Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierungsreport

BSI-DSZ-BSZ-0003-2021

zu

LANCOM Business VPN Router 'LANCOM 1900EF' with LANCOM Systems Operating System 'LCOS 10.32.0029 PR' and IPsec VPN, Firmwareversion 10.32.0029 PR, Hardwareversion MOD C11

der

LANCOM Systems GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-BSZ-0003-2021 (*)

Netzwerk- und Kommunikationsprodukte

LANCOM Business VPN Router 'LANCOM 1900EF' with LANCOM Systems Operating System 'LCOS 10.32.0029 PR' and IPsec VPN
Firmwareversion 10.32.0029 PR, Hardwareversion MOD C11

von LANCOM Systems GmbH

Das in diesem Zertifikat genannte IT-Produkt wurde von einer in Anerkennung befindlichen 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 Produktes 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.

Die Evaluation wurde in Übereinstimmung mit den Bestimmungen des Zertifizierungsschemas des Bundesamtes für Sicherheit in der Informationstechnik durchgeführt. Die im Evaluationsbericht enthaltenen Schlussfolgerungen der Prüfstelle sind in Einklang mit den erbrachten Nachweisen.

Dieses Zertifikat ist keine generelle Empfehlung des IT-Produktes durch das Bundesamt für Sicherheit in der Informationstechnik oder eine andere Organisation, die dieses Zertifikat anerkennt oder darauf Einfluss hatte. Eine Gewährleistung für das 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.

Bonn, 16. Juni 2021

Bundesamt für Sicherheit in der Informationstechnik

Im Auftrag

Sandro Amendola L.S.
Abteilungsleiter

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

Gliederung

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 Produktes wird auf Veranlassung des Herstellers oder eines Vertreibers - im folgenden Antragsteller genannt - durchgeführt.

Bestandteil des Verfahrens ist die technische Prüfung (Evaluierung) des Produktes 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 Produktes, 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
- BSI-Zertifizierung: Verfahrensdokumentation zum Zertifizierungsprozess (BSZ-Produkte) [1]
- BSI-Zertifizierung: Verfahrensdokumentation zu Anforderungen an Prüfstellen, deren Anerkennung und Lizenzierung (BSZ-Stellen) [1]
- BSI-Zertifizierung: Anwendungshinweise und Interpretationen zum Schema (AIS B) [2]

1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009, Bundesgesetzblatt I S. 2821

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 des BMI für individuell zurechenbare öffentliche Leistungen indessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) vom 2. September 2019,Bundesgesetzblatt I S. 1365

3. 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 LANCOM Business VPN Router 'LANCOM 1900EF' with LANCOM Systems Operating System 'LCOS 10.32.0029 PR' and IPsec VPN, Firmwareversion 10.32.0029 PR, Hardwareversion MOD C11 hat das Zertifizierungsverfahren beim BSI durchlaufen.

Die Evaluation des Produkts LANCOM Business VPN Router 'LANCOM 1900EF' with LANCOM Systems Operating System 'LCOS 10.32.0029 PR' and IPsec VPN, Firmwareversion 10.32.0029 PR, Hardwareversion MOD C11 wurde von SRC Security Research & Consulting GmbH durchgeführt. Die Evaluierung wurde am 4. Mai 2021 abgeschlossen. Das Prüflabor SRC Security Research & Consulting GmbH ist eine vom BSI in Anerkennung befindliche Prüfstelle (ITSEF)[4].

Der Antragsteller ist: LANCOM Systems GmbH.

Das Produkt wurde entwickelt von: LANCOM Systems GmbH.

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

4. Gültigkeit des Zertifizierungsergebnisses

Dieser Zertifizierungsreport bezieht sich nur auf die angegebene Version des Produktes. 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 Produktes gemäß den Sicherheitsvorgaben zum Zeitpunkt der Ausstellung.

Um in Anbetracht der sich weiter entwickelnden Angriffsmethoden eine unbefristete Anwendung des Zertifikats trotz der Erfordernis nach einer Neubewertung nach den Stand der Technik zu verhindern, wurde die maximale Gültigkeit des Zertifikats begrenzt. Dieses Zertifikat, erteilt am 16. Juni 2021, ist gültig bis 15. Juni 2023. Die Gültigkeit kann im Rahmen einer Rezertifizierung erneuert werden.

