OT-Patch-Management: So klappt’s auch ohne WSUS

Peter Lukesch
CEO
ondeso GmbH

Ihr Speaker

PETER LUKESCH

CEO
ondeso GmbH

- Ingenieur für Elektrotechnik und technische Informatik
- Langjähriger IT-Leiter in Office- und Produktionsumgebungen
- Mehr als 10 Jahre Erfahrung in medizinischer und militärischer IT-Sicherheit

Das „WIR“ ist ondeso!

UNSERE FIRMA

- ✓ Gegründet 2010
- ✓ 2 Standorte in Deutschland
- ✓ Kontinuierlicher OT-Fokus

UNSERE SOFTWARE-LÖSUNGEN

- ✓ Auf allen 5 Kontinenten im Einsatz
- ✓ Über 100.000 OT-Endgeräte
- ✓ 100% made in Germany

ondeso SR ondeso OM ondeso DC

„State of OT Security Report 2024“ von Palo Alto Networks

„Fast 70% der Industrieunternehmen haben letztes Jahr einen Cyberangriff erlebt.“

Befragung von weltweit 1.979 Führungs- und Fachkräfte aus dem Bereich OT und IT aus 16 verschiedenen Branchen

Quelle: https://www.paloaltonetworks.com/resources/research/state-of-ot-security-report

Wer ist der nächste?

Produktion lahmgelegt: Hackerangriff auf Lemken

News
16. Mai 2024 • 2 Minuten

Cyberkriminalität

Aufgrund einer Cyberattacke hat der Landmaschinenhersteller Lemken seine Produktion gestoppt.

Die Produktion des Landmaschinenherstellers Lemken steht aktuell still. Ursache ist ein Hackerangriff.

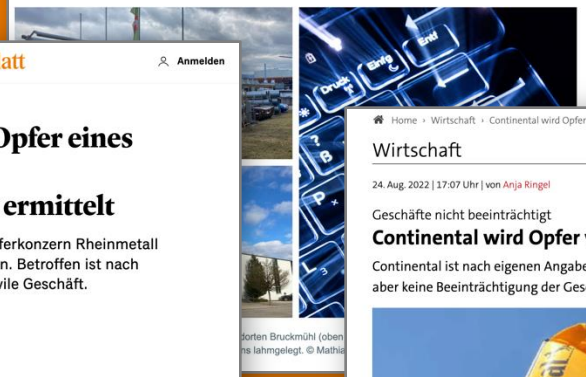
Foto: Woogloosqr – shutterstock.com

ovb-online-de › Rosenheim › Region Bad Aibling

„Gezielt ausgeführter Angriff“: Cyberattacke legt komplette Fritzmeier Group lahm

18.01.2023, 18:49 Uhr
Von: Eva Lagler, Mathias Weinzierl

Kommentare Drucken



dorten Bruckmühl (oben
ns lahmgelegt. © Mathia

Handelsblatt Anmelden

Rüstungskonzern

Rheinmetall wird Opfer eines Hackerangriffs – Staatsanwaltschaft ermittelt

Der Rüstungs- und Automobilzulieferkonzern Rheinmetall ist von Hackern angegriffen worden. Betroffen ist nach Unternehmensangaben nur das zivile Geschäft.

Larissa Holzki
17.04.2023 - 11:08 Uhr

Artikel anhören nicht verfügbar

Home › Wirtschaft › Continental wird Opfer von Cyberangriff

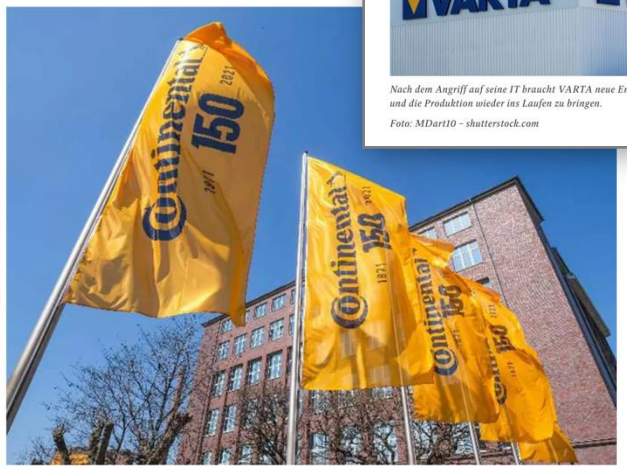
Wirtschaft

24. Aug. 2022 | 17:07 Uhr | von Anja Ringel

Geschäfte nicht beeinträchtigt

Continental wird Opfer von Cyberangrif

Continental ist nach eigenen Angaben Opfer eines Cyberangr
aber keine Beeinträchtigung der Geschäfte. Was bekannt ist.



Cyberattacke auf Batteriehersteller Hacker legen VARTA lahm

Analyse
14. Feb. 2024 • 3 Minuten

Cyberkriminalität

Nach einem Angriff auf seine IT-Systeme musste VARTA seine Produktion und Verwaltung herunterfahren und vom Netz nehmen.

Nach dem Angriff auf seine IT braucht VARTA neue Energie, um den Betrieb und die Produktion wieder ins Laufen zu bringen.

Foto: MDart10 – shutterstock.com

Award Mediadaten Magazin

it-daily.net

Menü Newsticker NIS2 Quanten Computing IT-Recht KI Wee

100 GB an Daten

RansomHub attackiert deutschen Sanitärhersteller Grohe

24. Januar, 2025 08:37

Bildquelle: Karolis Kavolelis/Shutterstock.com

Warum ist Patchen von OT-Systemen so wichtig?

- **Fertigungsindustrie im Fokus von Ransomware**
  Teure Ausfallzeiten = Hohe Bereitschaft Lösegelder zu zahlen
- **OT wird zunehmend zu einem strategischen Ziel**
  Immer mehr gezielte Attacken auf industrielle Systeme, auch durch staatliche Akteure
- **Compliance und Gesetze verlangen aktives Patch-Management**
  Interne Richtlinien, NIS2, CRA, IEC 62443 & Co. machen Patch-Prozesse zur Pflicht
- **Virtuelles Patchen reicht nicht aus**
  Firewalls helfen nur bedingt, Innentäter und Memory Leaks bleiben ein Risiko
- **Patchen reduziert das Gesamtrisiko**
  Weniger Schwachstellen bedeuten geringere Angriffsfläche

Patch-Definition nach ISA/IEC 62443-2-3

„The current technical report addresses the installation of patches, also called software updates, software upgrades, firmware upgrades, service packs, hot fixes, basic input/output system updates, and other digital electronic program updates that resolve bug fixes, operability, reliability, and cybersecurity vulnerabilities.“

=

Alles, was die bereits installierte Software (installierte Basis) verändert!

