ESET Mailsecurity Exchange

Patrik Werren

ESET Mailsecurity Exchange – Agenda

- ESET Mailsecurity Exchange Architektur
- ESET Clustermodus - Besonderheiten
- NDR – DKIM - SPF

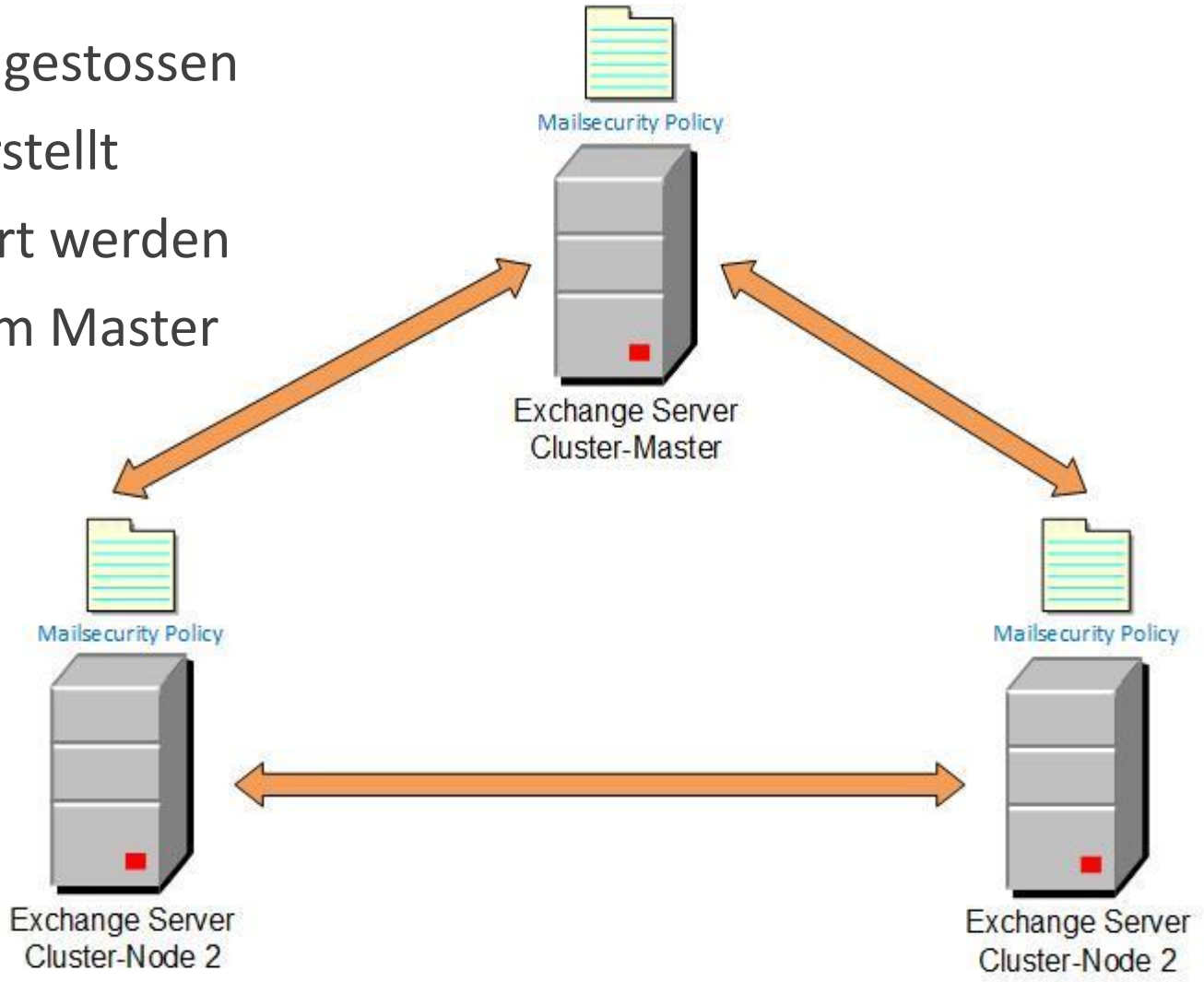
- Policy Einstellungen
    - Viren und Spyware Schutz
    - Spam Schutz
    - Phishing Schutz
    - Greylisting
    - Regeln für Postfachdatenbank und Mail-Transport-Schutz
    - Unterschiedliche Quarantänen

- 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

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

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

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 Nachriten 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 Maailserver 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=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvi0IegM87KrTtjm3hD1cfi5DbDOByXWa637WyXssemq1d+BXfFr+Ztdx5Ry/+dZ984zv/y4v8hnFerGEWsusc4dixZ4Jy+wqSJKhS2nHPVKQgC7WAM7v0sX6LoMTXtSH0pClBUx0qsTjL5TD2eVw5/rQJ97C9PkQHlbK87FXkWb0vn9RgkFaOjv96n0qhUvXANuRNXZGIuZqIsfw3WCNfjipjbLPzb0iBKR7VyB0vdmsBNCumk6C9FP8yvl+JLxjxb3JPYkjkUyy9CyDswWusLdOL3ughezvTPpq0cOcowwcGwwEiA+pWvX46LDOgKeKZX0MumJqWLycnvP+pyDLywIDAQAB;	default._domainkey.[redacted]	IN	14399

DKIM Record Generator

Lookup DKIM

Use this tool to generate your DKIM record.