Der Inhaber des Zertifikats ist verpflichtet,

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

[4] Information Technology Security Evaluation Facility

3. eingehende Meldungen bezüglich potenzieller Schwachstellen des Produktes unverzüglich zu prüfen und die Prüfung zu dokumentieren, hierzu gehört insbesondere die Prüfung der über die Kontaktadresse gemäß 2. gemeldeten Schwachstellen,
4. die Zertifizierungsstelle des BSI unverzüglich über Schwachstellen des Produktes zu informieren, die nach dem Zeitpunkt der Zertifizierung durch Ihn oder Dritte festgestellt wurden, und den Anwendern des Produktes unverzüglich kostenfrei über den in Teil B Sektion 2.5 genannten sicheren Update-Kanal eine Fehlerkorrektur und auf Wunsch des Anwenders ergänzend Informationen zur Auswirkung der Schwachstelle zur Verfügung zu stellen,
5. die „Secure User Guidance for LANCOM Business VPN Router ‘LANCOM 1900EF’ with LANCOM Systems Operating System ‘LCOS 10.32.0029 PR’ and IPsec VPN“ Version 1.25 vom 21.01.2021 unverzüglich nach Erteilung des Zertifikats verfügbar zu machen,
6. in den Sicherheitsvorgaben vor Veröffentlichung im Kapitel „Cryptographic Mechanisms (Ipsec)“ das Signaturverfahren “RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-1” sowohl für Authentizität als auch für Authentifizierung zu entfernen, oder ausdrücklich als „nicht in der zertifizierten Konfiguration enthalten“ zu kennzeichnen,
7. die zertifizierte Version bzw. den Software-Zweig 10.32 PR während der Gültigkeit der Zertifizierung mit Sicherheitsupdates zu pflegen. Diese Sicherheitsupdates auf müssen auf der zertifizierten Version basieren und nur Behebung von der aufgetretenen Schwachstellen dienen. Auf der Webseite https://www.lancom-systems.de/produkte/firmware/versionsuebersicht/ wird diese Version in die Kommunikation zum LCOS Lifecycle aufgenommen und die gegebenenfalls notwendigen zukünftigen Sicherheitsupdates werden unter https://www.lancom-systems.de/downloads/ zum Download bereitgestellt.

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

5. Veröffentlichung

Das Produkt LANCOM Business VPN Router 'LANCOM 1900EF' with LANCOM Systems Operating System 'LCOS 10.32.0029 PR' and IPsec VPN, Firmwareversion 10.32.0029 PR, Hardwareversion MOD C11 ist in die BSI-Liste der zertifizierten Produkte, die regelmäßig veröffentlicht wird, aufgenommen worden (siehe auch Internet: https://www.bsi.bund.de). Nähere Informationen sind über die BSI-Infoline 0228/9582-111 zu erhalten.

Weitere Exemplare des vorliegenden Zertifizierungsreports können beim Hersteller des Produktes 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

Der Evaluierungsgegenstand (EVG) ist der 'LANCOM 1900EF' mit dem Betriebssystem 'LCOS 10.32.0029 PR'. Dieses Produkt ist ein Business Router mit VPN und Firewall Funktion.

1.1. Produktbeschreibung

Der LANCOM Business VPN Router 'LANCOM 1900EF' ermöglicht sichere VPN Standortvernetzung über unsicher Netze wie z. B. das Internet. Zusätzlich schützt eine Stateful-Firewall-Funktion das Netzwerk mit „Intrusion Prevention“ und bietet Schutz gegen einige Denial-of-Service-Angriffe (DoS).

Schnittstellen:

Der Router besitzt 4 LAN Ethernet Ports, 2 WAN Ethernet Ports, einen COM Port für serielle Kommunikation und einen USB Port. Sowohl die LAN als auch die WAN Ethernet Ports unterstützen Gigabit Ethernet und können individuell verwendet werden, um den EVG mit vertrauenswürdigen lokalen Netzen (LAN), oder nicht-vertrauenswürdigen entfernten Netzen (WAN) zu verbinden. Ein COM Port erlaubt die direkte Kommunikation zwischen einem Computer und dem Router zu Administrationszwecken. Ein USB Port unterstützt USB 2.0 und ist für Verwaltungsaufgaben vorgesehen.