Quelle: https://www.isa.org/intech/201810standards

Rückblick: Von Security Rollup Packages zum modernen Patchen

ondeso

2000 — **Security Rollup Packages und Service Packs**
Teils sogar auf Medien bereitgestellt

2002 — **Automatische Aktualisierungen,** später Windows Update Agent **und Software Update Services (SUS)**

2003 — **Windows Server Update Services (WSUS)**
Zwischenzeitlich auch als MUS und WUS bezeichnet

2005 — **Windows Server Update Services (WSUS) 2.0**
Umstellung auf MS SQL-Datenbank

2007 — **Windows Server Update Services (WSUS) 3.0**

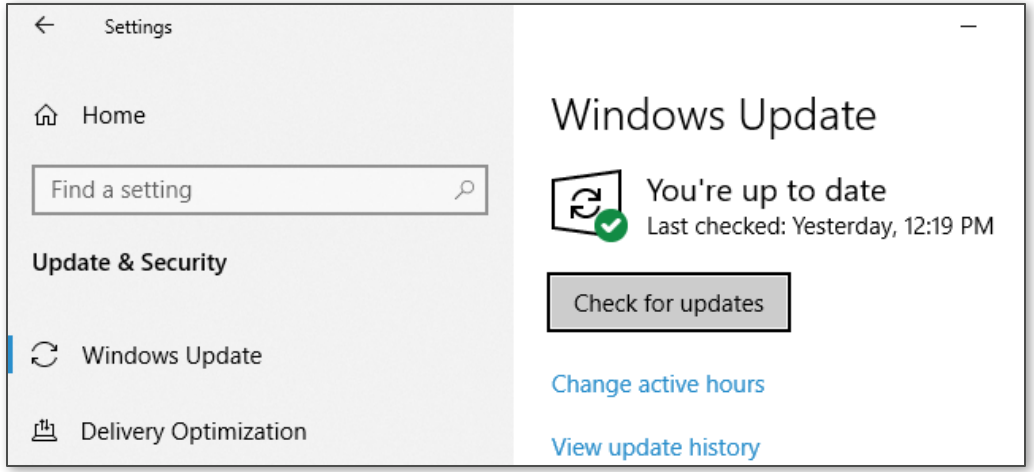
2012 — **Windows Server Update Services (WSUS) 4.0**

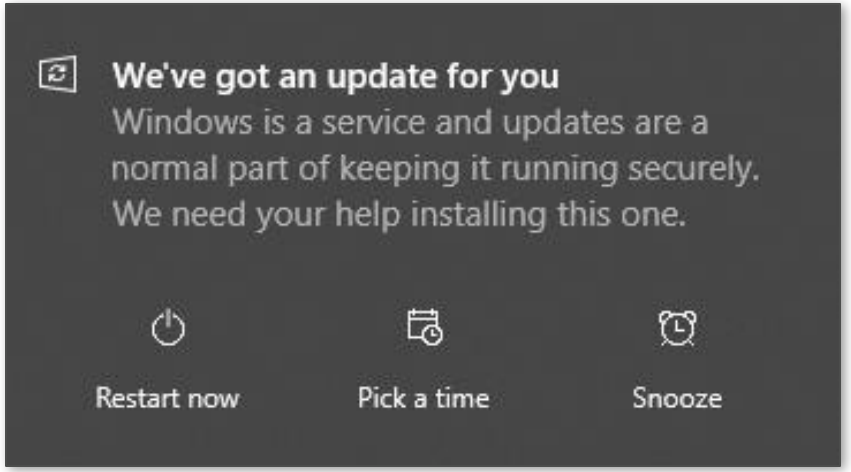
2015 — **Windows 10 mit Rolling Releases und halbjährlichen Funktionsupdates**

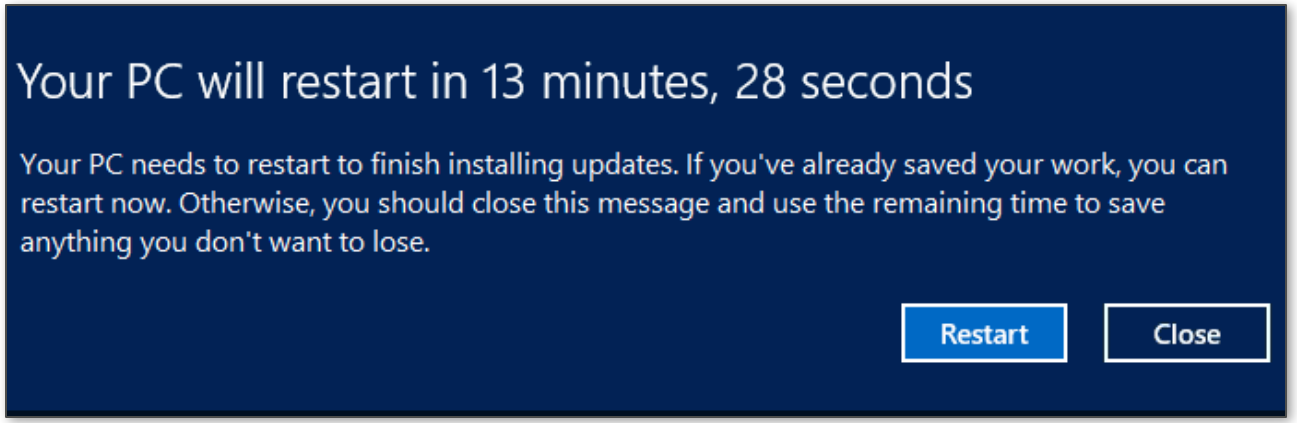
2016 — **Windows Server Update Services (WSUS) 5.0 und Long Term Servicing Branch (LTSB)**

SEIT 2019 — **Windows Server Update Services (WSUS) 6.0 und Long Term Servicing Channel (LTSC)**

Patch-Management: The Office Way …







Währenddessen in der Produktion …

- **Heterogene OT-Clients**
- **Jahrzehnte an Betriebssysteme**
- **24/7 – 3-Schicht-Betrieb**
- **Keine Domänen oder Verzeichnisdienste**
- **Unterschiedlichste Netzwerktypen**

Microsoft Tech Community Blog im Juli 2024

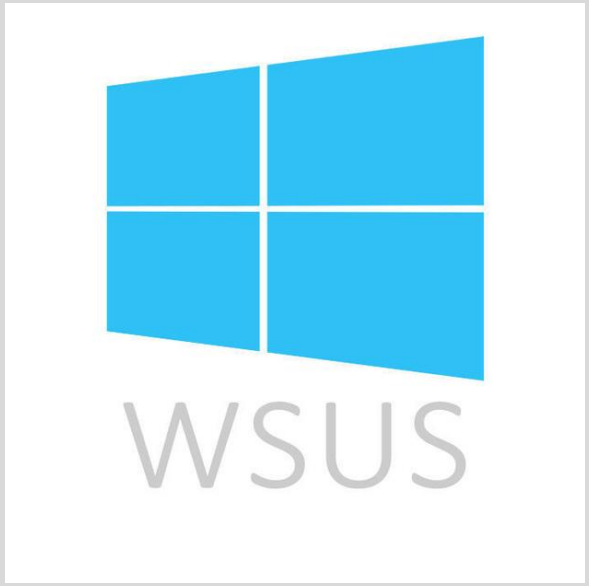
Neuer Eintrag

„Im Rahmen unserer Vision für eine vereinfachte Windows-Verwaltung aus der Cloud kündigt Microsoft den ‚deprecated'-Status für WSUS an."

