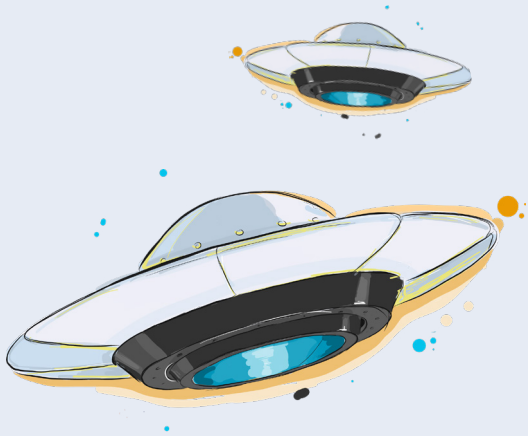
macmon
intelligent einfach



nac

UFOS ERKENNEN MIT MACMON NETWORK ACCESS CONTROL

UFOs = unbekannte fremde Objekte

5x EINFACH

1. GRUPPENBASIERTE KONFIGURATION

Unternehmensendgeräte werden in logische Gruppen sortiert. An diesen erfolgt die Konfiguration für die Behandlung der Endgeräte im Netzwerk, inklusive der weitergehenden Zugriffsberechtigungen. Auf diese Weise ist macmon NAC in der Lage, das Regelwerk dynamisch zu erstellen und bei Änderungen anzupassen. Das funktioniert für die SNMP- als auch die RADIUS-basierte Umsetzung gleichermaßen.

2. 802.1X (MIT UND OHNE ZERTIFIKATE)

In macmon NAC können anhand der gruppenbasierten Konfiguration leicht verschiedene Sicherheitslevel mit unterschiedlichen Berechtigungen definiert werden. Dadurch können in Abhängigkeit der Ausweisqualität mit User/Passwort oder mit Zertifikat unterschiedliche Netzwerkzugänge gewährt werden. Der Aufwand und die Komplexität werden erheblich reduziert, unabhängig davon, ob 802.1X ohne oder mit Zertifikaten umgesetzt wird!

3. GÄSTEPORTAL

Ausgelegt für hohe Flexibilität und verschiedenste Einsatzzwecke, sorgt das Gästeportal für eine Unterscheidung zwischen Gästen und Gastgeräten. Die integrierte Sponsor-Funktionalität erlaubt die Delegierung der Gutscheinerstellung und -verwaltung an beliebige Mitarbeiter. Bei Bedarf dient das Portal auch zur Zulassung von Mitarbeitergeräten (BYOD). macmon NAC liefert Ihnen automatisch eine aktuelle Übersicht über die mitgebrachten Geräte.

4. EFFEKTIVE VLAN-BERECHNUNG

Aufbauend auf der gruppenbasierten Konfiguration besteht die Möglichkeit, diverse Vorgaben für die Zugangsberechtigungen zu machen. macmon NAC berechnet das jeweils situativ benötigte VLAN und führt die Autorisierung durch. Dabei werden Details wie Standorte, Switches, Compliance Status und weitere einbezogen.

5. AD-INTEGRATION MIT MAPPING

macmon NAC bietet die Möglichkeit der Authentifizierung von Endgeräten mittels Identitätsquellen (AD, LDAP, SAML etc.). Dabei können sowohl Benutzerkonten als auch Gerätekonten verwendet werden. Das bedeutet eine erhebliche Vereinfachung bei der Einführung von 802.1X, da keine Zertifikate ausgerollt werden müssen. Endgerätegruppen oder Organisation Units (OUs) aus dem AD können dabei einfach mit den macmon-Endgerätegruppen verknüpft werden. Hier greift das automatische Regelwerk ebenso.

DIE ADD-ONS FÜR MACMON NAC:

PAST VIEWER: FORENSISCHE ANALYSEN DURCHFÜHREN

Der macmon Past Viewer bietet die Möglichkeit, die bereits erhobenen Daten strukturiert zu sammeln und aufzubereiten, um eine historische Sicht der Endgeräte im Netzwerk zu erhalten. Pro Endgerät und pro Switch-Port 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.

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. Zudem wird die Nachweispflicht gemäß ISO, PCI und der DSGVO bzgl. einer Dokumentation von sicherheitsrelevanten Vorkommnissen im Netzwerk erfüllt.

SWITCH VIEWER: SCHNELL ERFASSBARE DETAILS ÜBER DEN IST-ZUSTAND

Der macmon Switch Viewer liest von vorhandenen Netzwerkkomponenten solche Details wie Seriennummern, Portkonfigurationen bezüglich Geschwindigkeit, den Betriebsmodus, VLANs, Interface-Details und Standort sowie zukünftig weitere Inventory-Daten aus.

