IHK Industrie- und Handelskammer Halle-Dessau

Abschlussprüfung IT-Berufe
Betriebliche Projektarbeit

Projektdokumentation

Name, Vorname: Höbald, Alexander

(IHK-)Identnummer: [redacted] [redacted] (siehe Anmeldung / Einladung / Portal)

Ausbildungsberuf: Fachinformatiker

ggf. Fachrichtung: Systemintegration

Projektbezeichnung: (Wortlaut wie im genehmigten Antrag)

Einrichtung von Software Restriction Policies für Active-Directory-Gruppenrichtlinienobjekte

Genehmigungsdatum: 15.02.2024 (Ende-Datum der Genehmigungsphase)

Bearbeitungszeitraum: vom 19.03.2024 bis 02.05.2024

Eidesstattliche Erklärung

Ich versichere durch meine Unterschrift, dass ich die betriebliche Projektarbeit und die dazugehörige Dokumentation selbständig angefertigt und den in der Verordnung zum Ausbildungsberuf vorgegebenen Zeitrahmen eingehalten habe.

[redacted], 12.05.2024

Ort, Datum

[redacted]

Unterschrift des Prüfungsteilnehmers

Um die Lesbarkeit des Antragsformulars zu vereinfachen, wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen sind explizit als geschlechtsunabhängig zu verstehen.

Inhaltsverzeichnis

1. Projektdefinition

1.1. Vorstellung

Die Abena GmbH Heideloh, fortlaufend Abena genannt, ist eine Tochtergesellschaft der dänischen ABENA A/S und in Deutschland als Großhandel für pharmazeutische Erzeugnisse, hauptsächlich Inkontinenzprodukte, sowie andere Hygiene- und Einwegartikel tätig. Ihren Umsatz erarbeitet Abena hauptsächlich durch Lieferaufträge an und Ausschreibungen von Alten- und Pflegeheimen, Krankenhäusern und Kliniken, als auch durch Erfüllung von Kassenrezepten von Patienten in solchen Einrichtungen oder von Privatkunden.

ABENA wurde in Dänemark im Jahr 1953 gegründet und befindet sich seitdem im Familienbesitz. Auch der deutsche Standort hat 2021 bereits sein 30-jähriges Jubiläum gefeiert.

Das Team umfasst derzeit etwa 200 Mitarbeiterinnen und Mitarbeiter an den Standorten in Zörbig (Sachsen-Anhalt) und Glinde (Schleswig-Holstein) in unterschiedlichen Bereichen. Global beschäftigt ABENA A/S in über 90 Märkten ca. 2000 Mitarbeiter in 20 unterschiedlichen Tochtergesellschaften.

Die eigene IT-Abteilung von Abena teilt sich in drei Mitarbeiter und einen Auszubildenden auf, die hauptsächlich in den Bereichen Administration und Support arbeiten. Weiterhin hat ABENA eine Tochtergesellschaft in Dänemark, ABENA Data ApS, welche für Standorte weltweit Support bietet und in IT-Bereichen global die Richtung weist.

Mitarbeiter von ABENA Data ApS haben auch Unterstützung bei der Durchführung des Projekts geboten.

1.2. Projektumfeld

Das Projektumfeld besteht aus dem Microsoft Active Directory auf einer virtuellen Serverumgebung, einem PC-Arbeitsplatz und voll ausgestatteten Packtisch – Arbeitsplätzen im Lager mit Label-Druckern, A4-Druckern und Handscannern. Alle Arbeitsplätze verwenden das Betriebssystem Windows 10.

Auftraggeber des Projektes für die Abschlussprüfung ist [redacted], Geschäftsführer der Abena GmbH. Das Projekt soll nach Fertigstellung an allen Packtisch-Arbeitsplätzen am Standort eingesetzt werden. Gewonnene Erfahrungen werden für mögliche ähnliche Projekte an Teilgesellschaften der ABENA A/S verwendet.

An der Informationsbeschaffung und der Planung des Projektes sind beteiligt:

- [redacted] (Systemadministrator / IT Helpdesk)
- [redacted] (Qualitätssicherung und Management Warehouse)
- [redacted] (Systemadministrator, ABENA Data ApS)
- [redacted] (Global IT Operations Manager)

1.3. Das Projekt

Im Projekt „Einrichtung von Software Restriction Policies für Active-Directory-Gruppenrichtlinienobjekte“ soll erreicht werden, dass an allen Arbeitsplätzen im Lager, an denen mit Shared User Accounts gearbeitet wird, nur noch Programme und Dateien ausgeführt werden können die spezifisch für die Arbeitsaufgaben an diesen nötig sind.

1.4. Projektziele

Abena arbeitet mit sensiblen Patientendaten, daher ist Datensicherheit von hoher Wichtigkeit. Unerlaubte Zugriffe müssen zwingend so weit wie möglich eingeschränkt werden. Sicherheit wird zwar durch bestehende Systeme, wie einer Firewall, bereits geboten, aber die Verwendung von Shared User Accounts an bestimmten Systemen benötigt weitere Maßnahmen, um unerlaubte Zugriffe einzuschränken.

Höhere Sicherheit soll im Arbeitsalltag an diesen Systemen erlangt werden, ohne die gewohnten Arbeitsprozesse der betroffenen Mitarbeiter einzuschränken.

Das soll mit Einrichtung von Software Restriction Policies für Active-Directory-Gruppenrichtlinienobjekte erreicht werden.

1.5. Ansprechpartner / Schnittstellen

Der Auftraggeber des Projekts ist [redacted]. Bei Fragen zu Arbeitsprozessen an Packtisch-Arbeitsplätzen bietet [redacted] Unterstützung. Ansprechpartner bei technischen Fragen sind [redacted], [redacted] und [redacted]. Für die Abnahme des Projektes und der Dokumentation sind [redacted] und [redacted] zuständig.

1.6. Kostenbetrachtung

Die Aufstellung einer Nutzen-Kosten-Analyse ist für dieses Projekt nicht in klassischer Form möglich, da der Nutzen kein direkt wirtschaftlicher ist. Die Zielsetzung des Projekts ist eine erhöhte IT-Sicherheit durch die Einführung von Richtlinien zur Softwareeinschränkung als Präventivmaßnahme. Der Nutzen besteht darin etwaige wirtschaftliche Schäden durch Angriffe und Schadsoftware einzuschränken.

In einem Szenario, an dem ein einzelner Packstrecken-Arbeitsplatz von Schadsoftware betroffen ist, muss dieser mit neuer Technik bestückt werden, die betroffenen Geräte müssen sichergestellt und neu aufgesetzt werden und der Vorfall muss aufgeklärt und dokumentiert werden. Man kann hier mit einem Zeitaufwand von insgesamt 4 Stunden für den bearbeitenden Systemadministrator rechnen, mit Kosten von [redacted] pro Stunde, zusätzlich zu dem Verdienstausfall des betroffenen Lagermitarbeiters von circa einer Stunde mit Kosten von [redacted] (Personalkosten [redacted], Material- / Energiekosten [redacted]).

Der Zeit- und Kostenaufwand ausgelöst durch eine Infektion mit Schadsoftware steigt exponentiell mit der Anzahl an betroffenen Systemen. Die Infektion und Ausfall einer,

mehrerer oder aller Packstrecken-Arbeitsplätze führt zu Lieferverzug, Versäumnis von Aufträgen und Verlust von Kundenvertrauen und -Zufriedenheit. In solchen Fällen kann auch das gesamte Firmennetzwerk von einer Infektion betroffen sein. Auch wird nicht nur das Tagesgeschäft verhindert und eingeschränkt, Cyberangriffe bringen in der Regel auch ein datenschutzrechtliches Fiasko mit sich.
Die kurzfristigen sowie langfristigen wirtschaftlichen Schäden lassen sich nur schwer abschätzen und haben oft eine schwerwiegende Wirkung auf das Unternehmen, weshalb die Umsetzung eines solchen Projektes nur befürwortet werden kann.
Um die Kosten des Projekts zu ermitteln, werden Abena Pauschalsätze verwendet.
(siehe 7.3.1. Tabelle 1 Pauschalsätze, 7.3.2. Tabelle 2 Kostenaufstellung)
Die Materialkosten für den Aufbau des Testarbeitsplatzes belaufen sich auf 550,00 € für den verwendeten Mini-PC, 150,00 € für den Monitor und 30,00 € für Eingabegeräte. Diese Kosten wurden in der Berechnung nicht berücksichtigt, da diese nach Abschluss des Projekts wieder in den Bestand an Technik für Arbeitsplätze aufgenommen werden.

2. Analysephase

2.1. Ist-Analyse

Aktuell werden bei Abena keine Software Restriction Policies verwendet, jeder User kann alle Programme ausführen und Dateien öffnen, die sich auf dem Rechner befinden und auf die er Zugriffsrechte hat. So können auch etwaige heruntergeladene schädliche Dateien ausgeführt werden, die von anderen Sicherheitsvorkehrungen nicht aufgehalten werden konnten. Jegliche Programminstallationen werden bereits auf Administrator-Accounts mit jeweiligen Rechten beschränkt.
Für diese Maßnahme existiert global bei [redacted].
Diese Einschränkungen verhindern jedoch nicht das Ausführen von Executables im Portable-Format, also Programme, die ohne eine Installation über den Windows-Installer funktionsfähig sind und deswegen ohne Kenntnis der IT-Abteilung an Arbeitsplätzen ausgeführt werden können.