Administrationsdienste:

Der Router stellt einen HTTPS-Server bereit, über den er mittels einer grafischen Nutzeroberfläche (WEBconfig) konfiguriert werden kann. Außerdem wird ein SSH-Server bereitgestellt, der eine Konfiguration über ein Command Line Interface ermöglicht. Das Monitoring des Routers kann über den bereitgestellten SNMPv3-Server erfolgen.

Internetzugang:

Der Router erlaubt die Steuerung des Netzwerkverkehrs zwischen dem vertrauenswürdigen lokalen Netzwerk (LAN) und einem nicht vertrauenswürdigen Netz, wie dem Internet mittels IPv4 Network Address Translation (NAT).

VPN Verbindung:

Der Router ermöglicht VPN Verbindungen. Diese Verbindung erlaubt Vertraulichkeit, Integrität und Authentizität der übertragenen Daten über ein unsicheres Netzwerk, wie das Internet, indem die Daten verschlüsselt und signiert werden.

Firewall und Routing:

Der Router hat eine IPv4 Stateful Inspection Firewall die Kommunikationsverbindungen konfigurationsabhängig erlaubt oder verweigert. Außerdem stellt die Firewall DoS-Schutz und „Intrusion Detection/Prevention -Dienste zur Verfügung. Wenn eine Verbindung durch die Firewall erlaubt ist, wird der Pfad zum Ziel durch den Routingdienst vorgegeben.

Hinweis:

Die im Router enthaltenen IPv6 Dienste sind nicht Teil der evaluierten Konfiguration und sind damit nicht Gegenstand dieses Zertifikats.

1.2. Produktidentifikation

Nr	Typ	Identifier	Version
1	Firmware	LCOS 10.32.0029 PR	10.32.0029 / 14.01.2021
2	Hardware	LANCOM 1900EF	C 2019-09-12 MOD C11
3	Dokument	Security Target for LANCOM Business VPN Router ‘LANCOM 1900EF’ with LANCOM Systems Operating System ‘LCOS 10.32.0029 PR’ and IPsec VPN, LANCOM,	Version 1.25, 21.01.2021
4	Dokument	Secure User Guidance for LANCOM Business VPN Router ‘LANCOM 1900EF’ with LANCOM Systems Operating System ‘LCOS 10.32.0029 PR’ and IPsec VPN, LANCOM,	Version 1.25, 21.01.2021

Tabelle 1: Auslieferungsumfang des EVG

Die Firmwareversionsnummer kann über das Web Interface unter dem Pfad 'Systeminformation' > 'Systemdaten' > 'Firmwareversion' (wie in den Sicherheitsvorgaben "Security Target", "Introduction", "Product Identification", Seite 5, angegeben) abgerufen werden.

Die Hardwareversion kann über das Web Interface unter dem Pfad 'Systeminformation' > 'Systemdaten' > 'Hardware-Release' abgerufen werden und ist auch auf dem Schild auf der Unterseite des Geräts angegeben.

1.3. Sicherheitsfunktionalität des EVG

Die Werte, die durch den EVG geschützt werden, sind in den Sicherheitsvorgaben [4] auf Seite 13 und 14 unter „Assets“ definiert. Basierend auf diesen Werten stellen die Sicherheitsvorgaben die Sicherheitsumgebung in Form von Annahmen, Bedrohungen und Angreifern auf den Seiten 12 bis 17 dar. Der EVG bietet die in Tabelle 2 aufgezählte Sicherheitsfunktionalität an, um die Werte vor den beschriebenen Bedrohungen zu schützen. Diese Sicherheitsfunktionalität des EVG wurde in der Evaluation betrachtet.

Sicherheitsfunktionalität des EVG	Beschreibung
SecFunc.HTTPS	Der EVG implementiert den Zugriff auf die WEBconfig über HTTP/1.1 mit TLS 1.2 (HTTPS) an. Diese Protokolle ermöglichen dem Administrator sichere Anmeldung und sicheren Zugriff auf die Administrationsschnittstelle. Es wird die Vertraulichkeit, Integrität und Authentizität der zwischen Administrator und EVG übertragenen Daten geschützt.
SecFunc.SSH	Der EVG implementiert den Zugriff auf das Comand Line Interface mittels SSH. Dieses Protokoll ermöglichen dem Administrator sichere Anmeldung und sicheren Zugriff auf die Administrationsschnittstelle. Es wird die Vertraulichkeit, Integrität und Authentizität der zwischen Administrator und EVG übertragenen Daten geschützt.

