ARP-GUARD

Schutzschild gegen interne Bedrohungen im Netz.

Network Access Control (NAC)

Layer-2 IPS

Netzmanagement

Endpoint Security

GORDION®

Lösungen für komplexe Rechner - Netzwerke.

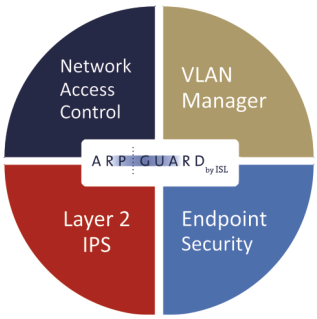
GORDION
Data Systems Technology GmbH
Mottmannstraße 13
53842 Troisdorf

Telefon: 02241 49040

Email: info@gordion.de

Internet: www.gordion.de

ARP-GUARD



Der Motorenhersteller DEUTZ AG schützt sich mit *ARP-GUARD* vor fremden Geräten und möglichen internen Bedrohungen im LAN.

Die Security Lösung *ARP-GUARD* des deutschen Herstellers *ISL GmbH* bietet Network Access Control (NAC), Layer-2 IPS, Network Management und Endpoint Security

Von Oliver Lindlar und Mirco Jakuszeit, GORDION.

Natürlich werden Rechner-Netzwerke (LANs) heutzutage gegen externe Bedrohungen wie Viren, Würmer, Trojaner und fremde Zugriffe geschützt. Hier stehen Investitionen für Firewalls und Security Gateway Systeme im Vordergrund. Der Schutz gegen interne Bedrohungen im Netz steht dagegen nicht selten nur in der zweiten Reihe.

Der Artikel beschreibt das Potential möglicher interner Bedrohungen im Netz und zeigt auf, wie man sein Netz mittels ARP-GUARD einfach und effizient dagegen schützen kann. Einer unserer Referenzkunden zu dieser Lösung ist der Kölner Motorenbauer DEUTZ AG.

Zunehmende Gefahr von internen Angriffen

Ein hochverfügbares Rechner-Netzwerk als Kommunikations-Infrastruktur ist heutzutage die notwendige Voraussetzung für einen reibungslosen Ablauf der Geschäftsprozesse. Die lokalen Netze basieren dabei auf Ethernet und TCP/IP und sind Verbindungsglied für PCs und Server respektive für die Applikationen und deren Zugriff auf die Daten(banken). Der Zugriff auf diese Daten sollte jedoch reglementiert sein, insbesondere müssen unberechtigte Zugriffe verhindert werden. Den externen Schutz nach außen übernehmen hier Firewalls und Security Gateway Systeme. Des Weiteren unterstützen Intrusion Detection- (IDS-), Intrusion Prevention- (IPS)- und Virenschutz-Systeme, welche jedoch für einen internen Schutz nicht immer ausreichend sind. Dabei entwickeln sich Gefahr und Schäden von internen Angriffen zunehmend, korrelierend mit der Digitalisierung der Prozesse.

Betroffen sind alle Unternehmen und Organisationen, welche sensible Daten verarbeiten. Im Prinzip kann jeder, der Zugang zum Netzwerk hat, interne Angriffe ausführen. Geeignete und leicht zu bedienende Angriffssoftware ist vielfach im Internet verfügbar. Angefangen bei der Erlangung von persönlichen Vorteilen, über Wirtschaftsspionage, Neugier, Erpressung, Sabotage und Mobbing bis hin zum Ehrgeiz von „Hobby-Hackern“ und Skript-„Kids“: an Motiven für Angriffe mangelt es nicht. Nicht zuletzt können Angriffe auch unabsichtlich und durch technische Unwissenheit erfolgen, z.B. durch Malware auf „verseuchten“ Notebooks von Gästen im Netz.

Bedrohung durch unerlaubte Zugriffe im internen Netz

Über das Netzwerk werden alle möglichen Inhalte in Form von digitalen Daten übertragen. Zum Beispiel Emails mit Dateien oder Tabellen, Inhalte von Datenbanken und Applikationen oder auch Telefonate (VoIP) und Videokonferenzen. Die Kommunikation im Netz verläuft dabei zwischen den digitalen Ressourcen (auf dem Server) und den Endgeräten (PC, Notebook, Drucker, Telefon etc.).

