Kurz-Check:

BENÖTIGT APPLE EINE ANTIVIRENSOFTWARE?

MacOS gilt als das Paradebeispiel für ein sicheres Betriebssystem. Daran beißen sich Cyberkriminelle die Zähne aus, behaupten eingefleischte Apple-Jünger. Für den Hersteller selbst reichen die integrierten Bordmittel für die überschaubare Gefahr durch Cybercrime völlig aus. Die Security-Forscher von ESET machten sich ein eigenes Bild von macOS.

Sicherheitslücken in Microsoft Exchange, Hacker-Angriff bei Solarwinds, Ransomware im Düsseldorfer Uniklinikum und in der Funke Mediengruppe: Die Presse berichtet täglich über sicherheitsrelevante Vorfälle.

Interessanterweise verknüpft kaum jemand Sicherheitsprobleme mit macOS, bei digitalem Ungemach fällt als erstes der Name Microsoft. Möglicherweise deshalb, weil Windows nach wie vor die dominierende Plattform auf Endpoints ist. Doch das Blatt wendet sich: Seit Jahren erobert das Apple Betriebssystem immer mehr Marktanteile, zu Ungunsten von Microsoft. Inzwischen basiert fast jedes fünfte Gerät auf macOS.

Für die Präsenz von Apple-Computern in Unternehmen gibt es zwei Gründe. Macs sind seit langem bei Mitarbeitern in kreativen Berufen - beispielsweise in internen Grafikteams, Multi-Media-Unternehmen oder Werbeagenturen - sehr beliebt. Die Architektur des Betriebssystems eignet sich besonders für Grafikdesign, Videoschnitt und Desktop Publishing. In diesen Fällen wird der Rechner aufgrund einer klaren geschäftlichen Notwendigkeit eingesetzt.

Auf der anderen Seite entscheiden sich Anwender vor allem aus persönlichen Vorlieben für Macbooks oder den iMac. Als Grund dafür werden häufig die intuitiv zu bedienende Benutzeroberfläche von Betriebssystem und Software oder das High-End-Design genannt.

Bleibt aber die spannende Frage: Wie gefährdet ist macOS wirklich und welche Sicherheitsmythen rund um das Betriebssystem sind korrekt?