Sicherheitsfunktionalität des EVG	Beschreibung
SecFunc.SNMPv3	Der EVG implementiert den Zugriff auf die SNMP-Schnittstelle mittels SNMPv3. Dieses Protokoll ermöglichen dem Administrator sichere Anmeldung und sicheren Zugriff auf die SNMP-Schnittstelle. Es wird die Vertraulichkeit, Integrität und Authentizität der zwischen Administrator und EVG übertragenen Daten geschützt.
SecFunc.IPsec	Der EVG implementiert die IPsec-VPN-Verbindungen mittels IPsec. Das Protokoll ermöglicht sicher Datenübertragung über unsichere Netzwerke. Es wird die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten geschützt.
SecFunc.Ipsec.Log	Der EVG zeichnet sowohl erfolgreiche als auch nicht erfolgreiche Verbindungsaufbauversuche auf und speichert sie.
SecFunc.Firewall.Sessions	Der EVG implementiert eine IPv4 Firewall und Routing Dienste. Basierend auf der EVG Konfiguration erlauben diese Dienste Zugang aus dem sicheren lokalen Netzwerk in ein unsicheres Netzwerk (Internet) und verweigert den Zugang vom unsicheren Netzwerk in das sichere lokale Netzwerk. Außerdem erlauben diese Dienste den Zugang aus dem sicheren lokalen Netzwerk in ein sicheres entferntes Netzwerk mittels IPsec VPN Verbindungen.
SecFunc.Firewall.DoS.IDS	Der EVG implementiert eine IPv4 Firewall die DoS-Schutz und Intrusion Detection/Prevention (IDS) Services bietet. Der DoS Schutz registriert und reagiert auf TCP SYN flooding, Smurf, LAND, Ping of Death, Teardrop und Bonk Angriffe. Die IDS registrieren und reagieren auf IP spoofing und Portscans.
SecFunc.Firewall.Log	Der EVG zeichnet Verbindungsversuche, die von der Firewall verweigert wurden auf und speichert sie.
SecFunc.Auth.AdmCrds	Der EVG authentifiziert Administratoren mittels Nutzername und Passwort, bevor er Zugriff auf die WEBconfig, das Comand Line Interface (CLI) oder SNMP-Schnittstelle gewährt. Für die CLI ist auch Authentifizierung mittels SSH Schlüssels möglich.
SecFunc.Auth.AdmPwdChrs	Der EVG verlangt, dass Administratorkennwörter mindestens 8 Zeichen lang sind und mindestens 3 der 4 folgenden Zeichentypen enthalten: Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen.
SecFunc.Auth.BrtFrcCtr	Der EVG erschwert brute-force Angriffe auf die Passwortabfrage mittels einer zeitlichen Sperre nach einer zu konfigurierenden Anzahl falscher

Sicherheitsfunktionalität des EVG	Beschreibung
	Eingaben.
SecFunc.Auth.AutoLogOut	Der EVG logt einen Administrator automatisch, nach einer einer zu konfigurierenden Zeit der Inaktivität, aus.
SecFunc.Auth.Log	Der EVG zeichnet erfolgreiche und nicht erfolgreiche Loginversuche auf und speichert sie.
SecFunc.Mgmt.NoInet	In der evaluierten Konfiguration verweigert der EVG den Zugriff auf die WEBcofing, das CLI und die SNMP-Schnittstelle aus dem unsicheren Netzwerk.
SecFunc.Mgmt.Ports	Der EVG erlaubt, dass die Protokolle HTTPS, SSH und SNMPv3 über Nichtstandard TCP/UDP-Ports arbeiten.

Tabelle 2: Sicherheitsfunktionalität des EVG

1.4. Konfiguration des EVG

Dieses Zertifikat gilt nur für die im Secure User Guide [6] beschriebene Konfiguration des EVG. Insbesondere sind die folgenden Funktionen, die in den Sicherheitsvorgaben [4] auf Seite 18 unter „Limits of Evaluation“ beschrieben sind, von der Evaluation ausgeschlossen und nicht vom Zertifikat abgedeckt:

- Der COM Port für Administrationszwecke
- Der USB Port für Administrationszwecke
- Die IPv6 Funktionalität des Routers

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

Auf Seite 11 der Sicherheitsvorgaben [4] 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 möglich ist. Hierbei sind die folgenden Punkte relevant:

- Der physische Zugang zum EVG ist beschränkt.
- Nur Administratoren haben physischen Zugang zum EVG.
- Administratoren nutzen nur die Protokolle HTTPS, SSH und SNMP um auf den EVG zuzugreifen und zu konfigurieren.
- Administratoren richten den EVG gemäß des Secure User Guide [6] ein.