Ein interner Zugang zum Netz ist in der Regel durch zahlreiche Netzwerk-Anschlüsse (Ports) verfügbar:

- im Büro (PC oder VoIP-Telefon)
- im Konferenzraum
- am Drucker
- an sonstigen Endgeräten wie z.B. Produktionsmaschinen, Kopierern, Fax- und Erfassungsgeräten
- über Wireless LAN (WLAN)

Das Problem: es können sich auch fremde Dritte unerlaubt einen Zugang zu diesen „Netz-Eingängen“ verschaffen und dann eine Attacke ausüben. Neben den üblichen Schäden durch Viren, Würmer und Trojaner droht dann noch eine weitere Gefahr. Der Zugang von nicht autorisierten Dritten zur Kommunikation im Netz und deren Bedrohung, Daten abzuhören, zu manipulieren oder umzuleiten.

So gab es zum Beispiel den Fall in einer Bankfiliale, wo nach einem Einbruch nichts fehlte. Nur die Fensterscheibe war zerstört. Ein paar Wochen später bemerkte man dann

Anomalien in den Zahlungsanweisungen und etwas später bemerkte man auch den fremden Wireless Access Point unter einem Schreibtisch in der vermeintlich nicht beraubten Filiale. Die Einbrecher hatten sich per WLAN einen internen Zugang zum Banknetz verschafft.

Die Konsequenzen durch solche Angriffe sind natürlich unangenehm und zumeist geschäftsschädigend. Neben Imageschäden, Kosten und Wettbewerbsnachteilen drohen oft auch rechtliche Folgen und Haftungsprobleme.

Bedrohung durch interne Angriffe im Detail

Geplante Angriffe in den OSI-Layern 3-7 sind eher schwierig, denn sie erfordern ein tiefes Know-how und detaillierte Hintergrundinformationen. Zudem besteht ein Risiko einer Enttarnung (IDS/IPS), denn es werden Spuren hinterlassen.

Im OSI Layer 2 dagegen ist ein Angriff leicht durchführbar und ein tiefes Know-how dabei nicht zwingend erforderlich. Im Prinzip ist nur eine IP-Adresse notwendig und eine der leicht verfügbaren Angriffssoftwares. Spuren werden nicht hinterlassen, sodass kaum ein Risiko der Entdeckung besteht.

Ein Angreifer, der direkten Zugriff auf ein Netzwerk hat, kann eine Vielzahl von Attacken ausführen, z.B. *ARP-Spoofing / ARP-Poisoning- (Man-in-the-middle-)*, *MAC-Flooding-*, *IP- und MAC-Spoofing*-Angriffe.

Mit zu den gefährlichsten Angriffsszenarien zählen die sogenannten ARP- und MAC-Spoofing-Attacken, welche wir nachfolgend etwas näher beleuchten.

ARP und MAC

Ein Endgerät im lokalen Ethernet-Netzwerk wird anhand der weltweit eindeutigen (physikalischen) Adresse seiner Netzwerkkarte adressiert. Diese Hardware-Adresse bezeichnet man auch als *MAC-Adresse* (MAC ≡ Media Access Control).

ARP (Address Resolution Protocol) ist ein im Netzwerk notwendig genutztes Protokoll, welches die Zuordnung zwischen den Hardware-Adressen (MAC) und Protokoll-Adressen (IP) erbringt. Da ein Sender im Netz oft nur die IP-Adresse des Empfängers kennt, hilft das ARP-Protokoll, die gesuchte MAC-Adresse des Empfängers zu ermitteln. Diese MAC ↔ IP Adress-Zuordnungen werden in einer (ARP-) Tabelle im Endgerät gespeichert, um nicht bei jedem zu sendenden Paket erneut per ARP-Protokoll die MAC ↔ IP Adress-Zuordnung ermitteln zu müssen.

