Einrichtung von Richtlinien für Softwareeinschränkungen (Software Restriction Policies)

Dokumentation der betrieblichen Projektarbeit
im Rahmen der Abschlussprüfung
zum Fachinformatiker für Systemintegration

Fabian Kollenberg
Kampstraße 12
45468 Mülheim an der Ruhr
Identnummer: 122603314

PVS holding GmbH
Remscheider Str. 16
45481 Mülheim an der Ruhr

Inhalt

1. Einleitung

1.1 Das Unternehmen

Die PVS holding GmbH, fortlaufend PVS genannt, ist ein Dienstleistungsunternehmen im Gesundheitswesen. Ihren Gewinn erzielt die PVS primär durch private und gesetzliche Honorarabrechnungen für Ärzte und Chefärzte, für die eine Gebühr berechnet wird. Ärzte und Chefärzte werden durch die Dienstleistung der PVS in ihrem wirtschaftlichen Alltag entlastet.

Gegründet wurde die PVS in Mülheim an der Ruhr. Hier befindet sich auch der Hauptsitz, an dem zur Zeit 300 Mitarbeiter/-innen angestellt sind. Zusammen mit zwölf weiteren Standorten in Deutschland beschäftigt die PVS rund 700 Mitarbeiter/-innen.

Die PVS hat eine eigene IT-Abteilung mit insgesamt 27 Mitarbeiter-/innen, die in der Hauptverwaltung tätig sind.

Für die tägliche Arbeit als Dienstleistungsunternehmen wird Individualsoftware benötigt, die von der IT-Entwicklung entwickelt und ständig verbessert wird. Alle Mitarbeiter im Unternehmen arbeiten an einem eigenen PC-Arbeitsplatz, an dem Hard- oder Softwareprobleme entstehen können. Um diese Probleme kümmert sich die IT-Technik. Außerdem gibt es noch die Bereiche IT-Support und IT-Koordination.

Die Abteilung teilt sich folgendermaßen auf:

- IT-Entwicklung: 11 Mitarbeiter, 1 Auszubildender
- IT-Technik: 7 Mitarbeiter, 2 Auszubildende
- IT-Support: 4 Mitarbeiter
- IT-Koordination: 2 Mitarbeiter.

1.2 Projektumfeld

Das Projektumfeld setzt sich aus den Benutzerrichtlinien von Windows 7 Professional, einem voll ausgestatteten PC-Arbeitsplatz mit dem Betriebssystem Windows 7 Professional und der umfangreichen Verwaltungssoftware ZENworks von Micro Focus zusammen.

Auftraggeber des Projektes für die Abschlussprüfung ist Herr Müller, Leiter der IT-Abteilung. Das fertiggestellte Projekt soll zukünftig an jedem PC-Arbeitsplatz und in allen Geschäftsstellen der PVS zum Einsatz kommen.

Bei der Planung des Projektes sowie an der Informationsbeschaffung beteiligt sind:

- Herr Müller (Abteilungsleitung IT, Projektleiter)
- Herr Braun (Systemadministrator)

1.3 Motivation und Zielsetzung

Da die PVS mit sensiblen Patientendaten arbeitet, ist die Datensicherheit ein wichtiges Thema. Mit meinem Projekt möchte ich zu dieser Sicherheit beitragen und unerlaubte Zugriffe, die zwar durch andere Systeme, wie zum Beispiel der eingesetzten Firewall, bereits gut geblockt werden, noch weiter einschränken.

Ziel des Projektes ist es, eine noch höhere Sicherheit der Computer im Arbeitsalltag zu erlangen, die von den Mitarbeiter/-innen tagtäglich benutzt werden, ohne dabei den bisher gewohnten Komfort einzuschränken. Dieses soll mithilfe des Projektes „Einrichtung von Richtlinien für Softwareeinschränkungen (Software Restriction Policies)" erreicht werden.

1.4 Projektschnittstellen

In der angesetzten Projektlaufzeit von 35 Stunden werden folgende Schnittstellen hergestellt:

Auftraggeber	Herr Müller
Festlegen der Anforderungen	Herr Braun
Ansprechpartner bei technischen Fragen	Herr Braun
Abnahme des Projektes und der Dokumentation	Herr Müller

1.5 Projektabgrenzung

Das Projekt beschränkt sich auf die Einrichtung der Software Restriction Policies die unter Zuhilfenahme der Windows Gruppenrichtlinien definiert werden sowie die Implementierung in die vorhandene Infrastruktur. Die Verteilung auf alle Standard PC´s erfolgt mit dem Software-Management- und Verteilungstool ZENworks.

1.6 Erklärung Software Restriction Policies

Software Restriction Policies, zu Deutsch Richtlinien für Softwareeinschränkungen, ist eine in Windows vorhandene Funktion (siehe 6.2, Abbildung 2). Mit ihr ist es möglich, das Ausführen von Software und Dateien beliebig stark einzuschränken. Das hilft Firmen dabei, die Zuverlässigkeit, Integrität und Verwaltbarkeit der Computer von Mitarbeiter/-innen zu verbessern.

2. Projektbeschreibung

2.1 Ist-Analyse

Derzeit bestehen im Betrieb keine Software Restriction Policies. Jeder Benutzer kann daher alle Dateien und Programme ohne Einschränkungen ausführen, die sich auf dem PC befinden. Bisher werden nur Downloads aus dem Internet durch die eingesetzte Astaro Surf Protection, eine Firewall-Lösung der Firma Sophos, beschränkt und Programminstallationen auf den Benutzer-Accounts bei fehlenden Administratorrechten verhindert.

Für letztere Maßnahme wird bei der Einrichtung eines neuen Computers und vor der Auslieferung an Mitarbeiter/-innen, automatisch ein lokales Administratorprofil erstellt. Dieser passwortgeschützte Administrator-Account kann und darf nur von der IT-Abteilung benutzt werden.

Der jetzige Stand verhindert jedoch nicht das Ausführen von beispielsweise Executables, die im Portable-Format vorliegen. Das sind Programme, die auch ohne den Windows-Installer lauffähig sind und dementsprechend keine Administratorrechte voraussetzen. Mitarbeiter/-innen könnten solche portablen Programme von zu Hause auf einem USB-Stick oder einer CD mitbringen und ohne Kenntnis der IT-Abteilung am eigenen PC-Arbeitsplatz ausführen.

Hierdurch entsteht ein potenzielles Sicherheitsrisiko, da Mitarbeiter/-innen somit unbeabsichtigt Schadsoftware verbreiten könnten. Außerdem kann, aufgrund fehlender vorausgegangener Softwaretests durch die IT-Abteilung, nicht garantiert werden, dass es durch die mitgebrachte, portable Software nicht zu Kompatibilitätsproblemen mit anderen Programmen kommt.

2.2 Soll-Analyse

Nach der Fertigstellung des Projektes und der Integration in das Produktivsystem soll das System so konfiguriert sein, dass jedes Ausführen einer nicht zugelassenen Software oder Datei unterbunden wird.

