WebConnect Co-Router
Eine datenschutzrechtliche Betrachtung

Dieses Dokument betrachtet den WebConnect Co-Router aus datenschutzrechtlicher Sicht und geht auf die folgenden Fragen ein:

- Was ist WebConnect Co-Router?
- Wie funktioniert der WebConnect Co-Router?
- Welche datenschutzrechtlich relevanten Daten werden erhoben?
- Gilt der Betrieb von WebConnect Co-Router als Auftragsverarbeitung?

Was ist WebConnect Co-Router?

WebConnect Co-Router ist eine einfach zu installierende Hardware-Alternative zu VPNs, die völlig ohne Software-Installationen auf Infrastrukturkomponenten (Server, Workstations, etc.) auskommt.

WebConnect Co-Router ist in zwei Ausführungen erhältlich: als Box (eine kleine zigaretten-schachtelgrosse Hardwareeinheit) und als Image, welches auf einem virtuellen Server oder auch auf einem NAS (z.B. Synology NAS) implementiert werden kann. Die Unterschiede liegen im Wesentlichen in der Anzahl gleichzeitig unterstützter Connections.

In diesem Dokument wird nur der WebConnect Co-Router als Box betrachtet. Die Analyse erfolgt aufgrund der Angaben des Herstellers und eigenen Erfahrungen bei der Installation.

Betrachtungs-Gegenstand:

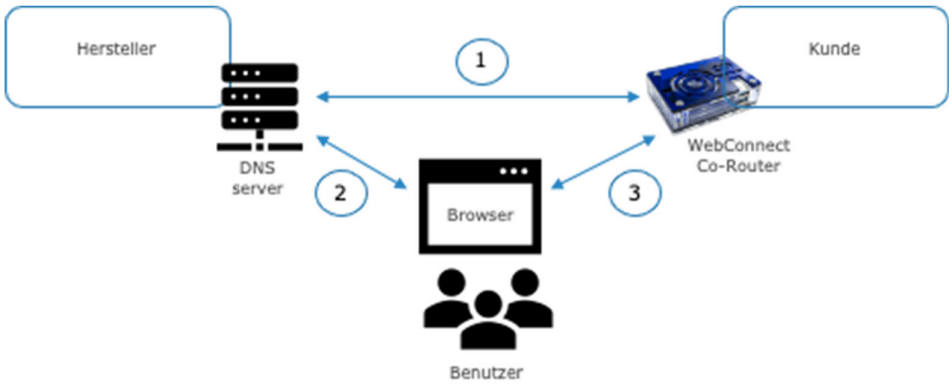
Auftraggeber:	WebConnect World S.L., ES-Madrid
Produkt:	WebConnect Co-Router
Hersteller:	WebConnect World S.L., ES-Madrid
Software-Version:	0.1.19
Webseite:	https://webconnect.pro/de/
Dokumentation:	https://help.webconnector.pro/
Datenschutzrecht:	Datenschutzgrundverordnung (DSGVO).

Bernd Wilkens
Diplom-Informatiker (FH)
Zertifizierter Externer Datenschutzbeauftragter
+41 (0)61 551 04 30
bernd.wilkens@bw-fcc.com

bw-fcc GmbH
Zehntenfreistrasse 11
CH-4103 Bottmingen
Registergericht: Basel-Landschaft (Schweiz)
VAT: CHE-116.224.474

Wie funktioniert der WebConnect Co-Router?

Der WebConnect Co-Router wird kundenseitig üblicherweise hinter der Firewall an einem Switch oder Router installiert. Die Erstkonfiguration ist einfach und weitgehend automatisiert. Danach werden Benutzer erfasst und den Devices (Workstations, Server, etc.) zugewiesen, auf die sie Zugriff haben sollen.



(1) Software-Updates erfolgen automatisch (initiiert vom WebConnect Co-Router)
(2) die Verbindung zum WebConnect Co-Router erfolgt via HTTPS, die zugehörige URL wird durch einen DNS-Nameserver des Herstellers aufgelöst
(3) die Kommunikation (der Session Stream) findet dann ausschliesslich zwischen dem Browser und dem WebConnect Co-Router statt.

Welche datenschutzrechtlich relevanten Daten werden erhoben?