Der macmon Switch Viewer bietet zudem eine grafische Darstellung des tatsächlichen Switch Layout. Für weitergehende Aufgaben kann der macmon-RADIUS- Server für eine gesicherte Anmeldung mit Authentifizierung genutzt werden.

SCALABILITY: HOCHVERFÜGBARE MACMON NAC-SZENARIEN

Je nach Einsatz einer Network Access Control-Lösung und der verwendeten Technologien bestehen unterschiedliche Anforderungen an die Verfügbarkeit dieser Lösung. macmon begegnet diesen Anforderungen durch die Möglichkeit mit einer verteilten Serverstruktur zu agieren und diese in unterschiedlichen Architekturen bzw. Design-Varianten zu nutzen.

Der Einsatz hängt dabei stark von den Anforderungen bzw. der Zielsetzungen ab. Vom „Hidden Master"- Prinzip über einfache Ausfallsicherheit bis hin zur Kompensation von WAN-Verbindungsausfällen wird so die Verfügbarkeit von macmon NAC sichergestellt.

Jeder macmon-Server kann dabei wahlweise durch eine virtuelle oder eine physikalische Appliance gestellt werden.

nac
Network Access Control

macmon secure GmbH
Alte Jakobstr. 79-80 | 10179 Berlin
Telefon +49 30 2325 777-0 | nac@macmon.eu | www.macmon.eu

SCHNITTSTELLEN UND PARTNERSCHAFTEN

FÜR IHRE SICHERHEIT

Koppeln Sie macmon Network Access Control (NAC) mit anderen Sicherheitslösungen und erzielen Sie echte Mehrwerte!

Unsere eigens entwickelte NAC-Lösung macmon liefert Ihnen nicht nur die beste Antwort darauf, wie Sie ungesicherte Netzwerkzugriffe verhindern können, Sie können macmon NAC auch in andere Security-Produkte integrieren. Die Einteilung der Anbindungen erfolgt in Asset Management, Compliance, Identitätsquellen und Infrastruktur, wobei der Informationsaustausch jeweils bidirektional erfolgen kann.

ASSET MANAGEMENT

Mit der bidirektionalen Kopplung von Asset Management-Lösungen wie CMDBs, Inventory, Client Management und anderen Systemen, lassen sich die Information über Endgeräte und Netzwerkgeräte automatisch synchronisieren.

COMPLIANCE

Sollte eine vorhandene Sicherheitslösung bei der Überprüfung des Endgerätes einen Sicherheitsverstoß feststellen, werden die Identität, der Grund und der neue Compliance-Status an macmon NAC übermittelt. Das Gleiche gilt bei Infizierung durch ein Schadprogramm oder wenn das Endgerät Teil eines Botnetzes ist.

IDENTITÄTSQUELLEN

Bereits im Netzwerk vorhandene Identitätsquellen können von macmon NAC für die qualifizierte Authentifizierung von Endgeräten genutzt werden. Dazu zählen Mobile Device Management-Lösungen, AD-/ LDAP-Dienste, SAML, RADIUS-Server oder weitere Systeme.

INFRASTRUKTUR

macmon NAC findet schnell heraus welche Endgeräte sich im Netzwerk befinden, indem es die Daten der Netzwerkinfrastruktur ausliest oder übermittelt bekommt.

MACMON NAC LIFECYCLE

Der macmon NAC LifeCycle unterteilt sich in drei Phasen, die gleichzeitig die Grundlagen für erfolgreiche NAC-Projekte bilden:

1 Erhalten der vollständigen Netzwerkübersicht und Aufspüren von UFOs

ÜBERSICHT

Das Entscheidende ist, dass die bestehende Infrastruktur genutzt wird und die vollständige Netzwerkübersicht bereits innerhalb weniger Stunden in der intuitiven Web-GUI von macmon NAC zur Verfügung steht. Der geringe Einführungs- und Betriebsaufwand liegt deswegen im Fokus. Die gewonnene Übersicht erlaubt eine erste Beurteilung des Netzwerkzustands in Bezug auf die Menge und Art der UFOs (unbekannte fremde Objekte). Gleichzeitig wird ermittelt welchen Status das Netzwerk für die Einführung von NAC hat und welche Schritte noch berücksichtigt werden müssen.

