Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Zertifizierungsreport

BSI-DSZ-BSZ-0007-2023

zu

NoSpamProxy Server, Version 14.0.5.62

der

Net at Work GmbH

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Service Center +49 (0)800 274 1000
bsz@bsi.bund.de
Internet: https://www.bsi.bund.de/bsz

Deutsches IT-Sicherheitszertifikat

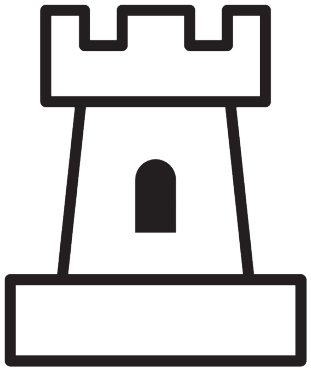
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-BSZ-0007-2023(*)

NoSpamProxy Server, Version 14.0.5.62

von **Net at Work GmbH**

für den Geltungsbereich:
Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte



Beschleunigte Sicherheitszertifizierung

Das in diesem Zertifikat genannte IT-Produkt vom Produkttyp E-Mail-Security-Gateway wurde von einer anerkannten Prüfstelle nach der Evaluationsmethodologie für die Beschleunigte Sicherheitszertifizierung (BSZ) des Bundesamtes für Sicherheit in der Informationstechnik evaluiert.

(*) Dieses Zertifikat gilt nur für die angegebene Version des Produkts in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport und -bescheid. Details zur Gültigkeit sind dem Zertifizierungsreport Teil A, Kap. 4 zu entnehmen.

Das Zertifizierungsverfahren wurde in Übereinstimmung mit den Anforderungen und Regeln des BSI eigenen Programms zur Beschleunigten Sicherheitszertifizierung (BSZ) durchgeführt.

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produkts durch das Bundesamt für Sicherheit in der Informationstechnik oder einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder einer anderen Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

Bonn, 29. November 2023
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola L.S.
Abteilungsleiter

Inhaltsverzeichnis

A Zertifizierung

1 Vorbemerkung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemäß BSIG[1] die Aufgabe, für Produkte (Systeme oder Komponenten) der Informationstechnik Sicherheitszertifikate zu erteilen.

Die Zertifizierung eines Produkts wird auf Veranlassung des Herstellers oder eines Vertreibers – im folgenden Antragsteller genannt – durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produkts gemäß den vom BSI öffentlich bekannt gemachten oder allgemein anerkannten Sicherheitskriterien.

Die Prüfung wird in der Regel von einer vom BSI anerkannten Prüfstelle oder vom BSI selbst durchgeführt.

Das Ergebnis des Zertifizierungsverfahrens ist der vorliegende Zertifizierungsreport. Hierin enthalten sind u. a. das Sicherheitszertifikat (zusammenfassende Bewertung) und der detaillierte Zertifizierungsbericht.

Der Zertifizierungsbericht enthält die sicherheitstechnische Beschreibung des zertifizierten Produkts, die Einzelheiten der Bewertung und Hinweise für den Anwender.

2 Grundlagen des Zertifizierungsverfahrens

Die Zertifizierungsstelle führt das Verfahren nach Maßgabe der folgenden Vorgaben durch:

- BSI-Gesetz[1]
- BSI-Zertifizierungs- und Anerkennungsverordnung[2]
- Besondere Gebührenverordnung BMI (BMIBGebV)[3]
- besondere Erlasse des Bundesministeriums des Innern und für Heimat
- Produktzertifizierung im BSI: Programm Beschleunigte Sicherheitszertifizierung (BSZ-Produkte) [1]
- Anerkennung von Prüfstellen im BSI: Programm im Bereich Beschleunigte Sicherheitszertifizierung (BSZ-Prüfstellen) [2]
- Anwendungshinweise und Interpretationen zum Schema für die BSZ (AIS B) [3]

Das Verfahren wurde im Geltungsbereich **„Allgemeine Netzwerkkomponenten und eingebettete IP-vernetzte Geräte“** der Beschleunigten Sicherheitszertifizierung durchgeführt.

[1] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 11 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist

[2] Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und Anerkennungsverordnung - BSIZertV) vom 17. Dezember 2014, Bundesgesetzblatt Jahrgang 2014 Teil I, Nr. 61, S. 2231

[3] Besondere Gebührenverordnung BMI (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019 (BGBl. I S. 1359), die zuletzt durch Artikel 1 der Verordnung vom 10. September 2021 (BGBl. I S. 4429) geändert worden ist

3 Anerkennungsvereinbarungen

Um die Mehrfachzertifizierung des gleichen Produkts in verschiedenen Staaten zu vermeiden, besteht ein Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten der Programme CSPN (Certification de sécurité de premier niveau) und BSZ zwischen dem BSI und der französischen ANSSI (Agence nationale de la sécurité des systèmes d'information) [4]. Das Abkommen ist zunächst befristet auf zwei Jahre, d.h. bis zum 07.06.2024. Damit werden grundsätzlich alle CSPN-Zertifikate in Deutschland vom BSI und alle BSZ-Zertifikate von der ANSSI anerkannt.