k1 _domainkey. beispiel.de

Generate DKIM Record

Private key

Copy

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+toHlNpg
zhUV4iUzwFIpshRPhk9SeaCPYTXGcSEccdMA1QUvowc3L1eXo7yzCEpv+mBJsegi
ux/zniTcd2gS1UIoExVSxRx37HtYWUyydiy1CVe/JPTVeIMThvVaeDdCcQIDAQAB
AoGALQ93fIn65EawOvkmk0ptBIxkALGmkIbt70GyD41OYSiO8Zo/7Uv3ydL2T70c
9Fl2fMkYYhA856DJHtMmuIafp/4zeeNEPfvBfVGGfRLbDDcOcRAg3ufvKxMQj7M3
bgMbB/diXb+SGLce7N2b2+aI7IT1x8iJ3uhTnY7rojdWYkECQQDhJrSkvHh9a20I
3noJjXkVI8WwKIkdihQaKkXIZ6wkeWlg5IiKZCuI9p0b6tUndbblr1Cv0/xEoR9D
ChDwA9QFAkEA1cKT6pHpZPErJHyXXiyE6NutvUSJoYc4uU9a+TOexw/hy0AoAXxi
ZyzKa5cI4WDTzOsLEhQD3bnU7tO8N66MfQJBALCJIrbQOEFOy+1aU6HN1ZSk1ZyM
DAanT1+8qX6bGzR2JhQc3Jp2NFRt2X4cQQlxmPi6368drf05wENWTzWCKukCQApK
YrqRKa49WflYsiTLed6H7NZGvWV0UAvDwTpr/MHShuk0/ngL1+TlqB0D2V6YPboI
urC1G/aJorGYqd/4XDUCQQDcz6+6OniTl5z/ygeotzGbpm3z5xWfNn3Vqcw/6SDr
ZANK58NLYiXsa+pue2/dBk6jdd59FXHKi/bbpXgCh82p
-----END RSA PRIVATE KEY-----
```

Public key

Copy

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-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8AFW5fRb7ydXqHmdVOCIkh3kj
4ZwI0zCJafRqo9ps+toHlNpgzhUV4iUzwFIpshRPhk9SeaCPYTXGcSEccdMA1QUv
owc3L1eXo7yzCEpv+mBJsegiux/zniTcd2gS1UIoExVSxRx37HtYWUyydiy1CVe/
JPTVeIMThvVaeDdCcQIDAQAB
-----END PUBLIC KEY-----
```

Generated DKIM Record

```
v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8AFW5fRb7ydXqHmdVOCIkh3kj4ZwI0zCJafRqo9ps+toHlNpgzhUV4iUzwFIpshRPhk9SeaCPYTXGcSEccdMA1QUvowc3L1eXo7yzCEpv+mBJsegiux/zniTcd2gS1UIoExVSxRx37HtYWUyydiy1CVe/JPTVeIMThvVaeDdCcQIDAQAB
```

Copy

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 schütz 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 Mailsever sendet, greift SPF nicht. Thema Relaying.

