ARP GUARD by ISL

Network Access Control (NAC)
mit ARP-GUARD

Effizient und wirtschaftlich.

Lösungen für komplexe Rechner - Netzwerke.

GORDION®

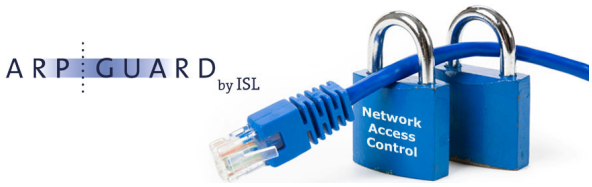
GORDION
Data Systems Technology GmbH
Mottmannstraße 13
53842 Troisdorf

Telefon: 02241 49040
Telefax: 02241 490490

Email: info@gordion.de
Internet: www.gordion.de

Network Access Control (NAC) mit ARP-GUARD

Es gibt gute Gründe für eine Netzwerk-Zugangskontrolle (NAC).
Doch welches Verfahren ist effizient und wirtschaftlich sinnvoll?



Die NAC-Lösung „ARP-GUARD“ der Hagener Firma ISL nutzt u.a. einen Geräte-Fingerprint und erreicht die gewünschte Sicherheit mit einem überschaubaren Aufwand in nur wenigen Tagen.

Von Oliver Lindlar und Mirco Jakuszeit, GORDION.

Eine Zugangskontrolle zum Unternehmensnetz wird heutzutage immer wichtiger. Genau wie bei Personen, die mit Ausweis versehen nur dann eingelassen werden, wenn sie eingeladen wurden, sollte man auch bei Notebooks, mobilen Geräten und jeder Form von Netzwerkkomponenten nur erwünschte Geräte zulassen. Der Artikel beleuchtet verschiedene Ansätze zu NAC und zeigt auf, warum eine Zugangskontrolle zum Netz mittels ARP-GUARD sicher, effizient und wirtschaftlich zu realisieren ist.

Zugangskontrolle „nur anhand der MAC“ bietet niedrige Sicherheit

Eine einfache Form von Network Access Control stellt die Zugangskontrolle per *Media Access Control (MAC)*-Adresse dar. Da die MAC-Adresse auf jedem Endgerät weltweit eindeutig ist, können Endgeräte anhand ihrer MAC klar identifiziert werden. Managebare Router und Switches unterstützen i.d.R. zwei Verfahren zur Umsetzung einer MAC-Identifizierung: mit dem *Simple Network Management Protocol (SNMP)* steht eine reaktive Variante zur Verfügung, während mittels des *Remote Authentication Dial-In User Service (RADIUS)* eine proaktive Alternative genutzt werden kann, welche jedoch ausfallsicher betrieben werden sollte.

Unter wirtschaftlicher Betrachtung schneidet die Zugangskontrolle „nur per MAC“ jedoch eher mittelmäßig ab. Die notwendigen managebaren Switches stehen zwar oftmals bereits in der IT-Infrastruktur zur Verfügung, der entsprechende Aufwand zur Administration und Pflege der MAC-Adressen ist jedoch sehr hoch. Problematisch ist zudem, dass MAC-Adressen leicht gefälscht werden können (*MAC-Spoofing*), sodass die erreichbare Sicherheit eher niedrig ist [1].

Zugangskontrolle per IEEE 802.1X ist sehr aufwändig

Mit *IEEE 802.1X* (Port Based Network Access Control) steht ein internationaler Standard zur Port-basierten Zugangskontrolle in Netzen zur Verfügung, welcher insbesondere das *Extensible Authentication Protocol (over LAN) [EAP(OL)]* sowie *RADIUS* mit einbezieht. Vorteil: EAP nutzt zur Authentisierung (und ggf. auch zur Verschlüsselung) kryptographische Protokolle. Dies macht das Verfahren sicher. Im Wireless LAN (WLAN)-Bereich ist dies sehr gut gelöst, da EAP hier neben der Authentisierung (möglichst gegenseitig und mit Zertifikaten) und einem authentischen Schlüsselaustausch insbesondere auch die Verschlüsselung der Nutzdaten zwischen Endgerät und Access Point ermöglicht. In kabelgebundenen Netzen, in denen Switches mit Kuper- oder Glasfaserkabeln operieren, ist eine solche Verschlüsselung i.d.R. nicht machbar. Denn die Rechenleistung (CPU) der Switches ist nicht dafür ausgelegt, z.B. Datenströme von 24 mal 1Gbps zu verschlüsseln. Daher hat man hier auf einen Schlüsselaustausch verzichtet und beschränkt sich auf eine reine Authentisierung.