Es können allerdings Zertifikate von der Anerkennung ausgenommen werden. Dies kann sowohl durch die ausstellende Seite als auch durch die anerkennende Seite geschehen.

4 Durchführung der Evaluierung und Zertifizierung

Die Zertifizierungsstelle führt für jede einzelne Evaluierung eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Produkt NoSpamProxy Server, Version 14.0.5.62 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluierung des Produkts NoSpamProxy Server, Version 14.0.5.62 wurde von der secuvera GmbH durchgeführt. Die Evaluierung wurde am 6. Oktober 2023 abgeschlossen. Das Prüflabor ist eine vom BSI anerkannte Prüfstelle (ITSEF)[4].

Der Antragsteller ist: Net at Work GmbH.

Das Produkt wurde entwickelt von: Net at Work GmbH.

Die Zertifizierung wurde damit beendet, dass das BSI die Übereinstimmung mit den Kriterien überprüft und den vorliegenden Zertifizierungsreport erstellt hat.

5 Gültigkeit des Zertifizierungsergebnisses

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produkts. Die Ergebnisse der Zertifizierung gelten nur, wenn das Produkt unter den folgenden Bedingungen betrieben wird:

- Alle Auflagen hinsichtlich der Generierung, der Konfiguration und des Einsatzes des Evaluierungsgegenstands (EVG), die in diesem Report gestellt werden, werden beachtet.
- Das Produkt wird in der Umgebung betrieben, die in diesem Report und in den Sicherheitsvorgaben beschrieben ist.

Das Zertifikat bestätigt die Vertrauenswürdigkeit des Produkts gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung.

Um in Anbetracht der sich weiter entwickelnden Angriffsmethoden eine unbefristete Anwendung des Zertifikates trotz dem Erfordernis nach einer Neubewertung nach den Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikates begrenzt. Dieses Zertifikat, erteilt am 29. November 2023, ist gültig bis 28. November 2025. Die Gültigkeit kann im Rahmen einer Rezertifizierung erneuert werden.

Der Inhaber des Zertifikates ist verpflichtet,

1. bei der Bewerbung des Zertifikates oder der Tatsache der Zertifizierung des Produkts auf den Zertifizierungsreport hinzuweisen sowie jedem Anwender des Produkts den Zertifizierungsreport und die darin referenzierten Sicherheitsvorgaben und Benutzerdokumentation für den Einsatz oder die Verwendung des zertifizierten Produkts zur Verfügung zu stellen,
2. eine Kontaktadresse zur Meldung von potenziellen Schwachstellen durch Dritte (psirt@nospamproxy.com) zu betreiben,

[4] Information Technology Security Evaluation Facility

3. eingehende Meldungen bezüglich potenzieller Schwachstellen des Produkts unverzüglich zu prüfen und die Prüfung zu dokumentieren, hierzu gehört insbesondere die Prüfung der über die Kontaktadresse gemäß 2. gemeldeten Schwachstellen,
4. die Marktaufsicht des BSI unaufgefordert und unverzüglich nach Bekanntwerden und Bewertung über Schwachstellen des Produkts zu informieren, die nach dem Zeitpunkt der Zertifizierung durch den Inhaber des Zertifikates oder Dritte festgestellt wurden, und den Anwendern des Produkts unverzüglich kostenfrei über den in Teil B Abschnitt 2.5 genannten sicheren Update-Kanal eine Fehlerkorrektur und auf Wunsch des Anwenders ergänzend Informationen zur Auswirkung der Schwachstelle zur Verfügung zu stellen. Des Weiteren muss der Inhaber des Zertifikates den Anwendern des Produkts unverzüglich kostenfrei über den im Zertifizierungsreport genannten sicheren Update-Kanal eine Fehlerkorrektur und auf Wunsch des Anwenders ergänzende Informationen zur Auswirkung der Schwachstelle zur Verfügung zu stellen.

Bei Änderungen am Produkt kann die Gültigkeit des Zertifikats auf neue Versionen ausgedehnt werden. Voraussetzung dafür ist, dass der Antragsteller zur Aufrechterhaltung der Vertrauenswürdigkeit eine Rezertifizierung in Übereinstimmung mit den entsprechenden Regeln beantragt und die Evaluierung keine Abweichungen von den Sicherheitsvorgaben und weiteren Anforderungen aufdeckt.

6 Veröffentlichung

Das Produkt NoSpamProxy Server, Version 14.0.5.62 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de/bsz).

