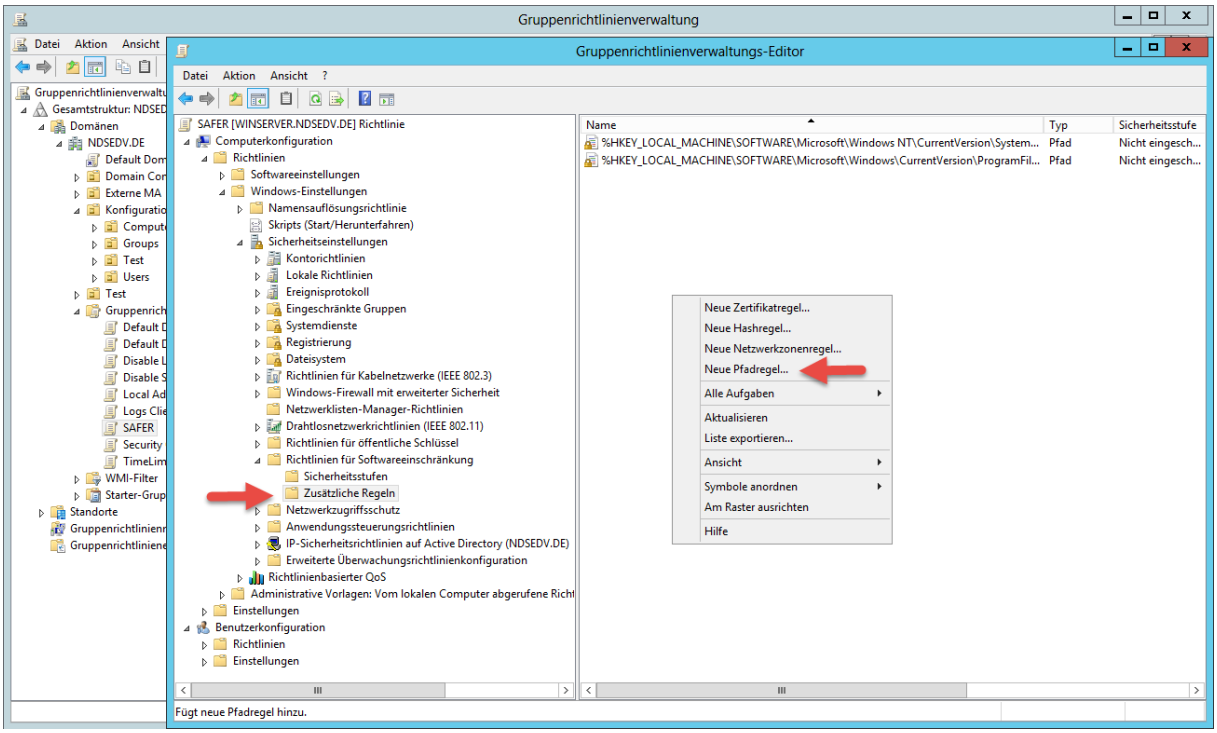


Die Sicherheitsstufen lassen wir unberührt.

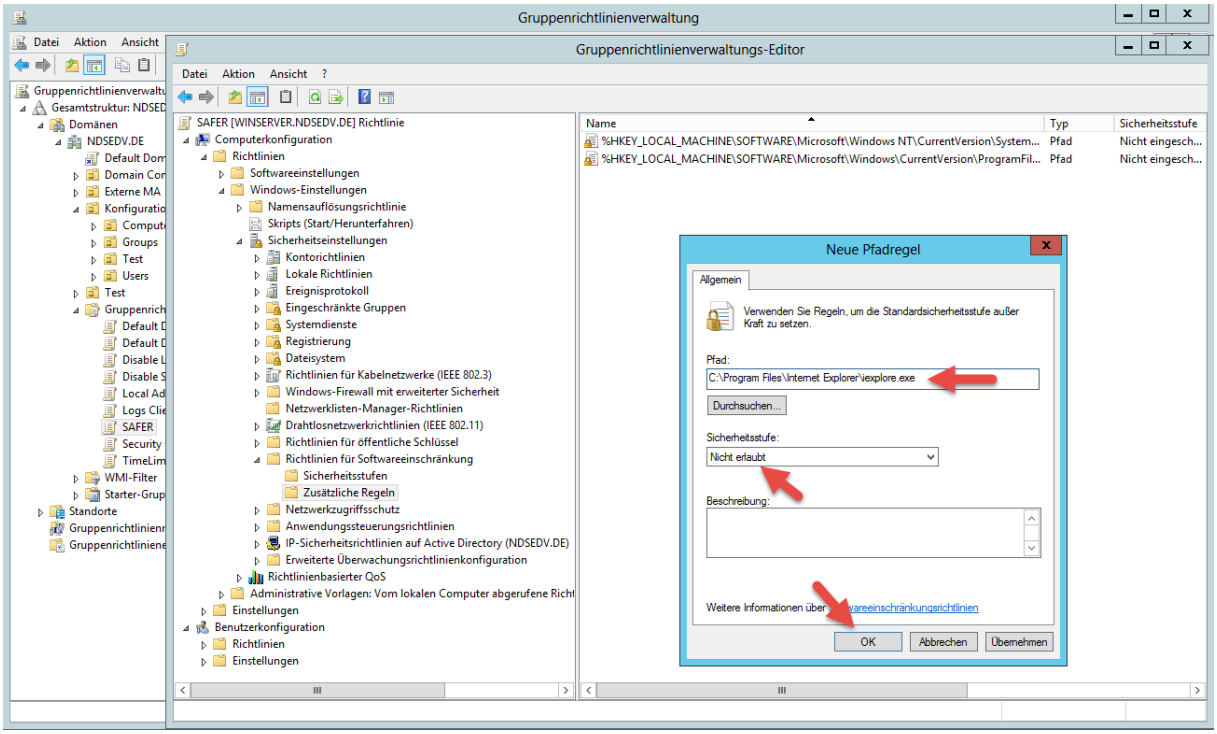


Server 2012 – Gruppenrichtlinie Softwareeinschränkungen

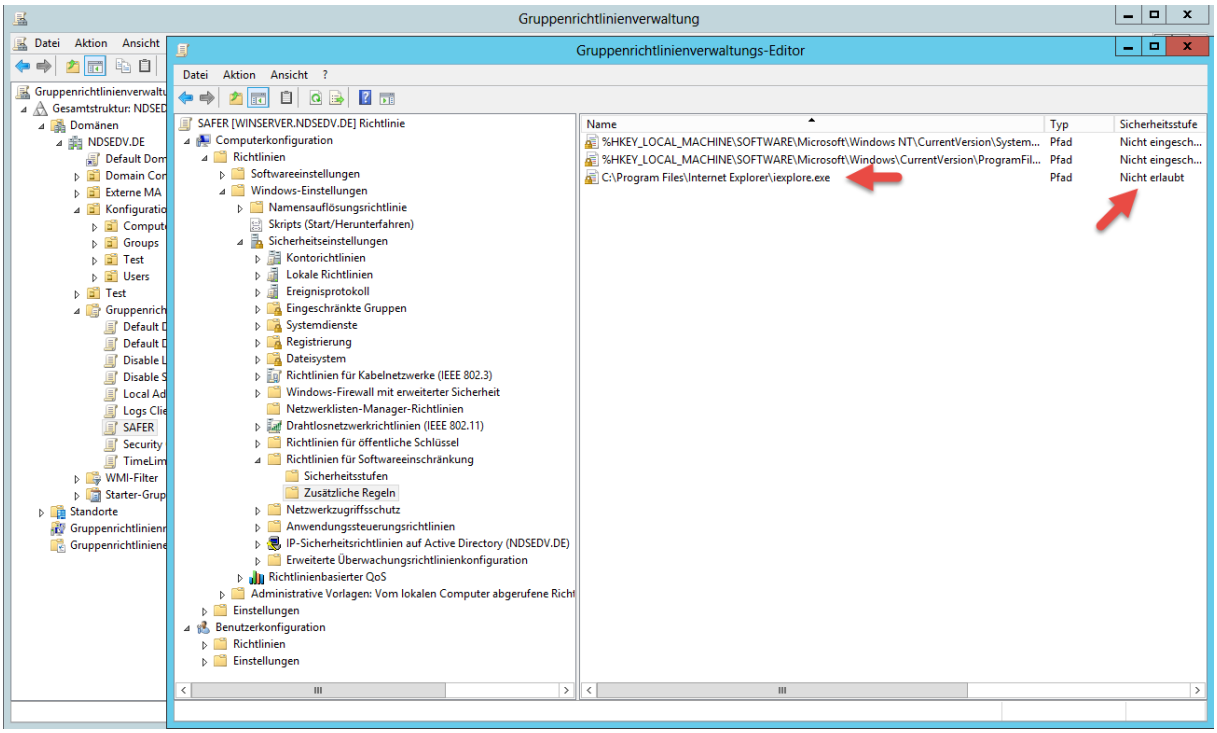
Wir definieren in diesem Beispiel eine **> Neue Pfadregel...**



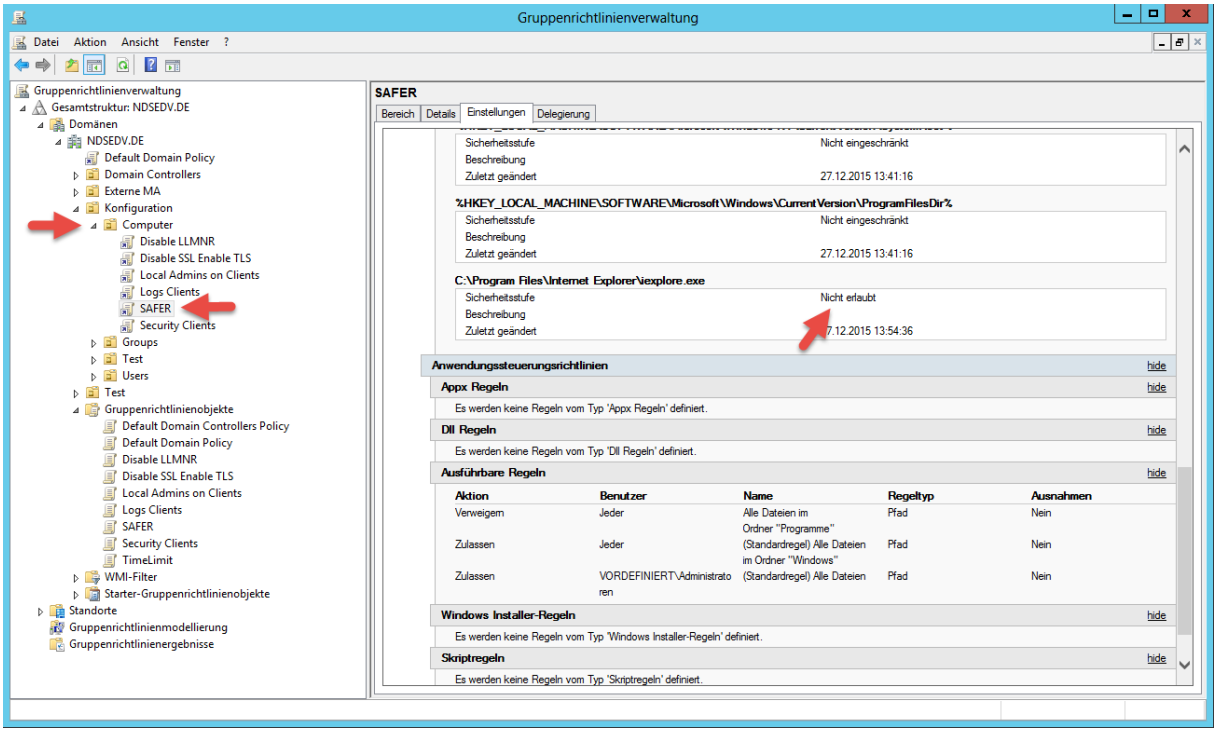
...und schränken die Nutzung des Internet Explorer durch das setzen der Sicherheitsstufe auf **> Nicht erlaubt** ein.



