macmon 802.1X

802.1X - „out of the Box“

Das Institute of Electrical and Electronics Engineers (IEEE) ist ein weltweiter Verband mit Gremien für die Standardisierung von Techniken, Hardware und Software. Der Standard 802.1X wurde bereits mehrfach überarbeitet und erneuert und stellt eine sehr ausgereifte Empfehlung zur sicheren Authentifizierung von Geräten in Netzwerken dar. macmon unterstützt diesen Standard und erleichtert die Einführung und den Betrieb.

Möglichkeiten von IEEE 802.1X

Die Thematik, sowohl im kabellosen als auch im kabelgebundenen Netzwerk für eine eindeutige Authentifizierung der Endgeräte zu sorgen, ist bekannt. Bei technisch relativ einfach umzusetzenden Verfahren, wie der Kontrolle der MAC-Adressen, wird häufig argumentiert, dass die Systemeigenschaften zu leicht zu fälschen sind. macmon hat daher bereits in der grundsätzlichen Technologie weitaus mehr Eigenschaften als nur die MAC-Adresse zur Identifizierung herangezogen und kann so einen Footprint der Systeme überprüfen (unter anderem IP-Adresse, Betriebssystem, IP-Ports) – alle auf einmal zu fälschen erfordert bereits ein sehr hohes Maß an krimineller Energie.

Key facts

- ✓ Nutzung eines offenen Standards kombiniert mit Best Practice
- ✓ Möglichkeit des gemischten Betriebs - mit und ohne 802.1X
- ✓ Geräteortung durch Kommunikation mit den Switches und Access Points
- ✓ Anbindung von AD/ LDAP und weiteren Identitätsquellen
- ✓ Dynamisches & automatisches Regelwerk
- ✓ Einfach in der Implementierung und im Betrieb
- ✓ Gruppenbasierte Konfiguration statt umfangreichem Regelwerk
- ✓ Etablierung und Umsetzung von Konzepten für Sicherheitszonen

Noch einen Schritt weiter kann allerdings der Standard 802.1X gehen. Hier wird für die Authentifizierung ein RADIUS-Server mit einbezogen, der die Entscheidung über das Gewähren des Zugangs trifft. Als Ausweis bzw. Authentifizierungsmittel können dabei verschiedene Eigenschaften, wie die MAC-Adresse, Benutzername/ Passwort oder Zertifikat zum Einsatz gebracht werden. Da der Zugang zum Netzwerk durch den Switch erst nach erfolgter Bestätigung durch den RADIUS-Server erfolgt, gibt es keine ungenutzten oder unsicheren Ports, wie es auch vom BSI empfohlen wird.

Mit der Gewährung des Zugangs können zusätzliche Regeln mitgegeben werden, die vom Switch umgesetzt werden. Ist der Switch technisch dazu in der Lage (Layer 3), können so ein bestimmtes VLAN, definierte ACLs oder nahezu beliebige weitere Attribute vergeben werden.

Umsetzung von IEEE 802.1X

Die Einführung eines so leistungsfähigen und differenzierten Zugangsschutzes erfordert eine sorgfältige Planung. Die Nutzung des Standards ist sinnvoll, da immer mehr Komponenten, wie die verschiedenen Endgeräte aber auch die Switche, die Anforderungen erfüllen. Zu beachten ist allerdings, dass der Einsatz von 802.1X nicht per se sicher ist, sondern auch hier unterschiedliche Möglichkeiten existieren, die Identität des Endgerätes festzustellen, was unterschiedliche Sicherheitslevel nach sich zieht.

Dient lediglich die MAC-Adresse als Ausweis, so ist eine Fälschung sehr einfach möglich und der Sicherheitszugewinn durch die Einführung eher fraglich. Mit macmon Network-Access-Control kann die MAC-Adresse für die Authentifizierung verwendet werden, während zusätzlich der bereits oben erwähnte Footprint genutzt wird, um Eindringlinge mit gefälschter MAC-Adresse wieder vom Netzwerk auszusperren. Auf diese Weise können auch Endgeräte, die nicht in der Lage sind höherwertige Ausweise zu liefern möglichst sicher integriert werden.

Die höchste Sicherheit in Verbindung mit 802.1X wird erreicht, wenn für die Authentifizierung Zertifikate zum Einsatz kommen. Für die verwendeten Zertifikate muss jedoch wiederum eine entsprechende Infrastruktur geschaffen werden, um mittels dieser PKI (Public Key Infrastructure) die Zertifikate zu verwalten und auch deren Gültigkeit zu überwachen.