- Normale Nutzer (User) haben keinen physischen Zugriff auf den EVG.
- Normale Nutzer (User) im sicheren lokalen Netzwerk sind vertrauenswürdig.
- Alle Nutzer in unsicheren entfernten Netzwerken (z. B. Internet) sind nicht vertrauenswürdig.
- Normale Nutzer (User) in sicheren entfernten Netzwerken, die über IPsec VPN Verbindungen nutzen, sind vertrauenswürdig.
- Für den IPsec VPN wird das IPsec Protokoll genutzt.
- Es wird kein IPv6 genutzt.

1.6. Dokumente

Die evaluierten Dokumente, die in Tabelle 1 aufgeführt sind, werden zusammen mit dem Produkt zur Verfügung gestellt. Diese enthalten die zum sicheren Umgang mit dem EVG benötigt Informationen.

Zusätzliche Hinweise und Auflagen zum sicheren Gebrauch des EVG, die in Teil B Kapitel 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) [2] beachtet. Insbesondere wurde die AIS B4 „Requirements for Evaluation according to BSZ“ befolgt.

Basierend auf dem risikogetriebenen Ansatz mit fester Evaluierungszeit der BSZ wurde der Prozess der Inbetriebnahme, die Übereinstimmung des EVG zu der Beschreibung in den Sicherheitsvorgaben und der AIS B6 „Anforderungen an TOEs für die BSZ“ überprüft. Hauptteil der Evaluation war die Untersuchung der Widerstandsfähigkeit der Sicherheitsfunktionalitäten mittels Penetrationstests.

2.1. Inbetriebnahme und Konfiguration

Der EVG wurde wie in AIS B4 [2] gefordert in Betrieb genommen und konfiguriert.

Der EVG kann durch die Beschreibung im Secure User Guide [6] in die benötigte sichere Konfiguration gebracht werden.

2.2. Konformität und Funktionsanalyse der Sicherheitsfunktionalität

Die tatsächliche Sicherheitsfunktionalität des EVG stimmt mit der in den Sicherheitsvorgaben beschriebenen Sicherheitsfunktionalität (siehe Tabelle 2) überein. Alle der in AIS B6 [3] geforderten Sicherheitsfunktionen sind im EVG enthalten.

2.3. Widerstandsfähigkeit der Sicherheitsfunktionalitäten

Das EVG wurde einem Penetrationstest unterzogen um die Widerstandsfähigkeit der Sicherheitsfunktionalitäten zu überprüfen. Hierbei wurde untersucht, ob die auf den Seiten 12 bis 17 der Sicherheitsvorgaben[4] beschriebenen Angreifer die Sicherheitsfunktionalitäten unter Ausnutzung von Schwachstellen brechen oder umgehen konnten. Es konnten keine ausnutzbaren Schwachstellen gefunden werden.

2.4. Ergebnis der kryptografischen Bewertung

Die Implementierung der kryptografischen Funktionalitäten wurden nach [2] (AIS B2) geprüft. Sie ist konform zu den in [2] geforderten SCES-ACM und BSI-TR-02102 Vorgaben und es konnten keine ausnutzbaren Schwachstellen gefunden werden.

Die kryptografische Algorithmenstärke wurde in diesem Zertifizierungsverfahren nicht bewertet (siehe BSIG §9, Abs. 4, 2). Jedoch können kryptografische Funktionen mit einem Sicherheitsniveau unterhalb von 100 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) entnommen werden.

Die Tabelle in Anhang B gibt einen Überblick über die in der Sicherheitsfunktionalität des EVG enthaltenen kryptografischen Funktionalitäten und legt deren Bewertung des Sicherheitsniveaus aus kryptografischer Sicht dar.

2.5. Updatemechanismus

Der EVG verfügt über einen sicheren Updatemechanismus der gegebenenfalls notwendige Sicherheitsupdates ermöglicht. Der Prozess ist auf Seite 8 des Secure User Guides [6] beschrieben.