Nir Froimovici
Product Manager bei Microsoft

Quelle: https://techcommunity.microsoft.com/blog/windows-itpro-blog/windows-server-update-services-wsus-deprecation/4250436

Bedeutet: WSUS-Weiterentwicklung eingestellt



- Keine funktionalen Neuerungen
- Lediglich Sicherheits- und Kompatibilitätsupdates

Microsoft legt Fokus auf Cloud-basierte Lösungen

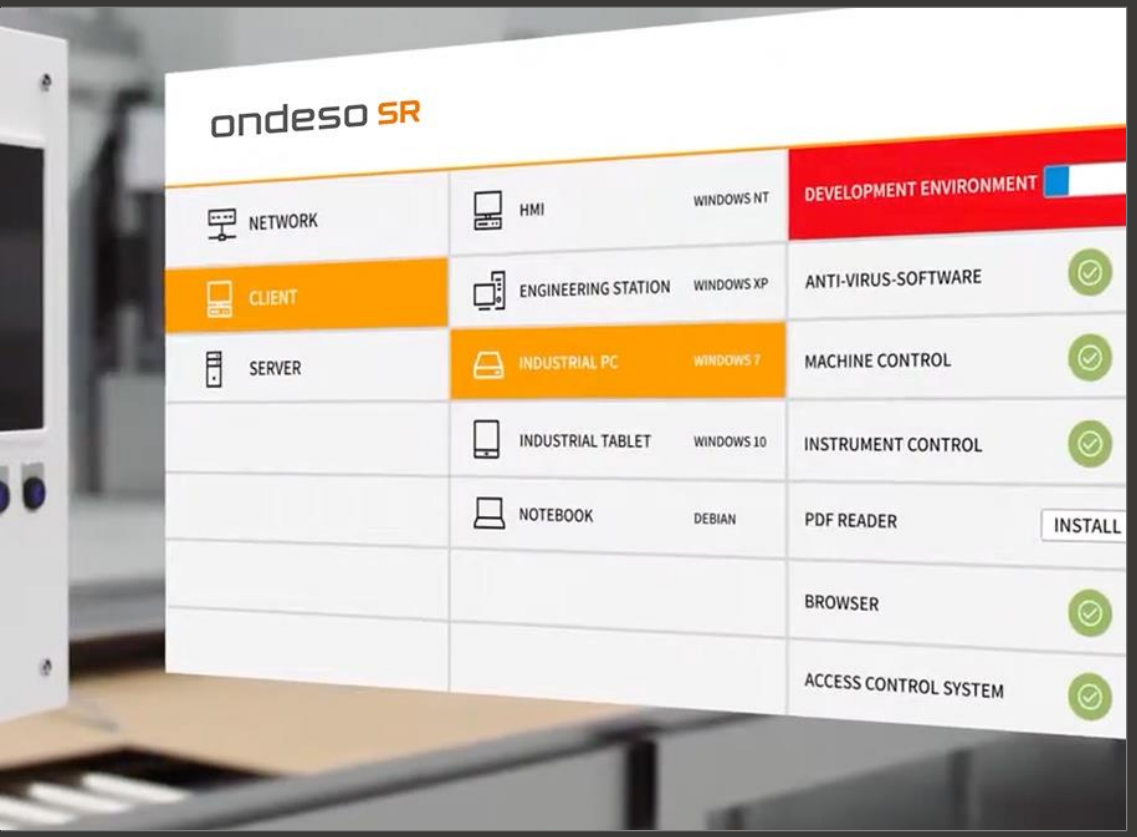
(z.B. Microsoft Intune, Azure Update Manager, …)

ABER: Cloud für OT-Umgebungen ungeeignet

- Kein Internetzugang
- Kein Domänenanschluss
- Heterogene Systemlandschaften

Was sind die Alternativen?

Patchen ohne WSUS: Eine mögliche Alternative

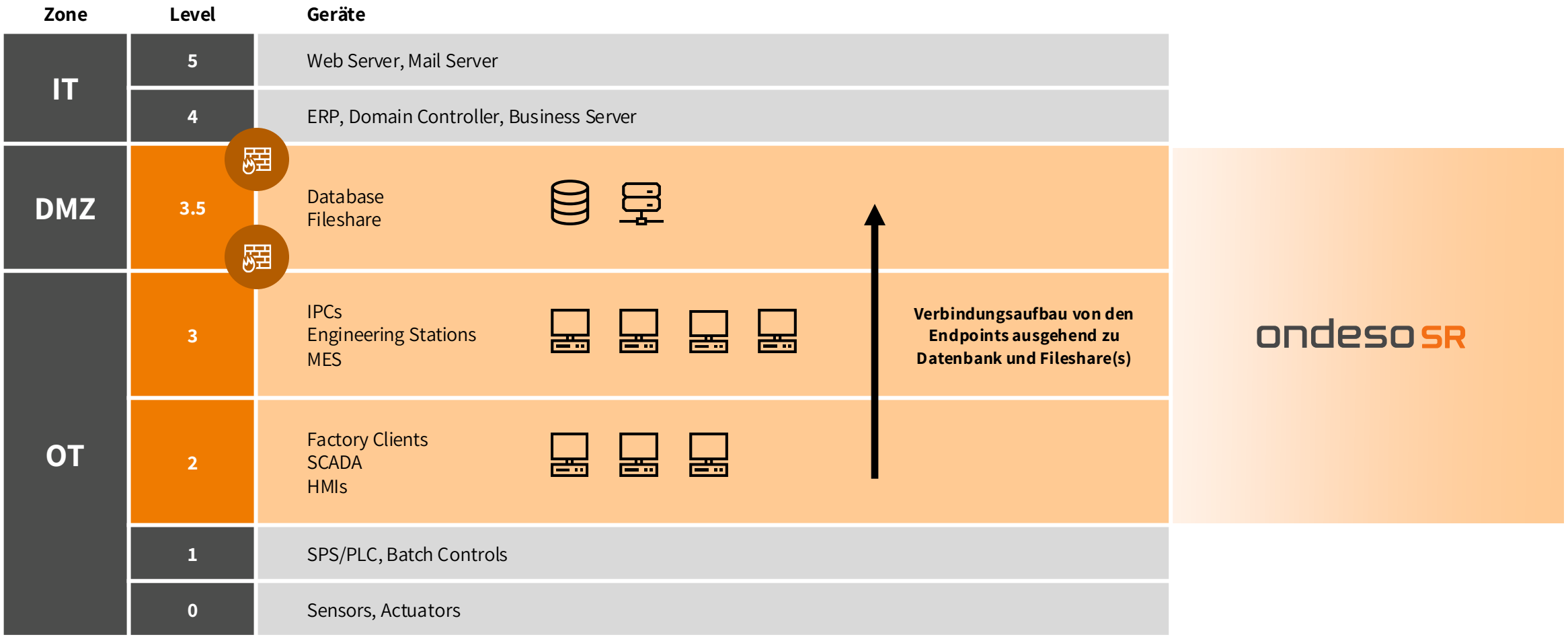


ondeso SR

Patch-Management-Software für OT-Umgebungen

- ✓ Client-Management ab Windows XP SP3
- ✓ Herstellerübergreifend einsetzbar
- ✓ On-Premise-Betrieb
- ✓ Ohne Active Directory und WSUS einsetzbar
- ✓ Updatelisten nach IEC 62443-2-3
- ✓ 100 % made in Germany