- Pflichtdaten
  - IP-Adresse des WebConnect Co-Routers
    wird nur in einem DNS-Server beim Hersteller gespeichert, um den WebConnect Co-Router direkt via Internet erreichbar zu machen
  - Username / Password
- Optionale Daten
  - Name (Vor-, Nachname)
  - eMail-Adresse
  - Organisation
  - Telefonnummer

Gilt der Betrieb von WebConnect Co-Router als Auftragsverarbeitung?

Der Hersteller speichert ausser der externen IP-Adresse des Kunden keinerlei Daten von Nutzern des WebConnect Co-Routers. Alle anderen Daten werden ausschliesslich auf dem WebConnect Co-Router gespeichert. Die IP-Adresse dient dabei lediglich zur Erstellung eines Eintrags in einem DNS-Nameserver, um den WebConnect Co-Router direkt über das Internet erreichbar zu machen. Diese Nutzung begründet nach Auffassung des Autors keine Auftragsverarbeitung im Normalbetrieb.

Eine Ausnahme bildet der Remote-Support, der vom Kunden ein- oder ausgeschaltet werden kann. Nimmt ein Kunde diese Dienstleistung des Herstellers in Anspruch, hat der Hersteller

Bernd Wilkens
Diplom-Informatiker (FH)
Zertifizierter Externer Datenschutzbeauftragter
+41 (0)61 551 04 30
bernd.wilkens@bw-fcc.com

bw-fcc GmbH
Zehntenfreistrasse 11
CH-4103 Bottmingen
Registergericht: Basel-Landschaft (Schweiz)
VAT: CHE-116.224.474

Zugriff auf die Benutzerdaten – dies begründet nach Art. 28 Abs. 3 DSGVO eine Auftragsverarbeitung.
Zwar würden sich die Benutzerdaten auch frei von einem Personenbezug erfassen lassen (z.B. Hase26 statt dem Klarnamen und ohne sonstige Angaben wie eMail-Adresse und Telefonnummer etc.), doch wird das in der Praxis kaum Anwendung finden da sonst innerbetrieblich zusätzlich eine Zuordnungstabelle geführt werden müsste, um Standardprozesse wie z.B. die Löschung eines Benutzers zu ermöglichen.
Nach Angaben des Herstellers werden mit einem der nächsten Software-Releases die Nutzerdaten analog zum Verfahren der Passwortverschlüsselung verschlüsselt (der Schlüssel liegt dabei ausschliesslich beim Kunden, d.h. der Hersteller hat keinen Zugriff auf die Nutzerdaten). Damit wird auch die Notwendigkeit eines Auftragsverarbeitungsvertrags entfallen.

Fazit

Der WebConnect Co-Router lässt sich von Kunden mit minimalen datenschutztechnischen Massnahmen betreiben. Dazu zählen:

- sichere Authentifizierung: da hier externer Zugriff auf die IT-Infrastruktur gewährt wird, wird die Nutzung der Zwei-Faktor-Authentifizierung dringend empfohlen
- Aufnahme des WebConnect Co-Router in das Verarbeitungsverzeichnis
- Löschpflicht: Benutzerkonten auf dem WebConnect Co-Router, die nicht mehr benötigt werden, z.B. von Mitarbeitenden, die das Unternehmen verlassen haben, sollten gelöscht werden (das wird im Normalfall hoffentlich! schon aus Sicherheitsgründen geschehen)
- Abschluss eines Auftragsverarbeitungsvertrages, falls Remote-Support durch den Hersteller gewünscht ist (entfällt, sobald die angekündigte Verschlüsselung der Nutzerdaten implementiert ist).

Es ist erfreulich zu sehen, dass der Hersteller das Prinzip der Datenminimierung bereits in der Designphase geplant und dann auch konsequent umgesetzt hat.

30. Oktober 2022
Bernd Wilkens
Zertifizierter Externer Datenschutzbeauftragter

Bernd Wilkens
Diplom-Informatiker (FH)
Zertifizierter Externer Datenschutzbeauftragter
+41 (0)61 551 04 30
bernd.wilkens@bw-fcc.com

bw-fcc GmbH
Zehntenfreistrasse 11
CH-4103 Bottmingen
Registergericht: Basel-Landschaft (Schweiz)
VAT: CHE-116.224.474