ARP-Spoofing (ARP-Poisoning) — Man-in-the-Middle

ARP-Spoofing-Angriffe (engl. „spoofing“ ≡ Manipulation) werden durchgeführt, indem mittels geeigneter Tools gefälschte ARP-Pakete erzeugt und gezielt an andere PCs im gleichen Subnetz gesendet werden. Eine besondere Form der ARP-Spoofing-Angriffe sind dabei die sogenannten *ARP-Poisoning*-Angriffe. Hierbei werden die ARP-Tabellen von anderen PCs gezielt manipuliert, mit dem Zweck, daß die Kommunikation zwischen zwei Computern über den Angreifer erfolgt. Er ist dann der sogenannte „*Man-in-the-Middle*“. Nachfolgende Abbildung-1 skizziert diese Vorgehensweise.

Mittels *ARP-Spoofing* (ARP-Poisoning) ist es somit möglich, Daten abzuhören, Passwörter zu sammeln sowie Daten zu manipulieren, zu blockieren oder umzuleiten. Dies ist oft auch bei verschlüsselten Verbindungen (SSH / SSL) machbar, da die notwendigen Zertifikate nicht immer ausreichend geprüft werden. Auch Telefonate (VoIP) können abgehört werden.

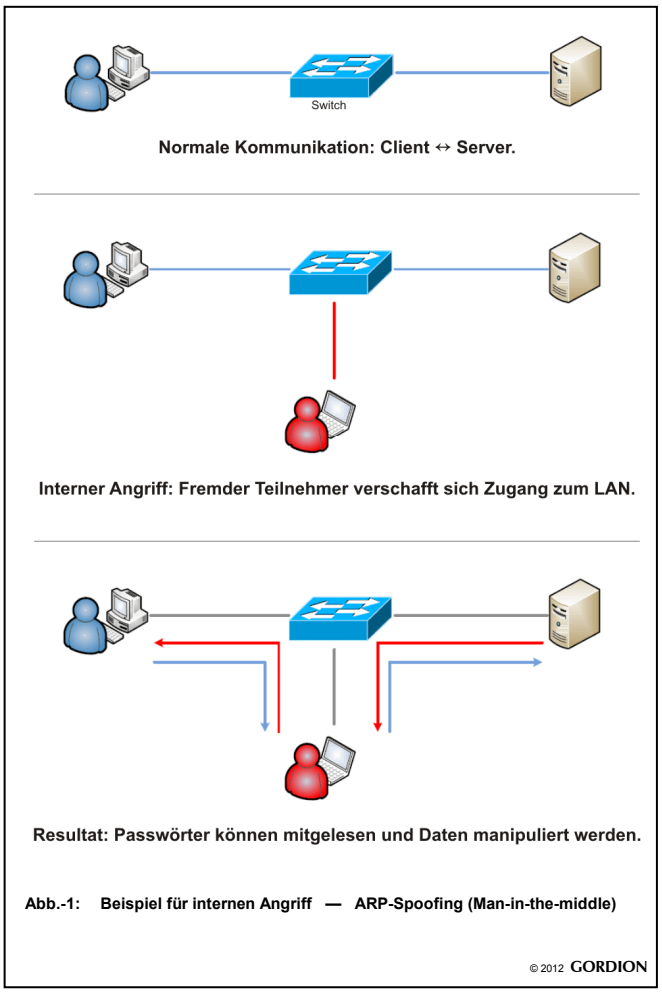


Abb.-1: Beispiel für internen Angriff — ARP-Spoofing (Man-in-the-middle)

MAC-Spoofing und MAC-Flooding

Mit Hilfe von geeigneten Tools ist es einem Angreifer möglich, sich gegenüber dem Netz mit einer anderen MAC-Adresse zu „maskieren“. Mit Verwendung dieser kopierten 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.

MAC-Flooding-Angriffe (engl. flooding ≡ Überflutung) werden mit dem Ziel geführt, die CAM-Tabellen des Switches zum Überlauf zu bringen. In den CAMs (Content Addressable Memory) sind MAC ↔ Switchport-Zuordnungen gespeichert, mit deren Hilfe ein Switch die für eine MAC adressierten Pakete nur auf dem Port weiterleitet, an welchem die Empfänger-MAC angeschlossen ist.

