



ESET Mailsecurity Exchange

Patrik Werren

ESET Mailsecurity Exchange – Agenda

- ESET Mailsecurity Exchange Architektur
- ESET Clustermodus - Besonderheiten
- NDR – DKIM - SPF
- Policy Einstellungen
 - Viren und Spyware Schutz
 - Spam Schutz
 - Phishing Schutz
 - Greylisting
 - Regeln für Postfachdatenbank und Mail-Transport-Schutz
 - Unterschiedliche Quarantänen
- Lokale Postfach Scans über das GUI
- Postfach Scans über Scan Ziele und Tasks im PROTECT

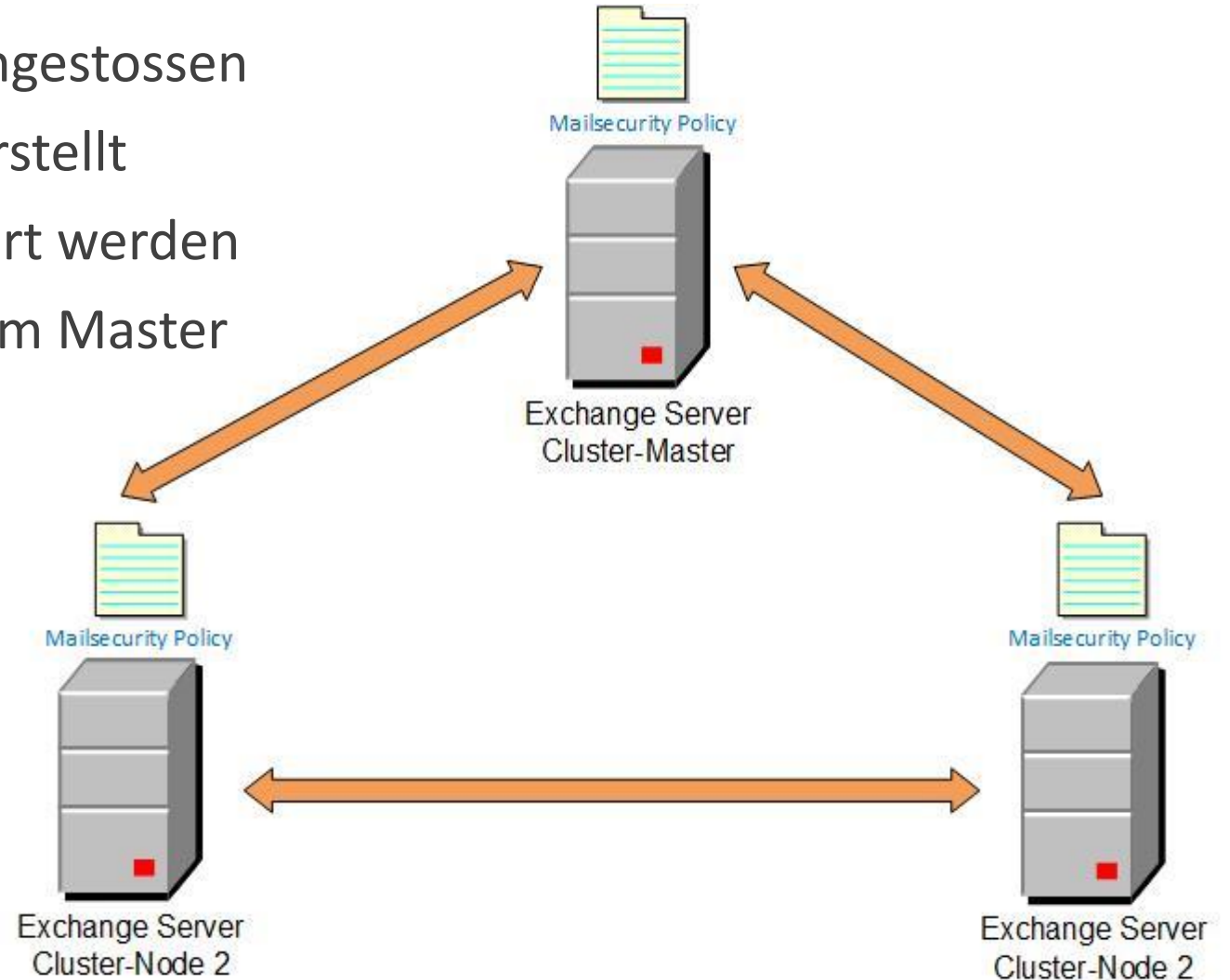




ESET Architektur

ESET Mailsecurity Exchange Architektur

- Cluster Wizzard wird vom Master angestossen
- Policy wird initial auf dem Master erstellt
- Policy kann auf jedem Node geändert werden
- ESET Exchange Mailsecurity wird vom Master auf die Nodes verteilt
- Der ESET Agent muss immer vom PROTECT aus verteilt werden !



ESET Clustermodus

The background of the slide is a dark blue, abstract digital landscape. It features numerous bright blue light trails and streaks that create a sense of motion and depth, resembling data flowing through a network. In the upper portion, there is a faint, glowing outline of a city skyline with various building shapes. The overall aesthetic is high-tech and futuristic.

ESET Mailsecurity Clustermodus – Besonderheiten

- In der aktuellen Version, kann ein Mailsecurity Cluster nur im lokalen GUI angestossen werden
- Die SPAM-Quarantäne liegt immer auf dem Mailserver, welcher das Cluster initialisiert hat
- Ohne PROTECT wird die Policy im Cluster synchronisiert, egal auf welchem Cluster-Member die Policy angepasst wird
- Mit PROTECT wird die Policy zentral verwaltet und bei lokalen Änderungen immer wieder überschrieben
- Über den PROTECT sind Berichte möglich
- Über den PROTECT sind Scans einzelner Exchange Server und einzelner Postfächer möglich

Policy Einstellungen