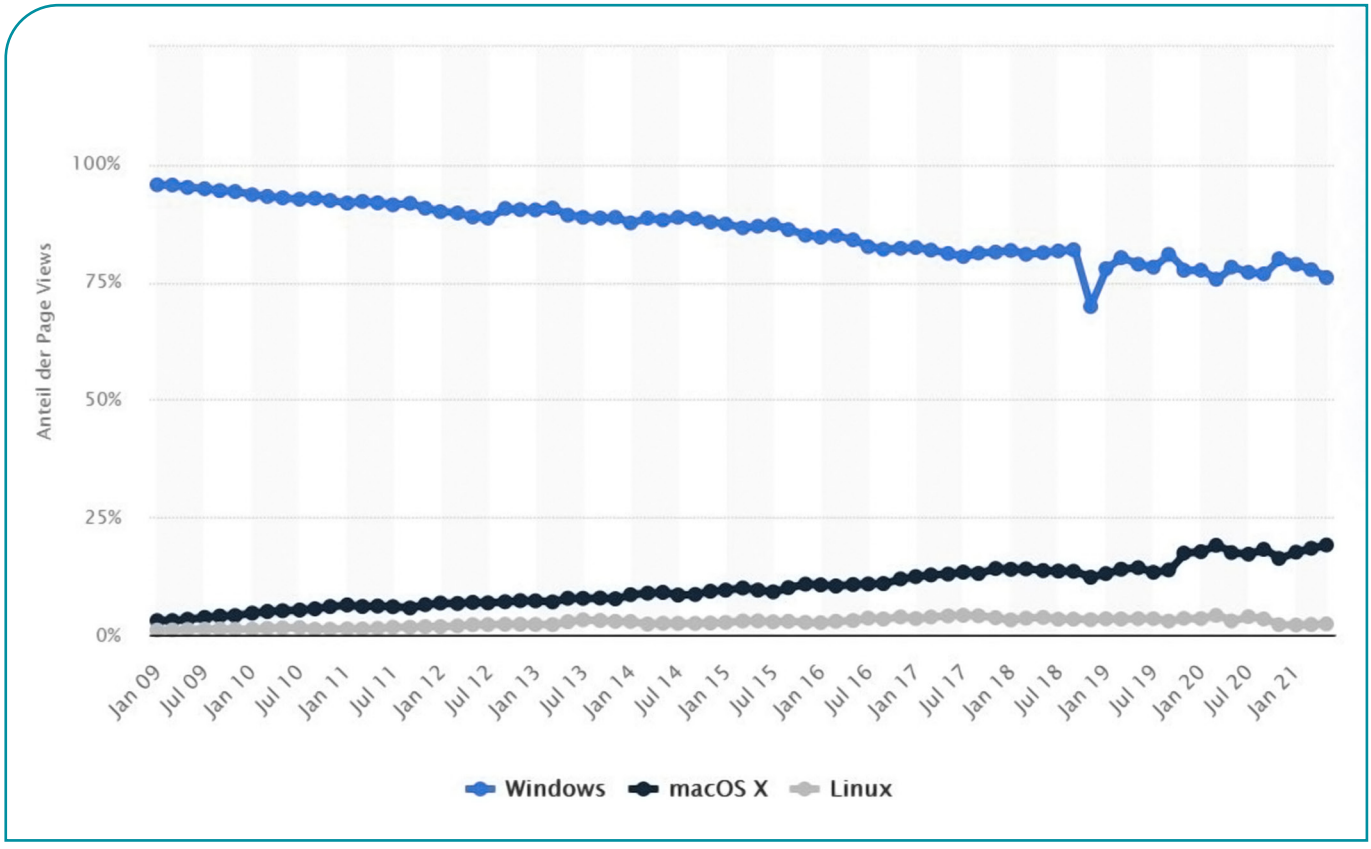

Abb. 1 Die Marktanteile der Betriebssysteme verschieben sich (Quelle: https://netmarketshare.com/, Stand 01/2021)

Mythos 1: Es gibt keine Malware für macOS

FALSCH: Es gibt sie und zwar tausendfach. Wie das Magdeburger Testinstitut AV-Test ermittelte, hat sich die Anzahl der Malware im Laufe der letzten Jahre vervielfacht. Zum gleichen Ergebnis kommt das Innsbrucker Testlabor AV-Comparatives. Auch die ESET Telemetrie verzeichnet immer mehr Schadcode für macOS. Wie man in der Grafik (s.u.) erkennt, hat vor allem die Quantität im 4. Quartal 2020 sprunghaft zugenommen.

Und die Malware-Funde haben es in sich. Im November 2020 stellte Apple eine Reihe von Macs mit dem selbst entwickelten neuen Apple Silicon M1-Chip vor. Die Veröffentlichung der neuen Hardware erregte auch die Aufmerksamkeit eifriger Cyberkrimineller.

Sie sorgten nach nur wenigen Wochen für eine Premiere, nämlich maßgeschneiderte Malware für die neuen Apple-Chipsätze. Die als GoSearch22 bezeichnete Anwendung ist eine Variante der Pirrit-Adware-Familie, einer verbreiteten, auf Mac-Nutzer abzielenden Bedrohung. Sie scheint sich selbst als böswillige Safari-Erweiterung zu installieren und als LaunchAgent Persistenz zu erlangen.

Die Beliebtheit von Kryptowährungen schlägt sich auch in der Vielzahl von Malware wieder. ESET entdeckte kürzlich eine verseuchte Krypto-Trading-Software für macOS, die Browser-Cookies und Krypto-Wallets stiehlt und als kleine "Zugabe" Screenshots vom Rechner des Opfers macht.

Dabei versahen Cyberkriminelle die ursprünglich legitime Trading-Anwendung Kattana mit ihrer Malware, benannten sie um und vertrieben sie auf einer Kopie der ursprünglichen Webseite. In verschiedenen Kampagnen nannten sich die fiktiven Apps Cointrazer, Cupatrade, Licatrade und Trezarus.