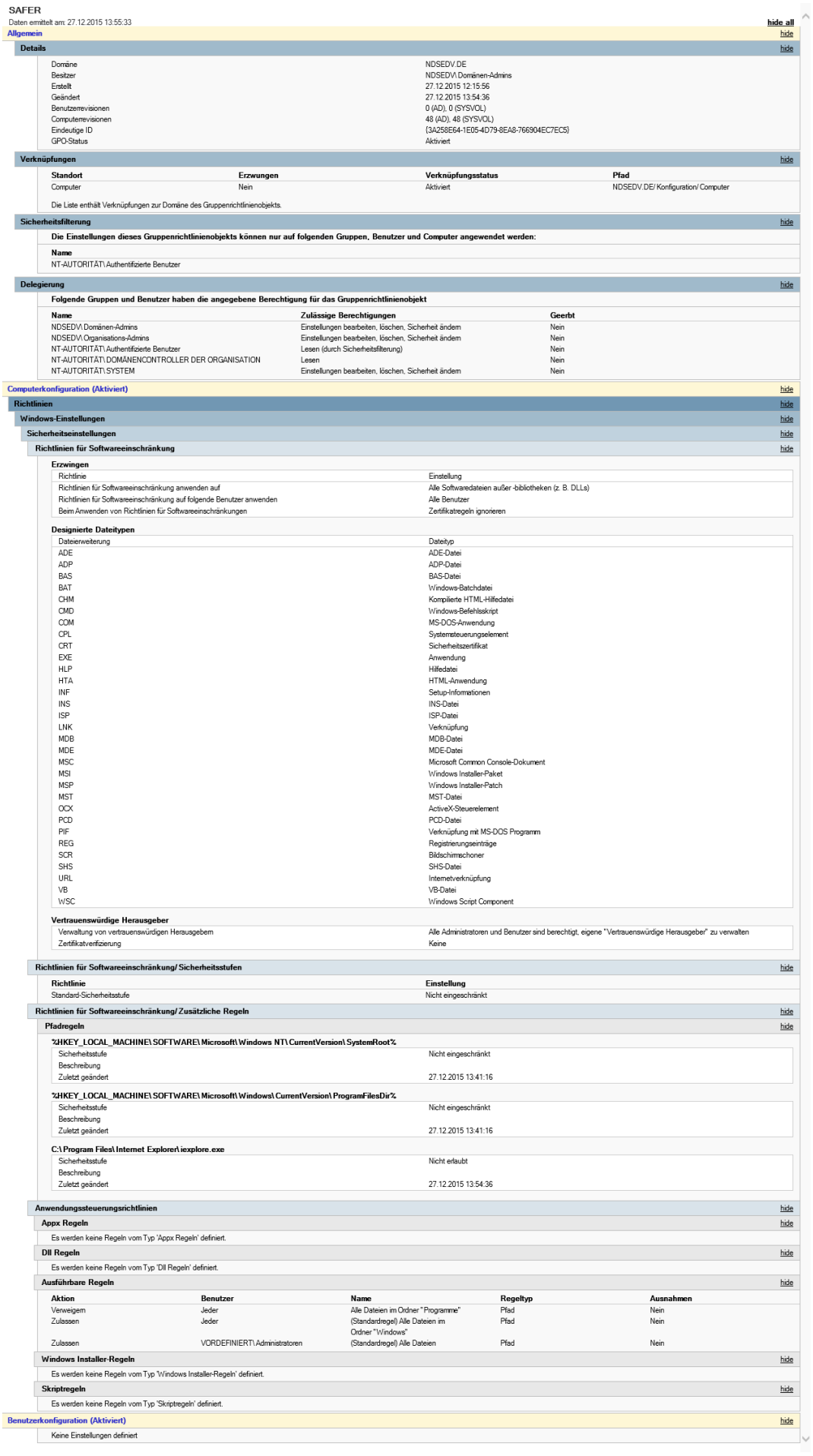
Die Konfiguration ist abgeschlossen.



