

Leistungsbeschreibung

O₂ Business Webguard

Stand: April 2025

1. Leistungen von Telefónica Germany

Im Rahmen von O₂ Business Webguard stellt Telefónica Germany dem Kunden Funktionalitäten für Sicherheitsdienste der in Ziffer 2 beschriebenen Cloud-Software zur Verfügung. Der Anbieter der Cloud-Software ist Whalebone, s.r.o., Jezuitská 14/13, 602 00 Brno, Czech Republic ("Whalebone"). Der Kunde erlangt ein nicht ausschließliches, nicht übertragbares und nicht unterlizenzierbares Recht, O₂ Business Webguard für die Dauer des Vertragsverhältnisses mit Telefónica Germany auf der jeweils definierten Anzahl und Art von Geräten zu nutzen. Alle sonstigen Rechte in Bezug auf O₂ Business Webguard und der Cloud-Software verbleiben bei Telefónica Germany.

Der Kunde hat bei Nutzung von O₂ Business Webguard alle technischen Beschränkungen in der Cloud- und oder Client-Software einzuhalten, die Art und Umfang der Nutzung der Software vorgeben. Insbesondere ist dem Kunden untersagt,

- eine Kopie der Software anzufertigen, es sei denn, dies geschieht für Archivierungszecke;
- technische Beschränkungen in der Software auszuschalten oder zu umgehen;
- die Software zurückzuentwickeln, zu dekompileieren oder zu zerlegen, es sei denn, dies ist durch geltendes Gesetz trotz dieser Beschränkung ausdrücklich gestattet;
- die Software zu veröffentlichen oder anderen zum Zwecke des Kopierens zur Verfügung zu stellen;
- die Software oder Teile von dieser abzuändern oder abgeleitete Werke zu schaffen (außer durch geltendes Gesetz werden die vorbenannten Beschränkungen oder die Lizenzbedingungen, durch welche die Nutzung von in der Client-Software enthaltenen Open Source-Komponenten geregelt wird, vollumfänglich oder gegebenenfalls in einem bestimmten Umfang verboten);
- die Software zu vermieten, zu verleasen oder zu verleihen, oder sonst Dritten zur Verfügung stellen;
- dritten eine Unterlizenz an der Software einzuräumen.

2. Funktionalität

Mit O₂ Business Webguard erhält der Kunde Zugang zu einer Cloud-Software mit den nachfolgend aufgeführten Funktionalitäten zur Abwehr von Cyberangriffen, innerhalb der O₂ Mobilfunknetzes, die z.B. vor Phishing, Malware und Betrugsseiten warnt. Eine Installation auf Endgeräten ist nicht nötig, da es sich um einen netzwerkbasierten Schutz, ein sog. Sicherheitsdienst als Cloud-Software, handelt. O₂ Business Webguard hilft, einen höheren Grad an Sicherheit bei Datenverbindungen im O₂ Mobilfunknetz zu erreichen. Eine in jedem Fall zutreffende Erkennung von Sicherheitsgefahren kann nach dem derzeitigen Stand der Technik aber nicht gewährleistet werden. Wichtig ist, dass die Sicherheitsfunktionen von O₂ Business Webguard nicht funktionieren können, wenn der Endnutzer die IP-Adresse einer Website anstelle der Domain angibt. Die Funktionalitäten von O₂ Business Webguard können folgende Funktionalitäten umfassen:

- Sicherheitsfilter und Sperrseite

Die Funktion Sicherheitsfilter und Sperrseite auf Basis eines DNS Sicherheits-Routings trägt dazu bei, dass bösartige Domains, die der Verbreitung von Malware-, Phishing-, und Spamsite-Angriffen bzw. sonstigen Gefahren dienen, möglichst erkannt und blockiert werden. Diese Funktion wird automatisch bei der Aktivierung des Dienstes eingeschaltet. Beim versehentlichen Klicken auf verdächtige Links wird eine Warnseite angezeigt. Es prüft in Echtzeit alle aufgerufenen Internetadressen anhand einer Datenbank mit aktuell gefährlichen Seiten. Dafür werden Verkehrsdaten genutzt.

- Webfilterfunktionen

Die Webfilterfunktionen bieten einen Mechanismus zur Kategorisierung und Filterung von Domains. Mit diesen Filtern können Domains wie „Inhalte ab 18“ (insb. pornografische Inhalte), „Applikationen“ (wie soziale Netzwerke, Spiele, Videostreaming) oder „Werbung“ (einschließlich solcher, die Nutzeraktivitäten verfolgen) blockiert werden. Diese

Funktion ist standardmäßig nicht aktiviert. Der Administrator des Kunden kann in dem O₂ Business Webguard-Portal einstellen, welcher Mitarbeiter für welche Kategorien von Webseiten gesperrt wird. Die Kategorisierung von Webseiten kann Fehler enthalten, eine in jedem Fall zutreffende Erkennung der Kategorie kann nach dem derzeitigen Stand der Technik nicht gewährleistet werden.