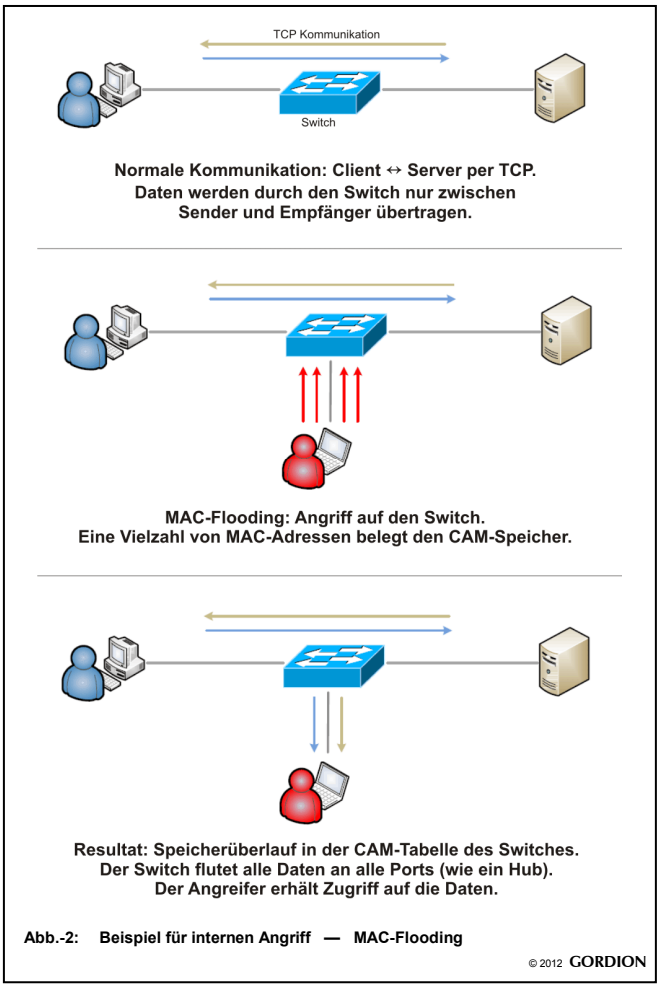


Abb.-2: Beispiel für internen Angriff — MAC-Flooding

Läuft der CAM-Speicher über, ist der Switch gezwungen, alle Daten an alle Ports weiterzuleiten (zu fluten). Der Switch verhält sich dann wie seinerzeit ein Hub und der Angreifer erhält Zugriff auf die Daten. Ein ähnliches Switch-Verhalten kann im Rahmen von Redundanz-Umschaltungen mit dem Spanning Tree Protokoll entstehen. In dessen Umschaltphase flutet der Switch ebenfalls alle Daten an alle Ports.

Fremde Hardware im Netz. Wie löst man das Problem?

Wie verhindert man interne Angriffe bzw. unerlaubte Hardware in seinem Netz? Und wie berücksichtigt man dabei unumgängliche, fremde Hardware im Netz, z.B. in Form von Notebooks von externen Beratern oder Besuchern im Konferenz- oder Besprechungsraum?

Die IT-Abteilung könnte jegliche fremde Hardware vorab analysieren, was jedoch sehr arbeitsaufwendig wäre und zudem ohne Admin-Rechte wenig sinnvoll. Auch Haftungserklärungen bieten keinen effektiven Schutz, ebenso wie ein Verbot von fremder Hardware. Denn auch hier gilt meist: Vertrauen ist gut — Kontrolle ist besser.

Die Pflege von statischen ARP-Tabellen wäre ebenfalls schlichtweg zu aufwendig und die Nutzung von Intrusion Detection-Systemen (IDS) ist meist suboptimal, da diese Lösungen i.d.R. keine ARP-Angriffe erkennen können. Ebenso sind DHCP-Konfigurationen nur bedingt zur Abwehr von fremden Geräten geeignet, denn sie können leicht umgangen werden. Port-Security ist nur schwer administrierbar. Port-Authentifizierung gemäß IEEE 802.1x ist Support-intensiv (kostenaufwändig) und zudem trotzdem angreifbar.