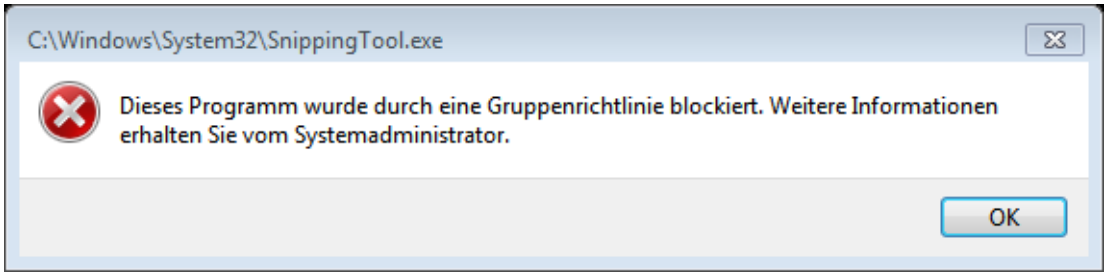
Außerdem soll neben der Software Restriction Policies ein separates Skript erstellt werden, das dazu in der Lage ist, Informationen über mögliche Fehler zu sammeln, die anschließend von einem Administrator analysiert werden können.

Nach Rücksprache mit den Projektbetreuern habe ich entschieden, dass die Software Restriction Policies mit einer Whitelist arbeiten sollen. Zukünftig sollen alle Programme, Dateien oder Verknüpfungen, die nicht in der Whitelist vorzufinden sind, nach der Integration gesperrt werden. Dies soll dafür sorgen, dass das System der PVS sicherer gegen Schadprogramme aller Art wird.

Eine Alternative wäre eine Blacklist, die an dieser Stelle nicht sinnvoll ist, da sie nur bekannte Programme und Dateien blockiert. Sie hilft nur bedingt gegen Viren und unerlaubte Aktionen. Eine Blacklist-Lösung ist zudem wartungsaufwendiger, da immer wieder Einträge ergänzt werden müssen.

Sonstige eingesetzte Schutzmaßnahmen sollen trotz der Software Restriction Policies weiterhin greifen. Die Lösung soll keinen Einfluss auf die bereits bestehenden Sicherheitssysteme haben, sondern parallel dazu arbeiten.

Wenn ein Benutzer versucht, eine nicht erlaubte Software oder Datei zu öffnen, soll er eine Fehlermeldung erhalten, die ihm mitteilt, dass das Programm blockiert wurde.



Fehlermeldung beim Ausführen einer blockierten Datei

Sollte der Benutzer der Ansicht sein, dass das Programm oder die Datei zu Unrecht gesperrt ist, so kann er sich an die IT-Abteilung wenden. Ein IT-Mitarbeiter mit entsprechender Kenntnis prüft den Sachverhalt anschließend und kann gegebenenfalls Änderungen in den Einstellungen der Software Restriction Policies vornehmen.

2.3 Abweichungen vom Projektantrag

Sollte es bei der Umsetzung zu Problemen kommen, die im Vorfeld nicht vorhersehbar waren, so soll es mittels eines kleinen Skriptes in Form einer Batch-Datei möglich sein, eine Logdatei auf dem betroffenen Computer zu generieren, die Aufschluss über mögliche Fehlerquellen gibt.

3. Projektplanung

3.1 Projektphasen

Für das Projekt wurden folgende Phasen geplant:

1. Vorbereitung	**6 Stunden**
Ist-Analyse	2 Stunden
Soll-Analyse	2 Stunden
Planung	2 Stunden
2. Durchführung	**17 Stunden**
Image-Installation	2 Stunden
Kontaktaufnahme mit Benutzern mit spezieller Software	1 Stunde
Konfiguration der Windows Gruppenrichtlinien	9 Stunden
Test der Funktionalität	5 Stunden
3. Abschlussphase	**12 Stunden**
Abnahme durch den Projektleiter	1 Stunde
Übernahme in die Produktivumgebung	2 Stunden
Dokumentation	9 Stunden
Insgesamt:	**35 Stunden**

3.2 Kosten-/Nutzenanalyse

Für die Ermittlung der Projektkosten werden die Pauschalsätze der Controlling-Abteilung der PVS verwendet. Bei einem Auszubildenden im dritten Lehrjahr belaufen sich diese auf 8,50 Euro die Stunde. Die Personalkosten eines Mitarbeiters der IT-Abteilung belaufen sich auf 50,00 Euro die Stunde.

Für die beteiligten Mitarbeiter wird eine branchenübliche Kostenpauschale von 35,00 € für die Nutzung von Räumlichkeiten, Strom und Arbeitsmaterialien berechnet.

So ergeben sich folgende Gesamtkosten:

Vorgang	Mitarbeiter	Zeit	Kosten pro Stunde	Gesamtkosten
Durchführung	Herr Kollenberg	35 Stunden	43,50 €	1.522,50 €
Fachgespräche	Herr Braun	4 Stunden	85,00 €	340,00 €
Abnahme	Herr Müller	1 Stunde	85,00 €	85,00 €
Kosten gesamt				**1.947,50 €**

Die Kosten für den für das Projekt verwendeten Computer, auf dem die Testumgebung läuft, betragen 295,00 € im Einkauf. Diese sind für die Berechnung der Projektkosten nicht weiter relevant, da dieser üblicherweise als Arbeitsstation für Mitarbeiter verwendet wird. Somit wird der PC nach Beendigung des Projektes als solcher weiter verwendet.

Der Nutzen im Vergleich zu den anfallenden Kosten lässt sich nur bedingt ausrechnen, da die Integration der Software Restriction Policies eine reine Präventivmaßnahme ist. Stattdessen können vier Szenarien angenommen werden, die realistisch sind, sollte sich Schadsoftware den Weg in die Firma bahnen.

Im besten Fall beschränkt sich die Infektion lokal auf lediglich einen Computer. Möglicherweise kann das Schadprogramm durch ein eingesetztes Antivirensystem entfernt werden, im schlechtesten Fall muss der Rechner gegen einen neuen ausgetauscht werden. Das erste Szenario dauert circa eine Stunde und verursacht Kosten in Höhe von 43,50 Euro für den ausführenden IT-Auszubildenden. Hinzu kommt der Verdienstausfall des betroffenen Mitarbeiters, der laut der Controlling-Abteilung bei durchschnittlich 50,00 Euro pro Stunde liegt.

Lässt sich der Infekt nicht beheben, muss der befallene Rechner neu bespielt und später wieder in den Kreislauf eingeschleust werden. Diese Tätigkeit ist ebenfalls von einem IT-Auszubildenden durchführbar und dauert zwei Stunden. Es fallen Kosten in Höhe von 87,00 Euro für den Auszubildenden an, der Verdienstausfall des betroffenen Mitarbeiters liegt bei 100,00 Euro.

Eine Infektion aller Windows-Clienten ist ebenfalls möglich. Sollte die Softwareverteilung, auf die später ausführlicher eingegangen wird, nach dem Infekt noch funktionieren, so kann die Schadsoftware durch das Installieren eines Programms, welches den Infekt behebt, entfernt werden. Hierfür muss ein Systemadministrator circa vier Stunden arbeiten, was Kosten in Höhe von 340,00 Euro verursacht. Da alle anderen ca. 700 Angestellten während dieser Zeit ebenfalls nicht arbeiten können, entsteht ein durchschnittlicher Verdienstausfall in Höhe von 140.000,00 Euro.

Im schlimmsten Fall breitet sich die Schadsoftware auf alle Windows-Systeme aus und eine Behebung des Schadens ist nur noch durch das Neuaufspielen des Betriebssystems zu beheben. Bei 700 Mitarbeitern dauert diese Prozedur ungefähr 1.400 Stunden, die gesamte IT-Abteilung würde mit Hochdruck daran arbeiten den Arbeitsalltag so schnell wie möglich wiederherzustellen. Ohne den Verdienstausfall der Mitarbeiter, der mehrere Tage andauern und voraussichtlich pro Mitarbeiter 400,00 Euro pro Tag betragen würde, fallen zusätzliche Arbeitskosten in Höhe von 119.000 Euro für die IT-Mitarbeiter an.

Die Umsetzung des Projektes ist nach der Kosten-/Nutzenanalyse nur zu befürworten.

3.3 Projektablauf

Bevor das eigentliche Projekt beginnt, findet ein Gespräch mit Herrn Braun statt, in dem die genauen Anforderungen geklärt werden. Herr Braun steht mir während der gesamten Projektphase für technische Fragen zur Verfügung.

Zu Beginn besteht meine Aufgabe darin, einen Testrechner mit unserem Standard-Image zu bespielen. Dieses Abbild der Standard-PC´s besteht aus dem Betriebssystem Windows 7 Professional, einem Softwarepaket, bestehend aus verschiedenen Programmen wie Adobe Reader und Mozilla Firefox, sowie von der PVS selbst entwickelten Programmen und vordefinierten Einstellungen.

Nach der Installation definiere ich die Software Restriction Policies mit den Windows Gruppenrichtlinien. Anschließend findet ein Test statt, um nachvollziehen zu können, ob alles wie vorgesehen funktioniert. Ist dies nicht der Fall, kann über ein selbst erstelltes Batch-Skript eine Logdatei lokal auf dem Rechner generiert werden, in dem nachgesehen werden kann, an welcher Stelle ein Fehler vorliegt.

War der Test erfolgreich, werden die Software Restriction Policies exportiert und zusammen mit dem Logskript auf alle Standard-PC´s der PVS verteilt. Dafür wird die Software ZENworks von Micro Focus genutzt. Die Verteilung auf alle PC´s erfolgt nach der abgeschlossenen Testphase.

3.4 Projektterminplan

Aufgabe/Tätigkeit	Datum
Dokumentationsbeginn	23.10.2017
Ist-/Soll-Analyse	23.10.2017
Projektplanung	24.10.2017
Installation der Testumgebung	24.10.2017
Konfiguration der Software Restriction Policies	24.10.2017
Testphase	25.10.2017
Erstellung des Skriptes für die Logdatei	25.10.2017
Fortsetzung der Dokumentation	25.10.2017
Anpassungen der Software Restriction Policies	26.10.2017
Zweite Testphase	26.10.2017
Exportieren der Software Restriction Policies	27.10.2017
Übergabe des Projekts	27.10.2017

Übernahme in die Produktivumgebung	02.11.2017
Abschluss der Dokumentation	02.11.2017

4. Projektdurchführung

4.1 Umsetzung

Im ersten Schritt muss auf dem Testrechner Windows 7 Professionell installiert werden. Ich wähle dieselbe Vorgehensweise wie bei jedem Standard-PC der PVS, weil so gesichert ist, dass die gleichen Voraussetzungen gegeben sind und die spätere Integration erfolgreich verläuft.

Dafür rufe ich zunächst das Bootmenü über die Funktionstaste F12 auf und nehme die nachfolgenden Einstellungen vor. Im Bootmenü wird die Netzwerkkarte als Bootmedium ausgewählt, um im nächsten Schritt den firmeneigenen PXE-Boot-Server mittels DHCP zu kontaktieren. So gelange ich schließlich in den ZENworks-Bootmanager. Dort wird das zu dem verwendeten PC passende Image ausgewählt, welches sich anschließend eigenständig über das Netzwerk installiert.

Nach der Installation gebe ich den PC-Namen ein und starte den PC neu. Bei der Installation wurde automatisch ein Konto mit Administratorrechten erstellt. Dieses Profil wird später dazu benutzt, um die Richtlinien erstellen zu können. Ist der Neustart vollendet und eine Anmeldung als Administrator erfolgt, werden alle Programme, die nicht bereits im Image integriert sind, durch ZENworks hinzugefügt, nachdem der PC über das Webinterface der Verwaltungssoftware aufgenommen wurde.

Anschließend öffne ich das Ausführen-Fenster mit der Tastenkombination:

$$Windowstaste + R$$

In diesem Fenster wird der Befehl *secpol.msc* eingegeben, um die lokalen Sicherheitsrichtlinien zu öffnen (siehe 6.2, Abbildung 1).

Über das Kontextmenü in der linken Spalte gelange ich an die Einstellungsmöglichkeiten der lokalen Sicherheitsrichtlinien.
Diese stelle ich wie folgt ein:

- Rechtsklick auf *Richtlinien für Softwareeinschränkungen*: Auswahl *neue Richtlinien für Softwareeinschränkungen erstellen*
- Untermenü *Sicherheitsstufen*: Auswahl *Nicht erlaubt*
  Diese Einstellung definiert, welche Sicherheitsstufe als Standard gilt (siehe 6.2, Abbildung 3 und 4).

Dieser erste Schritt sorgt dafür, dass alle Dateitypen, die unter *Richtlinien für Softwareeinschränkungen* | *Designierte Dateitypen* zu finden sind, nicht mehr vom Benutzer ausführbar sind (siehe 6.2, Abbildung 5). Dieser Schritt ist notwendig, um eine Whitelist zu erstellen.

Zu der Windows-Standardliste wurden von mir folgende Endungen hinzugefügt:

.class, .js, .jse,.vbs, .vbe, .wsf, .wsh, .docm, .dotm, .xlm, .xlsm, .pptm, .potm, .pptm, .sldm, .ws, .ps1

Anschließend wird der Objekttyp *Erzwingen* konfiguriert. Dazu nehme ich folgende Einstellungen vor:

- Bei *Richtlinien für Softwareeinschränkungen anwenden auf:* Option *Alle Softwaredateien* auswählen
- Bei *Richtlinien für Softwareeinschränkungen auf folgende Benutzer anwenden:* Haken setzen in *Alle Benutzer außer den lokalen Administrator*.
- Bei der Einstellung *Beim Anwenden von Richtlinien für Softwareeinschränkungen*: *Zertifikatregeln ignorieren* auswählen angegeben.

Anschließend müssen die Änderungen mit einem Klick auf OK bestätigt werden (siehe 6.2, Abbildung 6).

Beim Objekttyp *Designierte Dateitypen* wird bestimmt, auf welchem Dateityp die Regelung angewendet wird. Unter dem Menüpunkt *Zusätzliche Regeln* kann ich nun genau festlegen, welche Programme, Pfade oder Dateien erlaubt oder blockiert werden. Hier lassen sich vier verschiedene Regeltypen anlegen.

Der erste Regeltyp ist die Pfadregel. Sie bestimmt, welche Pfade erlaubt oder blockiert werden. Eine andere Funktion übernimmt die Hashregel. Sie bestimmt mit Hilfe des kryptografischen Fingerabdrucks, ob eine Datei ausgeführt wird oder nicht.
Die Zertifikatsregel verwendet das digital signierte Zertifikat eines Softwareherausgebers. Die letzte der vier Regeln ist die Netzwerkzonenregel. Da sie allerdings nur für den Internet Explorer gültig ist und nicht für andere Webbrowser, die in der PVS eingesetzt werden, wird sie nicht genutzt (siehe 6.2, Abbildung 7).

Für mein Projekt füge ich als Erstes die Pfade %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%, %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir% und %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir (x86)% als Pfadregel hinzu (siehe 6.2, Abbildungen 8, 9 und 10). Damit wird garantiert, dass alle wichtigen Windowsprozesse ohne Probleme funktionieren. Keinem Benutzer, mit Ausnahme des Administrators, ist es möglich, eigene Dateien in diese Ordner hineinzukopieren, weil die Ordner schreibgeschützt sind.

