

ARP GUARD

NETWORK ACCESS CONTROL - LAYER 2 IPS - NETWORK MANAGEMENT - ENDPOINT



SCHUTZ VOR FREMDEN GERÄTEN UND INTERNEN ANGRIFFEN

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Einleitung

Herzlich willkommen!

- In der Vergangenheit wurde viel Energie in die Erkennung und Abwehr von externen Angriffen (Hacker, Viren usw.) investiert.
- Durch gute Produkte und Dienstleistungen kann man heute weitreichende Sicherheit in diesem Bereich herstellen.
- Gegen interne Angriffe – sei es von eigenen Mitarbeitern oder Dritten – wurden jedoch kaum Schutzmaßnahmen getroffen.
- Dabei kommen bis zu 80% aller Angriffe von innen (KPMG)!

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Inhalt

- ISL
- Interne Angriffe
 - Bedrohung
 - Motive/Konsequenzen
 - Alternativen
- Fremde Geräte
 - Bedrohung
 - Alternativen
- ARP-GUARD
 - Module
 - Produkte
 - ARP-GUARD Appliance
 - Endpoint
 - Referenzen
- Kontakt

SECUDOS

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ISL

- ISL steht für Internet Sicherheitslösungen und firmiert als GmbH.
- ISL wurde im April 1999 als deutsches Unternehmen mit Sitz in Hagen gegründet.
- ISL hat sich zunächst einen Überblick über alle Aspekte der IT-Sicherheit verschafft und sich dann auf interne Bedrohungen konzentriert.
- Das Produkt ARP-GUARD wurde erstmals auf der Systems 2003 vorgestellt.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Interne Angriffe: Bedrohung

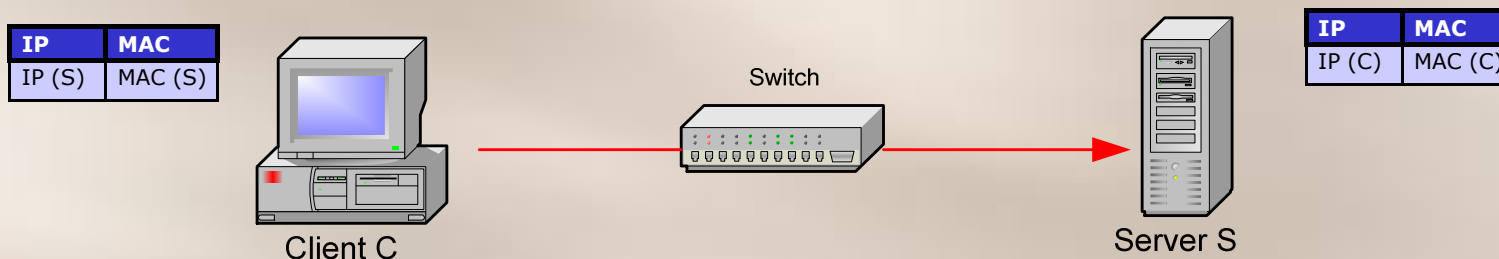
- Mit internen Angriffen (z.B. ARP-Spoofing) kann man beliebig Daten abhören, Passworte sammeln und sogar Daten manipulieren.
- Das funktioniert oft auch bei verschlüsselten Verbindungen (SSH, SSL, PPTP), da Zertifikate nicht ausreichend geprüft werden.
- ARP-Angriffe können auch über WLANs ausgeführt werden.



Int. Angriffe: Bedrohung

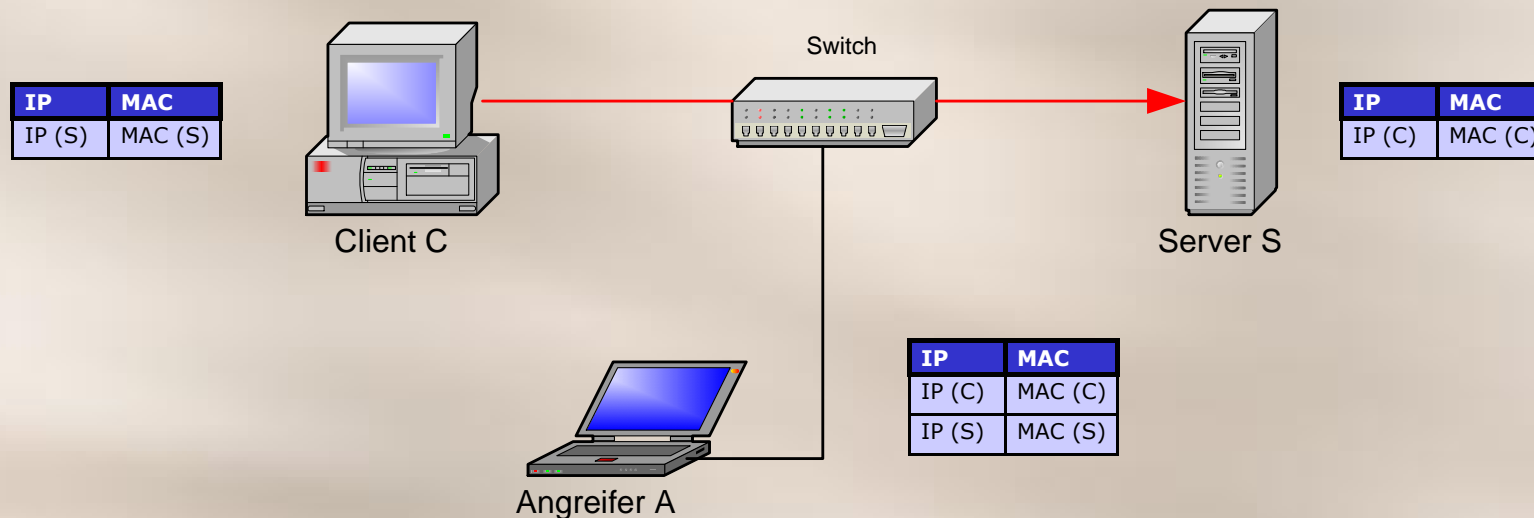
Ausgangssituation:

Die Adressen der Netzwerkkarten (MAC-Adressen) sind ordnungsgemäß im ARP-Cache der jeweiligen Rechner gespeichert.