[1] Einem Angreifer ist es leicht möglich, sich gegenüber dem Netz mit einer anderen MAC-Adresse zu „maskieren“. Mit Verwendung dieser manipulierten MAC-Adresse, dem sogenannten *MAC-Spoofing*, erscheint er wie „verkleidet“ im Netz, im Prinzip als jemand anderes respektive als eine andere Hardware. Dies ist insbesondere problematisch bei Anschlüssen von Netzwerk-Druckern. Diese sind wie PCs offizielle Teilnehmer im Netz und werden ebenfalls durch ihre (weltweit) eindeutige MAC-Adresse identifiziert. Drucker jedoch bieten auch einem fremden Dritten alle notwendigen Informationen zum Netz (IP-Adresse, Gateway etc.), sodass er per MAC-Spoofing mit seinem Notebook unerlaubt und „verkleidet als Drucker“ Zutritt ins Netz erlangen kann.

Der 802.1X-Standard wird jedoch von vielen älteren Endgeräten nicht unterstützt. Diese werden dann (nur) anhand ihrer MAC-Adresse identifiziert. Moderne Geräte unterstützen meist 802.1X, allerdings erfordert der Standard einen hohen zeitlichen Aufwand. Denn für jedes Endgerät müssen Zertifikate generiert, ausgerollt und gepflegt werden. Dies ist zwar z.B. für Windows-Endgeräte relativ leicht möglich, jedoch nicht für Drucker, VoIP-Telefone, Produktionsmaschinen, Videokameras u.v.a. Geräte mit einem Zugang zum Netz.

Bei einem Defekt muss zudem das alte Zertifikat widerrufen, ein neues Zertifikat generiert, an den Standort übertragen und dort auf das Ersatzgerät aufgespielt werden. Hinzu kommt die Tatsache, dass 802.1X im kabelgebundenen LAN ebenso Angriffspunkte bietet wie eine Zugriffskontrolle nur per MAC. Denn mit Hilfe eines simplen Hubs kann das Verfahren mittels *Session Hijacking* umgangen werden. Es gibt zwar Weiterentwicklungen, wie z.B. MACsec, jedoch macht dies die Sache noch aufwändiger und ist zudem kaum verbreitet. In einer wirtschaftlichen Betrachtung drängt sich daher die Frage auf, ob ein derartiger Aufwand überhaupt empfehlenswert ist für eine funktionierende Zugangskontrolle.

Zugangskontrolle mit ARP-GUARD nutzt Fingerprinting und reduziert Aufwand erheblich

Man könnte doch z.B. zur Identifizierung solche kryptographischen Zertifikate/Schlüssel/Signaturen nutzen, welche bereits auf den Endgeräten aktiv sind. Dies würde den Aufwand erheblich reduzieren. Die Zugangskontrolle „ARP-GUARD“, entwickelt von der Hagener Firma *ISL*, hat diesen pragmatischen Ansatz verfolgt und bietet ein eigenentwickeltes *Fingerprinting*, welches zunächst nach bereits vorhandenen bzw. aktiven Zertifikaten/Schlüsseln/Signaturen auf den Endgeräten sucht und diese als Referenzwert in einer Datenbank speichert. Sollte dasselbe Endgerät nochmals im Netz aktiv werden, wird erneut ein Fingerprint vom Endgerät heruntergeladen und mit dem Referenzwert verglichen. Bei Nicht-Übereinstimmung mit der Referenz in der Datenbank wird das Gerät aus dem Netzwerk entfernt. Selbst für Endgeräte, welche keine kryptographische Verfahren unterstützen (z.B. Drucker), können zumindest noch vereinfachte Fingerprints genutzt werden (z.B. eine Liste der offenen TCP-Ports), sodass die erzielbare Sicherheit immer noch weit über eine einfache MAC-Adressen-Prüfung hinausgeht. Das Fingerprinting ist dabei nicht nur auf Windows-Komponenten begrenzt. Auch Linux-Geräte, VoIP-Telefone, Drucker u.v.a. Endgeräte können per Fingerprinting identifiziert werden [2].

