Patch Management ist keine Raketen Wissenschaft mehr

Meine Erfahrungen und einfache Schritte

Jürgen Rinelli

Jürgen Rinelli Am Eichet 6a 85302 Alberzell info@success.eu.com

. P

Inhaltsverzeichnis

1. Ein paar Worte	1
2. Schritt für Schritt	2
2.1 Automatisiertes Test und Freigabeverfahren:	2
2.2 Automatische Verteilungen einrichten:	8
2.3 Überprüfung weiterer Schwachstellen im Thread Management:	15
2.4 Zeit für den Cappuccino – Dashboards prüfen:	18
3. About the Author:	22

1

1. Ein paar Worte

Als Senior Consultant sehe ich immer wieder Firmen, die gehackt wurden, und unterstütze diese beim Neuaufbau. Meist ist der Grund eine unzureichende oder nicht vorhandene Endpoint-Management-Strategie. Was früher noch mit viel Aufwand einherging, ist heute keine Raketenwissenschaft mehr.

Bei der Vielzahl an Cyberthreads und durch Nutzung von KI Technologien der Angreifer, werden Attacken immer intelligenter, schneller und anpassungsfähiger.

In diesem kleinen E-Book teile ich meine Best Practices für das Endpoint-Patch-Management und zeige wie einfach eine umfangreiche Patch-Strategie eingerichtet werden kann. Meine persönlich bevorzugte Lösung und Grundlage auf welcher die Screenshots und Einstellungen basieren, ist von ManageEngine.

Ich nutze und empfehle die EndpointCentral Security Edition, wobei meine Best Practices bezogen auf das reine Patchmanagement dieses mini E-Books, auch mit dem VulnerabilityManager Plus angewendet werden können.



"Patch-Management" und "Endpoint Security" sind Begriffe, welche sich heute keinesfalls mehr trennen lassen. Ich erzähle auch nichts Neues, wenn ich sage, dass es die Endgeräte sind, welche am anfälligsten für Cyberattacken sind. **Alle** Endgeräte – worunter ich auch die User zähle!

Während ich bei Usern ein "Patch-Management" nur über konsequente Schulungen durch gefakte E-Mails, Links, etc. durchführen kann – und sollte, lässt sich Hardware mit deutlich geringerem Widerstand und Aufwand patchen.

Was ist für mich wichtig und welche Schritte gehe ich beim Patch-Management?

- 1. Ich richte ein automatisches Test und Freigabeverfahren ein.
- 2. Ich richte **zwei** automatische Verteilungen der freigegebenen Patches ein.
- 3. Ich prüfe, welche Schwachstellen noch offen sind im Threat-Management und behebe diese.
- 4. Ich prüfe regelmäßig die Dashboards bei einer guten Tasse Cappuccino.

Nach diesem ersten einfachen Schritt der Patch-Automatisierung durch automatisches Testen und anschließender automatischer Verteilung, ist eine Grundsicherheit der Geräte gegeben. Das damit die Endpoints nicht komplett gesichert sind, habe ich schon erwähnt. Es gilt auch biologische Endpoints (User) an die Hand zu nehmen. Auf diesen Punkt gehe ich in einem separaten E-Book mit den Themen Device-Control, Applikation-Control, Data-Loss-Prevention, Anti-Ransomware und ganz wichtig – Browser Security ein.

Sollen wir loslegen?

2. Schritt für Schritt

2.1 Automatisiertes Test und Freigabeverfahren:

Da ein Patch auch zu unerwünschtem Verhalten führen kann, gebe ich Patches nur in den seltensten Fällen ungeprüft raus. Ja – besser wäre es, alles zu testen!

Um mir die Arbeit einfacher zu machen, gebe ich das Testen ab. Hierzu erstelle ich zuerst eine Testgruppe mit meinen eigenen Testgeräten sowie auch Geräten von Key-Usern. Also User aus jeder Abteilung, welche mit der Software täglich arbeiten. Mir ist es oft aus Lizenz und Berechtigungsgründen nicht möglich, Aktionen in der Software auszuführen. Oft kann ich die Software überhaupt nicht auf meinen Testgeräten installieren, wegen fehlender Lizenz. Also benötige ich User mit dieser Software welche auch Aktionen in dieser ausführen. Nur so kann sichergestellt werden das ein weiterführender Link z.B. zu einer Reader-Applikation, auch funktioniert. Bei den Key-Usern binde ich vor allem die User ein welche sich bisher auch schon häufig mit Fehlern

oder langsamen Systemen gemeldet haben. – Ich will ja Feedback und den möglichst schnell!

Wie eingangs bereits erwähnt zeige ich die Einrichtungsschritte exemplarisch an meinem Favoriten dem EndpointCentral UEMS von ManageEngine, denn einfacher und intuitiver habe ich es bisher in noch keiner anderen Endpoint Management Lösung auf dem Markt gefunden – und ich habe mit vielen gearbeitet in den letzten 25 Jahren.

Zuerst erstelle ich eine statische Computergruppe über Admin/Custom Group und packe alle Testsysteme und Key-User Systeme hinein.

😜 Endpoint Central Home Configurations Threats & Patches Software Deployment Inventory OS Deployment Mobile Device Mgmt Tools Agent Admin B

V Global Settings User Administration	Custom Group Syr	nc Settings Settings				
Custom Group	+Create New Group ▼	Filter By : Created By	▼ Group Cate	gory - Grou	р Туре 👻	
Domain	🖵 Computer الس	Group Type	Group Category	Members	Creation Time	Description
Rebranding	Luser User	Computers	Dynamic	NA	Feb 11, 2019 12:02 PM	
Mobile App	😭 Device Management T	Computers	Static	0	Nov 19, 2020 03:50 PM	
Self Service Portal Settings	C DLP Group	Computers	Static	1	Feb 24, 2023 07:25 AM	

C Endpoint Central Hor	me Configurations Threats & Patches S	Software Deployment Inventory	OS Deployment Mo	bile Device Mgmt	Tools Agent	Admin Browsers
✓ Global Settings User Administration	Custom Group > Create New Computer Group Create New Computer Group					
Custom Group	Name and Description					N
Domain						63
Rebranding	Group Name *	Pilot Gruppe	× 88	Add Description		
Mobile App	Category	Static ? St	atic Unique ? Dynar	mic ?		
Self Service Portal Settings	Membership	Assign Manually	AD Groups			
Credential Manager						
Custom Field	Select Computers					
Add Custom Data for Comput	Available Computers				Addeo	Computers (1)
SAML Authentication				Cont. of		•
Endpoint Security	Tree List Import			Sort -		
✓ SoM Settings	٩				٩	Search
Scope of Management	APP01-EM-TEST (em)					AD01-EM-TEST (em)
Agent Settings	EM-SRV-EXCO1 (em)					

Weiter gehts in Threads & Patches/Deployment/Test and Approve, um ein automatisches Test- und Freigabeverfahren einzurichten.