Danach aktiviere ich die Logfunktion der Softwarerichtlinien mittels des folgenden Befehls:

reg.exe add "HKEY_LOCAL_MACHINE|SOFTWARE|Policies|Microsoft|Windows|Safer|CodeIdentifiers" /v LogFileName /d c:|logs|srplog.txt

Zur vereinfachten Handhabung habe ich den Befehl in einer Batch-Datei abgespeichert. Die Aktivierung bietet die Möglichkeit, nachvollziehen zu können, wo es noch zu Problemen mit den gesetzten Richtlinien kommt.

Ursprünglich war vorgesehen, dass ich die Logdateien von allen Benutzern auf einem Netzlaufwerk ablege. Da beim Erstellen der Logdateien, wie im angeführten Beispiel sichtbar wird, jedoch miterfasst wird, wer der Benutzer des Computers ist und es deshalb datenschutzrechtliche Bedenken gibt, habe ich davon abgesehen. Stattdessen speichere ich die Logdateien lediglich lokal auf dem betroffenen PC (siehe 6.2, Abbildung 12).

Anbei ein Beispiel, aus dem das Problem ersichtlich wird:

*explorer.exe (PID = 4896) identified C:|Users|**fkollenberg**|Desktop|PVS2000|ZENTRALE-NEU.LNK as Disallowed using path rule, Guid = {8f2befb9-7e75-4ff7-bc11-0f9f27bbd1c9}*
*explorer.exe (PID = 4896) identified C:|Users|**fkollenberg**|Desktop|PVS2000|ZENTRALE.LNK as Disallowed using path rule, Guid = {8f2befb9-7e75-4ff7-bc11-0f9f27bbd1c9}*

Nach Beendigung der Logphase muss der Eintrag in der Registry wieder gelöscht werden, um die Logfunktion zu deaktivieren. Das geschieht mit folgendem Befehl, der in einer zweiten Batchdatei abgespeichert wird:

reg.exe delete "HKEY_LOCAL_MACHINE|SOFTWARE|Policies|Microsoft|Windows|Safer|CodeIdentifiers" /v LogFileName /f

Darüber hinaus habe ich festgestellt, dass erst dann eine Logdatei in C:\logs geschrieben wird, wenn der Ordner tatsächlich existiert. Deshalb muss die erste Batchdatei um folgenden Befehl ergänzt werden, der zunächst den genannten Ordner anlegt:

if not exist C:|logs (md C:|logs)
reg.exe add "HKEY_LOCAL_MACHINE|SOFTWARE|Policies|Microsoft|Windows|Safer|CodeIdentifiers" /v LogFileName /d c:|logs|srplog.txt

Danach gebe ich noch den Pfad *Q:|data|PVS* mit einer weiteren Pfadregel frei, da hier PVS interne Programme liegen. Auch die Ordner *C:|orawin95* und *C:|produkt* werden per Pfadregel als nicht eingeschränkt definiert. Das ist notwendig, um die Funktionalität der Oracle-Masken, hinter denen sich weitere Programme befinden, die die Mitarbeiter für ihre Arbeit benötigen, zu gewährleisten.

Alle auf dem Desktop befindlichen PVS Standardverknüpfungen werden von mir ebenfalls einzeln per Pfadregel freigegeben. So zum Beispiel:

C:|%USERNAME%|Desktop|Mozilla Firefox.lnk

Aufgrund dieser Einstellung ist es nicht möglich, unerwünschte Programme, unter anderem auch portable Anwendungen, zu starten. Dies ist auch nicht möglich, wenn der Benutzer Verknüpfungen in eine von der IT freigegebene Verknüpfung umbenennt, da hierfür die Zieldatei auch freigegeben werden oder sich in einem freigegebenen Ordner befinden muss. Die freigegebenen Ordner sind so eingestellt, dass nur der Administrator Dateien ändern oder verschieben kann.

Da alle Richtlinien definiert und beim Testen alles reibungslos funktioniert hat, öffne ich den Webbrowser Mozilla Firefox und stelle eine Verbindung mit der umfangreichen Verteilungs- und Verwaltungssoftware ZENworks her, die nur lokal im Firmennetz erreichbar ist, um meine Richtlinien zu verteilen. In ZENworks können eine ganze Reihe von Einstellungen, Richtlinien und Installationen hochgeladen und auf Computern, die sich im entsprechenden Netzwerk befinden, verteilt werden.

Nach dem Login, in dem die Anmeldung über persönliche Zugangsdaten erfolgt, wähle ich in der linken Spalte den Reiter *Richtlinien* aus. Auf der geladenen Seite klicke ich auf *Neu* und anschließend auf *Neue Richtlinien erstellen*. Als Betriebssystem wird Windows ausgewählt. Dies und auch die nächsten Schritte werden mit drücken des *Weiter*-Buttons bestätigt.

Im nächsten Schritt wird *Windows-Konfigurationsrichtlinien* angeklickt, dann wähle ich *Windows-Gruppenrichtlinien* aus. Im Anschluss daran wird der Name *Projekt Richtlinien für Softwareeinschränkungen* für die Richtlinien vergeben. Im letzten Schritt wird bei *Typ der zu verwaltenden Gruppenrichtlinie* die Option *Lokale Gruppenrichtlinie eingestellt.* Bei *Wählen Sie die Konfigurationseinstellung aus, die auf das verwaltete Gerät angewendet werden soll* wird *Computerkonfiguration* sowie *Nur Sicherheitseinstellungen anwenden* ausgewählt.

Nach dem Bestätigen wird die neu erstelle Richtlinie im Menü *Richtlinien* angezeigt. Zum Verteilen auf alle Standardrechner der PVS wird auf die von mir erstellte Richtlinie geklickt, dort wird der Reiter *Beziehungen* gewählt. Anschließend klicke ich auf *Hinzufügen* und wähle alle Arbeitsstationen aus. Nach dem Bestätigen werden die

Richtlinien auf allen Standardrechnern ausgerollt. Hierbei kann ausgewählt werden, ob die Richtlinien sofort, zu einer bestimmten Uhrzeit oder periodisch verteilt werden.

4.2 Tests

Zum Testen wurden von mir fünf Mitarbeiter ausgewählt:

- Ein Mitarbeiter/-in aus der IT
- Ein Mitarbeiter/-in aus der Kundenbuchhaltung
- Ein Mitarbeiter/-in aus dem Service-Center
- Ein Mitarbeiter/-in aus dem Forderungsmanagement
- Ein Mitarbeiter/-in aus der Rechtsabteilung.

Allen Mitarbeiter/-innen wurden die Richtlinien per ZENworks auf ihrem Computer installiert. Die Mitarbeiter/-innen sind von mir so ausgewählt worden, dass möglichst alle Programme, die in den verschiedenen Abteilungen in der PVS genutzt werden, getestet werden können. Damit es auch nach der Testphase zu keinerlei Problemen bei der Übernahme meiner Richtlinien auf allen Computern kommt, habe ich im Anschluss die fünf freiwilligen Mitarbeiter/-innen befragt, wie ihre Systeme funktioniert haben und ob ihnen beim Testen unerwünschte Einschränkungen aufgefallen sind.

