noSpam proxy® SERVER

Secure User Guidance

im Rahmen der Beschleunigten Sicherheitszertifizierung (BSZ)

Version 14

Net at Work
Building IT-Excellence.

Rechtliche Hinweise

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Deutschland

DIESES DOKUMENT WURDE ZULETZT AM 03. NOVEMBER 2023 ÜBERARBEITET.

Inhalt

Versionsverlauf

Datum	Version	Autor	Änderungen
18.10.2023	1.0	Joepen	Die Dokumente " NoSpamProxy Configuration Guidelines" und "Secure Installation Guide" wurden nach den Konventionen des BSI BSZ zusammengefasst.

Einleitung

Dieses Dokument wird im Rahmen der BSI-BSZ-Zertifizierung des E-Mail Security Gateways NoSpamProxy bereitgestellt. Es bezieht sich auf NoSpamProxy Server Version 14 und Windows Server 2022 und spezifiziert die Installations- und Konfigurationsregeln, die für den Betrieb des Produkts in der zertifizierten Konfiguration gelten.

Die Schritt-für-Schritt-Anleitung bezieht sich auf das Benutzerhandbuch zur NoSpamProxy Server Suite Version 14:

- **Deutsch| https://docs.nospamproxy.com/Server/14/pdf/de/NoSpamProxy-Server-Suite-Manual.pdf**
- **Englisch| https://docs.nospamproxy.com/Server/14/pdf/en/NoSpamProxy-Server-Suite-Manual.pdf**

Außerdem sich dieses Dokument auf das NoSpamProxy-Installationshandbuch:

- **Deutsch| https://docs.nospamproxy.com/Server/14/pdf/de/NoSpamProxy-Server-Installation-Manual.pdf**
- **Englisch| https://docs.nospamproxy.com/Server/14/pdf/en/NoSpamProxy-Server-Installation-Manual.pdf**

Die hier beschriebenen Konfigurationsschritte müssen durchgeführt werden, um ein ordnungsgemäß funktionierendes NoSpamProxy-System zu erhalten, das den Sicherheitsvorgaben entspricht, die im Dokument *BSZ Security Target* für NoSpamProxy beschrieben sind.

Installation von NoSpamProxy

1. Nach der Installation ist ein selbstsigniertes Zertifikat für die Web App hinterlegt, das durch ein vertrauenswürdiges Zertifikat ersetzt werden sollte. Verfahren Sie so, wie im **Installationshandbuch** unter **Nach der Installation > Konfigurieren des Zertifikats für die Web App** beschrieben. Das Zertifikat sollte von einer CA ausgestellt sein, die im Microsoft Trusted CA Store gespeichert ist. Es muss außerdem die Anforderungen von BSI TR-02102-1 und TR-02103 erfüllen.
2. Konfigurieren Sie den Eintrag *Local Security Authority Hostname*. Folgen Sie dabei Hinweisen unter **Das Web Portal wird parallel zur Gatewayrolle und/oder Intranetrolle betrieben** auf der Seite **Hinweise zur Einbindung des Web Portals**. Stellen Sie sicher, dass Sie alle gewünschten Hostnamen für den Konfigurationseintrag verwenden.
3. Erstmalige Konfiguration von NoSpamProxy: Führen Sie den NoSpamProxy-Konfigurationsassistenten im NoSpamProxy Command Center (NCC) aus, sofern dies nicht bereits im Rahmen der Ersteinrichtung erfolgt ist.
4. Nehmen Sie die folgenden Einstellungen/Konfigurationen im NoSpamProxy Command Center vor:
    - Stellen Sie sicher, dass **Verlange STARTTLS (empfohlen)** für den eingehenden Sendekonnektor aktiviert ist:

Pfad	**Konfiguration/E-Mail-Routing/Eingehende Sendekonnektoren/Konnektor/SMTP-Verbindungen/Konfigurierte Verbindung/Verbindungssicherheit**
Element	**Sicherheit der Transportschicht (TLS)**
Empfohlener Wert	**Verlange STARTTLS**

Standardwert	**Erlaube STARTTLS (empfohlen)**
Grund/Auswirkung	**Keine - Einstellung entspricht der Standardkonfiguration.**

