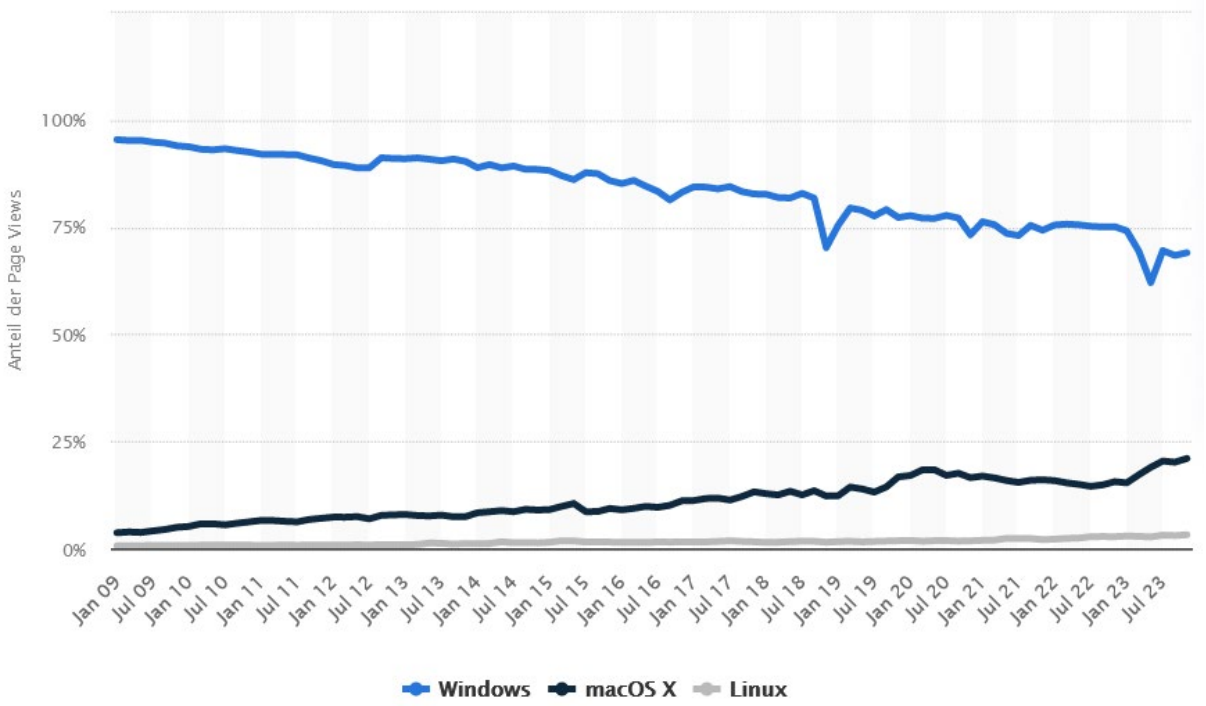
Whitepaper - Brauche ich am MacBook eines Unternehmens ein Antivirus Programm?

Noch bis heute hält sich der Mythos, dass MacBooks im Vergleich zu Windows-Computern weniger anfällig für Malware und Viren sind und deswegen kein Antivirus Programm installiert werden muss. Leider ist es nicht mehr als ein Irrglaube, dass diese Art der PCs ausreichend vor Schadsoftware geschützt sind. Es gibt zwar einige Sicherheitsfeatures, die Windows Geräte nicht haben, aber im Unternehmenskontext ist das noch immer zu wenig, und man sollte sich nicht in Sicherheit wiegen.

Gerade im Unternehmen müssen Sie zu jederzeit wissen, was auf den Geräten vorgeht. Sollte ein*e Mitarbeiter*in eine Phishing-Mail anklicken und Daten angeben, so können Sie das direkt über dieses Antivirus Programm auswerten und Maßnahmen dagegen ergreifen. Außerdem ist es relevant zu wissen, was das Gerät, und der User, macht. Sollten Sie also keine Sicherheitssoftware installiert haben gehen Ihnen wichtige Informationen verloren und ein Cyberangriff steht schon in den Startlöchern.

Woher kommt der Mythos, dass MacBooks weniger anfällig auf Viren sind?

Betrachtet man die Marktanteile der drei großen Betriebssysteme, so sieht man eindeutig, dass Windows noch immer mit rund 69% weit über MacOS (21%) und Linux (3%) dominiert. Klar, dass da Cyberangreifer hauptsächlich die große Masse versuchen zu attackieren. Da ist es am einfachsten auch dieses Betriebssystem zu fokussieren, um den größten Gewinn für die geringste Arbeit zu erhalten. Dieser Schluss ist aber nicht vollkommen richtig, denn wenn man bedenkt, dass nur 21% aller Betriebssysteme MacOS sind, so hört man auch einfach weniger von Angriffen. Das bedeutet auch wiederrum, dass viele noch immer den Mythos glauben, MacBooks wären weniger anfällig nur weil sie weniger davon mitbekommen.



Welche Sicherheitsfeatures hat ein MacBook?