ondeso SR in der Purdue Enterprise Reference Architecture



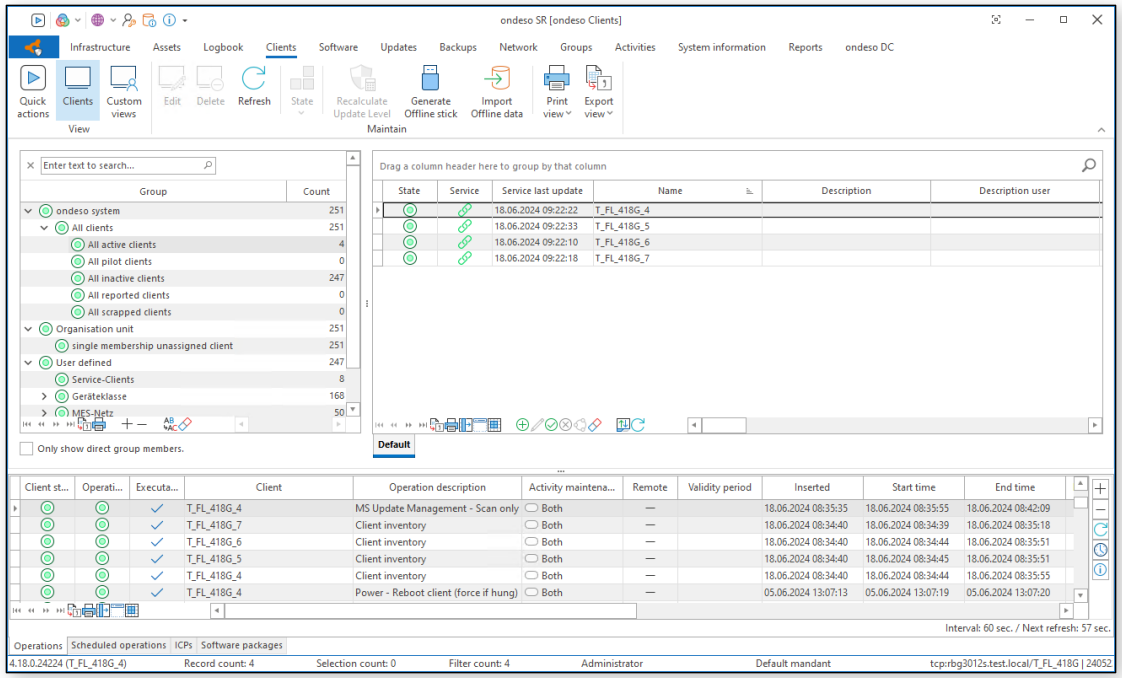
ondeso SR AdminGUI

So sieht es Instandhalter Karl

ondeso SR Start Center

So sieht es IT-Admin Max

ondeso SR AdminGUI

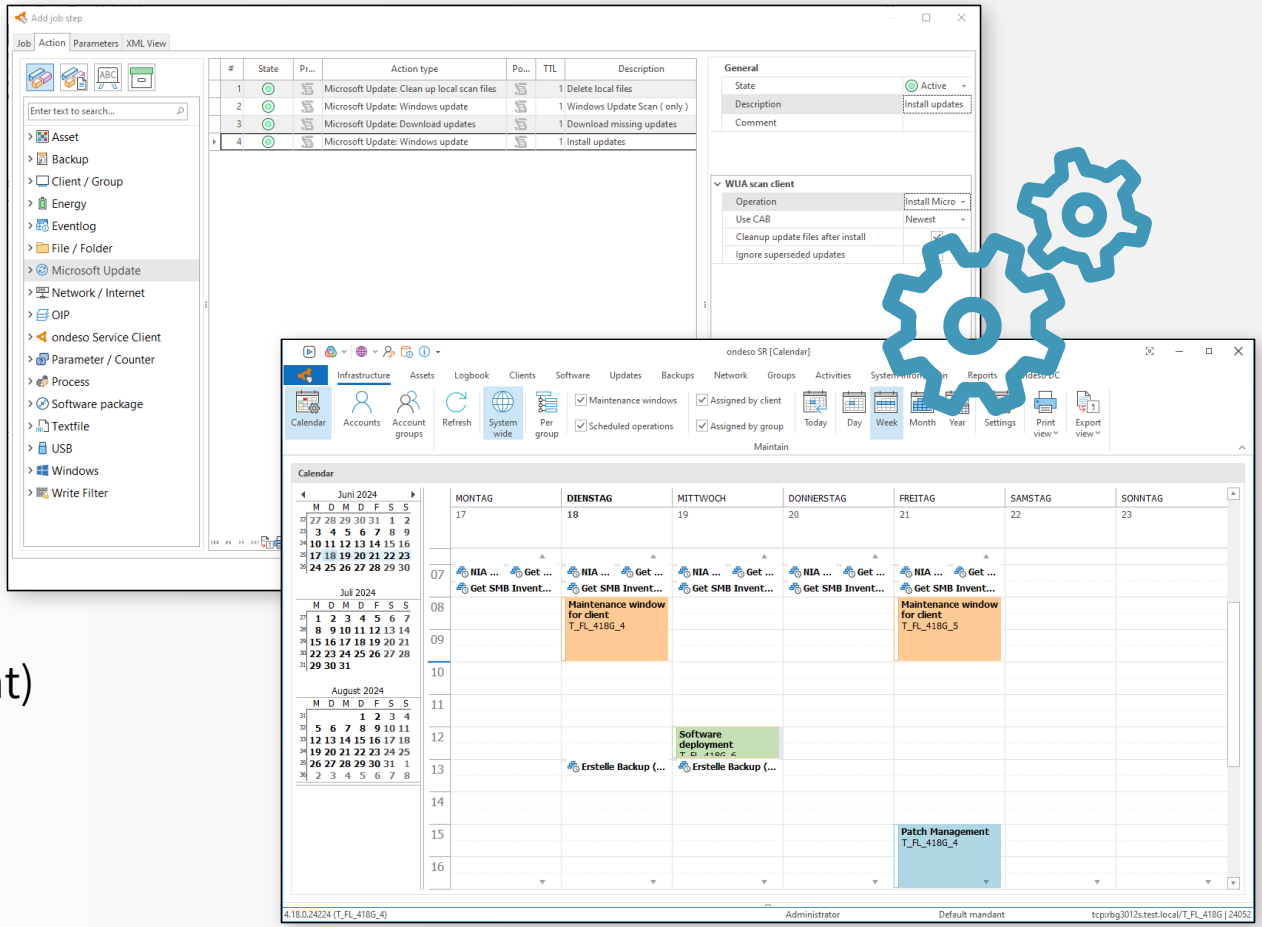


Workflow-Automation mit klarem Ziel

Sie bleiben handlungsfähig, ohne den Betrieb zu stören

Definieren Sie eigene Workflows und nutzen Sie die flexiblen Ausführungsmöglichkeiten

- ✓ Manuelle Ausführung per Knopfdruck
- ✓ In definierten Wartungsfenstern (geplant/ungeplant)
- ✓ Über regelmäßige Scheduler