Die neue Richtlinie wurde auf die **OU = Computer** verlinkt.



Server 2012 – Gruppenrichtlinie Softwareeinschränkungen



SAFER

Daten ermittelt am: 27.12.2015 13:55:33 — hide all

Allgemein — hide

Details — hide

Domäne	NDSEDV.DE
Besitzer	NDSEDV\Domänen-Admins
Erstellt	27.12.2015 12:15:56
Geändert	27.12.2015 13:54:36
Benutzerrevisionen	0 (AD), 0 (SYSVOL)
Computerrevisionen	48 (AD), 48 (SYSVOL)
Eindeutige ID	{3A258E64-1E05-4D79-8EA8-766904EC7EC5}
GPO-Status	Aktiviert

Verknüpfungen — hide

Standort	Erzwungen	Verknüpfungsstatus	Pfad
Computer	Nein	Aktiviert	NDSEDV.DE/ Konfiguration/ Computer

Die Liste enthält Verknüpfungen zur Domäne des Gruppenrichtlinienobjekts.

Sicherheitsfilterung — hide

Die Einstellungen dieses Gruppenrichtlinienobjekts können nur auf folgenden Gruppen, Benutzer und Computer angewendet werden:

Name
NT-AUTORITÄT\Authentifizierte Benutzer

Delegierung — hide

Folgende Gruppen und Benutzer haben die angegebene Berechtigung für das Gruppenrichtlinienobjekt

Name	Zulässige Berechtigungen	Geerbt
NDSEDV\Domänen-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NDSEDV\Organisations-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NT-AUTORITÄT\Authentifizierte Benutzer	Lesen (durch Sicherheitsfilterung)	Nein
NT-AUTORITÄT\DOMÄNENCONTROLLER DER ORGANISATION	Lesen	Nein
NT-AUTORITÄT\SYSTEM	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein

Computerkonfiguration (Aktiviert) — hide

Richtlinien — hide

Windows-Einstellungen — hide

Sicherheitseinstellungen — hide

Richtlinien für Softwareeinschränkung — hide

Erzwingen

Richtlinie	Einstellung
Richtlinien für Softwareeinschränkung anwenden auf	Alle Softwaredateien außer -bibliotheken (z. B. DLLs)
Richtlinien für Softwareeinschränkung auf folgende Benutzer anwenden	Alle Benutzer
Beim Anwenden von Richtlinien für Softwareeinschränkungen	Zertifikatregeln ignorieren

Designierte Dateitypen

Dateierweiterung	Dateityp
ADE	ADE-Datei
ADP	ADP-Datei
BAS	BAS-Datei
BAT	Windows-Batchdatei
CHM	Kompilierte HTML-Hilfedatei
CMD	Windows-Befehlsskript
COM	MS-DOS-Anwendung
CPL	Systemsteuerungselement
CRT	Sicherheitszertifikat
EXE	Anwendung
HLP	Hilfedatei
HTA	HTML-Anwendung
INF	Setup-Informationen
INS	INS-Datei
ISP	ISP-Datei
LNK	Verknüpfung
MDB	MDB-Datei
MDE	MDE-Datei
MSC	Microsoft Common Console-Dokument
MSI	Windows Installer-Paket
MSP	Windows Installer-Patch
MST	MST-Datei
OCX	ActiveX-Steuerelement
PCD	PCD-Datei
PIF	Verknüpfung mit MS-DOS Programm
REG	Registrierungseinträge
SCR	Bildschirmschoner
SHS	SHS-Datei
URL	Internetverknüpfung
VB	VB-Datei
WSC	Windows Script Component