Die ARP-GUARD-Lösung als wirksamer Schutzschild

ARP-GUARD bietet einen wirksamen Schutzschild, welcher die Sicherheitslücke effektiv schließt und sich zudem einfach und problemlos in eine bestehende IT-Sicherheits-Infrastruktur integrieren lässt. Die Lösung arbeitet Hersteller- und Plattform-unabhängig und ist beliebig skalierbar. Insbesondere sind keine Investitionen in neue Endgeräte oder Strukturen erforderlich.

ARP-GUARD ist ein Produkt des deutschen Herstellers *Internet Sicherheitslösungen GmbH (ISL)* mit Sitz in Hagen und wurde bereits 2003 auf der Systems in München erstmals der Öffentlichkeit vorgestellt. ARP-GUARD ist eine Sicherheitslösung, welche gezielt vor internen Angriffen und fremden Geräten im Netz schützt und diese auch automatisiert

abwehren kann. Die Lösung erkennt aktuelle Bedrohungen (Beobachter) und reagiert nur im konkreten Angriffsfall. ARP-GUARD bietet:

- Network Access Control (NAC)
- Layer-2 IPS
- VLAN- und Netzwerk-Management
- Endpoint Security

Network Access Control (NAC) mit ARP-GUARD

ARP-GUARD unterstützt eine vollständige Zugangskontrolle zum Netzwerk, durch

- MAC-Authentisierung
- 802.1X
- RADIUS
- Microsoft AD
- und/oder Mischformen

Neue Geräte werden in Echtzeit erkannt und gemeldet. Hierbei entscheidet eine Benutzer-definierte Festlegung von Zugangs- und Sicherheitsrichtlinien (Regeln), wie mit unautorisierter Hardware vorgegangen werden soll: z.B. mit Alarmierung und/oder automatischer Port-Abschaltung oder mit einer Verlegung in spezielle (Gast-) VLANs. Ebenfalls möglich sind zeitlich beschränkte Zugangsberechtigungen.

Layer2 Intrusion Prevention System (IPS) mit ARP-GUARD

ARP-GUARD erkennt und lokalisiert interne Angriffe auf Layer-2 und wehrt diese automatisch ab. Hierzu zählen u.a. *ARP-Spoofing / ARP-Poisoning- (Man-in-the-middle-)*, *MAC-Flooding-*, *IP- und MAC-Spoofing*-Angriffe.

Erkennung von Spoofing-Attacken mit ARP-GUARD

Auf Basis seiner Adressdatenbank kann die ARP-GUARD-Lösung Veränderungen von Adressdaten (z.B. eine neue CAM-Zuordnung, welche durch eine gespoofte MAC-Adresse erfolgt ist) erkennen, alarmieren und abwehren. Das System nutzt die ermittelten Fingerprints der legitimierten Hardware im Netz, und erkennt neben MAC-Spoofing auch IP-Spoofing sowie eine Kombination aus beiden Angriffsszenarien.

Erkennung ungewollter Adresskonflikte mit ARP-GUARD

Ebenso erkennt das ARP-GUARD-System eventuelle IP- und MAC-Adresskonflikte. Dies sind meist irrtümliche Szenarien, in denen mehrere Geräte im Netz mit der gleichen Adresse arbeiten, was zwangsläufig zu Störungen im Netz führt.

Präventive Ansätze mit ARP-GUARD

ARP-GUARD enthält eine präventive Komponente, die z.B. Angriffe auf das Spanning Tree Protokoll sowie auf Discovery Protokolle verhindern kann.

Endpoint Security mit ARP-GUARD

Das optionale Endpoint Security Modul verhindert den Zugang von Endgeräten in das Netz, welche nicht dem festgelegten Sicherheitsstandard (Betriebssystem- und AV-Updatestatus) entsprechen. Eine Client-Installation auf den Endgeräten ist nicht erforderlich. Erfasste Geräte können mittels individuellem Quarantänemanagent in spezielle VLANs geschoben werden.

Netzwerk-Management mit ARP-GUARD

Das zentrale ARP-GUARD Managementsystem bietet eine umfassende Übersicht über alle Geräte im Netz. Das integrierte Adressmanagement erkennt, zeigt und protokolliert alle Veränderungen. So lassen sich z.B. Bestandslisten einfach auf einem aktuellen Stand halten. Alle Konfigurationen und Regeln werden zentral eingestellt und wirken global. Unterstützende Features, wie z.B. Gruppenbildung bei Geräten/Ports reduzieren den Admininstrationsaufwand erheblich, da eine Einzel-Konfiguration pro Switch entfällt. Eine Alarmierung im Angriffsfall kann flexibel per Email, SNMP Trap, SMS, oder Skript erfolgen.