Beispiel aus der Praxis

CVE-2017-0144

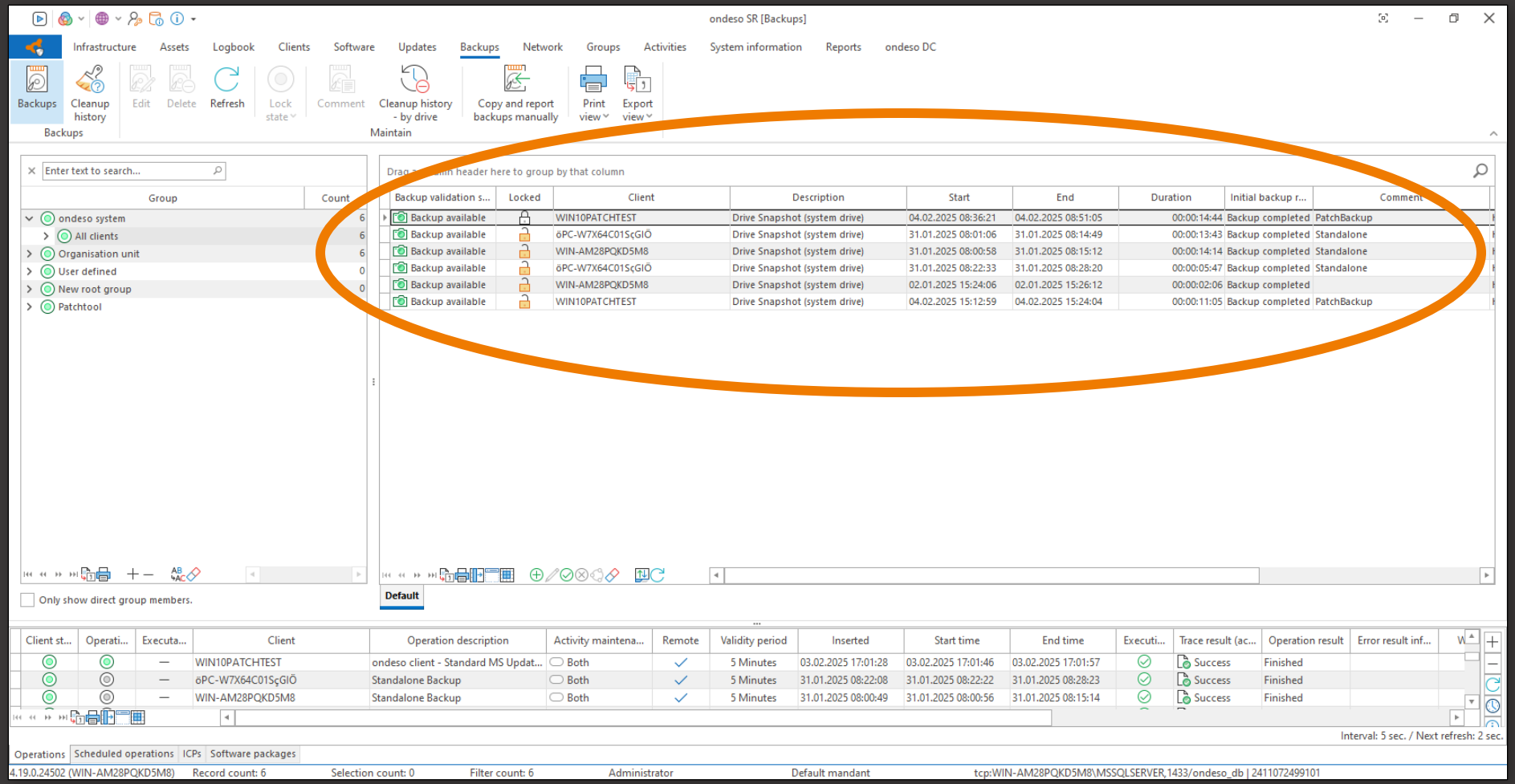
Patchten der EternalBlue-Schwachstelle mit ondeso SR

Beschreibung:	Schwachstelle im smb-Protokol
Angriffsvektor:	Remote Code Execution
Betroffene Geräte:	Windows XP, 7, 8, Server 2003/2008/2012, …
Ausgenutzt von:	WannaCry Ransomware (Mai 2017) NotPetya Wiper (Juni 2017
Gesamtschaden:	> 14 Mrd. USD

1.

Vorbereitende Maßnahmen durchführen.

Zum Beispiel Client-Backup

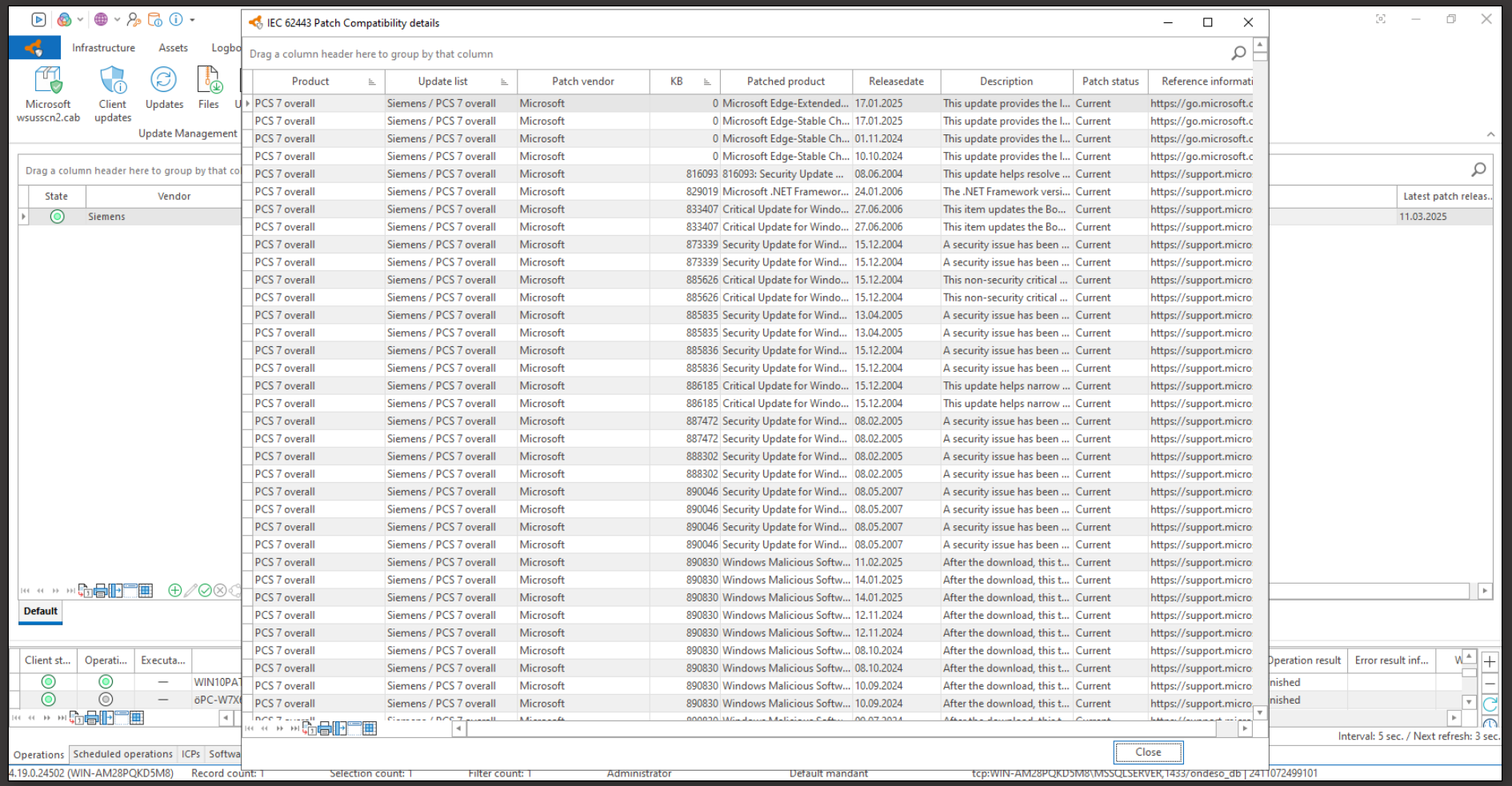


2.

