

Anleitung: MICROSOFT EXCHANGE POC



ESE

100% Made

in EU Securit



Inhaltsverzeichnis

Beschreibung des MS Exchange PoC
Installation der Sicherheitslösung für die ESET Mailsecurity for Exchange
Konfiguration im PROTECT oder im lokalen ESET Mailsecurity GUI6
Erklärung der wichtigsten Einstellungen im ESET Exchange GUI6
Regeln - Postfachdatenbankschutz8
Regeln – Mail-Transportschutz9
Clustermodus - Policy Synchronisation11
Cluster aktivieren und konfigurieren11
ESET Shell Kommandos12
Lokale Tasks in der ESET Mailsecurity for Exchange anlegen und konfigurieren
Lokale ESET Mailsecurity for Exchange Quarantäne15
Weitere Quarantäne Möglichkeiten15
Konfiguration im ESET PROTECT – NDR16
Konfiguration in ESET PROTECT - DKIM16
Konfiguration in ESET PROTECT - SPF17
ESET Mailsecurity for Exchange Berichte

in the second second

ESET.DE | ESET.AT | ESET.CH

Beschreibung des MS Exchange PoC

Der MS Exchange PoC umfasst eine komplette Installation mit einem potentiellen Neukunden, der seine Exchange Server damit absichern möchte. Wir zeigen Ihnen, welche Möglichkeiten unsere Lösung beinhaltet und richten das Produkt entweder in einer Stand Alone Umgebung (ohne ESET PROTECT) oder in einer verwalteten Umgebung mit dem ESET PROTECT ein. Zur Grundkonfiguration gehört auch, ein Regelwerk mit dem Kunden zu definieren, welche Postfächer in die Exchange Datenbank nach Malware gescannt werden. Darüber hinaus sichern wir auch die eingehenden E-Mails ab und scannen nach Malware und Spam. Die blockierten Objekte landen in der Quarantäne und wie diese im täglichen Umfeld bedient wird, zeigen wir ebenfalls in diesem Dokument.

Installation der Sicherheitslösung für die ESET Mailsecurity for Exchange

Die Installation kann auf den 3 möglichen Wegen erfolgen.

- 1. Erstellen eines Installers im ESET PROTECT
- 2. MSI direkt runterladen und installieren
- 3. Installation durch die Aktivierung des Cluster-Modus

Erstellen eines Installer im ESET PROTECT

Kunden, welche die Exchange Server über ESET PROTECT verwalten, können die Lösung direkt als Installer oder per Task auf die Server verteilen.

Gehen Sie hierzu auf Installationsprogramme und klicken auf Installationsprogramm erstellen. Im Anschluss öffnet sich diese Maske:



Konfigurieren Sie den Installer anhand dieser Maske mit Ihren vorgegebenen Einstellungen. Klicken Sie danach auf *Weiter*.

In der nächsten Maske wählen wir bei Sicherheitsprodukt den aktuellen Exchange Schutz und die gewünschte Sprache aus. Die Lizenz wird automatisch von ESET PROTECT ausgewählt.

Wenn Sie bereits eine Konfiguration für die ESET Mailsecurity for Exchange haben, kann sie hier hinterlegt werden.

Installationsprogramme > ESET Ma	il Security for Microsoft Exchange Server		
Algemein	· ciula de la ciu		
Produkteinrichtung	 Sicherheitsprodukt ESIT Mail Security for Microsoft Exchange Security Venion 11.0.10008.0. Security Englisch, WMD0WS 		
Verteilung	Schutz- und Installationseinstellungen		
	SET LiveGrid * Feedbacksystem aktivieren ③		
	Erfassung potenziell unerwünschter Anwendungen aktivieren 🕥		
	Änderungen an den Schutzeinstellungen während der Installation erlauben		
	• Endbenutzer-Lizenzvereinbarung i		
	C Ich akzeptiere die Endbenutzen-Lizenzvereinbarung und die Datenschutzenklarung.		
	Weitere Einstellungen anpassen 🔨		
	Uzenz		
	ESET Mail Security, Public ID 348-342-DGB, Eigentümer Patrik Werren (patrikwerren@eset.com), Ablauf 22, August X 2025 05:59-59		
	Konfiguration		
	Exchange Server 2019 🗙		
	ESET AV Remover ausführen		
	Wenn Sie den ESET AV Remover aktivieren, akzeptieren Sie die entsprechende Endberutzer-Lizenzvereinbarung.		

Klicken Sie auf *Fertig Stellen*, danach kann der Installer als 64-bit Version runtergeladen werden.



Sie können den Installer direkt auf die Server verteilen und mit einem *Doppelklick* ausführen. Das ist der schnellste Weg, wenn Sie nur wenige Exchange Server damit ausrollen möchten.

Bei einer größeren Anzahl Exchange Server können Sie den Installer auch über das ESET Remote Deployment Tool verteilen. <u>>Link</u>

ESET Remote Deployment Tool	Distribution option Select one of the cotions to distribute installer cackage.
Source selection	Select the source to be used:
Configurate servicion Configuration Deployment	Active Directory Active Directory. Scient computers from Active Directory. Scan your local network Scan your local network Import Ist Centerab Import a list of hostnames or IP Addresses. Addresses Addresses manually.
	Bodi, Next Cancel

Das Tool bietet die Möglichkeit, die Exchange Server über das Active Directory auszuwählen, was wir auch empfehlen. Alternativ können Sie die Share-Point Server über eine csv Liste oder von Hand erstellen, was allerdings einen erheblichen Mehraufwand für Sie bedeutet.

