WHITEPAPER
ADVANCED SECURITY

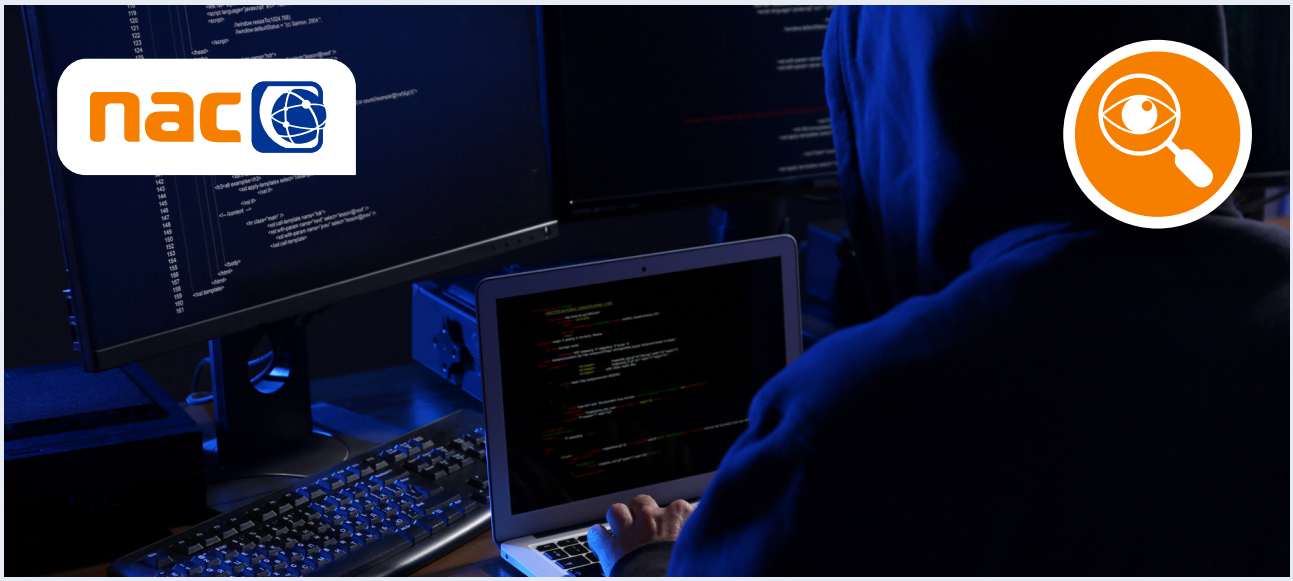
macmon intelligent einfach

Advanced Security – das Extra-Level an Netzwerksicherheit

Der Betrieb einer Network-Access-Control-Lösung wie macmon NAC stellt im Bereich der Sicherheit zwei grundlegende Anforderungen. Zum einen müssen Endgeräte so genau wie möglich identifiziert werden, um immer genau die richtigen Endgeräte in das dafür vorgesehen Netzwerksegment zuzulassen oder (bei unerwünschten Geräten) aus dem Netzwerk auszusperren. Zum anderen geht mit der genauen Identifizierung auch das Erkennen von Angriffen – eben der Fälschung einer Identität – einher. macmon Advanced Security begegnet genau diesen Anforderungen mit einer Reihe von unterschiedlichen Technologien und ist damit ein wichtiger Bestandteil der effektiven Kontrolle der Netzwerkzugänge und sowohl im Network Bundle als auch im Premium Bundle enthalten.

Endgeräte anhand von Zertifikaten identifizieren – auch ohne 802.1X
➡ **ab Seite 2**

Netzwerkgerätemessdaten wie ARP-Caches, DHCP- und DNS-Daten werden erhoben und korreliert. Endgeräte werden per WMI, SNMP, Footprinting und Fingerprinting gescannt, um Details zur Identifizierung zu ermitteln, aber auch auf Veränderungen zu überwachen. Die Summe der Informationen erlaubt neben der Identifizierung damit auch eine effektive Bekämpfung von Sicherheitsvorfällen wie ARP-Spoofing, MAC-IP-Mismatch, MAC-Address-Flooding und MAC Spoofing.



Angriffserkennung und -abwehr

macmon NAC ermittelt die Netzwerkinformationen durch die Kommunikation mit der Netzwerkinfrastruktur von zentraler Stelle aus, so dass im Vergleich zu vielen anderen Produkten am Markt keine Sensoren in den einzelnen Netzwerksegmenten benötigt werden.