Nach neuen Updates scannen.

Diese mit eigenen bzw. hersteller-bezogenen Freigabelisten abgleichen

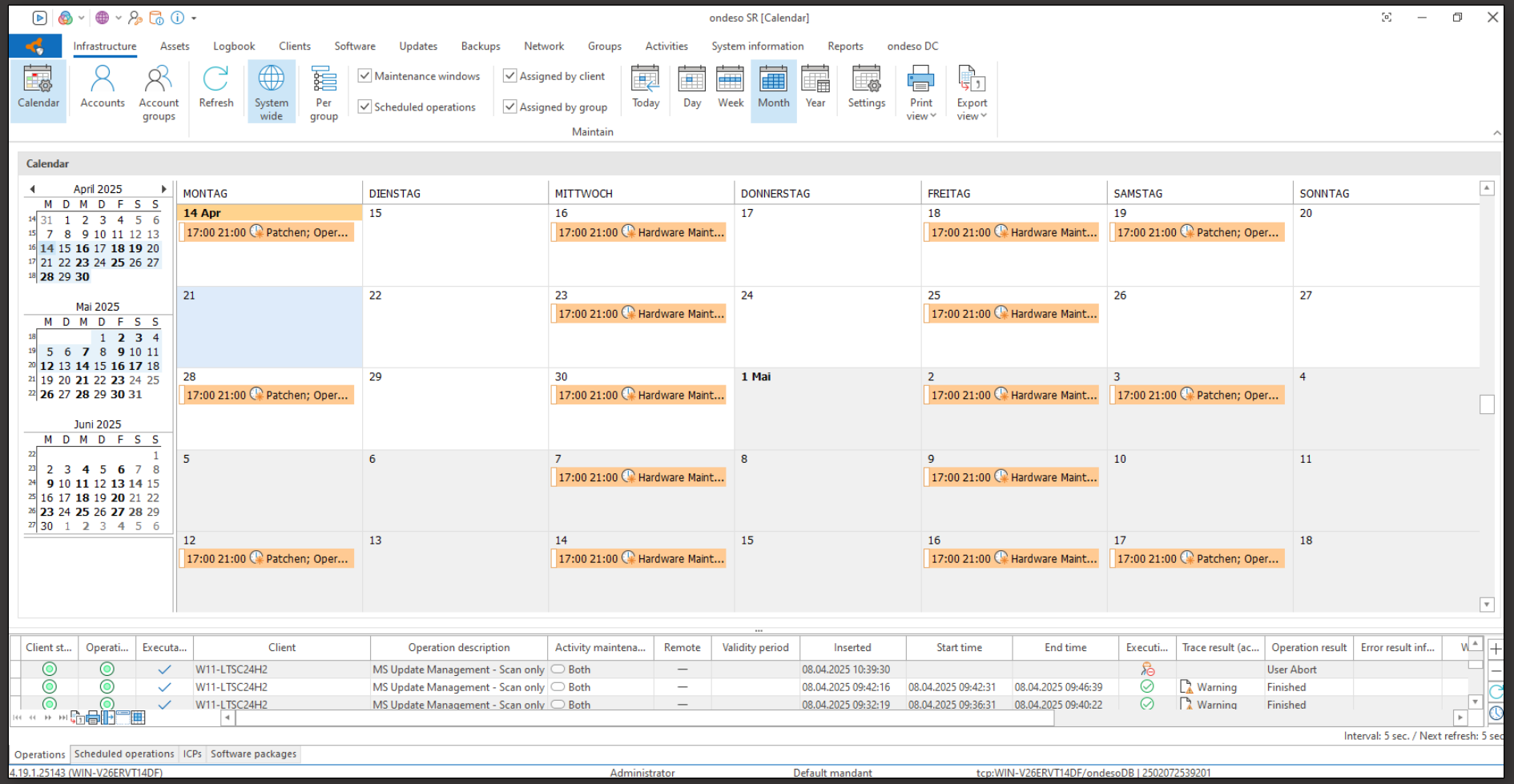
GOOD TO KNOW
ondeso SR ist derzeit das einzige Patch-Management-Tool mit offizieller Freigabe für Siemens SIMATIC PCS 7.



3.

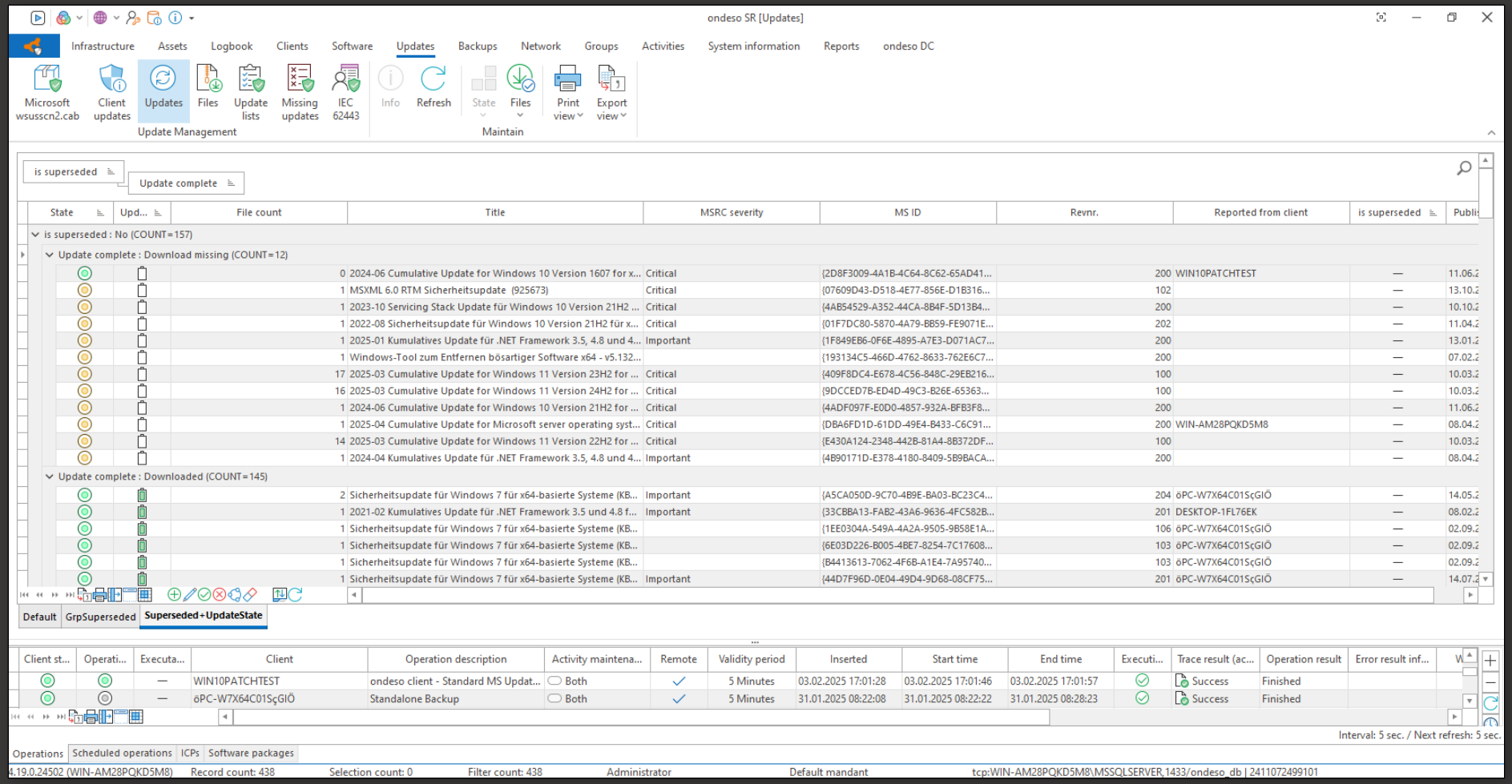
Zeitpunkt der Ausführung zuweisen.