- Stellen Sie sicher, dass **Verlange STARTTLS** für den ausgehenden Sendekonnektor aktiviert ist:

Pfad	**Konfiguration/E-Mail-Routing/Ausgehende Sendekonnektoren/Konnektor/Zustellung**
Element	**Sicherheit der Transportschicht (TLS)**
Empfohlener Wert	**Verlange STARTTLS**
Standardwert	**Erlaube STARTTLS (empfohlen)**
Grund/Auswirkung	**Keine - Einstellung entspricht der Standardkonfiguration. Eine Verschärfung führt gegebenenfalls zu Problemen bei der E-Mail-Zustellung.**

- Stellen Sie sicher, dass **Verlange STARTTLS** für den Empfangskonnektor aktiviert ist:

Pfad	**Konfiguration/E-Mail-Routing/ Empfangskonnektoren/Konnektor/Verbindungssicherheit**
Element	**Sicherheit der Transportschicht (TLS)**
Empfohlener Wert	**Verlange STARTTLS**
Standardwert	**Erlaube STARTTLS (empfohlen)**
Grund/Auswirkung	**Keine - Einstellung entspricht der Standardkonfiguration. Eine Verschärfung führt gegebenenfalls zu Problemen beim Empfang von E-Mails.**

- Stellen Sie sicher, dass die Benutzerinformationen gesichert übermittelt werden:

Pfad	**Identitäten/Unternehmensbenutzer**
Element	**Automatischer Benutzerimport**
Empfohlener Wert	**On-Premises-Active-Directory: Aktivieren Sie die Option "Aktiviere Verschlüsselung (empfohlen)"** **Generisches LDAP: Setzen Sie den Port auf 686 und hinterlegen Sie einen Benutzer zur Authentifizierung.**
Standardwert	**On-Premises-Active-Directory: Unverschlüsselte Verbindung**
Grund/Auswirkung	**Die empfohlene Konfiguration bewirkte eine gesicherte Übertragung der Benutzerinformationen.**

- Deaktivieren Sie die Nutzung von Open Keys:

Pfad	**Identitäten/Öffentliche Schlüsselserver**
Element	**Open Keys**
Empfohlener Wert	**Deaktiviert**
Standardwert	**Aktiviert**
Grund/Auswirkung	**Es werden keine Schlüssel mehr über den Dienst Open Keys ermittelt und automatisch zur Verschlüsselung genutzt.**

- Erhöhen Sie die Verschlüsselungsstärke für PDF-Dokumente:

Pfad	**Konfiguration/Regeln/Ausgehende Regeln/Aktionen/Anhänge mit einem Passwort schützen/Verschlüsselungseinstellungen/Anforderung bearbeiten/Verschlüsselungsanforderungen**
Element	**Verschlüsselungsalgorithmus**
Empfohlener Wert	**AES-256 (erfordert Acrobat 9 oder neuer)**
Standardwert	**AES-128 (empfohlen, erfordert Acrobat 6 oder neuer)**
Grund/Auswirkung	**Höherer Verschlüsselungsgrad. Schmälert die Kompatibilität der PDF-Reader. Wiederholen Sie diesen Schritt für alle ausgehenden Regeln („All outbound mails“).**

- Deaktivieren Sie das Einsammeln von Signaturzertifikaten:

Pfad	**Konfiguration/Regeln/Eingehende Regeln/Aktionen/S/MIME- und PGP-Überprüfung sowie Entschlüsselung (vorzugsweise eingehend)/Überprüfungsoptionen/Einsammeln von Schlüsseln**
Element	**Importiere angehängte S/MIME-Zertifikate (empfohlen)** **Importiere angehängte PGP-Zertifikate (empfohlen)**
Empfohlener Wert	**Deaktivieren**
Standardwert	**Aktiviert**
Grund/Auswirkung	**Nach der Deaktivierung müssen Sie manuell das Schlüsselmaterial Ihres Kommunikationspartners importieren und sicherstellen, dass die entsprechenden Schlüssel als ausreichend sicher angesehen werden.**

- Erzwingen Sie die Adressen-Überprüfung bei S/MIME-Signaturen:

Pfad	**Konfiguration/Regeln/Eingehende Regeln/Aktionen/S/MIME- und PGP-Überprüfung sowie Entschlüsselung (vorzugsweise eingehend)/Überprüfungsrichtlinien/S/MIME-signierte E-Mails**
Element	**Erfordere zusätzlich, dass die Adressen des Signierenden und des Absenders exakt übereinstimmen**
Empfohlener Wert	**Aktivieren**
Standardwert	**Deaktiviert**
Grund/Auswirkung	**Die Signaturadresse sowie die Absenderadresse müssen vollständig übereinstimmen.**

- Erzwingen Sie die Adressen-Überprüfung bei PGP-Signaturen:

Pfad	**Konfiguration/Regeln/Eingehende Regeln/Aktionen/S/MIME- und PGP-Überprüfung sowie Entschlüsselung (vorzugsweise eingehend)/Überprüfungsrichtlinien/S/MIME-signierte E-Mails**
Element	**Erfordere zusätzlich, dass die Adressen des Signierenden und des Absenders exakt übereinstimmen**
Empfohlener Wert	**Aktivieren**

Standardwert	**Deaktiviert**
Grund/Auswirkung	**Die Signaturadresse sowie die Absenderadresse müssen vollständig übereinstimmen.**

- Erzwingen Sie nur bekannte PGP-Signaturen:

Pfad	**Konfiguration/Regeln/Eingehende Regeln/Aktionen/S/MIME- und PGP-Überprüfung sowie Entschlüsselung (vorzugsweise eingehend)/Überprüfungsrichtlinien/PGP-signierte E-Mails**
Element	**Überspringe die Signaturprüfung, falls der Signaturschlüssel nicht verfügbar ist (empfohlen)**
Empfohlener Wert	**Deaktiviert**
Standardwert	**Aktivieren**
Grund/Auswirkung	**Unbekannte Absender werden blockiert. Ein initialer separater Austausch von PGP-Schlüsseln ist notwendig.**

- Erzwingen Sie die Verschlüsselung ausgehender E-Mails:

Pfad	**Konfiguration/Regeln/Ausgehende Regeln/Aktionen**
Element	**-**
Empfohlener Wert	**Automatische Verschlüsselung aller E-Mails auf dem Server erzwingen**
Standardwert	**Den Benutzer entscheiden lassen, ob E-Mails verschlüsselt werden sollen oder nicht**
Grund/Auswirkung	**Alle ausgehenden E-Mails werden verschlüsselt gesendet.**

- Erhöhen Sie die Passwortstärke für PDF-E-Mails:

Pfad	**Konfiguration/NoSpamProxy-Komponenten/Web Portal/Einstellungen/PDF Mail**
Element	**Passwortstärke**

Empfohlener Wert	**Dritte Option "Passwörter müssen mindestens 12 Zeichen lang sein. Zeichen aus mindestens 4 dieser Kategorien müssen enthalten sein [...]"**
Standardwert	**Erste Option "Passwörter müssen mindestens 8 Zeichen lang sein. Zeichen aus mindestens 2 dieser Kategorien müssen enthalten sein [...]"**
Grund/Auswirkung	**Die Sicherheit des Passworts erhöht die Sicherheit einer verschlüsselten PDF und somit den schützenswerten Inhalt.**

- Stellen Sie sicher, dass ein DNSSEC-fähiger DNS Server verwendet wird:

Pfad	**Konfiguration/Verbundene Systeme**
Element	**DNS-Server**
Empfohlener Wert	**Ein DNSSEC-fähiger DNS-Server. - Hinweis: Dies kann durch eine separate Angabe der Server passieren oder indem sicher gestellt wird, dass der in Windows konfigurierte DNS-Server DNSSEC fähig ist.**
Standardwert	**Nutze die Server, die in Windows konfiguriert sind**
Grund/Auswirkung	**Sicherstellung, dass, wann immer es möglich ist, die DNS-Kommunikation abgesichert ist und DANE als Sicherheitsmechanismus für SMTP genutzt werden kann. - Hinweis: DANE ist standardmäßig aktiv, wenn ein DNSSEC-fähiger DNS-Server genutzt wird.**

- Stellen Sie sicher, dass E-Mails nur signiert verschickt werden:

Pfad	**Konfiguration/Regeln/Ausgehende Regeln/Aktionen/S/MIME- und PGP-Signatur sowie Verschlüsselung (vorzugsweise ausgehend)/Signaturoptionen**
Element	**Eine digitale Signatur stellt die Authentizität einer E-Mail sicher. Um eine E-Mail zu signieren, muss ein privater kryptographischer Schlüssel auf dem Knoten 'Zertifikate' oder 'PGP-Schlüssel' hinterlegt sein.**
Empfohlener Wert	**Signiere E-Mails oder weise sie ab, wenn kein kryptographischer Schlüssel verfügbar ist**
Standardwert	**E-Mails signieren, wenn ein kryptographischer Schlüssel verfügbar ist und alle anderen E-Mails ohne Signatur versenden**
Grund/Auswirkung	**Sämtliche ausgehenden E-Mails müssen per S/MIME oder PGP signiert sein. Andernfalls werden diese nicht nach extern zugestellt.**

- Stellen Sie sicher, dass E-Mails nur verschlüsselt verschickt werden:

Pfad	**Konfiguration/Regeln/Ausgehende Regeln/Aktionen/S/MIME- und PGP-Signatur sowie Verschlüsselung (vorzugsweise ausgehend)/Verschlüsselungsoptionen**
Element	**Verschlüsselung stellt sicher, dass der Inhalt der E-Mail während der Übermittlung nicht von Dritten gelesen werden kann. Für diese Option müssen die öffentlichen kryptographischen Schlüssel der Empfänger auf dem Knoten 'Zertifikate' oder 'PGP-Schlüssel' hinterlegt sein.**
Empfohlener Wert	**Verschlüsselung erzwingen und die Auslieferung ablehnen, wenn kein öffentlicher kryptographischer Schlüssel verfügbar ist" mit aktiviertem Unterpunkt "Besprechungsanfragen und -aktualisierungen dürfen unverschlüsselt gesendet werden"**
Standardwert	**E-Mails wenn möglich verschlüsseln**
Grund/Auswirkung	**Sämtliche ausgehenden E-Mails müssen per S/MIME oder PGP verschlüsselbar sein. Andernfalls werden diese nicht nach extern zugestellt.**

- Aktivieren Sie den menschenlesbaren Prüfbericht für E-Mails:

Pfad	**Konfiguration/Benutzer-Benachrichtigungen**
Element	**Prüfbericht**
Empfohlener Wert	**Anhängen falls sie sicherheitsverwandte Eigenschaften (empfohlen) *und* Einen menschenlesbaren Prüfbericht an mit dieser Vorlage anhängen:**
Standardwert	**Niemals anhängen**
Grund/Auswirkung	**Der Prüfbericht ermöglicht es Nutzern, festzustellen, ob eine E-Mail beispielsweise signiert oder verschlüsselt war**

- Stellen Sie sicher, dass ein Zertifikat zum Signieren des Prüfberichts vorhanden ist:

Pfad	**Identitäten/Zertifikate**

Element	**Zertifikatsverwaltung**
Empfohlener Wert	**Es liegt ein S/MIME-Zertifikat vor, welches zum Signieren des Prüfberichts genutzt werden soll. Andernfalls importieren Sie dieses.**
Standardwert	**Keine Zertifikate vorhanden**
Grund/Auswirkung	**Das Zertifikat sollte von einer CA ausgestellt sein, die im Microsoft Trusted CA Store gespeichert ist und muss die Anforderungen von BSI TR-02102-1 und TR-02103 erfüllen.**

- Stellen Sie sicher, dass die Authentizität des Prüfberichts sichergestellt werden kann:

Pfad	**Konfiguration/Benutzer-Benachrichtigungen**
Element	**Prüfbericht**
Empfohlener Wert	**Wählen Sie ein Zertifikat aus, um den Prüfbericht zu signieren.**
Standardwert	**Nicht definiert**
Grund/Auswirkung	**Durch die Signatur des Prüfberichts kann sichergestellt werden, dass Mitarbeiter nach einer internen Schulung in der Lage sind, die Echtheit des Prüfberichts sicherzustellen.**

- Stellen Sie sicher, dass ein ausreichend sicheres Passwort für den Schutz sensibler Daten hinterlegt ist:

Pfad	**Konfiguration/Erweiterte Einstellungen/Schutz sensibler Daten**
Element	**Schutz sensibler Daten**
Empfohlener Wert	**Legen Sie ein sicheres Passwort zum Schutz besonders sensibler Daten fest, falls dies nicht schon geschehen ist. Dabei sind die BSI-Empfehlungen für sichere Passwörter zu beachten (8-12- Zeichen lang, mindestens je ein Großbuchstabe, ein Kleinbuchstabe, eine Zahl und ein Sonderzeichen).**
Standardwert	**Nicht definiert**
Grund/Auswirkung	**Durch das Definieren eines Passworts werden sensible Daten zusätzlich verschlüsselt gespeichert.**

- Unterbinden Sie die öffentliche Sichtbarkeit des verwendeten Produkts auf SMTP-Ebene:

Pfad	**Konfiguration/Erweiterte Einstellungen/SMTP-Protokolleinstellungen/Statusmeldungen**
Element	**Willkommensnachricht**
Empfohlener Wert	**%h - Hinweis: "%h" verweist auf den konfigurierten SMTP-Servernamen.**
Standardwert	**%h - NoSpamProxy ready**
Grund/Auswirkung	**Unterbinden der Bekanntgabe des genutzten Produkts auf SMTP-Ebene.**

5. Nehmen Sie folgende Einstellungen/Konfigurationen in der Windows-Konfiguration vor:
   - Deaktivieren Sie sämtliche bestehenden Windows-Firewall-Regeln für die eingehende Kommunikation:

Pfad	**Einstellungen/Netzwerk und Internet/Status/Windows-Firewall/Firewall- & Netzwerkschutz/Erweiterte Einstellungen/Eingehende Regeln**
Element	**Alle eingehenden Regeln**
Empfohlener Wert	**Deaktivieren Sie alle bestehenden eingehenden Regeln**
Standardwert	**Vordefinierte Windows-Regeln sind aktiv**
Grund/Auswirkung	**Unterbinden Sie sämtliche eingehende Netzwerk-Kommunikation, die nicht notwendig ist, um so mögliche angreifbare Dienste zu schließen.**

   - Geben Sie die notwendigen Ports für NoSpamProxy in der Windows-Firewall frei:

Pfad	**Einstellungen/Netzwerk und Internet/Status/Windows-Firewall/Firewall- & Netzwerkschutz/Erweiterte Einstellungen/Eingehende Regeln**
Element	**Neue Regel erstellen**

Empfohlener Wert	**Öffnen Sie die Windows Firewall für Port 25 - TCP**
Standardwert	**Nicht definiert**
Grund/Auswirkung	**Erlaubt die Kommunikation zu NoSpamProxy.**

- Stellen Sie sicher, dass "Kontosperrungsdauer" auf den Wert "15 oder mehr Minuten" gesetzt ist:

Pfad	**Gruppenrichtlinien/Computer/Windows-Einstellungen/ Sicherheitseinstellungen/Kontorichtlinien/ Kontosperrungsrichtlinien**
Element	**Kontosperrungsdauer**
Empfohlener Wert	**15 oder mehr Minuten**
Standardwert	**10 Minuten**
Grund/Auswirkung	**Unterbindet Brute-Force-Angriffe auf administrative Accounts.**

- Stellen Sie sicher, dass "Kontosperrungsschwelle" auf den Wert "10 oder weniger ungültige Anmeldeversuche, aber nicht 0" gesetzt ist:

Pfad	**Gruppenrichtlinien/Computer/Windows-Einstellungen/ Sicherheitseinstellungen/Kontorichtlinien/ Kontosperrungsrichtlinien**
Element	**Kontosperrungsschwelle**
Empfohlener Wert	**10 oder weniger ungültige Anmeldeversuche, aber nicht 0**
Standardwert	**10 Anmeldeversuche**
Grund/Auswirkung	**Unterbindet Brute-Force-Angriffe auf administrative Accounts.**

- Stellen Sie sicher, dass "Zurücksetzungsdauer des Kontosperrungszählers" auf den Wert "15 oder mehr Minuten" gesetzt ist:

Pfad	**Gruppenrichtlinien/Computer/Windows-Einstellungen/ Sicherheitseinstellungen/Kontorichtlinien/ Kontosperrungsrichtlinien**
Element	**Zurücksetzungsdauer des Kontosperrungszählers**
Empfohlener Wert	**15 oder mehr Minuten**
Standardwert	**10 Minuten**
Grund/Auswirkung	**Unterbindet Brute-Force-Angriffe auf administrative Accounts.**

- Stellen Sie sicher, dass alle notwendigen Ausnahmen für die Windows-seitige Loopback-Überprüfung gesetzt sind:

Pfad	**Registrierungs-Editor: Computer\HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**
Element	**BackConnectionHostNames - Hinweis: Benutzen Sie den Typ "Multi-String Value"**
Empfohlener Wert	**Die Hostnamen, die für das Ansprechen des Systems verwendet werden. Beispiel: der aktuelle Computername. - Hinweis: Dies ist eine Sicherheitsausnahme basierend auf der Microsoft KB 926642.**
Standardwert	**Nicht definiert**
Grund/Auswirkung	**Der Zugriff auf den lokalen Host über einen Hostnamen kann zu Problemen führen, da dies von Microsoft untersagt wird. Durch die Ausnahmen-Definition wird dies für die entsprechenden Hostnamen aufgehoben.**

- Härten Sie die globale Transport-Kommunikation:

Pfad	**PowerShell**
Element	**Führen Sie das Skript *Windows_SCHANNEL_hardening.ps1* aus, das auf www.nospamproxy.de/bsz bereitgestellt wird**
Empfohlener Wert	**-**
Standardwert	**-**
Grund/Auswirkung	**Unsichere Protokolle und Cipher-Suiten sollten deaktiviert werden, um einen Angriff auf Transportebene möglichst ausschließen zu können.**

6. Fügen Sie einen oder mehrere Unternehmensbenutzer zu NoSpamProxy hinzu und konfigurieren Sie diese(n) wie im Kapitel "Unternehmensbenutzer" beschrieben.

   > **HINWEIS:**
   >
   > - Es ist möglich, gleichzeitig manuell hinzugefügte Benutzer und mehrere automatische Benutzerimporte zu verwenden.
   > - Beachten Sie, dass die Option "Aktiviere Verschlüsselung (empfohlen)" gemäß Schritt 4 der NCC-Konfiguration eingestellt wurde.

7. Importieren Sie kryptographisches Material für S/MIME- und PGP-Verschlüsselung und -Signatur.

HINWEIS:

- NoSpamProxy kann Nachrichten automatisch mittels S/MIME und PGP signieren und verschlüsseln.
- Um S/MIME-Aktionen zu ermöglichen, müssen Schlüssel und Zertifikate NoSpamProxy bekannt sein und wie im Kapitel "Zertifikate verwalten" beschrieben importiert werden.
- Um PGP-Aktionen zu ermöglichen, müssen Schlüssel importiert werden, wie im Kapitel "PGP-Schlüssel verwalten" beschrieben.
- Stellen Sie sicher, dass das kryptographische Material vertrauenswürdig ist: SMIME-Zertifikate sollten von einer CA ausgestellt sein, die im Microsoft Trusted CA Store gespeichert ist und müssen die Anforderungen von BSI TR-02102-1 und TR-02103 erfüllen. PGP-Schlüssel müssen die Anforderungen von BSI TR-02102-1 erfüllen.

8. Legen Sie notwendige Partner gemäß dem Kapitel "Partnerdomänen hinzufügen" an.

HINWEIS:

- Stellen Sie sicher, dass im Konfigurationsschritt "Ende-zu-Ende-Verschlüsselung" für den S/MIME-Algorithmus die Option "Nutze immer die unten stehenden Algorithmen" ausgewählt ist.
- Setzen Sie im Bereich "Signatur" das "Padding" auf "PSS".
- Setzen Sie im Bereich "Verschlüsselung" den "Algorithmus" auf "AES-128-GCM".
- Setzen Sie im Bereich "Verschlüsselung" das "Padding" auf "OAEP".

9. Importieren Sie kryptographisches Material für die Partner.

HINWEIS:

- Um S/MIME-Aktionen zu ermöglichen, müssen die Partnerzertifikate NoSpamProxy bekannt sein und wie im Kapitel "Zertifikate verwalten" beschrieben importiert werden.
- Um PGP-Aktionen zu ermöglichen, müssen die PGP-Schlüssel der Partner importiert werden, siehe Kapitel "PGP-Schlüssel verwalten".