ESET Mailsecurity Exchange – SPF

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

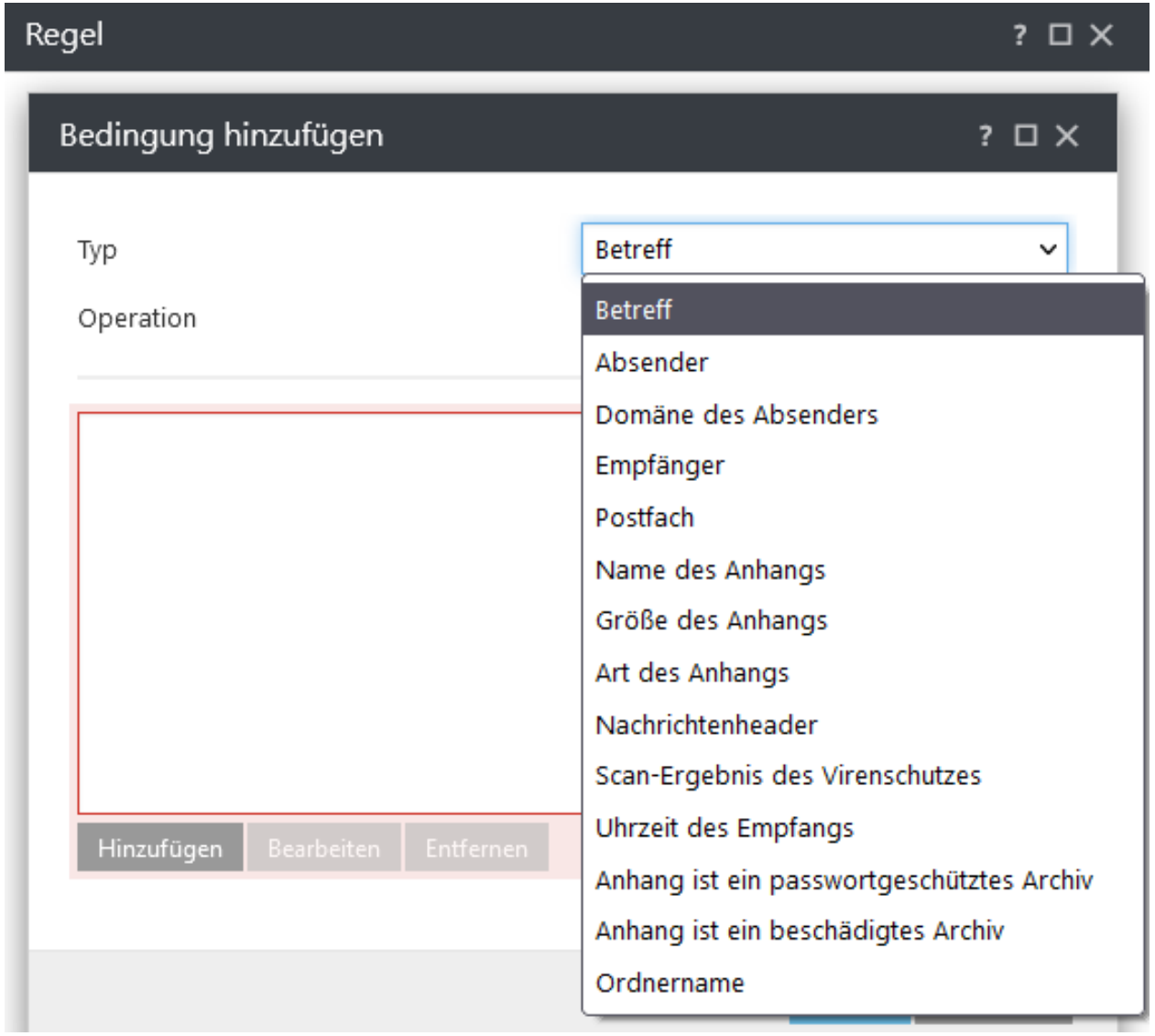
– gmx.com

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

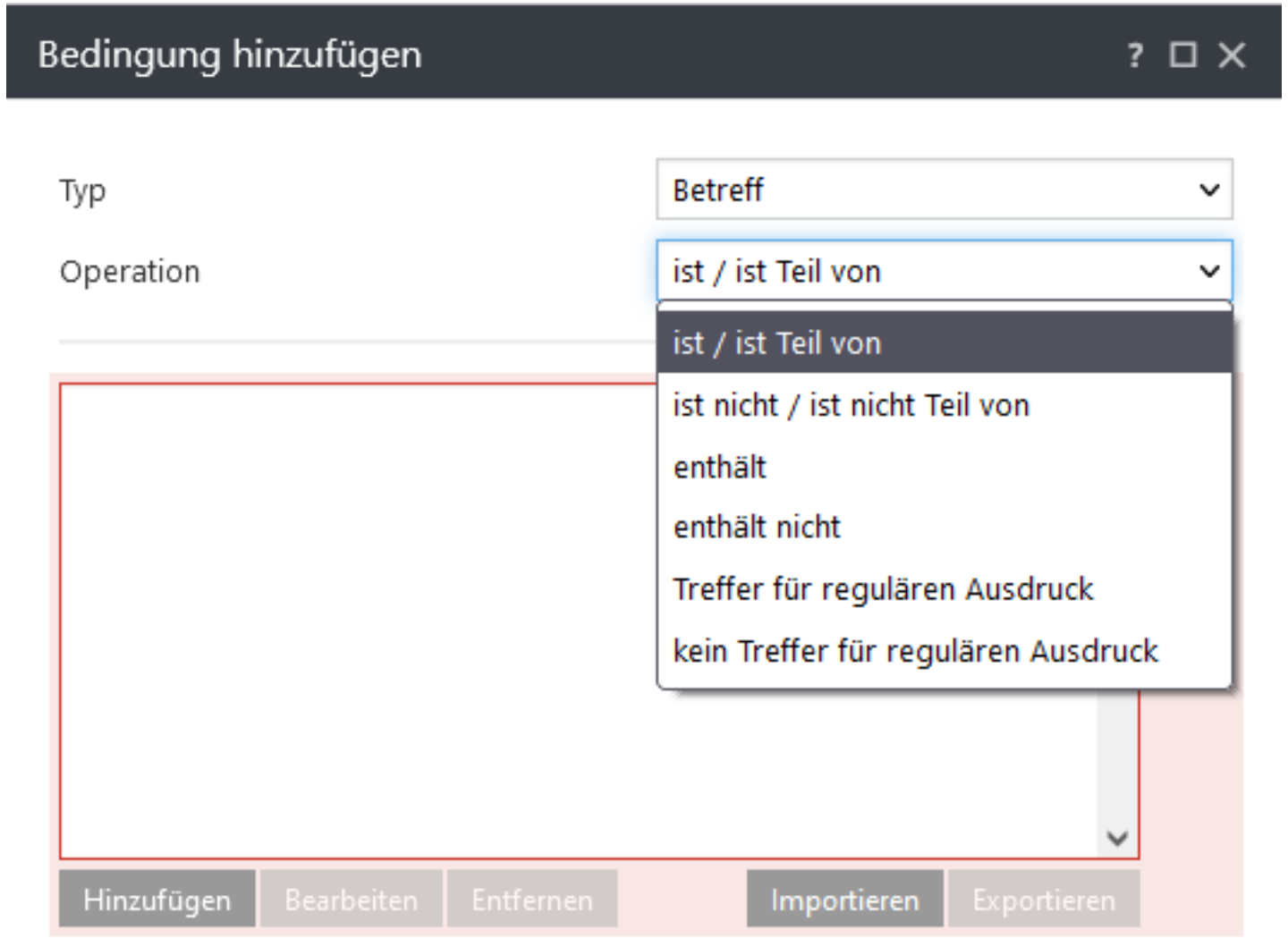
- *213.165.64.0/23*
- *74.208.5.64/26*
- *74.208.122.0/26*
- *212.227.126.128/25*
- *212.227.15.0/24*
- *212.227.17.0/27*
- *74.208.4.192/26*
- *82.165.159.0/24*
- *217.72.207.0/27*