Graphische Topologie-Erkennung mit ARP-GUARD

Sehr nützlich in der Praxis ist auch die graphische Topologie-Erkennung mit Hilfe des ARP-GUARD Management-Systems. Sie liefert die automatische Erstellung eines Netzplans mit allen involvierten Geräten, inklusive der Information, an welchem Switchport diese Geräte angeschlossen sind.

VLAN-Management mit ARP-GUARD

Praktisch ist auch das integrierte VLAN-Management. Es zeigt u.a. zentral (über alle Switches) an, ob sich eine IP-Adresse im richtigen VLAN befindet. Die notwendigen Regeln hierzu werden einmal und zentral im Management erstellt und können individuell sowie nach Bedarf definiert werden. Zum Beispiel auch für eine automatische Erkennung von irrtümlich doppelt vergebenen IP-Adressen.

Elegant ist zudem die Möglichkeit, VLANs in Abhängigkeit von Regeln dynamisch zu konfigurieren. So können z.B. die Ports aus der Gruppe „Besprechungsräume“ standardmäßig im Gäste-VLAN betrieben werden. Sobald jedoch ein interner Mitarbeiter ins Netz geht, wird dessen internes VLAN aktiv,

sodass der Mitarbeiter immer seine gewohnte Umgebung vorfindet. Umgekehrt kann in den Büros standardmäßig das interne VLAN konfiguriert sein. Schließt sich jedoch ein Besucher dort an das Netz, dann wird der Port sofort in das Gäste-VLAN geschoben.

Arbeitsweise und Sensoren mit ARP-GUARD

Mittels drei verschiedener Sensortypen (SNMP-, RADIUS-, und LAN-Sensor) können selbst große, verteilte Netze mit wenig Hardwareaufwand konsequent geschützt werden. Dabei ist ARP-GUARD beliebig skalierbar, kann als Cluster betrieben werden und arbeitet ohne Single Point of Failure. ARP-GUARD nutzt insbesondere das SNMP-Protokoll (*Simple Network Management Protocol*) zum Adressdaten-Abgleich mit den im Netzwerk befindlichen Switches und Routern. Mit Hilfe der Adressdatenbank kann ARP-GUARD nicht nur fremde Geräte erkennen, lokalisieren (an welchem Switchport befindet sich das Gerät bzw. der Angreifer?) und abwehren, sondern auch interne Zugriffsberechtigungen abbilden.

Die Beobachtung und Nutzung der in den Switches und Routern vorhandenen Informationen sowie deren Abfrage per SNMP setzen voraus, daß die Geräte SNMP-managebar sind. Aber auch Angriffe über unmanaged Switches (z.B. in Büros) können insofern erkannt und abgewehrt werden, daß sie beim ersten SNMP-managebaren Gerät auffallen und der entsprechende Port (an dem die Anomalie auftritt) ermittelt und abgeschaltet wird.

Wichtige Ports, z.B. von Uplinks, Server- oder Routersystemen, können als VIP (Very Important Port) definiert werden. VIP-Ports werden durch ARP-GUARD nicht abgeschaltet. Falls gewünscht, schaltet das System den Port eines Angreifers sofort herunter (mit SNMP-Sensor nach ca. 300ms). Nach einer individuell konfigurierten „Bedenkzeit“ wird der Port wieder aktiviert, um festzustellen, ob der Angriff beendet worden ist. Die Freischaltung von neuen Geräten kann einfach durch definierte Lernports realisiert werden.