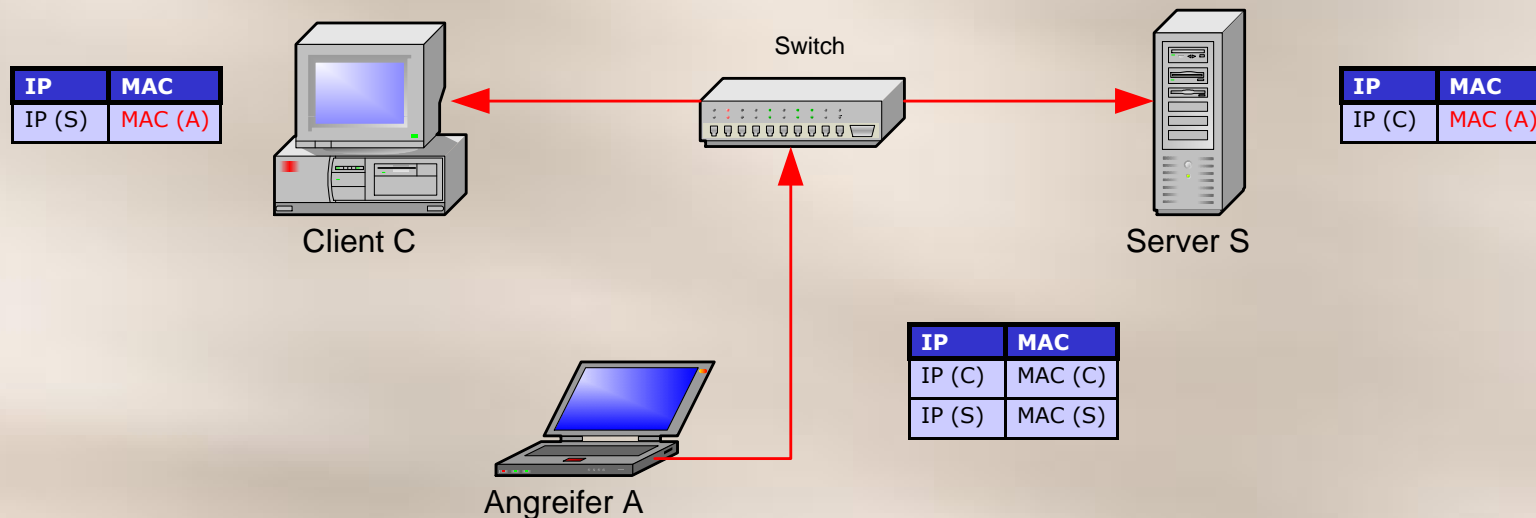
Int. Angriffe: Bedrohung

Angreifer A schließt sein Notebook an das Netzwerk an und ermittelt die MAC-Adressen der anderen angeschlossenen Rechner.



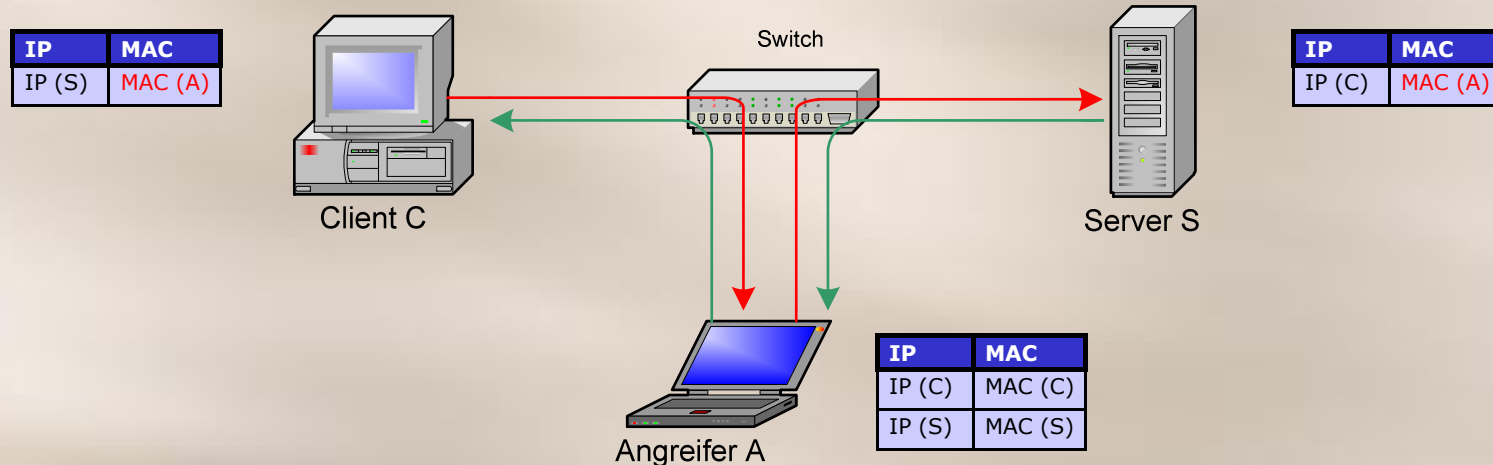
Int. Angriffe: Bedrohung

Fälschlicherweise wird die MAC-Adresse des Angreifers den IP-Adressen der anderen Rechner zugeordnet und in den ARP-Caches gespeichert.