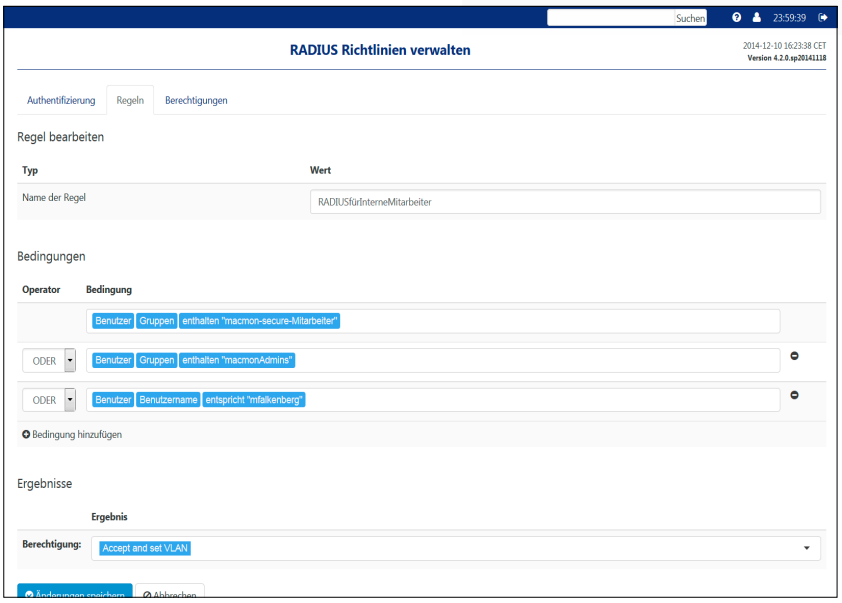
Häufig ist daher die mittlere Sicherheitsstufe ein sehr guter Kompromiss zwischen dem höchsten Ziel und dem damit verbundenen Aufwand. Benutzername und Passwort sind jedoch bereits sehr hochwertige Authentifizierungsmittel, so dass je nach Einsatz nichts gegen die Nutzung spricht. Nun kann natürlich nicht jedes Gerät mit einem eigenen Benutzernamen und

Passwort versehen werden, ohne erheblichen Aufwand zu verursachen.

macmon bietet daher verschiedene Varianten, um bereits bestehende Mittel zu verwenden und den Aufwand zu minimieren. So können mittels der Active Directory Anbindung die Konten aller im Verzeichnisdienst bereits enthaltenen Geräte (und auf Wunsch auch der Benutzer) zur Authentifizierung verwendet werden. Einzelnen Geräten, die nicht enthalten sind, können separate Zugangsdaten gegeben werden. Gruppen von gesonderten Systemen, wie z.B. VoIP Telefonen, können Zugangsdaten gegeben werden.

Entscheidend ist dabei jedoch, dass auch diese erweiterte Möglichkeit innerhalb von macmon wieder intelligent einfach umgesetzt wurde. So können nahezu beliebige Identitätsquellen wie AD, LDAP oder Datenbanken zur Überprüfung von Identitäten live angebunden werden, während sich das Regelwerk im Hintergrund automatisch erstellt. Durch eine einfache Zuweisung der Gruppen aus z.B. dem Active Directory zu den macmon Gerätegruppen ist eine erheblich vereinfachte Konfiguration möglich. macmon erstellt anhand der Gruppenkonfigurationen automatisch die notwendigen RADIUS-Regeln und bietet zusätzlich durch einen geführten Regel-Editor jederzeit die Möglichkeit, beliebige Ausnahmen zu definieren. Doch das ist bereits der Unterschied –
Sie definieren nur noch die Ausnahmen…

Mit macmon vereinfachen Sie die Umsetzung von 802.1X um ein Vielfaches und decken gleichzeitig die Bereiche Ihres Netzwerkes mit ab, die noch nicht 802.1X-fähig sind.



Auch eine schrittweise Implementierung sowie ein gemischter Betrieb, sind so ohne weiteres möglich.

Die Nutzung Ihrer bestehenden Infrastruktur und Ihrer bestehenden Unternehmensidentitäten, das intuitive und selbstgenerierende Regelwerk zusammen mit dem geräte- und gruppenbezogenen Ansatz von macmon, sowie eine Reihe weiterer Vereinfachungen führen dazu, dass ein eigentlich komplexer Sicherheitsstandard so einfach und schnell wie nur möglich, erfolgreich umgesetzt werden kann.
macmon macht es anders –
testen Sie uns!

Die Identifizierung und Authentifizierung der Geräte in Ihrem Netzwerk erfolgt mit macmon ganz nach den Gegebenheiten und Möglichkeiten Ihrer Infrastruktur. macmon ist sogar in der Lage, selbständig den 802.1X-Modus am Switch zu aktivieren und zu deaktivieren. Damit besteht nicht mehr die Notwendigkeit, starr festzulegen, in welchen Netzwerkbereichen Sie 802.1X verwenden möchten und in welchen nicht –
macmon konfiguriert Ihre Switche anhand der Gruppenkonfiguration automatisch.

Von der MAC-Adresse kombiniert mit weiteren Systeminformationen, bis hin zum Industriestandard IEEE 802.1X mit seinen verschiedenen Ausprägungen (MAC-Address Bypass, Benutzername/Passwort, AD/LDAP oder Zertifikat), sind im macmon network bundle alle Möglichkeiten enthalten.

Für noch höhere Sicherheitsanforderungen bieten wir separat das Modul macmon TP (Authentifizierung durch den TPM-Chip) an.

macmon secure gmbh
Charlottenstraße 16
D-10117 Berlin
Telefon +49 30 2325 777-0
Telefax +49 30 2325 777-200
vertrieb@macmon.eu
www.macmon.eu

Ihr Ansprechpartner: