



IP-Scan

Inventarisierung von IP-Systemen

TITEL	IP-Scan
AUTOR	Docusnap Consulting
DATUM	12.12.2023
VERSION	4.0 gültig ab 28.11.2023

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die Docusnap GmbH zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte vorbehalten.

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of Docusnap GmbH. All rights reserved.

INHALTSVERZEICHNIS

1.	Einleitung	4
2.	Voraussetzungen	5
2.1	Gefahren und Schwierigkeiten	5
3.	IP-Scan	6
3.1	IP-Scan-Assistent	6
3.2	Analyse und Ergebnis	7
3.3	MAC-Filter für IP-Systeme	7
4.	Optional: IP-Scan Analyse-Tool	9
4.1	Verwendungszweck	9
4.2	Anwendung des Test-Programms	10
4.2.1	Scan	10
4.2.2	Analyse	10
4.2.3	Hilfe	10
4.3	Übertragung in Docusnap	11
4.3.1	Ergebnisse analysieren	11
4.3.2	Anpassung der Docusnap IP-Scan Konfiguration	11
5.	Anwendungsfälle und Praxisbeispiele	13
5.1	Erstinventarisierung	13
5.2	Erhöhen der Datenqualität	13
5.3	Sicherheitslücken erkennen	14

1. Einleitung

Der IP-Scan in Docusnap liefert Ihnen die Möglichkeit, Ihr Netzwerk oder das eines Kunden umfangreich nach aktiven Systemen zu durchsuchen. Alles was Sie für diesen ersten Überblick, oder der Überprüfung auf eine vollständige Inventarisierung benötigen, sind die relevanten IP-Adressbereiche. Für den IP-Scan werden keinerlei Anmeldeinformationen oder Community Strings verwendet. Auf diesem Weg können Sie ein neues Netzwerk sehr schnell und einfach inventarisieren und sich dabei einen Überblick verschaffen.

In Ihrem eigenen Netzwerk können Sie auf diesem Weg jene aktiven Komponenten erfassen, die Sie mit einem detaillierteren Scan noch nicht erfasst haben. Gründe hierfür können u.a. sein, dass das System nicht bekannt ist oder die nötigen Anmeldeinformationen fehlen.

Dieses HowTo beschreibt die Nutzung des IP-Scans und ist in folgende Kapitel unterteilt:

- In [Kapitel 1](#) wird die Notwendigkeit und Installation des NPCAP Treibers erklärt
- In [Kapitel 2](#) wird der eigentliche IP-Scan beschrieben
- In [Kapitel 3](#) wird gezeigt, wie Sie NMAP Parameter testen und anschließend in Docusnap übertragen können
- In [Kapitel 4](#) werden Anwendungsfälle und Praxisbeispiele genannt

Docusnap unterscheidet zwischen einem normalen und dem erweiterten IP-Scan. Beide IP-Scans funktionieren auf Basis von **NMAP (Network Mapper)**. Der normale IP-Scan verwendet Funktionen wie SYN-ACK, ARP-Request, ICMP Anfragen und eine Namensauflösung. Antwortende Systeme werden mit rudimentären Netzwerkinformationen erfasst.

Durch die Verwendung spezieller NMAP Parameter ist es dem erweiterten IP-Scan möglich zusätzliche Informationen, wie z. B. das Betriebssystem, zu erkennen.

Voraussetzung für den erweiterten IP-Scan ist die Installation des **NPCAP Treibers** auf dem inventarisierenden System.

2. Voraussetzungen

Ein erfolgreicher IP-Scan setzt im ersten Schritt nur die Bekanntheit der zu inventarisierenden IP-Adressbereiche voraus.

Wie bereits angesprochen, wird zwischen dem einfachen und dem erweiterten IP-Scan unterschieden. Für den erweiterten IP-Scan wird der NPCAP Treiber vorausgesetzt. Der NPCAP Treiber wird jeweils auf dem System benötigt, von dem aus der IP-Scan durchgeführt wird. Dies kann den Docusnap Server, Docusnap Client und die Docusnap Discovery Systeme betreffen.

Die Installation des NPCAP Treibers wird Ihnen im Zuge der Docusnap Installation angeboten und ist standardmäßig aktiv.