Int. Angriffe: Bedrohung

Angreifer A leitet die Kommunikation zwischen den Rechnern über seinen Computer um.



Interne Angriffe: Bedrohung

- Jeder, der Zugang zu Ihrem Netzwerk hat, kann interne Angriffe ausführen, ohne zu riskieren, dass dies bekannt wird!
- Betroffen sind alle Unternehmen, die sensible Daten verarbeiten, z.B. Banken, Versicherungen und Behörden.
- Auch Telefonate (Voice over IP) können abgehört werden!
- Die Angriffssoftware ist im Internet vielfach (u.a. bei Heise) verfügbar und leicht zu bedienen.
- Interne Angriffe werden von den Unternehmen oft verschwiegen, weil sie ein negatives Image erzeugen.
- In Israel ist jedoch z.B. ein Banküberfall bekannt geworden, der offensichtlich auf ARP-Angriffen basiert.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Interne Angriffe: Motive

- Verschaffung von persönlichen Vorteilen
- Wirtschaftsspionage
- Neugierde
- Ehrgeiz von Hobby-Hackern
- Erpressung
- Sabotage/Schädigung des Unternehmens
- Mobbing

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Int. Angriffe: Vergleich

Angriffe auf Layer 3-7:

- Detaillierte Hintergrundinfos erforderlich
- Tiefes Know-How erforderlich
- Spezielle Exploit-Software erforderlich
- Risiko der Entdeckung besteht (IPS), es werden Spuren hinterlassen

Kaum machbar!

Angriffe auf Layer 2:

- Nur IP-Adresse erforderlich
- Kein besonderes Know-How erforderlich
- Angriffssoftware:
 - Linux: Ettercap
 - Windows: Cain
- Kein Risiko der Entdeckung, keine Spuren

Leicht machbar!

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Int. Angriffe: Konsequenzen

- Imageschäden
- Wettbewerbsnachteile / Kosten
- Haftung des Unternehmens
- Rechtliche Konsequenzen / Strafbarkeit
- Schadensersatzpflicht
- Persönliche Haftung (KonTraG)

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Int. Angriffe: Alternativen

- Statische ARP-Tabellen: Viel zu aufwändig
- arpwatch: Nur für kleinste Netze und statische Adressen
- Bildung kleinerer Subnetze: Hohe Kosten für Router
- Verhinderung fremder Software: Nicht durchführbar
- Intrusion Detection: Viel zu teuer, die meisten IDS erkennen keine ARP-Angriffe

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Int. Angriffe: Alternativen

- Einschränkung der Verkehrsbeziehungen: Hoher Managementaufwand, evtl. eingeschr. Funktionalität
- Schutzfunktionen im Endgerät: Nur beschränkt wirksam, nur teilweise verfügbar, kann zu Fehlfunktionen führen
- Dynamic ARP Inspection (Cisco): Teuer und sehr aufwändig zu konfigurieren

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Fremde Geräte: Bedrohung

- Jeder, der Zugang zu Ihrem Gebäude hat, kann unbemerkt ein unautorisiertes Gerät in das Netzwerk einbringen!
- Bereits ein einziges unautorisiertes Gerät (Notebook, WLAN access point) kann in einem Unternehmensnetz Tür und Tor für fatale Sicherheitsrisiken öffnen!
- Verbreitung von Viren, Würmern und Trojanern
- Interne Angriffe
- Wirtschaftsspionage, Sabotage und Schädigung des Unternehmens

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Fremde Geräte: Alternativen

- Physikalischer Schutz (bauliche Maßnahmen): Oft nicht machbar
- Konfiguration DHCP: Leicht zu umgehen
- Port Security: Extrem schwer zu administrieren
- 802.1x: Kostenaufwändig und kinderleicht angreifbar
- NAC/NAP/TAP/...: Zu komplex, zu wenig kompatibel