Portable Executables, sowie heruntergeladene schädliche Dateien, stellen ein besonders großes Risiko an Arbeitsplätzen dar, an denen Shared User Accounts benutzt werden. Derartige Accounts sind Benutzerkonten, welche nicht einer individuellen natürlichen Person zugeordnet werden können und von unterschiedlichen Mitarbeiten mit den gleichen Zugangsdaten verwendet werden. Bei Abena werden solche Benutzerkonten an Packtisch-Arbeitsplätzen im Bereich Lager und Logistik verwendet und der Zugriff auf sie kann nicht ausreichend genug überwacht oder nachvollzogen werden, um eine zufriedenstellende Datensicherheit zu gewährleisten.

2.2. Soll-Analyse

Das Ziel des Projektes soll die Integration der Richtlinien für Softwareeinschränkung in das Live-System des Lagers sein. Das Ausführen von nicht erlaubter Software und Dateien soll eingeschränkt werden. Wenn eine solche Software oder Datei von einem Benutzer ausgeführt wird, soll dieses blockiert und dem Benutzer anhand einer Fehlermeldung mitgeteilt werden, dass dies nicht zulässig ist (siehe 7.2.1. Abbildung 1, 7.2.2. Abbildung 2). Ist der Benutzer der Ansicht, dass die blockierte Datei oder das Programm für den normalen Arbeitsprozess benötigt wird, kann er oder sein Vorgesetzter sich an einen Helpdesk-Mitarbeiter der IT-Abteilung wenden. Die IT-Abteilung kann den Vorfall überprüfen und gegebenenfalls die Konfiguration der Software Restriction Policies anpassen.

Rücksprache mit Projektbeteiligten und -betreuern hat ergeben, dass die Software Restriction Policies mit einer Whitelist arbeiten wird. In dieser Form der Konfiguration blockiert die SRP das Ausführen aller Dateien und Programme, die nicht in der Whitelist festgelegt und damit erlaubt sind.

Bereits eingesetzte sonstige Schutzmaßnahmen wie Cyber-Sicherheitssoftware soll nicht von Software Restriction Policies betroffen sein, die Sicherheitssysteme sollen unbeeinflusst von neuen Richtlinien arbeiten. Die Zielsetzung soll es sein, mithilfe der Software Restriction Policies eine weitere Schutzmauer gegen Schadprogramme aller Art aufzubauen.

2.3. Alternativenbetrachtung

Im Rahmen von Software Restriction Policies ist eine Alternative die Verwendung einer Blacklist. Im Gegensatz zur verwendeten Whitelist werden in dieser Form der Konfiguration alle bekannten ausführbaren Dateien und Programme blockiert, die in der Blacklist festgelegt sind. An dieser Stelle ist die Verwendung einer Blacklist aber nicht zielführend, da unbekannte Schadsoftware nicht in dieser festgelegt und damit ausführbar ist. Außerdem geht eine Blacklist mit konstanten Wartungsaufwand einher, weil diese immer weiter um neue Einträge ergänzt werden muss.

Eine Alternative zur Verwendung von Software Restriction Policies ist Microsoft AppLocker. AppLocker funktioniert ähnlich wie SRP, zielt aber eher auf Regeln für Benutzer und Benutzergruppen ab. In Rücksprache mit den Projektbeteiligten fiel die Entscheidung zur Verwendung von Software Restriction Policies, da die Richtlinien auf den gesamten Rechner, unabhängig welcher Benutzer angemeldet ist, greifen sollen. Außerdem soll Konflikt mit bereits bestehenden AppLocker Gruppenrichtlinien vermieden werden.

3. Projektplanung

3.1. Phasenplanung

1. Informationen	8 Stunden
▪ Ist-Analyse	2 Stunden
▪ Ermittlung des Anwendungsbestands	4 Stunden
▪ Festlegung des Arbeitsumfangs	2 Stunden
2. Planung	8 Stunden
▪ Aufgaben und Zeitplanung	3 Stunden
▪ Inhaltlicher Entwurf der geplanten Beschränkungen	2 Stunden
▪ Alternativenbetrachtung	1 Stunde
▪ Überprüfung der technischen Umsetzbarkeit	2 Stunden
3. Durchführung	12 Stunden
▪ Aufbau Testarbeitsplatz	1 Stunde
▪ Anlegen einer OU und GPO	2 Stunden
▪ Konfiguration der Gruppenrichtlinien	4 Stunden
▪ Übernahme in Live-Umgebung	5 Stunden
4. Kontrolle	12 Stunden
▪ Test der Funktionalität	4 Stunden
▪ Fehlerüberprüfung / -behebung	2 Stunden
▪ Ausblick auf mögliche Erweiterungen	1 Stunden
▪ Dokumentation	5 Stunden
Gesamt	40 Stunden

3.2. Projektablauf

Vor Beginn des Projektes werden in einer Konferenz mit [redacted] und [redacted] technische Fragen und solche zu nötigen Berechtigungen für Arbeiten an betroffenen Systemen geklärt und die Freigabe zur Durchführung des Projektes eingeholt. Als nächstes findet ein Gespräch mit [redacted] und [redacted] statt um die genauen

Anforderungen an das Projekt festzulegen. Weiterhin wurden Termine mit [redacted] für bestimmte Arbeiten festgelegt, um das Tagesgeschäft im Lager nicht zu stören.

Im ersten Schritt wird mithilfe eines Protokollierungsfeatures von SRP ein Anwendungsbestand auf drei Packstreckenarbeitsplätzen in Form einer lokal gespeicherten Logdatei ermittelt. Im Active Directory (AD) wird eine Organisationseinheit (OU) und eine Sicherheitsgruppe für PCs erstellt, die mit der Software Restriction Policy versorgt werden sollen. Im Group Policy Management wird ein zugehöriges Gruppenrichtlinienobjekt (GPO) erstellt und die Sicherheitsgruppe mit diesem verknüpft. Im Gruppenrichtlinienobjekt werden die Software Restriction Policies anhand geklärter Anforderungen und ermitteltem Anwendungsbestand definiert.

Anschließend wird ein Testarbeitsplatz eingerichtet. Der PC verwendet ein Standard-Image von Abena (Betriebssystem Windows 10) mit Standard-Software wie das Microsoft Office Paket, Google Chrome und Adobe Reader. Zusätzlich muss das im Lager verwendete Warehouse Management System LFS von EPG auf dem PC installiert werden. Zunächst wird die Software Restriction Policy auf diesem Testarbeitsplatz auf grundsätzliche Funktion überprüft. Danach wird die Richtlinie auf zwei ausgewählte Arbeitsplätze im Lager angewendet, um die Funktion im laufenden Betrieb zu testen.

Wenn diese Tests erfolgreich ablaufen, werden alle PCs im Lager in die neue OU verschoben und mit der Sicherheitsgruppe versehen, die auf das GPO der Software Restriction Policies verweist, um die Richtlinie auf diese anzuwenden.

3.3. Terminplanung

Das Projekt beginnt mit dem Start der Dokumentation am 19.03.2024 und endet mit dem Abschluss dieser am 02.05.2024. Für den Besuch der Berufsschule (zwei Wochen) und im Zeitraum der schriftlichen Abschlussprüfung (eine Woche) wird das Projekt pausiert. (siehe 7.3.3. Tabelle 3 Terminplanung)

4. Durchführung

Um Richtlinien für Softwareeinschränkung mit der Sicherheitsstufe *Nicht erlaubt (Disallowed),* also mit einer Zulassungsliste (Whitelist) an erlaubten Programmen und Dateien, effektiv zu nutzen, muss genau bestimmt werden welche Anwendungen für alle Arbeitsprozesse notwendig sind.

SRP verfügt über ein Protokollierungsfeature, mit dem alle ausgeführten Anwendungen auf einem Gerät ermittelt werden können. Um dieses zu verwenden, müssen für die Testumgebung zuallererst lokale Software Restriction Policies mit der Sicherheitsstufe *Uneingeschränkt (Unrestricted)* bereitgestellt werden. Wenn nun keine zusätzlichen Regeln

konfiguriert sind, werden alle ausgeführten Anwendungen von der Richtlinie überwacht. Die Überwachung kann mithilfe einer Logdatei und einem Registrierungswert protokolliert werden. Als erstes wird auf drei ausgewählten PCs im Lager lokal folgender Pfade erstellt:

c:\logs\SRPLog.txt

Um das Protokollierungsfeature für diese Logdatei zu aktivieren, wird folgender Befehl in der Windows-Eingabeaufforderung ausgeführt:

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

Diese Protokollierung findet in Absprache der betroffenen Mitarbeiter und der Leitung des Lagers statt. Nach mehreren Früh- und Spätschichten wird die Protokollierung mit der Entfernung des Registrierungswerts mit folgendem Befehl wieder deaktiviert:

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

Die entstandenen Logdateien müssen nun gefiltert werden. Protokollierte Anwendungen aus bekannten, schreibgeschützten Pfaden, die in der Whitelist der kommenden SRP nach Standard erlaubt sind, werden ausgeblendet. Anhand der gefilterten Logdateien (siehe 7.2.3. Abbildung 3) kann nun ein Bestand an benötigten Anwendungen festgestellt werden. Bevor mithilfe dieses Anwendungsbestands ein Gruppenrichtlinienobjekt (GPO) mit SRP erstellt wird, muss eine Testumgebung für erste rudimentäre Funktionstests aufgebaut werden. Dazu wird ein bereits fertig installierter PC mit Windows 10 Enterprise an einen Monitor und Eingabegeräte an der Installations- und Teststrecke in der IT-Abteilung angeschlossen. Zusätzlich wird auf dem Rechner die Warehouse-Management-System Software LFS von EPG installiert. Diese ist für Arbeitsprozesse im Lager unerlässlich.