End 🤆	point Central Home	Configurations	Threats & Patches	Software Deployment	Inventory	OS Deployment	NextGen Antivirus
Dashboard	 Deployment Manual Deployment 	Patch A	pproval Status				
Threats	Test and Approve Automate Patch Deployment Disable Automatic Updates		Approve Patches	A	utomatically wit II the patches wi	hout testing Modify II be marked as "Appro	oved" automatically. If you
Patches	Security Configurations Software Uninstallation Deployment Policies	Арр	roval to Deploymen	nt Workflow	Test & Approv	Approval mode	ally/Manually
Beployment	Script Repository Trash		All Missi	ing Patches			

Dort stelle ich – falls noch nicht geschehen – den Patch Approval Status über den Modify-Button von "Automatically without testing" um auf "Test and Approve" und "Mark Patch as not Approved" um die bereits automatisch freigegebenen Patches sicherheitshalber auf nicht freigegeben, zu setzen.

	E DO YOU WAIL II
Patch Approval Status	
Approve Patches	O Automatically without testing O Test and Approve You can choose to create a test group, and test patches before deploying it to all the computers. Tested patches can be approved manually or you can choose to automate it.
For the Existing Patches	Retain Approval Status Mark Patch as Not Approved All the patches, except "Declined Patches" will be marked as "Not Approved".
	Save Cancel

Nach dem Speichern der Einstellung kann ich über "AddGroup" meine erste Testgruppe anlegen. Es können verschiedene erstellt werden für unterschiedliche Szenarien. Ich trenne Clients und Server auf jeden Fall voneinander. Ja – auch Server können zu einem gewissen Teil automatisch gepatcht werden.

Im ersten Schritt wähle ich die Plattform aus: Windows, Mac oder Linux

Dann wird die zuvor erstellte Gruppe benötigt – "Pilot Gruppe" in diesem Beispiel.

Test and Approve > Test group settings				
Test Group Deployment				
Define Task				
Platform *	🔾 Windows 🔷 Mac 🔷 Linux			
Group Name	Pilot Gruppe	*	C	Create Custom Groups

eployment Option				
Microsoft Updates				
Updates & Severities	Security Updates Optional Updates	Non Security Updates Select Updates	and Severities	
	Security Updates	Service Packs	<table-cell> Non Security Updates</table-cell>	
	Critical	Feature Packs	Critical	
Third Party Updates		🗹 Important		
	Moderate	Rollups	2 Moderate	
	Low	Preview Rollups	C Low	

In den "Deployment Options" wähle ich bei Microsoft Updates wie folgt:

Service Packs, Feature Packs und der Gleichen teste ich weiterhin manuell oder erstelle eine spezielle Testgruppe hierfür.

Bei Third Party Updates definiere ich alles.

Third Party Updates								
Updates & Severities	Critical	Important	Moderate	Low	Unrated	Select Updates and S	everities	
	🗹 All							
		Critical	~	Importa	nt	🗹 Moderate	🗹 Low	🗹 Unrated
Driver Updates								

Wenn ich aus den Auswahldialogen gehe, kann ich spezielle Anwendungen bei Microsoft Updates und Third Party Updates auch vom Patchen ausschließen. Z.B. spezielle VPN Lösungen, Workspace Applikationen, SQL, Java, etc.

	Critical Important Moderate Low Unrated Select Updates and Severities
	Patch All Applications Patch Specific Applications O Patch All Applications Except
	Search applications
	Show only Installed Applications
-	1Password
	3D XML Player (x64)
	4K Video Downloader
th the is ope	4K Video Downloader (x64)
	7 zip (.msi package)

Treiber Updates teste ich persönlich manuell oder teste diese über eine spezielle Gruppe an Geräten in einem weiteren Automatismus.

Deployment Criteria, damit kann ich eine Verzögerung definieren, also einen Zeitpunkt ab dem Patch-Release, ab welchem das Patch ausgerollt werden soll. Ich belasse das auf 0 Tage, da ich in eine Testgruppe verteile und ich eine Freigabe des Patches im späteren Verlauf, nicht noch länger hinausschieben möchte.

Ja – auch wenn es bedeutet, dass ein System u.U. einmal ausfallen kann! Dann setze ich das System einfach neu auf, kompromittiere damit aber nicht meine Gesamtsicherheit.

Deployment Criteria					
Only patches that have not been marked as Approved or Declined will be deployed to the Test Group					
Deploy patches after	0	~ ~	Days	from vendor release	

Im nächsten Schritt wähle ich die Deployment Policy – also das "Wann und Wie" der Verteilung.

Deployment Settings				
Apply Deployment Policy *	Pilot Gruppe Patches - Clients	•	C	View Details

Hier erstelle ich eine eigene Policy, um das Verteilungsfenster auch unabhängig anpassen zu können.

Also rauf auf "Create/Modify/Save As Policy", was mich in ein neues Tab, zu den Deployment Policies führt. Hier auf "Create Policy" gehen.



Aussagekräftigen Namen geben.

Deployment Policies		
Pilot Gruppe Patches - Clients		
1 Deployment Schedule	Template Name*	Pilot Gruppe Patches - Clients
2 Pre-deployment Activities	Description	
3 Pre-deployment user notification		Save Cancel
4 Post-deployment Activities	Ŧ	

Im Schritt 1 gebe ich das Zeitfenster an. Ich bevorzuge hier täglich wochentags (wenn die IT am Wochenende besetzt ist, dann auch Samstag und Sonntag), sowie zwei Zeitfenster, um auch auf flexiblere Arbeitszeiten zu reagieren. Man könnte jetzt fragen warum nicht gleich 24/7 patchen oder von 07:00 – 21:00 Uhr. Mein Gedanke bei einer festen Patch-Zeit ist, das ich auch die freundlichen Key-User nicht den ganzen Tag stressen möchte. Ich kann so den freundlichen Helfern eine fest Zeit geben in der die Patches installiert werden und sie können sich darauf einstellen. Die Mittagszeit bietet sich dazu auch am besten an.

