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:

Cyberangriffe auf deutsche Seehäfen

Seit Beginn des russischen Angriffskriegs haben Cyberangriffe auf deutsche Seehäfen stark zugenommen, insbesondere auf den Hamburger Hafen, wo sich die Angriffe mehr als verhundertfacht haben. Auch Bremerhaven und Wilhelmshaven sind betroffen. Die Hamburger Hafenverwaltung (HPA) verweist auf eine erfolgreiche Abwehrstrategie und internationale Zusammenarbeit. Während viele Angriffe automatisiert abgewehrt werden, konnten größere Angriffe mit Hilfe des BSI rechtzeitig gestoppt werden. Die Herkunft bleibt oft unklar, doch destruktive politische Entwicklungen gelten als mögliche Ursache. Laut Bundesinnenministerium nimmt die Cyberkriminalität insgesamt zu.

→ **Mehr zum Fall erfahren**

Cyberattacke auf die Deutsche Flugsicherung (DFS)

Im September 2024 wurde die Deutsche Flugsicherung (DFS) Ziel eines Cyberangriffs, der die administrative IT-Infrastruktur betraf. Obwohl die Bürokommunikation beeinträchtigt war, blieben die Flugverkehrsoperationen unbeeinträchtigt.

→ **Mehr zum Vorfall erfahren**

Ransomware-Angriff auf Medion AG

Ende November 2024 wurde bekannt, dass die Ransomware-Gruppe BlackBasta einen Angriff auf die Medion AG verübt hatte. Dabei wurden 1,5 Terabyte an Daten kopiert, darunter vertrauliche Geschäftsdaten und Informationen zu Angestellten. Die Gruppe drohte mit der Veröffentlichung der Daten, sollte keine Lösegeldzahlung erfolgen.

→ **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 Sophos, Norton 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.

Laut dem Bundeskriminalamt (BKA) nimmt die Cyber-Kriminalität in Deutschland weiter stark zu.

Für 2024 wird ein Anstieg der polizeilich erfassten Fälle von Cybercrime um über 20% gegenüber dem Vorjahr erwartet. Besonders besorgniserregend ist die Zunahme von Erpressungsdelikten wie Ransomware-Angriffen, die um über 30% gestiegen sind. Diese Entwicklung stellt insbesondere für kleine und mittelständische Unternehmen (KMU) eine existenzielle Bedrohung dar, da sie oft nicht über ausreichende Sicherheitsmaßnahmen verfügen.

→ Weitere Informationen

Viele Mittelständler unterschätzen Cyberrisiken, trotz Sicherheitslücken und häufiger Angriffe.

Eine Forsa-Umfrage im Auftrag des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) ergab, dass 66 % der befragten mittelständischen Unternehmen das Risiko eines Cyberangriffs für ihr eigenes Unternehmen als gering einschätzen. Gleichzeitig wiesen 69 % der Unternehmen erhebliche Sicherheitslücken auf, wie seltene oder unzureichende Datensicherungen und fehlende Software-Updates. Zudem gab jedes vierte Unternehmen an, bereits Opfer eines erfolgreichen Cyberangriffs gewesen zu sein.

→ Mehr dazu

2. Warum der Microsoft Defender heute zur ersten Liga gehört

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.

Datendiebstahl und Erpressung kosten deutsche Wirtschaft 266 Milliarden Euro jährlich

Laut einer Umfrage aus dem Jahr 2024 belief sich die geschätzte Schadenssumme für die deutsche Wirtschaft aufgrund von Datendiebstahl, Industriespionage oder Sabotage auf über 266 Milliarden Euro. Davon entfielen 13,4 Milliarden Euro auf Kosten durch Erpressung mit gestohlenen oder verschlüsselten Daten.

→ **Quelle: Statista**

Viele KMU-Mitarbeiter erhalten keine Schulung zu IT-Sicherheitsrisiken

42 % der befragten Arbeitnehmer in KMU gaben an, in den vergangenen zwei Jahren keine sicherheitsspezifischen Trainings erhalten zu haben, während 29 % angaben, noch nie eine entsprechende Schulung von ihrem Arbeitgeber erhalten zu haben.

→ **Weitere Informationen**

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

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 11 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.

Deutsche Unternehmen: Für den digitalen Notfall gut gerüstet?

Nach den neuesten Studien und Umfragen, die 2025 veröffentlicht wurden, sind deutsche Unternehmen nur bedingt für digitale Notfälle, insbesondere im Bereich Cyberangriffe, vorbereitet.

Zwei Drittel (64 %) der Bevölkerung sehen Deutschland insgesamt als schlecht vorbereitet, nur 24 % halten Behörden und Verwaltung für gut vorbereitet. Zwar beziehen sich diese Zahlen auf die allgemeine Cybersicherheitslage, sie geben aber einen klaren Hinweis auf den Handlungsbedarf auch in der Wirtschaft.

→ **Quelle: Bitkom**

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

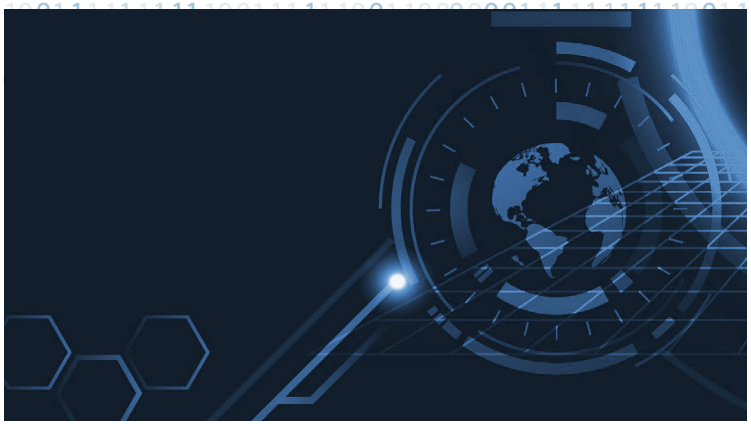
Nach Angaben des Digitalverbands Bitkom und des Marktforschungsinstituts IDC stiegen 2024 die Ausgaben für Sicherheitssoftware in Deutschland um 17,3 % auf insgesamt 5,8 Milliarden Euro. Damit macht Sicherheitssoftware, insbesondere Antivirenschutz, einen der größten Wachstumstreiber innerhalb der IT-Sicherheitsausgaben aus.

Die Gesamtausgaben für IT-Sicherheit in Deutschland erreichten 2024 rund 11,2 Milliarden Euro. Dieser Trend zeigt: Unternehmen investieren kontinuierlich steigende Beträge, um ihre Systeme gegen Cyberbedrohungen abzusichern

→ **Quelle: Bitcom**

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.

Microsoft Defender gehört weiterhin zu den besten kostenlosen Antivirenlösungen – insbesondere für Unternehmen. In den Tests überzeugte er mit starker Bedrohungserkennung, geringen Fehlalarmen und zuverlässiger Performance auch bei hoher Systemauslastung.

→ **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 vorgesehene Lösung Intune hat 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 10/2025

GetApp BEST FUNCTIONALITY & FEATURES 2024

techconsult PUR 2025 Professional User Rating ★ 5-FACH ★ ★ CHAMPION ★

READERS' CHOICE IP INSIDER AWARD 2024

Software Advice BEST CUSTOMER SUPPORT 2024

Aagon
CLIENT MANAGEMENT PLATFORM