Aagon
CLIENT MANAGEMENT PLATFORM

Stay safe!
Der Microsoft Defender als kostengünstige Antivirensoftware

Lohnt sich der Umstieg
für Unternehmen?

www.aagon.com

1. Spyware, Trojaner, Viren & Co.: großes Gefahrenpotenzial für Unternehmen

Wenn Unternehmen Digitalisierungsprojekte angehen, stellen sich obligatorisch auch Fragen nach der IT-Sicherheit. Zur großen Angriffsfläche wird dabei die zunehmende Vernetzung nach innen und nach außen durch Digitalisierung, Homeoffice und Remote Work. Sofern der Schutz der IT-Infrastruktur dann vernachlässigt wird, eröffnen sich für potenzielle Angreifer ungeahnte Möglichkeiten – das Schadpotenzial für Unternehmen ist unermesslich. Prominente Beispiele aus der Vergangenheit zeigen, wie hoch die Verluste durch Cyberangriffe sein können:

Ende Juli 2021 haben Erpresser die Aerzener Maschinenfabrik attackiert.

Dadurch entstanden dem Unternehmen mit mehr als 1.100 Mitarbeitern Umsatzeinbußen in Höhe von 30 Mio. €. Die Wiederherstellung der IT dauerte in der Folge mehrere Monate; die Produktion stand acht Wochen lang still. Mangels Erfolgsaussichten wurde die Entwicklung eingestellt.

→ **Mehr zum Fall erfahren**

Ein besonders prominenter Fall war 2020 der Angriff auf den Bundeswehr-Fuhrparkservice mit der Schadsoftware Emotet.

Der Service bietet Fahrdienste für Bundestag, Bundeswehr und das Verteidigungsministerium. Emotet war dabei nur die Vorhut; in kurzer Folge luden die Angreifer einen weiteren Trojaner sowie eine Schadsoftware in das IT-Netz mit dem Ziel, den Fahrdienst zu erpressen und im schlimmsten Fall personenbezogene Daten aus Politkreisen abzuziehen.

→ **Mehr zum Vorfall erfahren**

Im Sommer 2021 wurde ein großer Verpackungsetikettenhersteller aus Grünstadt Opfer eines Hackerangriffs.

Ziel dabei war die digitale Datenbank des Unternehmens. Bei der Attacke entstand ein Schaden von ca. 1 Mio. €; außerdem war die Produktion vorübergehend nur eingeschränkt möglich.

→ **Mehr erfahren**

Es gibt also genügend Beispiele, die zeigen, warum sich Unternehmen dringend mit dem Schutz und der Sicherheit ihrer IT-Infrastruktur auseinandersetzen sollten, gerade in Zeiten zunehmender Digitalisierung. Geht es dann um die Auswahl einer bestimmten Antivirensoftware, landen Entscheider schnell bei bekannten Marken wie Kaspersky, Norton, Avira oder Avast. Dabei gibt es mit dem Microsoft Defender eine hochkarätige Alternative, die zudem standardmäßig und kostenfrei in Windows enthalten ist.

Gerade weil das Programm kostenfrei ist, eilt ihm der Ruf voraus, keinen sicheren Schutz für die IT-Landschaft zu bieten. Dabei handelt es sich jedoch um ein klares Vorurteil; der Microsoft Defender wurde in den vergangenen Jahren zu einer echten Allzweckwaffe gegen Hackerangriffe weiterentwickelt. Deshalb lohnt es sich, die Vorzüge der Software genauer in den Blick zu nehmen und ihre Eignung für Unternehmen zu überprüfen.

Nicht zu selten sind es veraltete Sicherheitsarchitekturen, die schuld sind am Einbruch von Schadsoftware.

Laut Avast gaben 60 % der Opfer von Sicherheitsverletzungen an, dass sie aufgrund einer bekannten, nicht gepatchten Sicherheitslücke verletzt wurden, für die ein Patch verfügbar war. 37 % der Befragten meinten sogar, dass sie nicht einmal nach Schwachstellen suchen.

→ Quelle: Avast

Die Umfrage „Allianz Risk Barometer 2022" ergab Überraschendes:

Noch mehr als vor Corona fürchten die 2650 Unternehmenschefs, Risikomanager und Versicherungsmakler aus 89 Ländern Angriffe auf IT-Systeme. Fast jeder zweite äußerte diese Sorge.

→ Zu den Umfrageergebnissen

2. Totgesagte leben länger: Warum der Microsoft Defender wieder in der ersten Liga spielt

Heutzutage sind Unternehmen jeglicher Größenordnungen Ziel von Angriffen aus dem Cyberspace. Das Thema IT-Sicherheit spielt deshalb unabhängig von der Unternehmensgröße eine immer wichtigere Rolle. Dazu bedarf es keine teure Zusatzsoftware eines Spezialanbieters. Ein hohes Sicherheitsniveau lässt sich bereits mit den Bordmitteln des Microsoft Defenders erreichen.

