O2 Business

O2 Business Protect

FAQs

Powered by

McAfee

EINE Telefónica BUSINESS-LÖSUNG

Einfach mehr unternehmen.

O_2 Business Protect FAQs für Kunden & Interessenten

O_2 Business Protect powered by McAfee schützt Ihre PCs, Macs, Laptops, Tablets und Smartphones - vor Viren, Spam, Malware und Identitätsdiebstahl. Einmal installiert, können Ihre Mitarbeiter die Geräte orten, sperren, sichern oder die Daten löschen. Ganz einfach über eine Online-Plattform. Das Paket beinhaltet auch McAfee TrueKey zum sicheren Speichern all Ihrer Benutzernamen und Passwörter.

Übersicht

1. Was ist Cyber Security?

Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. (Quelle: Bundesamt für Sicherheit in der Informationstechnik)

2. Wer ist von Cyber Kriminalität betroffen?

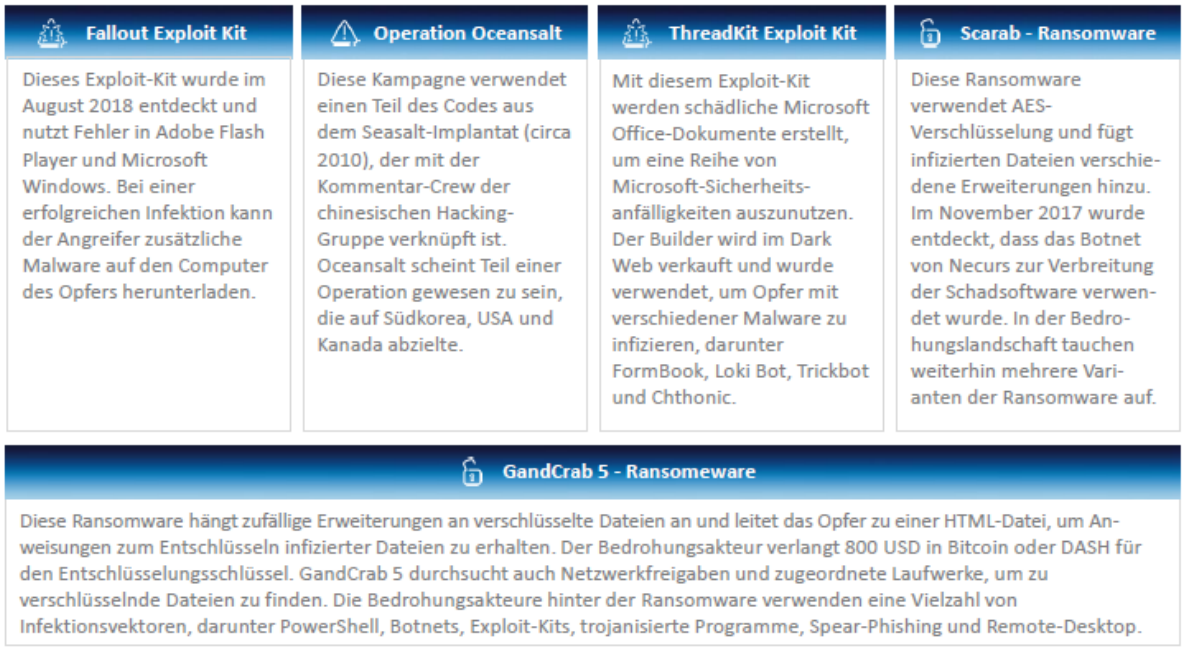
Cyber-Security betrifft jeden. Vom privaten Nutzer über Selbstständigen, kleine Unternehmen bis hin zu großen Konzernen – egal in welchen Branchen. Niemand darf sich zu sicher fühlen.