4.3 Resultate der Tests

Die Mitarbeiter/-innen haben während der Testphase normal gearbeitet, sie haben ihre Aufgaben wie sonst auch ohne Einschränkungen erfüllen können. Allen Mitarbeiter/-innen wurde im Vorfeld mitgeteilt, dass sie bestehende Verknüpfungen nicht ändern oder in Ordner verschieben dürfen, da die Funktion des Programmes aufgrund der eingestellten Richtlinie sonst nicht mehr gegeben ist. Sollte die Verknüpfung geändert oder verschoben werden, ändert sich der Pfad, welcher dann nicht mehr auf der Whitelist freigeben ist. Somit wird das Programm nicht ausgeführt.

Ausschließlich bei einem Mitarbeiter musste nachträglich eine Desktop-Verknüpfung freigeben werden, weil dieser mit einer Sondersoftware arbeitet, die ich nicht beachtet habe. Diese Pfadfreigabe wurde in den Richtlinien für Softwareeinschränkungen hinzugefügt und wird später mit allen anderen Richtlinien an alle Mitarbeiter verteilt. Die Testphase war somit erfolgreich.

Weil die Richtlinien später auf allen Rechnern gleichzeitig und nicht nach und nach verteilt werden sollen, wurden die zugewiesenen Richtlinien für Softwareeinschränkungen auf den Computern der freiwilligen Teilnehmer nach dem Test wieder gelöscht.

5. Abschluss des Projektes

5.1 Übergabe

Das abgeschlossene Projekt wurde an den Leiter der IT, Herrn Müller und dem Administrator Herrn Braun übergeben (siehe 6.2, Abbildung 11). Zusammen mit Herrn Braun werden die Richtlinien für Softwareeinschränkungen zu einem später festgelegten Termin über ZENworks in die Produktivumgebung eingespielt, da zurzeit zeitliche Engpässe in der IT-Abteilung bestehen.

5.2 Fazit

Die Testphase wurde erfolgreich abgeschlossen und das Projekt von allen beteiligten Personen als Erfolg angesehen, auch wenn es noch nicht in der Firma realisiert worden ist. Ich konnte das Projekt in der dafür vorgesehenen Zeit und ohne nennenswerte Rückschläge oder unvorhersehbare Ergebnisse durchführen.

Die Testphase hat gezeigt, dass Software Restriction Policies einen großen Zugewinn an Sicherheit bringen können, wenn sie sorgfältig eingerichtet und auf allen PC´s der Firma integriert werden.

Auch wenn der grundsätzliche Umgang mit Software Restriction Policies, ein gewisses Grundverständnis über die Funktionsweise vorausgesetzt, relativ leicht einstellbar ist, muss mit ihnen sehr behutsam umgegangen werden. Die kleinste Unachtsamkeit oder jeder Tippfehler können verheerende Folgen hinsichtlich möglicher Einschränkungen nach sich ziehen und einen PC mit wenigen Klicks unbrauchbar machen. Daher ist es wichtig, konzentriert zu arbeiten und im Zweifel zur Sicherheit einen anderen Mitarbeiter (Vier-Augen-Prinzip) aus der IT die Einstellungen kontrollieren zu lassen.

5.3 Quellen

Bei der Umsetzung des Projektes wurden Informationen aus folgenden Internetquellen verwendet:

https://www.novell.com/documentation/zenworks-2017-update-1/zen_cm_policies/data/bau5n2g.html

https://msdn.microsoft.com/de-de/library/hh831534(v=ws.11).aspx

https://technet.microsoft.com/de-de/library/cc731745(v=ws.11).aspx

https://technet.microsoft.com/de-de/library/dn452420(v=ws.11).aspx

https://msdn.microsoft.com/de-de/library/jj966254(v=ws.11).aspx

https://msdn.microsoft.com/de-de/library/hh994597(v=ws.11).aspx

https://www.nt4admins.de/nc/news/newsdetails/article/anwenden-von-srp-regeln- fuer-applikationen.html?tx_felogin_pi1%5Bforgot%5D=1&tx_ttnews%5BbackPid%5D=107

6. Anhang

6.1 Glossar

Batch-Datei	Auch .bat genannt. Stapelverarbeitungsdatei, die von Windows ausgeführt wird.
Blacklist	Liste mit gesperrten Anwendungen, auch Sperrliste genannt.
Bootmanager	Ermöglicht die Auswahl mehrerer Betriebssysteme.
CLASS	Auch Java Class File genannt. Ist eine Developerdatei, die von Oracle erfunden wurde.
DHCP	Dynamic Host Configuration Protocol Kommunikationsprotokoll, welches Netzwerkkonfigurationen an Clients verteilt.
DOCM	Word-Datei mit eingebetteten Makros.
DOTM	Word-Datei-Vorlage, die Einstellungen und Makros beinhalten kann.
Executables	Auch .exe genannt Ausführbare Dateien in Windows.
Hashregel	Prüft anhand der Prüfsumme, ob die Datei ausgeführt werden darf.
Image-Installation	Installation eines Betriebssystems mit voreingestellten Einstellungen und Treibern.
JS	JavaScript File ist eine Datei die Javascript beinhalten. Javascript ist eine Skriptsprache
JSE	Eine Verschlüsselte Javascript - Datei
Kryptografischer Fingerabdruck	Geheime Prüfsumme.
Oracle-Masken	Programme, die die Mitarbeiter für ihre tägliche Arbeit benötigen.
Portable-Format	Programm, welches ohne Installation ausgeführt werden kann.
POTM	PowerPoint-Datei-Vorlage, die Einstellungen und Makros beinhalten kann.
PPSM	PowerPoint-Datei, die eine Makro-fähige Diashows enthält.
PPTM	PowerPoint-Datei, die eine Makro-fähige Präsentation enthält.
PS1	Endung von PowerShell-Dateien. PowerShell ist eine Scriptsprache.
PXE	Preboot Execution Environment. Eine Erweiterung des Bootens über Rechnernetze mittels DHCP
Skript	Führt automatisch Aktionen aus.
SLDM	PowerPoint-Datei, die Makros enthalten kann.
Software Restriction Policies	Definiert, welche Software/Dateien ausgeführt oder gesperrt werden.

Surf Protection	Webproxy vom Sophos. Ein Webproxy unterbindet das aufrufen von ungewünschten Webseiten.
VBE	VBScript Encoded Script File, ist eine Verschlüsselte Visual Basic Script Datei.
VBS	Visual Basic Script ist eine von Microsoft entwickelte Skriptsprache.
Webbrowser	z.B. Mozilla Firefox oder Google Chrome
Whitelist	Eine Liste mit vertrauenswürdigen Anwendungen, auch Ausnahmeliste genannt.
WS	Microsoft Windows Script Format ist eine Skriptdatei.
WSF	Microsoft Windows Script Format ist eine Skriptdatei.
WSH	Windows Script File sind Dateien, die von VBScript ausgeführt werden.
XLM	Eine Microsoft-Excel-Datei, die ein Marko enthält.
XLSM	Eine Microsoft-Excel-Datei, die ein Marko enthält.
ZENworks	Software Verwaltungstool, der Firma Micro Focus.

