

Self Defending Networks

Dror-John Röcher
droecher@ernw.de



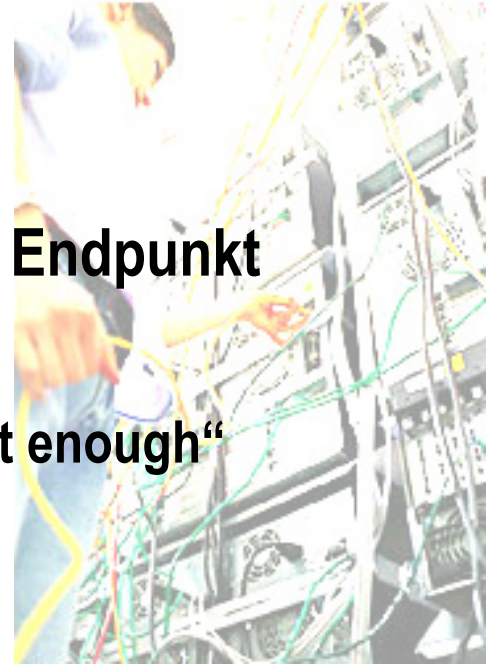
Agenda

1. Fokus: Sicherheit am Endpunkt
 1. Kritik der Perimeter-Security
 2. Aufgaben der Endpunkt-Security
2. Self-Defending Networks
 1. Allgemeine Konzepte
 2. Beispiel Cisco NAC (Network Admission Control)



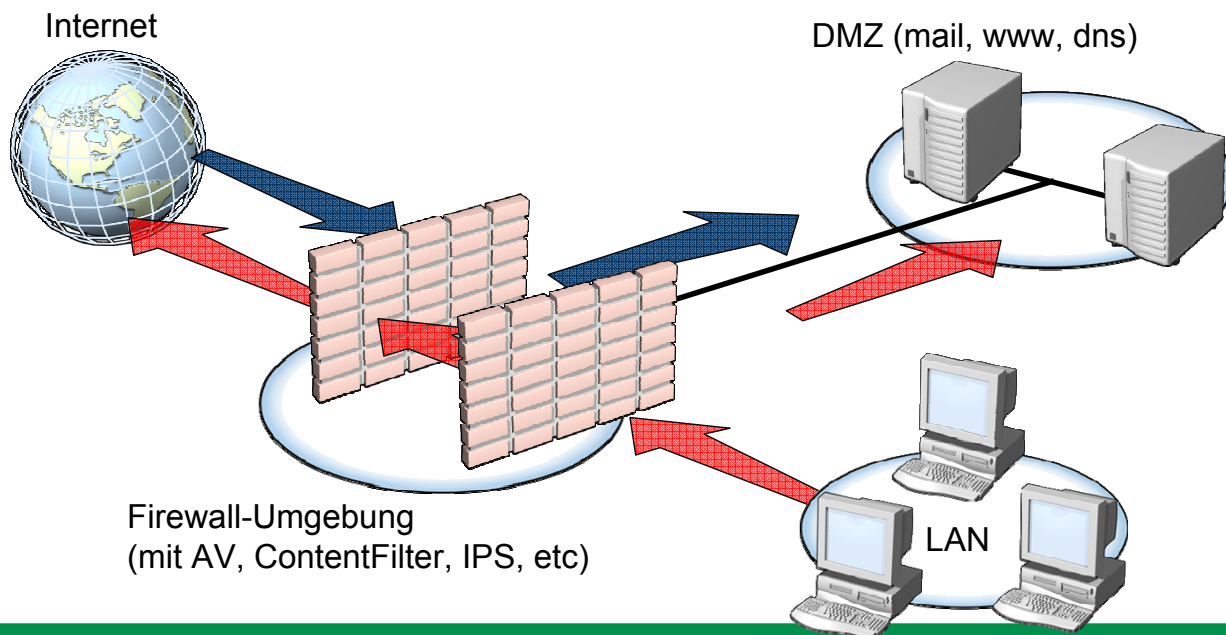
1. Fokus: Sicherheit am Endpunkt

„Perimeter Security is not enough“



1.1 Kritik der Perimeter Security





Das klassische Firewall Konzept

- Das „klassische“ Firewall-Konzept entspricht dem heute noch sehr weit verbreiteten Design.
- Die „Firewall“ kann dabei durchaus aus mehreren Einzelkomponenten bestehen.
- Zentrale Komponenten sind dabei:
 - Perimeter Defense (Abwehr der Gefahren an der Netzwerk-Grenze)
 - Choke Point: Der gesamte Verkehr muss über diesen Punkt fließen und wird dort kontrolliert.
- Das Design setzt (implizit) voraus:
 - Alle internen Hosts sind vertrauenswürdig
 - Alle internen Systeme haben denselben Schutzbedarf.
 - Es gibt eine klare Grenze zwischen 'innen' und 'außen'
 - Gefahren kommen in erster Linie 'von außen'.
 - Die Firewall kann diese Gefahren erkennen und abwehren.