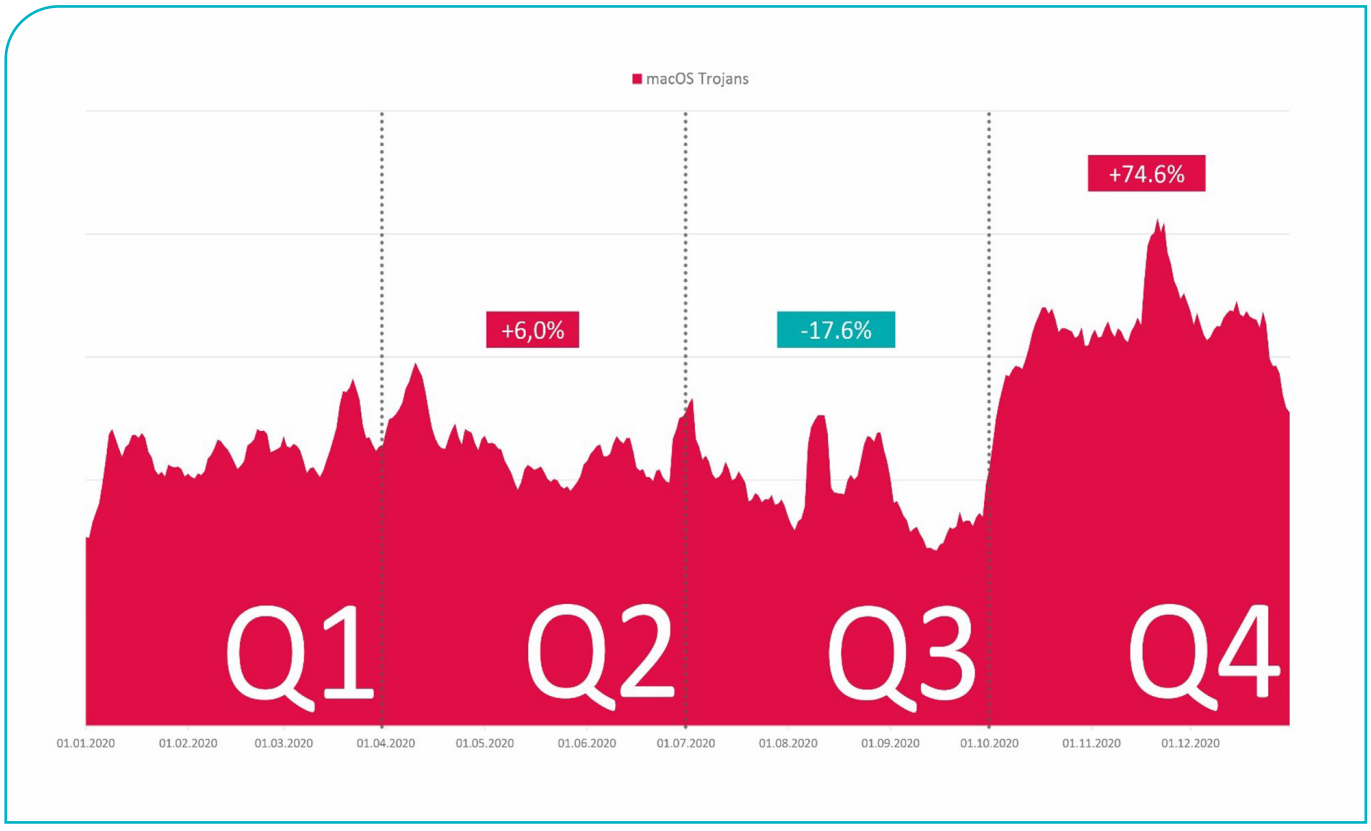

Abb. 2 Anzahl der Trojaner für macOS stieg in 2020 deutlich (Quelle: www.eset.com; Threat Report 1/2021)

Mythos 2: Das Betriebssystem ist sicher

WAHR: Apple stattet in puncto Sicherheit sein Betriebssystem sehr gut aus und kommt dem von ESET geforderten Multi-Secured-Endpoint schon sehr nah: Mit Virenschutz, Firewall, Verschlüsselung und Datensicherung sind Anwender auf alle Eventualitäten vorbereitet. Neue Geräte besitzen auch einen Fingerprint-Sensor ("Touch ID") für eine Multi-Faktor-Authentifizierung und komplettieren den Multi-Secured-Endpoint. Hinzu kommt von Betriebssystemseite her der vorsichtige Umgang mit Programmen. Jede ausgeführte Software befindet sich in einer sogenannten Sandbox, die Berechtigungen während des Einsatzes begrenzt. Somit ist sichergestellt, dass sich jedes Programm nur so verhält, wie es zu erwarten ist. Das erschwert die Ausführung von Schadcode oder das Ausnutzen von Anwendungen.