Im nächsten Schritt wird im Active Directory (AD) des Unternehmens eine neue Organisationseinheit (OU) erstellt (siehe 7.2.4. Abbildung 4, 7.2.5. Abbildung 5), auf die die geplanten SRP-Gruppenrichtlinien wirken soll (siehe 7.2.6. Abbildung 6). Die OU heißt [redacted].

Nun wird eine neue Sicherheitsgruppe erstellt, diese heißt nach Abena Naming Convention [redacted] (siehe 7.2.7. Abbildung 7, 7.2.8. Abbildung 8). Die Sicherheitsgruppe ist nötig, damit in dem GPO festgelegt werden kann, für welche Benutzer oder Geräte diese gilt.

Für diese OU kann nun ein Gruppenrichtlinienobjekt (GPO) mit Software Restriction Policies angelegt werden. Im Group Policy Management des AD wird in die zuvor angelegte OU navigiert und dort mit *Create a GPO in this domain, and Link it here* (siehe 7.2.9.

Abbildung 9) ein neues GPO mit dem Namen [redacted] erstellt (siehe 7.2.10. Abbildung 10). Dieses wird mit *Enforced – No, Link Enabled – Yes, GPO Status – Enabled* konfiguriert. In dem GPO können Sicherheitsgruppen festgelegt werden, auf die die Richtlinie wirkt. Hier wird unter *Security Filtering* die Sicherheitsgruppe [redacted] hinzugefügt (siehe 7.2.11. Abbildung 11).

Nun kann die Konfiguration der Software Restriction Policy beginnen. Der Group Policy Management Editor wird im Interaktionsmenü (Rechtsklick auf GPO) geöffnet. Dort wird zu Software Restriction Policies navigiert (siehe 7.2.12. Abbildung 12). Als nächstes werden diese wie folgt konfiguriert:

- Auswahl *neue Richtlinien für Softwareeinschränkungen erstellen*
- Im Untermenü *Security Levels – Sicherheitsstufen* (siehe 7.2.13. Abbildung 13) Auswahl *Disallowed – Nicht erlaubt* (siehe 7.2.14. Abbildung 14)

Dieser Schritt ist notwendig, um die SRP mit einer Zulassungsliste (Whitelist) zu betreiben. Im Moment wird das Ausführen aller Anwendungen mit Dateiendungen, die unter *Designated File Types – Designierte Datentypen* (siehe 7.2.15. Abbildung 15) festgelegt und nicht unter *Additional Rules – Zusätzliche Regeln* erlaubt sind.

Zunächst wird die „ *.lnk "* Dateiendung aus der Standardliste entfernt. Die .lnk-Erweiterung stammt von Verknüpfungsdateien und muss erlaubt werden, um eine reibungslose Funktion des Windows-Startmenüs zu ermöglichen. Als nächstes werden folgende Endungen zur Liste hinzugefügt:

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

Enforcement – Erzwingen wird wie folgt konfiguriert (siehe 7.2.16. Abbildung 16):

- Richtlinien für Softwareeinschränkung anwenden auf *Alle Softwaredateien außer Bibliotheken (z.B. DLLs)*
- Richtlinien für Softwareeinschränkung anwenden auf *Alle Benutzer außer den lokalen Administrator*
- Beim Anwenden von Richtlinien für Softwareeinschränkungen *Zertifikatregeln ignorieren*

Jetzt kann unter *Additional Rules – Zusätzliche Regeln* die genaue Zulassungsliste für Programme und Dateien definiert werden. Es gibt vier unterschiedliche Arten von Regeln. Zertifikatregeln erlauben es der SRP Anwendungen anhand ihres Signaturzertifikats zu identifizieren und je nach Konfiguration zu erlauben oder zu blockieren. Bei Hashregeln erstellen die SRP mithilfe eines Hashalgorithmus eine eindeutige Reihe von Bytes mit fester Länge, anhand derer das Programm oder die Datei identifizierbar sind. Wenn ein Benutzer

ein Programm öffnet, vergleicht die Richtlinie den Hash des Programmes mit dem zugehörigen Hash in der Hashregel. Internetzonenregeln gelten ausschließlich für Windows Installer-Pakete aus festgelegten Internetzonen im Internet Explorer, daher ist dieses Feature hier nicht nützlich. Der letzte Regeltyp, Pfadregeln, identifiziert Programme und Dateien anhand ihres Dateipfads. Wenn die Sicherheitsstufe *Nicht erlaubt* konfiguriert ist, kann somit für Benutzer Zugriff auf Programme und Dateien aus aufgelisteten Dateipfaden erlaubt werden.

Im Rahmen des Projekts wurde sich entschieden mit Pfadregeln zu arbeiten, um eine möglichst reibungslose Funktion der SRP zu erlauben.

Der zuvor erwähnte Anwendungsbestand hat ergeben, dass sich alle nötigen Anwendungen in schreibgeschützten Standardpfaden von Windows befinden. Diese können ohne größere Sorgen in den zusätzlichen Regeln definiert werden, da normale Benutzer nicht in der Lage sind eigene Programme oder Dateien in schreibgeschützte Ordner hineinzukopieren.

Folgende Pfade wurden mit Pfadregeln (siehe 7.2.17. Abbildung 17, 7.2.18. Abbildung 18) definiert:

- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%
    - *Auf Hinweis eines Kollegen der IT-Abteilung werden diese Pfade mit normalen Pfaden zusätzlich der Registrierungswerte definiert*
- C:\Windows
- C:\Program Files
- C:\Program Files (x86)
- C:\Windows\System32
- \\%USERDNSDOMAIN%\Sysvol\
    - *Diese Pfadregel erlaubt das Ausführen von Log On Skripten bei der Anmeldung von Benutzern*

(siehe 7.2.19. Abbildung 19)

4.1. Funktionstests

Für einen ersten rudimentären Funktionstest der Richtlinien wird der Test-PC im AD in die zuvor angelegte OU verschoben und mit der zugehörigen Sicherheitsgruppe versehen. Da willkürlich gewählte und ausgeführte unerlaubte Installationsdateien erfolgreich blockiert werden, kann zum nächsten Test übergegangen werden. Hierzu werden zwei ausgewählte

PCs an Packstrecken im Lager mit den Software Restriction Policies versehen, um die Funktion in der Live-Umgebung zu überprüfen. Die Mitarbeiter im Lager arbeiten wie gewohnt mit Shared User Accounts an den gewählten Arbeitsplätzen. Der zweite Funktionstest verläuft erfolgreich, es können keine Probleme oder Störungen bei normalen Arbeitsprozessen festgestellt werden, die eine Abänderung der Richtlinien veranlassen.

4.2. Übernahme in die Live-Umgebung

Nach erfolgreichen Funktionstests kann die Richtlinie vollständig in die Live-Umgebung integriert werden. Alle übrigen PCs von Packstrecken-Arbeitsplätzen werden in die OU [redacted] verschoben und in die Sicherheitsgruppe [redacted] aufgenommen. Während des nächsten Schichtwechsels werden die Rechner neu gestartet und damit die greifenden Gruppenrichtlinien aktualisiert. Somit sind alle Arbeitsplätze im Lager mit Software Restriction Policies abgesichert und das Projektziel ist erreicht (siehe 7.2.20. Abbildung 20)

5. Abschluss

5.1. Übergabe des Projekts

Nach Abschluss des Projekts wird dieses an den Projektbetreuer [redacted] und den Verantwortlichen in der Abteilung Lager [redacted] übergeben. Mit [redacted] wird ein Termin vereinbart, um mögliche künftige Änderungen an der Konfiguration und deren Umsetzung zu besprechen.

5.2. Geänderte Anforderungen

Nach Übergabe des Projekts treten durch geänderte Arbeitsprozesse neue Anforderungen an den Software Restriction Policies auf. Mitarbeitern im Lager soll es ermöglicht werden auf unsere Zeiterfassungs-Software [redacted] zuzugreifen. Um dies zu erreichen wird eine zusätzliche Pfadregel in der Richtlinie definiert:

- C:[redacted]

Der Ordner unter diesem Pfad ist schreibgeschützt und kann somit ohne große Sorgen freigegeben werden.