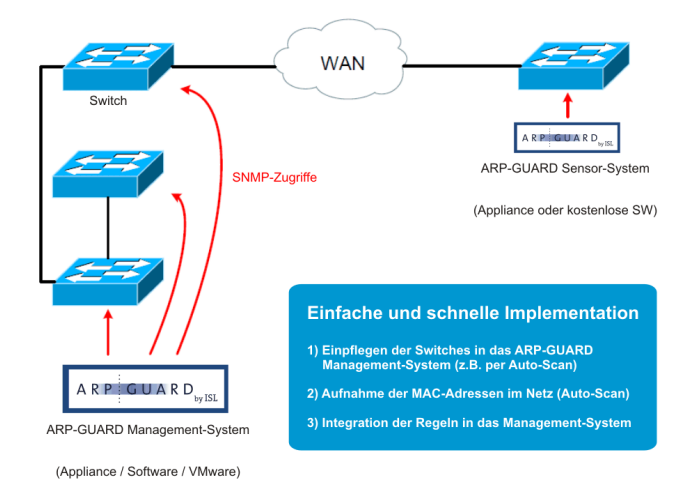


Abb.-3: ARP-GUARD Management-System und -Sensoren im Netz

ARP-GUARD beim Kölner Motorenbauer DEUTZ AG

ARP-GUARD ist von der SySS GmbH und durch den Heise-Verlag intensiv getestet worden. Branchenübergreifend schützen sich Banken, Behörden, Industrie, Krankenhäuser, Messen, Ministerien und Hochschulen mittels ARP-GUARD vor internen Bedrohungen. So schützt die Kölner DEUTZ AG mit ARP-GUARD die komplette IT-Systemstruktur der Motorenproduktion. „Auch wir möchten nur autorisierte Geräte in unserem Netzwerk“, erläutert Martin Feller, Leiter Systeme bei DEUTZ, die Schließung der Sicherheitslücke. Die Kölner Motorenbauer nutzen das System zudem zur Überwachung von SPS-Wartungsarbeiten (SPS ≡ Speicherprogrammierbare Steuerung). Denn die Ersatzgeräte für defekte SPS-Einheiten erhalten dieselbe MAC-Adress-Konfiguration wie der jeweilige Vorgänger. Wird hier versehentlich eine falsche MAC konfiguriert, kommt es zu unerwünschten Anomalien im Produktionssystem. „ARP-GUARD meldet uns sofort eine Abweichung in der MAC-Konfiguration und unterstützt somit einen stabilen Produktionsprozess“, ergänzt Feller. Neben den primären Sicherheitsfeatures bietet das zentrale ARP-GUARD Adress-Management eine praktische ad-hoc Gerätelokalisierung im Netz, passend zur Antwort nach der häufigen Frage: „Ich suche ein bestimmtes Gerät. An welchem Switchport ist eigentlich die IP-Adresse xyz angeschlossen?“.

Martin Feller

Leiter Systeme
DEUTZ Montage
Köln-Porz

Einfache und schnelle Implementation in 1½ Tagen

Die ARP-GUARD Implementation geht einfach und schnell, ohne Eingriff in bestehende Systeme. Bei DEUTZ erfolgte die Integration in drei Schritten innerhalb von 1½ Tagen.

1) Einpflegen der Switches in das ARP-GUARD Management-System (z.B. per Auto-Scan)

2) Aufnahme der MAC-Adressen im Netz (per Auto-Scan)

3) Integration der Regeln im Management-System

ARP-GUARD lässt sich insbesondere problemlos in bereits bestehende IT-Sicherheitsumgebungen einbinden. Denn ARP-GUARD greift nicht in interne Applikationen ein (vgl. Abb.-3).

Überschaubare Kosten für die ARP-GUARD-Lösung

ARP-GUARD stützt sich auf internationale Standards. Somit arbeitet die Lösung Hersteller- und Plattform-unabhängig mit allen gängigen Routern und Switches. Investitionen in neue Endgeräte oder neue Strukturen sind nicht erforderlich. Das ARP-GUARD Management-System ist als Appliance (Bundle von Hard- und Software) sowie als reine Softwarelösung respektive als VMware-Paket erhältlich. Die Software läuft unter Linux (Red Hat oder CentOS) und unter Windows (nur für Sensoren). Die Kosten für die ARP-GUARD-Lösung sind überschaubar. 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. Der Aufwand für Implementation und Konfiguration ist mit wenigen Manntagen abgedeckt. Auch die Wartungskosten sind niedrig. Sowohl für die Lizenzen (Preis pro MAC-Adresse im Netz) als auch für die Pflege vor Ort. Selbst Kunden mit deutlich über fünftausend MAC-Adressen im Netz berichten von einem Pflegeaufwand von lediglich fünf Minuten pro Tag.