6.2 Screenshots

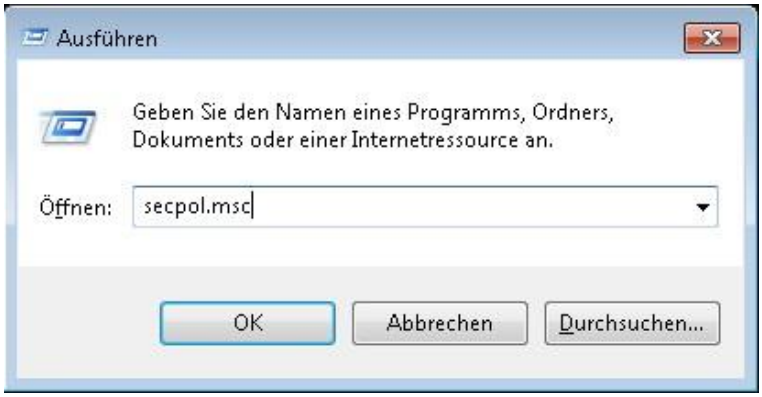


Abbildung 1 - Lokale Sicherheitsrichtlinien öffnen

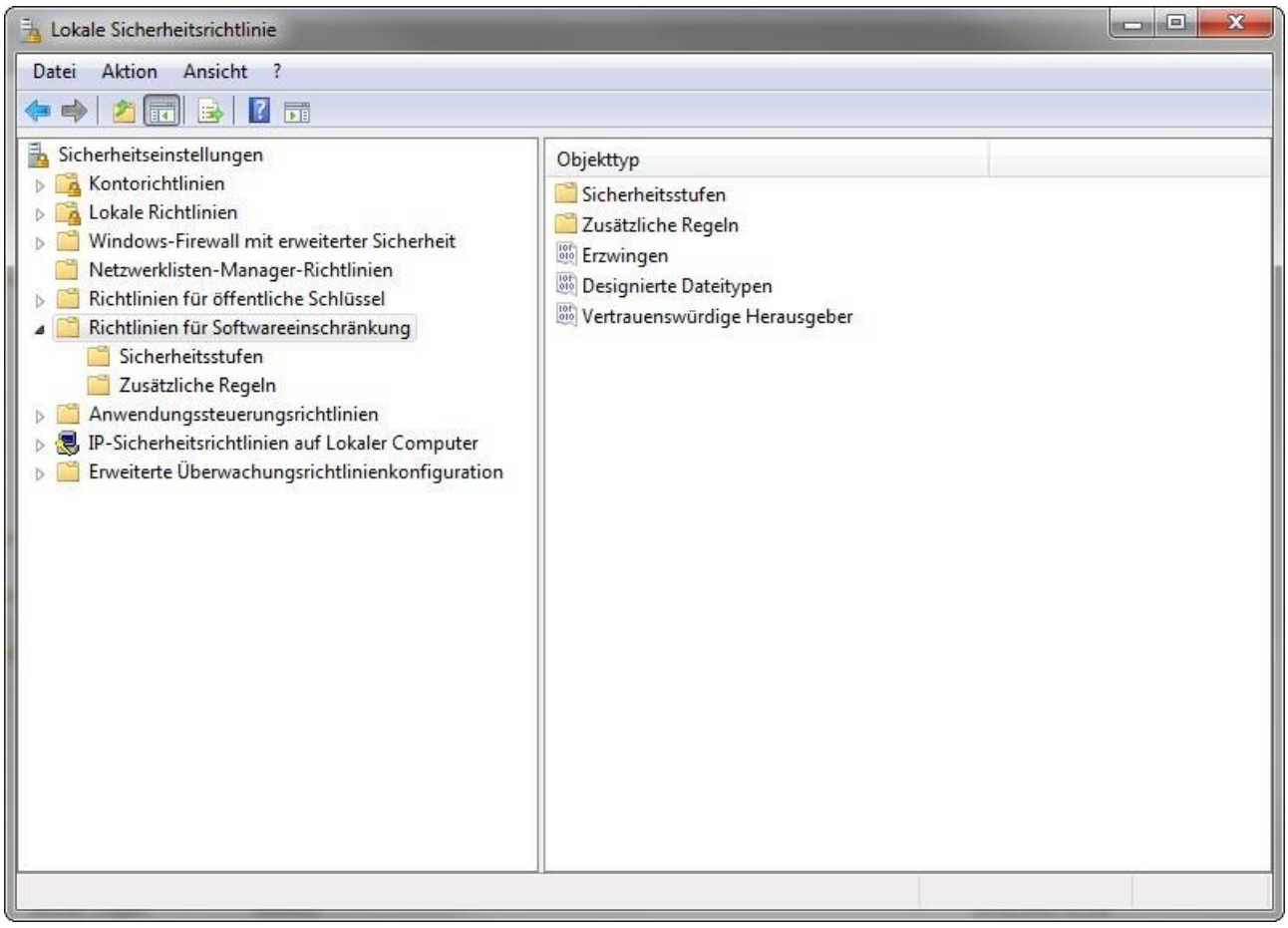


Abbildung 2 - Übersichtsfenster Software Restriction Policies

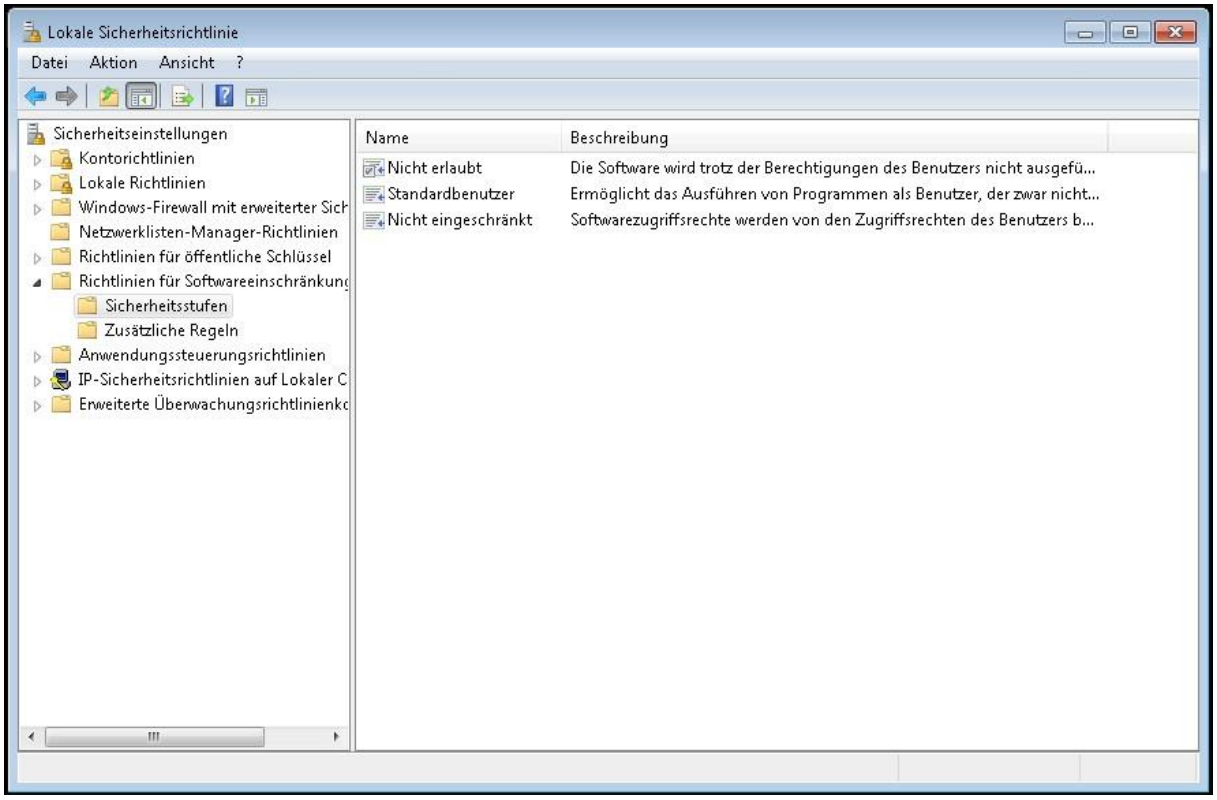


Abbildung 3 - Übersicht der Sicherheitsstufen

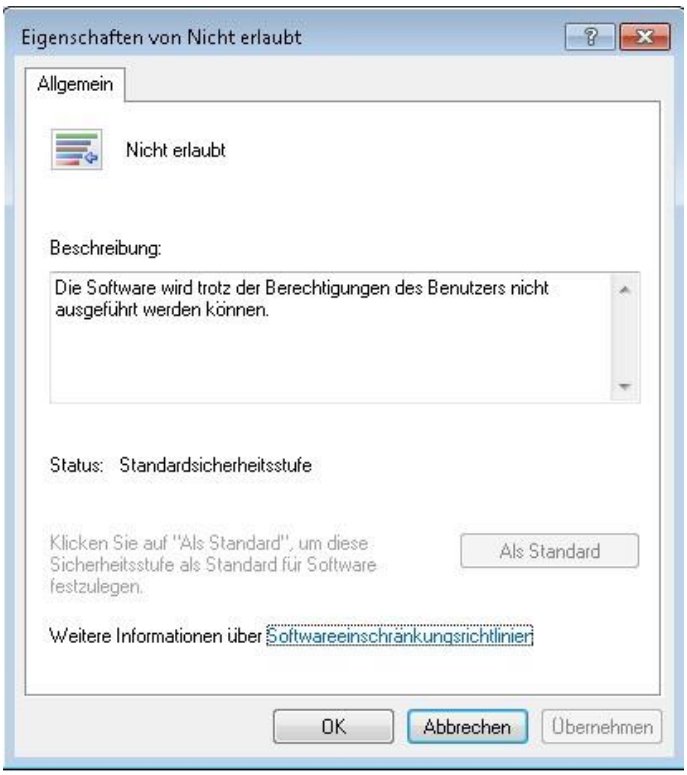


Abbildung 4 - *Nicht erlaubt* als Standard setzen

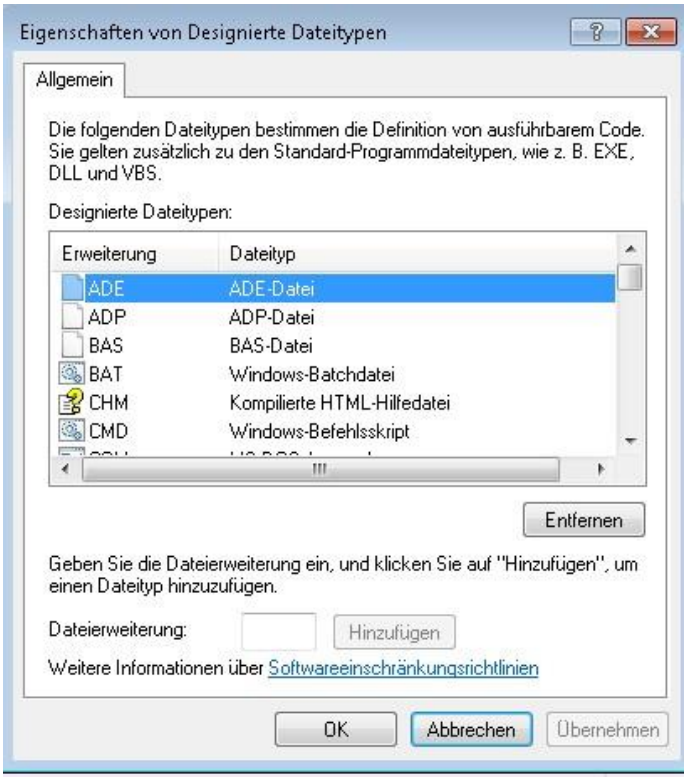


Abbildung 5 - Auswahl der designierten Dateitypen

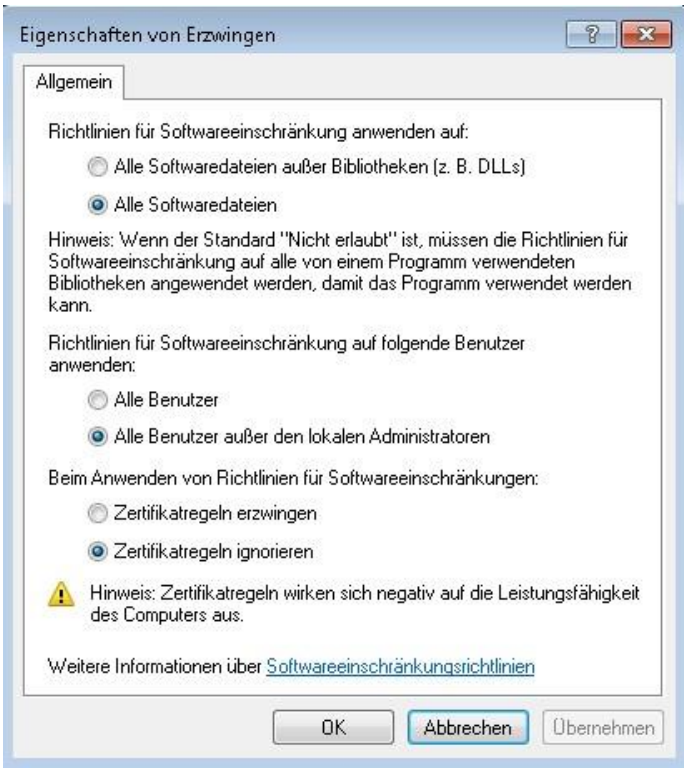


Abbildung 6 - *Eigenschaften von Erzwingen* definieren

Abbildung 7 - Neue Regeln hinzufügen

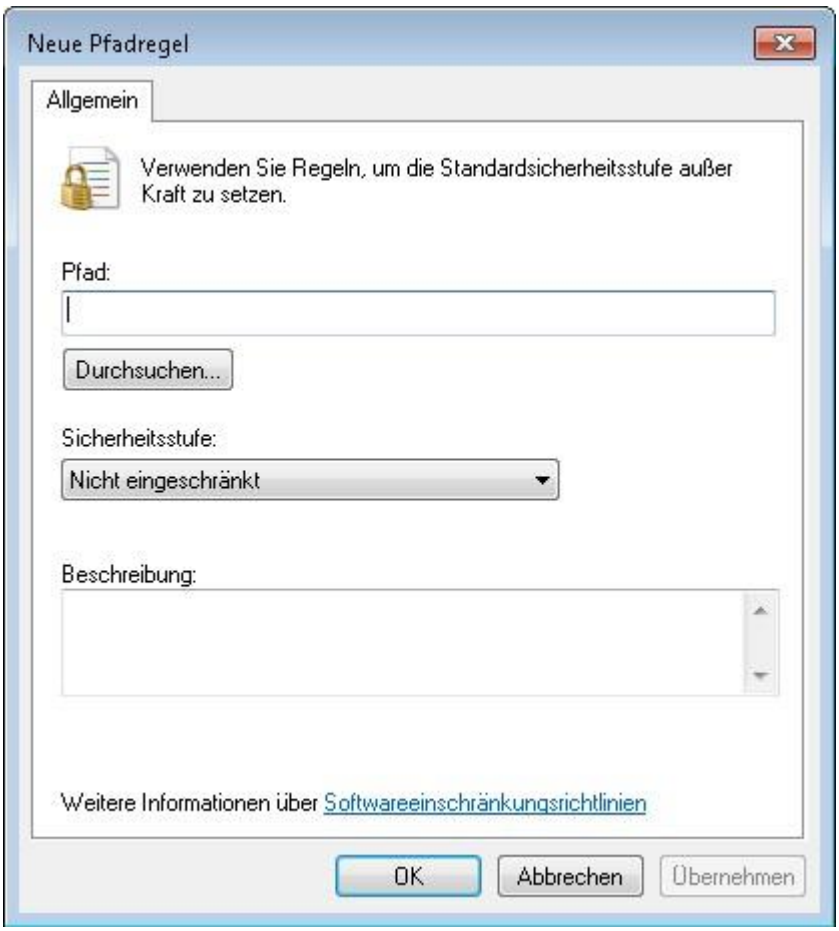


Abbildung 8 - Pfadregel definieren

Abbildung 9 - Pfad der betroffenen Datei auswählen

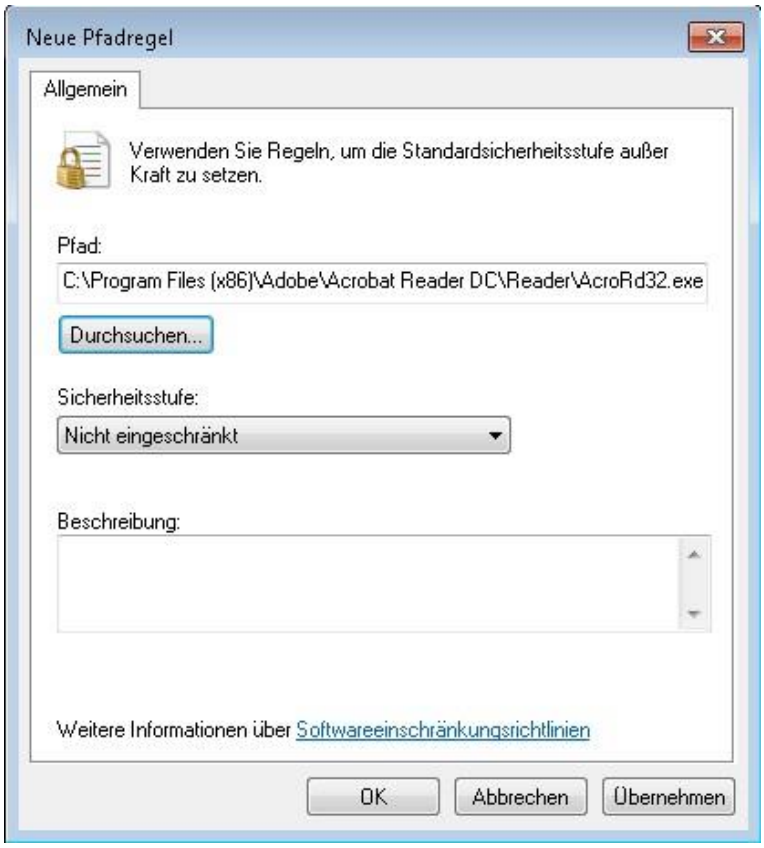