■ „Vertrauenswürdige interne Systeme“

- In den internen Netzen sind zunehmend Geräte, die dort nur temporär sind (Laptops, PDAs/MDAs, Geräte ext. Mitarbeiter, ggf. private PCs)
- Die Vertrauenswürdigkeit hängt von der Konfiguration (Patch-Level, Signaturen, Hardening) ab
- Dies können Firewall-Administratoren i.d.R. nicht einschätzen, da unterschiedliche Abteilungen für Firewalls und Desktops zuständig sind.



■ „Grenze zwischen Innen und Außen“

- Grenze wird aufgeweicht durch temporär angeschlossene Geräte.
- Netze werden logisch erweitert (VPNs), die Endpunkte sind „jenseits“ der Kontrolle.
- Netze werden physisch erweitert (WLAN, Bluetooth).
- Dazu kommen noch Partnerzugänge, Wartungszugänge... die den Firewall-Regelsatz unübersichtlich und damit fehleranfällig machen



Klassische Perimeter-Security wird aktuellen Architekturen nicht gerecht.

Endpunktsicherheit ist eine zentrale Komponente einer erfolgreichen IT-Security Strategie.

p.s.

Und trotzdem versuchen immer mehr Hersteller Ihnen die „eierlegende-Perimeter-Defense-Wollmilchsau“ zu verkaufen, die an sich schon gegen eines der grundlegenden Prinzipien der Netzwerksicherheit, `segregation of duties`, verstößt.



1.2 Aufgaben der Endpunkt-Security



„Endpoint Security“ vs. „Perimeter Defense“

	Perimeter Defense	Endpoint Security
Netzwerk Umgebung	<ul style="list-style-type: none"> ■ 10-50 Systeme, die zu schützen sind. ■ ~ 10 Mbps Verkehr, der zu inspizieren und kontrollieren ist. 	<ul style="list-style-type: none"> ■ > 1000 Systeme, die zu schützen sind. ■ > 1000 Mbps Verkehr, der zu inspizieren und kontrollieren ist.
Applikations Umgebung	<ul style="list-style-type: none"> ■ ~ 10 Applikationen. ■ ~ 10 Protokolle. ■ standardisierte Applikationen. ■ standardisierte Protokolle, strikte Einhaltung der Standards. ■ Client-Server Applikationen. 	<ul style="list-style-type: none"> ■ > 500 Applikationen. ■ > 100 Protokolle. ■ Eigenentwicklungen. ■ nicht standardisierte Protokolle, bzw. keine strikte Einhaltung der Standards. ■ Peer-to-Peer & Client-Server Applikationen.
Management Umgebung	<ul style="list-style-type: none"> ■ ~ 10 User-Gruppen bzgl. der Policy. ■ Alles unbekannte wird geblockt. ■ I.d.R. zentral verwaltet. 	<ul style="list-style-type: none"> ■ > 100 verschiedene User-Gruppen und Rollen. ■ Beobachte unbekanntes Verkehr, aber bitte nicht blocken (bloß kein Unterbrechung des Produktivbetriebs). ■ I.d.R. dezentral/lokal verwaltet.



Bedrohungen durch Endpunkte

- Verfügbarkeit von Systemen/Netzen
 - Z.B. Verfügbarkeit des Netzwerkes bei SQL-Slammer Ausbruch.

- Vertraulichkeit von Daten
 - Spyware sammelt Benutzerverhalten, Passwörter, Zugangskennungen ein.
 - Speziell angepasster Malicious Code sammelt gezielt vertrauliche Dokumente eines einzigen Opfers (Stichwort: Wirtschaftsspionage). [1]

- Missbrauch von Ressourcen
 - Gehackter Endpunkt als Relay für weitere Angriffe.
 - Gehackter Endpunkt als Knoten eines Botnet (Spam-Schleuder, DDoS Plattform, Stealth-Hosting)



Sicherheit rund um den Endpunkt...

