macmon
nac intelligent einfach

WHITEPAPER
Management Summary

Warum NAC, warum jetzt und vor allem wie?

Intelligent einfach - mit wenig Aufwand viel erreichen.

Das Thema Netzwerkzugangskontrolle oder Network Access Control – NAC ist ein sehr aktuelles Thema, das in vielen Unternehmen plötzlich diskutiert wird. Doch warum? Und warum jetzt, wo es doch bereits seit vielen Jahren sowohl offene Netzwerkports als auch entsprechende Produkte gibt?

Der Hauptgrund für die Zunahme des Bedarfs an funktionierenden NAC-Lösungen dürfte der rasante Anstieg der vielen verschiedenen Endgeräte sein. Jeder Benutzer bzw. Mitarbeiter hat heute ein Smartphone oder einen eigenen Laptop. Die Möglichkeiten und der Komfort, die diese Geräte bieten, erwarten die Mitarbeiter heute und zukünftig auch an ihrem Arbeitsplatz. Viele Unternehmen halten dem Druck, mitarbeitereigene Geräte zuzulassen zwar noch stand, aber es kann nur eine Frage der Zeit sein, bis diese Standhaftigkeit zumindest in Teilen aufweicht. Zudem sind viele Geräte, wie auch einfache Access Points heute so kinderleicht zu bedienen, dass Mitarbeiter ohne weiteres entsprechende „Verteiler" mitbringen, anschließen und betreiben können – ohne, dass es die IT-Abteilung mitbekommen würde.

Die Mitarbeiter selbst haben jedoch oft kein Gefühl und auch nicht das Knowhow für „gefährliche" Geräte. Die genutzten Geräte sind aber in der Regel gar nicht für den Unternehmenseinsatz gedacht und damit auch nicht einfach zentral managebar. Das Zulassen auch nur einzelner Geräte öffnet jedoch den Zugang für alle anderen, wenn nicht zeitgleich oder vorher eine entsprechende Kontrollinstanz eingeführt wurde. Diese Instanz heißt Network Access Control.

Ein weiterer Grund, warum die Netzwerkzugangskontrolle aktuell auf dem Vormarsch ist, sind die inzwischen vorhandenen funktionierenden Lösungen. Bis vor kurzem noch basierten die meisten der angebotenen Produkte auf Technologien und Lösungsansätzen, die nicht oder nicht zufriedenstellend arbeiteten. So sollten flächendeckend Appliances im Netzwerk verteilt werden, die den Traffic von unerwünschten Systemen blocken, Software auf allen Clients installiert werden, die nur die Kommunikation zu eigenen Geräten erlauben oder die Infrastruktur aufwendig auf Komponenten eines Herstellers umgerüstet werden. Die hohen Aufwände und auch die Kosten für solche Implementierungen führten fast zwangsläufig zum Scheitern der Projekte und auch zu einem negativen Touch des gesamten Themas.

- Heute geht es besser!

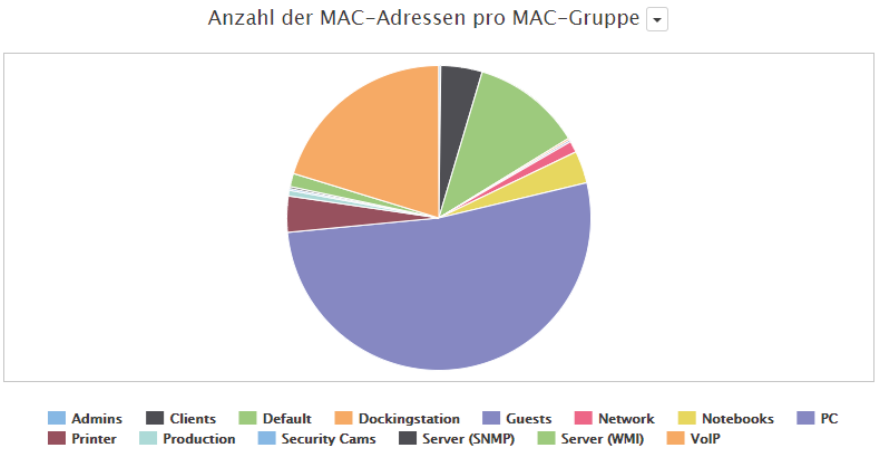
Neue und alte, aber dafür gereifte Technologien bieten heute die Möglichkeit, eine Kontrolle und damit eine zentrale Sicherheitsinstanz einzuführen. Das bestehende Netzwerk muss nicht angepasst werden, es stehen keine hohen Investitionen an und der Aufwand ist absolut überschaubar. Doch bevor wir auf Lösungsstrategien eingehen, lassen Sie uns die aktuellen Anforderungen an Network Access Control und Einsatz-Szenarien betrachten:

Aktuelle Anforderungen an NAC und Einsatz-Szenarien:

1. Übersicht und Kontrolle aller Netzwerkzugänge

Wichtig ist, dass die eingesetzte Lösung nicht nur den Zugriff kontrolliert, sondern auch zu einem signifikanten Anstieg der Transparenz im eigenen Netzwerk führt. Nur wenn bekannt ist, was genau und wo genau vorhanden und zugelassen ist, kann effektiv auf unbekannte und unerwünschte Systeme und Komponenten reagiert werden.

- Mitarbeiter dürfen nicht mehr unbemerkt fremde Geräte anschließen.
- Besucher dürfen nicht mehr einfach zugängliche Netzwerkzugänge nutzen.
- Nutzen Angreifer die unwissenden Mitarbeiter aus und tarnen sich z.B. als Servicetechniker im Blaumann, dürfen trotzdem keine Geräte wie z.B. Drucker, unbemerkt eingebracht oder getauscht werden.



2. **Vollständige Unabhängigkeit von den eingesetzten Betriebssystemen**
   - Schnell sind neue Betriebssysteme wie iOS oder Android aufgetaucht und jederzeit können neue dazu kommen. NAC muss unabhängig von den Endgeräten funktionieren und damit auch neue Geräte und „einfache" Geräte wie Drucker, etc. abdecken.
   - Da es unwahrscheinlich ist, Agenten für alle Betriebssysteme vorzuhalten, ist die vollständig agentenlose Variante auf jeden Fall vorzuziehen.

3. **Unabhängigkeit von den eingesetzten Netzwerk-Komponenten**
   - Heute sind vielleicht Cisco, HP, Nexan und Microsens im Einsatz, aber welche Switches oder Router sind es morgen?
   - Auch das vollständige Tauschen und Herstellen einer homogenen Umgebung darf keine Option sein, um sich nicht vollständig abhängig zu machen.
   - Auch alte Geräte sollten unterstützt werden – niemand darf erwarten, dass Komponenten, die noch einwandfrei funktionieren, getauscht werden.

4. **Erhalten und Erhöhen der Flexibilität für kurzfristige Zugangsanforderungen**
   - Spontane Besucher (Dienstleister, etc.) müssen weiterhin auch spontan Internetzugriff oder sogar Zugriff auf das produktive Netzwerk erhalten können.
   - Auch intern kann die Anforderung bestehen, kurzfristig Geräte zuzulassen.
   - Nicht mehr genutzte Geräte sollten auffindbar sein, um zu entscheiden, ob das Zugriffsrecht erhalten bleiben soll, oder nicht.

5. **Minimaler Pflegeaufwand**
   - Jedes Unternehmen und jede IT-Abteilung hat ohnehin bereits genug zu tun und genügend Aufgaben. Die Pflege der NAC-Lösung muss sich auf ein Minimum reduzieren und zu einem großen Teil automatisiert erfolgen.
   - Auch die Pflege der zugelassenen Systeme muss „nebenbei" erfolgen können.
   - Idealerweise nimmt NAC Ihnen sogar sehr viel Arbeit ab.