5.3. Fazit und Ausblick

Das abgeschlossene Projekt wird von Projektbeteiligten und betroffenen Mitarbeitern als positive Bereicherung für das Unternehmen wahrgenommen. Sicherheitsmaßnahmen sind wichtig, um den reibungslosen Ablauf täglicher Arbeitsaufgaben zu gewährleisten. Sorgfältig konfigurierte Software Restriction Policies bieten in vielerlei Hinsicht einen Zugewinn an Sicherheit, der sich nicht negativ auf bestehende Arbeitsprozesse auswirkt.

Die zügige Umsetzung neuer und geänderter Anforderungen zeigt, dass leicht auf solche reagiert werden kann.
Im Rahmen von Modernisierungsarbeiten, Wechsel des Standardbetriebssystems von Windows 10 auf Windows 11 und Neuaufbau unterschiedlicher Systeme in kommenden Jahren können mit dem Aufbau von Software Restriction Policies Erfahrungen gemacht werden um in Zukunft modernere Sicherheitsmaßnahmen wie AppLocker oder WDAC fein abgestimmt für unterschiedliche Anwendungsbereiche im gesamten Unternehmen aufzubauen.

6. Quellenverzeichnis

IAD: Application Whitelisting using Software Restriction Policies
Veröffentlicht August 2010
Letzter Zugriff 28.03.2024
https://www.isssource.com/wp-content/uploads/2012/02/ISSSource-Application_Whitelisting_Using_SRP.pdf

„sourcejedi“: Antwort auf Applocker vs Software restriction policy
Veröffentlicht 07.08.2015
Letzter Zugriff 02.05.2024
https://serverfault.com/questions/447078/applocker-vs-software-restriction-policy

Wolfgang Sommergut: Application whitelisting: Software Restriction Policies vs. AppLocker vs. Windows Defender Application Control
Veröffentlicht 28.03.2019
Letzter Zugriff 02.05.2024
https://4sysops.com/archives/application-whitelisting-software-restriction-policies-vs-applocker-vs-windows-defender-application-control/

Jason Gerend, et al. : Festlegen der Zulassen bzw. Verweigern-Liste und des Anwendungsinventars für Richtlinien für die Softwareeinschränkung
Veröffentlicht 09.03.2023
Letzter Zugriff 28.03.2024
https://learn.microsoft.com/de-de/windows-server/identity/software-restriction-policies/determine-allow-deny-list-and-application-inventory-for-software-restriction-policies

Bryan Doe: Deploying a whitelist Software Restriction Policy to prevent Cryptolocker and more
Veröffentlicht November 2013
Letzter Zugriff 02.05.2024
https://community.spiceworks.com/t/deploying-a-whitelist-software-restriction-policy-to-prevent-cryptolocker-and-more/1008381

Jason Gerend, et al. : Arbeiten mit Regeln der Richtlinien für die Softwareeinschränkung
Veröffentlicht 11.04.2023
Letzter Zugriff 02.05.2024
https://learn.microsoft.com/de-de/windows-server/identity/software-restriction-policies/work-with-software-restriction-policies-rules

7. Anhang

7.1. Glossar

Begriff	Erklärung
AD	Active Directory, Verzeichnisdienst in Windows-Netzwerken.
AppLocker	Software zum Unterbinden der Ausführung unerwünschter Software.
Blacklist	Liste mit gesperrten Anwendungen, auch Sperrliste genannt.
class	Auch Java Class File genannt, eine Developerdatei von Oracle.
DLL	Dynamic Link Library, dynamische Programmbibliothek
docm	Word-Datei mit eingebetteten Makros.

dotm	Word-Datei-Vorlage, die Einstellungen und Makros beinhalten kann.
Executable	Auch .exe genannt, ausführbare Dateien in Windows.
GPO	Group Policy Object/Gruppenrichtlinienobjekt, digitale Richtlinie für verschiedene Einstellungen.
Group Policy Management	Konsole mit zentraler Sicht auf Gruppenrichtlinienobjekte, Organisationseinheiten, Domänen.
Hashwert	Verarbeitung eines Inhalts zu einem eindeutigen numerischen Wert.
Image	Ein Windows Systemabbild mit konfigurierten Einstellungen und Treibern.
js	JavaScript File ist eine Datei die Javascript beinhalten. Javascript ist eine Skriptsprache.
jse	Eine Verschlüsselte Javascript – Datei.
OU	Organisationseinheiten (Organizational Unit), kleinste Einheit, der Gruppenrichtlinieneinstellungen oder Kontenberechtigungen zugewiesen werden kann.
Portable-Format	Programm, welches ohne Installation ausgeführt werden kann.
potm	PowerPoint-Datei-Vorlage, die Einstellungen und Makros beinhalten kann.
pptm	PowerPoint-Datei, die eine Makro-fähige Präsentation enthält.
ps1	Dateiendung von Powershell-Skripts.
Registrierungswert	Ein Datenelement in der Windows-Registrierung.
Sicherheitsgruppe	Verwaltbare Einheiten von Benutzer-/Computerkonten und weiterem im AD.
sldm	PowerPoint-Datei, die Makros enthalten kann.
SRP	Software Restriction Policies definieren welche Software/Dateien ausgeführt oder gesperrt werden.
vbe	VBScript Encoded Script File eine Verschlüsselte Visual Basic Script Datei.
vbs	Visual Basic Script ist eine von Microsoft entwickelte Skriptsprache.

WDAC	Windows Defender Application Control, Software, um Ausführen gefährlicher Anwendungen im Netzwerk zu verhindern
ws	Windows-Skript, ein ausführbares Skript
wsf	Windows Script File, enthält ausführbare Skripte
wsh	Windows Script Host Settings, ein Skript mit dem Computeraktionen durchgeführt werden können
xlm	Eine Microsoft-Excel-Datei, die ein Makro enthält.
xlsm	Eine Microsoft-Excel-Datei, die ein Makro enthält.

7.2. Screenshots

7.2.1. Fehlermeldung Ausführen einer Anwendung blockiert 1

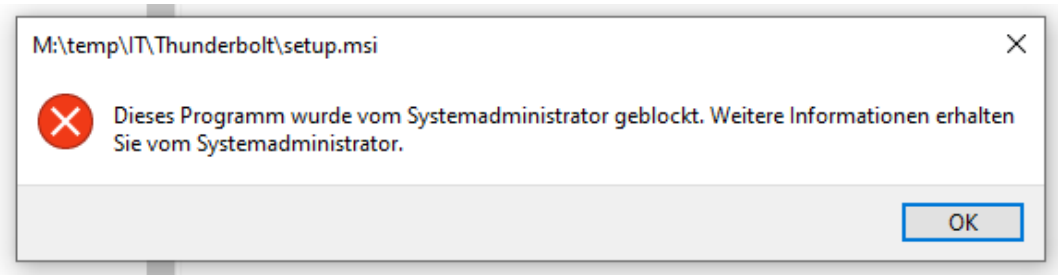

Abbildung 1

7.2.2. Fehlermeldung Ausführen einer Anwendung blockiert 2

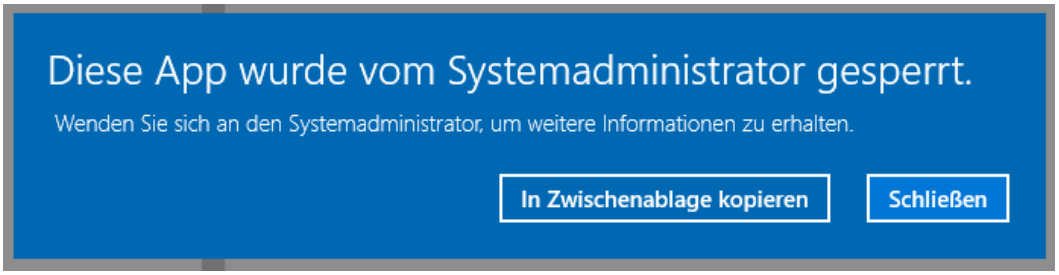

Abbildung 2

7.2.3. Auszug einer Logdatei

SRPLog - edited.txt

```
1  explorer.exe (PID = 6784) identified C:\Users          AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System T
2  winlogon.exe (PID = 18276) identified fontdrvhost.exe as Unrestricted using default rule, Guid = {11015445-d282-4f86-
3  winlogon.exe (PID = 18276) identified dwm.exe as Unrestricted using default rule, Guid = {11015445-d282-4f86-96a2-9e4
4  explorer.exe (PID = 11796) identified C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Outlook.lnk as Unrestricte
5  powershell.exe (PID = 17936) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
6  powershell.exe (PID = 18244) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
7  powershell.exe (PID = 19496) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
8  powershell.exe (PID = 18476) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
9  powershell.exe (PID = 20064) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
10 powershell.exe (PID = 11916) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
11 powershell.exe (PID = 12552) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
12 powershell.exe (PID = 20856) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
13 powershell.exe (PID = 9204) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColle
14 powershell.exe (PID = 2684) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColle
15 powershell.exe (PID = 13588) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
16 powershell.exe (PID = 18080) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColl
17 winlogon.exe (PID = 1008) identified fontdrvhost.exe as Unrestricted using default rule, Guid = {11015445-d282-4f86-9
18 winlogon.exe (PID = 1008) identified dwm.exe as Unrestricted using default rule, Guid = {11015445-d282-4f86-96a2-9e48
19 powershell.exe (PID = 5808) identified C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\DataColle
20 svchost.exe (PID = 5808) identified ctfmon.exe as Unrestricted using default rule, Guid = {11015445-d282-4f86-96a2-9e
21 powershell.exe (PID = 10584) identified C:\Users\pak03\AppData\Local\Temp\__PSScriptPolicyTest_j1hhitxe.qin.ps1 as Un
22 powershell.exe (PID = 13272) identified C:\Users\pak03\AppData\Local\Temp\__PSScriptPolicyTest_3ujektif.4kq.ps1 as Un
23 powershell.exe (PID = 13900) identified C:\Users\pak03\AppData\Local\Temp\__PSScriptPolicyTest_euj5ozs2.3hi.ps1 as Un
24 explorer.exe (PID = 10600) identified C:\Users\Public\Desktop\E+P Start Center (64-bit).lnk as Unrestricted using def
25 explorer.exe (PID = 10600) identified C:\Users\pak03\AppData\Local\Microsoft\Teams\Update.exe as Unrestricted using d
```