Specify when patches/packages sh	ould be deployed to the client machines.		
Week Split type	Regular Split P Based on Patch Tuesday (Tue to next Mon) P		
Schedule Name	Preferred day(s)	Deployment Window	Actions
Schedule1	First, Second, Third, Fourth, Last - Mon, Tue, Wed, Thu, Fri	11:00 to 14:30	
Schedule2	First, Second, Third, Fourth, Last - Mon, Tue, Wed, Thu, Fri	17:00 to 21:00	

Patches lasse ich bereits Cashen wenn diese bereitstehen und verteilt werden soll zu jeder Zeit innerhalb des definierten Zeitfensters. So spare ich Bandbreite und Zeit.

Download patches from server to agent	Only during Deployment Window O Any time agent contacts the server The agent will not wait for the deployment window to download the patch binaries. The patch binaries will be downloaded in in the deployment window.
Initiate Deployment at	○ System Startup ○ Refresh Cycle
	Save & Continue Cancel

Nach "Save & Continue" kann ich Pre-deployment Activities definieren. Wake-on-Lan sollte ich eine Verteilung nachts durchführen wollen, Pre-Deployment reboot oder ein Custom Skript laufen lassen. In meinem Beispiel definiere ich nichts und gehe gleich auf "Save & Continue".

Deployment Schedule	Go Wake-on-LAN	🖒 Pre-Deployment reboot	😥 Custom Script	۵ 🖿
Pre-deployment Activities				
3 Pre-deployment user notification				
Post-denloyment &rtivities +		Save & Continue Cancel		

Schritt 3, bietet mir die Möglichkeit, die User vor der Verteilung zu benachrichtigen und ihnen ein Überspringen zu ermöglichen. Auch hier definiere ich nichts und gehe mit "Save & Continue" weiter. Wenn ich ein Überspringen der Installation erlauben würde, kompromittiere ich meine Sicherheit. Außerdem werden die User dann wieder mit einem Dialog genervt. Wir sind aus dem digitalen Mittelalter heraus, Patches laufen zu 95% ohne eine Unterbrechung im Hintergrund.

1 Deployment Schedule			Notify user(s) about Deployment (Windows and Linux only)
2 Pre-deployment Activities	+	Deployment Message Title *	Patch deployment notification
3 Pre-deployment user notification		Notification Message during Deployment*	Your Administrator has configured patches/software/service pack to be installed on this computer
User Notification		Notification timeout *	5 $\stackrel{<}{\sim}$ minute(s)
4 Post-deployment Activities	+		Allow Users to Skip Deployment Show deployment progress on the client systems

Schritt 4 und damit der Letzte bei der Definition der Deployment Policy, bietet mir die Möglichkeit einen Reboot oder Shutdown nach dem Deployment zu initiieren. Auch hiervon mache ich für den Fall der Key-User Pilotverteilung, keinen Gebrauch und gehe auf weiter mit "Save & Continue". Bei Feature und Server Packs und dergleichen, erstelle ich eine manuelle Verteilung, welche dann auch mit einem Hinweis auf einen Reboot versehen ist. Ich halte diese Art der Patches aus dem täglichen automatischen Testverfahren heraus.

1 Deployment Schedule	Post Reboot / Shutdown	Custom Script	۵ 🛤
2 Pre-deployment Activities +			
3 Pre-deployment user notification			
4 Post-deployment Activities +			
Drag and drop the action(s) in the sequence required		Save & Continue	Cancel

Nun erhalte ich noch einmal eine Übersicht und bestätige diese wieder mit "Save & Continue".

icy Name	\$	Pilot Gruppe Patches - Clients	
scription	1		
stall Option	1	During system startup or refresh cycle, whichever is earlier wi	hin the 'Deployment Window'.
utomatically wake computers before deployment	1	Disabled	
ownload Patches/Software during subsequent Refresh Cycle	:	Any time agent contacts the server	
loyment Schedule			
eferred Week(s) for Deployment	Preferred day(s) for D	Deployment	Deployment Window
I Weeks	Monday, Tuesday, W	fednesday , Thursday , Friday	11:00 to 14:30
Installe	Monday, Tuesday, W	ednesday, Thursday, Friday	17:00 to 21:00

Zurück im Tab mit der Testgruppe welche wir erstellen, wähle ich die Policy aus.

Deployment Settings			
Apply Deployment Policy*	Pilot Gruppe Patches - Clients	•	C View Details

Bleibt die Frage nach Benachrichtigungen im nächsten Schritt. Ich persönlich halte von der E-Mail Flut nicht viel. Diese landen in einem Ordner, welcher irgendwann gelöscht wird. Ich baue auf die Dashboards, welche mir übersichtlich zu jeder Zeit einen Status geben. Dort kann ich ggfs. den fehlerhaften Patches nachgehen.

Notification Settings : [Optional]		
Note: Notification will be sent, whenever a patch is approv	ved or a patch deployment has failed. Enable Notification	
E-mail address		
	[Multiple addresses to be separated by comma]	
Mobile app notification	Select technician(s) to be notified	

Letzter Schritt ist der Haken beim Approval Mode. Hier definiere ich drei Tage. **Mehr nicht** da ich ein weiteres Rollout der Patches nicht verzögern will. In den drei Tagen bis zur automatischen Freigabe der erfolgreich installierten Patches kann ich entweder über meine eigenen Programmaufrufe oder durch die Key-User in der Testgruppe eventuell ungewünschtes Programmverhalten identifizieren und diese Patches dann speziell ablehnen. Ein Patch sollte bei einer solchen Lösung nur dann automatisch freigegeben werden, wenn auf allen beteiligten Rechnern die Installation erfolgreich war. Bei EndpointCentral ist das gegeben. Wenn z.B. nur auf einem von 20 oder auch 100 Rechnern ein Patch mit einem Fehler antwortet, dann wird das Patch nicht freigegeben.

Approval mode for tested patches					
	 Automatically approve tested patches after 	3	$\hat{\cdot}$	Days	
	Patches that are successfully installed in at least one	of the mach	nines, and h	ave not faile	ed in any machine, will be approved. Learn More
			Create	Cancel	
			Greate	Sancer	

Ein Klick auf "Create" erstellt mir dann meine Testgruppe.