6. **Zukunftssichere Technologien**
    - Wie eingangs beschrieben, gibt es verschiedene technologische Ansätze. Es sollte darauf geachtet werden, dass die Lösung Technologien einsetzt, die heute funktionieren, aber auch morgen.
    - Idealerweise sind verschiedene Technologien implementiert, um möglichst flexibel in der Art des Einsatzes zu sein.

All diese Anforderungen können durch heute verfügbare Produkte bereits erfüllt werden. Die Lösung macmon bietet dabei vor allem den Vorzug, auf gereifte und auf neue Technologien zu setzen, die Ihnen als Anwender dann intelligent einfach zur Verfügung stehen.

So besteht die gereifte Technologie vor allem darin, per SNMP mit allen Switches und Routern in Ihrem Netzwerk zu kommunizieren – unabhängig, von welchem Hersteller die Komponenten sind. Durch diese direkte Kommunikation mit der vordersten Front, erhalten Sie eine vollständige Netzwerkübersicht und die Gewissheit, dass nicht Teilbereiche ausgelassen werden, weil beispielsweise nicht genügend Appliances verteilt wurden.

macmon arbeitet von zentraler Stelle mit einem zentralen Server und kann von dieser Position heraus das gesamte Netzwerk auch mit verschiedenen Standorten abdecken. Neue Geräte werden sofort erkannt und anhand des eigenen und flexiblen Regelwerkes behandelt. Des Weiteren ist ein RADIUS-Server implementiert, um auch den Industriestandard IEEE 802.1X bedienen zu können. Modernere Netzwerkbereiche können damit auch durch diese „neue" Technologie abgedeckt werden – je nach der Beschaffenheit Ihres Netzwerkes und das auch im gemischten Betrieb.
Anpassungen sind damit definitiv unnötig. Hohe Investitionskosten entstehen nicht und die Einführung ist an einem oder in wenigen Tagen (je nach Netzwerkgröße) umgesetzt. Zusätzlich entstehen weitere Mehrwerte durch die Einführung von macmon.

Mehrwerte durch die Einführung von macmon

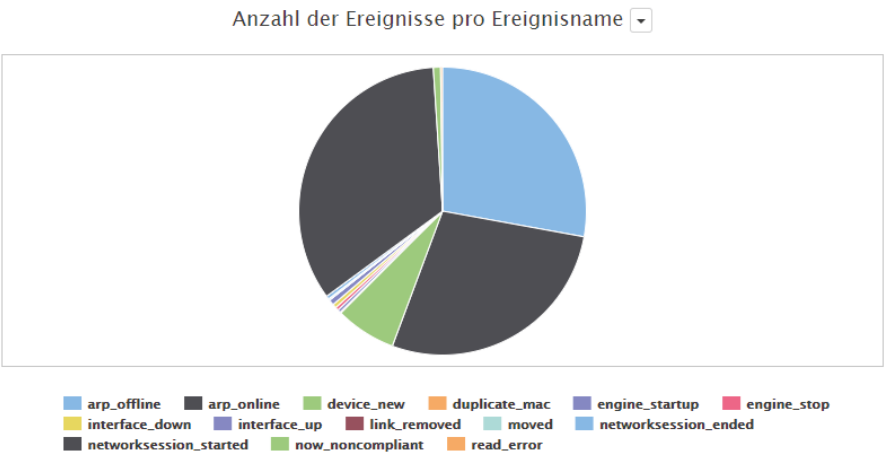
1. **Reduzieren von administrativem Aufwand**
    - Geräte innerhalb des Netzwerkes finden ist eine Kleinigkeit. Je Gerät stehen die Informationen zur Verfügung, an welchem Switch und an welchem Port oder an welchem Access-Point im WLAN es betrieben wird.
    - Tägliche Netzwerkaufgaben, wie beispielweise das manuelle Patchen von Switchports entfallen, da das dynamische VLAN-Management die Ports automatisch so konfiguriert, dass alle Geräte in das hinterlegte VLAN sortiert werden.
    - macmon hilft, statt Aufwand zu erzeugen.

2. **Live-Bestandsmanagement**
    - macmon hält ein stets aktuelles Live-Bestandsmanagement vor, das optimal zur Weitergabe an andere Systeme genutzt werden kann. CMDBs wie die uniDB oder auch Notfallmanagement-Lösungen wie INDART Professional können so stets aktuell gehalten werden.
    - Die Daten können über verschiedene Schnittstellen einfach angezapft werden.

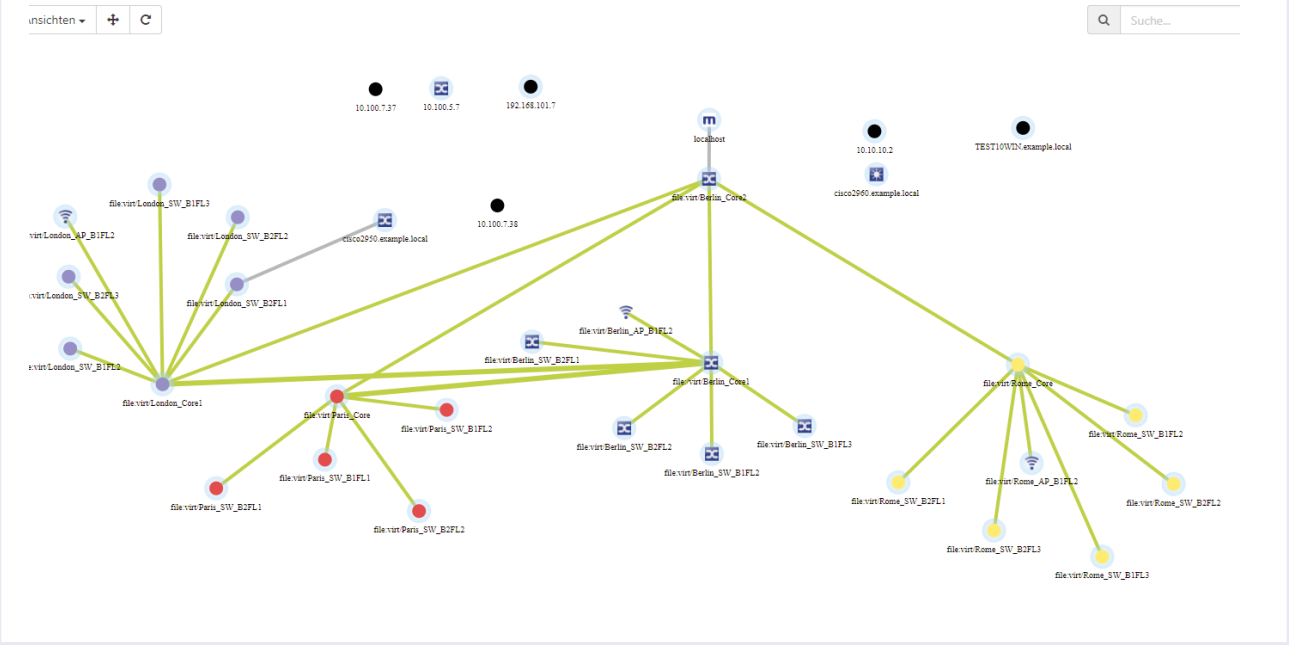
3. **Integration mit beliebigen anderen Produkten zur Steigerung der Effizienz**
    - macmon kann über eine Vielzahl von Schnittstellen nicht nur Informationen bereitstellen, sondern auch Befehle empfangen. Das ermöglicht das automatisierte Isolieren von Gefahrenquellen oder auch die Schaffung eines zentralen Compliance-Status mit automatisierter Behandlung von Geräten, die nicht den Sicherheitsanforderungen entsprechen.
    - Anbinden von beispielsweise WSUS, SCCM, AntiVirus, Schwachstellenmanagement, etc.