MSI direkt runterladen und installieren

Über den folgenden Link ist es möglich, den ESET Mail Security für Exchange Installer direkt von unserer Webseite herunterzuladen:

<u>>www.eset.com/ch-de/business/download/</u> mail-security-exchange/

 Download ESET Mail Security für Microsoft Exchange Server

 Download konfigurieren

 Operating systemi Bit

 Winders Server 2002 (Gebälle)

 Download konfigurieren

 Download konfigurieren

 Download konfigurieren

 Deresting systemi Bit

 Download konfigurieren

 Download (Gebälle)

 Download (Gebälle)
 </t

Mittels der MSI-Datei können Sie die Installation anpassen, sowohl die Komponenten, die Sie installieren möchten als auch die Installationspfade.



ESET Mail Security Setup	× Welcome to the ESET Mail	ESET Mail Security Setup × Choose product components, which will be installed Custom setup
MAIL SECURITY	The Setup Wizard allows you to export your product settings or remove the installation if you do not want to use ESET Mail Security anymore.	 (Required Components) X • Real-time file system protection Network protection Device control Device control allows monitoring the use of devices on endpoint machines and applying rules
Progress. Protected.	< Back Next > Cancel	to specify how users can access devices (CD/DVD/USB, etc.). < Back Next > Cancel

Klicken Sie auf Next.

😸 ESET Mail Security S	Setup	×
Setup type		eser
Choose the setup t	ype that best suits your needs	GECT
○ Complete	All program features will be installed.	
Oustom	Choose which program features will be installed. Recommended for advanced users.	
	< Back Next >	Cancel

Im zweiten Schritt, geben wir an, ob die Installation Vollständig oder Benutzerdefiniert erfolgen soll.

Falls Sie die bestehende Sicherheitslösung für den MS Exchange Server beibehalten möchten und von ESET nur die Exchange Applikation absichern wollen, dann ist eine benutzerdefinierte Installation erforderlich.

In diesem Fall wählen Sie Benutzerdefiniert und klicken auf Weiter.

Deaktivieren Sie folgende Komponenten:

- 1. Echtzeit-Dateischutz
- 2. Netzwerk-Schutz
- 3. Gerätesteuerung

Danach klicken Sie auf Weiter.

Select Installation Folder	ese
To install in this folder, click "Install". To install to a different fold "Browse".	ler, enter it below or click
Product folder:	
Product folder: C:\Program Files\ESET\ESET Security\	Browse
Product folder: C:\Program Files\ESET\ESET Security\	Browse
Product folder: C:\Program Files\ESET\ESET Security\ Module folder:	Browse
Product folder: C:\Program Files\ESET\ESET Security\ Module folder: C:\Program Files\ESET\ESET Security\Modules\	Browse Browse
Product folder: C:\Program Files\ESET\ESET Security\ Module folder: C:\Program Files\ESET\ESET Security\Modules\ Data folder:	Browse

Im letzten Schritt besteht die Möglichkeit, die ESET Mailsecurity Exchange auf einem anderen Laufwerk als auf dem C:\-Laufwerk zu installieren, z. B. auf einem lokalen D:\-Laufwerk. Beachten Sie, dass Netzlaufwerke werden NICHT unterstützt werden.



Installation durch die Aktivierung des Cluster-Modus

Mit der Aktivierung des Cluster-Modus, wird auf sämtlichen ausgewählten Exchange Servern der ESET Schutz ausgerollt, falls er noch nicht installiert ist. Bei dieser Form der Einrichtung ist es erforderlich die ESET Software auf dem primären Exchange zu installieren und anschließend den Cluster-Modus zu aktivieren. Auf der nachfolgenden Seite finden Sie alle Informationen zum Cluster-Modus.

Konfiguration im PROTECT oder im lokalen ESET Mailsecurity GUI

Die Konfiguration für die ESET Mailsecurity for Exchange kann entweder über das ESET PROTECT Management oder lokal im GUI erfolgen.

ESET PROTECT: Das Management repliziert regelmäßig die Mailsecurity for Exchange Policy auf sämtliche Exchange Server.

Lokales ESET Mailsecurity for Exchange GUI: Möchte der Kunde kein zentrales Management einsetzen, kann die Policy auch lokal in der GUI der ESET Mailsecurity for Exchange konfiguriert werden. Die Replikation der Policy auf sämtliche Exchange Server übernimmt der ESET Cluster-Modus.

Es spielt dabei keine Rolle, auf welchem Server die Policy angepasst wird. Sobald auf einem Exchange Server eine Änderung an der Policy vorgenommen wird, ändert sich die Policy automatisch auf sämtlichen Exchange Servern.

Erklärung der wichtigsten Einstellungen im ESET Exchange GUI

Ohne das zentrale Management ESET PROTECT lassen sich die meisten Einstellungen direkt auf den Exchange Servern einstellen. Wir zeigen diese Themen kurz in der Demo auf.

CSCT MAIL SECURITY				
18 Monitoring	🗸 Υοι	u are protected		
♥ Log files Q. Scan C: Update ♥ Mail Quarantine ③ Setup ➡ Tools ⑧ Help and support	Module Last upd File Sys infected: Cleaned Cleaned Total:	es are up to date ale: 0210.3004 12.06.11 tem Protection Statistics 0 48'566 48'566		
Progress. Protected	Product version Server name System Computer Server uptime Mailbox count	11.0.100080 EXCHanslocal Windows Server 2019 Standard 64-bit (10.0.17763) Intellity Neorling Gold S2181; CPU @ 2.10GHz (2100 MHz), 32768 MB RAM 7 hours, 27 minutes 7 hours, 27 minutes		

In der ESET Mail Security for Exchange sehen Sie beim Reiter *Monitoring* den aktuellen Zustand der Module und die Statistiken zum Dateisystemschutz.

esr	MALSECURITY				
	Advanced setup				
	Sever Antifurian aprotection Anti-Number protection Anti-Number pro	 Integration Mult transport protection Deale mult transport protection Agent priority whop DEM signing Agent priority whop 	Ger Gor		
Progres.			 unboué extra serva 	ge og mennesses	etup

Die wichtigste Einstellung für den PoC ist die Aktivierung der Mail transport protection. Damit ist die ESET Sicherheitslösung in der Lage E-Mails, welche den Server erreichen, vor Speicherung in der Exchange Datenbank nach Malware zu scannen.