- Sie haben:
 1. Zentral administrierte clientseitige Antivirus-Lösung mit funktionierenden Updates
 2. Zentrale Spam-Filterung und Antivirus für Ihre Emails, inklusive Quarantäne
 3. HTTP-Zwangs-Proxies mit Content-Filter
 4. Zentral administrierte Desktop-Firewalls
 5. Softwareeinschränkungen durch Group Policy Objects im ActiveDirectory
 6. Eingeschränkte User-Rechte (auch für VIPs, Laptops und Entwickler)
 7. Einen funktionierenden Patch-Management Prozess (auch für MDAs und Unixe)
 8. 802.1x basierte Sicherheitsmechanismen (z.B. Identitäts-basierte VLAN-Zuordnung)
 9. Eine von Ihren Mitarbeitern gelebte Security Policy ;-)

- Wenn Sie mehr als 6 Punkte ohne Abstriche „bejahen“ können, sind Sie besser als der Durchschnitt (Herzlichen Glückwunsch!).



Sicherheitsmassnahmen am Endpunkt...

- Sie haben:
 1. Zentral administrierte clientseitige Antivirus-Lösung mit funktionierenden Updates
 2. Zentrale Spam-Filterung und Antivirus für Ihre Emails, inklusive Quarantäne
 3. HTTP-Zwangs-Proxies mit Content-Filter
 4. Zentral administrierte Desktop-Firewalls
 5. Softwareeinschränkungen durch Group Policy Objects im ActiveDirectory
 6. Eingeschränkte User-Rechte (auch für VIPs, Laptops und Entwickler)
 7. Einen funktionierenden Patch-Management Prozess (auch für MDAs und Unixe)
 8. 802.1x basierte Sicherheitsmechanismen (z.B. Identitäts-basierte VLAN-Zuordnung)
 9. Eine von Ihren Mitarbeitern gelebte Security Policy ;-)

- Wenn Sie mehr als 6 Punkte ohne Abstriche „bejahen“ können, sind Sie besser als der Durchschnitt (Herzlichen Glückwunsch!).

und trotzdem...



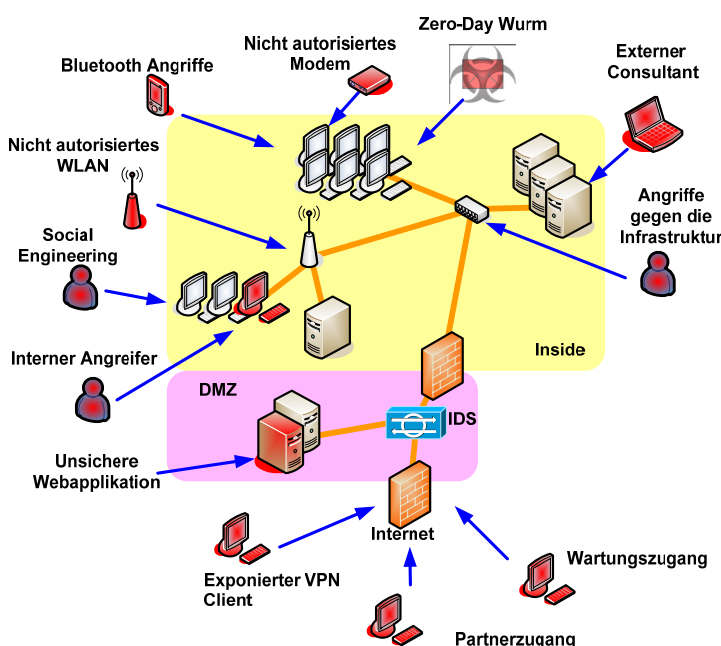
- Haben Sie Wurm-Traffic innerhalb Ihres Netzwerks?
- Sind nicht alle Systeme auf dem gleichen Patchlevel?

- Und wie begegnen Sie Zero-Day Angriffen?

- Oder anders ausgedrückt:
 - Die Endpunkte befinden sich nicht immer unter Ihrer Kontrolle... Je mobiler die Endpunkte, umso seltener sind diese im Unternehmensnetzwerk (wo sie Patches & Updates erhalten).
 - In Ihrem Netzwerk sitzen Endpunkte, die Sie nicht kontrollieren können (externe Berater, Partner, Kunden).
 - Endpunkte, von denen Sie keine Kenntnis besitzen, können Sie auch nicht kontrollieren.
 - Wie behandeln Sie Endpunkte, die z.B. veraltete Virensignaturen oder nicht den aktuellen Patchlevel haben, oder die in sonst irgendeiner Weise nicht Ihrer Security Policy entsprechen? Bekommen diese Zugang zum Netz?



Einige Bedrohungen im Überblick



- Perimeter Security versagt bei neuen Bedrohungen.
- Aktuelle Endpoint-Security Lösungen können gegen die Vielzahl an Bedrohungen wenig ausrichten, oder sind schlichtweg nicht managebar

- Da alles „am Netzwerk“ angeschlossen ist, ist „das Netzwerk“ der logische Ort um umfassende Kontrollmaßnahmen einzurichten.