4. **Zentrale Macht im Netzwerk**
   - Durch die zentrale Position und die Macht über alle Netzwerkzugänge kann macmon einfach als zentrale Macht genutzt werden. Unerwünschte Systeme kommen gar nicht erst ins Netzwerk und bereits zugelassene, aber gefährliche oder angreifende Systeme, können eventbasiert wieder ausgesperrt werden.
   - macmon NAC ist damit die effizienteste Lösung zur Richtliniendurchsetzung.

5. **Einfache und schnelle Netzwerkfehler-Analyse**
   - Geräte finden ist, wie schon beschrieben, sehr einfach möglich.
   - Ungenutzte Switchports sowie die Konfiguration und den Durchsatz sehen Sie auf einem Blick.
   - Unerwünscht mehrfach genutzte Ports fallen ebenfalls direkt auf.
   - Vollständige Netzwerkübersicht durch Darstellung der Topologie.



6. **Grafische Visualisierung des gesamten Netzwerkes**
   - Darstellung der Topologie inklusive aller Nachbarschaftsinformationen.
   - Selektion und Hervorhebung anhand verschiedener Filterkriterien.
   - Visualisierung von Engpässen und Schwachstellen der Netzwerkstruktur.



7. **Kostenersparnis durch Verwendung von dem, was gegeben ist**
   - Keine neue Infrastruktur anschaffen.
   - Keine neuen Endgeräte anschaffen.
   - Kein Wechsel von bestehenden Betriebssystemen.
   - Kein Wechsel der bestehenden Netzwerkbeschaffenheit.
   - macmon passt sich auf Sie an – und nicht umgekehrt.

8. **Gästeportal zum geregelten und einfachen Zulassen von Gästen**
   - Gewähren von zeitlich befristeten und nachverfolgbaren Zugängen durch ein komfortables Voucher System.
   - Einfaches Customizing der Portalseite auf das Firmendesign.
   - Unterscheidung der Zugriffsart je nach zugewiesener Gruppe.
     - Gäste nur im Internet
     - Dienstleister im entsprechenden Produktiv-LAN
     - Mitarbeiter mit eigenen Geräten im BYOD-LAN

Zusammenfassend lässt sich sagen, dass auf Basis definierter Anforderungen und dank eines einfachen Konzeptes eine schnelle NAC-Einführung und -Umsetzung möglich ist. Nutzen Sie die Chance, auf eine moderne Technologie und Lösung zu setzen, die Ihre Unternehmenssicherheit erhöht und gleichzeitig verschiedene Vereinfachungen und Vorteile mit sich bringt.

macmon secure GmbH – der Technologieführer für Ihre Netzwerksicherheit

Die macmon secure GmbH beschäftigt sich seit 2003 mit der Entwicklung von Netzwerksicherheitssoftware und hat ihren Firmensitz im Herzen Berlins. Die Network Access Control (NAC) Lösung macmon wird vollständig in Deutschland entwickelt und weltweit eingesetzt, um Netzwerke vor unberechtigten Zugriffen zu schützen.

Die Kunden von macmon secure kommen aus diversen Branchen und reichen von mittelständischen Firmen bis hin zu großen internationalen Konzernen.

Das Ziel: Jedem Unternehmen eine flexible und effiziente NAC-Lösung anzubieten, die mit geringem Aufwand, aber erheblichem Mehrwert für die Netzwerksicherheit des Unternehmens implementiert werden kann. macmon secure ist Mitglied der Trusted Computing Group und aktiv an verschiedenen Forschungsprojekten beteiligt.

macmon NAC – intelligent einfach!

Kontakt

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