HINWEIS:

- Stellen Sie sicher, dass das kryptographische Material vertrauenswürdig ist.
- SMIME-Zertifikate sollten von einer CA ausgestellt sein, die im Microsoft Trusted CA Store gespeichert ist und müssen die Anforderungen von BSI TR-02102-1 und TR-02103 erfüllen.
- PGP-Schlüssel müssen die Anforderungen von BSI TR-02102-1 erfüllen.

10. Überprüfen Sie den aktuellen Konfigurationsstatus. Wechseln Sie dazu im NoSpamProxy Command Center auf "Übersicht" und lesen Sie die "Vorfälle" aufmerksam durch. Wenn möglich/gewünscht, klicken Sie auf "Akzeptieren" oder "Verwerfen". Danach sollte nur noch ein grünes Häkchen vorhanden sein.
11. Aktivieren Sie NoSpamProxy Auditlog. Gehen Sie dazu folgendermaßen vor:
    1. Öffnen Sie den lokalen Gruppenrichtlinien-Editor und gehen Sie zu **Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Erweiterte Überwachungsrichtlinienkonfiguration/Systemüberwachungsrichtlinien – Lokales Gruppenrichtlinienobjekt/Objektzugriff**.
    2. Öffnen Sie den Eintrag für **Anwendung generiert überwachen** und überprüfen Sie die beiden Einträge **Erfolg** und **Fehler**.
    3. Öffnen Sie ein Powershell-Befehlsfenster und führen Sie die folgenden zwei Befehle aus:

- `Connect-Nsp -IgnoreServerCertificateErrors`
- `Set-NspAuditLog -Reads $false -Create $true -Updates $true -Deleted $true`

> **HINWEIS:** Reads sollten deaktiviert werden, da sie eine große Anzahl von Einträgen erzeugen und viel Speicherplatz benötigen.

4. Stellen Sie sicher, dass Sie das aktivierte Audit-Protokoll in der Ereignisanzeige sehen. Es wird unter "Windows-Protokolle/Sicherheit" angezeigt.

12. Importieren Sie ein TLS-Zertifikat für die Verwendung von STARTTLS.

> **HINWEIS:**
> - Das angeforderte TLS-Zertifikat muss von einer CA ausgestellt worden sein, die sich im Microsoft Trusted CA Store befindet.
> - Das angeforderte TLS-Zertifikat muss die richtigen Zertifikatsdetails enthalten (beispielsweise CN).
> - Das angeforderte TLS-Zertifikat muss die Anforderungen von BSI TR-02102-1, TR-02102-2 und TR-02103 erfüllen.

13. Importieren Sie das TLS-Zertifikat und den privaten Schlüssel in die Windows-Zertifikatspeicher aller Computer, auf denen eine Gatewayrolle installiert ist.

HINWEIS:

- Das Zertifikat sollte im persönlichen Speicher innerhalb des lokalen Computerspeichers abgelegt werden.
- Verwenden Sie die Microsoft Management Console, um den privaten Schlüssel Ihres TLS-Zertifikats zu verwalten.
- Fügen Sie eine Leseberechtigung für "nt service\NoSpamProxyGatewayRole" hinzu.

14. Starten Sie den Dienst "NoSpamProxy - Gateway Role" neu.

NoSpamProxy ist jetzt entsprechend der Annahmen und Vorgaben konfiguriert, die im Dokument "BSZ Security Target NoSpamProxy" definiert sind.

Sichere Deinstallation von NoSpamProxy

1. Deinstallieren Sie NoSpamProxy vollständig.
2. Entfernen Sie die virtuelle Maschine vollständig.
3. Überschreiben Sie bei der Nutzung dedizierter Hardware sämtliche Festplatten sicher oder shreddern Sie diese. Verfahren Sie analog mit der genutzten SQL-Datenbank beziehungsweise dem SQL-Server.

WARNUNG: Eine vollständige Deinstallation sollte mit größter Sorgfalt durchgeführt werden, um zu vermeiden, dass sensible Daten zu einem späteren Zeitpunkt abgegriffen werden können.