Aktuelle Endpunkt-Sicherheitsmassnahmen sind unzureichend.

**Neue Technologien zum Schutz der Unternehmens-IT sind notwendig:
Umfassende Security muß auf einer Verschmelzung von Netzwerk- und Endpoint-Security basieren.**



2. Self-Defending Networks - Konzepte

Am Beispiel: Cisco Security Agent & Cisco Trust Agent



2.1 Generelle Konzepte



Generelle Konzepte

1. Der Zugang zum Netzwerk wird reglementiert anhand des Zustands eines Endpunktes (Policy basierter Zugang):
 - Zugang kann z.B. bedeuten: VLAN, ACLs, URL-Redirection, Quarantäne
 - Zustand kann z.B. ermittelt werden anhand von: Authentifizierung, installierter Software (AV, Firewall), Patchlevel, installiertem Betriebssystem



Generelle Konzepte

2. Das Netzwerk reagiert auf Zustandsänderungen des Endpunktes:
 - Bei Infektion wird das System in Quarantäne genommen.
 - Angriffe auf einen Endpunkt können zu Reaktionen auf anderen Endpunkten führen.

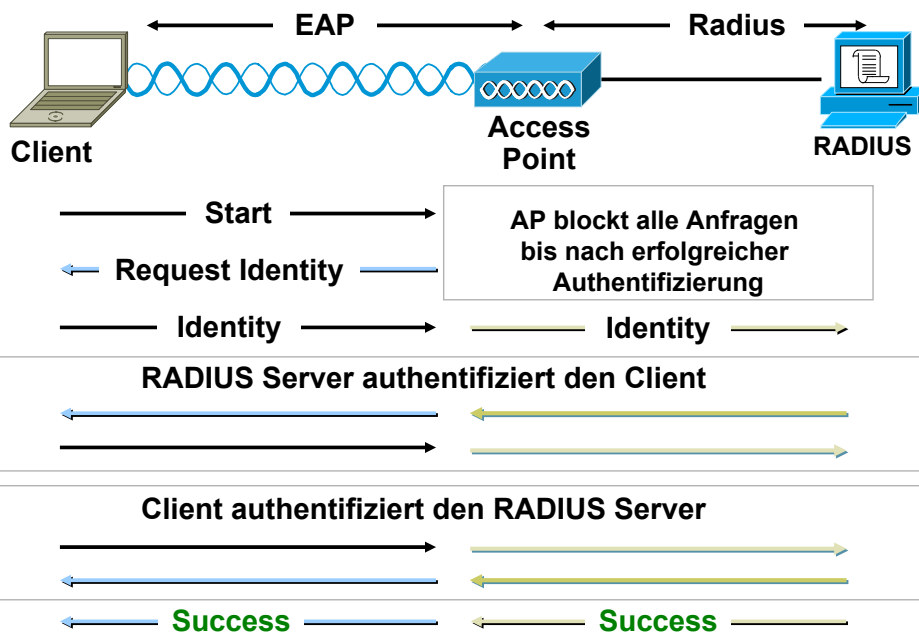


Generelle Konzepte

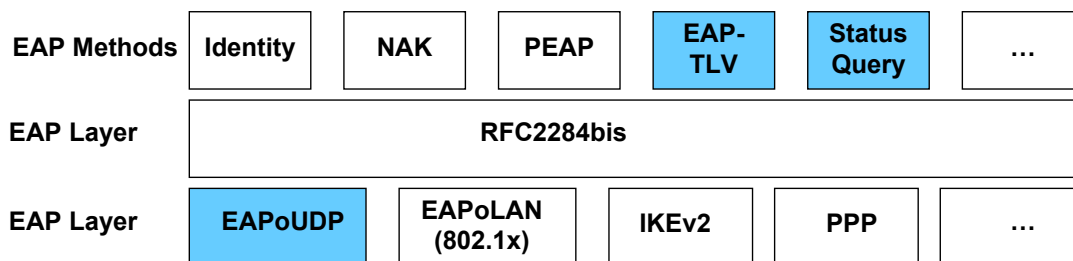
3. Ein Agent überwacht auf Betriebssystem-Kernel-Level alle Aktivitäten:
 - Potentiell schädliche Aktionen werden verhindert, wodurch unbekannte Angriffe oder Viren keine Auswirkungen haben (Schutz vor Zero-Day Angriffen).