Vertrauenswürdige Herausgeber

Verwaltung von vertrauenswürdigen Herausgebern	Alle Administratoren und Benutzer sind berechtigt, eigene "Vertrauenswürdige Herausgeber" zu verwalten
Zertifikatverifizierung	Keine

Richtlinien für Softwareeinschränkung/ Sicherheitsstufen — hide

Richtlinie	Einstellung
Standard-Sicherheitsstufe	Nicht eingeschränkt

Richtlinien für Softwareeinschränkung/ Zusätzliche Regeln — hide

Pfadregeln — hide

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%

Sicherheitsstufe	Nicht eingeschränkt
Beschreibung	
Zuletzt geändert	27.12.2015 13:41:16

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

Sicherheitsstufe	Nicht eingeschränkt
Beschreibung	
Zuletzt geändert	27.12.2015 13:41:16

C:\Program Files\Internet Explorer\iexplore.exe

Sicherheitsstufe	Nicht erlaubt
Beschreibung	
Zuletzt geändert	27.12.2015 13:54:36

Anwendungssteuerungsrichtlinien — hide

Appx Regeln — hide

Es werden keine Regeln vom Typ 'Appx Regeln' definiert.

Dll Regeln — hide

Es werden keine Regeln vom Typ 'Dll Regeln' definiert.

Ausführbare Regeln — hide

Aktion	Benutzer	Name	Regeltyp	Ausnahmen
Verweigern	Jeder	Alle Dateien im Ordner "Programme"	Pfad	Nein
Zulassen	Jeder	(Standardregel) Alle Dateien im Ordner "Windows"	Pfad	Nein
Zulassen	VORDEFINIERT\Administratoren	(Standardregel) Alle Dateien	Pfad	Nein

Windows Installer-Regeln — hide

Es werden keine Regeln vom Typ 'Windows Installer-Regeln' definiert.

Skriptregeln — hide

Es werden keine Regeln vom Typ 'Skriptregeln' definiert.

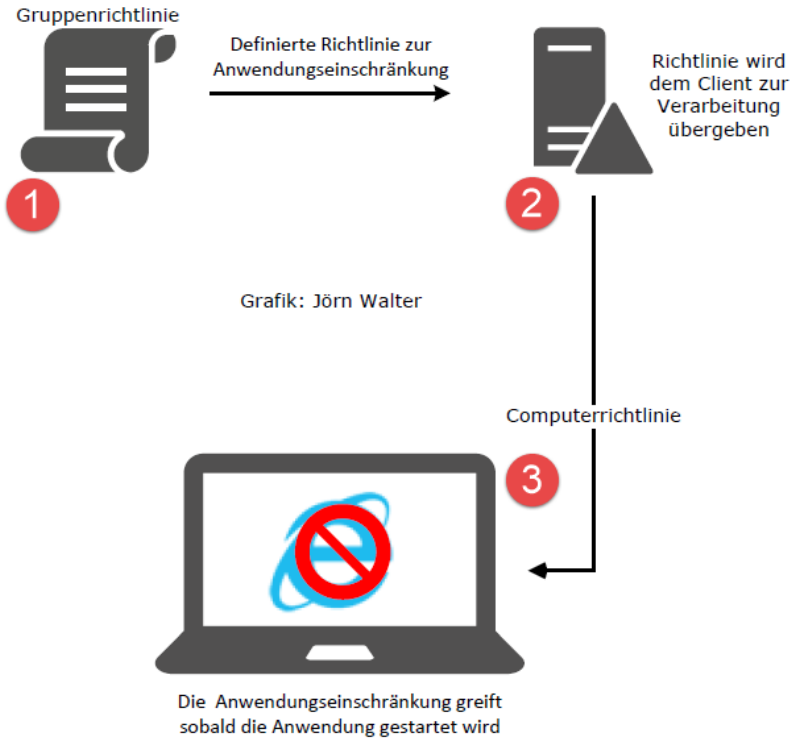
Benutzerkonfiguration (Aktiviert) — hide