Nicht Großunternehmen, sondern gerade Mittelständler sind besonders anfällig für Attacken aus dem Cyberspace.

Laut einer Studie hatte knapp die Hälfte der Befragten KMU 2020 keine Mitarbeiter, die sich dezidiert um Cyber-Sicherheit kümmerten.

→ Quelle: Hiscox Cyber Readiness Report 2020

Schlimm genug, wenn infolge eines Cyberangriffs bei Unternehmen ein Millionenschaden entsteht.

Aber auch vermeintlich „kleine" Fälle verursachen spürbaren Schaden: 2020 mussten betroffene Firmen in Deutschland im Schnitt 72.000 € für die Behebung einer Cyber-Attacke ausgeben.

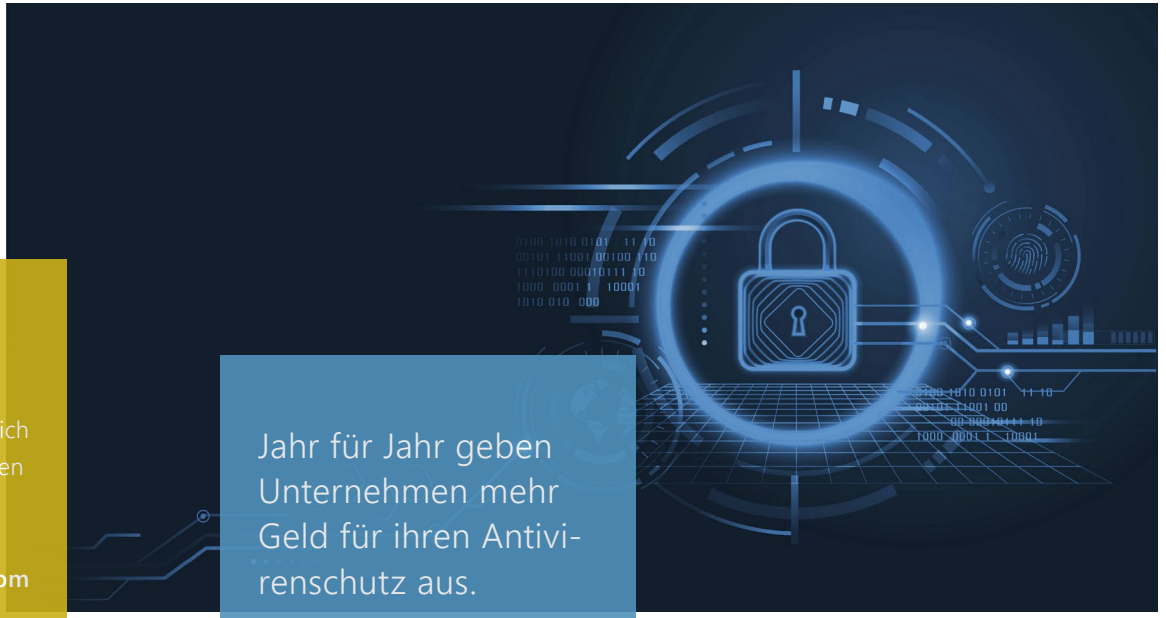
→ Quelle: Hiscox Cyber Readiness Report 2020

Der Microsoft Defender – ehemals Windows Defender – gehört schon seit vielen Jahren zum Lieferumfang von Microsoft Windows. Lange Zeit fristete die Sicherheitssoftware eher ein Nischen dasein und wurde von Anwendern meist mit Lösungen namhafter Anbieter wie Norton, Kaspersky und Co. ersetzt. In der Zwischenzeit hat sich die Microsoft-Lösung jedoch in der ersten Reihe etablierter Antivirenprogramme zurückgemeldet.

Beim Schutz der unternehmenseigenen IT-Struktur geht es immer um zwei Fragen: Wie kann ich Angriffe entdecken? Wie kann ich das Entdeckte wieder entfernen?

Der Microsoft Defender liefert für beide Fragen adäquate Antworten. Er dient der Frühzeiterkennung von Bedrohungen wie Viren, Schadsoftware und Spyware, die sich in E-Mails und Apps verstecken oder z. B. über Cloud-Anwendungen eindringen. Dabei setzt er auf einen Instrumentenmix, etwa einen Überblick über Funde, Bedrohungen und Updates, automatisierte Aktualisierungen der Bedrohungsdefinitionen oder einen überwachten Ordnerzugriff.

3. Was der Microsoft Defender alles kann



Deutsche Unternehmen: Für den digitalen Notfall gut gerüstet?

Nach einer Umfrage von bitkom besitzen lediglich 51 % der befragten Firmen aus diversen Branchen ein Notfallkonzept, 44 % hingegen nicht.

→ **Quelle: Bitkom**

Jahr für Jahr geben Unternehmen mehr Geld für ihren Antivirenschutz aus.

Allein in Deutschland ist dieser Wert zwischen 2019 und 2020 von 1,5 Mio. € auf 2 Mio. € im Firmendurchschnitt gewachsen. Die Kostenlosigkeit des Microsoft Defenders wird damit zu einem zentralen Pluspunkt.

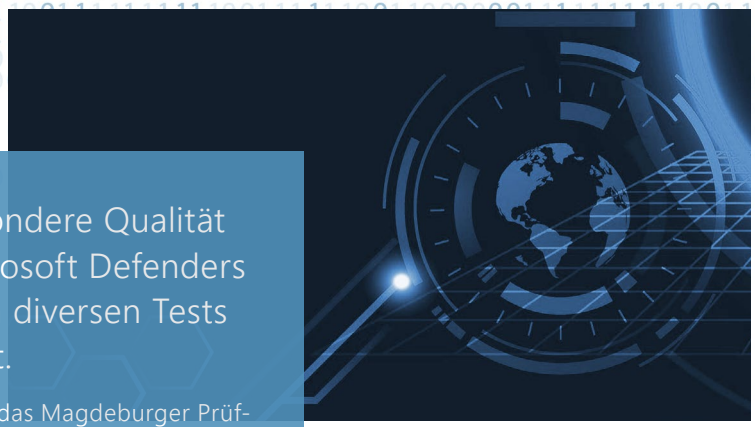
→ **Quelle: Hiscox Cyber Readiness Report 2020**

Der Microsoft Defender bringt einige Funktionen mit sich, von denen Unternehmen besonders profitieren:

Mit dem Microsoft Defender bleibt Entscheidern eine aufwendige Recherche nach Antivirensoftware sowie ein umfangreicher Auswahlprozess erspart. Das Schutzprogramm ist beispielsweise unter Windows 10 standardmäßig vorinstalliert und somit vom ersten Tag an verfügbar. Ein wesentlicher Pluspunkt ist die kostenfreie Verfügbarkeit des Microsoft Defenders. Grundsätzlich wird er mit einem großen Funktionsumfang ausgeliefert, der sich allenfalls in Abhängigkeit von Vertrag und Lizenzierung unterscheidet.

Schon mit dem Start des Clients beginnt die Schutzfunktion der Microsoft-Software.

Die Funktion „SecureBoot" erkennt Schadsoftware bereits beim Hochfahren und blockiert diese gegebenenfalls. Sie wird schon vor dem Laden des Windows-Betriebssystems aktiv und sichert den PC dadurch frühestmöglich. Andere Antivirenlösungen werden erst in der Windowsoberfläche geladen – möglicherweise zu spät, um einen Angriff zu erkennen.



Die besondere Qualität des Microsoft Defenders wurde in diversen Tests bestätigt.

So hat z. B. das Magdeburger Prüfinstitut AV-Test die Software eingehend untersucht. Dabei hat das Antivirenschutzprogramm 2021 wie im Vorjahr Bestnoten erreicht und eine Zertifizierung als „Top Product" erhalten. Im Test konnte der Microsoft Defender 100 % der Malware aus den vorausgegangenen vier Wochen erkennen. Alles in allem hat die Microsoftlösung mit seinem Funktionsumfang mittlerweile das Niveau der klassischen Spezialanbieter von Kaspersky über F-Secure, McAfee, Norton LifeLock bis zu Trend Micro erreicht.

→ Zu den Testergebnissen

Der Microsoft Defender erspart Anwendern eine mühselige händische Suche nach Schadsoftware. Vielmehr durchforstet die Software eigenständig Dateiverzeichnisse nach bösartigem Code und Prozessen, die das System befallen und möglicherweise die Leistung vermindern. Über die Einstellungen können solche Suchen automatisiert in bestimmten Zeitabständen programmiert werden. Die Leistungsfähigkeit des Rechners im laufenden Betrieb wird dadurch nicht beeinträchtigt.

Durch einen kontrollierten Ordnerzugriff werden Änderungen von nicht autorisierten Anwendungen an Dateien in speziell dafür vorgesehenen Ordnern blockiert. So kann einem Datenverlust durch Ransomware vorgebeugt werden. Dafür ist allerdings der Zugriff auf die Windows-Berechtigungsverwaltung erforderlich; externe Antivirensoftware bleibt hier außen vor.

