Sophos MDR -- Empfehlung oder nicht?

Beitrag von „wastenstoeckel“ vom 28. April 2023, 19:01

Kein Hackintosh-Thema, ich weiß... Dennoch:

Bei meiner Freundin in der Firma wollen die it-Fraggles jetzt "Sophos MDR" auf den Macs installieren, so eine Security/Anti-Viren-Software.

Kennt das jemand? Kann man das empfehlen? Oder ist das Abzocke? 

Beitrag von „al6042“ vom 28. April 2023, 19:56

Wenn es sich beim Mac deiner Freundin um einen Firmengerät handelt, stellt sich die Frage eigentlich erst gar nicht.

Wenn bei der Firma eine BYOD (Bring Your Own Device) Regel gilt, müssen die den entsprechenden Client in ihrer Sophos Central Umgebung zulassen.

Dabei werden für den Client keine Kosten anfallen, sondern der Firma die in der Sophos Central Cloud-Umgebung gemeldeten Endgeräte in Rechnung gestellt.

Auf alle Fälle gilt für die Firmen-IT hoffentlich immer: Du kommst hier nicht rein, wenn wir deine Möhre nicht kennen...

Beitrag von „wastenstoeckel“ vom 28. April 2023, 20:37

danke für die schnelle Antwort.

Beitrag von „talkinghead“ vom 28. April 2023, 21:02

Das ist für Endpoint Detection & Response. Damit werden im System Aktivitäten aufgezeichnet und in ein Analysebackend übertragen. Dort werden die Aktiviäten nach Mustern bzw Indicators of Compromise (IOC) untersucht.

Im Falle eines Incidents kann der IT Security Analyst sich in einer Art Timeline genau die aktivitäten rund um den Incidentzeitraum anschauen. So is es zumindest bei Microsoft Defender EDR. Durch die konsolidierte Datenhaltung kann man auch Rückwirkend nach IOCs suchen und Patient “0” identifizieren. Im Falle eines Incidents kann man ggfs auch alle Endgeräte, die die IOCs aufweisen, vom Netz isolieren.

Ist eine sehr hilfreiche Sache wenn ein 24x7 SOC dahinter sitzt.