Pilot Gruppe		
Download Pending	: 0	
Not Approved	: 0	

2.2 Automatische Verteilungen einrichten:

Nun, da ich ein Test und Freigabeverfahren eingerichtet habe, erstelle ich das erste automatische Deployment für die restlichen Endpoints im Unternehmen. Ich beginne mit den Critical and Important Patches.

Hierzu in "Automate Patch Deployment" wechseln und "Automate Task/Windows".

	✓ Deployment					
Dashboard	Manual Deployment					
Ē	Test and Approve	Show Tasks OCre	ated by All	Created by N	1e	
Threats	Automate Patch Deployment	+ Automate Task 🔻	Actions -	Filter By :	Platform	,
Ē	Disable Automatic Updates	🚝 Windows			Deployment Time	
Patches	Security Configurations	📹 Mac	nd Important Pa	tches - Client	11:00 to 14:30 🗳	
Ģ	Software Uninstallation	∆ Linux	o_Autopatch_M	icrosoft_Tes	01:00 to 03:00 🖬	
Systems	Deployment Policies	🗌 🞜 Autopate	h_TP_AllOffices		22:00 to 06:00 🗳	
e	Script Repository	🗌 👪 Autopate	h MS all Office	s	19:00 to 05:00 🛂	
Deployment	Trash					
¥.						
Campliance						

MyTask291 🖋		
	Microsoft Updates	
Select Applications	Updates & Severities	Select Updates and Soverties
Choose Deployment Settings	Third Party Updates	
0	Updates & Severities	Select Updates and Severities.
Define Target	Anti-virus Updates	
Configure Notifications	Supported Definition Updates: Microsoft	Defention Update Defender, Microsoft Forefront Endpoint Security, Microsoft Forefront Endpoint Protection 2010 Server Management, Microsoft Forefront Endpoint Protection 2010 Server Management add, Microsoft Forefront Client
	Driver Updates	(f) And Control Bolds of Exceptionals, Control and Exceptional Soci- (1) And Control Bolds of Exceptionals, Control and Exceptional Soci- (1) And Control Bolds of Exceptional Control and Control
	On enabling this checkbox, you will be pro-	Driver Updates
	Deployment Only patches that are approved (Manu	al or Test & Approvel will be disclowed using Automate Patch Deployment Task
	Deploy patches after	0 🛎 Days *
		Next Cover

Der Dialog ist ähnlich aufgebaut wie der aus der Testgruppe.

Wir geben dem Kind einen Namen und eine Beschreibung.

MyTask290 🖌							
	Task Name *	Critical and Important Patches - Client					
Č Select A	Description	Windows & 3rd Party Patches					
22		Save Cancel					
Choose Dep Setting	loyment gs						
	1	Updates & Severities Sele	ect Updates and Severities				

Bei den Microsoft und Third Party Patches wähle ich jeweils die Critcal und Important aus und definiere eventuelle Ausnahmen für Software, welche nicht automatisch gepatcht werden soll.

Anti-Virus Updates überlasse ich der Virensoftware. Meiner Überzeugung nach sollte dies das Einzige sein, welches die Clients von selbst herunterladen können dürfen. So kann ich sichergehen, das Virenpatterns aktuell sind – auch in dem Falle der Agent auf dem System nicht mit dem EndpointCentral-Server kommunizieren kann und damit keine Updates gepusht werden.

Treiber Updates verteile ich persönlich manuell oder in einem separaten Automatismus.

Letzter Punkt auf dieser Seite ist der Zeitpunkt, wann das Patch verteilt werden soll. Da ich eine Verteilung nicht weiter verzögern will – wir haben bereits drei Tage aus dem Testverfahren – gebe ich hier null Tage ab Freigabe an. Außerdem kann ich auf diese Weise auch gerade erschienene High Critical Patches manuell testen und Freigeben. Durch meine manuelle Freigabe werden diese dann im automatischen Deployment sofort berücksichtigt. Ich muss hierfür dann keine separate Konfiguration erstellen – wieder Zeit gespart.

Microsoft Updates	
Updates & Severities	Security Updates [Critical,Important] Select Updates and Severities
	• Patch All Applications • Patch Specific Applications • Patch All Applications Except
Third Party Updates	
Updates & Severities	Critical Important Select Updates and Severities
	O Patch All Applications O Patch Specific Applications O Patch All Applications Except
Anti-virus Updates	
	Definition Update
Supported Definition Updates: Microsoft Defender, M Security, Microsoft Forefront Client Security x64, Mic	licrosoft Defender x64, McAfee Endpoint Security, Microsoft Forefront Endpoint Protection 2010 Server Management, Microsoft Forefront Security Essentials, Microsoft Security Essentials x64
Driver Updates	
	Driver Updates
On enabling this checkbox, you will be provided with t deployment or proceed with this operation because th	he latest updates for Drivers. The missing Driver patches are identified, downloaded and deployed to the computers which require t ne network services will temporarily stop.
Deployment	
Only patches that are approved (Manual or Test & A	Approve) will be deployed using A Days from release nt Task Days from approval
Deploy patches after	0 0 Days +
	Next Cancel

Weiter mit Next und ich gelange auf die Deployment Settings. Hier wieder über Create eine Neue erstellen. Keine Angst ... wir können die Deployment Policy, welche wir zuvor für die Pilot Gruppe erstellt haben, duplizieren. Hierzu einfach auf den Action Button der "Pilot Gruppe Patches – Clients" Policy gehen und "Save As New" klicken.

Deployment Option	🗿 Dep	oy ? Publish to Self Service Portal (S	;SP) ?			
Apply Deployment Policy *	Critic	al und Important Patches - Client 🛛 👻	C View Details	Crea		
Publish to Self Service Portal (SSP)	No	2				
					Delete	
Pilot Gruppe Patches - Clients	admrinelli	Jan 8, 2024 03:07 PM		admrinelli	Delete	
					Save As New	ŋ 1

Wieder umbenennen und speichern.

lot Gruppe Patches - Clients_Copy	1	х.,	
1 Deployment Schedule	Template Name *	Critical and Important Patches - Clients × 60	
2 Pre-deployment Activities	Description	-	
3 Pre-deployment user notification		Save Cancel	
Post-deployment Activities	Ŧ	Schedule 2 First, Second;	Third,F

Anschließend jeden Dialog mit "Safe & Continue" abspeichern. Wir behalten alle Zeiten und Einstellungen bei.