The background is a dark blue, abstract digital landscape. It features a central perspective view of a corridor or path that recedes into the distance, flanked by glowing blue lines and dots that suggest data flow or network connections. The overall aesthetic is futuristic and technological.

BWI Training – Mailsecurity Exchange Policy

- Policy Einstellungen
 - Viren und Spyware Schutz
 - Spam Schutz (NDR – DKIM – SPF)
 - Phishing Schutz
 - Greylisting
 - Regeln für Postfachdatenbank und Mail-Transport-Schutz
 - Unterschiedliche Quarantänen

The background is a dark, abstract composition. It features a central perspective of a path or road receding into the distance, flanked by blurred, glowing blue lines that suggest motion or light trails. In the upper portion, there are faint, stylized outlines of city buildings or structures. The overall color palette is dominated by deep blues and blacks, with bright blue highlights from the light trails.

NDR – DKIM – SPF

ESET Mailsecurity Exchange – NDR

- NDR steht für Non Delivery Report und ist eine Reaktion auf eine Mail die nicht zugestellt werden kann
 - Zieldomäne nicht erreichbar
 - Zielpostfach nicht erreichbar / existent
 - Zielpostfach voll
 - Zielsystem lehnt Mail ab
- Der Absender muss bereit sein, die NDR anzunehmen
- Aus Sicht der SPAMER können z.B. Rückschlüsse gezogen werden, ob eine E-Mail auch ankommt.
- SPAMER tarnen auch Nachrichten als NDR
- NDR sind Sinnvoll, es muss aber gut überlegt sein, was man übermittelt.

ESET Mailsecurity Exchange – DKIM

- DKIM steht für DomainKeys Identified Mail
- Es ist eine E-Mail Authentifizierungstechnik um zu prüfen ob die E-Mail tatsächlich vom Inhaber seiner Domain gesendet und autorisiert wurde.
- E-Mails vom Absender werden dabei digital signiert.
- Der sendende Mailserver fügt eine digitale Signatur hinzu.
- Der empfangende Server überprüft die digitale Signatur mit dem zur Signatur passenden öffentlichen Schlüssel.
- Hierzu wird ein TXT-Eintrag auf dem Nameserver (DNS) hinterlegt.
- Der DKIM Record kann mittels einem Tool erstellt werden.

ESET Mailsecurity Exchange – DKIM Schlüssel

Type	Text	Name	Class	TTL
TXT	v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvi0IegM87KrTtjm3hD1 cfi5DbDOByXWa637WyXssemq1d+BXfFr+Ztdx5Ry/+dZ984zv/y4v8hnFerGEWsus c4dixZ4Jy+wqSJKhS2nHPVKQgC7WAM7v0sX6LoMTXtSH0pC1BUx0qsTjL5TD2eVw5 /rQJ97C9PkQH1bK87FXkWb0vn9RgkFaOjv96n0qhUvXA NuRNXZGIuZqIsfw3WCNfjipjbLPzb0iBKR7VyB0vdmsBNCumk6C9FP8yv1+JLxjxb 3JPYkjkUyy9CyDswWusLdOL3ughezvTPpq0cOcowwcGwwEiA+pWvX46LD0gKeKZX0 MumJqWLycnvP+pyDLywIDAQAB;	default._domainkey. [REDACTED]	IN	14399

Use this tool to generate your DKIM record.



k1

_domainkey.

beispiel.de

Generate DKIM Record

Private key



You must enter this key in your DKIM signer. **It must be kept secret, as anyone with access to it can stamp tokens pretending to be you**

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC8AFW5fRb7ydXqHmdVOCIkh3kj4ZwI0zCJafRqo9ps+toH1Npg
zhUV4iUzwFipshRPhk9SeaCPYTXGcSEccDMA1QUvowc3L1eXo7yzCEpv+mBJsegi
ux/zniTcd2gS1UIoExVSxRx37HtYWUyydiy1Cve/JPTVeIMThvVaeDdCcQIDAQAB
AoGALQ93fIn65EawOvkmk0ptBIxkALGmkIbt70GyD410YSi08Zo/7Uv3ydL2T70c
9F12fMkYYhA856DJHtMmuIafp/4zeeNEPfvBfVGGfRLbDDcOcRag3ufvKxMQj7M3
bgMbB/diXb+SGLce7N2b2+aIT1x8iJ3uhTnY7rojdlwYkECQQDhJrSkvHh9a20I
3noJjXkVI8WwKIKdihQaKkXIZ6wkelg5IiKZCuI9p0b6tUndbb1r1Cv0/xEoR9D
ChDwA9QFAkEA1cKT6pHpZPERJHyXXiyE6NutvUSJoYc4uU9a+TOexw/hy0AoAXxi
ZyzKa5cI4WDTz0sLEhQD3bnU7t08N66MfQJ8ALCJIrbQOEFOy+1aU6HN1ZSk1ZyM
DAanT1+8qX6bGzR2JhQc3Jp2NFRt2X4cQQLxmPi6368drf05wENWTzWCKukCQApK
YrqRka49WfLYsiTLed6H7NZGvWV0UAvDwTpr/MHShuk0/ngL1+TlqB0D2V6YPboI
urC1G/aJorGYqd/4XDUCQQDcz6+60niT15z/ygeotzGbp3z5xWfNn3Vqcw/6SDr
ZANK58NLYiXsa+pue2/dBk6jdd59FXHKi/bbpXgCh82p
-----END RSA PRIVATE KEY-----
```

Public key



This is the public key in the original raw "X509" format. It's not usable in DNS directly, but it might be useful for something else.

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQC8AFW5fRb7ydXqHmdVOCIkh3kj
4ZwI0zCJafRqo9ps+toH1NpgzhUV4iUzwFipshRPhk9SeaCPYTXGcSEccDMA1QUv
owc3L1eXo7yzCEpv+mBJsegiux/zniTcd2gS1UIoExVSxRx37HtYWUyydiy1Cve/
JPTVeIMThvVaeDdCcQIDAQAB
-----END PUBLIC KEY-----
```