Regeln – Postfachdatenbank - Schutz

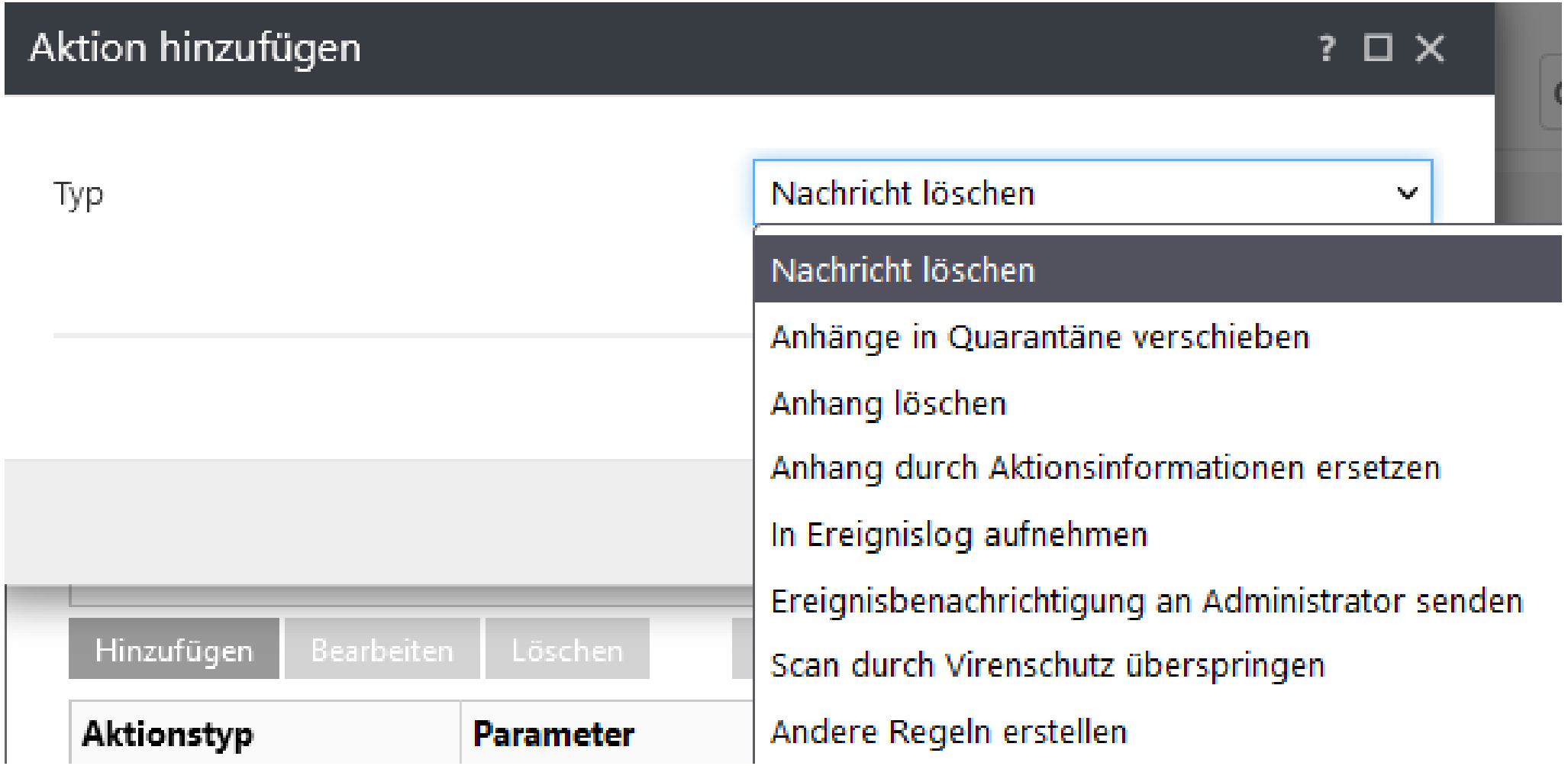
Regel Postfachdatenbank Schutz – Bedingung I



Regel Postfachdatenbank Schutz – Bedingung II

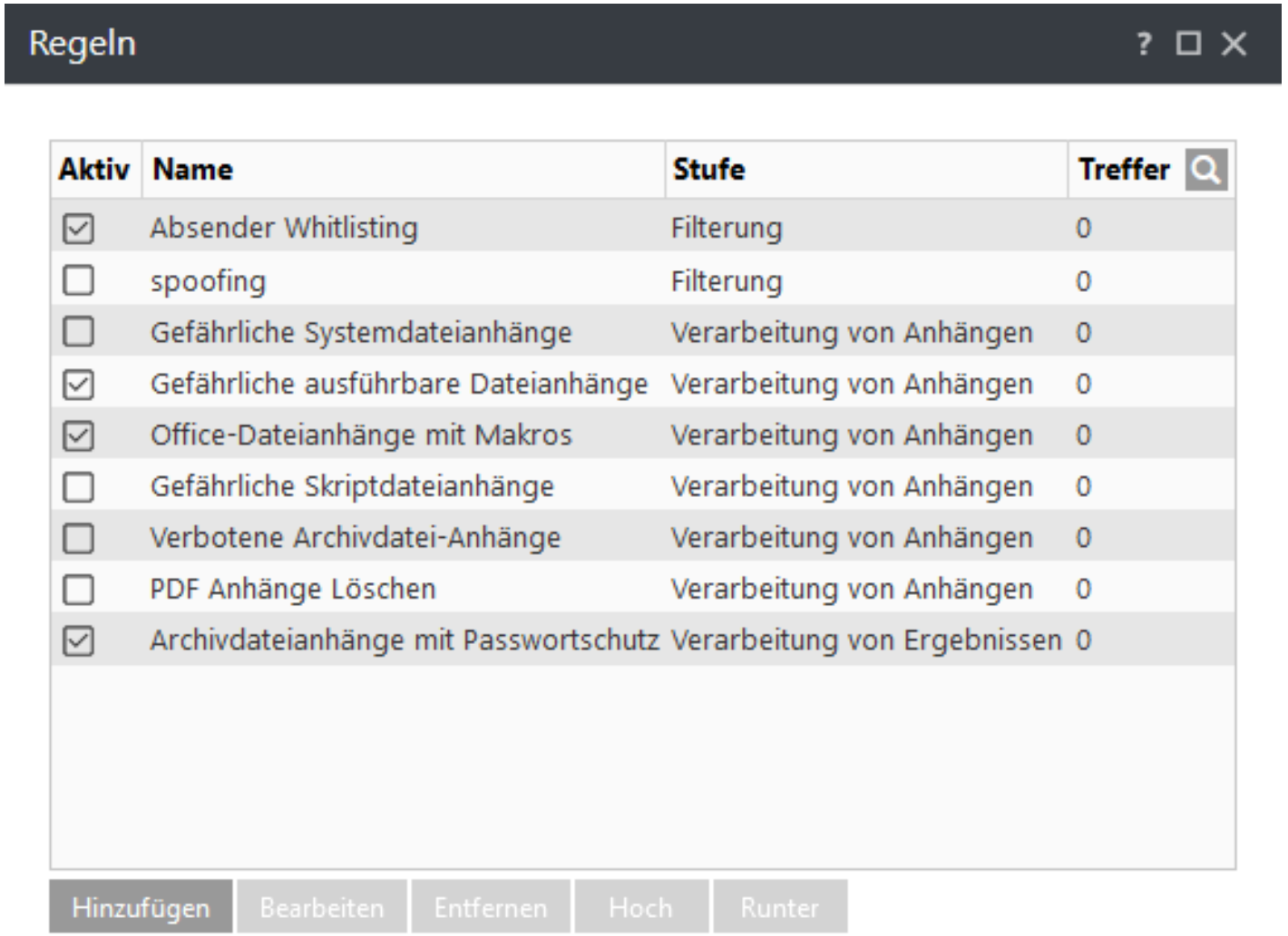


Regel Postfachdatenbank Schutz – Aktion

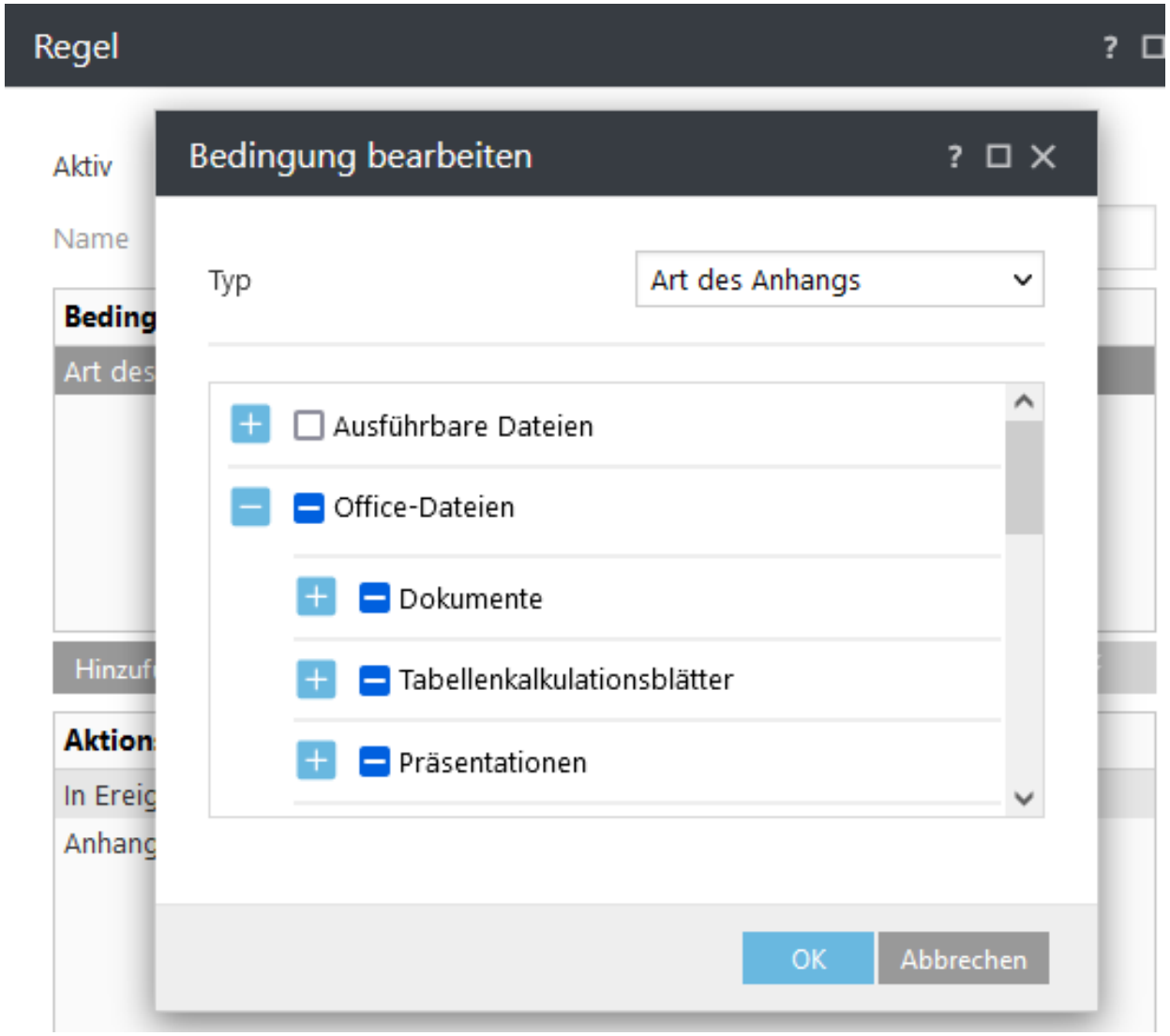