Zurück in das Tab mit der Automatischen Deployment Policy, können wir nach einem Klick auf den Refresh Button die eben erstellte Policy auswählen.

Deployment Option	O Deploy ? Publish to Self Service	Portal (SSP) ?
Apply Deployment Policy *	Critical und Important Patches - Client	✓ View Details Crea
Publish to Self Service Portal (SSP)	No (2	

Patches können auch im Self-Service-Portal bereitgestellt werden. In meinem Fall belasse ich es beim normalen Deployment. Das Self-Service-Portal bietet sich vor allem dann an, wenn ich Feature oder Servicepacks verteilen möchte. Auch bei OS-Upgrades nutze ich das SB Portal und gebe den Mitarbeitern so die Möglichkeit ein zeitintensiveres Patchen, selbst zu planen. Selbstverständlich gebe ich eine Deadline, zu welcher das Patchen dann erzwungen wird. Mir ist es wichtig, die User mit einzubinden.

Über "Next" gelange ich in die Ziele Definition.

Select Applications	Target 1	Remote Office/Domain	Choose either Remote Office or Domain					۲ 🛦
Choose Deployment Settings								
Define Target								
R				Previous	Next	Cancel		

Über das Targeting wähle ich ein Remote Office oder die Domäne, filtere nach den Systemen und exkludiere bestimmte Gruppen wie z.B. die Server Betriebssysteme oder Custom Groups, in welchen ich Systeme zusammengefasst habe, welche nichts **automatisiert** erhalten dürfen.

Filte	er Computers base	ed on					
Or	ganizational Unit	٣	Type & Select	h	6		
Excl	ude Target						
Op	perating System	-	Microsoft Windows Server 2022	Microsoft Windows Server 2019			
			Microsoft Windows Server 2016	Microsoft Windows Server 2012 R2			
			Microsoft Windows Server 2012	Microsoft Windows Server 2008 R2			
			Microsoft Windows Server 2008	Microsoft Windows Server 2003			
				li.			

Beim Klick auf "Next" gelange ich in den letzten Dialog mit den Benachrichtigungen. Auch hier sind E-Mail und Mobile-App Benachrichtigungen möglich. Ich selbst belasse es auch hier bei den Dash-Boards und klicke auf "Save" ohne weitere Auswahl.

Select Applications	Notification emails will be triggered only when there is a change Notify Download/Deployment Failure for every	in the status of Automate Patch Deployment Task
Choose Deployment Settings	Notify Deployment Status Report for every Attach Detailed Report	hour(s)
Define Target	Email*	mple@mydomain.com
	Mobile app notification Se	act technician(s) to be notified
Configure Notifications		Previous Save Cancel

Trommelwirbel bitte ... fertig ist unsere erste von zwei automatischen Verteilungen.

Show Tasks Created by All Created by Me					
+ Automate Task Actions Filter By:	Platform •				
Name	Deployment Time	Created Time	Current Status	Action	
Critical and Important Patches - Client	11:00 to 14:30 🗳	Jan 8, 2024 03:54 PM	No targets available		

Nun dupliziere ich diese über den Action Button mit allen Zielen um auch die restlichen Patches von Medium abwärts, zu verteilen.

116	Modify	>	ction	
us	Save As New	>	Without Target	
ailable	Suspend Task		With All Targets	վեղ
	Delete Task			0

Kurz umbenennen.

Critical and Important Patche	es - Client_Copy	·		
0=	Microsoft Up	Task Name *	Medium and Lower Patches - Clients	1
Select Applications	Updates & S	Description	Windows and 3rd Party Patches	ł
ŝ			Save Cancel	cej
Choose Deployment Settings	Third Party Up	dates		

Patches auswählen für Microsoft Updates. Optionale Updates verteile ich wie die Service und Feature Packs separat. Entweder in einem speziellen Automatismus oder über eine manuelle Konfiguration. Hier könnte sich ein monatlicher Zyklus anbieten.

Microsoft Updates			\$
Updates & Severities	Security Updates [Moderate,Low,Unrated]	Non Security Updates	Select Updates and Severities
	Security Updates	Service Packs	Non Security Updates Critical
Third Party Updates	☐ Important ✓ Moderate	Feature Packs Rollups	Moderate
Updates & Severities	Cow Conrated	Preview Rollups Optional Update	S Low Unrated

Gleiches gilt für die Third Party Patches.

Third Party Updates	
Updates & Severities	Moderate Low Unrated Select Updates and Severities
	Patch All Applications Patch Specific Applications Patch All Applications Except

Nach dem Klick auf Next gelangen wir zu den Deployment Settings. Hier erstellen wir wieder eine Neue, da ich diese zum Zeitpunkt dieses Buches nur zwei Mal pro Woche verteile. Also wieder auf "Create/Modify/Save As Policy" gehen.

Ich dupliziere die Critical and Important Patches – Client Policy, benenne diese um und definiere zu denselben Uhrzeiten lediglich Dienstag und Donnerstag als Verteilungstage. Der Rest bleibt wie gehabt und ich klicke durch alle Dialoge mit "Save & Continue".

Medium and lower Patches - Clients 🖌					
Deployment Schedule		Specify when patches/packages s	hould be deployed to the client machines.		
2 Pre-deployment Activities	+	Week Split type	Regular Split P Based on Patch Tuesday (Tue to next Mon) P		
3 Pre-deployment user notification		Schedule Name	Preferred day(s)	Deployment Window	Actions
		Schedule 1	First , Second , Third , Fourth , Last - Tue , Thu	11:00 to 14:30	
4 Post-deployment Activities	+	Schedule 2	First, Second, Third, Fourth, Last - Tue, Thu	17:00 to 21:00	

Zurück in unseren Automatismus Tab kann ich nach einem Refresh die neue Policy auswählen und bestätige alle weiteren Dialoge ohne Änderungen.

Deployment Option	Deploy Publish to Self Service Portal (SSP) ?		R
Apply Deployment Policy*	Medium and lower Patches - Clients	C View Details Create/Modify/Save As Policy	
Publish to Self Service Portal (SSP)	No ?		
Preferred Week(s) for Deployment		Preferred day(s) for Deployment	Deployment Window
First , Second , Third , Fourth , Last		Tuesday , Thursday	11:00 To 14:30
First, Second, Third, Fourth, Last		Tuesday , Thursday	17:00 To 21:00

Im Anschluss habe ich meine zwei Automatismen, welche mir alle freigegebenen Patches im Unternehmen ausrollen.