Eine nachträgliche Installation können Sie über das mitgebrachte Setup durchführen:

- %ProgramFiles%\Docusnap 13\MSI\npcap-oem.exe
- %ProgramFiles%\Docusnap Discovery\MSI\npcap-oem.exe

2.1 Gefahren und Schwierigkeiten

Voraussetzung für die Installation des NPCAP Treibers sind lokale Administrator Rechte.

Bei der Installation des NPCAP Treibers ist zu beachten, dass dieser in den Netzwerk-Bereich eingreift. Speziell bei Systemen wie z. B. einem Domänen Controller, Exchange-Server oder ähnlichem sollte eine Installation nicht leichtfertig durchgeführt werden.

Ebenfalls gilt zu beachten, dass eine Installation des NPCAP Treibers in Konkurrenz zu ähnlichen Netzwerktreibern stehen kann. Dies kann auch andere Versionen des NPCAP Treibers betreffen. So wird bei einer Wireshark oder PRTG Installation ebenfalls ein NPCAP, oder ehemals WINPCAP, Treiber installiert. Da es möglich ist, dass bei Wireshark oder PRTG andere Installationsoptionen gesetzt sind, können sowohl bei Wireshark als auch Docusnap fehlerhafte Resultate das Ergebnis sein.

Weitere Informationen zu den Voraussetzungen und Problematiken bei z. B. Firewall und Monitoring finden Sie in unserem [Whitepaper Docusnap Inventarisierung](#) im Kapitel IP-Scan.

3. IP-Scan

3.1 IP-Scan-Assistent

Der IP-Scan ist ein eigenständiger Inventarisierungsassistent in Docusnap. Unterschieden wird zwischen dem **Einfachen IP-Scan** und dem **Erweiterten IP-Scan**. Die Auswahl kann im Verlauf des Assistenten mittels einer Checkbox getroffen werden.

Den Assistenten für den IP-Scan finden Sie hier:

- Discovery – Alle Assistenten – IP Scan
- Inventar – Alle Assistenten – IP Scan
- Alle Aufträge – Alle Assistenten – IP Scan

IP-Scan

Der IP-Scan prüft mittels ICMP Anfragen die Adressen. Antwortet das angefragte System wird es als IP-System erfasst und mit zusätzlichen Informationen in der Datenbank gespeichert (Scandatum, IP-Adresse und Subnetzmaske). Zusätzlich versucht der IP-Scan den zugehörigen DNS-Namen aufzulösen. Ist dies erfolgreich, wird das System mit dem DNS-Namen erfasst.

Erweiterter IP-Scan

Mit Hilfe des Erweiterten Modus werden zusätzlich MAC-Vendor, Informationen zum Betriebssystem, Betriebszeit und der letzte Systemstart erfasst. Eine Genauigkeitsangabe der erfassten Informationen wird in Prozent angegeben. Dies kommt daher, dass NMAP das Betriebssystem etc. nicht immer zu 100% bestimmen kann. Anhand der Reaktion auf abgesetzte Anfragen schätzt NMAP diese Informationen ab.

Wird der Erweiterte IP-Scan aktiviert, so sucht Docusnap nach dem benötigten NPCAP Treiber. Ist dieser nicht vorhanden, kann der Erweiterte IP-Scan nicht verwendet werden.

Möchten Sie mehrere Netze zur Inventarisierung angeben empfiehlt sich die Verwendung des CSV Imports. Diesen können Sie über **Liste laden** aufrufen. In nachfolgender Abbildung wird der Aufbau der CSV Datei beschrieben.