“Alter Hut”: 802.1X Authentifizierung im WLAN



Extensible Authentication Protocol (EAP) [5]

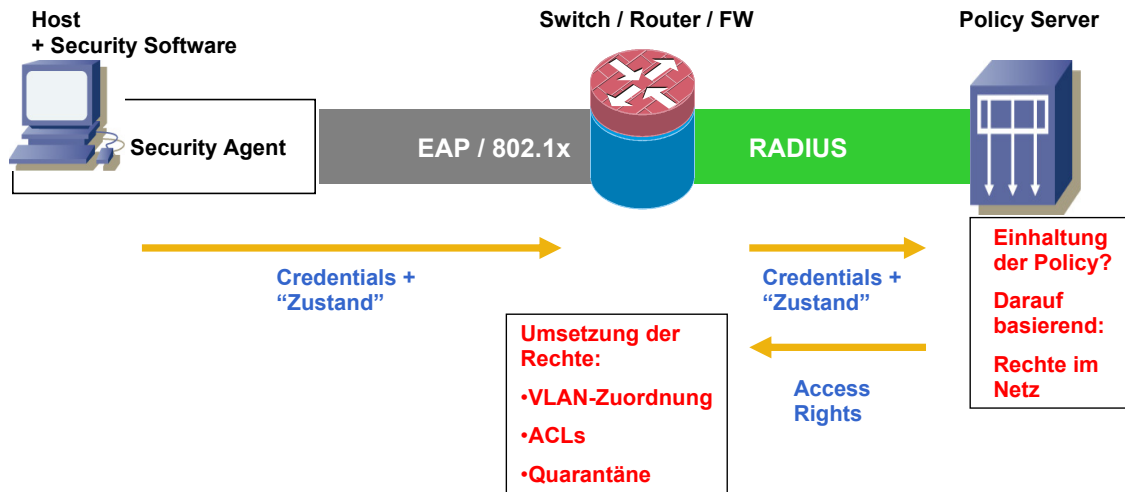


- EAP ist ein “request-response” Protokoll:
 - Austausch von Identität & Authentifizierungs-Informationen zwischen einem Peer und einem AAA Server
- Unterstützt eine Vielzahl verschiedenen Authentifizierungs-Mechanismen
 - EAP-MD5
 - EAP-MSCHAP
 - ...
- EAP muß für Policy basierte Zugangskontrolle erweitert werden
 - EAP-TLV: Zustands-Informationen
 - Status Query: neue EAP Methode um den Zustand eines Peers abzufragen
 - EAPoUDP: EAP Transport über IP (statt über Layer2 wie bei 802.1x)

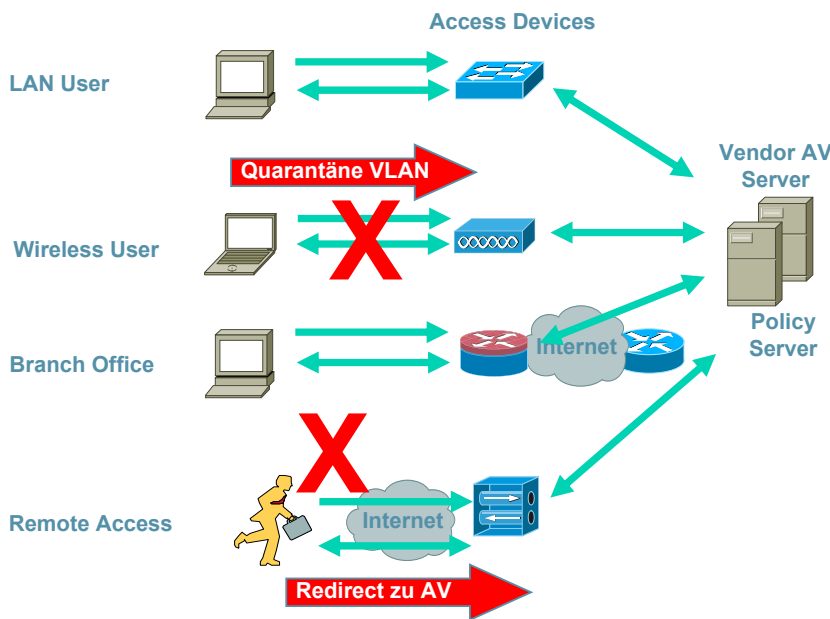
Neue Funktion



Kommunikationsschema: Policy basierte Zugangskontrolle



Policy-basierte Zugangskontrolle



1. Neue L2 oder L3 Verbindung durch Access Device festgestellt
2. Access Devices "befragt" Security Agenten auf dem Endpunkt
3. Policy Server vergleicht Information mit Policy. Entscheidung (OK, Deny, Quarantäne)
4. Access Device setzt Entscheidung um