Show Tasks Created by All O Created by Me						
+ Auto	mate Task Actions Filter By:	Platform •				
	Name 🌻	Deployment Time	Created Time			
	Critical and Important Patches - Client	11:00 to 14:30 🗗	Jan 8, 2024 03:54 PM			
	Medium and Lower Patches - Clients	11:00 to 14:30 🖸	Jan 8, 2024 04:07 PM			

Über die Statusanzeigen kann ich den Verlauf kontrollieren und ggfs. den fehlerhaften Verteilungen nachgehen.

Show	Show Tasks O Created by All Created by Me						
+ Auto	omate Task Actions Filter By:	Platform 🔻					
	Name 💂	Deployment Time	Created Time	Current Status	Action		
	Autopatch_MS_all_Offices	19:00 to 05:00 🖬	Oct 30, 2019 01:33 PM	13 1			
	Autopatch_TP_AllOffices	22:00 to 06:00 🖪	Oct 30, 2019 01:34 PM	7 3 4			
	🛿 Critical and Important Patches - Client	11:00 to 14:30 🖪	Jan 8, 2024 03:54 PM	No targets available			
	& EM_Demo_Autopatch_Microsoft_Tes	01:00 to 03:00 🖪	Aug 23, 2023 12:55 PM	3			
	😝 Medium and Lower Patches - Clients	11:00 to 14:30 🖸	Jan 8, 2024 04:07 PM	No targets available			

Noch ein Tipp! Wenn ich in Kundenumgebungen komme, in welchen es bisher die Speedy Gonzales Turnschuh-Administration gab, sehe ich mir zuerst die Menge an fehlenden Patches in der Übersicht an. Sind es zu viele, erstelle ich zwar beide Automatismen wie oben beschrieben, suspendiere jedoch die für Medium and Lower Patches. Ich lasse die ersten zwei Wochen **allein** die Critical and Important Patches ausrollen. Auf diese Art werden die Systeme und mein Netzwerk nicht überstrapaziert. Ich lasse sozusagen etwas Druck ab.

2.3 Überprüfung weiterer Schwachstellen im Thread Management:

Es gibt neben der normalen Patches auch eine Menge an weiteren Schwachstellen, um welche ich mich kümmern darf. Misskonfigurationen, Zero-Day Schwachstellen, offene Ports, Web-Server Misskonfigurationen, etc.

In der EndpointCentral Security Edition sowie im VulnerabilityManager Plus, ist hierzu ein zusätzlicher Bereich "Threats" geschaffen worden.

Hier finde ich noch einmal in Kategorien einteilbar eine Übersicht über meine noch offenen Schwachstellen inclusive ausführlicher Beschreibung und CVE Scores. Kann hier auch Ausnahmen definieren und/oder die Schwachstellen beheben.

✓ Threats	Summary View Detailed View		
Software Vulnerabilities	This table enumerates the vulnerabilities de	ected in Windows and Linux operating systems as well as third-party applications. View the complete list of all the vulnerabilities supported.	
Detected CVEs Zero-day Vulnerabilities System Misconfigurations	Q+ Search by EVE ID: EVE 30000300000	Ð	
Web Server Misconfiguration	Postgresql	55 V Critical Update Postgresql 11.5 fixes multiple vulnerabilities	* Manual Resolution
Port Audit Managa Exceptions	Image: Tomcat Java St Davelogment Kit (vd4) Coople Chrome Mysol Mysol Apsche Coople Chrome (vd4) Python Python	50 Citized Vulnerabilities CVE-2020-25696;CVE-2020-25694 are fixed in PostgreSQL 9.6.20 36 CVE 00 CVE 00 CVE 000-25996;CVE-2020-25994 31 CVE 3200-25996;CVE-2020-25994 CVE 000-25996;CVE-2020-25994 31 CVE 3200-25996;CVE-2020-25994 CVE 000-25996;CVE-2020-25994 31 CVE 3200-25996;CVE-2020-25994;CVE-2020-25994 CVE 000-25996;CVE-2020-25994 32 Repidet Status CVE 000-25996;CVE-2020-25994;CVE-2020-25994 33 No knownedlets available for this vulnerability CVE 000-25996;CVE-2020-25994;CVE-2020-2594;CVE-2020-2594;CVE-2020-2594;CVE-2020-2594;CVE-2020-2594;CVE-2020-2594;CVE-2020-2594;CVE-2020-2594;CVE-2020-25994;CVE-2020-25	No Solution
	Nainy	Critical Vulnerabilities CVE-2020-25696,CVE-2020-25695,CVE-2020-25694 are fixed in PostgreSQL 9.5.24	No Solution
	Curl For Windows	Critical Vulnerabilities CVE-2019-10211,CVE-2019-10210,CVE-2019-10208 are fixed in PostgreSQL 9.4.15	No Solution

Es gibt auch einen Bereich, welcher Zero-Day Schwachstellen aufzeigt, und ich kann entsprechend handeln.

Threats Software Vulnerabilities Detected CVEs	Summary View Detailed View This view displays zero day vulnerabilities like Wannacry, Melidown and Spectre, etc. that are present in you Filter By: Threat Category Platform w	r network,		
Zero-day Vulnerabilities	Threats	Threat Category	Affected Systems	Action
System Misconfigurations	Vulnerabilities CVE-2023-7024 are fixed in Google Chrome (120.0.6099.129, 120.0.6099.130)	CVE-2023-7024	1	* Fix
High Risk Software Web Server Misconfiguration	Vulnerabilities CVE-2023-7024 are fixed in Google Chrome (x64) (120.0.6099.129, 120.0.6099.130)	CVE-2023-7024	1	* Fix
	Windows Media Remote Code Execution Vulnerability for Windows Server 2016 for x64-based Syste	CVE-2023-20588	1	* Fix
Port Audit	Vulnerabilities CVE-2023-3079 are fixed in Google Chrome (114.0.5735.110)	CVE-2023-3079	2	* Fix
Lonale Exchange	Vulnerabilities CVE-2023-2133.CVE-2023-2134.CVE-2023-2135.CVE-2023-2136.CVE-2023-2137 a	CVE-2023-2136	1	¥ Fix
	Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2022-41082)	CVE-2022-41082	1	No fix available
	Microsoft Exchange Server Elevation of Privilege Vulnerability (CVE-2022-41040)	CVE-2022-41040	1	No fix available
	GhostCat: Vulnerabilities CVE-2020-1938,CVE-2020-1935,CVE-2019-17569 are fixed in 11 Februar	GHOST_CAT_VULNERABILITY	1	No fix available
	· · · · · · · · · · · · · · · · · · ·			1 - 8 of Total

Im Bereich "System Misconfigurations" schließe ich, was mir möglich ist oder definiere Ausnahmen. Natürlich kann vieles davon über die Active Directory konfiguriert werden. Ich kann die Ergebnisse dieser Überprüfung nutzen und ggfs. direkt in der AD konfigurieren.