Gegebenenfalls notwendige Sicherheitsupdates können über die Webseite www.lancom-systems.com/downloads/ bezogen werden. (Siehe auch Teil A Kapitel 4 Punkt 7.)

2.6. Auflagen und Hinweise zur Benutzung des EVG

Die in Tabelle 1 genannte Betriebsdokumentation enthält die notwendigen Informationen zur Anwendung des EVG und 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 möglich ist.

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

Die Begrenzung der Gültigkeit der Verwendung der kryptografischen Algorithmen, wie in Teil B Kapitel 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:

Die kryptografische Funktion SHA-1 ist auf dem Router enthalten, muss aber für eine sichere Konfiguration deaktiviert sein. Dies ist in der Konfiguration, die im Secure User Guide [6] beschrieben ist, der Fall. Siehe auch Teil A Kapitel 4 Punkt 6.

In der Version 1.26 der Sicherheitsvorgaben ("Cryptographic Specification", "Cryptographic Mechanisms (IPsec)", Seite 29) wurde das Signaturverfahren "RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-1" gemäß Punkt 6 in Teil A Kapitel 4 entfernt.

3. Definitionen

3.1. Abkürzungen

AIS Anwendungshinweise und Interpretationen zum Schema

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

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

BSZ Beschleunigte Sicherheitszertifizierung

CLI Comand Line Interface

EVG Evaluierungsgegenstand

ETR Evaluation Technical Report

IDS Intrusion Detecion/Prevention Services

IT Information Technology – Informationstechnologie

SF Security Function – Sicherheitsfunktion

SNMP Simple Network Management Protocol

ST Security Target – Sicherheitsvorgaben

VPN Virtual Private Network

WEBconfig Web-based management interface

3.2. Glossar

Evaluationsgegenstand – Software, Firmware und / oder Hardware und zugehörige Handbücher

Sicherheitsvorgaben – Die Sicherheitsvorgaben beschreibt die Sicherheitsfunktionalität, die Schnittstellen, das Bedrohungsmodel und die Einsatzumgebung des Evaluationsgegenstandes.

4. Literaturangaben

[1] BSI-Zertifizierung: Verfahrendokumentation zum Zertifizierungsprozess (BSZ-Produkte) und Verfahrensdokumentation zu Anforderungen an Prüfstellen, die Anerkennung und Lizenzierung (BSZ-Stellen), https://www.bsi.bund.de/zertifizierung

[2] Anwendungshinweise und Interpretationen zum Schema der BSZ (AIS), die für den EVG relevant sind[5] (Für das Pilotverfahren noch nicht veröffentlicht)

[5]Die für diese Zertifizierung geltenden AIS B:

- AIS B1 Requirements for Security Targets Version 0.95 03.09.2020
- AIS B2 Requirements for the evaluation of cryptographic mechanisms in the context of accelerated security certification (BSZ) Version 0.91 13.02.2019
- AIS B3 Requirements for user guidance Version 0.9 27.09.2018
- AIS B4 Requirements for Evaluation according to BSZ Version 0.95 03.09.2020
- AIS B5 Guideline for calculating the required man days for BSZ 0.95 03.09.2020
- AIS B6 Anforderungen an TOEs für die BSZ Version 0.91 10.07.2020

[3] Deutsche IT-Sicherheitszertifikate (BSI 7148), periodisch aktualisierte Liste, die auch auf der Internet-Seite des BSI veröffentlicht wird, https://www.bsi.bund.de

[4] Sicherheitsvorgaben BSI-DSZ-BSZ-0003-2021, Version 1.25 21.01.2021, Security Target for LANCOM Business VPN Router 'LANCOM 1900EF' with LANCOM Systems Operating System 'LCOS 10.32.0029 PR' and IPsec VPN, LANCOM Systems GmbH

[5] Evaluierungsbericht, 2.20, 20.04.2021, Evaluation Technical Report (ETR) 1 im Verfahren BSI-BSZ-0003, SRC Security Research and Consulting GmbH (vertrauliches Dokument)

[6] Secure User Guide für den EVG, Version 1.25, 21.01.2021, Secure User Guidance for LANCOM Business VPN Router ‘LANCOM 1900EF’ with LANCOM Systems Operating System ‘LCOS 10.32.0029 PR’ and IPsec VPN, LANCOM Systems GmbH

C. Anhänge

Liste der Anhänge zu diesem Zertifizierungsreport

Anhang A: Die Sicherheitsvorgaben werden in einem eigenen Dokument zur Verfügung gestellt.