Unternehmen mit besonders sicherheitssensibler Infrastruktur können die Funktionen des Microsoft Defenders mittels Update auf Defender ATP (Advanced Thread Protection) erweitern. Mit seiner „Always-on-Methode" lassen sich Bedrohungen schneller als auf Scan-Basis erkennen. Geräte werden außerdem automatisch aus dem Netzwerk entfernt, wenn eine Bedrohung erkannt wird. Nicht zuletzt aktualisiert ATP die Definition von Malware-Signaturen, indem er cloudbasierte Daten von allen anderen Endpunkten, die den Service nutzen, bezieht.

Auch beim Surfen im Netz sorgt das Antivirenprogramm für einen guten Schutz: Ein Bildschirmfilter blockiert bösartigen Code aus dem World Wide Web. Die meisten Browser benötigen hierfür ein Plugin; bei der Microsoft-Variante Edge läuft der Filter hingegen automatisch. Zusätzlich verhindert eine integrierte Firewall die Interaktion mit eingehenden Daten.

Nicht zuletzt schützt der Microsoft Defender sich auch selbst vor fremden Eingriffen. Ein Manipulationsschutz (Tamper Protection) verhindert, dass schädliche Apps wichtige Antivirus-Einstellungen des Defenders ändern. Er kann nur manuell am Client über die Oberfläche deaktiviert werden.

4. Was der Microsoft Defender nicht kann

So unbestritten die vielen Vorteile des Microsoft Defenders sind, so unhandlich ist leider dessen Steuerung in größeren IT-Strukturen, wie sie in modernen Unternehmen üblich sind. Die Anwenderoberfläche glänzt nicht mit Nutzerfreundlichkeit. Eine übergeordnete Management-Console erschwert die Bedienung zusätzlich; die von Microsoft vorgesehenen Lösungen Intune oder Endpoint Configuration Manager haben sich in der Praxis nicht durchsetzen können. Einstellungen können zudem nur umständlich über die Group Policy Objects (GPO) verwaltet werden oder müssen an jedem Client einzeln gesetzt werden. Nicht zuletzt fehlt eine gesammelte Übersicht bzw. Reportings über aktuelle Ereignisse, da die Daten dezentral auf den einzelnen Clients verfügbar sind.

Vorteile

- Kostenfreiheit
- standardmäßig in Windows vorinstalliert
- SecureBoot: schon vor Laden des Betriebssystems aktiv
- eigenständige Suche in Dateiverzeichnissen
- regelmäßige Suchen dank Automatisierung
- kontrollierter Ordnerzugriff
- Quarantänebereich
- Defender ATP: erweiterte Funktionen
- integrierte Firewall
- Bildschirmfilter für gängige Webbrowser
- Manipulationsschutz gegen fremde Eingriffe

Nachteile

- geringe Nutzerfreundlichkeit
- Einstellungen müssen an jedem Client angepasst werden
- keine zentrale Übersicht über Ereignisse einer kompletten IT-Struktur
- keine Reportings für eine gesamte IT-Landschaft

Insbesondere in der mangelnden zentralen Verwaltung und Steuerung unterscheidet sich der Microsoft Defender nicht von anderen Antiviren-Programmen. Im Gegensatz zu diesen gibt es für ihn jedoch am Markt eine Softwarelösung, die eine effiziente und einheitliche Verwaltung der Antivirensoftware in nur einer Oberfläche auf allen firmeneigenen Clients und Servern ermöglicht. Dadurch erhalten Unternehmen und Administratoren einen weiteren Mehrwert.

ACMP Defender Management

ACMP Defender Management ermöglicht es Administratoren, den Microsoft Defender Antivirus in nur einer Oberfläche auf allen Clients und Servern eines Unternehmens zu verwalten. Die Softwarelösung schafft die Grundlage für einen umfassenden, vollintegrierten Antivirenschutz der Unternehmens-IT und reduziert dabei Aufwand und Kosten.

→ Jetzt ACMP Defender Management kennenlernen

5. Fazit

Mit dem Microsoft Defender erhalten Unternehmen kostenlos eine hervorragende Software für den Antivirenschutz. Die AV-Lösung bietet jede Menge zielführende Funktionen und für Unternehmen jeder Größenordnung ein Höchstmaß an Sicherheit. Teure Zusatzlösungen werden dadurch überflüssig. Mit einer ergänzenden zentralen Steuerungsplattform für den Microsoft Defender gelingt es zudem, die Verwaltung der Antivirensoftware unternehmensweit zu vereinheitlichen und zu vereinfachen. So lassen sich Arbeitsplatzrechner und Server durch Administratoren zentral schützen.

Aagon GmbH
Lange Wende 33
59494 Soest
Telefon: +49 2921 789 200
E-Mail: info@aagon.com
www.aagon.com

Stand 4/2022

Aagon
CLIENT MANAGEMENT PLATFORM