Zudem überprüft die Sicherheitsfunktion "Gatekeeper" die Codesignatur heruntergeladener Programme, bevor sie ausgeführt werden können. Genau genommen überprüft sie, ob die Software seit der Signierung durch Apple und nach der "Aufnahme" in deren App-Store nicht verändert wurde. Oder wenn sie nicht aus dem Apple Store stammt, dass sie korrekt signiert ist und seitdem durch einen "identifizierten Entwickler" nicht verändert wurde. Dies verringert die Wahrscheinlichkeit, dass Malware versehentlich ausgeführt wird.

In den letzten Jahren hat sich Apple jedoch einige Fehler erlaubt, die dem guten Ruf schadeten. Besonders ärgerlich war ein selbstgeschaffenes Problem, welches das Root-Benutzerkonto von macOS betraf. Dabei konnte dieses Konto mit umfassenden Nutzerrechten von jedermann aufgerufen und genutzt werden. Es reichte schon, den Benutzernamen "root" sowie ein leeres Passwort einzugeben und dann wiederholt die Enter-Taste zu drücken. So konnten Fremde auch ohne große IT-Kenntnisse den Mac übernehmen.

Die Sicherheitslücken Spectre und Meltdown in den Prozessoren von Intel, AMD und ARM kratzten 2018 indirekt am Image von Apple. Sie sind in der Lage, den virtuellen Speicher auszulesen, auf den eigentlich niemand Fremdes Zugriff haben sollte. Dieser geschützte Speicherbereich enthält beispielsweise das Betriebssystem, seine Gerätetreiber und vertrauliche Informationen wie Kennwörter und Kryptografiezertifikate. Angreifer könnten so Sicherheitsmechanismen wie das Sandboxing umgehen oder Schadcode ausführen. Apple hat das Problem durch entsprechende Updates gelöst.

Auch der Übergang auf macOS Big Sur lief nicht so reibungslos, wie es Apple-Fans erwarteten. Lange Downloadzeiten und -abbrüche, jaulende Lüfter und eine langsame Performance verärgerten viele Anwender. Schuld daran waren Apple-Server, darunter auch der Signatur-Server, der eigentlich Malware herausfiltern soll. Fast noch schlimmer wog ein Privatsphärenproblem, das im gleichen Atemzug auftrat. So soll Apple Status-Protokolle übertragen haben, die neben den Daten zur geöffneten Software auch Informationen zum Datum, zur Uhrzeit und zur IP-Adresse enthielten. Die Übertragung erfolgte unverschlüsselt und somit konnte potentiell jeder, der Zugriff zum Netzwerk hat, diese Informationen einsehen. Nach Apple-Angaben soll dieses Problem im Sinne der Anwender gelöst sein.