Zusammenfassung

Die Vorteile der ARP-GUARD-Lösung liegen auf der Hand. Das System schützt effektiv vor fremden Geräten und deren Verbreitung von Malware im Netz sowie vor möglichen Angriffen, wie z.B. ARP- und MAC-Spoofing. Die Lösung gibt einen vollständigen Überblick über die Produktionsnetze und liefert eine Kontrolle und Protokollierung des Netzzugangs.

ARP-GUARD – NAC • Layer2 • IPS • Netzmanagement • Endpoint Security

- **Zentrales Management-System, inkl. Inventar- und Adressmanagement**
- **Benutzer-definierte Zugangs- und Sicherheits-Richtlinien (Regeln)**
- **Automatische Abwehr & Verlegung von unautorisierter HW in VLANs**
- **OS-Fingerprinting**
- **Keine Client-Software erforderlich**
- **Kostengünstige und pragmatische Alternative zu 802.1x**
- **Beliebig skalierbar**
- **Alarmierung per Email, SNMP-Trap, SMS oder Skript**
- **Niedriger Implementations- und Wartungsaufwand**

Weitere Informationen

www.gordion.de

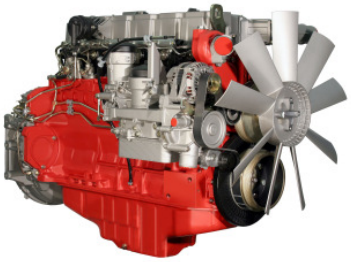
www.arp-guard.com

The engine company. DEUTZ®

Firmenprofil DEUTZ AG

1864 als N.A. Otto & Cie. in Köln gegründet, ist die DEUTZ AG heute die älteste Motorenfabrik der Welt und einer der weltweit führenden unabhängigen Motorenhersteller. Die Kernkompetenzen des Unternehmens liegen in der Entwicklung, Produktion, dem Vertrieb und Service von Dieselmotoren für professionelle Einsätze. Der Full-Line-Motorenspezialist verfügt über eine breite Palette flüssigkeits- und luftgekühlter Motoren in einem Leistungsspektrum von 20 KW bis 520 KW, die in Baumaschinen, Energie-Erzeugungsanlagen, Landmaschinen, Nutz- und Schienenfahrzeugen sowie Schiffen zum Einsatz kommen. DEUTZ-Kunden werden von 16 Vertriebsgesellschaften, 12 Vertriebsbüros, 16 Service-Centern und über 800 Vertriebs- und Service-Partnern in mehr als 130 Ländern weltweit betreut.

In der Kölner Montagehalle 40 werden pro Stunde 44 Motoren gefertigt. Mit zwei Montagelinien in bis zu drei Schichten an maximal sechs Tagen in der Woche sowie unter Berücksichtigung von rund 3.800 Varianten.



DEUTZ-Motor TCD 2013 L6 4V
für die industrielle Anwendung

ARP-GUARD als Schutzschild im Netzwerk.

DEUTZ schützt mit ARP-GUARD die komplette IT-Systemstruktur der Motorenproduktion vor fremden Geräten und möglichen internen Angriffen im LAN. Neben der primären Funktion als Schutzschild unterstützt ARP-GUARD die Motorenbauer durch seine praktische Managementfunktionalität, u.a. durch stets aktuelle Geräte-Bestandslisten, Adressmanagement inklusive netzweiter „MAC ↔ IP Darstellung“ und der Ad-hoc-Information, an welchem Switchport sich ein bestimmtes Endgerät (z.B. IP-Adresse) befindet. Im Rahmen von SPS-Austausch-Prozeduren meldet ARP-GUARD umgehend irrtümlich falsch konfigurierte MAC-Adressen und unterstützt so neben den Sicherheitsaspekten auch einen stabilen Produktionsablauf.

www.deutz.com

GORDION®

Lösungen für komplexe Rechner-Netzwerke.

Network Consulting

LAN / WAN • Security • Analyzing