2.2 Cisco „Self Defending Networks“



Cisco “Self Defending Network” - Komponenten

■ Endpoint Protection – CSA

Reduziert Patch- & AV-Signaturupdate Druck durch ‘verhaltens-basierten’ Schutz. [2]

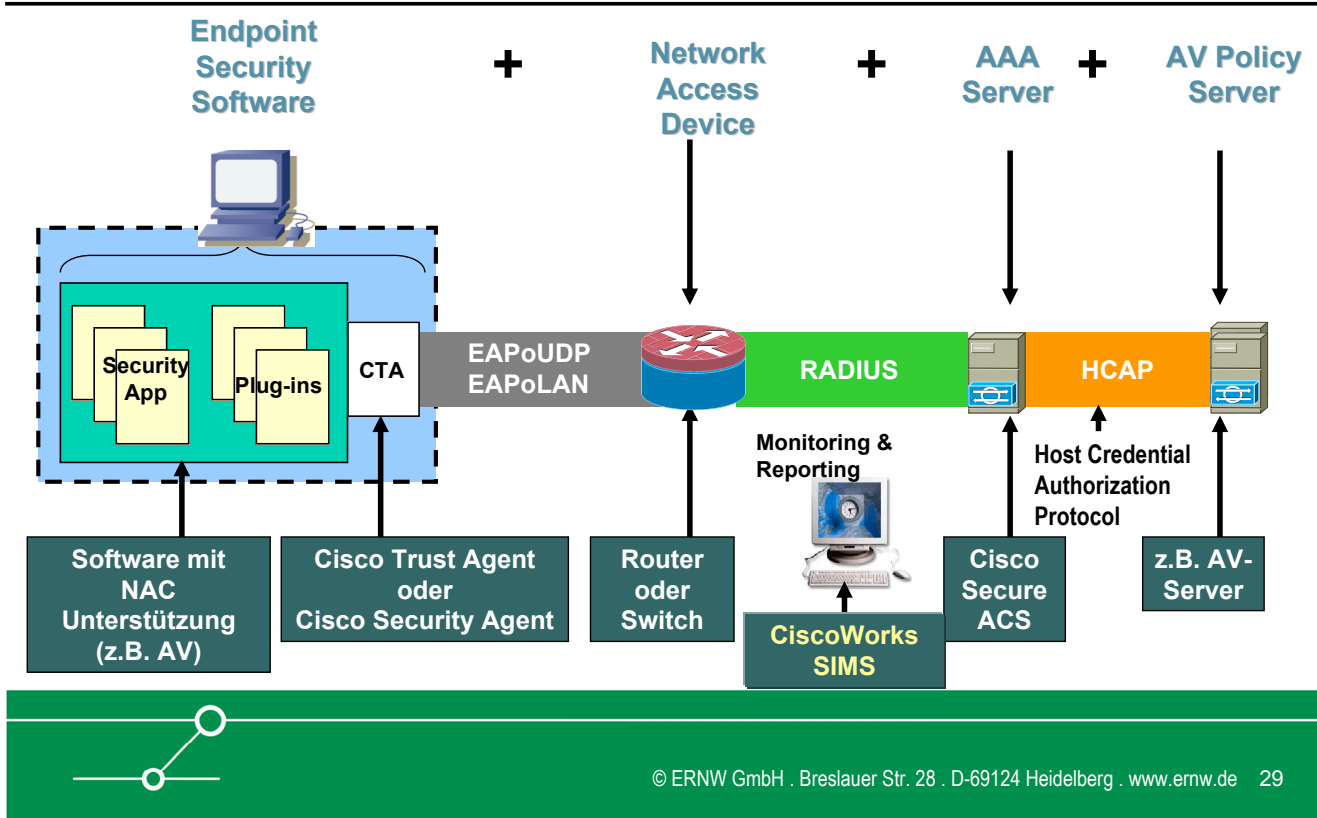
■ Network Admission Control – NAC

Auditierung und Durchsetzung der Endpoint Security Policy beim Zugriff auf das Netzwerk. [3]

■ Incident Control System - ICS

Eingrenzung der Auswirkungen von Infektionen durch Isolation infizierter Systeme. [4]





