DORA-PRÜFPAKET · TEIL 3 VON 8

Technische und organisatorische Maßnahmen

Netztrennung, Verschlüsselung, Protokolle, Zugriffe und Betrieb, mit einer Prüfliste für Ihre IT

Stand: 14. November 2026 · Beschützerbox GmbH, Großbeerenstr. 11, 10963 Berlin

Das Kunden-WLAN ist ein eigenes Netz, das nur durch einen verschlüsselten Tunnel ins Internet führt; fällt der Tunnel aus, sperrt die Box. Diese Unterlage nennt, was im Produkt umgesetzt ist, was Ihre IT einrichtet und was sie selbst prüfen kann. Was es nicht gibt, steht in Abschnitt 9.

1. Netztrennung

Eigenes Kundennetz	Die Box spannt ein eigenes Netz mit eigenem Adressbereich auf (192.168.133.0/24), mit einem WLAN-Namen je Funkband (2,4 und 5 GHz).
Client-Isolation	Auf beiden Funknetzen (2,4 und 5 GHz) ist die Client-Isolation eingeschaltet: Geräte im selben Funknetz erreichen sich nicht.
Weiterleitung nur in den Tunnel	Aus dem Kundennetz leitet die Box Verkehr nur in den Tunnel zu unseren Servern, nicht in das Netz, an dem sie hängt. Direkt über Ihren Anschluss gehen nur die Namensauflösung (DNS) und Streamingdienste, die Sie im Portal freischalten.
Sperre bei Tunnelausfall	Fällt die Verbindung zu unseren Servern aus, sperrt die Box den Zugang, statt Ihre Kunden über Ihren Anschluss weitersurfen zu lassen.
Keine Verwaltung aus Ihrem Netz	Von Ihrem Netz aus bietet die Box keinen Zugang zur Verwaltung an. Eingestellt wird sie im Portal, zur Fehlersuche schaltet sich unser Support über den Tunnel auf (Abschnitt 4).
Netzwerkbuchsen der Box	Auch die Netzwerkbuchsen führen nur in den Tunnel, trennen angeschlossene Geräte aber nicht voneinander. Geräte Ihrer Bank gehören deshalb nicht an die Box.

2. Verschlüsselung

Tunnel	WireGuard zwischen Box und unseren Servern; das Verfahren arbeitet mit Curve25519 für den Schlüsselaustausch und ChaCha20-Poly1305 für die Verschlüsselung.
Steuerung der Box	Serverliste, Verbindungsaufbau und Lebenszeichen laufen per HTTPS.
WLAN	WPA2 mit Passwort oder bewusst offen, im Portal einstellbar. Das Passwort ändern Sie im Portal jederzeit, etwa monatlich; für den Aushang erzeugt das Portal einen QR-Code.
Portal	nur per HTTPS erreichbar (cloud.beschuetzerbox.de)

3. Protokolle und Datensparsamkeit

Surfen Ihrer Kunden	Den Verkehr, den wir für Ihre Kunden ins Internet weiterleiten, protokollieren wir nicht. Auch DNS-Anfragen protokollieren wir nicht. Ausnahme ist die Vorschaltseite der Box 4 Pro (letzte Zeile).
Auf der Box	Geräteadresse (MAC), Gerätename und lokale IP-Adresse der verbundenen Geräte nur im Arbeitsspeicher, in der Adressliste höchstens eine Stunde nach der letzten Verbindung; ein Neustart löscht sie.
Auf unseren Servern	wann sich Ihre Box mit welchem Server verbindet, ihre Kennung und die öffentliche IP-Adresse Ihres Anschlusses, für Betrieb und Störungssuche, rund 8 Wochen lang
Im Portal	Die verbundenen Geräte zeigt das Portal live an; gespeichert wird die Liste nicht.

Box 4 Pro mit Vorschaltseite	Bei der Box 4 Pro mit Vorschaltseite speichern unsere Cloud und unser Portalserver zusätzlich Anmeldedaten (unter anderem eine pseudonymisierte Geräteadresse, Anmeldeart, Browserkennung und Sitzungszeiten), Zugangscodes und freiwilliges Feedback; beim Anmelden protokolliert der Portalserver auch die Seite, die das Gerät zuerst aufrufen wollte. Diese Daten verarbeiten wir in Ihrem Auftrag.

4. Zugänge und Verwaltung

Portal-Konten	Jedes Konto meldet sich mit E-Mail-Adresse und Passwort an und sieht nur die Boxen, die es aufgenommen hat. Eine Box nimmt nur auf, wer ihre Seriennummer und PIN kennt; bewahren Sie die PIN wie ein Passwort auf. Mehrere Konten können dieselbe Box verwalten, etwa IT und Organisation.
Fernwartung	Unser Support schaltet sich zur Fehlersuche über den verschlüsselten Tunnel auf die Box.
Firmware	Grundlage der Firmware der Beschützerbox 4 ist OpenWrt 25.12.