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produkts angefordert werden. Der Zertifizierungsreport kann ebenso in elektronischer Form von der oben angegebenen Internetadresse heruntergeladen werden.

B Zertifizierungsbericht

Der nachfolgende Bericht ist eine Zusammenfassung aus

- den Sicherheitsvorgaben des Antragstellers für den Evaluationsgegenstand,
- den entsprechenden Prüfergebnissen des Prüflabors und
- ergänzenden Hinweisen und Auflagen der Zertifizierungsstelle.

1 Zusammenfassung

NoSpamProxy Server ist eine E-Mail-Security-Software vom Typ E-Mail-Security-Gateway. Die Software sendet und empfängt E-Mails im Unternehmensumfeld und bietet weitere E-Mail-Security-Funktionalität wie Emailsignatur und Emailverschlüsselung nach aktuellem Stand der Technik an.

1.1 Produktbeschreibung

Der NoSpamProxy Server dient als E-Mailproxy und wird im Unternehmensnetzwerk als das erste System eingesetzt, das eingehende E-Mails empfängt und verarbeitet. Die Software kommuniziert durch das SMTP-Protokoll mit externen E-Mail-Servern, aber auch mit dem E-Mail-Server des Unternehmens. Administratoren können auf NoSpamProxy Server zugreifen und konfigurieren. Dadurch ist es möglich, die unternehmensweiten E-Mail-Sicherheitsrichtlinien für ein- und ausgehenden E-Mails zu steuern.

Der NoSpamProxy Server ist aus verschiedenen Komponenten aufgebaut, die zusammen die Funktionalität anhand von Modulen bereitstellen. Der NoSpamProxy Server besteht dabei aus den folgenden Komponenten:

- Management (Intranet Role und Managment Console):
  - Die Intranet Role ermöglicht die Konfiguration von NoSpamProxy Server und verwaltet die kryptographischen Schlüssel. Des Weiteren findet auf dieser Rolle die Synchronisierung von Benutzerdaten aus dem „Active Directory“ oder einem anderen Verzeichnisdienst, wie beispielsweise „Lotus Domino“ statt.
  - Das NoSpamProxy Command Center (NCC) ist die Benutzeroberfläche von NoSpamProxy Server. Das NCC dient der zentralen Verwaltung und Administration von NoSpamProxy Server.
- E-Mail Gateway:
  - Das E-Mail Gateway nimmt die E-Mails auf Port 25 an, prüft diese auf Spam und weist diese gegebenenfalls ab. Es stellt außerdem eine Schnittstelle zu De-Mail, Deutschland-Online-Infrastruktur und POP3-Postfächern bereit.
- Webportal:
  - Das Web Portal, das weitere Funktionen für Nutzer bereitstellt, ist nicht teil der zertifizierten Konfiguration.

Diese Komponenten stellen die folgenden Module bereit, die miteinander kombiniert werden können:

- Module Encryption:
  - Das Modul Encryption ermöglicht Ver- und Entschlüsselung von E-Mails sowie Signatur und Signaturprüfung von E-Mails. Die notwendigen S/MIME-Zertifikate und PGP-Schlüssel der Unternehmensnutzer und externen Kommunikationspartner werden zentral in NoSpamProxy abgelegt und verwaltet.
- Module Disclaimer:
  - Das Modul Disclaimer ermöglicht die Erstellung von sogenannten Disclaimer Texts, die abhängig von gewissen Mustern, wie z.B. Active Directory Gruppen, in die Emails eingefügt werden können.
- Module Protection:

    - Das Modul Protection ermöglicht die Erkennung von Spam und Schadprogrammen. Diese Funktion ist abhängig von externen und aktuellen Daten zur Spam und Schadprogrammerkennung und ist daher nicht Teil zertifizierten Konfiguration.
- Module Large Files:
    - Das Module Large Files, das sichere Übertragung von großen Dateien ermöglicht, ist nicht Teil der zertifizierten Konfiguration.

1.2 Produktidentifikation

Nr	*Typ*	*Identifier*	*Version*	*Auslieferungsart*
1	Software	NoSpamProxy Server	14.0.5.62	
2	Dokument	Security Target for NoSpamProxy Server Version 14	1.0 vom 14.11.2023	www.nospamproxy.de/de/BSZ
3	Dokument	Secure User Guidance (SUG) NoSpamProxy Server Version 14	1.0 vom 18.10.2023	www.nospamproxy.de/de/BSZ

Tabelle 1: Auslieferungsumfang des Evaluierungsgegenstands (TOE)

Der Evaluierungsgegenstand kann vor der Installation anhand der Installationsdateien identifiziert werden. Dabei muss das ZIP-Archiv der Installation entpackt, und die Eigenschaften der Datei „Setup.exe“ geprüft werden. Im Reiter „Details“ ist die „Dateiversion“ 14.0.5.62 sichtbar.