Keine Einstellungen definiert

Erstellt von Jörn Walter www.der-windows-papst.de – 27.12.2015

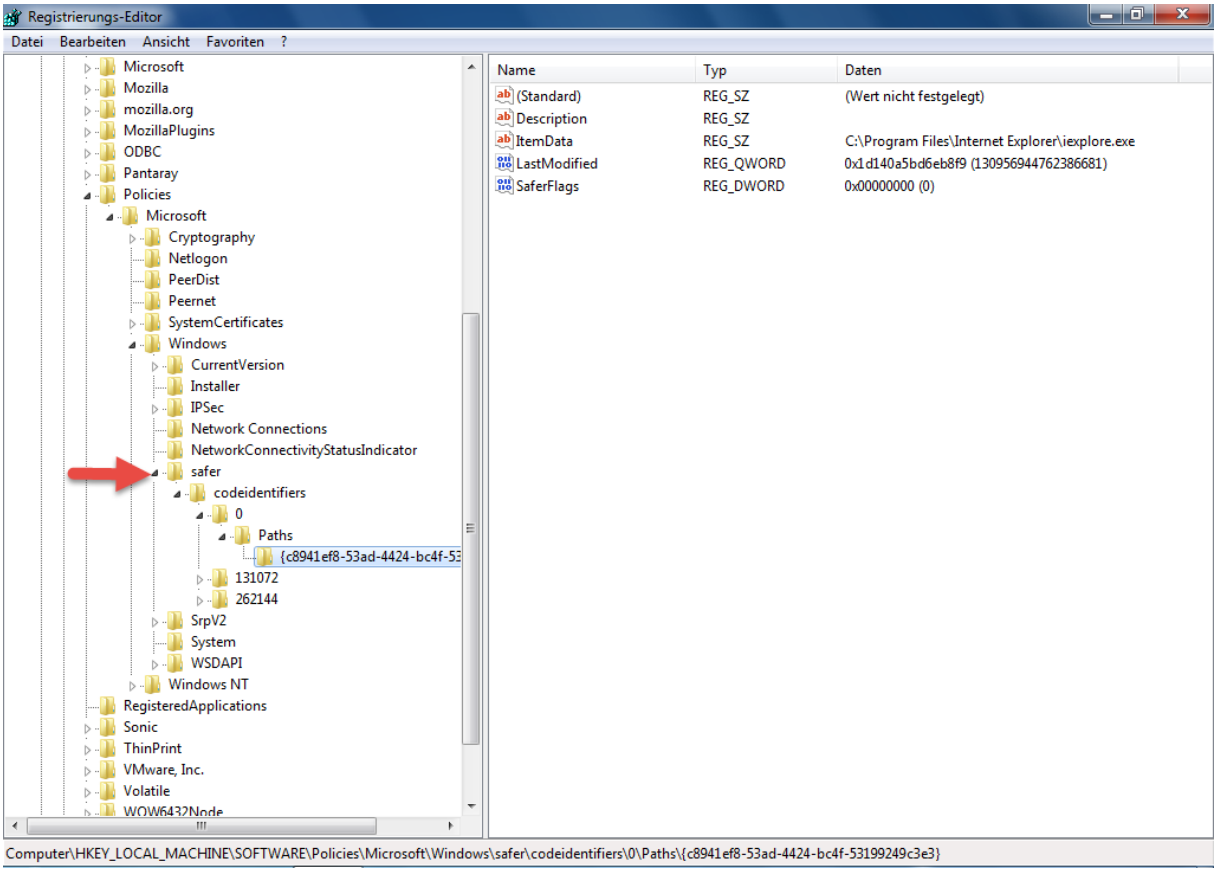
Server 2012 – Gruppenrichtlinie Softwareeinschränkungen