5. Betrieb und Rechenzentren

Rechenzentren	Unsere Server stehen in Deutschland, in Rechenzentren der Hetzner Online GmbH; Zertifizierung und Testat von Hetzner stehen in Teil 4.
Mehrere Server	Bei jedem Verbindungsaufbau holt die Box die aktuelle Liste unserer Server per HTTPS von unserem Listen-Server bei Hetzner, der unter zwei Domainnamen erreichbar ist. Alle zwei Minuten prüft sie die Verbindung und baut sie bei einem Fehler neu auf, wenn nötig zu einem anderen Server. Bis dahin ist das Kunden-WLAN ohne Internet.
Überwachung	Sinkt die Zahl der insgesamt verbundenen Boxen unter eine feste Schwelle, alarmiert das Portal unsere Technik per E-Mail. Für jede Box schickt das Portal auf Wunsch eine E-Mail, wenn sie bei drei Prüfungen im Abstand von fünf Minuten nicht mit unseren Servern verbunden ist, und eine zweite, wenn sie wieder online ist. Die Adresse für diese Meldungen stellen Sie im Portal ein, zum Beispiel das Postfach Ihrer IT.
Verfügbarkeit	Zugesichert sind 99 % Verfügbarkeit je Abrechnungsmonat. Fällt der Dienst in einem Abrechnungsmonat zusammengerechnet länger als 7,2 Stunden aus, entfällt das Entgelt für diesen Monat (AGB § 5.3). Ausfälle, die Dritte verursachen, etwa beim Internetanschluss, zählen nicht. Für Banken zählen nach der Vertragsanlage (Teil 8, § 4) auch Ausfälle unserer Unterauftragnehmer.

6. Rechtliche Bindung

Fernmeldegeheimnis	Beschützerbox ist an das Fernmeldegeheimnis gebunden (§ 3 TDDDG).
Schutzpflichten	Als Anbieter öffentlich zugänglicher Telekommunikationsdienste muss Beschützerbox angemessene technische und organisatorische Vorkehrungen zum Schutz des Fernmeldegeheimnisses, personenbezogener Daten und gegen Störungen treffen, nach dem Stand der Technik (§ 165 TKG).
Meldepflichten	bei erheblichen Sicherheitsvorfällen und bei Verletzungen des Schutzes personenbezogener Daten (§§ 168, 169 TKG), siehe Teil 5
Aufsicht	Bundesnetzagentur; für die Daten des Telekommunikationsdienstes die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (§ 29 TDDDG)

Was wo wie lange gespeichert wird, im Einzelnen: Datenschutz-Prüfpaket (beschuetzerbox.de/beschaffung/datenschutz), Abschnitt 4.

7. Was Ihre IT einrichtet

- Die Box hängt mit einem Kabel an einem eigenen Port oder Segment Ihrer Firewall, das nur Verbindungen ins Internet zulässt. Wer gar kein fremdes Gerät im Filialnetz haben will, schließt sie an einen eigenen DSL- oder Mobilfunkanschluss an.
- Ab Werk bezieht die Box ihre Adresse an diesem Port oder Segment per DHCP. Eine feste Adresse richtet unser Support auf Wunsch vor dem Versand ein.

- Beschränken Sie den Port der Box auf deren MAC-Adresse. Dann kommt ein fremdes Gerät an diesem Anschluss nicht ohne Weiteres in Ihr Netz.
- Schließen Sie keine Geräte Ihrer Bank an die Netzwerkbuchsen der Box an. Ein zweites WLAN für private Handys Ihrer Mitarbeitenden richtet unser Support auf Wunsch ein; Geräte der Bank gehören auch dort nicht hinein.
- Setzen Sie im Portal ein WLAN-Passwort und lassen Sie die Streaming-Freischaltung ausgeschaltet. Sie würde ausgewählte Videodienste direkt über Ihren Anschluss leiten.
- Schalten Sie im Portal je Box die Ausfallmeldung ein, am besten an das Postfach Ihrer IT.
- Beim WireGuard-Zugang: Erzeugen Sie das Schlüsselpaar selbst und lassen Sie das Gäste-VLAN nur durch den Tunnel ins Internet. Dann bleibt es auch bei einem Tunnelausfall zu.

8. Was Ihre IT selbst prüfen kann

Am besten während der 30 Tage, in denen Sie die Box in einer Geschäftsstelle testen:

1. Mit einem Handy ins Kunden-WLAN gehen und beschuetzerbox.de/ip aufrufen: Die Seite zeigt eine IP-Adresse von Beschützerbox.
2. Vom selben Handy einen Drucker oder Router im Banknetz über dessen Adresse aufrufen: Es kommt keine Verbindung zustande.
3. Zwei Handys im selben Funknetz (gleicher WLAN-Name) erreichen sich gegenseitig nicht.
4. Streaming-Freischaltung ausgeschaltet lassen und in Ihrer Firewall die Verbindungen der Box zu unseren Servern sperren: Das Handy kommt nicht mehr ins Internet.
5. Im Protokoll Ihrer Firewall erscheinen von der Box neben der Adressvergabe (DHCP) nur Verbindungen nach außen: HTTPS zu Adressen unter beschuetzerbox.de und beschuetzerbox.gmbh, der WireGuard-Tunnel (UDP), DNS und die Uhrzeit (NTP).

9. Grenzen

> - Beschützerbox selbst ist nicht nach ISO/IEC 27001 zertifiziert. Die Nachweise unseres Rechenzentrumsbetreibers Hetzner stehen in Teil 4.
> - Die Namensauflösung übernimmt bei der Box Google Public DNS, mit gebuchtem Kinderfilter OpenDNS FamilyShield; diese Anfragen schickt die Box über Ihren Anschluss.
> - Die Netzwerkbuchsen der Box trennen angeschlossene Geräte nicht voneinander (Abschnitt 1).

Weiter: Störungs- und Meldewege (beschuetzerbox.de/banken/dora/meldewege) · Notfall und Ausstieg (beschuetzerbox.de/banken/dora/notfall-und-ausstieg)

Beschützerbox GmbH · Großbeerenstr. 11 · 10963 Berlin · Telefon 030 692066258 · mail@beschuetzerbox.de · beschuetzerbox.de · Amtsgericht Charlottenburg, HRB 163551 B · USt-IdNr. DE298017998 · Bundesnetzagentur Registriernummer 15/029 · Alle Unterlagen: beschuetzerbox.de/banken/dora