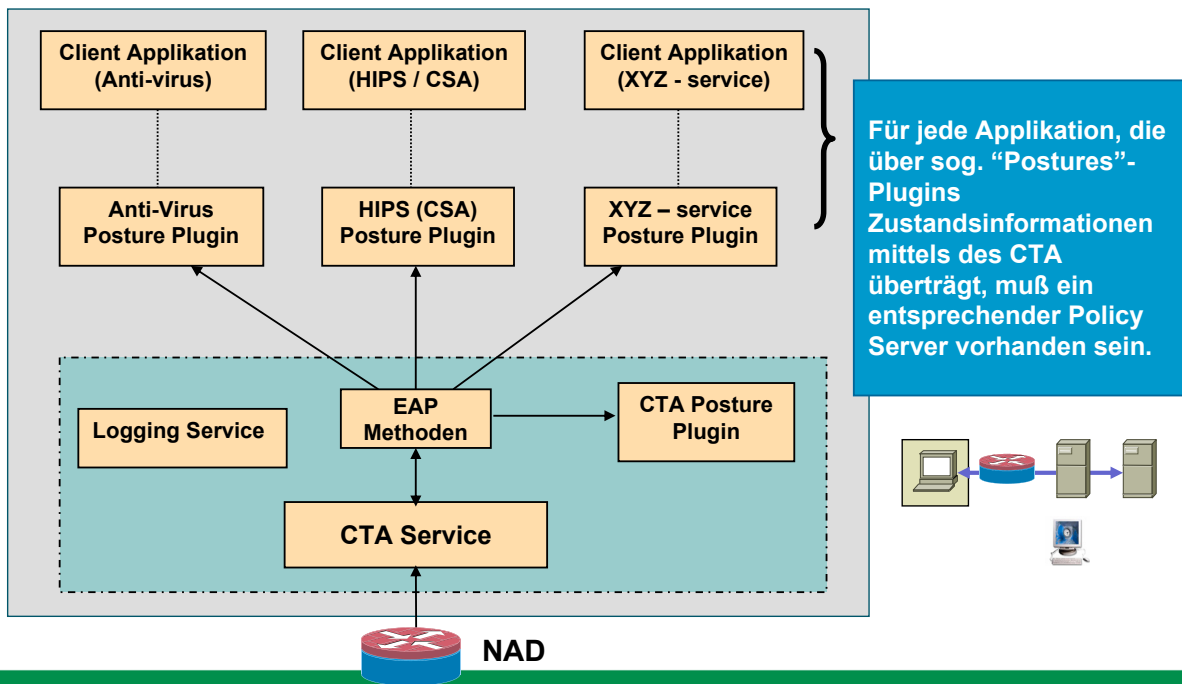
Cisco Trust Agent (CTA)

■ Cisco Trust Agent

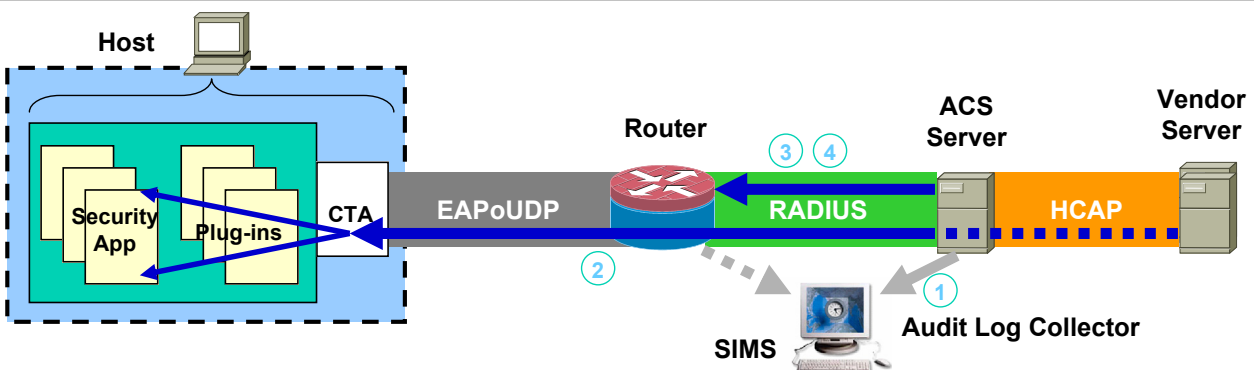
- Software, die auf dem Endpunkt installiert wird und die Kommunikation mit dem Network Access Device durchführt (EAPoUDP, EAPoLAN).
- Antwortet auf Anfragen von Network Access Devices mit Endpoint Security Credentials.
- Sammelt Security Zustandsinformationen von Endpoint Security Software (AV, CSA, etc.).
- Elementarer Bestandteil von Cisco Network Access Control (NAC).
- Wird gebündelt mit unterstützter AV Software (z.B. TrendMicro OfficeScan Enterprise, McAfee VirusScan / ePO).
- Initialer Fokus: AntiVirus