Im Betrieb kann der Evaluierungsgegenstand im NoSpamProxy Command Center im Reiter „Übersicht“ beim Klick auf die Version „14.0.5“ angezeigt werden. Dort ist die Version 14.0.5.62 des Evaluierungsgegenstands in der Komponente „NoSpamproxy“ sichtbar.

1.3 Sicherheitsfunktionen des EVG

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [6], Seite 12, definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und Angreifern auf den Seiten 12 bis 14 dar. Der EVG bietet die in Tabelle 2 aufgezählten Sicherheitsfunktionen an, um die Werte vor den beschriebenen Bedrohungen zu schützen. Diese Sicherheitsfunktionen des EVG wurden in der Evaluation betrachtet.

Sicherheitsfunktionen des EVG	*Beschreibung*
Sec.AdminAuth	Sichere Authentifizierung von Administratoren
Sec.SMTPAuth	Sichere SMTP Authentisierung zwischen E-Mail-Servern (RFC 5321)
Sec.LDAP	Nutzeradministration wird mittels Active Directory/LDAP durchgeführt
Sec.MultiTenant	Striktes Rollenmanagement für Administratoren.
Sec.EmailEncryption	Inhalt von E-Mail können mittels S/MIME 4.0 (RFC 8551) oder PGP (RFC 4880) verschlüsselt werden.
Sec.TLS	Der Evaluierungsgegenstand erzwingt Transport Layer Encryption (TLS) für die Kommunikation mit anderen E-Mail-Servern.
Sec.MessageTracking	Administratoren können Nachrichtenverfolgung zur Identifizierung von Angriffsversuchen via E-Mail nutzen.

Sicherheitsfunktionen des EVG	*Beschreibung*
Sec.NSPMonitoring	Administratoren werden durch das NoSpamProxy Control Center über neue E-Mail-Angriffe benachrichtigt und auf mögliche notwendige Konfigurationsänderungen, sowie auf zur Neige gehende Systemressourcen hingewiesen.
Sec.MailReject	Der Evaluierungsgegenstand akzeptiert keine E-Mails die als Spam oder bedrohlich eingestuft werden oder anderweitig durch die Konfiguration nicht erlaubt sind.[5]
Sec.KeyPass	Zur sicheren Speicherung von privaten Schlüsseln, werden Administratoren gezwungen ein Passwort einzugeben, mit diesem die privaten Schlüssel verschlüsselt und danach gespeichert werden.
Sec.ServerLogging	Der Evaluierungsgegenstand schreibt Logdaten zu relevanten Ereignissen in das Windows Security Event Log des Windows Servers. Der Zeitpunkt, Ereignis und Ergebnis werden aufgezeichnet.

Tabelle 2: Sicherheitsfunktionen des EVG

1.4 Konfiguration des EVG

Dieses Zertifikat gilt nur für die in den Sicherheitsvorgaben [6] und in der Secure User Guidance [8] beschriebenen Konfigurationen des EVG. Insbesondere sind die folgenden Funktionen, wie auf Seite 14 unter „Limits of Evaluation“ der Sicherheitsvorgaben [6] beschrieben, von der Evaluation ausgeschlossen und nicht vom Zertifikat abgedeckt:

- Sandbox Array service
- Die verteilte Installation des NoSpamProxy Servers auf mehreren Servern für höhere Leistung und Verfügbarkeit
- PDF Verschlüsselungsfunktion des Encryption Modules
- Erzeugung von PGP Schlüsselpaaren
- HTTPS via Port 6061
- Module Large Files Module
- Funktionen der Module Protection zur Erkennung von Spam und Schadprogrammen, die auf externen Daten beruhen.
- Plugin zur Kontrolle des NoSpamProxy Servers via Outlook
- ICAP Server
- Email threat evaluation network 32Guards
- SMS Dienste
- Email archive connector
- De-Mail connector
- digiSeal Server

Hinweis: Dieses Zertifikat gilt nur für die angegebene Version des Produkts in der evaluierten Konfiguration und nur in Verbindung mit dem vollständigen Zertifizierungsreport. Dieses Zertifikat ist keine generelle Empfehlung des IT-Produkts durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das

[5] Die Erkennung von Spam und Schadprogrammen ist abhängig von externen und aktuellen Daten zur Spam und Schadprogrammerkennung und wird in diesem Zertifikat daher nicht betrachtet.

IT-Produkt durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte, ist weder enthalten noch zum Ausdruck gebracht.