ESCT MAIL SECURITY				0	-		×
	Log files						
😰 Log files	Mail server protection (17)						
			Envelope sender	From	Recipien		
	Events Computer scan Sent Files Biocad Hes: Aude Hers Browser protection Network protection Network protection Pittered websites Device control Mailbor disabase scan Surth protection Mail server protection	000. 21. 21. 21. 21. 2003. 2003. 2003. 2003.	bourses-Ad17003 dec. Selectiane I Audit de Conselection de la conselectione de la conselection de la consel	nuth Joschnell. office@ketsol. dise_NA3@doc. ether_boscl. selet@kojget. orell_ina@foll. harisvaljeesc@. harisvaljeesc@. harisvaljeesc@. barisvaljeesc@. barisvaljeesc@.	info@ese info@ese info@ese info@ese info@ese info@ese patrik@e patrik@e patrik@e patrik@e patrik@e info@ese info@ese	t-pre, t-pre, t-pre, t-pre, t-pre, t-pre, t-pre, set-pr set-pr set-pr set-pre, t-pre, t-pre,	
	Filtering						

Im Bereich *Log files* finden wir folgende wichtige Reiter in Bezug auf die E-Mail Security:

- Sent files Alle Dateien, welche in der ESET Cloud Sandbox analysiert werden
- Mailbox database scan Informationen zu jedem einzelnen Mail Datenbank Scan
- SMTP protection Zum Beispiel als Spam klassifizierte E-Mails anhand dem SPF
- Mail server protection Sämtliche E-Mails die abgefangen wurden, mit Details der Herkunft und an welchen Benutzer sie ausgeliefert werden sollte

Suchen Sie gezielt nach einem Event, benutzen Sie den Filter.

 Image: Mail SECURITY
 <td

Der Log-Filter ermöglicht es nach Event-Namen, Spalten, Eintragstypen und über einen speziellen Zeitraum zu suchen.

(CSCT MAIL SECURITY	0 -	 <
	Scan	
Log files Con Scan Update Mail Quarantine	Mailbox database scan Macrosoft schange makbox database scan San al local disks and dean threats Removable media scan Removable media scan Removable media scan	
	^[®] Scanning of USE DVO. CD and other C [™] Mallbox database scars: 19:09.2034 11:05 ^[®] removable media [®] [®] [™] [®] [™] [®]	
Progress. Protected.		

Die Mail Security Datenbank kann direkt über das GUI nach Malware durchsucht werden. Wir empfehlen den zeitgesteuerten Scan über einen Task.

eser MAIL SECURIT			
	CECT MAILSECURITY		
Monitoring	Mailbox database scan		
🗊 Log files			
Q Scan	Scan only messages with attachments		
	Public folders Public folders /all		
國 Mail Quarantine			
l Setup			
🛱 Tools			
(?) Help and support	Mailboxes		
	Mailboxes		
	Qr Save Scan	Cancel	
Progress. Protected.			

Beim manuellen Scan ist es möglich, sämtliche E-Mails oder nur jene mit Anhang zu prüfen. Ebenfalls werden bei einem Scan die *Public folder* und die *Mailboxes* nach Malware durchsucht. Über *Edit* lassen sich die Public Folder und die Mailboxen einschränken, so dass nicht alle gescannt werden.



Danach läuft die Prüfung auf Malware. Die Dauer variiert stark nach der Größe der Datenbank. Bei einer großen Datenbank kann es auch bis zu mehreren Stunden dauern.

~	Mailbox database scan Scan completed	02.10.2024 13:41:15
	Detections occurred: 0 Detection Engine used: 29986 (20241002)	Dismiss
	Show log	

Ist der Scan komplett abgeschlossen, erhalten Sie eine Meldung. Möchten Sie den Inhalt des Scans sehen, klicken Sie auf *Log anzeigen*.

(CSCT) MAIL SECURITY		•	7	a	×
08 Monitoring	Setup				
🗊 Log files Q. Scan 🛛 🚯	Server				
C Update	Computer All required computer protection features are active.				
 Mail Quarantine Setup 	Network All required network protection features are active.				
Tools Help and support	(iii) Web and email All required internet protection features are active.				
	a Tools				
Progress. Protected.	⁺≟ Import/Export sett	ngs Ø	Advan	ced se	up

Wichtige Einstellungen zur Mailsecurity for Exchange finden Sie im Register Server.

Regeln – Postfachdatenbankschutz

Die Regeln für den Postfachdatenbankschutz betrifft sämtliche E-Mails, die bereits in ein Postfach zugestellt wurden. Mit den Regeln ist es möglich, nachträglich E-Mails aus den Postfächern zu entfernen.

Die Regeln enthalten immer zwei Eingabefelder:

Feld Nr.1 – Bedingung: Typ und die Operation

Feld Nr.2 – Aktion: Typ

Hierzu können z. B. Regeln erstellt werden, die nach einem Absender, einen Namen eines Anhangs oder auch nach einer bestimmten Uhrzeit filtern.