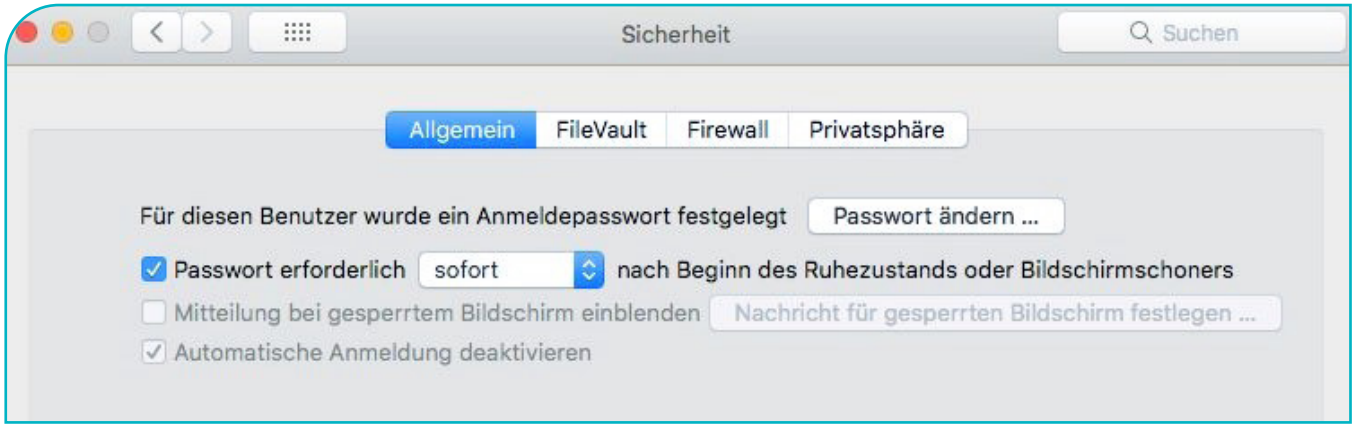

Abb. 3 Sicherheitseinstellungen in macOS (Quelle: ESET; Screenshot)

Mythos 3: Die paar Sicherheitslücken machen den Braten nicht fett

FALSCH: Mitte Dezember 2020 musste Apple wichtige Sicherheitsaktualisierungen für die Betriebssysteme Mojave und Catalina bereitstellen.

Mehr als 50 Schwachstellen, darunter auch mehrere als kritisch eingestufte, wurden damit behoben. Darunter fallen die Bereiche AMD- und Intel-Grafiktreiber, App-Store, Audio, Bluetooth, CoreAudio, CoreText, FontParser, HomeKit, ImageIO, Kernel, Systemeinstellungen und WLAN. Einige Schwachstellen ermöglichen Angreifern die Schadcode-Ausführung mit hohen Zugriffsrechten und sind daher besonders gefährlich.

Wenn dies nur ein Einzelfall wäre, hätte der Mythos sicherlich noch Bestand. Allein der Blick auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldeten Vorfälle zeigen deutlich, dass dem leider nicht so ist. (Quelle: www.bsi.bund.de, Stand: 07/2021)

Im Vergleich zu anderen Betriebssystemen war die Gesamtanzahl über die Jahre vergleichsweise gering. Sorge bereitet jedoch die stetige Zunahme in Quantität und Qualität der Sicherheitslücken. Laut VULDB.com hat Apple inzwischen den Spitzenplatz eingenommen.