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD

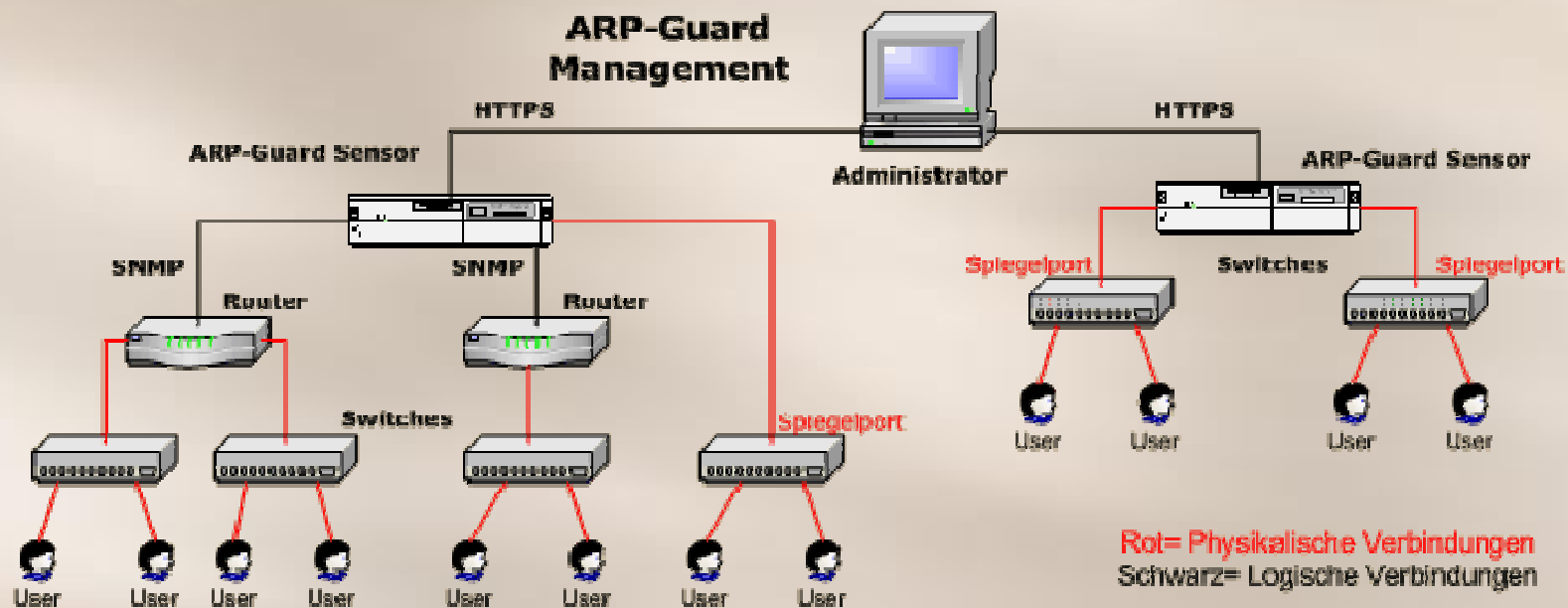
- ISL hat mit ARP-GUARD ein Produkt entwickelt, das gezielt vor internen Angriffen und fremden Geräten schützt und diese sogar automatisiert abwehren kann.
- Durch zwei verschiedene Sensoren (LAN- und SNMP-Sensor) können selbst große, verteilte Netze mit wenig Hardwareaufwand konsequent geschützt werden.
- ARP-GUARD ist bei verschiedenen Kunden (z.B. Mercedes AMG, Wincor Nixdorf, BMWI, ...) erprobt und von der Syss und vom Heise-Verlag ausgiebig getestet worden.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD



secudos

Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD

ARP-GUARD bietet Schutz vor internen Angriffen!

- Mit **ARP-GUARD** hat **ISL** weltweit erstmalig ein wirksames System zum Aufbau eines aktiven Schutzschildes gegen interne Angriffe entwickelt.
- Daten können nicht mehr unbemerkt ausspioniert, gelöscht oder manipuliert werden.
- Geheime Produktentwicklungen und firmeninterne Passworte sind vor unerwünschtem Zugriff gesichert.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD

Erkennung, Lokalisierung und Abwehr von

- ARP-Spoofing- und ARP-Poisoning-Angriffen
- IP- und MAC-Spoofing-Angriffen
- MAC-Flooding-Angriffen und MAC-Adresskonflikten
- IP-Adresskonflikten (Qualitätssicherung)

sowie präventiver Schutz:

- Angriffe auf Spanning Tree
- Angriffe auf GVRP
- Angriffe auf Discovery Protokolle

secudos


Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD

ARP-GUARD bietet Schutz vor unerwünschten Geräten!

- Das integrierte Adressmanagement bietet eine umfassende Übersicht über ihr Netzwerk.
- Neue Geräte, die ans Netz angeschlossen werden, erkennt und meldet ARP-GUARD automatisch. Der Anschluss unautorisierter Notebooks, WLAN- und sonstiger Geräte wird unterbunden.
- Bestandslisten werden auf dem neuesten Stand gehalten.
- Adressänderungen werden protokolliert und lassen sich zurückverfolgen.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port Security

Switches:

- Unterschiedliche Hersteller und Produkte (kein Standard verfügbar)
- Konfiguration gilt nur für einen Switch
- Oft Abhängigkeiten von anderen Features eines Switches
- Beschränkte Möglichkeiten
- Extrem aufwändige Konfiguration

ARP-GUARD:

- Unabhängigkeit von Herstellern und Produkten durch ARP-GUARD
- Zentrale Konfiguration, die für das ganze Netz gilt.
- Keine Abhängigkeiten (nur managed Switch erf.)
- Keine Beschränkungen
- Einfache Konfiguration durch Geräte- und Portgruppen

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port-Auth.: Einsatzbereiche

802.1x:

- Neue Switches
- Keine/wenig alte Endgeräte
- Zentrale Auth. verfügbar
- Kompatibilität geprüft
- Hochverfügbarkeit
 - Zentrale Auth.
 - Anbindungen zu anderen Standorten

ARP-GUARD:

- Universell einsetzbar
- Hochverfügbarkeit nicht zwingend erforderlich

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port-Auth.: Alte Switches

802.1x:

- Unmanaged Switches müssen ersetzt werden.
- Firmware-Upgrades
- Hardware-Erweiterungen
- Ersatz „alter“ Switches
- Vorhandene Switches sind evtl. nicht kompatibel zu alten Endgeräten (MAB)

ARP-GUARD:

- Basis: Managed Switches
- Erkennung fremder Geräte auch mit unmanaged Switches
- Alte Geräte sind kein Problem

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port-Auth.: Alte Endgeräte

802.1x:

- Portbasierte Konfiguration:
Viele Änderungen und hoher Admin-Aufwand!
- MAC-basierte Konfiguration (Beispiel Cisco MAB):
 - Proprietär
 - Neu (2007)
 - Kein Lernmechanismus
 - Kein tagged VoIP
 - Kein DHCP
 - Probleme mit MAC movement
 - Nicht kompatibel mit neu installiertem XP

ARP-GUARD:

- Universell einsetzbar!

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port-Auth.: Zentrale Auth.