Im ersten Feld legen wir fest, nach was wir gezielt suchen.

Bedingung hinzufügen	? ¤ X
TVD	Betreff
Operation	ist / ist Tail yon
operation	ict / ict Tail yon
	ist nicht / ist nicht Teil von
	enthält
	enthält nicht
	Treffer für regulären Ausdruck
	kein Treffer für regulären Ausdruck
Hinzufügen Bearbeiten Entfernen Aktion hinzufügen	Importieren Exportieren ? 🗆 X
Тур	Nachricht löschen
	Nachricht löschen
	Anhänge in Quarantäne verschieben
	Anhang löschen
	In Ereignislog aufnehmen
	Ereignisbenachrichtigung an Administrator senden
Hinzufügen Bearbeiten Löschen	Scan durch Virenschutz überspringen
Aktionstyp Parameter	Andere Regeln erstellen

Im zweiten Feld definieren wir die Operation wie z. B. ist Teil von, oder enthält.

Regel					?	⊐ × □
Aktiv						
Name			test			0
Bedingungstyn	Operation	Paramet	er			
Betreff	ist / ist Teil vor	test				
Hinzufügen B	earbeiten 🛛 Lös	chen	±	V	Ŧ	í.
Aktionstyp	Paran	neter				
Nachricht lösche	n					
Hinzufügen B	earbeiten 🛛 Lös	chen				
					Abbreck	nen

In diesem Beispiel suchen wir nach sämtlichen E-Mails, in welchen *test* im Betreff steht und löschen diese.

Regeln - Mail-Transportschutz

Die Regeln für den Mail-Transportschutz betrifft sämtliche E-Mails, die über den Mailtransport von extern nach innen zum Exchange-Server gelangen. Die Regeln lassen sich auch auf interne Verbindungen erweitern, wenn E-Mails zum Beispiel über mehrere Server geleitet werden.

Die Regeln enthalten immer zwei Eingabefelder:

Feld Nr.1 – Bedingung: Typ und die Operation

Feld Nr.2 – Aktion: Typ

Hierzu können z. B. Regeln erstellt werden, die nach einem Absender, einen Namen eines Anhangs, oder auch nach einer bestimmten Uhrzeit filtern.

Absender Whitlisting Filterung 0 spoofing Filterung 0 Gefährliche Systemdateianhänge Verarbeitung von Anhängen 0 Gefährliche ausführbare Dateianhänge Verarbeitung von Anhängen 0 Office-Dateianhänge mit Makros Verarbeitung von Anhängen 0 Gefährliche Skriptdateianhänge Verarbeitung von Anhängen 0 Verbotene Archivdatei-Anhänge Verarbeitung von Anhängen 0 PDF Anhänge Löschen Verarbeitung von Ergebnissen 0	Aktiv	Name	Stufe	Treffer Q
spoofing Filterung 0 Gefährliche Systemdateianhänge Verarbeitung von Anhängen 0 Gefährliche ausführbare Dateianhänge Verarbeitung von Anhängen 0 Office-Dateianhänge mit Makros Verarbeitung von Anhängen 0 Gefährliche Skriptdateianhänge Verarbeitung von Anhängen 0 Verbotene Archivdatei-Anhänge Verarbeitung von Anhängen 0 PDF Anhänge Löschen Verarbeitung von Ergebnissen 0	2	Absender Whitlisting	Filterung	0
Gefährliche Systemdateianhänge Verarbeitung von Anhängen 0 Gefährliche ausführbare Dateianhänge Verarbeitung von Anhängen 0 Office-Dateianhänge mit Makros Verarbeitung von Anhängen 0 Gefährliche Skriptdateianhänge Verarbeitung von Anhängen 0 Verbotene Archivdatei-Anhänge Verarbeitung von Anhängen 0 PDF Anhänge Löschen Verarbeitung von Anhängen 0 Archivdateianhänge mit Passwortschutz Verarbeitung von Ergebnissen 0		spoofing	Filterung	0
Gefährliche ausführbare Dateianhänge Verarbeitung von Anhängen 0 Office-Dateianhänge mit Makros Verarbeitung von Anhängen 0 Gefährliche Skriptdateianhänge Verarbeitung von Anhängen 0 Verbotene Archivdatei-Anhänge Verarbeitung von Anhängen 0 PDF Anhänge Löschen Verarbeitung von Anhängen 0 Archivdateianhänge mit Passwortschutz Verarbeitung von Ergebnissen 0		Gefährliche Systemdateianhänge	Verarbeitung von Anhängen	0
Office-Dateianhänge mit Makros Verarbeitung von Anhängen 0 Gefahrliche Skriptdateianhänge Verarbeitung von Anhängen 0 Verbotene Archivdatei-Anhänge Verarbeitung von Anhängen 0 PDF Anhänge Löschen Verarbeitung von Anhängen 0 Archivdateianhänge mit Passwortschutz Verarbeitung von Ergebnissen 0	7	Gefährliche ausführbare Dateianhänge	Verarbeitung von Anhängen	0
Gefährliche Skriptdateianhänge Verarbeitung von Anhängen 0 Verbotene Archivdatei-Anhänge Verarbeitung von Anhängen 0 PDF Anhänge Löschen Verarbeitung von Anhängen 0 Archivdateianhänge mit Passwortschutz Verarbeitung von Ergebnissen 0	~	Office-Dateianhänge mit Makros	Verarbeitung von Anhängen	0
Verbotene Archivdatei-Anhänge Verarbeitung von Anhängen 0 PDF Anhänge Löschen Verarbeitung von Anhängen 0 Archivdateianhänge mit Passwortschutz Verarbeitung von Ergebnissen 0		Gefährliche Skriptdateianhänge	Verarbeitung von Anhängen	0
PDF Anhänge Löschen Verarbeitung von Anhängen 0 Archivdateianhänge mit Passwortschutz Verarbeitung von Ergebnissen 0		Verbotene Archivdatei-Anhänge	Verarbeitung von Anhängen	0
Archivdateianhänge mit Passwortschutz Verarbeitung von Ergebnissen 0		PDF Anhänge Löschen	Verarbeitung von Anhängen	0
	7	Archivdateianhänge mit Passwortschutz	: Verarbeitung von Ergebnissen	0