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

Anhang B zum Zertifizierungsreport -0003-2021

Übersicht und Bewertung der im EVG enthaltenen kryptografischen Funktionalitäten

Nr.	Zweck	Krypto-grafische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Sicherheits-niveau mehr als 100 Bit
1	Vertrauens-würdiger Kanal	TLS 1.2	[RFC 5246] (TLS), [RFC 5746] (TLSRENEGO),	-	-
2	Authentizität	ECDSA signature generation and verification using SHA-2 (secp256r1, secp384r1, secp521r1)	[RFC 5246] (TLS), [RFC 8422](TLSECC), [RFC 4366] (TLSEXT), [ANSI X9.62](ECDSA), [SECG SEC2](ECC), [RFC 3280] (PKIX), [FIPS 180-4] (SHA)	256, 384, 521	ja
3		RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-2	[RFC 5246] (TLS), [RFC 3447] (PKCS#1 v2.1), [RFC 3280] (PKIX), [FIPS 180-2] (SHA)	2048, 3072, 4096	ja
4	Authentifi-kation	ECDSA signature generation and verification using SHA-2 (secp256r1, secp384r1, secp521r1) (for ECDHE_ECDSA)	[RFC 5246] (TLS), [RFC 8422] (TLSECC), [RFC 4366] (TLSEXT), [ANSI X9.62] (ECDSA), [SECG SEC2] (ECC), [RFC 3280] (PKIX), [FIPS 180-4] (SHA)	256,384,521	ja
5		RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-(forECDHE_RSA)	[RFC 5246] (TLS), [RFC 8422] (TLSECC), [RFC 4366] (TLSEXT), [RFC 8017] (PKCS#1 v2.2), [RFC 3280] (PKIX), [FIPS 180-4] (SHA)	2048, 3072, 4096	ja
6		RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-2 (for DHE_RSA)	[RFC 5246] (TLS), [RFC 4366],(TLSEXT), [RFC 3447] (PKCS#1 v2.1), [RFC 3280] (PKIX), [FIPS 180-2](SHA)	2048, 3072, 4096	ja
7		Challenge-response password authentication using SHA-256	[FIPS 180-2] (SHA),	256	ja

Nr.	Zweck	Krypto-grafische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Sicherheits-niveau mehr als 100 Bit
8	Key Agreement	ECDHE (secp256r1, secp384r1, secp521r1)	[RFC 8422] (TLSECC), [RFC 4366] (TLSEXT), [IEEE P1363] (ECDH), [SECG SEC2] (ECC),	256, 384, 521	ja
9		DHE	[RFC 5246] (TLS), [RFC 2631] (DH), [ANSI X9.42] (DH), [RFC 3526] (MODP)	2048, 3072, 4096	ja
10	Vertraulich-keit	AES in GCM mode	[RFC 5246] (TLS), [RFC 5288] (AESGCM), [RFC 5289] (AES-GCM), [RFC 5116] (AES-GCM), [FIPS 197] (AES), [SP 800-38D] (GCM)	128, 256	ja
11		AES in CBC mode	[RFC 5246] (TLS), [FIPS 197] (AES), [SP 800-38A] (CBC),	128, 256	ja
12	Integrität	AES in GCM mode	[RFC 5246] (TLS), [RFC 5288] (AESGCM), [RFC 5289] (AES-GCM), [RFC 5116] (AES-GCM), [FIPS 197] (AES), [SP 800-38D] (GCM)	128, 256	ja
13		HMAC with SHA-2	[RFC 5246] (TLS), [RFC 5289] (AESCBC), [FIPS 180-2] (SHA), [RFC 2104] (HMAC)	256, 384	ja
14	Vertrauens-würdiger Kanal	SSH	[RFC 4251] (SSH-ARCH), [RFC 4252] (SSH-USERAUTH), [RFC 4253] (SSH-TRANS), [RFC 4254] (SSH-CONNECT),	-	-
15	Authentifi-zierung	ECDSA signature generation and verification using SHA-2 (ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsasha2-nistp521)	[RFC 5656] (SSH-ECC), [SEC1] (ECC), [SEC2] (ECC), [ANSI X9.62] (ECDSA), [FIPS 180-2] (SHA)	256, 384, 521	ja