802.1x:

- Aufbau einer zentralen Authentisierung
- Vergabe von Berechtigungen für Anwender ist organisatorisch aufwändig.
- Oft lange Projektlaufzeiten
- Oft überzogene Budgets

ARP-GUARD:

- Einsatz einer ARP-GUARD Appliance
- Geräteadressen können einfach gelernt werden.
- Inbetriebnahme ist innerhalb kürzester Zeit (4 Wochen) möglich.
- Exakt kalkulierbare Kosten

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port-Auth.: Realisierung

802.1x:

- Homogene Switches?
- Einheitliche Authentisierungs-Verfahren für alle Switches?
- Kompatibilität?
- Konfiguration einzelner Ports:
 - Trunk?
 - Endgerät ohne 802.1x?
- Einspielen von Zertifikaten auf Endgeräten
- Viele neue Prozesse, hoher administrativer Aufwand!

ARP-GUARD:

- Kompatibel zu mindestens 16 großen Herstellern
- Kommunikation basiert auf (standardisiertem) SNMP
- Dadurch ist die Kompatibilität gegeben.
- Keine Konfiguration einzelner Switchports erforderlich
- Kein Einspielen von Zertifikaten erforderlich
- Kaum neue Prozesse, kaum administrativer Aufwand!

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port-Auth.: Compliance

802.1x:

- User based: Keine Aussage über Compliance möglich!
- Certificate based: Es wird sichergestellt, dass es sich um eigene Geräte handelt.

ARP-GUARD:

- Es wird in jedem Fall sichergestellt, dass es sich um eigene Geräte handelt.

Da eigene Geräte über eine zentrale Virenschutzlösung überwacht werden, ist die Compliance in beiden Fällen gegeben, solange keine user based Authentication eingesetzt wird!

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port-Auth.: Verfügbarkeit

802.1x:

- Nach einem Ausfall der 802.1x-Lösung kann ein Port theoretisch freigeschaltet werden.
- Praktisch fällt aber das komplette Netz aus, weil ja keine VLAN-ID für das Endgerät bekannt ist.
- Selbst mit HA-Lösung ist 802.1x kritisch, insbesondere für entfernte Standorte.

ARP-GUARD:

- Nach einem Ausfall des ARP-GUARD läuft das Netz unverändert weiter.
- Allerdings werden unberechtigte Geräte nicht mehr vom Netz getrennt.
- Eine HA-Lösung ist zwar verfügbar, aber nicht zwingend erforderlich.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Port-Auth.: Sicherheit

802.1x:

- Nicht die Person, sondern das Gerät trägt die Malware.
- Berechtigungen sind bei User-Auth. übertragbar.
- Bei vielen Switches kinderleichte Angriffe nach Anmeldung eines legitimen Users
- Viele Löcher durch alte Geräte (z.B. Drucker)

ARP-GUARD:

- Der Angreifer muss zunächst wissen, dass MAC-Adressen relevant sind.
- MAC-Adressen sind fälschbar, wenn
 - Know-How vorhanden
 - Admin-Rechte vorhanden
 - Legitime Adresse bekannt
- Darüber hinaus sind Portscans möglich!!!

Port-Auth.: Positionierung AG

Alternative zu 802.1x:

- ARP-GUARD ist eine pragmatische Alternative zu 802.1x.
- Wesentliche Vorteile:
 - Kosten und Zeitaufwand sind kalkulierbar.
 - Keine Probleme mit Kompatibilität
 - Geringer Admin-Aufwand

Migration zu MAB bzw. 802.1x:

- ARP-GUARD ermöglicht einen Mischbetrieb mit SNMP/MAB/802.1x und kann daher mit alten Switches bzw. alten Endgeräten umgehen.
- ARP-GUARD kann mit Sensoren auch für entfernte Standorte eine ausreichend hohe Verfügbarkeit sicherstellen.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

NAC/NAP/TAP/... (1)

- Alle Geräte, die einer vorgegebenen Security Policy entsprechen, werden im Netz zugelassen.
- Alle anderen Geräte bekommen keinen Zugang oder kommen in ein Quarantäne- oder Gäste-VLAN.
- Inwieweit dürfen Informationen von einem möglicherweise kompromittierten System verwendet werden, um zu prüfen, ob dieses Gerät der Security Policy entspricht und Zugang zum Netz erhalten kann?
- Alle Geräte, die im Besitz des Kunden sind oder ausdrücklich zugelassen werden, sind im internen Netz erlaubt.
- Bei verantwortungsbewusster Konfiguration dieser Geräte können keine Sicherheitsprobleme auftreten.
- Alle anderen Geräte bekommen keinen Zugang oder kommen in ein Quarantäne- oder Gäste-VLAN.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

NAC/NAP/TAP/... (2)

NAC/NAP/TAP/...:

- Von vielen Experten als zu komplex bezeichnet
- Kompatibilität ist nicht im Interesse der Hersteller (Bindung der Kunden an eigene Produkte).
- Client-Software ist gerade für Dritte ein Problem.