Im Regelwerk, können wir neue Regeln hinzufügen oder bestehende *ändern, aktivieren oder deaktivieren.*



tiv	Bedingung bearbeit	en	? 🗆 X
eding	Тур	Art des Anhangs	v
t des	+ Ausführbare	Dateien n	^
linzufi ktion Ereig	🛨 😑 Dokumo 🛨 🚍 Tabeller 🛨 🚍 Präsent	nte Ikalkulationsblätter ationen	

In den Bedingungen ist es bspw. möglich, gezielt nach Office Dokumenten zu filtern. Angehängte Dateien werden durch das festgelegte Regelwerk in den E-Mails entfernt.

Bedingung hinzufügen	X = 1	
TVp	Betreff	
Operation	Nachrichtengroße Nachrichtenheader Nachrichtentext	
	Interne Nachricht Ausgehende Nachricht Signierte Nachricht Verschüsselte Nachricht Scan-Ergebnis des Spam-Schutzes Scan-Ergebnis des Virenschutzes Scan-Ergebnis des Phishing-Schutzes	
Hinzufügen Bestenten Entfernen	Uhrzeft des Empfangs Enthält passwortgeschützes Archiv Enthält beschädigtes Archiv DikM-Ergebnis	
	SPF-Ergebnis	L
	DMARC-Ergebnis Hat Reverse-DNS-Eintrag NDR-Prüfergebnis	
BENUTZEROBERFLAC	SPF-Ergebnis - From-Header Vergleichsergebnis zwischen Umschlag-Absender und From-Header	2

Es besteht auch die Möglichkeit, dass z. B. nach einem SPF-Ereignis gesucht wird.

Aktion hinzufügen		? 🗆 X
Тур		Nachricht in Quarantäne verschieben 🗸
		Nachricht in Quarantäne verschieben
		Nachricht ablehnen
Kann von Benutzern	freigegeben werden	Nachricht automatisch löschen
		Anhänge in Quarantäne verschieben
		Anhang löschen
		DMARC-Policy übernehmen
-		SCL-Wert festlegen
Aktionstyp	Parameter	In Ereignislog aufnehmen
		Ereignisbenachrichtigung an Administrator senden
		Scan des Spam-Schutzes überspringen
		Scan durch Virenschutz überspringen
		Scan des Phishing-Schutzes überspringen
		Andere Regeln erstellen
Hinzufügen Bea	rbeiten Löschen	Betreffpräfix hinzufügen
		Header-Feld hinzufügen
		Header-Felder entfernen

Wird eine E-Mail mit einem SPF-Ereignis gefunden, kann diese abgelehnt, gelöscht oder auch in die Quarantäne verschoben werden.

Clustermodus – Policy Synchronisation

l	CSCT MAIL SECURITY		0 - 0	
		 Server 		
		Antivirus protection Enabled		
	Q Scan 9	Contraction Enabled		
		Anti-Phishing protection Enabled		
	log Setup	Contemporatic exclusions Enabled		
		Cluster Disabled Cluster is not created.		
	Help and support	Component setup		
		(巴) Cluster management 四-면 Satus: Not used	Solus: Not registered	
			1. Import/Export settings - O Advanced sets	
			 Importe Coport seconds Construction seconds 	*

Im Enterprise PoC empfiehlt es sich immer den Cluster-Modus zu aktivieren.

Der ESET Cluster ist eine P2P-Kommunikationsinfrastruktur aus der ESET Produktlinie für Microsoft Windows Server.

Diese Infrastruktur ermöglicht, dass ESET Serverprodukte miteinander kommunizieren, Daten wie z. B. Konfigurationen und Benachrichtigungen austauschen und die für den ordnungsgemäßen Betrieb einer Gruppe von Produktinstanzen erforderlichen Daten synchronisieren können.

Ein Beispiel einer solchen Gruppe ist eine Knotengruppe in einem Windows-Failover-Cluster oder einem Network Load Balancing (NLB)-Cluster mit installiertem ESET Produkt, bei der das Produkt im gesamten Cluster gleich konfiguriert sein muss. ESET Cluster garantiert diese Einheitlichkeit zwischen den Instanzen.

Der Clustermodus ist für Exchange sinnvoll, um die Quarantäne zu synchronisieren. Es gibt dabei einen Quarantänen-Master, auf welchem sämtliche SPAM und Malware E-Mails gespeichert werden. Daneben wird auch die Policy auf sämtliche Exchange Server synchronisiert. Die Policy der ESET Mailsecurity for Exchange kann auf einem x-beliebigen Exchange Knotenpunkt angepasst werden. Die Änderung wird anschließend automatisch auf sämtliche Exchange Server synchronisiert.

Cluster aktivieren und konfigurieren

- 1. Den Schiebregler Cluster einschalten.
- 2. Die Cluster-Member von Hand eintragen oder über die automatische Erkennung suchen.