CTA: Architektur & Komponenten



Posture Check Ergebnis



- Posture Check ergibt folgende Ergebnisse
 1. [Audit logging für administrativen Feedback](#)
 2. [In-band Benachrichtigung für Applikationen & User](#)
 3. [Out-of-band User-Feedback per URL-Redirection](#)
 4. [Dynamische Autorisierung per ACLs](#)
- Die ersten 3 Ergebnisse sind "Feedback Loops"
- Das letzte Ergebnis stellt den eigentlichen Zustand fest

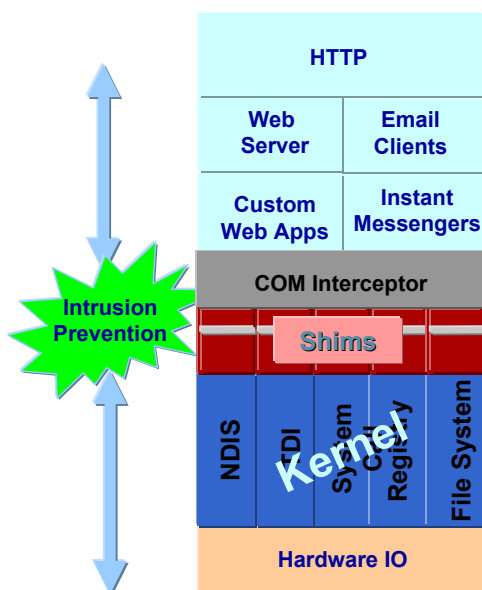
Cisco Security Agent (CSA)

- Security Agent mit umfangreicher Funktionalität
 - HIPS für Desktop & Server Betriebssysteme
 - Distributed Firewall
 - Schutz vor Malicious Code
 - Gewährleistung der Integrität des Betriebssystems
 - Windows, Solaris, Linux
 - Schutz vor „Zero Day“
 - Keine „Signatur-Updates“, da CSA das „Verhalten“ des Systems untersucht
 - CTA ist Bestandteil des CSA



CSA Betriebssystem Integration

CSA: Kernel Shim Wrappers



- Bietet Betriebssystem Credentials & Endpoint Integrität
 - BS Info inklusive Patches & Hotfixes
 - Härtung des Betriebssystems
 - Schützt CTA vor Anwendungs-Spoofing
- NAC Unterstützung
 - CSA 4.5 beinhaltet CTA



CSA & Traditionelle AV

	CSA	Anti-Virus
Malicious Code		
Stop bekannter Viren/Würmer	X	X
Stop Unbekannter Viren/Würmer	X	
Scan/Erkennung infizierter Dateien		X
“Clean” infizierter Dateien		X
Identifizierung von Viren/Würmern		X
Kommt ohne Signatur-Updates aus	X	
Distributed Firewall	X	
Betriebssystem Härtung	X	
Korrelation von Events über alle Endpunkte	X	



CSA & Traditionelle HIDS / Desktop Firewall

	CSA	Personal Firewall	Conventional Host-based IDS
Desktop/Laptop Protection	X	X	X
Block Eingehender Netzwerk Verbindungen	X	X	
Block Ausgehender Netzwerk Verbindungen	X	X	
Stateful Packet Inspection	X	X	
Detect /Block Port Scans	X	X	
Detect /Block Netzwerk DoS	X	X	
Detect /Prevent Malicious Code	X		X
Detect/Prevent Bekannte Buffer Overflows	X		Detect
Detect/Prevent Unbekannte Buffer Overflows	X		
Detect/Prevent Unautorisierte Dateimanipulation	X		Detect
Betriebssystem Härtung	X		X





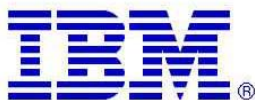
- NAI / Mcfée
 - Integration in VirusScan 8.0i
 - ePO & CTA Integration



- Symantec
 - SAV 9.0 [AV] & SCS 2.0 [AV, FW, HIDS] Integration
 - Policy Manager & CTA Integration



- Trend Micro
 - OfficeScan Corporate Edition
 - Trend Micro Control Manager & CTA Integration



- IBM
 - Tivoli Integration geplant



Referenzen

- [1] <http://www.heise.de/security/news/meldung/60056>
- [2] <http://www.cisco.com/go/csa>
- [3] <http://www.cisco.com/go/nac>
- [4] <http://www.cisco.com/go/ics>
- [5] <http://www.networksorcery.com/enp/rfc/rfc3748.txt>
- [6] <http://www.ieee802.org/1/pages/802.1x.html>



Vielen Dank!

Fragen und Antworten?