Zum Beispiel automatische Ausführung während des nächsten freien Wartungsfensters



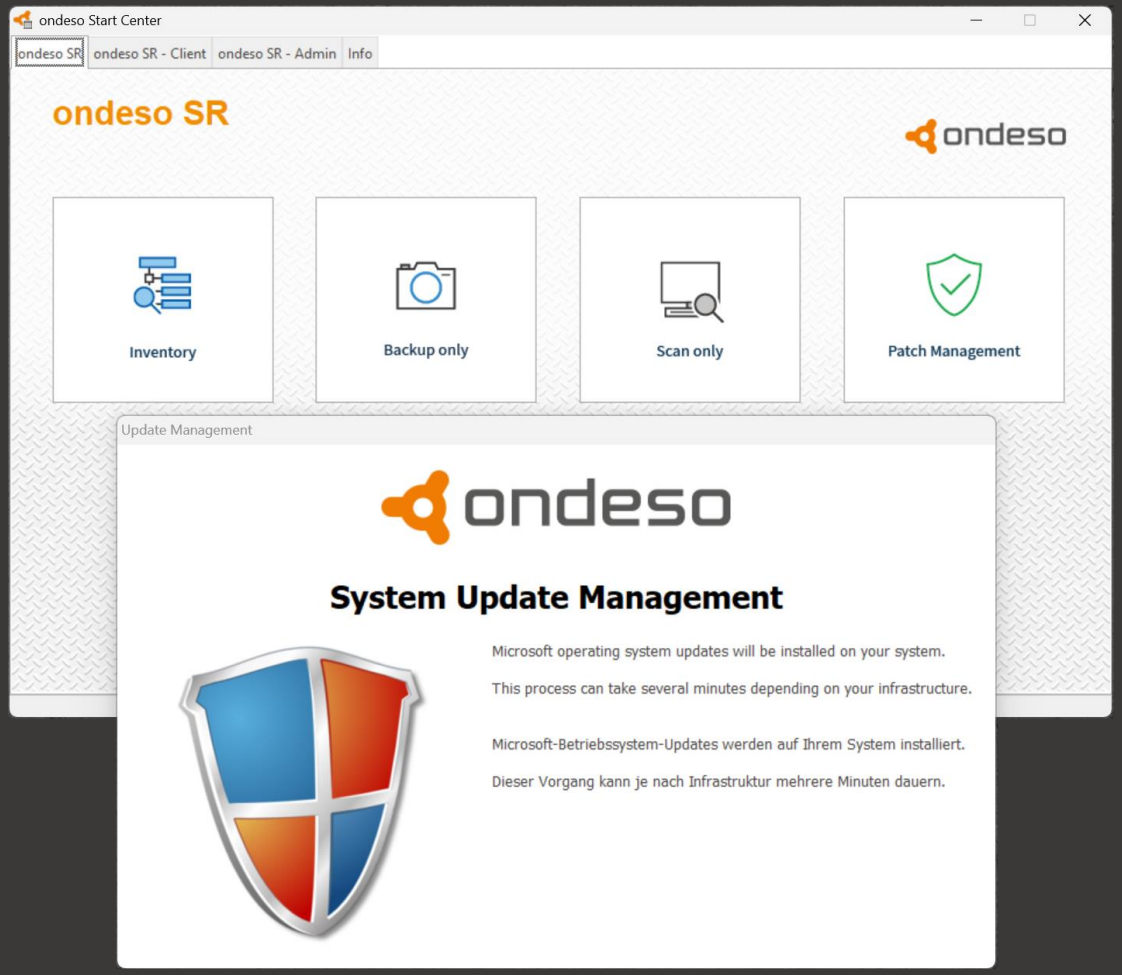
4.