Abbildung 3

7.2.4. Erstellen einer neuen OU 1

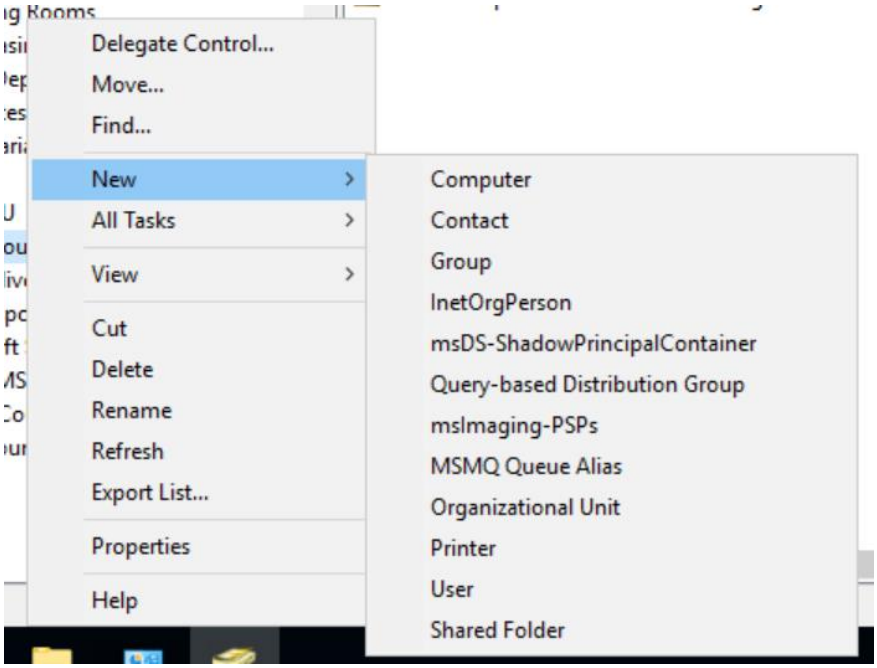

Abbildung 4

7.2.5. Erstellen einer neuen OU 2

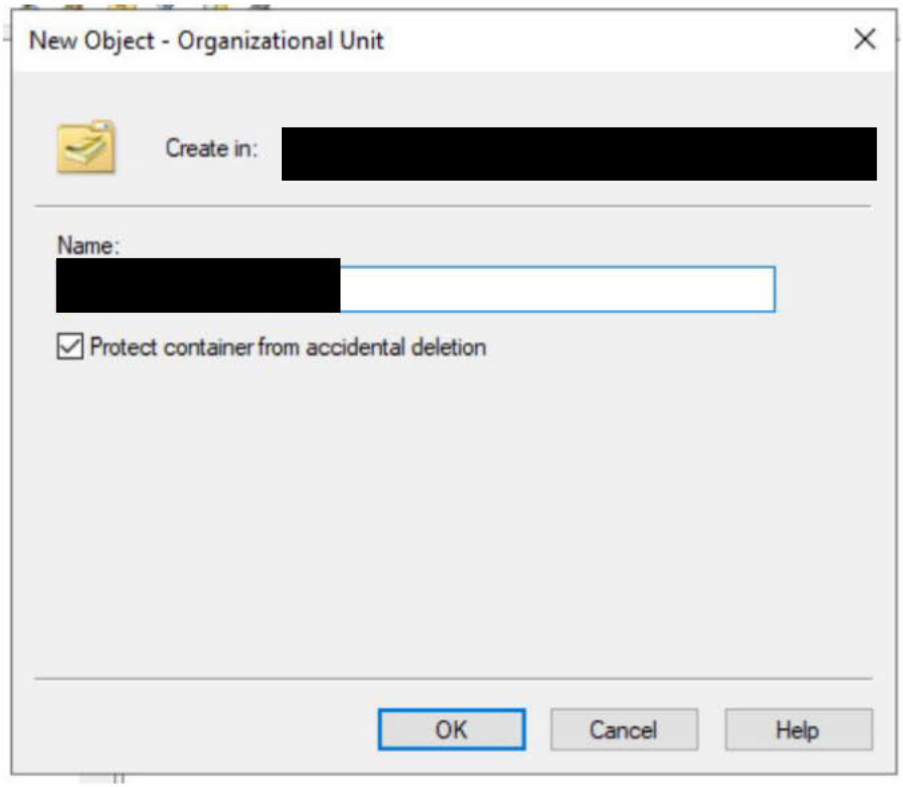

Abbildung 5

7.2.6. Neu erstellte OU

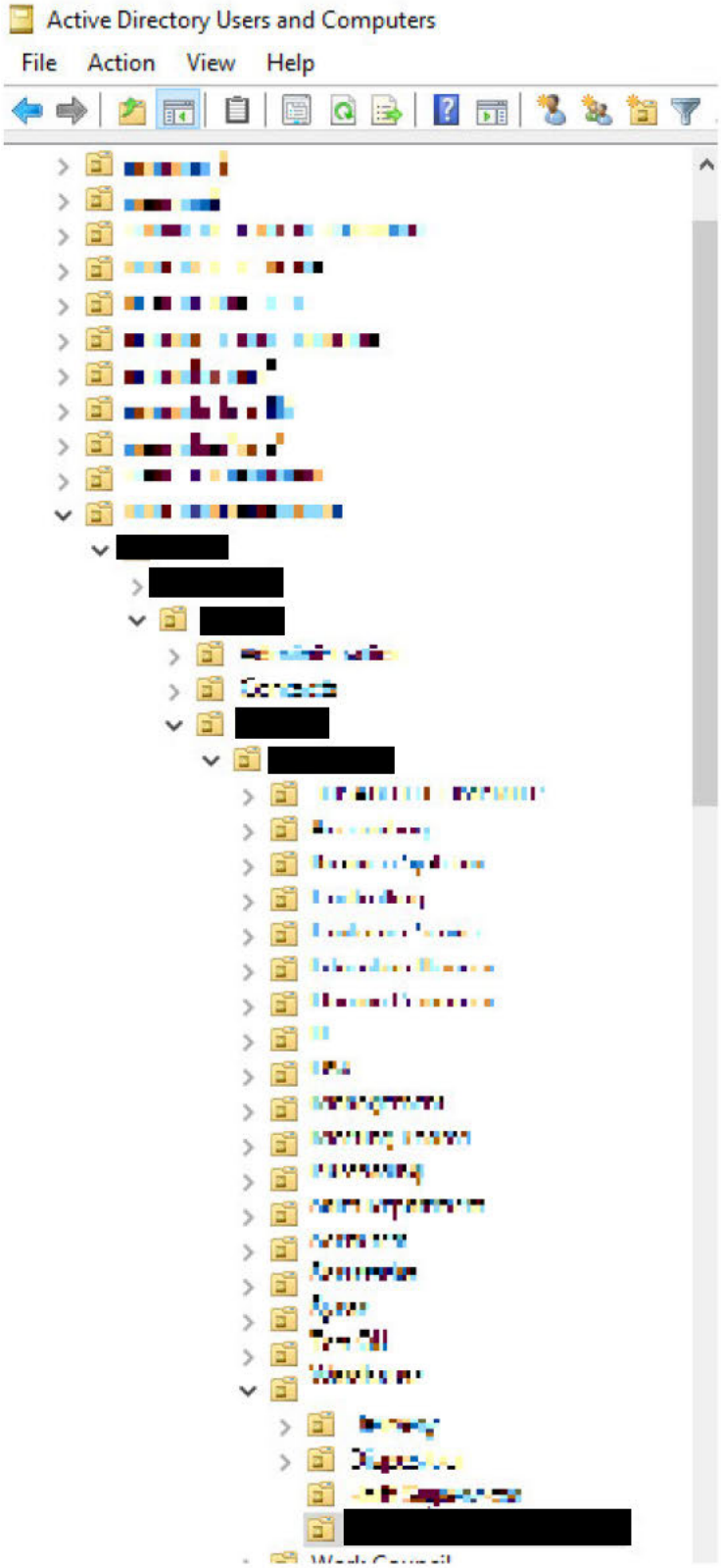

Abbildung 6

7.2.7. Erstellung einer neuen Sicherheitsgruppe

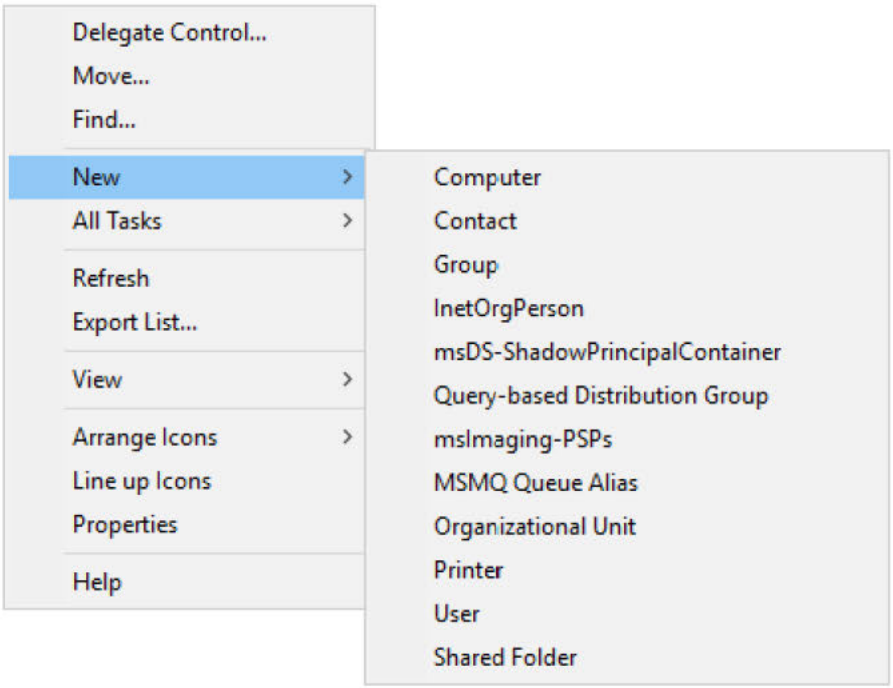

Abbildung 7

7.2.8. Erstellung einer neuen Sicherheitsgruppe 2

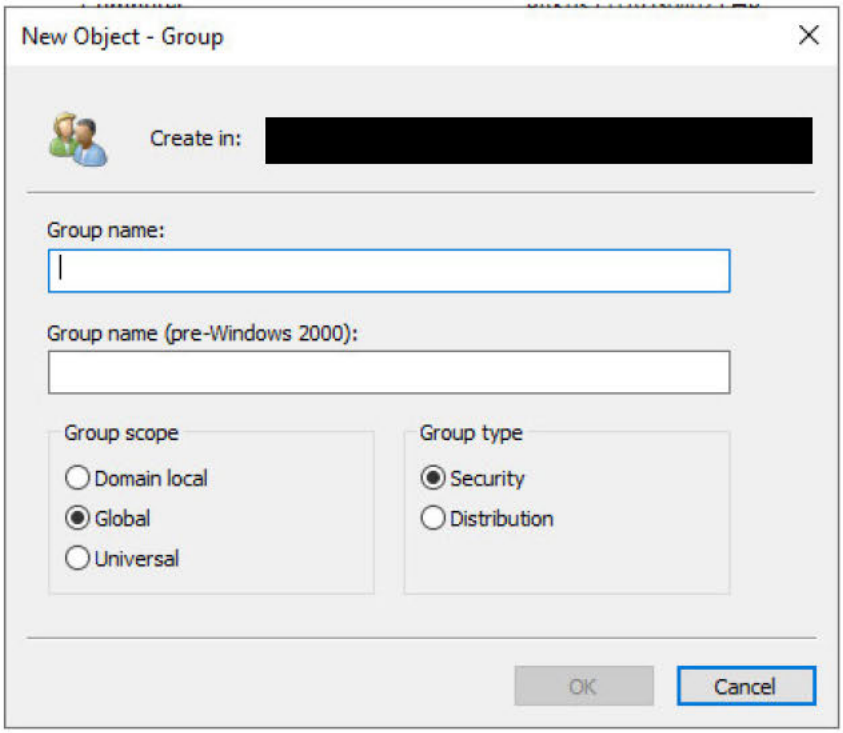

Abbildung 8

7.2.9. Erstellung einer neuen GPO 1

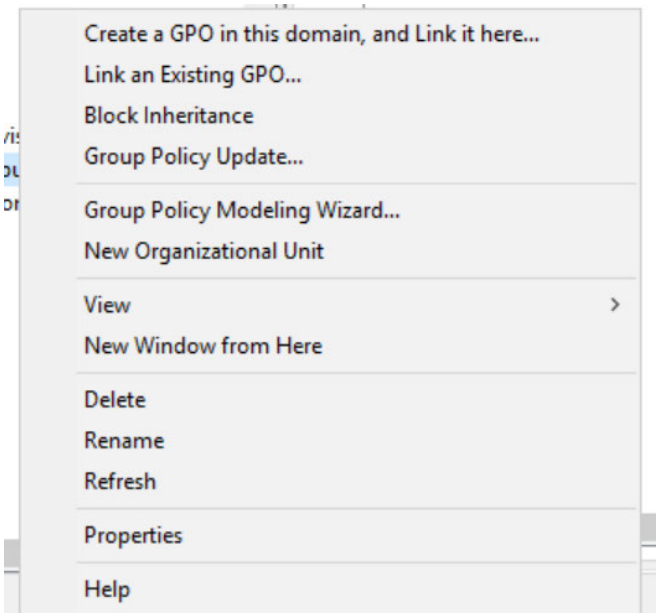

Abbildung 9

7.2.10. Erstellung einer neuen GPO 2

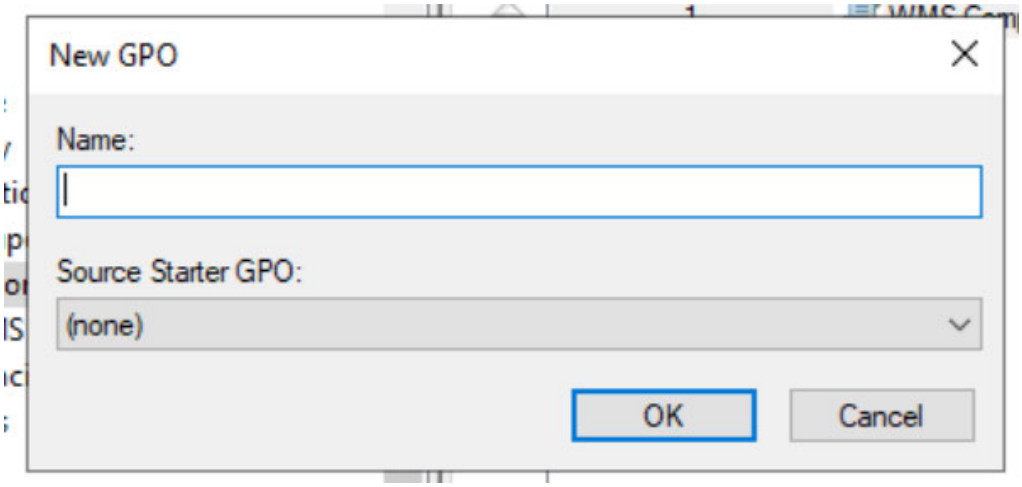

Abbildung 10

7.2.11. Verlinkung von GPO und Sicherheitsgruppe

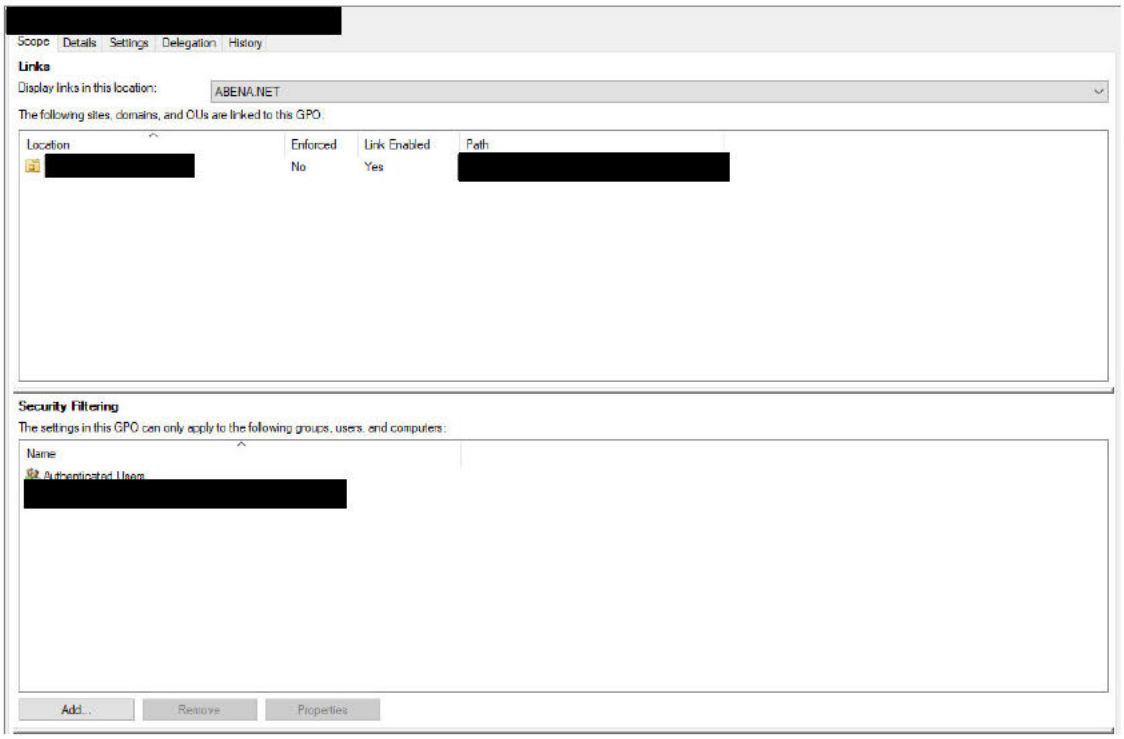

Abbildung 11

7.2.12. Erstellen von Software Restriction Policies in GPO

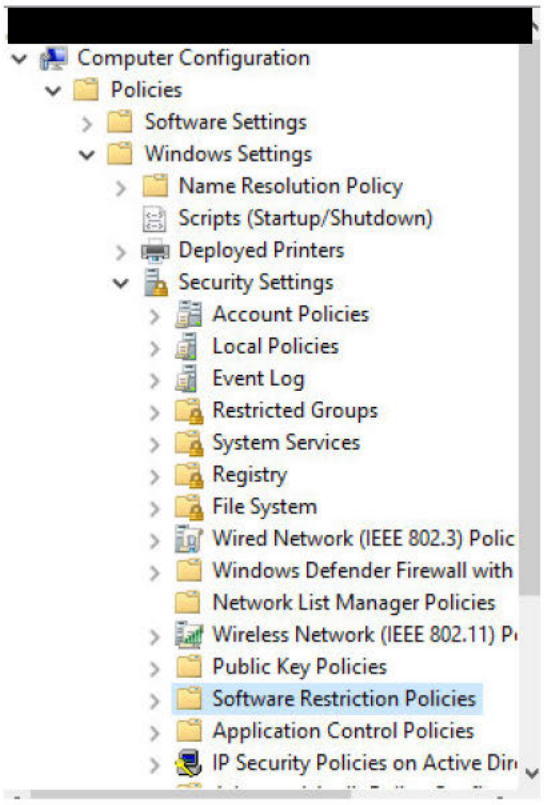

Abbildung 12

7.2.13. Security Levels – Sicherheitsstufen

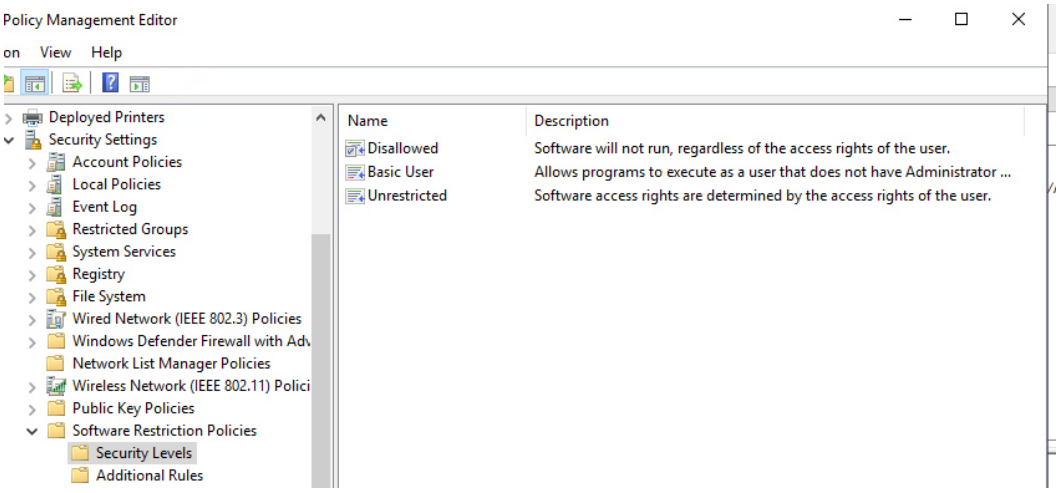

Abbildung 13

7.2.14. Sicherheitsstufe Disallowed - Nicht Erlaubt

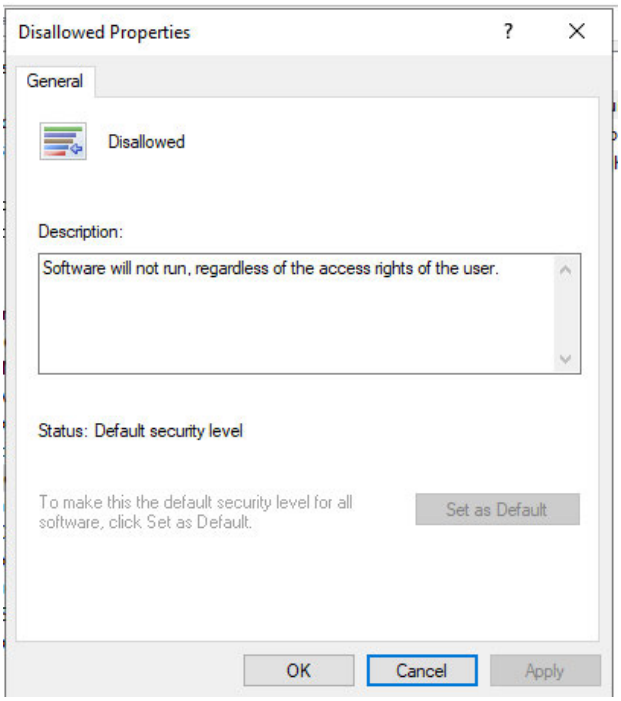

Abbildung 14

7.2.15. Designated File Types - Designierte Datentypen

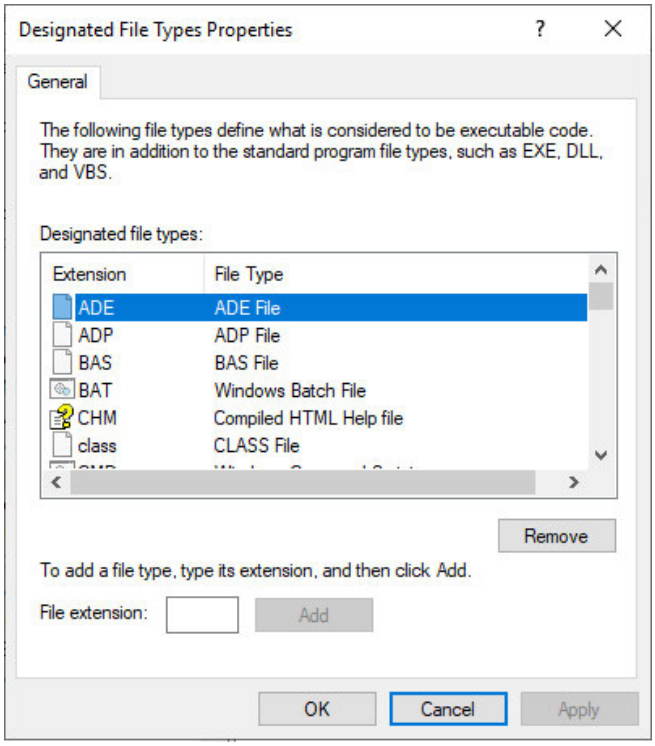

Abbildung 15

7.2.16. Definition Enforcement – Erzwingen

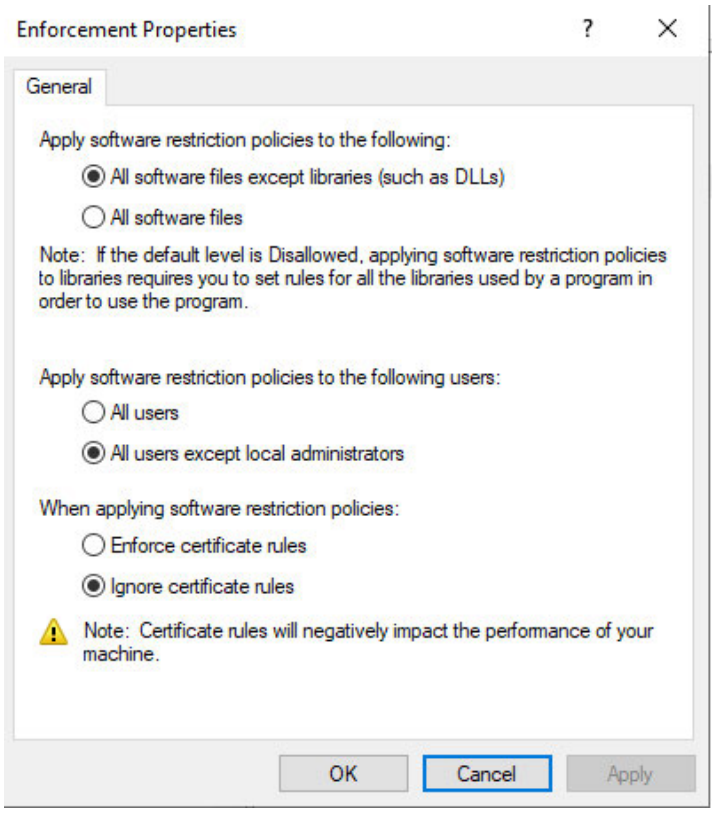

Abbildung 16

7.2.17. Neue Pfadregel 1

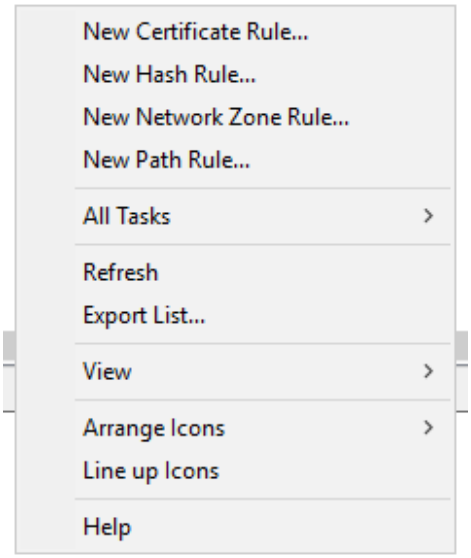

Abbildung 17

7.2.18. neue Pfadregel 2

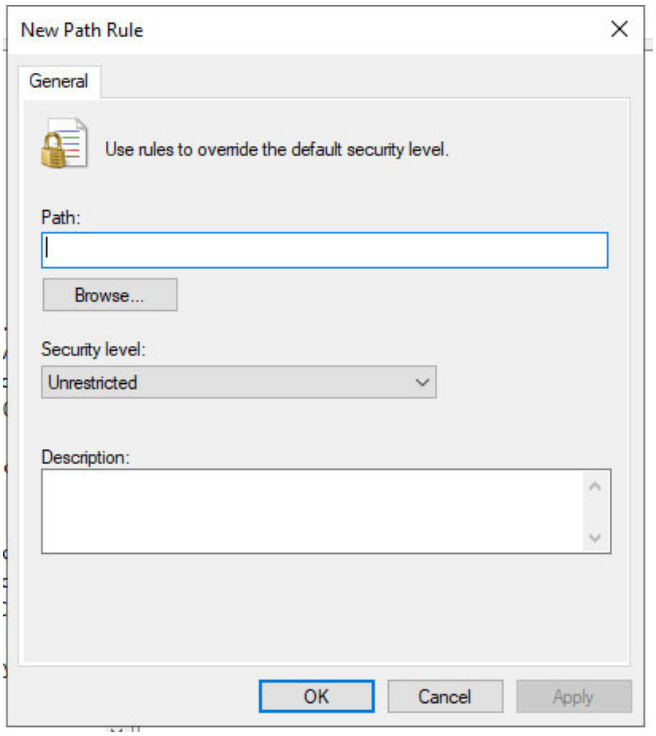

Abbildung 18

7.2.19. Zulassungsliste - Whitelist

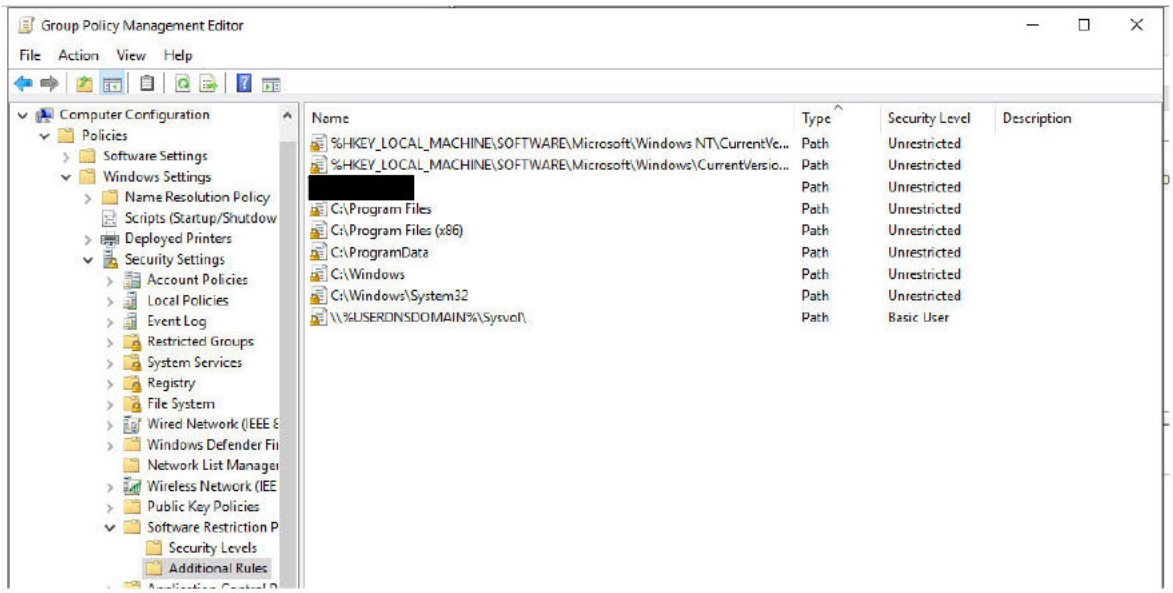

Abbildung 19

7.2.20. Abschluss OU