ARP-GUARD:

- Leicht administrierbar
- Hersteller wird sein Produkt nicht absetzen können, wenn keine Kompatibilität vorliegt.
- Keine Client-Software erforderlich

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD

- ARP-GUARD lässt sich problemlos in bereits bestehende IT-Sicherheitsumgebungen einbinden.
- ARP-GUARD greift NICHT in interne Applikationen ein, erkennt aktuelle Bedrohungen als Beobachter und reagiert nur im konkreten Angriffsfall.
- ARP-GUARD ist beliebig skalierbar.
- ARP-GUARD arbeitet hersteller- und plattformunabhängig mit allen gängigen Routern und Switches.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Kompatibilität

- 3Com Corporation
- Alcatel-Lucent
- Allied Telesyn
- Cisco Systems
- Dafür
- Dell
- D-Link
- Enterasys Networks
- Extreme Networks
- Foundry Networks
- Hewlett-Packard
- Hirschmann Industries
- Huawei/H3C
- Linksys
- Marconi
- MRV Communications
- Netgear
- Nexans
- Nortel Networks
- Alle Geräte, die internationale Standards unterstützen

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD

- Investitionen in neue Endgeräte oder neue Strukturen sind nicht erforderlich.
- **ARP-GUARD** zeichnet sich durch gar keine bzw. extrem wenige false positives aus.
- Im Vergleich zu Mitbewerber-Produkten (Cisco's Dynamic ARP inspection oder 802.1x) ist **ARP-GUARD** sehr preisgünstig.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Module

- ARP-GUARD Manage: Netzwerkmanagement mit Schwerpunkt auf den Endgeräten
- ARP-GUARD Access: Schutz vor fremden Geräten
- ARP-GUARD Access+: Schutz vor fremden Geräten und Zugangsschutz im LAN
- ARP-GUARD Defend: Erkennung, Lokalisierung und Abwehr von internen Angriffen
- ARP-GUARD Finance: Erkennung, Lokalisierung und Abwehr von internen Angriffen und Schutz vor fremden Geräten
- ARP-GUARD Premium: Erkennung, Lokalisierung und Abwehr von internen Angriffen und fremden Geräten sowie Zugangsschutz im LAN

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Neue Features I

- Mit der neuen Version 2.2.2 bietet ARP-GUARD die folgenden neuen Features:
 - Endpoint: Infos über AV-Pattern und OS-Updates ohne Client-Software
 - Ändern von VLANs auch auf tagged Ports (z.B. für VoIP)
 - Erkennung und Abwehr von MAC-Spoofing
 - Radius (z.B. mac-based 802.1x) und VQP/VMPS
 - Rechteverwaltung durch flexibles Rollenkonzept
 - Neues DOMOS 2 (mit IP V 6)
 - Dynamische Erkennung von Interfaces und Ports

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Neue Features II

- Erkennung und Änderung von Port-Modi (Trunk, Access, VQP, 802.1x, GVRP, ...)
- Hochverfügbarkeit und Lastverteilung
- Intelligent SNMP bug handling engine
- Schongang für wenig leistungsfähige Switches
- Analyse von Discovery-Informationen
- Starke Authentisierung (z.B. über LDAP)
- Unterstützung weiterer Switch-Hersteller: Huawei, H3C, Netgear, Dell u.a.
- Virtuelle Sensoren
- Diverse Kleinigkeiten, die einem das Leben leichter machen ...

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Produkte

- **ARP-GUARD** wird als Appliance (Bundle von Hard- und Software) sowie als reine Softwarelösung angeboten.
- Die Software ist unter Linux (Red Hat oder Centos) und Windows (nur Sensor) lauffähig.
- Seit 2009 wird ARP-GUARD auch als VMware-Paket angeboten.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Appliance

- In Zusammenarbeit mit der **SECUDOS GmbH** ist die ARP-GUARD Appliance entstanden.
- Die ARP-GUARD Appliance wird mit vorinstallierter Software geliefert (keine Probleme mit Betriebssystemversionen, Treibern, o.ä.) und wird komplett über ein Web-Interface konfiguriert.
- Es ist keine aufwändige Konfiguration erforderlich.








secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Appliance

 AG-140 Sensor	AG-242	AG-242 Rack	AG-432	AG-442	
					
Endgeräte	Max. 1 000	Max. 1 000	Max. 1 000	Max. 5 000	Max. 20 000
Gehäuse	Tisch	Tisch	19" 1HE Rack	19" 1HE Rack	19" 2U Rack
Ports	4* 10/100	4* 10/100	4* 10/100	6*10/100/1000	4*10/100/1000
Memory	256 MB	1 GB	1GB	2 GB	4 GB
CPU	400 MHz	1,5 GHz	1,5 GHz	Dual 2,5 GHz	Quad 2,0 GHz

secudos

 **Omicron**

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Appliance

- Neben dem Bundle aus Hardware, Software und Lizenz kann der Kunde Software Subscription und Supportleistungen erwerben.
- Software Subscription: Zugriff auf neue Versionen, Updates, Upgrades usw. sowohl für das Betriebssystem als auch für die ARP-GUARD Software.
- Das Support-Package enthält: Advanced Hardware Replacement (next business day, echte Hardware-Garantie) sowie priorisierten Telefon- und Email-Support

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Neues Add-on: Endpoint

Wie kann ich ohne zusätzliche Software auf dem Client Informationen über den Client bekommen?