1.5 Beschreibung der Einsatzumgebung

In den Sicherheitsvorgaben auf den Seiten 7-12 wird die Einsatzumgebung des EVG beschrieben. Hierbei werden Annahmen gemacht, die beim Einsatz des EVG zu praktischen Anforderungen an die Einsatzumgebung werden, ohne die ein im Sinne des Zertifikats sicherer Betrieb nicht bestätigt ist. Hierbei sind die folgenden Punkte relevant:

- Assumption.SecuredWindowsServer & Assumption.PhysicalAccess: Der NoSpamProxy Server muss auf einem Windows Server installiert werden. Der Zugang zu diesem Windows Server muss nach dem aktuellen Stand der Technik gegen physischen Zugriff geschützt sein und auf vertrauenswürdige Personen beschränkt sein. Das der Windows Servers muss nach den aktuellen Vorgaben [9] für sichere Konfiguration von Windows Server Betriebssystem konfiguriert sein.
- Assumption.FirstMailGateway: Der NoSpamProxy Server muss die erste Instanz in der Organisation des Produktnutzers sein, die E-Mails empfängt. Die Internetadresse des NoSpamProxy Server muss in den MX-Datensatz des DNS-Eintrags für die Domäne der Organisation des Produktnutzers eingetragen sein.
- Assumption.NetworkSecurity: Das lokale Netzwerk, in dem der NoSpamProxy Server installiert ist, muss sicher sein und durch Firewall auf dem aktuellen Stand der Technik geschützt sein.
- Assumption.AdminSecureAssets: Wenn Administratoren die Konfiguration oder andere schützenswerte Daten des NoSpamProxy Servers kopieren, um sie außerhalb des NoSpamProxy Servers zu speichern müssen diese sicher gespeichert werden.
- Assumption.OnlyAdminUsers: Nur NoSpamProxy Server Administratoren dürfen Zugriff auf den Windows Server haben, auf dem der NoSpamProxy Server installiert ist. Das heißt, dass es auf dem Windows Server nur Nutzerkonten geben darf, die diesen Administratoren zugeordnet sind und auch ausschließlich von diesen genutzt werden.
- Assumption.AdminNoEvil, Assumption.AdminKnowHow & Assumption.SecureCredentials: Die NoSpamProxy Server Administratoren müssen vertrauenswürdig sein. Des Weiteren müssen die Administratoren in der Lage sein, den NoSpamProxy Server sicher zu konfigurieren und zu verwalten. Administratoren müssen wissen über Bedrohungen durch Schadprogramme und potentiell gefährdete Dateitypen haben. Administratoren müssen sichere Zugangsdaten, wie Passwörter, erzeugen können.
- Assumption.SecureAdminClient: Wenn Administratoren einen weiteren Computer zum Management des Windows Server auf dem der NoSpamProxy Servers oder zum Managment des NoSpamProxy Servers benutzt muss dieser Computer sicher und gegen Angriffe geschützt sein.
- Assumption.SecureExternalCertificates: Administratoren dürfen keine nur Zertifikate [10] und Schlüssel mit ausreichende Schlüssellänge und die empfohlenen kryptographischen Algorithmen [11] verwenden nutzen.

1.6 Dokumente

Die evaluierten Dokumente Sicherheitsvorgaben [6] und Secure User Guidance [8], die in Tabelle 1 aufgeführt sind, werden zusammen mit dem Produkt zur Verfügung gestellt. Hier sind die Informationen enthalten, die zum sicheren Umgang mit dem EVG in Übereinstimmung mit den Sicherheitsvorgaben benötigt werden.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die im Teil B Abschnitt 2.6 enthalten sind, müssen befolgt werden.

2 Die Evaluation

Der EVG wurde nach der Evaluationsmethodologie für die Beschleunigte Sicherheitszertifizierung (BSZ) evaluiert. Hierbei wurden die Anwendungshinweise und Interpretationen zum Schema zur BSZ (AIS B) [3] beachtet. Insbesondere wurde die AIS B4 „Requirements for Evaluation according to BSZ“ befolgt.

Basierend auf dem Ansatz der BSZ mit risikogetriebener Evaluierung innerhalb einer fester Evaluierungszeit wurde der Prozess der Inbetriebnahme sowie die Übereinstimmung des EVG zu der Beschreibung in den Sicherheitsvorgaben und der AIS B6 „Requirements for a TOE“ überprüft. Hauptteil der Evaluation war die Untersuchung der Widerstandsfähigkeit der Sicherheitsfunktionen mittels Penetrationstests.

2.1 Inbetriebnahme und Konfiguration

Der EVG wurde wie in AIS B4 [3] gefordert in Betrieb genommen und konfiguriert.

Der EVG kann durch die Beschreibung in den Sicherheitsvorgaben [6], Seiten 11 - 12, und der Secure User Guidance [8] in die zertifizierte Konfiguration gebracht werden.

Für die Evaluierung wurde der Evaluierungsgegenstand in einer virtuellen Windows Server Maschine betrieben. Das zugrundeliegende Betriebssystem der virtuellen Maschine war ein Windows Server 2022 21H2 (Betriebssystembuild 20348.1787) [7].