Das gezielte Senden von gefälschten ARP-Paketen wird beim ARP-Spoofing oder auch ARP-Request-Poisoning dazu benutzt, um den Datenverkehr zwischen zwei Hosts in einem Datennetz abzuhören oder zu manipulieren. macmon Advanced Security schützt vor solchen Man-in-the-Middle-Angriffen, indem es ARP-Veränderungen erkennt und auf diese über die Ereignisverarbeitung reagiert.

Auch im DHCP-Server vorhandene fest, automatisch und dynamisch zugeordneten IP-Adressen sowie ihren Gültigkeitszeiten (Lease-Time) und Namens-Informationen werden eingelesen, verarbeitet und dem macmon-Berichtswesen zur Verfügung gestellt. macmon bietet Konnektoren zu allen gängigen DHCP-Servern, wie denen von Windows, Novell NDS und OES, Linux, HaneWIN, QIP DHCP und DHCP Enterprise, BlueCat oder Infoblox.

Stand: 11/2021

Stellt macmon Abweichungen zwischen den DHCP-Daten und den ARP-Daten fest, wird ein „mac_ip_mismatch“-Ereignis ausgelöst und es können im Regelwerk automatische Schutzmaßnahmen definiert werden.

Ein weiteres Angriffsszenario ist das Senden von sehr vielen MAC-Adressen – MAC Address Flooding, um so das verwendete Netzwerkgerät zu attackieren. Durch die direkte Kommunikation zwischen macmon NAC und den Switches werden auch diese Angriffe erkannt und können z. B. durch das sofortige Abschalten des verwendeten Switchports sofort gestoppt werden.

Das MAC-Spoofing wiederum ist ein Angriff, um unberechtigten Zugang zum Netzwerk zu erhalten. Für viele NAC-Systeme bildete die MAC-Adresse die Eintrittskarte zum Netzwerk. Dies ist zum einen der Tatsache geschuldet, dass es Geräte gibt, welche nicht über die Möglichkeiten verfügen, ein anspruchsvolleres Authentifizierungsverfahren – wie z. B. 802.1x – durchzuführen. Zum anderen ist die Einführung komplexerer Authentifizierungsverfahren, aus Sicht des einen oder anderen, auch sehr aufwendig, so dass sie wegen des befürchteten höheren Betriebsaufwandes bei Kunden nicht zum Einsatz kommen würden. Die MAC-Adresse lässt sich allerdings bei aktuellen Betriebssystemen sehr leicht fälschen, so dass Angreifer, die eine gültige MAC-Adresse in einem Netzwerk kennen, leichtes Spiel haben, um sich mit einem Fremdgerät Zutritt zu verschaffen. macmon NAC erkennt derlei Angriffe durch Identifizierungsmechanismen, die weit über die MAC-Adresse hinausgehen.

Geräteidentifizierung und -überwachung

macmon NAC ermittelt die Netzwerkinformationen durch die Kommunikation mit der Netzwerkinfrastruktur von zentraler Stelle aus, so dass im Vergleich zu vielen anderen Produkten am Markt keine Sensoren in den einzelnen Netzwerksegmenten benötigt werden.

Mit WMI und SNMP MAC-Spoofing verhindern

Diese beiden IP-basierten Advanced-Security-Optionen erlauben es zusätzliche Informationen zu einem Gerät zu sammeln. Da durch diese beiden Protokolle ein Gerät eindeutig identifiziert werden kann, kann MAC-Spoofing zuverlässig erkannt und verhindert werden. Im Rahmen der Scans wird geprüft, ob eine Anmeldung auf den Geräten möglich ist. Nach der Anmeldung wird bei WMI auf die Domäne, den Hostnamen und das Betriebssystem geprüft. Bei SNMP sind es die sysDescription, die systLocation und der sysName. Die Vorgaben für diese Parameter werden gruppenweise in der macmon GUI konfiguriert.

Wenn ein Angreifer die MAC-Adresse eines dieser Geräte spooft, erkennt macmon dies, da die Abfrage der Parameter oder der Login fehlschlagen. Es wird in macmon das Ereignis „corporate_check_failed“ erzeugt. Über das Ereignis-Regelwerk kann einheitlich oder durch Abgrenzung mittels Bedingungen individuell reagiert werden. Dadurch kann der Angreifer gemeldet und aus dem Netzwerk automatisiert ausgesperrt werden.

Footprinting

Footprinting ist eine weitere Option der Advanced-Security von macmon und kann entweder ergänzend zu WMI und SNMP genutzt werden oder separat für Geräte, welche die beiden Protokolle nicht unterstützen.