	Commencial Commencial	ealed View				
Software Vulnerabilities	This table enumerates the s	ecurity misconfigurations detect	ed in Windows and Linux machines. View the co	mplete list of all the misconfiguration supporte	d. D	
Detected CVEs	GFix thAdd Except	lons Filters	•			Total Records Q, III .
Zero-day Vulnerabilities	Misconfiguratio	NT .	Category	Affected Systems	Reboot Required	Action
System Misconfigurations	Administrate	ve Shares enabled	Share Permission Management	13	Not Required	No focavailable
High Risk Software Web Server Misconfiguration	Geolocation	is enabled to track users physical	 Chrome Security Hardening 	10	Not Required	. Deploy Secure Configuration
Port Audit	TLSv1.1 prot	ocol is enabled	SSL and TLS Security	13	Required	No fix available
Manage Exceptions	The Server M	tessage (llock (SMIR) v1 protocol	Legacy Protocols	1	Not Required	Copiloy Secure Configuration
	Windows Cre	edential Guard has been found d	OS Security Hardening	13	Required	No for available
	Insecure RC4	I cipher algorithms are not disabl		2	Required	No focavailable
	C Administrato	v accounts are enumerated duri.	Logon Security	13	Not Required	Deploy Secure Configuration
	User rights g	ranted to everyone group	Account Privilege Management	13	Not Required	No fix available
Software Vulnerabilities	This table enumerates the	e security misconfigurations de				
Detected CVEs Zero-day Vulnerabilities			tected in Windows and Linux machines. View t	he complete list of all the miscoofiguration su	pported	
Detected CVEs Zero-day Vulnerabilities System Misconfigurations	Chrome Security	y Hardening 15	ected in Windows and Linux machines. View t	he complete list of all the miscorriguration su	pported	Cheploy Secure Configurati
Detected CVEs Zero-day Vulnerabilities System Misconfigurations High Risk Software Web Server Misconfiguration	Chrome Security	y Hardening 15 unity 6	Info Geolocation is enabled Moderate Finewall traversal from	he complete bit of all the misophypication so I to track users physical location remote host is not disabled	pporred.	¥ Dieploy Secure Configurati ¥ Dieploy Secure Configurati
Detected CVEs Zero-day Vulnerabilities System Misconfigurations High Risk Software Web Server Misconfiguration Port Audit	Chrome Securit	y Hardening 15 urity 6 ull 6	 Info Geolocation is enabled Moderate Firewait traversal from Moderate Automatic update of C 	he complete bit of all the miscooff-guration so I to track users physical location remote host is not disabled hrome browser is not enabled	pported.	### ** Disploy Secure Configurati ** Disploy Secure Configurati ** Disploy Secure Configurati
Detected CVEs Zero-day Vulnersbillties System Misconfigurations High Risk Software Web Server Misconfiguration Port Audit Manage Exceptions	Chrome Security SSL and TLS Sec Windows Firewa OS Security Han Psyceptref dailoru	v Hardening 15 urity 6 all 6 dening 5	Info Geolocation is enabled Moderate Finewall traversal from Moderate Automatic update of C Moderate Chrome minimum TLS:	he complete bit of all the misconfiguration so I to track users physical location s remote host is not disabled hrome browser is not enabled //SSL connection must configured to TLS 1.	pporred.	Beplay Secure Configurati W Deplay Secure Configurati W Deplay Secure Configurati W Deplay Secure Configurati W Deplay Secure Configurati
Detected CVEs Zero-day Vulnerabilities System Misconfigurations High Risk Software Web Server Misconfiguration Port Audit Manage Exceptions	Chrome Securite Statund TLS Security Windows Freewill G OS Security Han Password Policy Network securit Network securit	v Hardening 15 unity 6 ull 6 dening 5 y 3	Info Geolocation is enabled Moderate Firewall traversal from Moderate Automatic update of C Moderate Chrome minimum TLS: Moderate Websites must be prev	he complete bit of all the inscool guration to to track users physical location remote host is not disabled hrome browser is not enabled //SSL connection must configured to TLS 1. vented from accessing USB devices	pported.	Beploy Secure Configuratio Configuratio Deploy Secure Configuratio Configuratio Configuratio Configuratio Configuratio Configuratio Configuratio Configuratio
Detected CVEs Zero-day Vulnersbillties System Misconfigurations High Risk Software Web Server Misconfiguration Port Audit Manage Exceptions	Chrome Securit Chrome Securit SSL and TLS Security Han Chrome Security Han Password Policy Network security Chrome Security C	y Hardening 15 unity 6 all 6 dening 5 y 3 a	Info Geolocation is enabled Moderate Firewail traversal from Moderate Automatic update of C Moderate Obrome minimum TLS: Moderate Websites must be prev Moderate Anonymized URL-large	he complete bit of all the inscool guration to to track users physical location remote host is not disabled hrome browser is not enabled VSEL connection must configured to TLS 1. vented from accessing USB devices d data collection by Google must be disabl	pported.	Deploy Secure Configuratio Secure Configuratio Secure Configuratio Secure Configuratio Secure Configuratio Secure Configuratio

Dann sehe ich nach ob es abgelaufene Software unter "High Risk Software" gibt bzw. wann vorhandene Software ihr Laufzeitende erreicht. Ein Thema, welches oft vernachlässigt wird und "urplötzlich" auftaucht.