2.2 Konformität und Funktionsanalyse der Sicherheitsfunkionen

Die tatsächlichen Sicherheitsfunktionen des EVG stimmen mit denen in den Sicherheitsvorgaben beschriebenen Sicherheitsfunktionen (siehe Tabelle 2) überein. Alle in AIS B6 [3] geforderten Sicherheitsfunktionen sind in der Kombination aus EVG und dem nach SUG [8] konfigurierten Windows Server, siehe Assumption.SecuredWindowsServer, enthalten. Hierbei werden die Anforderungen in Absatz 6, 7, 9, 13, 23, 28, 29 und 30 in der AIS B6 [3] durch den oder mit Unterstützung des Windows Server umgesetzt.

2.3 Widerstandsfähigkeit der Sicherheitsfunktionen

Das EVG wurde einem Penetrationstest unterzogen um die Widerstandsfähigkeit der Sicherheitsfunktionen zu überprüfen. Hierbei wurde untersucht, ob auf Seite 13 der Sicherheitsvorgaben [6] beschriebenen Angreifer die Sicherheitsfunktionen unter Ausnutzung von Schwachstellen brechen oder umgehen konnten. Es konnten keine ausnutzbaren Schwachstellen gefunden werden.

2.4 Ergebnis der kryptographischen Bewertung

Die Implementierung der kryptografischen Funktionen im EVG wurde nach AIS B2 [3] geprüft. Sie ist konform zu den in [3] geforderten SCES-ACM und BSI-TR-02102 Vorgaben und es konnten keine ausnutzbaren Schwachstellen gefunden werden. Für die Umsetzung des STARTTLS für die SMTPs Schnittstelle und der Zufallszahlengeneration greift der EVG auf Funktionen des Windows Servers auf dem der EVG installiert ist. Diese entliehenen Funktionen des Windows Servers wurde nur in der Nutzung durch den EVG geprüft und nicht tiefergehend und unabhängig vom EVG geprüft.

Die Stärke der kryptografischen Algorithmen wurde in diesem Zertifizierungsverfahren nicht bewertet (siehe BSIG §9, Abs. 4, 2). Jedoch können kryptografische Funktionen mit einem Sicherheitsniveau unterhalb von 120 Bit nicht länger als sicher angesehen werden, ohne den Anwendungskontext zu beachten. Deswegen muss geprüft werden, ob diese kryptografischen Funktionen für den vorgesehenen Verwendungszweck angemessen sind. Weitere Hinweise und Anleitungen können der „Technischen Richtlinie BSI TR-02102“ (https://www.bsi.bund.de/dok/6615148) entnommen werden. Hier ist insbesondere zu beachten, dass die Rauschquelle für die Zufallszahlenerzeugung durch den Windows Server bereitgestellt wird und nicht geprüft wurde.

Die Tabelle 3in Anhang A in Teil C dieses Reportes gibt einen Überblick über die im EVG enthaltenen kryptographischen Funktionen und legt deren Bewertung des Sicherheitsniveaus aus kryptografischer Sicht dar. Jede kryptografische Funktion, die in der Spalte 'Sicherheitsniveau mehr als 120 Bit' ein 'Nein' enthält, erreicht nur ein Sicherheitsniveau unterhalb von 120 Bit (im allgemeinen Anwendungsfall).

2.5 Updatemechanismus

Für ein Update wird der EVG durch einen Administrator neu auf dem Windowsserver installiert. Das Installationspaket ist signiert und wird durch den Windows Server geprüft. Das Ergebnis der Prüfung muss vom Administrator bei Beginn der Installation geprüft werden.

2.6 Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 1 genannte Secure User Guidance wird auf weiter Handbücher und Installationsanleitungen verwiesen, die weitere notwendigen Informationen zur Anwendung des EVG enthalten. Alle darin enthaltenen Sicherheitshinweise sind zu beachten. Zusätzlich sind die Anforderungen an die Einsatzumgebung des EVG aus den Sicherheitsvorgaben zu beachten, ohne die ein im Sinne des Zertifikats sicherer Betrieb nicht bestätigt ist.

Der Anwender des Produkts muss die Ergebnisse dieser Zertifizierung sowie die zeitliche Begrenzung der Gültigkeit des Zertifikats in seinem Risikomanagementprozess berücksichtigen.

Die Begrenzung der Gültigkeit der Verwendung der kryptographischen Algorithmen, wie in Teil B Abschnitt 2.4 dargelegt, muss ebenso durch den Anwender und seinen Risikomanagementprozess für das IT-System berücksichtigt werden.

Zusätzlich sind die folgenden Auflagen und Hinweise zu beachten:

- Das Zertifikat bezieht sich nur auf den Evaluierungsgegenstand und macht keine Aussagen zur Sicherheit der notwendigen Betriebsumgebung. Zu dieser Betriebsumgebung gehört der Windows Server auf dem der EVG installiert wird. Die notwendigen Maßnahmen um die Sicherheit der Betriebsumgebung zu gewährleisten liegen in der Verantwortung des Betreibers des EVGs.

3 Definitionen

3.1 Abkürzungen

AIS Anwendungshinweise und Interpretationen zum Schema

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

EVG Evaluierungsgegenstand

ETR Evaluation Technical Report

IT Information Technology – Informationstechnologie

SF Security Function - Sicherheitsfunktion

ST Security Target - Sicherheitsvorgaben

TOE Target of Evaluation – Evaluierungsgegenstand

MX Mail Exchange Resource Record

3.2 Glossar

Evaluierungsgegenstand – Software, Firmware und / oder Hardware und zugehörige Handbücher.

Sicherheitsvorgaben - Eine implementierungsabhängige Menge von Sicherheitsanforderungen für eine Kategorie von EVG.

4 Literaturangaben

[1] BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (BSZ- Produkte) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ-Produkte.html

[2]BSI-Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (BSZ-Prüfstellen), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ-Pruefstellen.html

[3] Anwendungshinweise und Interpretationen zum Schema (AIS), die für den EVG relevant sind[6] https://www.bsi.bund.de/bsz

[4] Anerkennungsabkommen: Mutual Recognition Agreement of Cybersecurity Evaluation Certificates issued under a Fixed-time Certification Process, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/BSZ/Abkommen_Anerkennung_ANSSI_BSI.pdf

[5] Deutsche IT-Sicherheitszertifikate, periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird, https://www.bsi.bund.de/bsz

[6] Die für diese Zertifizierung geltenden AIS B:
- AIS B1 Requirements for ST and IAR, Version 1.1, 25.05.2022
- AIS B2 Requirements for the evaluation of cryptographic mechanisms according to BSZ, Version 1.1, 25.05.2022
- AIS B3 Requirements for user guidance Version, 1.1, 25.05.2022
- AIS B4 Requirements for Evaluation according to BSZ, Version 1.1, 15.07.2022
- AIS B5 Guideline for determining the efforts for a BSZ evaluation, Version 1.1, 25.05.2022
- AIS B6 Requirements for a TOE, Version 1.1, 01.06.2022

[6] Sicherheitsvorgaben BSI-DSZ-BSZ-0007-2023, Version 1.0, 14.11.2023, Security Target for NoSpamProxy Server

Version 14, Net at Work GmbH

[7] Evaluierungsbericht, Version 3, 21.09.2023, GESAMTPRÜFBERICHT / ETR zu NoSpamProxy Server 14.0 von Net at Work GmbH, secuvera GmbH

[8] Secure User Guidance für den EVG, Version 1.0, 18.10.2023, Secure User Guidance (SUG) NoSpamProxy Server Version 14, Net at Work GmbH

[9] Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln, BSI, 2021, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen_zur_Haertung_von_Windows_10.html

[10] BSI TR-02103 X.509-Zertifikate und Zertifizierungspfadvalidierung, 2020, BSI, https://www.bsi.bund.de/dok/TR-02103

[11] BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2023, BSI, https://www.bsi.bund.de/dok/TR-02102

C Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Übersicht und Bewertung der im EVG enthaltenen kryptographischen Funktionalitäten

Anhang A zum Zertifizierungsreport BSI-DSZ-BSZ-0007-2023 Übersicht und Bewertung der im EVG enthaltenen kryptographischen Funktionalitäten

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*[7]	*Bemerkungen*
1	**Port 25 – Trusted Channel: Kommunikation zwischen E-Mail-Servern (SMTP)**	SMTPS mit STARTTLS	[RFC 5321] (SMTP)			EVG nutz hier die Funktionen des Windows Server
			TLS 1.2			
2	Sicherer Kanal für SMTP (TLS 1.2)	TLS 1.2	[RFC 5246] (TLS 1.2)			
3	Vertraulichkeit mit Nachrichten-authentizität	AES im GCM-Modus	[FIPS 197] (AES) [SP800-38D] (GCM)	128, 256	Ja	
4	Integrität	HMAC with SHA-2	[FIPS 180-4] (SHA) [RFC-2104] (HMAC) [RFC-5246] (TLS v1.2)	256, 384	Ja	
5	Schlüsselaushandelung	ECDHE (secp384r1, brainpoolP256v1)	[RFC 8422] (ECC für TLS 1.2) [RFC 7027] (Brainpool ECC für TLS 1.2)	256, 384	Ja	
6	Authentifizierung	RSA Signatur-erzeugung und -verifikation mittels SHA-256	[RFC-8017] (RSASSAPKCS1-v1_5) [FIPS 180-4] (SHA)	2048	nein	Verwendung von RSA mit Schlüssellänge von 2048 ist ab dem Jahr 2024 nicht mehr vom BSI empfohlen.
7		ECDSA (secp384v1, brainpoolP256r1)	[ANSI X9.62] (ECDSA)	256, 384	Ja	

[7] Hinweis für Produktnutzer: Die Bewertung des Sicherheitsniveaus von 120 Bit bezieht sich nur auf die Stärke der einzelnen kryptographischen Mechanismen. Das Sicherheitsniveau im Betrieb eines kryptographischen Protokolls kann von externen Faktoren abhängen, die nicht Teil des EVGs sind.