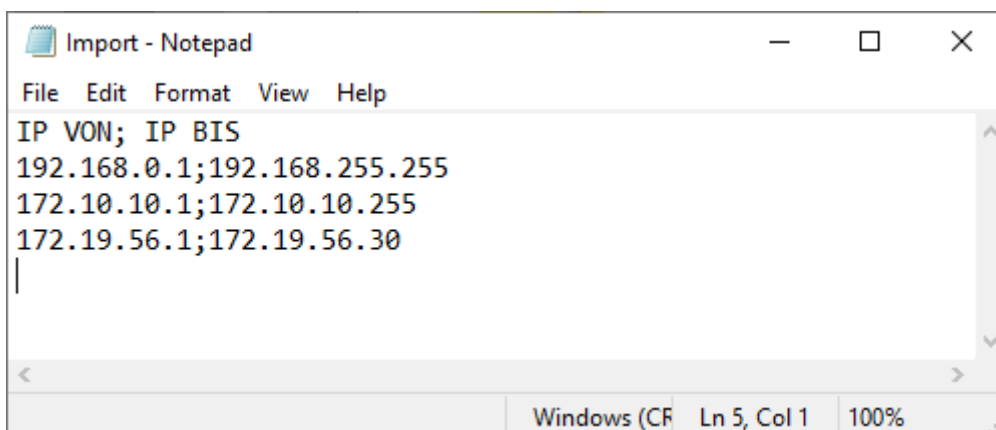


Abbildung 1 – IP-Bereiche - CSV Import

Die maximale Größe eines Netzsegments ist auf Class B (192.168.1.1 – 192.168. 255.255) beschränkt.

3.2 Analyse und Ergebnis

Die Ergebnisse Ihres IP-Scans finden Sie im Datenbaum von Docusnap unter

- Firma – Infrastruktur – Domäne – IP Systeme

Überblick der Informationen die erfasst werden können:

- Name: Name des Systems. Wenn ein DNS-Eintrag vorhanden ist, wird dieser als Name verwendet, ansonsten die IP-Adresse.
- Scandatum: Zeitpunkt, wann das System das letzte Mal per IP-Scan erfasst wurde
- IP-Adresse: IP-Adresse des Systems
- Subnetzmaske: Subnetzmaske des Systems
- MAC Adresse: MAC Adresse des Systems. **Hinweis: Die MAC-Adresse ist nur vorhanden, wenn sich das inventarisierte IP-System im gleichen Netzwerk wie der inventarisierende Part (Docusnap Server, Client, Discovery Service) befindet.**
- MAC-Vendor: Hersteller – Ergibt sich aus der erfassten MAC Adresse
- Betriebssystem: Information zu dem verwendeten Betriebssystem
- Hersteller: Hersteller des Betriebssystems
- Version: Versionsnummer des Betriebssystems
- Systemfamilie: Familie, z. B. Windows oder Linux
- Betriebszeit: Zeitangabe in Stunden
- Letzter Systemstart: Datum, wann das System das letzte Mal neu gestartet wurde
- Genauigkeit: Angabe zur Genauigkeit der erweiterten Informationen in Prozent

Mit Hilfe der erweiterten Informationen wie z. B. dem MAC-Vendor und Informationen zum Betriebssystem kann sich ein allgemeiner Überblick über das Netzwerk verschafft werden. Anschließend können die Systeme einem Assistenten für die weitere Inventarisierung zugeordnet werden.

IP-Systeme werden sowohl in Berichten als auch im Netzwerk- und Topologie Plan berücksichtigt.

3.3 MAC-Filter für IP-Systeme

Manche Systeme können nur via IP-Scan erfasst werden, da keine andere Standard Schnittstelle, z. B. SNMP unterstützt wird. Damit diese Systeme im Topologie Plan als z. B. Telefone dargestellt werden können, steht Ihnen ein MAC Filter zur Verfügung. Dadurch wird Ihnen die Unterscheidung der IP-Systeme im Topologie Plan erleichtert.

Vorgehensweise:

- Identifizieren sie den kleinsten gemeinsamen Nenner bei der MAC Adresse. Bei zwei IP-Telefonen mit jeweils einer MAC Adressen 00-1A-E8-EC-CA-70 und 00-1A-E8-EC-E9-DC wäre der kleinste gemeinsame Nenner 00-1A-E8- (= Hersteller).
- Wechseln Sie in die Docusnap **Administration – Inventar – MAC Filter**
- Hinterlegen Sie dort die MAC Adresse – 00-1A-E8-
- Unterstützte Wildcard Zeichen sind * um mehrere beliebige Zeichen und ? um genau ein beliebiges Zeichen anzugeben.

MAC Adressen vom Typ Ignorieren und Virtuell werden im Topologie Plan anschließend nicht mehr dargestellt.