Abbildung 10 - Neue Regel erstellen

Name	Typ	Sicherheitsstufe
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Pfad	Nicht eingeschränkt
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Pfad	Nicht eingeschränkt
C:\orawin95	Pfad	Nicht eingeschränkt
C:\produkt	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\Buc-Produktion\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\Buc-Produktion\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\Buc-Produktion\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\Buc-Produktion\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\Dateiliste_erstellen.lnk	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\Mozilla Firefox.lnk	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000[redacted].lnk	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000[redacted]-NEU.lnk	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\PVS2000\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\SnippingTool.exe - Verknüpfung.lnk	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\TV-Meeting.exe	Pfad	Nicht eingeschränkt
C:\Users\%USERNAME%\Desktop\[redacted]	Pfad	Nicht eingeschränkt
C:\Users\Public\Desktop\Acrobat Reader DC.lnk	Pfad	Nicht eingeschränkt
C:\Users\Public\Desktop\GroupWise.lnk	Pfad	Nicht eingeschränkt
C:\Users\Public\Desktop\Mozilla Firefox.lnk	Pfad	Nicht eingeschränkt
C:\Users\Public\Desktop\Swyxit!.lnk	Pfad	Nicht eingeschränkt
C:\Users\Public\Desktop\[redacted]	Pfad	Nicht eingeschränkt

Abbildung 11 - Auszug der Softwareregeln

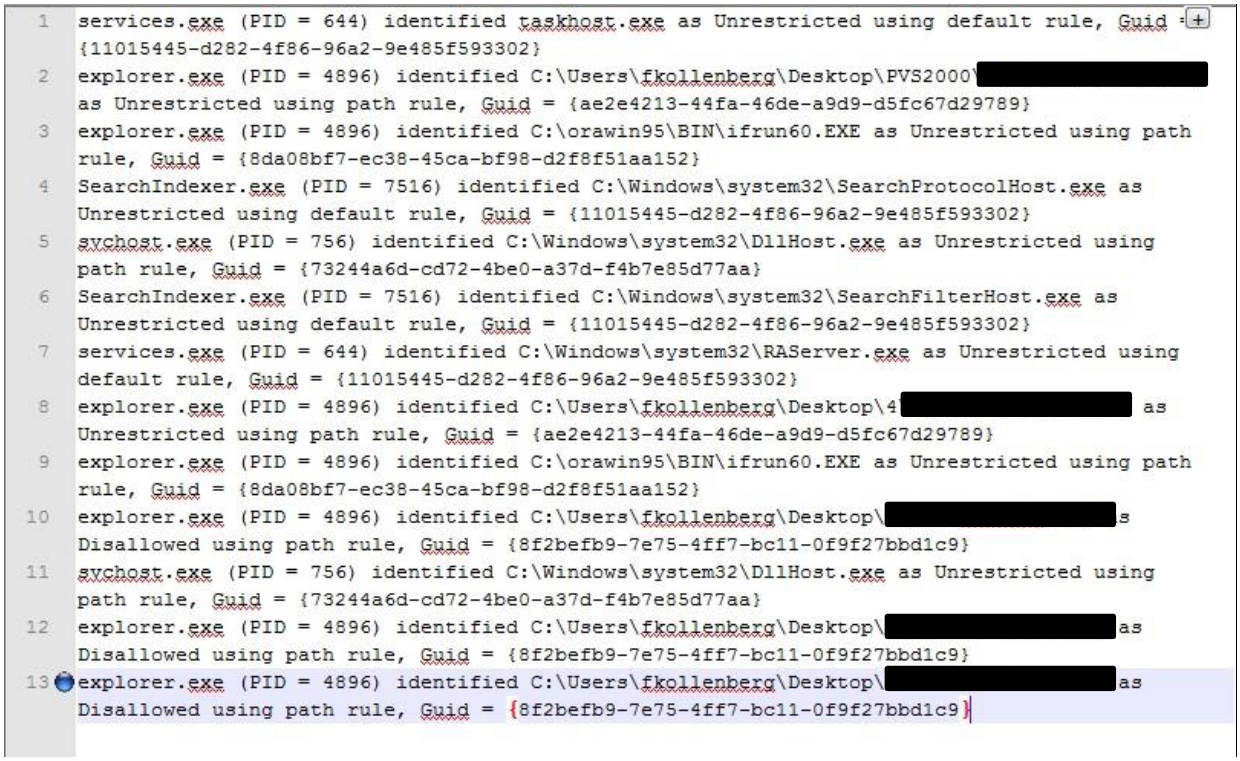


Abbildung 12 - Auszug der Logdatei