Generated DKIM Record

v=DKIM1;t=s;p=MIGfMA0GCsGSIb3DQEBAQUAA4GNADCBiQKBgQC8AFW5fRb7ydXqHmdVOCIkh3kj4ZwI0zCJafRqo9ps+toH1NpgzhUV4iUzwFipshRPhk9SeaCPYTXGcSEccDMA1QUvowc3L1eXo7yzCEpv+mBJsegiux/zniTcd2gS1UIoExVSxRx37HtYWUyydiy1Cve/JPTVeIMThvVaeDdCcQIDAQAB



Please, publish above DNS TXT record on **k1._domainkey.beispiel.de** subdomain

ESET Mailsecurity Exchange – SPF

- SPF steht für Sender Policy Framework.
- Der empfangende Mailserver prüft die Echtheit von Absenderadressen anhand einer IP-Adressen Liste die er über den SPF Record abfragen kann.
- Der empfangende Mailserver nimmt nur E-Mails von den gelisteten IP-Adressen an.
- SPF schützt nicht vor Spoofing. Ein Betrüger kann trotzdem einen falschen Absender in der E-Mail anzeigen.
- Auch ein Spammer kann SPF verwenden.
- Wenn jemand unautorisiert über ihren Mailserver sendet, greift SPF nicht. Thema Relaying.

ESET Mailsecurity Exchange – SPF

Beispiel: Der SPF-Eintrag von *gmx.com*

– *gmx.com*

```
v=spf1 ip4:213.165.64.0/23 ip4:74.208.5.64/26 ip4:74.208.122.0/26 ip4:212.227.126.128/25 ip4:212.227.15.0/24  
ip4:212.227.17.0/27 ip4:74.208.4.192/26 ip4:82.165.159.0/24 ip4:217.72.207.0/27 -all
```

- ☁ 213.165.64.0/23
- ☁ 74.208.5.64/26
- ☁ 74.208.122.0/26
- ☁ 212.227.126.128/25
- ☁ 212.227.15.0/24
- ☁ 212.227.17.0/27
- ☁ 74.208.4.192/26
- ☁ 82.165.159.0/24
- ☁ 217.72.207.0/27



Regeln – Postfachdatenbank - Schutz

Regel Postfachdatenbank Schutz – Bedingung I

Regel

Bedingung hinzufügen

Typ

Operation

Betreff

Absender

Domäne des Absenders

Empfänger

Postfach

Name des Anhangs

Größe des Anhangs

Art des Anhangs

Nachrichtenheader

Scan-Ergebnis des Virenschutzes

Uhrzeit des Empfangs

Anhang ist ein passwortgeschütztes Archiv

Anhang ist ein beschädigtes Archiv

Ordnername

Hinzufügen Bearbeiten Entfernen

Regel Postfachdatenbank Schutz – Bedingung II

Bedingung hinzufügen

?

□

×

Typ

Betreff

Operation

ist / ist Teil von

ist / ist Teil von

ist nicht / ist nicht Teil von

enthält

enthält nicht

Treffer für regulären Ausdruck

kein Treffer für regulären Ausdruck

Hinzufügen

Bearbeiten

Entfernen

Importieren

Exportieren

Regel Postfachdatenbank Schutz – Aktion

Aktion hinzufügen

Typ

Nachricht löschen

Nachricht löschen

Anhänge in Quarantäne verschieben

Anhang löschen

Anhang durch Aktionsinformationen ersetzen

In Ereignislog aufnehmen

Ereignisbenachrichtigung an Administrator senden

Scan durch Virenschutz überspringen

Andere Regeln erstellen

Hinzufügen

Bearbeiten

Löschen

Aktionstyp	Parameter
------------	-----------

The background is a dark, abstract composition. It features a city skyline in the distance, rendered in a dark blue tone. In the foreground, there are numerous bright blue light trails and streaks that radiate from the bottom center towards the horizon, creating a sense of motion and depth. The overall color palette is dominated by deep blues and blacks, with the light trails providing a vibrant contrast.

Regeln – Mail-Transport Schutz

Regel Postfachdatenbank Schutz – Regeln

Regeln

? □ ×

Aktiv	Name	Stufe	Treffer	🔍
☒	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 Anhängen	0	
☒	Archivdateianhänge mit Passwortschutz	Verarbeitung von Ergebnissen	0	

Hinzufügen

Bearbeiten

Entfernen

Hoch

Runter

Regel Postfachdatenbank Schutz – Bedingung I

Regel

Aktiv

Name

Beding

Art des

Hinzuf

Aktion

In Ereig

Anhang

Bedingung bearbeiten

Typ

Art des Anhangs

+ ☐ Ausführbare Dateien

- ☒ Office-Dateien

+ ☒ Dokumente

+ ☒ Tabellenkalkulationsblätter

+ ☒ Präsentationen

OK Abbrechen

Regel Postfachdatenbank Schutz – Bedingung II

Bedingung hinzufügen

Typ

Operation

Betreff

Nachrichtengröße

Nachrichtenheader

Nachrichtentext

Interne Nachricht

Ausgehende Nachricht

Signierte Nachricht

Verschlüsselte Nachricht

Scan-Ergebnis des Spam-Schutzes

Scan-Ergebnis des Virenschutzes

Scan-Ergebnis des Phishing-Schutzes

Uhrzeit des Empfangs

Enthält passwortgeschütztes Archiv

Enthält beschädigtes Archiv

DKIM-Ergebnis

SPF-Ergebnis

DMARC-Ergebnis

Hat Reverse-DNS-Eintrag

NDR-Prüfergebnis

SPF-Ergebnis - From-Header

Vergleichsergebnis zwischen Umschlag-Absender und From-Header

Hinzufügen Bearbeiten Entfernen

Regel Postfachdatenbank Schutz – Aktion

Aktion hinzufügen

Typ

Nachricht in Quarantäne verschieben

Kann von Benutzern freigegeben werden

Aktionstyp	Parameter

Hinzufügen

Bearbeiten

Löschen

Nachricht in Quarantäne verschieben

Nachricht ablehnen

Nachricht automatisch löschen

Anhänge in Quarantäne verschieben

Anhang löschen

DMARC-Policy übernehmen

SCL-Wert festlegen

In Ereignislog aufnehmen

Ereignisbenachrichtigung an Administrator senden

Scan des Spam-Schutzes überspringen

Scan durch Virenschutz überspringen

Scan des Phishing-Schutzes überspringen

Andere Regeln erstellen

Betreffpräfix hinzufügen

Header-Feld hinzufügen

Header-Felder entfernen

Unterschiedliche Quarantänen

The background of the slide is a dark, abstract composition. It features a central perspective view of a path or road that recedes into the distance, flanked by what appear to be stylized, glowing blue lines and structures. The overall color palette is dominated by deep blues and blacks, with bright blue highlights that create a sense of depth and movement. The title text is centered within a white rectangular border.

ESET Mailsecurity Exchange – Quarantänen

E-MAIL-QUARANTÄNE 10

Quarantänetyyp

- Lokale Quarantäne
- Quarantäne-Postfach
- MS Exchange-Quarantäne
- Lokale Quarantäne

Nachrichten für nicht vorhandene Empfänger speichern

Überprüfung von

ESET Mailsecurity Exchange – Lokale Quarantäne

- Die lokale Quarantäne stellt jedem AD-Benutzer seine individuelle Quarantäne zur Verfügung
- Weboberfläche kann z.B. in das Intranet integriert werden.
- Der Exchange-Administrator kann zusätzlich berechtigt werden.
- Vorteil: Jeder Benutzer weiß selber am besten welche E-Mails er benötigt und welche nicht.
- Jeder Benutzer kann durch gezieltes Reporting informiert werden, wenn sich neue Objekte in der Quarantäne befinden.
- SPAM oder False-Positive können durch den Benutzer freigegeben werden.
- Viren verbleiben immer in der Quarantäne, der Benutzer kann sie nicht freigeben.

ESET Mailsecurity Exchange – Lokale Quarantäne

 E-MAIL-QUARANTÄNE

?

 PRE\PATRIK

 KONTEN WECHSELN

 ABMELDEN

SUCHEN

eingehend

BETREFF

von

☒ SPAM

☒ SCHADSFTWARE

☒ REGEL

☒ PHISHING

☒ ABSENDER GEFÄLSCHT

AUSFÜHREN

EMPFANGSDATUM		BETREFF	UMSCHLAG-ABSENDER	VON	EMPFÄNGER	GRUND	TYP	OBJEKT	FREIGEBEN ALLE AUSWÄHLEN	LÖSCHEN ALLE AUSWÄHLEN	KEINE AKTION ALLE AUSWÄHLEN
2022-02-16 10:40		test link	patrik@werren.com	patrik@werren.com	patrik@eset-	https://www.amtso.org/check-	phishing		☐	☐	☒
2022-02-07 00:06		Fwd: Gr	patrik@werren.com	patrik@werren.com	patrik@eset-	Advanced heuristic classified mail as	spam		☐	☐	☒
2022-02-06 17:22		WG: [SP	patrik@werren.com	patrik@werren.com	patrik@eset-	URL (krugerwilliamorg.com) found	spam		☐	☐	☒
2021-09-15 04:33		LOAN O	info1@creditunions.co.uk	info1@creditunions.co.uk	info@eset-	Domain	spam		☐	☐	☒
2021-09-14 16:27		eeee	patrik@werren.com	patrik@werren.com	info@eset-	Found GTUBE test string	spam		☐	☐	☒

Gesamt: 5 Einträge

SEITENGRÖSSE 

AUSFÜHREN

ESET Mailsecurity Exchange – Quarantäne Postfach

- ESET Mail Security erstellt eine separate Wrapper-E-Mail mit zusätzlichen Informationen und den ursprünglichen E-Mails als Anhang, und stellt diese E-Mail an das Postfach zu.
- Der SPAM-Administrator kann in dem Postfach die E-Mail falls nötig an die Mitarbeiter weiterleiten.
- Der Mitarbeiter hat selber keinen direkten Zugriff auf die Quarantäne.

ESET Mailsecurity Exchange – MS Exchange-Quarantäne

- Der Exchange Server ist für die Zustellung der E-Mail an das Postfach verantwortlich. Das Postfach muss in Active Directory auf der Organisationsebene als Quarantäne festgelegt werden. Verwenden Sie dazu den unten gezeigten PowerShell-Befehl.
- E-Mails werden an dieser Stelle im Original gespeichert.
- Die interne Quarantäne ist in Microsoft Exchange Server standardmäßig deaktiviert.

PowerShell: `Set-ContentFilterConfig -QuarantineMailbox name@domain.com`



SPAM, Phishing & Virenschutz testen

SPAM, Phishing & Virenschutz testen

Um den **Spam-Schutz** zu testen, verschicken Sie eine E-Mail mit der folgenden 68 Byte-Zeichenfolge im Nachrichtentext:

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

Um den **Phishing-Schutz** zu testen, senden Sie eine E-Mail mit dem folgenden Link (URL) im Nachrichtentext oder im Betreff:

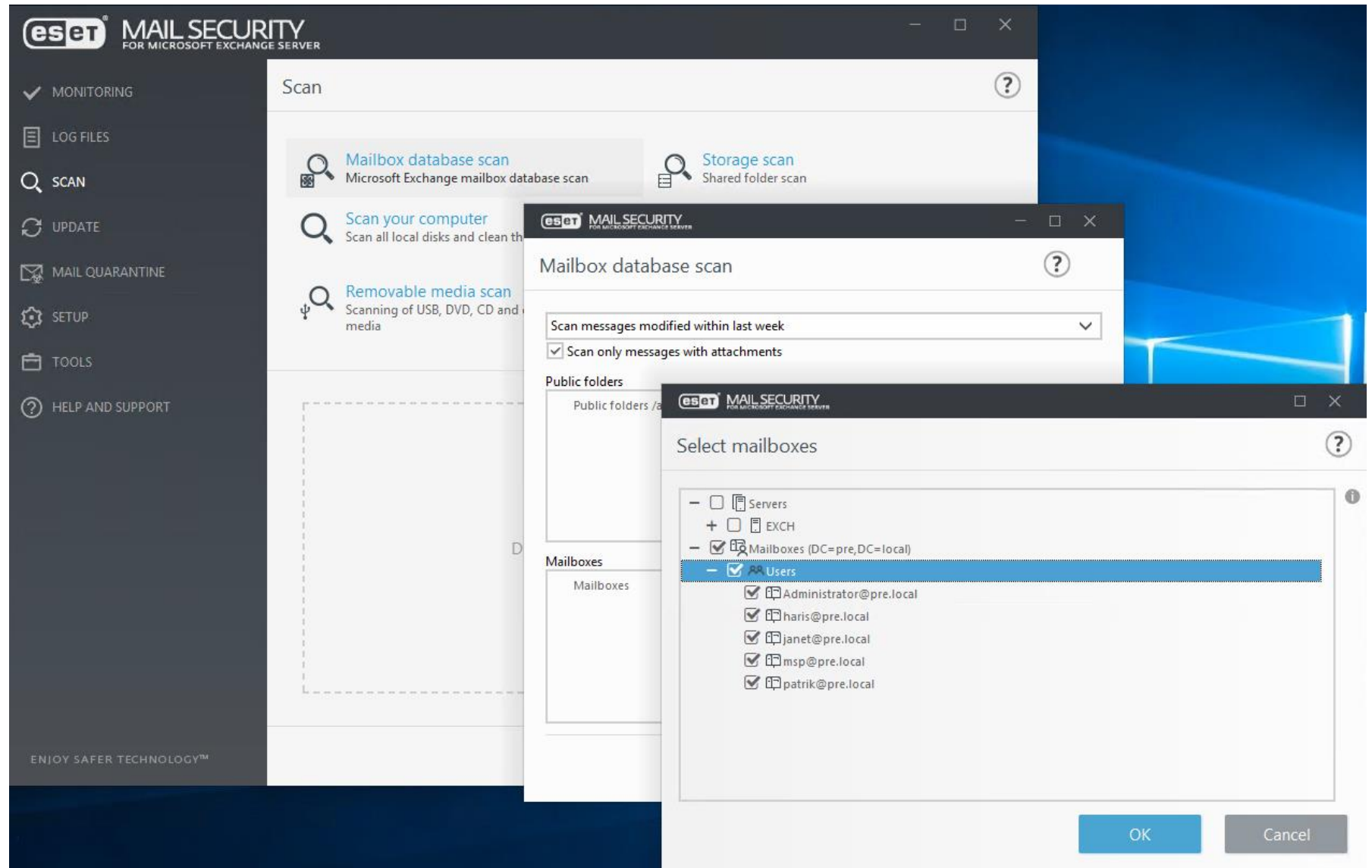
<https://www.amtso.org/check-desktop-phishing-page/>

Um Ihre **Virenschutzfunktion** zu testen, erstellen Sie eine Textdatei, die die folgende Zeichenfolge enthält und verschicke diese per E-Mail an ihre interne Adresse:

X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Postfach Scan über GUI

Postfach Scan über Mailsecurity GUI



Postfach Scan über PROTECT

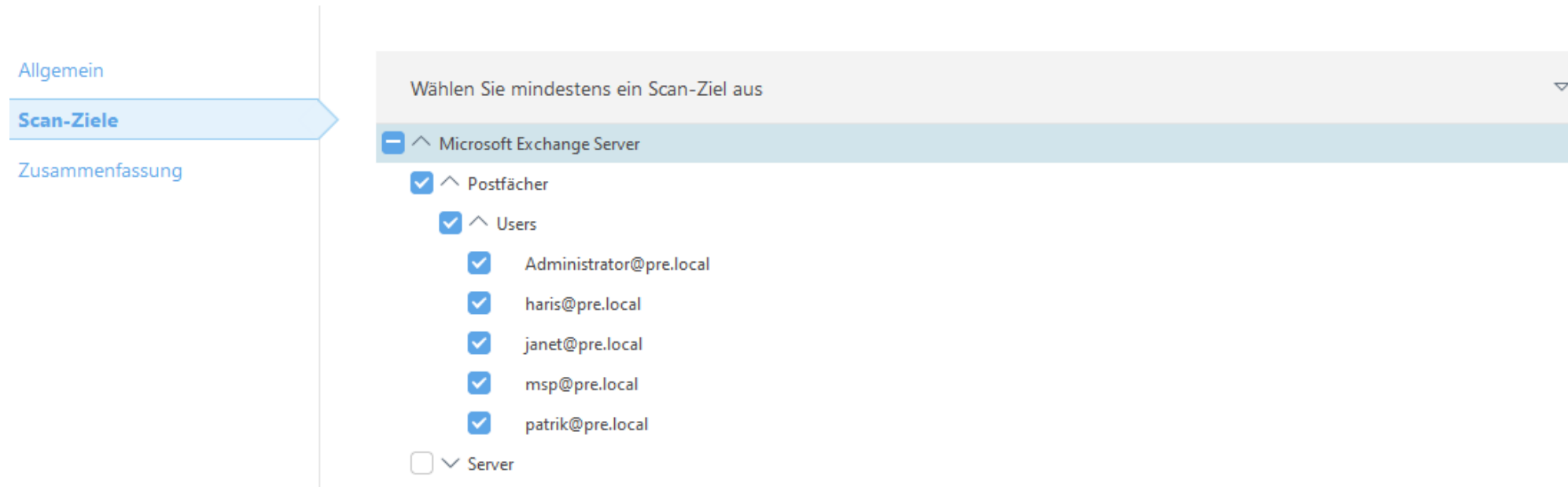
Postfach Scan über PROTECT

- Damit der ESET PROTECT die Exchange Server oder einzelne Mailboxen zentral scannen kann, müssen die Scan Ziele ausgelesen werden.
- Die Einstellung wird in der ESET Exchange Policy gemacht.

The screenshot displays the ESET PROTECT management console interface. On the left, a sidebar menu under the heading 'TOOLS' (with a count of 7) lists several options: 'Log-Dateien', 'Proxyserver' (with a count of 3), 'Benachrichtigungen', 'Präsentationsmodus', 'Diagnose', and 'Cluster'. The main content area on the right shows a list of configuration items. The first two are 'LIZENZ' and 'WMI-ANBIETER'. The third item, 'SCAN-ZIELE FÜR DIE ESET MANAGEMENT-KONSOLE' (with a count of 2), is expanded to show two settings: 'Liste der Ziele generieren' (checked with a blue toggle) and 'Aktualisierungsintervall [Minuten]' (set to 360).

Postfach Scan über PROTECT

- Der Scan wird über einen Client-Task als «Server Prüfung» eingerichtet.



- Der Trigger kann auf täglicher, wöchentlicher oder monatlicher Basis erfolgen !

The background is a dark teal color. It features several bright, glowing teal lines that curve and radiate across the frame, creating a sense of motion and depth. In the upper right corner, there is a faint, stylized image of a cityscape or architectural structure, also in a teal hue, which blends into the overall color scheme.

Vielen Dank !!!