Weitere Informationen zum MAC Filter finden Sie im Docusnap Handbuch im Bereich MAC Filter. (F1 Taste im entsprechenden Bereich innerhalb der Docusnap Administration) oder im [HowTo Inventarisierung und Auswertung von SNMP](#) in der Docusnap Knowledge Base.

4. Optional: IP-Scan Analyse-Tool

Das IP-Scan Analyse-Tool erhalten Sie auf Anfrage beim Docusnap Support.

4.1 Verwendungszweck

Jedes Netzwerk ist anders. Somit kann es vorkommen, dass der IP-Scan in seltenen Fällen keine bzw. mangelhafte Ergebnisse liefert. Ursache kann hierfür der Virenschanner, die Konfiguration der Firewall oder auch ein Proxy sein. Verschiedenste Netzwerkkomponenten können sich auf die Ergebnisse des IP-Scans auswirken. Der Docusnap IP-Scan verwendet im Standard Parameter, welche bei einem Großteil der Netzwerke erfolgreich Daten inventarisiert. Damit Sie auch in Ihrem Netzwerk die besten Ergebnisse mit dem IP-Scan erhalten, haben Sie die Möglichkeit mit Hilfe des IP-Scan Analyse-Tools die für Sie richtigen NMAP Parameter herauszufinden. Anschließend können Sie diese an Docusnap übergeben.

Das IP-Scan Analyse-Tool ist eine eigenständige Applikation. Es wird keine Docusnap Installation vorausgesetzt. Voraussetzung ist die Installation des NPAC Treibers.

Für eine bestmögliche Analyse sollten Sie das IP-Scan Analyse-Tool auf demselben System ausführen, auf dem der Docusnap IP-Scan ebenfalls ausgeführt wird, z. B. Docusnap Server oder Docusnap Discovery Service.

Standard Parameter des Docusnap IP-Scans, Docusnap Version 10.0.1472.2:

```
-F -T3 -O --osscan-guess --script smb-os-discovery.nse
```

4.2 Anwendung des Test-Programms

Wenn Sie das IP-Scan Analyse-Tool mit einem Doppelklick starten, öffnet sich ein neues Fenster. Innerhalb dieser GUI können Sie einen IP-Scan durchführen, Parameter beeinflussen und anschließend die Ergebnisse analysieren.

Das Analyse-Tool ist in drei Bereiche unterteilt. **Scan**, **Analyse** und **Help**.

4.2.1 Scan

Innerhalb des **Scan** Bereichs ist es Ihnen möglich die Parameter Ihrem Netzwerk entsprechend anzupassen. Dabei können Sie ebenfalls auf **Presets** zurückgreifen. Die vorgegebenen Presets unterscheiden sich in den verwendeten Parametern. Dabei stehen Ihnen folgende Presets zur Verfügung:

- PingScan: Parameter `-PE` – Ping. (Echo-Reply wird erwartet)
- Nmap PingScan: Parameter `-sP` – einfacher IP-Scan in Docusnap
- Docusnap Version: Verwendet NMAP Parameter der jeweiligen Docusnap Version

Eine Anpassung der zu verwendenden Parameter können Sie unter **Parameter Section** durchführen. Parameter können mittels der Checkboxen ausgewählt oder über eine Texteingabe im Feld **Parameter** hinzugefügt werden. Eine detaillierte Übersicht aller verfügbaren NMAP Parameter finden Sie unter <https://nmap.org/>.

Im nachfolgenden Beispiel wird der Scan mit dem Preset der letzten Docusnap Version durchgeführt. Die Parameter werden automatisch mit einem Klick auf das jeweilige Preset gesetzt. Mit dem Button **Start Scan** wird dieser mit den angegebenen Parametern gestartet.

Die verwendeten Parameter sowie Pfadangabe der Logdatei finden Sie in den jeweiligen Textboxen. Logfiles werden in einem automatisch angelegten Ordner auf Ihrem Desktop gespeichert. Im Logging sehen Sie Informationen zum aktuellen Status des Scans.

Beispiel:

Um die Durchführung des IP-Scans zu beschleunigen wird die Geschwindigkeit erhöht, sowie die Maßnahmen zur Betriebssystemerkennung minimiert.

Beachten Sie, dass eine Erhöhung der Geschwindigkeit die Qualität der Ergebnisse beeinflussen kann.