- Zulassungsliste und Sperrliste

In der Zulassungsliste können vom Administrator des Kunden definierte Domains freigegeben werden und Sperrung durch O₂ Business Webguard ausgeschaltet werden. Unerwünschte Domains können vom Administrator des Kunden in der Sperrliste gesperrt werden.

- Identitätsschutz

Die Identitätsschutzfunktion trägt zum Schutz der Privatsphäre bei. Wenn der Kunden bzw. der Endnutzer diese Funktion einschalten, werden kontinuierlich Datenschutzverletzungen überwacht, die gestohlene Telefonnummern betreffen. Sobald eine Sicherheitslücke erkannt wird, erfolgt eine Benachrichtigung per E-Mail an den Administrator des Kunden.

- Das O₂ Business Webguard-Portal

Der Administrator des Kunden erhält Zugriff auf das O₂ Business Webguard-Portal mit Zugangsdaten und Passwort. Nur der Administrator des Kunden hat die Übersicht der Endnutzer auf dem O₂ Business Webguard-Portal und kann Änderungen der oben genannten Funktionen vornehmen. Andere Mitarbeiter haben keinen Zugriff auf das Portal.

Das O₂ Business Webguard-Portal liefert eine Übersicht der erkannten Sicherheitsvorfälle der letzten 60 Tage, Statistiken sowie Einstellungen zu den o.g. Funktionen.

Der Administrator des Kunden kann regelmäßige Sicherheitsberichte bestellen oder abbestellen und sog. Alerts als Alarmhinweise für Sicherheitsvorfälle einstellen.

3. Nutzungsvoraussetzungen und -einschränkungen

1. O₂ Business Webguard steht für die meisten gängigen Endgeräte wie Smartphones, Tablets, Laptops, Desktop-PC, Spielkonsolen und Smart-Home Geräte zur Verfügung, die sich im Mobilfunknetz von O₂ befinden.
2. Die ordnungsgemäße und vollumfängliche Erbringung der vertraglich vereinbarten Leistungen für den Service O₂ Business Webguard setzt die Bereitstellung und Verarbeitung bestimmter (personenbezogener) Daten der Endnutzer voraus. Hierzu zählen insbesondere die geschäftliche Telefonnummer sowie Verkehrsdaten, welche zur Vertragserfüllung und Inanspruchnahme der Dienstleistung an den externen Dienstleister Whalebone übermittelt werden. Sofern der Umfang der bereitgestellten oder zur Verarbeitung freigegebenen Daten eingeschränkt wird, kann dies die Funktionsfähigkeit und den Leistungsumfang des angebotenen Services beeinträchtigen.
3. Die Nutzung von O₂ Business Webguard setzt eine Verbindung zum Internet voraus. Die Bereitstellung und Überlassung des für die Nutzung von O₂ Business Webguard erforderlichen Internetzugangs, die Verbindungen zum Internet sowie erforderliche Equipment und/oder Mobilfunkendgerät sind nicht Bestandteil der O₂ Business Webguard Leistungen.
4. O₂ Business Webguard steht nur für die Endgeräte und Tarife zur Verfügung, für die O₂ Business Webguard erworben wurde.
5. Die ordnungsgemäße Funktionalität von O₂ Business Webguard setzt voraus, dass die DNS-Zugangspunkte der Cloud-Software ordnungsgemäß auf Endgeräten konfiguriert ist und alle zur Verfügung gestellten Software-Updates unverzüglich und ordnungsgemäß auf den Endgeräten installiert sind.
6. Falsch-positive Erkennung und Kategorisierung von Inhalten wird nicht als Inzidenz betrachtet. Der Administrator des Kunden kann den Zugriff auf falsch-positive Domains sofort über die Zulassungsliste im O₂ Business Webguard-Portal erlauben.
7. Aus rechtlichen Gründen gesperrte Domains können nicht auf die Zulassungsliste gesetzt werden.
8. Die Sicherheitsfunktionen von O₂ Business Webguard funktionieren nicht, wenn:
 - der Endnutzer die IP-Adresse einer Website anstelle der Domain angibt;
 - der DNS-Resolver im Endgerät geändert wird;

- der Endnutzer einen VPN-Dienst einsetzt;
- der Endnutzer Proxy-Dienste einsetzt;
- der Endnutzer nicht mit dem Netz von O₂ Telefónica verbunden ist (z. B. über einen anderen Anbieter oder WiFi/WLAN);
- der Endnutzer sich in bestimmten Roaming-Situationen befindet.