Wichtig: Der Standardport ist 9777, falls dieser Port bereits belegt ist, verwenden Sie eine andere Portnummer.



3. Klicken Sie auf *Next* und das Cluster wird automatisch gebaut. Sollte auf einem der Clusternodes noch keine ESET Mailsecurity Exchange Software installiert sein, wird diese automatisch über den Cluster Wizzard ausgerollt und installiert.





Der Quarantäne- bzw. Cluster-Master ist immer der Exchange Server, auf welchem der Cluster Wizzard initial ausgeführt wird.

Wichtig: Der Cluster-Master kann nicht an einen anderen Cluster-Node verschoben werden.

ESET Shell Kommandos



Unter Tools finden Sie den Taskplaner für zeitgesteuerte Exchange Mailbox Scans sowie den Aufruf der ESET Shell Kommandos:



Die ESET-Shells können remote per PowerShell über einen Server Task im ESET PROTECT Management aufgerufen werden.

Hier finden Sie den Link zu der Beschreibung:

<u>>help.eset.com/eshp/11.0/de-DE/work_eshell.html</u>

Lokale Tasks in der ESET Mailsecurity for Exchange anlegen und konfigurieren



Im Taskplaner sind schon einige vorgefertigte Tasks hinterlegt, wie zum Beispiel die Log-Wartung, Update und die Prüfung der Systemstartdateien.



Als Beispiel erstellen wir im PoC eine Demo zum Thema Mailbox Scan. Hierzu klicken wir auf *Task hinzufügen* und vergeben in den Taskdetails einen Taskname. Bei Tasktyp wählen wir *Mailbox database scan* aus.

(Bet MAIL SECURIT				
DB Monitoring	Scheduler			
D Log files	GENT MAIL SECURITY			Last run
Q Scan	Task execution			02.10.2024 05:52:57
🗘 Update		O Once		02.10.2024 13:05:57
🖏 Mail Quarantine		O Repeatedly O Daily		
🞯 Setup		Weekly Event triggered		02 10 2024 06:06:18
💼 Tools	Skip task when running on battery pow			02.10.2024 12:06:13
Help and support				19.09.2024 01:00:14
				19.09.2024 02:00:14
				02.10.2024 06:00:57
		Back	ext Cancel	16.09.2024 00:00:15
				16.09.2024 00:00:15
	Marbox database scan test pw Send mail server protection	Task will be run only o		07.07.2023 15:48:44
Progress. Protected,	Add task	Edit ODelete	S Default	

Den Mailbox Datenbank-Scan planen wir in einer wöchentlichen Ausführung.

CSCT MAIL SECURIT	Y		0 - a ×
	Scheduler		
	CERT MALSECURITY		Last run
	Task timing		02.10.2024 05:52:57
			02.10.2024 13:05:57
		O Monday	02.10.2024 06:06:18
💼 Tools		U Tuesday Wednesday	02.10.2024 12:06:13
		Li Thursday	19.09.2024 01:00:14
		🖸 Saturday 🛃 Sunday	19.09.2024 02:00:14
			02.10.2024 06:00:57
		Back Next Cancel	16.09.2024 00:00:15
			16.09.2024 00:00:15
	Mailbox database scan test pw Sand mail samer protection r		07.07.2023 15:48:44
		tdit SDelete SDelault	

Damit der Exchange Server in der Leistung nicht beeinträchtigt wird, wird die Ausführung des Tasks auf Sonntag 00:15 Uhr gelegt.



Der Task soll zur nächsten geplanten Ausführungszeit ausgeführt werden.

	Scheduler		
	Task	Triggers Next run	Last run
Q Scan 🛛 🕚	Update Automatic update after dial-up connection	Dial-up connection to Event trigger	
💭 Update	Update Automatic update after user logon	User logon (once per Event trigger	
S Mail Quarantine	System startup file check Automatic startup file check	User logon Task will n Event trigger	
🕅 Setun	System startup file check Automatic startup file check	Successful module up Event trigger	
.	Mailbox database scan D8 Scan Postfach Patrik		
Tools	Mailbox database scan DB Scan Postfach Michael		
Help and support	Send mail quarantine reports	Task will be run every 03.10.2024 0	
	Send mail server protection report Server Prot Report		
	Send mail server protection report Mail report weekly		
	Mailbox database scan	Task will be run only o	
	Send mail server protection report Report-Haris		
	Mailbox database scan		

Der Task wird hinzugefügt und wir finden ihn immer an unterster Stelle.



Per Default werden immer sämtliche Public Folder und alle Mailboxen gescannt. Änderungen lassen sich über *Edit* vornehmen. Damit ist es möglich die Public Folder und die Mailboxen der Mitarbeiter auszuwählen, welche gescannt werden sollen.

Lokale ESET Mailsecurity for Exchange Quarantäne

Sämtliche Objekte und E-Mails, welche sich in der Quarantäne befinden, können direkt auf dem Exchange Server wieder ins Postfach verschoben werden.

Wie oben beschrieben, liegt die Quarantäne bei einem ESET Cluster auf dem Master.

Werden die Exchange Server über ESET PROTECT verwaltet, finden Sie die Quarantäne Objekte direkt im Management und sie müssen dort freigegeben werden.



Weitere Quarantäne Möglichkeiten

Die ESET Mailsecurity for Exchange bietet 3 mögliche Quarantänetypen an:



Lokale Quarantäne

Die lokale Quarantäne stellt jedem ActiveDirectory Benutzer seine individuelle E-Mail-Quarantäne zur Verfügung. Zugriff hat der Benutzer über eine Web-Oberfläche, auf der er nur seine SPAM-E-Mails sieht.