4.2.2 Analyse

Im **Analyse** Bereich können Sie die Ergebnisse Ihres letzten, oder von vorherigen Scans auswerten. Genauere Informationen zur Analyse finden Sie im nachfolgenden Kapitel [Ergebnisse analysieren](#)

4.2.3 Hilfe

Innerhalb des **Help** Tabs finden Sie weitere Informationen zu den **Timing-Einstellungen** sowie zur **Analyse**.

4.3 Übertragung in Docusnap

4.3.1 Ergebnisse analysieren

Im Analyse-Bereich können Sie die Ergebnisse Ihrer Scans anschließend auswerten. Im Standard öffnet das IP-Scan Analyse-Tool den letzten durchgeführten Scan. Möchten Sie einen bestimmten Scan auswerten, können Sie über **File Selection** die gewünschte .xml Datei in das Analyse-Fenster laden.

Unterschieden wird zwischen der **einfachen Analyse** und der **Analyse mit Cleanup**.

Bei der **einfachen Analyse** werden lediglich die Ergebnisse aus dem Scan ausgewertet. Falsch erkannte Hosts, z. B. ausgelöst durch einen transparenten Proxy, werden hierbei nicht gefiltert.

Bei einer **Analyse mit Cleanup** werden die erkannten Hosts anschließend auf dieselbe Weise wie in Docusnap gefiltert. Damit wird versucht fälschlicherweise als positiv erkannte Hosts herauszufiltern. Bei Netzwerken mit einem transparenten Proxy kann es vorkommen, dass dieser auf jede Anfrage des IP-Scans antwortet. Somit werden alle Adressen als positiv erkannt. Mit Hilfe der Cleanup Funktion werden die falsch erkannten Systeme herausgefiltert. Die Ergebnisse Ihres Scans können Sie anschließend im Analyse-Fenster sehen und z. B. in eine CSV Datei exportieren.

Entsprechen die Resultate des Scans den Systemen Ihres Netzwerks, können Sie anschließend die von Ihnen gesetzten Parameter an Docusnap übergeben.

4.3.2 Anpassung der Docusnap IP-Scan Konfiguration

Die NMAP Parameter für den IP-Scan werden in der **DocusnapSettings.xml** durchgeführt. Zu beachten ist, dass diese Anpassung auf jedem System durchgeführt werden muss. Haben Sie z. B. mehrere Docusnap Discovery Services im Einsatz, muss auf dem jeweiligen System die **DocusnapSettings.xml** angepasst werden.

Sind keine Parameter gesetzt, verwendet der Docusnap IP-Scan automatisch die Parameter der jeweiligen Docusnap Version.

Im Standard finden Sie die **DocusnapSettings.xml** auf dem Docusnap-/ bzw. Docusnap Discovery Service Hostsystem in folgendem Verzeichnis:

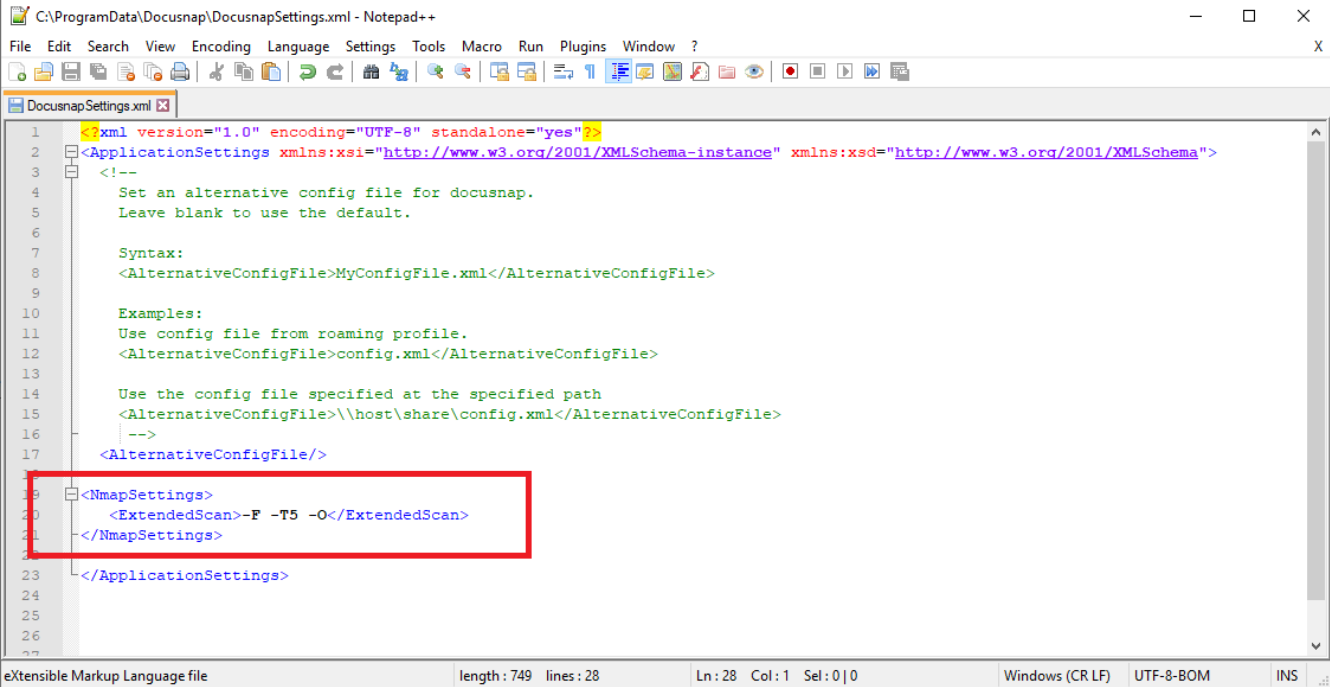
C:\ProgramData\Docusnap\DocusnapSettings.xml

Mit einem Texteditor, z. B. Notepad, können Sie die **DocusnapSettings.xml** bearbeiten.

Innerhalb der **<ApplicationSettings>** Tags werden die neuen Tags eingefügt. Zwischen den **<ExtendedScan>** Tags können Sie anschließend Ihre Parameter hinterlegen.

NMAP Parameter Tags für **DocusnapSettings.xml**:

```
<NmapSettings>  
  <ExtendedScan></ExtendedScan>  
</NmapSettings>
```



```
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <ApplicationSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
3   <!--
4     Set an alternative config file for docusnap.
5     Leave blank to use the default.
6
7     Syntax:
8     <AlternativeConfigFile>MyConfigFile.xml</AlternativeConfigFile>
9
10    Examples:
11    Use config file from roaming profile.
12    <AlternativeConfigFile>config.xml</AlternativeConfigFile>
13
14    Use the config file specified at the specified path
15    <AlternativeConfigFile>\\host\share\config.xml</AlternativeConfigFile>
16    -->
17   <AlternativeConfigFile/>
18
19   <NmapSettings>
20     <ExtendedScan>-F -T5 -O</ExtendedScan>
21   </NmapSettings>
22
23 </ApplicationSettings>
```

eXtensible Markup Language file length: 749 lines: 28 Ln: 28 Col: 1 Sel: 0 | 0 Windows (CR LF) UTF-8-BOM INS

Abbildung 2 - NMAP Parameter in Docusnap - DocusnapSettings.xml

5. Anwendungsfälle und Praxisbeispiele

5.1 Erstinventarisierung

Eine vollständige und detaillierte Inventarisierung einer Netzwerkkumgebung ist nur mit ausreichend privilegierten Benutzern möglich. Oftmals hat die inventarisierende Person bei einem neuen Kunden weder einen root Zugang zu Linux Systemen noch einen administrativen Zugang zu den Windows Systemen zur Verfügung. Trotzdem wird von dem Netzwerk ein erster Überblick benötigt.

Mit Hilfe des erweiterten IP-Scans können Sie die gewünschten Netzwerke analysieren, ohne dass administrative Rechte benötigt werden. Dabei können Sie herausfinden, wie viele Systeme vorhanden sind. Mit Hilfe der Betriebssysteminformationen ist anschließend eine Unterteilung in entsprechende Kategorien möglich.

- ➔ Anzahl der Windows Systeme
- ➔ Anzahl der Linux Systeme
- ➔ Anzahl der möglichen SNMP Systeme
- ➔ Etc.