- Erfassung der gesamten Infrastruktur und aller Endgeräte als Live-Bestandsmanagement
- Herstellerunabhängigkeit zur Abdeckung jedes Netzwerkes auch mit gemischten Komponenten unterschiedlicher Generationen
- Darstellung der Ereignisse im Netzwerk, wie bzw. Angriffe wie ARP oder MAC Spoofing
- Hoch flexible Anbindungsmöglichkeiten von Drittanbietern über die offene REST API für Asset Management-, CMDB-Lösungen usw.
- Grafische Darstellung der Netzwerktopologie mit umfangreichen Analysemöglichkeiten
- Umfassendes Reporting der im Netzwerk ermittelten Messdaten
- Aufspüren von UFOs und bekannten Endgeräten im Netzwerk

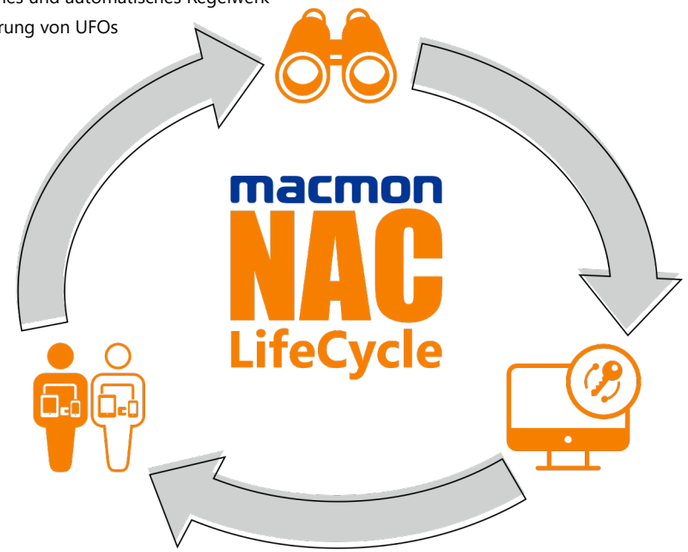
2 Steuerung der Zugänge auf Basis der Endgeräte-Identitäten

NETWORK ACCESS CONTROL

Ob Sie für die Kontrolle der Zugänge den reaktiven Ansatz per SNMP, den proaktiven Ansatz über 802.1X oder einen gemischten Betrieb nutzen möchten, macht administrativ durch das einheitliche und automatische Regelwerk in macmon NAC keinen Unterschied.

Die Netzwerksegmentierung erhöht die Sicherheit im Netzwerk und bildet auch BSI-konforme Sicherheitskonzepte ab. Die Kombination von macmon NAC mit bestehenden Identitätsquellen – CMDBs, Asset Management, AD/LDAP oder auch Mobile Device Management (MDM) – führt zu einer zentralen und vollständigen Sicht, die permanent aktuell ist.

- Technologieunabhängig: Mischbetrieb mit und ohne 802.1X/RADIUS
- Variabel: Abbildung und Umsetzung jeglicher VLAN-Konzepte
- Kompatibel: Anbindung beliebiger Identitätsquellen zur automatischen Pflege der Systeme
- Effizient: Gästeportal mit Sponsor- und BYOD-Funktionalität zur Reduzierung von Administrationsaufwänden
- Flexibel: Etablierung von Sicherheitszonen und zweckgebundenen Zugängen
- Mächtig: dynamisches und automatisches Regelwerk
- Automatisch: Isolierung von UFOs



3 Steuerung der Zugänge auf Basis des Sicherheitsstatus von Endgeräten

COMPLIANCE

macmon NAC ist die zentrale Macht im Netzwerk. Ergänzend werden auch die Endgeräte auf ihre Sicherheitseinstellungen bzw. ihr Sicherheitslevel kontrolliert. Dafür bietet macmon NAC diverse Überprüfungsmöglichkeiten. Die mächtigste Möglichkeit bietet die Integration von Drittanbieterlösungen. In der Regel ist bereits eine Lösung im Einsatz, die das Sicherheitslevel prüft und damit die entscheidenden Informationen bereithält. Endgeräte, die nicht den Anforderungen entsprechen, werden automatisch isoliert und nach erfolgter Heilung wieder in den ursprünglichen Zugang versetzt.

- Proaktive Reaktion auf Infektionsquellen
- Automatisierte Isolation von unsicheren Endgeräten im Netzwerk
- Flächendeckende Abbildung der Compliance-Zustände durch beliebige, herstellerunabhängige Datenlieferanten und wahlweise durch den macmon-Agenten
- Direkte Kopplung führender Antivirus-Anbieter zur automatisierten Reaktion auf kritische Ereignisse
- Problemlose Anbindung von Drittanbieterlösungen

MIT MACMON NAC BLEIBT IHR NETZWERK UFO FREI