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*[7]	*Bemerkungen*
			TLS 1.3			
8	Sicherer Kanal für SMTP (TLS 1.3)	TLS 1.3	[RFC 8446] (TLS 1.3)			
9	Vertraulichkeit mit Nachrichten-authentizität	AES im GCM-Modus	[FIPS 197] (AES) [SP800-38D] (GCM)	128, 256	Ja	
10	Integrität	HMAC mit SHA-2	[RFC 8446] (TLS1.3) [FIPS 180-4] (SHA)	256, 384	Ja	
11	Schlüsselaushandelung	ECDHE (secp384r1, brainpoolP256v1)	[RFC 8446] (TLS 1.3)	256, 384	Ja	
12	Authentifizierung	RSA Signatur-erzeugung und verifikation mittels SHA-256	[RFC-8017] (RSASSAPKCS1-v1_5) [FIPS 180-4] (SHA)	2048	nein	Verwendung von RSA mit Schlüssellänge von 2048 wird ab dem Jahr 2024 nicht mehr vom BSI empfohlen.
13		ECDSA (secp384r1, brainpoolP256v1)	[ANSI X9.62] (ECDSA)	256, 384	Ja	
14	**E-Mail Verschlüsselung mittels PGP**	PGP	[RFC 4880] (OpenPGP)			
15	Vertraulichkeit	AES im CBC-Modus	[FIPS 197] (AES) [SP 800-38A] (CBC)	128, 192, 256,	Ja	
16	Vertraulichkeit mit Nachrichten-authentizität	AES im GCM-Modus	FIPS 197] (AES) [SP800-38D] (GCM)	128, 256	Ja	
17	Authentizität und Integrität	RSA	[RFC 2313] (RSA)	2048, 3072, 4096	Nein für 2048, sonst Ja	Verwendung von RSA mit Schlüssellänge von 2048 wird ab dem Jahr 2024 nicht mehr vom BSI empfohlen.
18		SHA-2	[FIPS 180-4] (SHA)	256, 384, 512	Ja	
19		OAEP	[RFC 8017] (RSAES-OAEP)			

Nr.	*Zweck*	*Kryptografische Funktion*	*Implementierungs-standard*	*Schlüsselgröße in Bit*	*Sicherheits-niveau mehr als 120 Bit*[7]	*Bemerkungen*
20	Authentizität und Integrität	PKCS1.5	[RFC-8017] (RSASSAPKCS1-v1_5)			
21		PSS	[RFC 8017] (RSASSA-PSS)			
22		ECDSA	[ANSI X9.62] (ECDSA) [RFC 6637] (ECDSA)	256, 384, 512	Ja	
23	**E-Mail Verschlüsselung mittels S/MIME**	S/MIME	[RFC 8551] (S/MIME)			
24	Vertraulichkeit	AES im CBC-Modus	[FIPS 197] (AES) [SP 800-38A] (CBC)	128, 192, 256,	Ja	
25		Tripple DES im CBC-Modus	[FIPS 46-3] (DES)	112	Nein	Wird nicht vom BSI empfohlen. Kann nur zur Entschlüsselung eingesetzt werden.
26	Vertraulichkeit mit Nachrichten-authentizität	AES im GCM-Modus	FIPS 197] (AES) [SP800-38D] (GCM)	128, 256	Ja	
27	Authentizität und Integrität	RSA		2048, 3072, 4096	Nein für 2048, sonst Ja	Verwendung von RSA mit Schlüssellänge von 2048 wird ab dem Jahr 2024 nicht mehr vom BSI empfohlen.
28		SHA-2	[FIPS 180-4] (SHA)	256, 384, 512	Ja	
29		OAEP	[RFC 8017] (RSAES-OAEP)			
30		PKCS1.5	[RFC-8017] (RSASSAPKCS1-v1_5)			
31		PSS	[RFC 8017] (RSASSA-PSS)			
32		ECDSA	[ANSI X9.62] (ECDSA) [RFC 6637] (ECDSA)	256, 384, 512	Ja	

Tabelle 3: Kryptografische Funktionen des EVG

Bemerkung: Ende des Reportes