Moderate Chrome background apps running con

Moderate Importing of saved passwords is not disabled

He Anonymous browser usage and crash-related data col

rate Chrome password manager is not disabled

Moderate Cloud print sharing via Chrome is not disabled

ow Third party cookies must be blocke

on by Google is not disa

Moderate Ensure browser history is saved

" Moderate Pop-ups must be blocked

Share Permission Management

Account Privilege Management

😫 Internet Explorer Hardening

Antivirus Protection

BitLocker Encryption

Legacy Protocols

Luser Account Management

Linux - Password Policies

Linux - User Account Ma

2

2

2

1

1

1

1

0

~ Mode

✓ Threats	Summary View Detailed View							
Software Vulnerabilities	End Of Life (14) Peer to Peer (0) Remote Desktop Sharing (0)							
Detected CVEs								
Zero-day Vulnerabilities	This view usprays all the sortware in the network who	na view objekty ali the software in the network whose expiry because are available.						
System Misconfigurations	Filters				Tota			
High Risk Software	Software Name	Vendor	Expiry Date	Days to Expire	Affected Systems			
Web Server Misconfiguration	Microsoft Visual C 2008 Redistributable (x86)	Microsoft	Apr 9, 2013	Expired	5			
Port Audit	Microsoft Visual C++ 2010 Redistributable (x64)	Microsoft	Jul 10. 2015	Expired	1			
Manage Exceptions	Microsoft Visual C++ 2010 Redistributable (x64)	Microsoft	Jul 10, 2015	Expired	4			
	Microsoft Visual C++ 2010 Redistributable (x86)	Microsoft	Jul 10, 2015	Expired	1			
	Microsoft Visual C++ 2010 Redistributable (x86)	Microsoft	Jul 10, 2015	Expired	4			
	Microsoft Visual C++ 2008 Redistributable (x64)	Microsoft	Apr 10, 2018	Expired	4			
	Windows Server 2016 Datacenter Edition (x64)	Microsoft	Jan 10, 2022	Expired	1			
	Microsoft SQL Server 2017 Developer Edition (x.,	Microsoft	Oct 11, 2022	Expired	1			
	Windows Server 2012 R2 Datacenter Edition (x64)	Microsoft	Oct 9, 2023	Expired	1			
	PostgreSQL (Less than version 12)	Postgre5QL	Nov 9, 2023	Expired	7			
	Tomcat 8.5	Tomcat	Mar 31, 2024	81 days left to expire	4			
	Python 3.9	Python Software Foundation	Oct 31, 2025	660 days left to expire	1			
	PostgreSQL 14	PostgreSQL Global Development Group	Nov 12, 2026	1.037 days left to expire	4			
	NET Framework 3.5 (x64)	Microsoft	Jan 10, 2029	1.827 days left to expire	5			

Weitere Schwachstellen betreffen die Webserver. In diesem Bereich bekomme ich eine Übersicht mit Lösungsvorschlägen, mit deren Hilfe ich Schwachstellen auf den Webservern beheben kann.



Und zum Schluss sehe ich mir an, welche Ports auf welchen Systemen offen sind.

Zero-day Vulnerabilities	Port Number	Port Type	Instances	Description
System Misconfigurations	22	TCP	2	The Secure Shell (SSH) Protocol
High Risk Software	25	TCP	1	Simple Mail Transfer
Web Server Misconfiguration	69	UDP	6	Trivial File Transfer
Port Audit	80	TCP	4	World Wide Web HTTP
Manage Exceptions	81	тср	2	NT Kernel & amp; System; Apache HTTP Server
	123	UDP	14	Network Time Protocol
	135	тср	14	DCE endpoint resolution
1	137	UDP	13	NETBIOS Name Service
	138	UDP	13	NETBIOS Datagram Service
	139	тср	13	NETBIOS Session Service
	161	UDP	14	SNMP
	162	UDP	4	SNMPTRAP
	443	тср	7	http protocol over TLS/SSL
	444	тср	1	Simple Network Paging Protocol
	1442	100	1.42	Advantage Pag

2.4 Zeit für den Cappuccino – Dashboards prüfen:

Anstelle mich durch eine Flut an Benachrichtigungs- und Status E-Mails zu wühlen, gehe ich in die Dashboards. Das Threats & Patches Dashboard liefert mir alle nötigen Informationen auf einen Blick und ich wechsle durch das Dashboard in Bereiche welche meiner Aufmerksamkeit bedürfen. Ein übersichtliches Dashboard mit direkten Verlinkungen ist ein MUSS für mich.



Einmal eine saubere Patchstrategie definiert brauche ich mich nur noch um die noch fehlenden nicht freigegebenen Patches kümmern und ggfs. ein Troubleshooting, wenn auf einem System ein Patch nicht erfolgreich installiert werden konnte.

Zugegeben, es ist ein initialer Aufwand eine Strategie zu konfigurieren. Einmal eingerichtet jedoch, reduziert es meinen bisherigen manuellen Aufwand erheblich und bietet maximalen Schutz der Endpoints. Was mir an der Lösung von ManageEngine so gefällt ist, das ich übersichtlich und einfach Patchautomatismen anlegen kann – ohne Raketenwissenschaften studiert zu haben. Auch brauche ich mit guten Dashboards und Reports keine Glaskugel zu Rate zu ziehen und orakeln lassen wie sicher meine Clients sind.

Das ist meine Strategie beim Endpoint Patching. Durch diese schaffe ich mir freie Zeit, welche ich nutzen kann um die weiteren Schwachstellen wie USB Devices, Applikationen, Browser, Bitlocker, etc. anzugehen. Auch hierzu gibt es viele Lösungen auf dem Markt und natürlich auch in meiner bevorzugten Managementlösung EndpointCentral.

Gerade in einer Zeit in welcher ich es schwer habe neue Kollegen in der IT zu finden, benötige ich eine Lösung, welche mir Freiräume schafft. Mit EndpointCentral habe ich solch eine Lösung, bei welcher ich außerdem einen exzellenten Support von ManageEngine und dem deutschen Partner MicroNova AG, zur Verfügung habe.

Also worauf noch warten?

Viel Spaß und haltet Eure Endpoints Up-To-Date!

Jürgen Rinelli

3. About the Author:

MCITP, MCTS, MCP, MOS, Enterprise Administrator, Senior Software Consultant, SCCM-Spezialist, Autor, Coach, Reiki-Lehrer ...

Jürgen Rinelli wurde 1970 in Deutschland geboren. In seinem ereignisreichen und oft abenteuerlichen Leben hat er in vielen Ländern gelebt und gearbeitet. Ob als Geschäftsmann, Manager, Mechaniker, Trainer, Taucher oder IT-Experte, er findet immer einen Weg, seine Träume zu verfolgen.