- Allein 68% der deutschen Unternehmen waren Opfer von Sabotage, Datendiebstahl oder Spionage in den vergangenen zwei Jahren, vor allem kleine und mittlere Unternehmen. (Quelle: Bitkom Studienbericht 2018: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie).
- Cyberkriminalität in Deutschland hat im 2017 im Vergleich zu 2016 um 4% zugenommen (86.000 Fälle). Durch Computerbetrug ist ein Schaden von 71,4 Millionen Euro entstanden. (Quelle: Bundesamt für Sicherheit in der Informationstechnik).

3. Was sind typische Online Bedrohungen?

Einige Beispiele von typische Online Bedrohungen sind Ransomware, Kryptominer, Banking-Trojaner, Phishing-Angriffe, Spam-Versand, Spyware, WLAN-Attacken, Infizierte Websites und mobile Apps, Adware.

Die derzeit größten Cyber-Sicherheitsbedrohungen wurden vom Bedrohungsforscherteam unseres Partners McAfee als die Bedrohungen mit der derzeit größten Wirkung identifiziert und analysiert. Dazu gehört unter anderem die Bedrohung der Netzwerksicherheit und der Informationssicherheit.



4. Brauche ich wirklich ein Antivirus Software für mein Handy und Tablet?

Smartphones und Tablets werden immer leistungsfähiger und sind nahezu überall im Einsatz. Man sollte daher nicht vergessen, dass auch mobile Geräte – genau wie PCs und Notebooks – durch Viren und Malware infiziert werden können.

- Es gibt 700.000 neue Viren pro Tag und 35 gezielte Malware-Angriffe pro Woche (Quelle: McAfee Labs Threats Report Sept 2018).
- Jeder fünfte Nutzer in Deutschland musste schon einmal den Verlust eines Tablets, Notebooks oder Smartphones beklagen. Obwohl 63% ihr Gerät nie mehr wiedersehen, verwenden nur 32% eine Anti-Diebstahl-Software. 67,9% verzichten auf den digitalen Schutz (Quelle: Umfrage "Lost and Found" des IT-Security-Herstellers Eset).

5. Mit welchen Tarifen/Produkte kann ich O_2 Business Protect buchen/kombinieren?

Mit den o2 Business Mobilfunk Tarifen: o2 Free Business und o2 Unite sowie mit unserem o2 Business Spot LTE Router und unserem Rundum-Paket für Mobilfunk, Internet und Festnetztelefonie o2 Business Fusion.

6. Kann ich das Produkt Standalone kaufen?

Nein, O_2 Business Protect kann nur zusammen mit unseren O_2 Business Mobilfunk Tarifen gebucht werden.

7. Ich bin O_2 Business Kunde und habe bereits einige O_2 Business Mobilfunktarife aber noch kein O_2 Business Protect. Wie kann ich in diesem Fall das Produkt buchen?

Zu bestehenden Tarifen kann O_2 Business Protect als Option dazu gebucht werden sofern die restliche Vertragslaufzeit 12 Monate noch nicht unterschritten hat.

8. Welche Kosten entstehen mir durch die Nutzung?

O_2 Business Protect kostet nur 2,50€ im Monat pro Lizenz. Jede Lizenz beinhaltet den Schutz von bis zu 5 Geräten in beliebiger Kombination aus PC, Mac, Tablet und Smartphone. Das Paket beinhaltet auch 5 McAfee True Key Lizenzen zum sicheren Speichern all Ihrer Benutzernamen und Passwörter. Für Internetverbindungen können weitere Kosten gemäß Ihrem Tarif anfallen.

9. Für wen eignet sich O_2 Business Protect powered by McAfee?

Es eignet sich für vor allem für Unternehmen mit bis zu 50 Mitarbeitern aller Branchen. Besonders interessant ist das Produkt für Unternehmen ohne eigene IT-Sicherheitsabteilung, da sie den Anwendern eine professionelle Sicherheitslösung aus einer Hand bietet.

10. Verlangsamt Sicherheits-Software nicht den Computer?

Nein, das Hochleistungs-Scan-Modul von O_2 Business Protect schützt Ihren PC ohne Leistungseinbußen. O_2 Business Protect wurde speziell als ressourcenschonendes Produkt entwickelt, das Ihren PC nicht beeinträchtigt. Es hat keine negativen Auswirkungen auf Ihr Gerät.