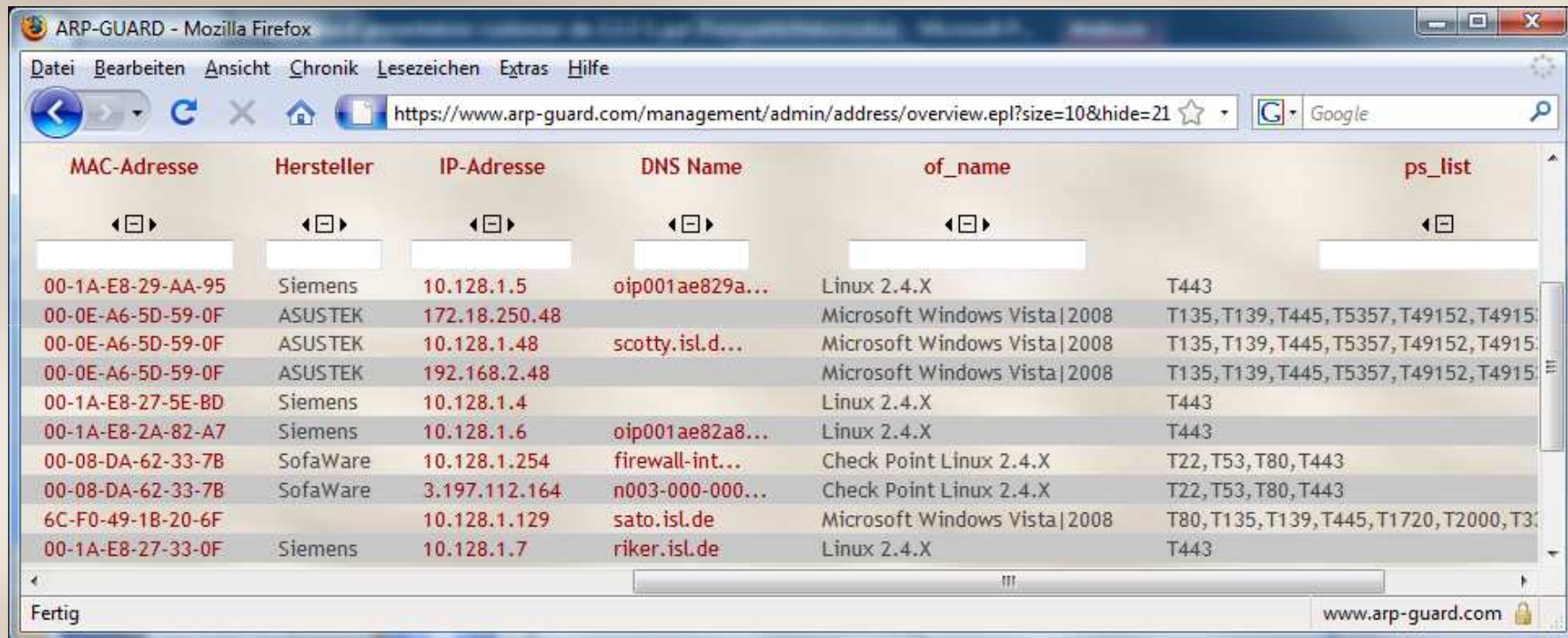
1. Port Scans/OS fingerprinting
2. Analyse der Kommunikation mit Update-Servern
3. Auswertung von Informationen von vorhandener Client-Software
 1. Blacklisting
 2. Whitelisting

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Endpoint: Port scan/OS fingerp.



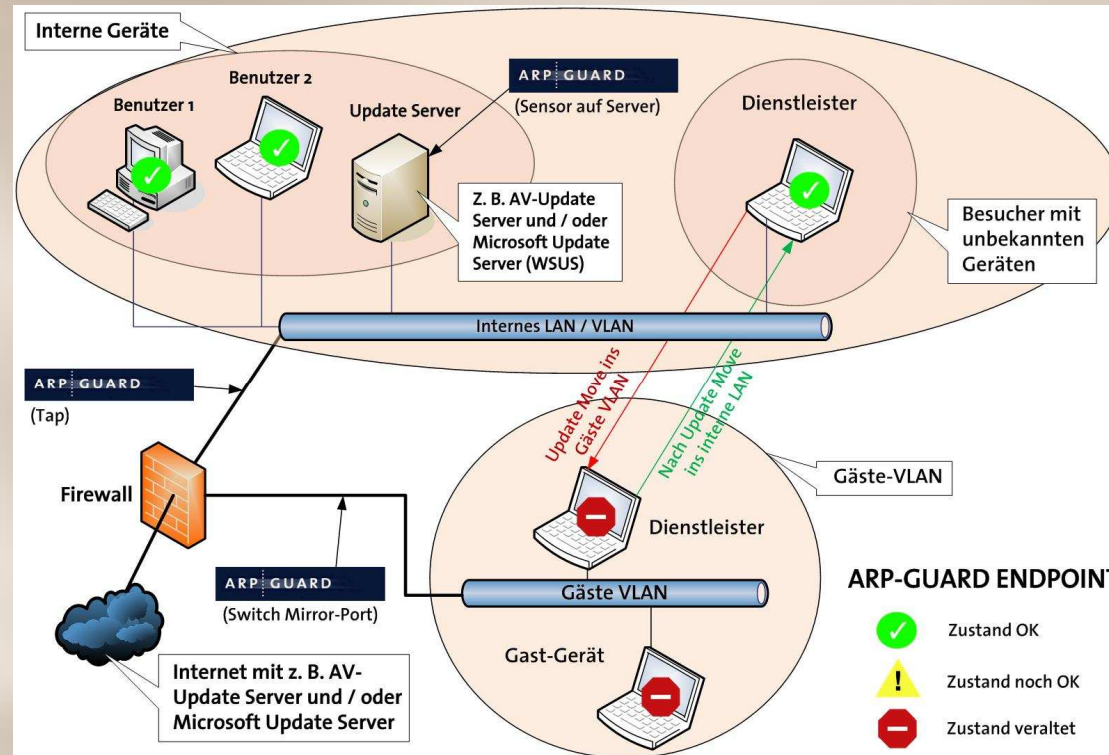
MAC-Adresse	Hersteller	IP-Adresse	DNS Name	of_name	ps_list
00-1A-E8-29-AA-95	Siemens	10.128.1.5	oip001ae829a...	Linux 2.4.X	T443
00-0E-A6-5D-59-0F	ASUSTEK	172.18.250.48		Microsoft Windows Vista 2008	T135, T139, T445, T5357, T49152, T4915...
00-0E-A6-5D-59-0F	ASUSTEK	10.128.1.48	scotty.isl.d...	Microsoft Windows Vista 2008	T135, T139, T445, T5357, T49152, T4915...
00-0E-A6-5D-59-0F	ASUSTEK	192.168.2.48		Microsoft Windows Vista 2008	T135, T139, T445, T5357, T49152, T4915...
00-1A-E8-27-5E-BD	Siemens	10.128.1.4		Linux 2.4.X	T443
00-1A-E8-2A-82-A7	Siemens	10.128.1.6	oip001ae82a8...	Linux 2.4.X	T443
00-08-DA-62-33-7B	SofaWare	10.128.1.254	firewall-int...	Check Point Linux 2.4.X	T22, T53, T80, T443
00-08-DA-62-33-7B	SofaWare	3.197.112.164	n003-000-000...	Check Point Linux 2.4.X	T22, T53, T80, T443
6C-F0-49-1B-20-6F		10.128.1.129	sato.isl.de	Microsoft Windows Vista 2008	T80, T135, T139, T445, T1720, T2000, T3...
00-1A-E8-27-33-0F	Siemens	10.128.1.7	riker.isl.de	Linux 2.4.X	T443