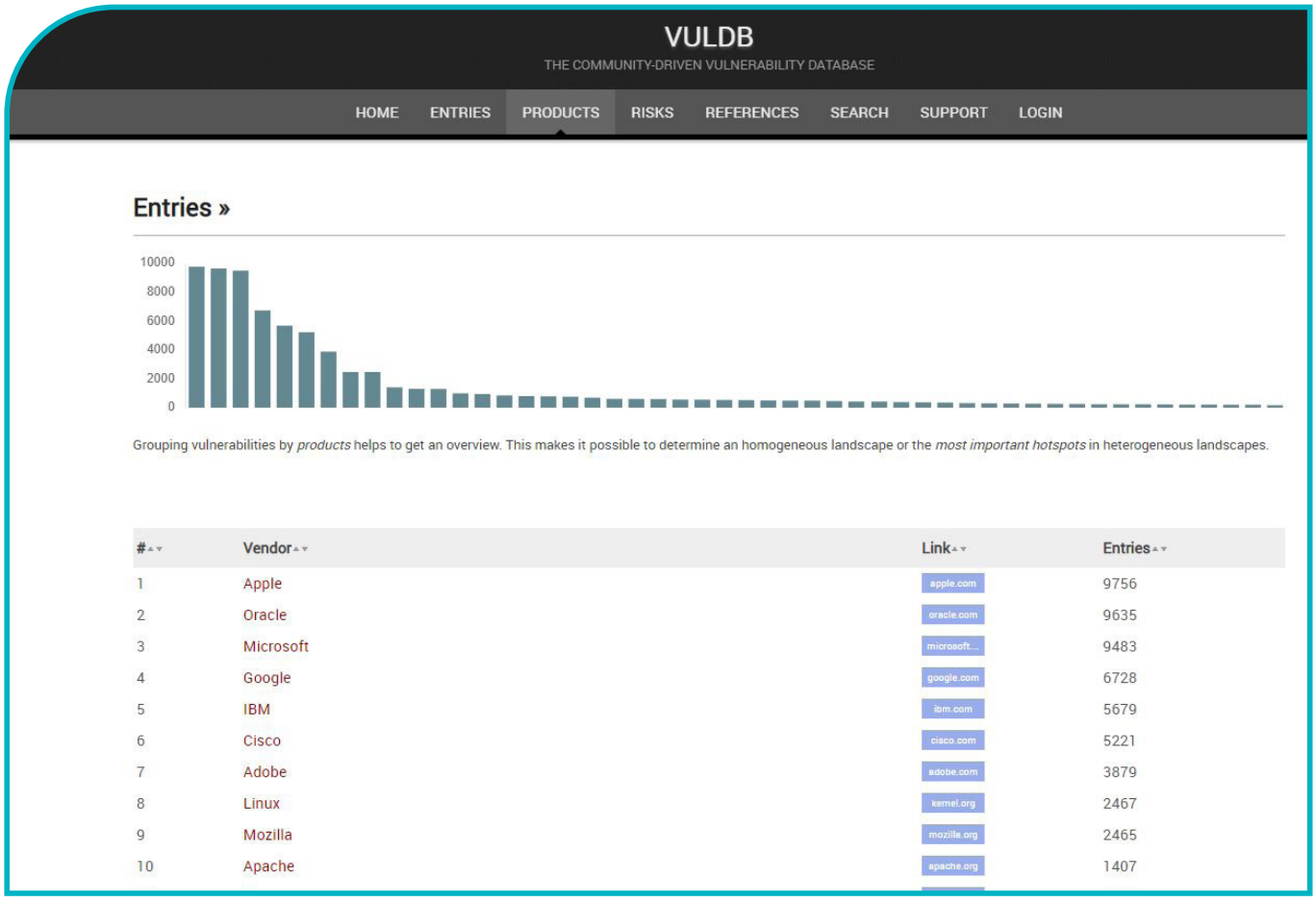

Abb. 4 VULDB.com analysiert Sicherheitslücken weltweit (Quelle: www.vuldb.com; Stand 12/2020)

Mythos 4: Hacker interessieren sich nicht für Apple

HALBWAR: Für Cyberkriminelle war macOS lange Zeit wenig lukrativ. Eine vergleichsweise geringe Anzahl von Anwendern und ein sicheres Betriebssystem bedeuteten viel Arbeit für minimalen finanziellen Gewinn.

Die permanent wachsende Beliebtheit von Apple-Geräten verändert das gerade. Wer sein iPhone oder iPad liebt, greift anscheinend immer öfter auch zu Mac-Rechnern anstatt Windows-PCs. Dies belegen die aktuellen Absatzzahlen, die das Analystenhaus Canalys kürzlich veröffentlichte.

Apple konnte im 1. Quartal 2021 rund 6,6 Millionen Macs verkaufen. Dies stellt gemessen am Vorjahresquartal ein Wachstum von satten 105 Prozent dar.

Im Vergleich: Der Marktdurchschnitt beläuft sich auf 54 Prozent. Der Marktanteil von Apple stiegt in Q1/2021 auf über acht Prozent.

Doch nicht nur die steigende Anzahl an Mac-Fans macht Cyberkriminellen das Betriebssystem schmackhaft. Einer US-Umfrage von RJI Online nach scheinen Besitzer von Apple-Geräten mehr zu verdienen als beispielsweise Android-Anwender. Dies bedeutet für Hacker im Umkehrschluss: Dort gibt es finanziell mehr zu holen.

Es ist also kein Wunder, dass immer mehr Sicherheitslücken aktiv gesucht, ausgenutzt und erst später publik werden. Denn über sie gelangen Kriminelle leichter an wertvolle Daten. Es ist für Sie einfacher mit Ransomware Gelder zu erpressen als über den Umweg "Fehlverhalten des Besitzers" zu gehen.