11. Wie erfolgt die Aktivierung der Lizenzen?

Nach dem Kauf von O_2 Business Protect erhält der Administrator/Abwickler im Unternehmen eine Begrüßungs-E-Mail. Diese enthält einen Link zur Online-Plattform “My Digital Workplace” und den Benutzernamen sowie eine Anleitung zum Erstellen eines Passworts und Einrichtung des Administrator-Kontos. Zunächst hinterlegt der Admin die E-Mail Adressen seiner Mitarbeiter womit diese wiederum eine Begrüßungsmail erhalten in welcher Sie aufgefordert werden, Ihre Geräte zu schützen. Innerhalb der McAfee Verwaltungsoberfläche können Sie so ihre (bis zu 5) Geräte per SMS oder E-Mail Download Link mit McAfee schützen

12. Ich bin noch kein O_2 Business Kunde. Kann ich O_2 Business Protect auch nutzen?

O_2 Business Protect können Sie nur mit einem Mobilfunkvertrag mit monatlicher Laufzeit von O_2 Business bestellen.

13. Was ist der TrueKey Password Manager?

True Key ist der Password Manager unseres Partners McAfee (5 Lizenzen im O_2 Business Protect bereits inkl.). True Key verwendet Ihre individuellen Merkmale, um Sie ohne Kennwörter anzumelden. Wir bieten Ihnen verschiedene Optionen, sogenannte "Komponenten", für die Anmeldung. Sie möchten nicht Ihr Gesicht verwenden? Wählen Sie einfach eine andere Komponente. Zum Verifizieren Ihrer Identität verwenden wir immer mindestens zwei Komponenten. Sie wählen die erste, und True Key überprüft, ob Sie sich auf einem vertrauenswürdigen Gerät befinden – so einfach ist das. Wenn Sie sich mehr Sicherheit wünschen, können Sie weitere Komponenten beim Anmelden hinzufügen, um Ihr Profil noch stärker zu machen. True Key speichert Ihre Kennwörter automatisch und gibt sie ein, damit Sie das nicht tun müssen. Ihre Kennwörter werden lokal auf Ihrem Gerät gespeichert und mit Ihrem Profil unter Verwendung der stärksten verfügbaren Verschlüsselung synchronisiert. Wenn Sie eine App starten oder eine Website besuchen, gibt True Key automatisch Ihre Kennwörter ein und meldet Sie an. True Key synchronisiert auf sichere Weise Ihre Passwörter auf allen Ihren Geräten, damit Sie sie von überall aus abrufen können.

14. Warum brauche ich einen Passwortmanager?

Passwörter zu erraten ist oftmals für Hacker sehr einfach. Meistens liegt u.a. der größte Fehler darin das gleiche Password für alle Accounts zu verwenden. Das ist verständlich, da

die meisten Menschen heute über dutzende Accounts und Zugänge verfügen und sich keine langen, sicheren und einzigartigen Passwörter für jeden Account merken können.

Trotz vieler verfügbaren Tipps und Tricks für sichere Passwörter gehören erstaunlicherweise "123456" oder "passwort" immer noch zu den Kennwörtern, die am häufigsten verwendet werden (Quelle: Hasso-Plattner-Institut (HPI) „ Die Top Ten deutscher Passwörter“).

- 63 Prozent aller Datendiebstähle sind auf unsichere oder gestohlene Passwörter zurückzuführen. Mehr als eine Viertelmillion User verwendeten das Passwort „123456“, 92.000 nutzten einfach „password“. Beliebt waren auch „lastfm“ (67.000), „123456789“ (64.000) und „abc123“ (36.000) (Quelle: Data Breach Investigations Report 2018 von Verizon).