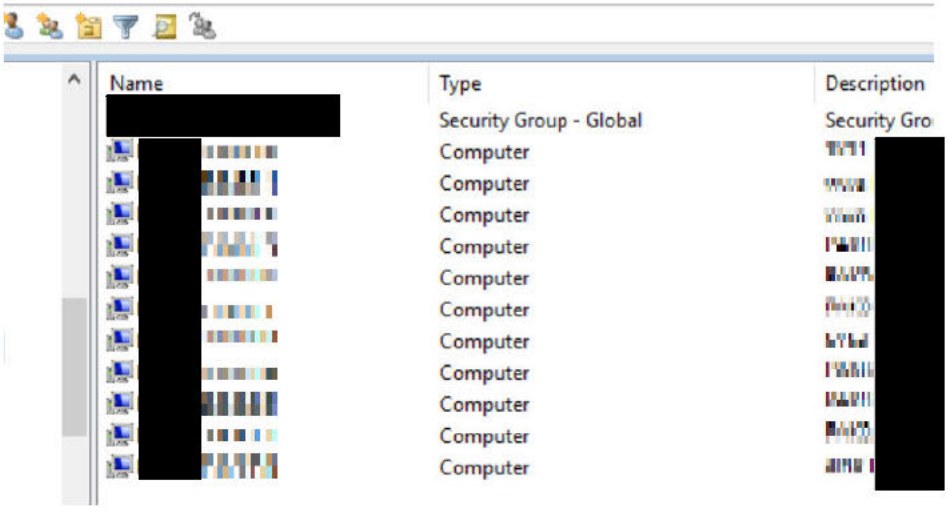

Abbildung 20

7.3. Tabellen

7.3.1. Pauschalsätze

Tabelle 1 Pauschalsätze

Auszubildender im dritten Lehrjahr	
Personalkosten	[redacted]
Material- und Energiekosten	[redacted]
Systemadministrator IT-Abteilung	
Personalkosten	[redacted]
Material- und Energiekosten	[redacted]
Qualitätssicherung und Management Lager	
Personalkosten	[redacted]
Material- und Energiekosten	[redacted]
Global IT Operations Manager, ABENA Data ApS	
Kosten	[redacted]
Systemadministrator, ABENA Data ApS	
Kosten	[redacted]

7.3.2. Kostenaufstellung

Tabelle 2 Kostenaufstellung

	Mitarbeiter	Zeitaufwand in Stunden	Kosten pro Stunde	Kosten
Durchführung	Alexander Höbald	40	[redacted]	[redacted]
Planung	[redacted]	2	[redacted]	[redacted]
Fachgespräche	[redacted]	1	[redacted]	[redacted]
Fachgespräche	[redacted]	1	[redacted]	[redacted]
Fachgespräche	[redacted]	2	[redacted]	[redacted]
Abnahme	[redacted]	1	[redacted]	[redacted]
Gesamtkosten				[redacted]

7.3.3. Terminplanung

Tabelle 3 Terminplanung

Tätigkeit	**Datum**
Beginn der Dokumentation	19.03.2024
Ist-Analyse	19.03.2024
Festlegung der Anforderungen	22.03.2024
Ermittlung des Anwendungsbestands	25.03.2024
Aufbau Testarbeitsplatz	25.03.2024
Anlegen von OU und GPO	25.03.2024
Konfiguration der Software Restriction Policies	26.03.2024
Erster Funktionstest	27.03.2024
Fortsetzung Dokumentation	28.03.2024
Test in Live-Umgebung	15.04.2024
Übernahme in Live-Umgebung	17.04.2024
Übergabe des Projekts	29.04.2024
Anpassung der SRP nach geänderten Anforderungen	30.04.2024
Abschluss der Dokumentation	02.05.2024