Ablauf:



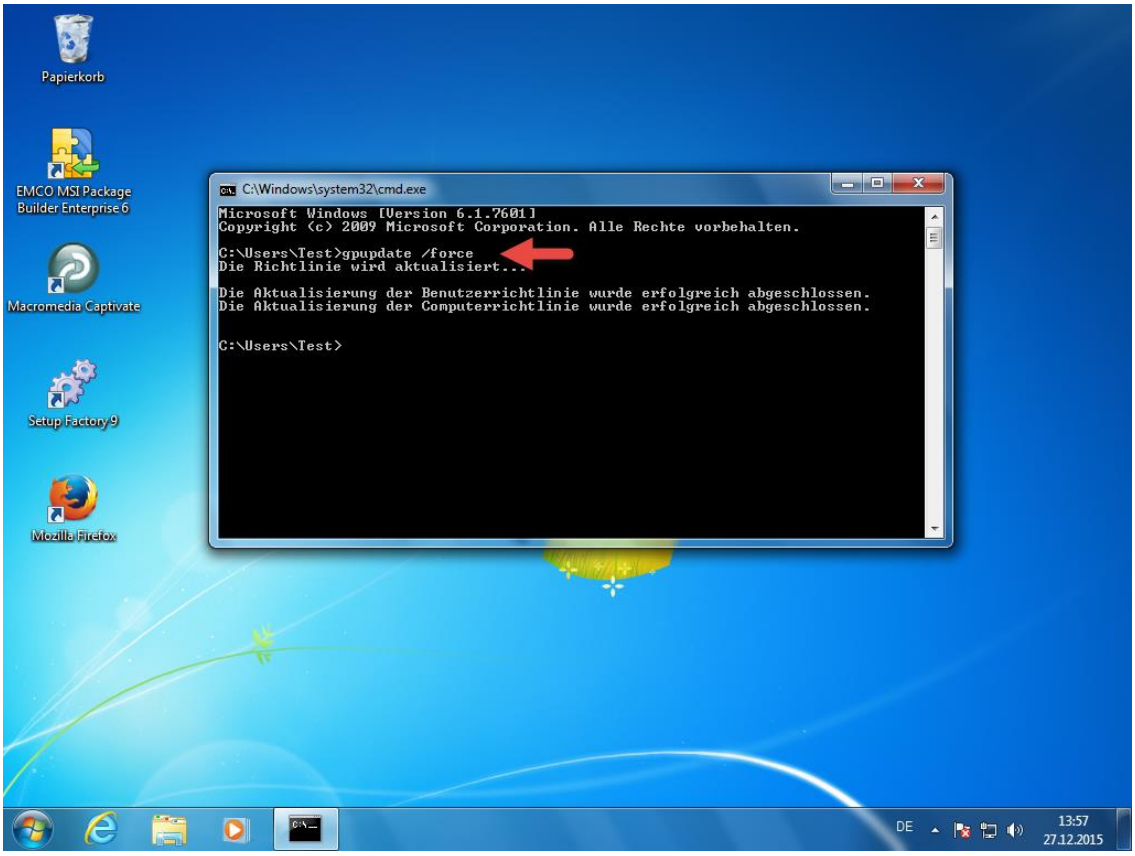
In der Registry finden wir die Einstellungen an folgender Stelle wieder:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer



Server 2012 – Gruppenrichtlinie Softwareeinschränkungen

Nach einem GPUPDATE /FORCE auf dem Client, wird die neue Richtlinie zur Verarbeitung übertragen.



Beim Versuch den IE zu starten, wird dieser durch die Richtlinie außer Kraft gesetzt.