Gestohlene oder unsichere Passwörter gefährden die Unternehmensdaten. Auch komplexe Passwortrichtlinien sind manchmal nicht ausreichend, aber heutzutage sollte sich keiner komplexe Passwörter mehr merken müssen. Dafür gibt es Passwort-Manager wie z.B. True Key von McAfee in ihre O_2 Business Protect bereits inkludiert.

15. Ist der Passwortmanager TrueKey sicher genug?

Die Passwörter werden auf den Endgeräten verschlüsselt und dann in der Cloud gespeichert. Das ist der gängige Standard bei allen Passwortmanagern. Ihre Kennwörter und die Elemente in Ihrer Börse werden auf Ihrem Gerät mit AES-256 verschlüsselt, dem stärksten Verschlüsselungsalgorithmus überhaupt. Es werden keine lesbaren Kennwörter oder in Ihrer Börse gespeicherten Daten über das Internet gesendet - nicht einmal an unsere Server.

16. Welche Nutzungsvoraussetzungen gibt es?

Unterstützte Betriebssysteme:

- Android 4.1 oder höher, Android One
- Microsoft Windows 10, 8.1, 8 und 7 (32- und 64-Bit)
- Mac OS X 10.10 oder höher
- Google Android 4.1 oder höher für Smartphones und Tablets
- Apple iOS 10 oder höher

Unterstützte Browser:

- Internet Explorer 10.0 oder höher
- Firefox 30 oder höher
- Safari 6.1 oder höher
- Google Chrome

Internetverbindung:

Schnelle Internetverbindung empfohlen

Unterstützte E-Mail-Programme:

- POP3 – Windows Mail, Outlook, Netscape, IncrediMail, Thunderbird, Becky, Shuriken
- MAPI – Outlook
- Web – MSN/Hotmail oder E-Mail-Konto mit IMAP-/POP3-Zugriff

Hardware für Windows-PCs:

- 2 GB RAM für Windows 7 oder höher
- 500 MB freier Festplattenspeicher
- 1-GHz-Prozessor

Für die Anti-Spam-Symbolleiste erforderlich:

- Microsoft Outlook 2007, 2013, 2016
- Thunderbird 38.0 oder höher
- McAfee Anti-Spam unterstützt auch andere POP3-E-Mail-Clients (ohne SSL) und Web-Konten

17. Wie erfolgt die Abrechnung?

Die Abrechnung Ihres Paketpreises erfolgt bei Vertragskunden bequem über die Telefonrechnung.

18. Habe ich im Falle, dass mir trotz Schutzsoftware ein Schaden entstanden ist einen Ersatzanspruch?

Der Schadensersatzanspruch wird über die McAfee EULA geregelt, die der Kunde bei der Installation akzeptiert.

19. Was ist O_2 Business Spot Protect?

Der O_2 Business Spot Protect besteht aus eine O_2 Business Protect Lizenz, die flexibel auf bis zu 5 Geräten (Android-Smartphone und -Tablet ab Betriebssystem 2.2, iOS-Smartphone und -Tablet sowie PC oder Mac) eingesetzt werden kann, unser O_2 Business Spot (Askkey) LTE Router und das O_2 Business Data mit 50 GB LTE Datenvolumen. Alles für nur 20 Euro pro

Monat (und einmalig 50 Euro). Mehr Informationen unter
www.o2business.de/businessspot

***Wichtige Information zur Lizenz**: Eine Lizenz für 1 Benutzer deckt 5 Geräte ab, z. B. Ihr Smartphone, Ihr iPad und Ihren Laptop. Sie sollten aber nicht eine Lizenz für mehrere Benutzer verwenden, da alle die gleichen Anmeldedaten verwenden und auf Ihre Kontakte, Fotos und Textnachrichten zugreifen können.*

EINE Telefónica BUSINESS-LÖSUNG

O2 Business

Telefónica Germany GmbH & Co. OHG · Kundenbetreuung · D 90345 Nürnberg
o2business.de/protect · E business-interessenten@telefonica.com · T 0800 33 99 93 3

Stand: 02/2019