Regeln – Mail-Transport Schutz

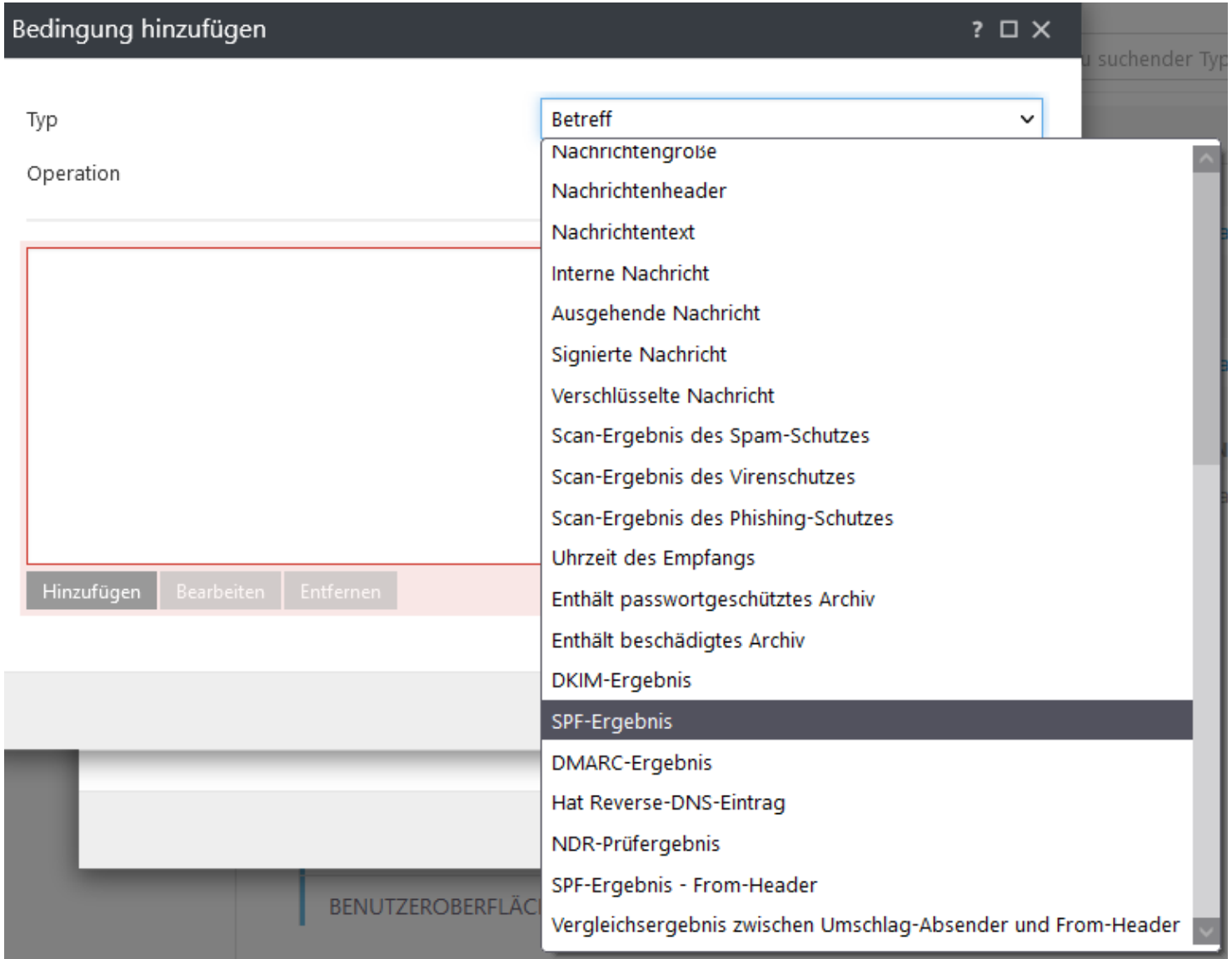
Regel Postfachdatenbank Schutz – Regeln



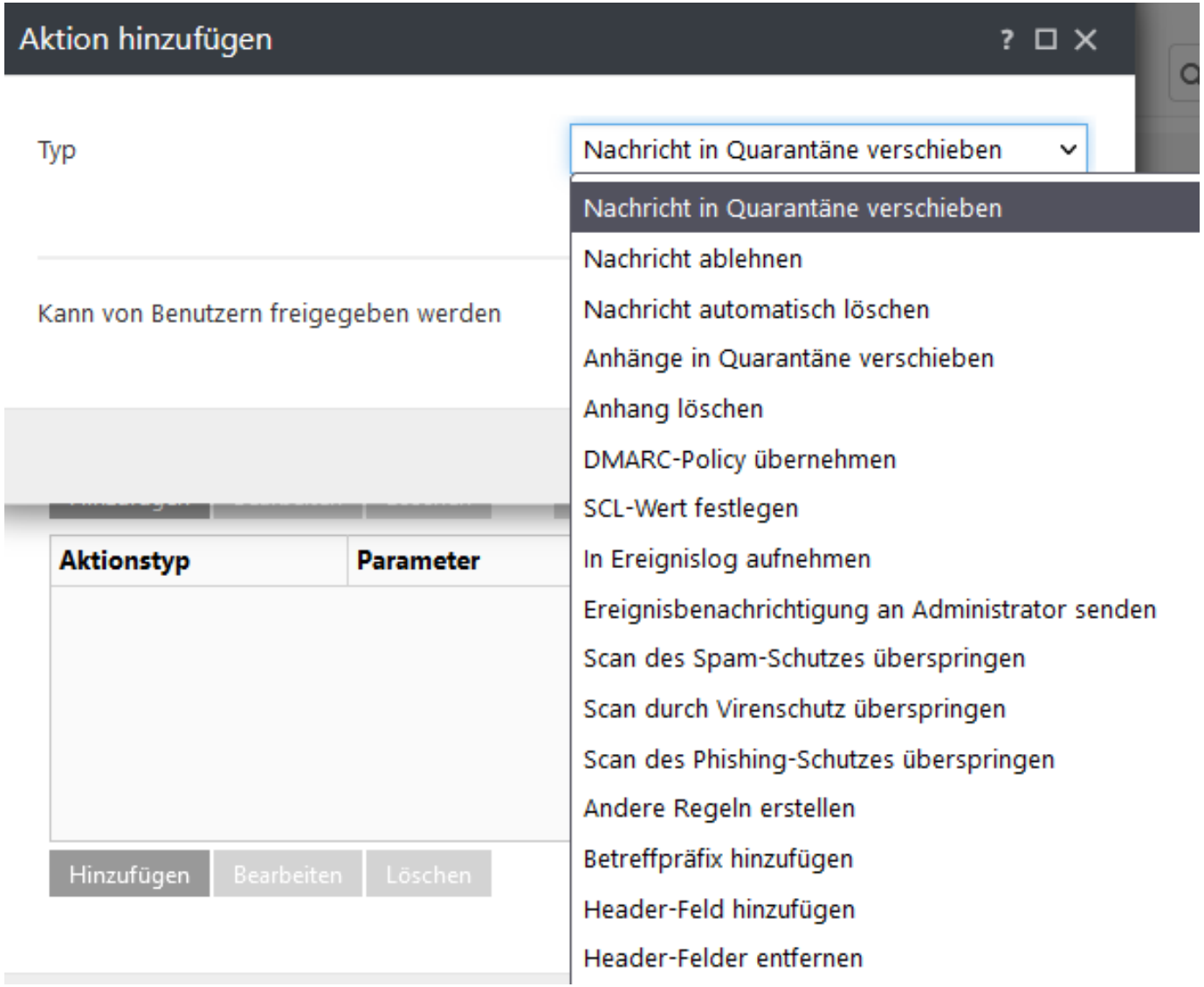
Regel Postfachdatenbank Schutz – Bedingung I