Die ARP-GUARD-Lösung arbeitet Client-, Plattform- und Hersteller-unabhängig, bietet ein dynamisches VLAN-Management und integriert insbesondere auch ältere und solche Geräte, welche nicht 802.1X-tauglich sind. Beim Fingerprinting sind zwar im Prinzip ebenfalls Session Hijacking Attacken möglich wie bei 802.1X, das ARP-GUARD-System prüft jedoch noch zahlreiche weitere Bedingungen für den Netzzugang (u.a. auf der Basis von IP-Adressen) und bietet dadurch ein deutlich höheres Sicherheitsniveau.

NAC-Realisierung mit ARP-GUARD in wenigen Tagen

Das Erlernen der zugelassenen MAC-Adressen, das Hinterlegen der korrelierenden Fingerprints in der System-Datenbank, das Erstellen von Regeln und schliesslich das „Scharfschalten“ der ARP-GUARD-Lösung benötigt dabei nur wenige Manntage. Die Kosten für die ARP-GUARD-Lösung sowie deren Pflegeaufwand sind überschaubar [3]. Selbst Kunden mit deutlich über 5.000 MAC-Adressen im Netzwerk berichten von einem Pflegeaufwand von lediglich fünf Minuten pro Tag. Somit bietet die ARP-GUARD-Lösung auch unter wirtschaftlicher Betrachtung deutliche Vorteile.

Nachfolgende Tabelle skizziert die verschiedenen Ansätze anhand der Kriterien Nutzen, Anschaffungskosten sowie dem Aufwand für Realisation und Betrieb. Für den Einsatz in der Praxis ist insbesondere die Wirtschaftlichkeit von Lösungen relevant, welche oft am Kosten/Nutzen-Verhältnis gemessen wird. Die Kosten beziehen sich hier nicht nur auf die Beschaffungskosten, sondern insbesondere auch auf laufende Kosten (z.B. für die Administration & Pflege), während der Nutzen hauptsächlich in der erreichbaren Sicherheit und Arbeitserleichterung dargestellt wird.

[2] So nutzen Linux-Geräte i.d.R den SSH- oder VoIP-Telefone den HTTPS-Dienst, welche sogar einen kryptographischen Fingerprint ermöglichen.

[3] Benötigt werden ein ARP-GUARD Management-System (welches gleichzeitig auch als Sensor arbeiten kann) sowie eine entsprechende Anzahl von Lizenzen, welche mit der Summe der MAC-Adressen im Netz korreliert. Zudem gibt es ein funktionales Lizenzmodell, sodass (je nach Wunsch und Priorität) auch nur Teilfunktionen gebucht werden können. Eventuell zusätzlich benötigte Software-Sensoren sind kostenlos, z.B. für das Monitoring von kleineren Außenstellen (vgl. www.gordion.de).

	Nutzen / Leistung / Sicherheit	Kosten / Preis	Zeitlicher Aufwand für Realisation & Betrieb	Wirtschaftlichkeit
Zugangskontrolle nur per MAC	Niedrig	Niedrig	Mittel	+ +
802.1X	Mittel	Hoch	Hoch	+
ARP-GUARD, u.a. mit Fingerprinting	Hoch	Mittel	Niedrig	+ + +

Tabelle: Übersicht verschiedener Verfahren zur Netzwerk-Zugangskontrolle im kabelgebundenen LAN

Zusammenfassung

Eine Zugangskontrolle sollte ein Unternehmensnetz schützen und unerwünschten Geräten (und Angreifern) keinen Zutritt ermöglichen. 802.1X, RADIUS und EAP stellen hierbei ein sehr komplexes Thema dar, bei dem insbesondere Details eine wichtige Rolle spielen. Im kabelgebundenen LAN ist die Wirtschaftlichkeit aufgrund der hohen Kosten und einer mittelmäßigen Sicherheit allerdings eher schlecht. Das ARP-GUARD-System bietet dagegen u.a. eine Fingerprinting-Lösung, welche auch den Einbezug von älteren und nicht Windows-basierten Endgeräten ermöglicht. ARP-GUARD bietet darüber hinaus ein dynamisches VLAN-Management, eine Anzahl erweiterter Sicherheitsfeatures und ist Client-, Plattform- und Hersteller-unabhängig. Der Pflegeaufwand liegt im einstelligen Minutenbereich pro Tag, eine Integration ist in wenigen Manntagen realisierbar. ARP-GUARD ist seit 2003 verfügbar und branchenübergreifend im Einsatz, darunter auch in über 80 Sparkassen, in Krankenhäusern, in Ministerien und im Produktionsumfeld.

Weitere Informationen

www.gordion.de • www.arp-guard.com