			200 0 23	and the series of the series o	(pena)	ABSENCO	GEN43CHT		ADVIDUAL
	UMICHERC ADDRESS	-	methors	CRUND	-	-	PRESIDEN	COSCHEM	NEWS ARTICIN
3022-00-16 10-40	pdrk@uerer.com	patrib@usnet.com	patricit de conte	https://www.ambo.org/check-	ومتختفو		0	0	۲
3022-02-07-00.04	perilduerer.com	patricidwares.com	patric@exet-	Advanced hearistic classified mail as	12411		0	0	
3022-02-06 1722 🖬 Will (19	petrik@weren.com	patric@wener.com	patris@vort-	URL (Inspervillamorp.com) found	spans		0	0	۲
2021-08-15 6433 🖬 LOAN 3	info1@creditorions.co.uk	indo 1@crealitumicers.co.uk	info@wort-	Domain	1,247		0	0	۲
3021-06-14 16/27	publik@weren.com	park@verer.com	info@eset-	Found £72/8E test string	quam		0	0	۲
									General 1 Evens

Der Benutzer kann in diesem Portal als falsch klassifizierte SPAM-E-Mails selbständig freigeben. E-Mails, die Malware beinhalten, können durch den Benutzer nicht freigegeben werden. Der Exchange Administrator kann zusätzlich berechtigt werden.

Quarantäne-Postfach

ESET Mailsecurity for Exchange erstellt eine separate Wrapper-E-Mail mit zusätzlichen Informationen sowie den ursprünglichen E-Mails als Anhang, und stellt diese E-Mail ans Postfach zu.

Der SPAM-Administrator kann im Postfach die E-Mail falls nötig an die Mitarbeitenden weiterleiten. Der Mitarbeitende selbst hat keinen direkten Zugriff aufs Quarantäne-Postfach.

MS Exchange-Quarantäne

Der Exchange Server ist hierbei für die Zustellung der E-Mail ans definierte SPAM-Postfach verantwortlich. Das Postfach muss in ActiveDirectory auf der Organisationsebene als Quarantäne festgelegt werden. Sämtliche SPAM-E-Mails, die in das Postfach gelangen, werden im Original gespeichert.

Die interne Quarantäne ist in Microsoft Exchange Servern standardmäßig deaktiviert. Sie muss per nachfolgendem Power Shell-Befehl definiert und aktiviert werden:

Set-ContentFilterConfig-QuarantineMailbox name@domain.com

Konfiguration im ESET PROTECT – NDR

NDR steht für Non Delivery Report und ist eine Reaktion auf eine E-Mail die nicht zugestellt werden kann. Folgende Fehlermeldungen werden dabei vom E-Mail-Server ausgegeben:

- Zieldomäne nicht erreichbar
- Zielpostfach nicht erreichbar / existent
- Zielpostfach voll
- Zielsystem lehnt Mail ab

Der E-Mail-Server vom Absender muss so eingestellt sein, dass er NDR annimmt. Aus Sicht eines Spammers können Rückschlüsse gezogen werden, ob eine E-Mail auch tatsächlich ankommt. Er kann so einen Empfänger als positiv markieren und in weitere SPAM-Datenbanken als verifiziert integrieren.

Spammer tarnen auch teilweise Nachrichten als NDR, in der Hoffnung, dass sie vom Empfänger

geöffnet werden.

NDR ist sinnvoll, es sollte aber gut überlegt sein, was Sie dem Absender übermitteln.

In der ESET Mailsecurity for Exchange kann NDR im Bereich Backscatter-Schutz aktiviert werden. Hierzu wird ein frei erfundener Signatur-Seed hinterlegt.

BACKSCATTER-SCHUTZ	@ 2 7.0 B	0	
O Ø			0
🔾 👳 🗧 NDR-Nachrichten automatisch verwerfen, wenn die Prüfung fehlschlägt			
○ ● ÷ Signatur-Seed	7erthj9fh9		
BABSENDER-SPOOFING-SCHUTZ	@ 2 4.0 D	0 • +	

Die ESET Mailsecurity for Exchange prüft sämtliche NDR-Nachrichten, ob der Signatur-Seed vorhanden ist. Kommen gefälschte NDR-Nachrichten ohne den Signatur-Seed an, werden diese automatisch als SPAM klassifiziert und in die Quarantäne verschoben.

Konfiguration in **ESET PROTECT – DKIM**

DomainKeys Identified Mail (DKIM) ist eine Methode zur E-Mail-Authentifizierung. Sie verhindert, dass sich Spammer und andere böswillige Parteien als legitime Domain ausgeben.

Alle E-Mail-Adressen haben eine Domain – das ist der Teil der Adresse, der nach dem "@"-Symbol kommt. Spammer und Angreifer versuchen, sich beim Senden von E-Mails als eine Domain auszugeben, um Phishing-Angriffe oder andere betrügerische Aktivitäten durchzuführen.

Angenommen, Chuck möchte Alice dazu bringen, ihm vertrauliche Unternehmensinformationen zu schicken. Alice arbeitet bei example.com. Also schickt er ihr eine E-Mail, die angeblich von *bob@example.com* stammt, damit sie glaubt, dass er auch für example. com arbeitet.

DKIM in Verbindung mit Sender Policy Framework (SPF) und Domain-based Message Authentication Reporting and Conformance (DMARC) macht es Angreifern viel schwerer, sich auf diese Weise als Domains auszugeben. E-Mails, die DKIM und SPF nicht bestehen, werden als "Spam" markiert oder von E-Mail-Servern gar nicht erst zugestellt. Wenn example.com DKIM, SPF und DMARC für ihre Domain eingerichtet hat, wird Alice die böswillige E-Mail von



Chuck wahrscheinlich nie lesen, da sie entweder in ihrem Spam-Ordner landet oder vom E-Mail-Server ganz abgelehnt wird.