Regel Postfachdatenbank Schutz – Bedingung II

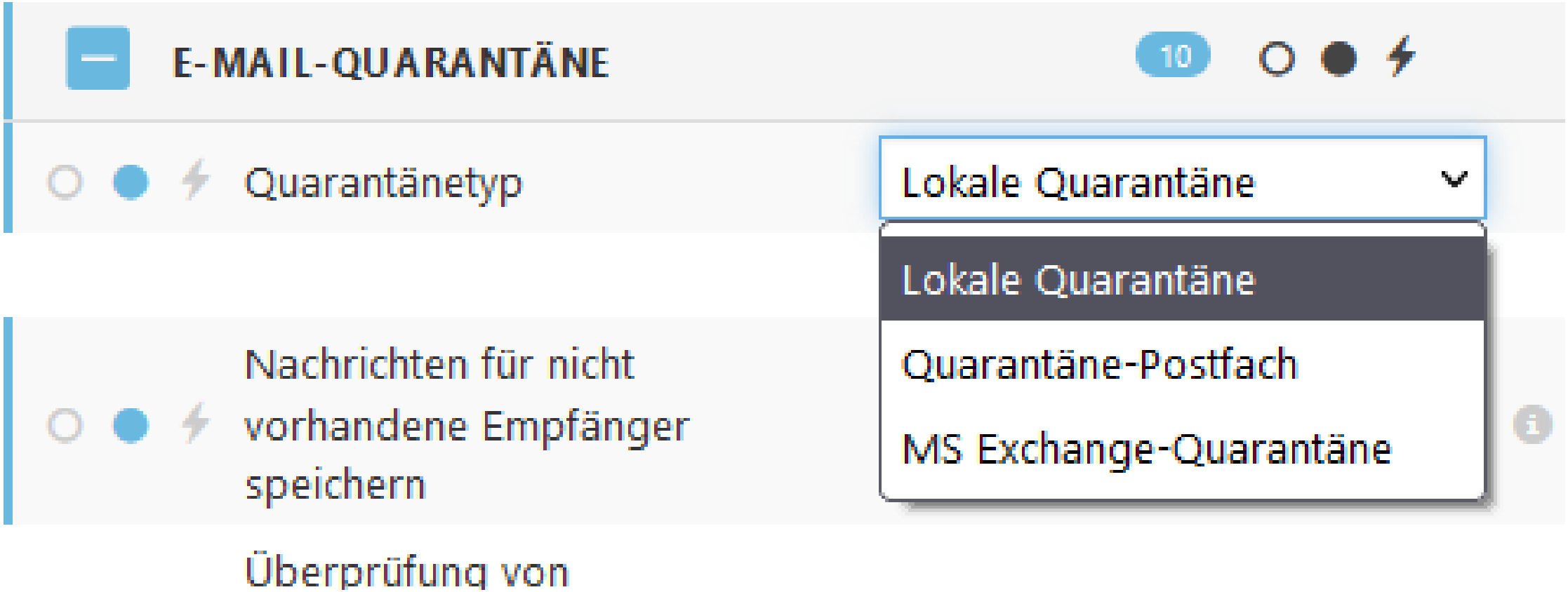


Regel Postfachdatenbank Schutz – Aktion



Unterschiedliche Quarantänen

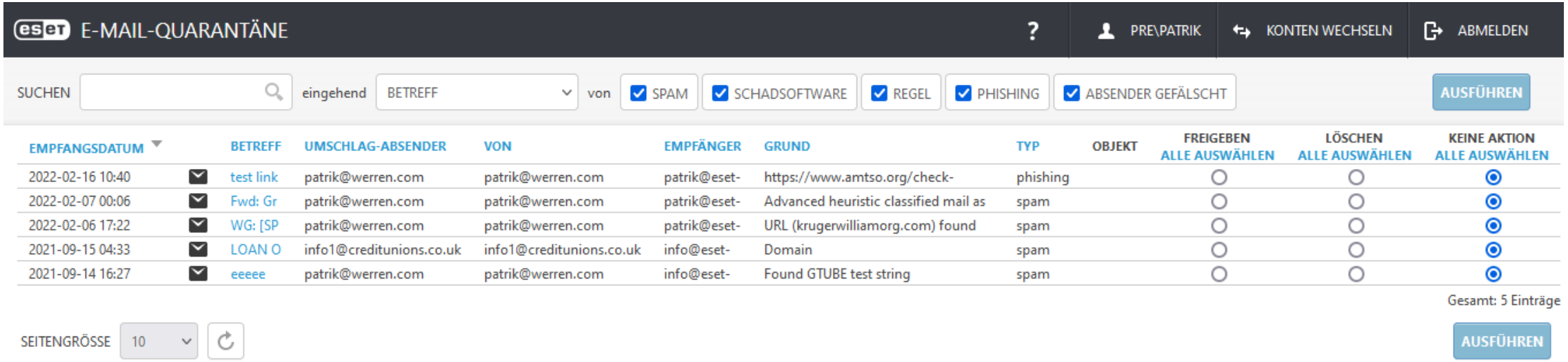
ESET Mailsecurity Exchange – Quarantänen



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



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:

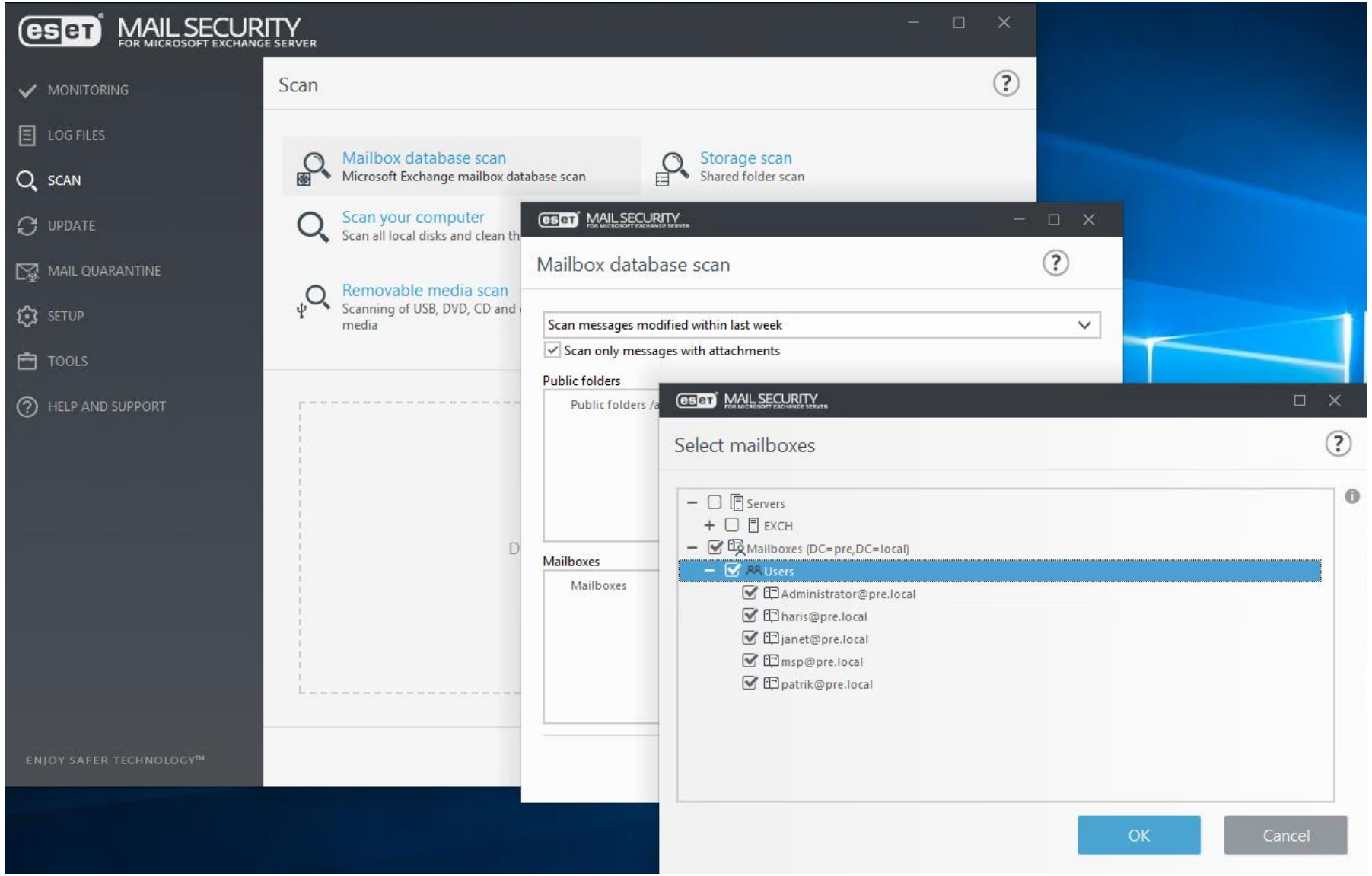
https://www.amtso.org/check-desktop-phishing-page/

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



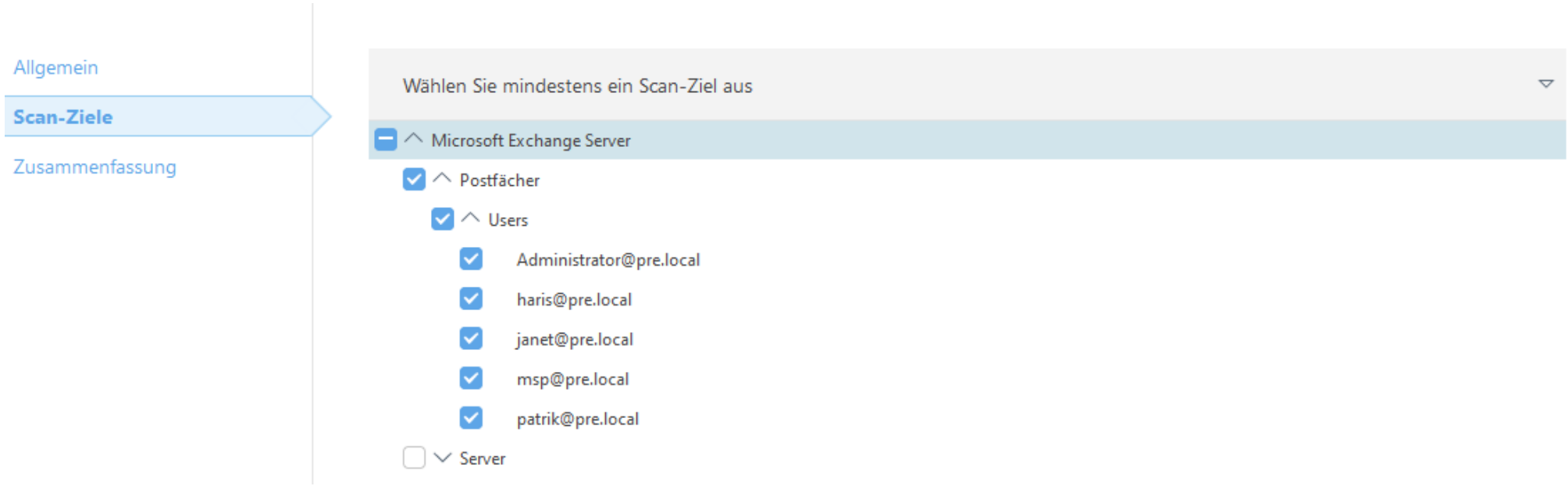
Postfach Scan über PROTECT

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.

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 !

Vielen Dank !!!