Updates installieren



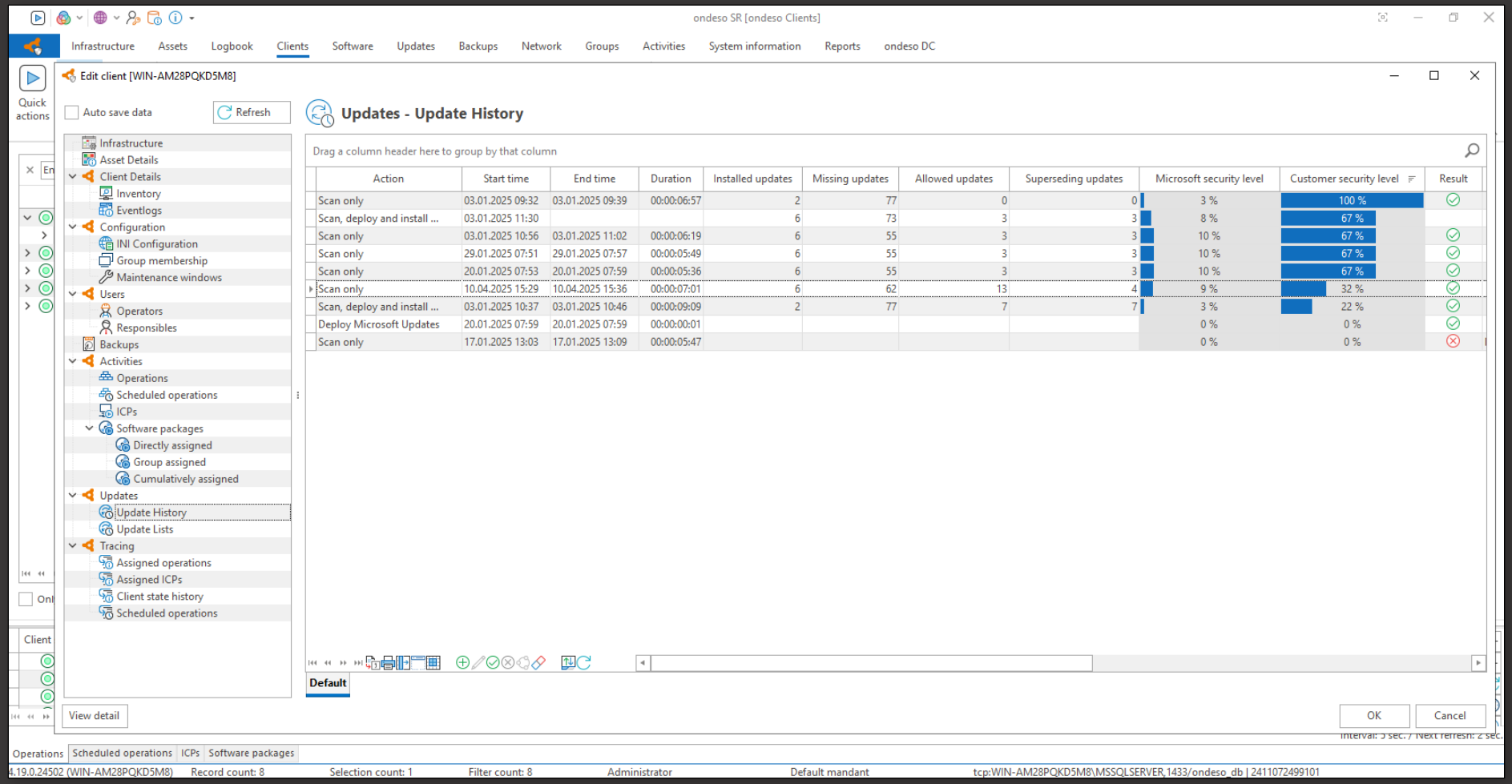
4.

Updates installieren



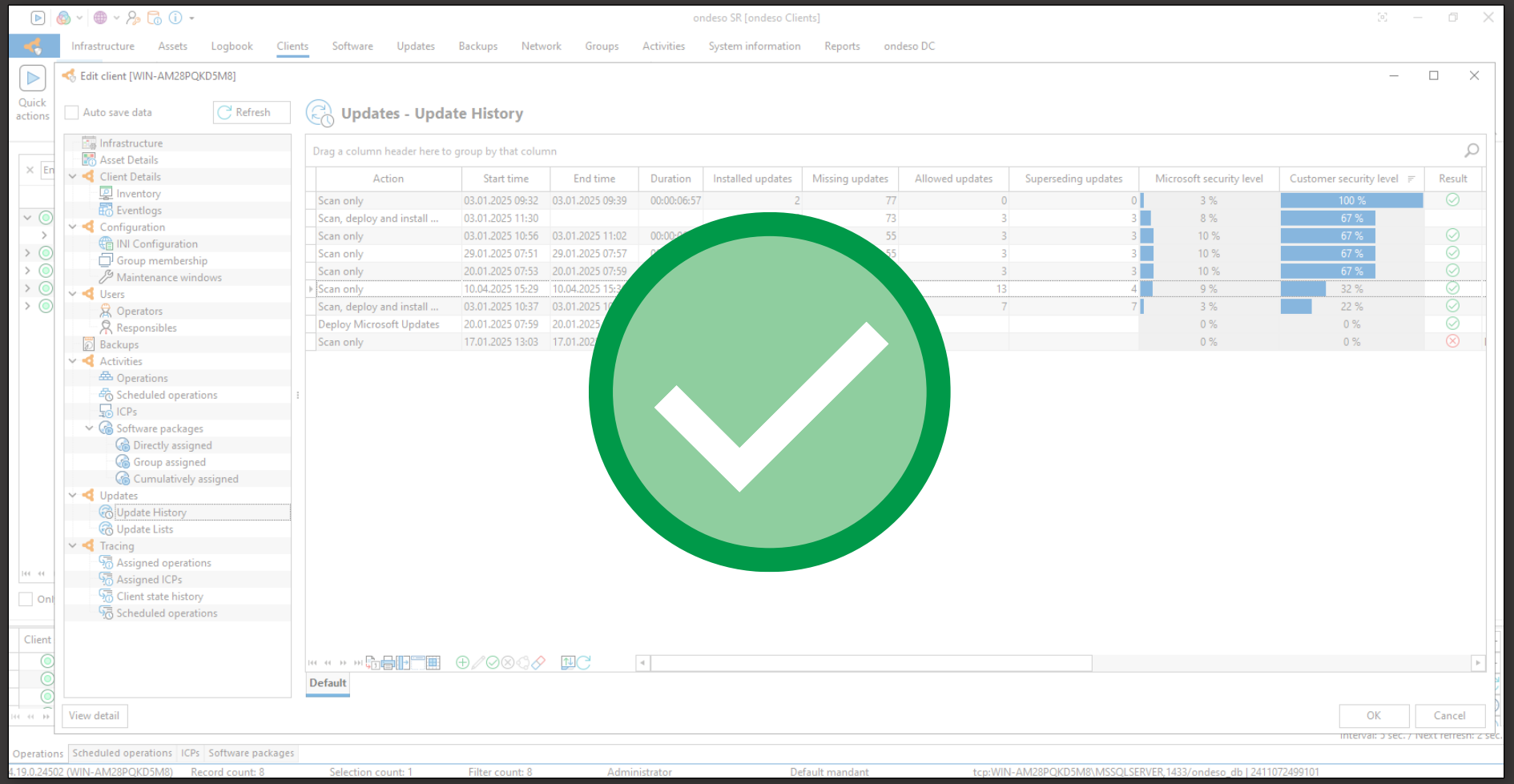
5.

Neues Updatelevel feststellen



6.

Schwachstelle gepatcht



Gestalten Sie Ihren OT-Alltag einfacher

✓ **Kontrolle behalten**
Permanente Client-Übersicht und Handlungsfähigkeit ab Windows XP SP3

✓ **Risiko minimieren**
Zentrale Umsetzung von Security-Maßnahmen mit On-Premise-Betrieb

✓ **Zeit sparen**
Entlastung dank Workflow-Automatisierung

Weitere Informationen

Direkt vom Speaker

itsa 365

Peter Lukesch, CEO

Online unter

www.ondeso.com

OT-Reifegrad-Check

Wo steht Ihr Unternehmen heute im Bereich Industrial IT und wohin kann es sich entwickeln?

- ✓ **Schnell & kostenlos – nur 15 Fragen**
- ✓ **Sofort-Ergebnis**
- ✓ **Praktische Tipps**

Jetzt starten und Überblick verschaffen!

https://ondeso-ot-reifegrad-check.scoreapp.com/p/itsa-pr

ondeso

BRINGING TOGETHER OT AND IT

ondeso GmbH · Osterhofener Str. 16 · 93055 Regensburg · phone: +49 941 462932-0 · email: info@ondeso.com

www.ondeso.com