MACMON NAC
PAST VIEWER

Historische Tatsachen

macmon Past Viewer bietet ergänzend die Möglichkeit, die bei Network Access Control üblicherweise verworfenen anfallenden Daten strukturiert zu sammeln und aufzubereiten, um neben der Live-Sicht auch eine historische Sicht zu erhalten. Pro Endgerät lässt sich damit darstellen, wann und wo das Gerät im Netzwerk betrieben wurde, welche IP-Adressen und welche Namen es hatte oder in welchem VLAN es war.

Erkenntnisse aus Ihren eigenen Informationen

Historische Daten sind oftmals sowohl für forensische Analysen in der Vergangenheit als auch für zukunftsorientierte Betrachtungen wertvoll. macmon Past Viewer sammelt über lange Zeiträume (wahlweise auch über den Zeitraum von Jahren) Informationen über Ihr Netzwerk bzw. die Netzwerkverbindungen. Auf Basis von Ereignissen wird protokolliert, welche Geräte wann und wo im Netzwerk waren, samt der entsprechenden Eigenschaften.

Pro Endgerät und pro Switchport werden „Endgeräte-Sessions" dargestellt, die den vollständigen Verlauf einer Verbindung abbilden. So sind Details bzgl. verwendeter IP-Adressen, Namen und Autorisierungen sowie die entsprechend genutzten Layer 2 und Layer 3 Netzwerkkomponenten vom Zeitpunkt des Starts bis zum Ende enthalten.

macmon Past Viewer ist darauf ausgelegt, viele Daten lange aufzubewahren und trotzdem schnellstmöglich zu analysieren. Eine lange Historie kann damit bei Sicherheitsvorfällen zur forensischen Suche beitragen aber auch generelle Informationen liefern, die für Audits und Zertifizierungen notwendig sind. Durch die Information welche Geräte in einem bestimmten Zeitraum in einem entsprechend zu überprüfenden Netzwerksegment verbunden waren – und damit auch welche nicht verbunden waren, lässt sich die Nachweispflicht gemäß ISO oder PCI-Compliance erheblich vereinfachen.

Auch die DSGVO fordert eine Dokumentation der sicherheitsrelevanten Vorkommnisse im Netzwerk – mit macmon Past Viewer ist dies genauso gegeben wie die Möglichkeit eine Risikoanalyse für Netzwerkbereiche durchzuführen.

Das Wissen über die Menge und Art der Geräte, welche in der Vergangenheit z. B. in einem bestimmten Gebäude verbunden waren bietet die Chance einer Abwägung von Auswirkungen bei Veränderungen der Netzwerkinfrastruktur oder bei Ausfällen.

Vorteile & Funktionen

- ✓ **Erfüllung von Nachweispflichten gemäß ISO, PCI oder auch DSGVO-Vorgaben**
- ✓ **Unterstützung von forensischen Analysen bei Sicherheitsvorfällen**
- ✓ **Impact-Analysen für Netzwerkbereiche, Orte oder einzelne Netzwerkgeräte**

Kontakt macmon secure GmbH | Alte Jakobstraße 79-80 | 10179 Berlin | Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Stand: 07/2021