Nr.	Zweck	Krypto-grafische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Sicherheits-niveau mehr als 100 Bit
16		RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-2 (rsa-sha2-256, rsa-sha2-512)	[RFC 8332] (SSH-AUTH-SHA2), [RFC 4253] (SSH-TRANS), [RFC 4252] (SSH-USERAUTH), [RFC 8017] (PKCS#1 v2.2), [FIPS 180-4] (SHA)	2048,3072,4096	ja
17	Schlüssel-austausch	ECDH with SHA-2 (ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521)	[RFC 5656] (SSH-ECC), [SEC1] (ECC), [SEC2] (ECC), [ANSI X9.63] (ECC), [FIPS 180-2] (SHA)	256, 384, 521	ja
18		DH with SHA-2 (diffie-hellman-groupexchange-sha256)	[RFC 4419] (SSH-DH-GEX) [HAC] (DH), [FIPS 180-2] (SHA)	2048, 3072, 4096	ja
19	Vertraulich-keit	AES in GCM mode	[RFC 5647], [RFC 5116] (AESGCM), [FIPS 197] (AES), [SP 800-38D] (GCM)	128, 256	Ja
20		AES in CTR mode	[RFC 4344], [FIPS 197] (AES), [SP 800-38A] (CTR)	128, 192, 256	ja
21		AES in CBC mode	[RFC 4253] (SSH-TRANS), [FIPS 197] (AES), [SP 800-38A] (CBC),	128,192, 256	ja
22	Integrität	AES in GCM mode	[RFC 5647], [RFC 5116] (AESGCM), [FIPS 197] (AES), [SP 800-38D] (GCM)	128, 256	ja
23		HMAC with SHA-2	[RFC 6668], [FIPS 180-2] (SHA), [RFC 2104] (HMAC)	256, 512	ja
24	Vertraulich-keit	AES in CFB mode	[RFC 3826] (SNMP-AES), [FIPS 197] (AES), [SP 800-38A] (CFB)	128, 192, 256	ja
25	Integrität	HMAC with SHA-2	[RFC 7860] (SNMP-SHA-2), [RFC 6234] (SHA-2), [FIPS 180-4] (SHA), [RFC 2104](HMAC)	256, 384, 512	ja

Nr.	Zweck	Krypto-grafische Funktion	Implementierungs-standard	Schlüsselgröße in Bit	Sicherheits-niveau mehr als 100 Bit
26	Vertrauens-würdiger Kanal	IPsec with IKEv2 and ESP	[RFC 4301] (IPsec), [RFC 7296] (IKEv2), [RFC 8247] (ALGO-IKE), [RFC 4303] (ESP), [RFC 8221] (ALGO-ESP),	-	-
27	Authentizität & Authentifi-zierung	RSA signature generation and verification (RSASSA-PSS) using SHA-2	[RFC 7427] (IKEv2-SIGAUTH), [RFC 5280] (PKIX), [RFC 3447] (PKCS#1 v2.1), [FIPS 180-4] (SHA)	2048, 3072, 4096	ja
28	Authentifi-zierung	MAC generation and verification using pre-shared keys and SHA-2	[RFC 7296] (IKEv2), [FIPS 180-4] (SHA)	256, 384, 512	ja
29	Schlüssel-austausch	ECDH (secp256r1, secp384r1, secp521r1)	[RFC 5903] (IKE-ECP), [IEEE P1363] (ECDH), [SECG SEC2] (ECC),	256, 384, 521	ja
30		DH	[RFC 2631] (DH), [ANSI X9.42](DH), [RFC 3526] (MODP)	2058, 3072, 4096	ja
31	Vertraulich-keit	AES in GCM mode	[RFC 5282], [RFC 5116], [RFC 4106], [FIPS 197] (AES), [SP 800-38D] (GCM)	128, 192, 256	ja
32		AES in CBC mode	[RFC 3602], [FIPS 197](AES), [SP 800-38A] (CBC),	128, 192, 256	ja
33	Integrität	AES in GCM mode	[RFC 5282], [RFC 5116], [RFC 4106], [FIPS 197] (AES), [SP 800-38D] (GCM)	128, 192, 256	ja
34		HMAC with SHA-2	[RFC 4868], [FIPS 180-2] (SHA), [RFC 2104] (HMAC)	256, 384, 512	ja

Tabelle 3: Kryptografische Funktionen des EVG

Bemerkung: Ende des Reportes