DKIM wird dabei über einen Record Generator erstellt. Der Public Key wird anschließend auf dem E-Mail-Server abgelegt.

Туре	Text	Name	Class	TTL
TAT		defaultdomainkey.	28	14399

Konfigurationsmöglichkeiten in der ESET Mailsecurity for Exchange

5	PF UND DKIM		O • f
0.0 +	DNS-Server automatisch erkennen	() ≥ 6.4	
0 . 4	IP-Adresse des DNS-Servers	() ≥ 6.4	
0	Zeitüberschreitung für DNS-Abfrage (Sekunden)	(2) ≥ 6,4	5
	Nachrichten bei fehlgeschlagener SPF-Prüfung automatisch ablehnen	(2) ≥ 6.4	
0 0 4	Helo-Domäne in der SPF-Auswertung verwenden	() ≥ 9.0	
0 • 4	From:-Header verwenden, wenn MAIL FROM leer ist	(e) ≥ 6.4	
	Greyfisting bei bestandener SPF-Prüfung automatisch umgehen	(2) ≥ 6.4	
	SMTP-ABLEHNUNGSANTWORT		
0 0 7	Antwortcode	(1) ≥ 6.4	550
0 • +	Statuscode	@ 2 6.4	5.7.1
0 . /	Antwortnachricht	(€ ≥ 6.4)	SPF check failed

ESET prüft dabei, ob die SPF-Prüfung erfolgreich war, oder nicht. Im zweiten Fall wird die E-Mail automatisch als SPAM klassifiziert und in die Quarantäne geschoben.

Konfiguration in ESET PROTECT – SPF

SPF steht für Sender Policy Framework.

Der empfangende E-Mailserver prüft die Echtheit von Absenderadressen anhand einer IP-Adresse, welche er über den SPF-Record abfragen kann.

Befindet sich die sendende IP-Adresse auf der Liste, wird die E-Mail durch den E-Mailserver angenommen.

Bitte seien Sie sich bewusst, dass SPF nicht vor Spoofing schützt. Ein Betrüger kann trotzdem einen falschen Absender in der E-Mail anzeigen.

	gmx.com
/=0	ipl1 (p4 213.165.64.0/23 (p4.74.208.5.64/26 (p4.74.208.122.0/26 (p4.212.227.126.128/25 (p4.212.227.15.0/24 .212.227.17.0/27 (p4.74.208.4.192/26 (p4.82.165.169.0/24 (p4.217.72.207.0/27.4ii)
	■ 213.165.64.0/23
	► 74.208.5.84/28
	▶ 74.208.122.0/28
	▲ 212.227.128.128/25
	212.227.15.0/24
1	■ 212.227.17.0/27
1	▲ 74.208.4.192/26
1	82.105.169.0/24
	217.72.207.0/27

ESET Mailsecurity for Exchange Berichte

In ESET PROTECT gibt es 3 Berichte zur E-Mail-Quarantäne. Sie finden sie im Reiter *E-Mail-Server*:

	#	0	=	0	=	Lo
Neues Bericht- Template	Häufigste Sp Absender	am-	Häufigste Sp Domains	am-	Häufigste Sp Empfänger	pam-
	E-Mail-Adress	sen, die in	E-Mail-Doma	ins, die in	E-Mail-Adres	isen, die in

- 1. Häufigste Spam-Absender
- 2. Häufigste Spam-Domains
- 3. Häufigste Spam-Empfänger

Die Berichte können angepasst, bzw. erweitert werden. Hierzu klicken Sie auf das Zahnrad oberhalb des Berichtes und wählen *bearbeiten* aus.

In diesem Beispiel erweitern wir die Tabelle um den Wert *Aufgetreten um*. So haben wir im Quarantäne Bericht zusätzlich die Uhrzeit.

Bitte wählen Sie ein Element aus	2 ×	
P Toppen Saraur Soche	V A	
Status der Computerhardware	^	42.6
Ursprung		* 7 @
Häufigste Spam-Absender		1 6 8
Aufgetreten um		
IP-Adressen im Netzwerk		
IPv4-Adresse des Adapters		
IPv4-Subnetzwerk		
IPv6-Adresse des Adapters		
IPv6-Subnetzwerk		
Primäre IP-Adresse		
Primäres IP-Subnetzwerk		
Statische Gruppe		
Beschreibung der statischen Gruppe		
Name der statischen Gruppe		

Sobald der Wert selektiert ist, wird die Tabelle auf drei Tabellenspalten erweitert.

Ilgemein	Tabellenspalten	
Jiagramm	Häufigste Spam-Absender . Absender	12 8
Jaten	Haufigste Spam-Absender - Anzahl	↓↑2 ≜
ortierung	Häufigste Spam-Absender , Aufgetreten um	÷ 2* ≣
lusammenfassung	Spatte hinzufügen	
	Vorschau	
	Vorschau anzeigen	

Der Bericht sieht im Anschluss folgendermaßen aus:

PROTECT		Häufigste Spam-Absender
Bericht: Häufigste Spam-Absender		
Endelit um 15. Oktober 2024 50:30:32 (UIC+02:00)		
Absarder	Anabi	Auforitarian um
bounces = 46370303 - 968b info reset pre-chi@em9986.schnellikes.ch	1	20. August 2024 17 28-45



ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen. Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.







velive security (esen)

eset Digital Security Guide

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200