MacBooks werden vom Werk aus nicht mit einem Antivirus Programm ausgeliefert. Dennoch stellt Apple verschiedene Funktionen zum Schutz vor Viren bereit:

- XProtect: XProtect von Apple, enthält bekannte Malware-Definitionen. Beim Herunterladen neuer Programme überprüft diese Datei automatisch, ob eine ihrer Definitionen in den Dateien enthalten ist. (Es handelt sich hierbei um eine Signaturbasierte Malware Erkennung)
- Malware Removal Tool (MRT): Dieses Tool, das bereits in macOS integriert ist, entfernt Malware, die sich in Ihre Datein eingeschlichen hat. Der Prozess läuft automatisch im Hintergrund ab, sobald XProtect eine neue Bedrohung erkennt.
- Gatekeeper: Diese von Apple bereitgestellte Software blockiert unbekannte Apps und überprüft, ob diese manipuliert wurden.
- Sicherheits- und Datenschutzeinstellungen von Apple: In diesen Einstellungen ist festgelegt, dass macOS die Installation von Drittanbieter-Software untersagt, sofern sie nicht aus dem App Store oder von verifizierten Entwicklern stammt.

- **Sandboxing:** Statt Apps vollen Zugriff auf Benutzerdaten zu gewähren, verwenden Macbooks ein sogenanntes Sandboxing. Das bedeutet, dass diese Apps nur auf die für ihre Funktionen unbedingt erforderlichen Daten zugreifen können. Sie haben keinen Zugriff auf andere Anwendungen, das Betriebssystem oder wichtige Einstellungen, was sie weniger anfällig für Angriffe macht.
- **FileVault:** FileVault ist Apples Umsetzung zur Sicherung Ihrer Daten auf macOS und Mac-Hardware. Es verschlüsselt sämtliche Daten auf Ihrer Festplatte. Sobald FileVault aktiviert ist, erfolgt die Verschlüsselung Ihrer Daten in Echtzeit (on-the-fly), und dies geschieht nahtlos und kontinuierlich im Hintergrund.

Gibt es konkrete Gründe, warum ein MacBook in Unternehmen immer ein Antivirus Programm benötigt?

Ein Unternehmen muss die eigenen Daten immer bestmöglich schützen. Dafür ist schlichtweg eine Sichtbarkeit auf den IT-Systemen erforderlich. Nur wenn man weiß, was darauf auch passiert kann man dagegen vorgehen. Neben diesen Hauptgrund gibt es auch einige Punkte, die beachtet werden müssen:

1. **Zunehmende Bedrohungen für macOS:** Obwohl MacBooks historisch betrachtet als sicherer galten, ist die Bedrohungslage für macOS in den letzten Jahren gestiegen. Es gibt mittlerweile Malware, die speziell für macOS entwickelt wurde. Unternehmen sollten sich der aktuellen Bedrohungen bewusst sein und ihre Sicherheitsmaßnahmen entsprechend anpassen. [1] [2] [3]
2. **Netzwerk- und Geräteheterogenität:** In Unternehmen gibt es oft eine Vielzahl von Geräten und Betriebssystemen im Einsatz. Wenn ein gemischtes Ökosystem aus Macs und anderen Geräten vorhanden ist, könnte die Implementierung eines einheitlichen Sicherheitsstandards, einschließlich Antivirus Programm, sinnvoll sein.
3. **Proaktive Maßnahmen:** Antivirensoftware bietet proaktiven Schutz, indem sie bekannte und auch unbekannte Bedrohungen erkennen und blockieren kann, bevor sie Schaden anrichten. Dies kann dazu beitragen, Sicherheitsvorfälle zu verhindern, bevor sie auftreten.
4. **Compliance-Anforderungen:** Bestimmte Branchen und regionale Vorschriften können die Verwendung von Antivirensoftware vorschreiben, um bestimmten Compliance-Anforderungen zu genügen.

5. Signatur basierte Antivirus Scanner sind nicht genug: Insgesamt ist es ratsam, nicht ausschließlich auf signaturbasierte Scanner zu setzen. Unternehmen und Privatanwender sollten stattdessen umfassende Sicherheitsstrategien implementieren, die verschiedene Technologien und Ansätze kombinieren, um sich gegen eine breite Palette von Bedrohungen zu schützen. Dazu gehören regelmäßige Aktualisierungen der Sicherheitssoftware, Verhaltenserkennung der Antivirus Software, Schulungen für die Benutzer*innen zur Sensibilisierung für Sicherheitsrisiken, sowie die Implementierung von Sicherheitsrichtlinien.

Zusammenfassung

Die verbreitete Annahme, dass ein MacBook im Vergleich zu Windows-Computern weniger anfällig für Malware sind und daher kein Antivirus Programm benötigen, ist ein Mythos. Obwohl Macs einige Sicherheitsfeatures bieten, ist allein darauf nicht zu vertrauen, insbesondere im Unternehmenskontext. Es entscheidend, die Aktivitäten auf den Geräten zu überwachen, um auf mögliche Bedrohungen reagieren zu können. Antivirensoftware spielt hierbei eine wichtige Rolle, indem sie die Analyse von Phishing-Angriffe erleichtert und Maßnahmen einfacher ergriffen werden können. Marktanteile zeigen, dass Windows immer noch dominierend ist, aber dies macht ein MacBook nicht immun gegen Angriffe.

Es ist ratsam, eine umfassende Sicherheitsstrategie zu implementieren, die verschiedene Technologien kombiniert und regelmäßige Schulungen für Benutzer einschließt. Unternehmen sollten sich bewusst sein, dass die Sicherheit von MacBooks nicht automatisch gewährleistet ist, und entsprechende Schutzmaßnahmen ergriffen werden müssen. Wir unterstützen Sie gerne dabei.