Im Rahmen des Footprintings wird der IP-Protokoll-Stack aller Geräte der konfigurierten Gruppe im Netzwerk untersucht. Mittels eines Port-Scans werden weitere Informationen zur MAC-Adresse erfasst und in der Benutzeroberfläche präsentiert. Vorgaben können an der Endgerätegruppe vorgenommen werden. So bietet sich die Möglichkeit, Betriebssystem- und Portvorgaben zu definieren.

Stand: 11/2021

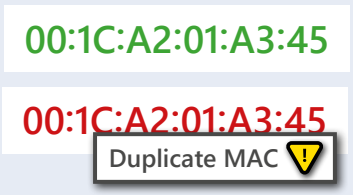
Footprinting ist nicht eindeutig

Die so durch Port-Scans gesammelten Informationen über das Betriebssystem und den offenen Ports eines Geräts nennen sich Footprint, da es sich hierbei – im Gegensatz zum Fingerprint – um keine eindeutige Identifikation eines Gerätes handelt. So haben z. B. zwei Drucker desselben Models, oder auch zwei gleich konfigurierte Windows-Rechner den gleichen Footprint.

Wenn ein Angreifer nun eine MAC-Adresse eines Druckers spooft und sein Linux-System mit dieser MAC-Adresse im Netzwerk anschließt, erkennt macmon die Änderung des IP-Protokoll-Stacks. Bei Abweichungen des Betriebssystems wird das Ereignis „corporate_check_failed“ ausgelöst. Gibt es Abweichungen bei den verwendeten Ports zu den Vorgaben an der Gruppe wird das Ereignis „now_nonportcompliant“ ausgelöst. Letzteres eignet sich auch zum Überwachen von Arbeitsplatzrechnern. Auf die Ereignisse kann analog wie bei WMI/SNMP gehandelt werden.

Erkennung von duplizierten MAC-Adressen

Das mehrfache Auftauchen einer MAC-Adresse im Netzwerk, erkennt macmon mit Advanced-Security automatisch. Wird eine MAC-Adresse von macmon an zwei unterschiedlichen Stellen gleichzeitig erkannt, wird das Ereignis „duplicate_mac“ ausgelöst.



Dieses Ereignis kann jedoch unterschiedliche Ursachen haben. Wenn Links zwischen zwei von macmon NAC überwachten Switches nicht erkannt werden und auch manuell nicht konfiguriert wurden, kann dieses Ereignis ausgelöst werden. Dies geschieht auch, wenn Endgeräte redundant am Netzwerk angebunden sind und deren Netzkarten im Teaming-Mode betrieben werden. Auch kann das Ereignis auftreten, wenn Endgeräte im laufenden Betrieb in einem sehr kurzen Zeitraum von einem Netzwerkgerät in ein anderes Netzwerkgerät umgesteckt werden.
Schlimmstenfalls handelt es sich eben auch um ein Endgerät, das zeitgleich mit derselben konfigurierten MAC-Adresse betrieben wird, z. B. durch einen Angriff mittels MAC-Spoofing. Insofern kann macmon NAC hier sofort Maßnahmen einleiten.

Sichere kryptografische Erkennung durch Fingerprinting

Über SSH (Secure Shell) liest macmon NAC den öffentlichen Schlüssel eines Endgerätes aus, speichert diesen und vergleicht ihn durch periodische erneute Abfragen. Stimmt der öffentliche Schlüssel des Endgerätes nicht mit dem in macmon NAC hinterlegten Schlüssel überein, wird das Ereignis „fingerprint_failed“ erzeugt, da davon ausgegangen werden muss, dass sich die Identität des Endgerätes verändert hat – es sich also um ein anderes Gerät handelt. Wie gewohnt kann mithilfe des Ereignisses nach Belieben auf die Situation reagiert werden.

Wird dem neuen Schlüssel vertraut, weil er beispielsweise durch eine Neuinstallation des Unternehmensgerätes entstanden ist, kann er in macmon NAC hinterlegt werden. Der neue Schlüssel ersetzt den zuvor gespeicherten Schlüssel und wird nun zur periodischen Prüfung herangezogen.

Ein ähnliches Verfahren kann macmon NAC auch für die von den Endgeräten verwendeten Zertifikate anwenden. Da Zertifikate im Vergleich zu Schlüsseln diverse weitere Eigenschaften aufweisen, ist hier eine granularere Prüfung möglich. So können neben einem Hashwert als Fingerprint auch einzelne Zertifikatseigenschaften wie der allgemeine Name, die Organisation oder der öffentliche Schlüssel zum Vergleich herangezogen werden.

Die feineren Justierungsmöglichkeiten erlauben damit eine sehr anwendungsfreundliche Nutzung dieser hoch sicheren Technologie bei gleichzeitiger Vermeidung von Fehlalarmen.

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

Stand: 11/2021