5.2 Erhöhen der Datenqualität

Voraussetzung für eine qualitativ hochwertige Dokumentation ist eine gute Datenqualität in Docusnap. Da oftmals keine Übersicht der bestehenden Systeme vorhanden ist, ist ein Gegenprüfen der inventarisierten Systeme nicht möglich. Mit Hilfe des IP-Scans ist es Ihnen möglich eine Übersicht mit noch unbekanntem Systemen zu erstellen und gezielt zu erfassen.

Ausgangssituation:

Alle Drucker des Unternehmens befinden sich im Netz XYZ. Dieses Netz wird bereits regelmäßig per SNMP inventarisiert. Um sicher zu gehen, dass wirklich alle Systeme innerhalb des Netzes erfasst werden, wird zusätzlich noch regelmäßig der IP-Scan eingesetzt.

Sind in diesem Fall Geräte noch nicht in Docusnap erfasst, werden diese nun zu den IP-Systemen hinzugefügt.

Anschließend sollten Sie die erfassten IP-Systeme bezüglich der SNMP Schnittstelle prüfen.

Werden diese Systeme zukünftig als SNMP Systeme erfasst, wird der Eintrag unterhalb der IP-Systeme verschoben. Eine Herabstufung hingegen ist nicht möglich – z. B. SNMP zu IP-System.

5.3 Sicherheitslücken erkennen

Bring your own Device, alte Netzwerkkomponenten und Internet of Things. Oftmals werden diese Systeme in Verbindung mit Sicherheitslücken gebracht. Nachfolgend wird Ihnen beschrieben, wie Sie mittels des Docusnap IP-Scans Sicherheitslücken erfassen, dokumentieren und darauf reagieren können.

Alte Netzwerkkomponenten erkennen:

In einem wachsenden Netzwerk kommt es im Laufe der Zeit vor, dass immer mehr alte Systeme vorhanden sind. Je nach Funktion kann dadurch eine Sicherheitslücke entstehen. Unterstützen diese Systeme als Schnittstelle nicht mindestens das SNMP Protokoll wird es schwierig diese zu erfassen, dokumentieren und entsprechend zu reagieren.

Mit Hilfe des IP-Scans können Sie einen regelmäßigen Scan Ihres Netzwerks durchführen. Ist z. B. noch ein alter Switch im Einsatz, wird dieser durch den IP-Scan erfasst. Dadurch vermeiden Sie z. B. den Ausfall Ihres Netzwerks aufgrund veralteter Hardware.

Bring your own Device / Internet of Things

Die Aussage „Jeder neue Kühlschrank hat eine IP-Adresse“ entspricht nicht ganz der Realität, trifft den Nagel jedoch auf den Kopf. Mit den Netzwerken eines Unternehmens sind verschiedenste Systeme verbunden. Von Arbeitsplatzrechnern, Servern, privaten Mobiltelefonen bis hin zu Systemen des Alltags ist alles dabei. Aufgrund der Sicherheit des Netzes werden diese oftmals in verschiedene Bereiche eingeteilt. Zu Sicherheitslücken kann es kommen, wenn die Kaffeemaschine plötzlich im selben VLAN wie die Switches verfügbar ist.

Um eine solche Fehlkonfiguration zu erkennen, bietet sich der IP-Scan an. Da alle aktiven Systeme im Netzwerk erfasst werden, finden Sie auch die Systeme des Alltags sowie die sonstigen Geräte und können deren Netzwerkkonfiguration prüfen.

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1 – IP-BEREICHE - CSV IMPORT 6
 ABBILDUNG 2 - NMAP PARAMETER IN DOCUSNAP - DOCUSANPSETTINGS.XML12

VERSIONSHISTORIE

Datum	Beschreibung
07.10.2019	Version 1.0 – Beschreibung des IP-Scans
22.04.2020	Version 2.0 - Überarbeitung des HowTos für Docusnap 11
01.08.2022	Version 2.1 – Erweiterung um die fehlenden MAC-Adressen aus anderen Netzwerken
10.01.2023	Version 3.0 – Überarbeitung des HowTos für Docusnap 12
28.11.2023	Version 4.0 – Überarbeitung des HowTos für Docusnap 13