Worldwide desktop, notebook and workstation shipments (market share and annual growth)
Canalys PC Market Pulse Q1 2021

Vendor (company)	Q1 2021 shipments	Q1 2021 market share	Q1 2020 shipments	Q1 2020 market share	Annual growth
Lenovo	20,400	24.7%	12,702	23.8%	60.6%
HP	19,237	23.3%	11,701	21.9%	64.4%
Dell	12,948	15.7%	10,496	19.6%	23.4%
Apple	6,605	8.0%	3,219	6.0%	105.2%
Acer	5,690	6.9%	3,125	5.8%	82.1%
Others	17,795	21.5%	12,227	22.9%	45.5%
Total	**82,675**	**100.0%**	**53,470**	**100.0%**	**54.6%**

Note: Unit shipments in thousands. Percentages may not add up to 100% due to rounding.
Source: Canalys PC Analysis (sell-in shipments), April 2021

Abb. 5 Der Marktanteil von Apple-Geräten nimmt weiter zu (Quelle: www.canalys.com; Stand 04/2021)

Mythos 5: Macs benötigen kein Virenschutzprogramm

HALBWAHR: Viele Anwender von Apple-Rechnern wissen nicht einmal, dass ein vollwertiger Virenschutz unter der Haube permanent nach Malware Ausschau hält. Diese integrierte, leistungsstarke Antivirustechnologie nennt sich XProtect. Anders als das Windows-Pendant kommt hier "nur" eine signaturbasierte Erkennung von Schadprogrammen zum Einsatz. Das System verwendet YARA-Signaturen, die Apple regelmäßig aktualisiert. Das Unternehmen überwacht Malware-Neuinfizierungen und -Verläufe und aktualisiert die Signaturen automatisch und unabhängig von System-Updates, um Mac-Computer vor Infizierungen zu schützen. Sollte sich tatsächlich bösartiger Code auf einem Mac einschleichen, bietet macOS auch gleich ein Werkzeug (Malware Removal Tool oder MRT) zur Bereinigung an.

Apple überwacht das Ökosystem nicht nur auf Malware-Aktivitäten, um im XProtect Aktualisierungen anzustoßen, sondern stellt auch Updates für MRT bereit, um die Systeme von Schadcode zu bereinigen. MRT entfernt Malware nach dem Empfang aktualisierter Informationen und prüft bei Neustarts und Anmeldevorgängen weiterhin auf Infektionen.

Grundsätzlich reichen XProtect und MRT aus, um den einzelnen Mac-Anwender sicher vor Malware zu schützen. Befindet sich dessen Gerät allerdings in einem Netzwerk mit Windows-PCs, sieht die Lage anders aus. Macbooks und iMacs können dazu verwendet werden, Schadprogramme in den Rechnerverbund einzuschleusen. Wenn der betreffende Mac-Computer nicht geschützt ist, kann er Windows-Malware auf Windows-Geräte im Unternehmensnetzwerk übertragen. In diesem Fall verbindet sich die Malware mit dem Netzwerk, umgeht die Netzwerk-Firewall oder Sandbox und infiziert das Unternehmensnetzwerk. Insofern ist eine Antimalware-Lösung, die sowohl gegen Mac- als auch Windows-Schadprogramme schützt, für Unternehmen sehr sinnvoll und im Sinne von Zero-Trust-Security sogar ein Muss.

Fazit

Apples macOS zählt zu den aktuell sicheren Betriebssystemen auf dem Markt. Ungeachtet der geschilderten Sicherheitslücken bietet der Hersteller eine sehr gute Security-Architektur, die permanent weiterentwickelt wird. Dennoch garantiert auch Apple keine 100%-ige Sicherheit. Es empfielt sich daher, eine weitere Security-Schicht einzubauen, um dem Optimalziel nahezukommen. Experten regen an, eine zuverlässige und unabhängig getestete Lösung mit mehreren Schutztechnologien zu verwenden. Diese könnte beispielsweise ESET Cyber Security für macOS sein.

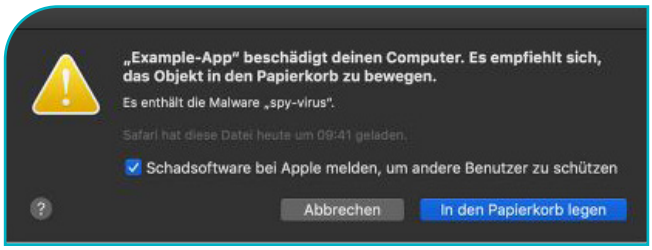

Abb. 6 Sicherheitswarnung von macOS
(Quelle: ESET; Screenshot)