secudos

Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Endpoint: Update-Server



Endpoint: Vorhandene Client-SW

Blacklisting:

- Endgeräte, die sich per Trap als veraltet oder infiziert melden, werden vom Netzwerk getrennt oder in die Quarantäne verschoben.

Whitelisting:

- Endgeräte, die regelmäßig Updates melden, werden als „aktuell“ geführt. Nach einer vorgegebenen Zeit ohne Update gelten die Geräte als „veraltet“ und werden vom Netzwerk getrennt oder in die Quarantäne verschoben.

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Beispiel: Trend Micro: 35 Traps

Blacklisting:

- VirusFound
- CM_SpecialVirusAlert
- CM_VirusOutbreakAlert
- DiskFull
- OtherError
- OutbreakAlert
- QuarantineAlert

Whitelisting:

- EncyclopediaUpdateSuccess
- EngineUpdateSuccess
- ManualScanStartSuccess
- ManualScanStop
- PatternUpdateSuccess
- ProgramUpdateSuccess
- RealtimeScanStartSuccess
- RealtimeScanStop
- ScanNowSuccess
- ScheduleScanStartSuccess
- ScheduleScanStop

Endpoint: Beispiel

The screenshot shows the ARP-GUARD management interface in Mozilla Firefox. The browser address bar displays <https://www.arp-guard.com/management/admin/endpoint/result/status.epl?hide=9>. The interface has a navigation menu with 'Info', 'Sensor', and 'Management' tabs. The 'Management' tab is active, and the 'Endpoint' section is selected in the left sidebar. The main content area is titled 'Endpoint Zustand' and displays a table of endpoint status.

10 Einträge | Seite 1 | Seitenlänge 10 20 50 100 Max.

Endpoint-Status	MAC-Adresse	MAC-Name	MAC-Gruppe	Hersteller
⊖	00-0C-29-90-60-DA	Server quark.isl.de	Windows-Server	VMware
⊕	00-24-E8-DB-B4-E0	Notebook von Frau Eidmann	Windows-Notebooks	Dell
⊖	A4-BA-DB-C4-A1-38	Neues Notebook von Herrn Thermann	Windows-Notebooks	
⊕	00-0C-29-E5-56-52	Server paris.isl.de	Windows-Server	VMware
⊕	00-0C-29-1D-50-94	Server odo.isl.de	Windows-Server	VMware
⊕	00-25-11-1C-18-34	PC von Frau Schmermbeck	Windows-PCs	ELITEGROUP
⊕	00-0E-A6-5D-59-0F	PC von Herrn Thermann	Windows-PCs	ASUSTEK
⊕	6C-F0-49-1B-20-6F	TK-Anlage	Windows-Server	
⊕	A4-BA-DB-B3-56-BA	Neues Notebook von Herrn Rieke	Windows-Notebooks	
⊕	00-0C-29-3D-86-CB	Server picard.isl.de	Windows-Server	VMware

Fertig

secudos

Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

Roadmap

Wir haben uns viel für dieses Jahr vorgenommen:

- Grafische Darstellung der Topologie
 - Export in Standardformate
- Erweiterungen für RADIUS/802.1x
- Ausbau Reporting
 - Periodisch generierte PDFs
- Viele andere kleinere Verbesserungen

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Referenzen

Printmedien:

- ntz
- LANline
- Linux-Magazin
- deutsches Fernsehen
- <kes>
- c` t
- Heise Security
- iX

Messen:

- Systems 2003 – 2008
- it-sa 2009
- Cebit 2005 - 2010
- Security 2008
- ITIP 2008 – 2009 (Philippinen)
- Infosecurity (Brüssel/Utrecht)
- Orbit IEX (Basel)

Demnächst: it-sa 2010

SECUDOS

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.

ARP-GUARD: Referenzen



Es ist selbstverständlich, dass nur diejenigen Kunden dargestellt sind, die dem ausdrücklich zugestimmt haben.



MIT SICHERHEIT IN DIE ZUKUNFT.

Kontakt

Thomas Stutz, Omicron AG

Industriestrasse 50b, CH 8304 Wallisellen

Fon: +41 (0)44 839 11 11, Fax: +41 (0)44 839 11 00

<http://www.omicron.ch/>, Thomas.Stutz@Omicron.ch

Dr. Andreas Rieke, ISL Internet Sicherheitslösungen GmbH

Bergstrasse 128, D 58095 Hagen

Fon: +49 (0)2331/34956-0, Fax +49 (0)2331/34956-29

<http://www.isl.de/>, andreas.rieke@isl.de

V 2.2.2 R 1

secudos

 Omicron

ISL
MIT SICHERHEIT IN DIE ZUKUNFT.