

Schluss mit dem Versteckspiel !

Laptops und schnurlose IP-Telefone bringen enorme Produktivitätsvorteile, bieten aber auch zusätzliche Angriffspunkte für Computerviren, Würmer oder Hackerangriffe. Mobilität macht das Unternehmensnetz verwundbar, weshalb sich Schutzvorrichtungen mehr und mehr vom Netzwerkrand ins Innere verlagern. Die Verteidigungsintelligenz ist heute quer über die ganze Infrastruktur auf Router, Switch-Ports und auf Wireless Access Points und die Endgeräte verteilt. Nur: Wie lassen sich in einem derart dezentralen Abwehrszenario Sicherheitsrichtlinien situationsgerecht und mit vertretbarem Aufwand zum Beispiel auf einer Distributed Firewall einrichten und durchsetzen? Nutzeridentität und Hardwarekennung helfen allein nicht mehr weiter. Denn das Netzwerk und das Endgerät müssen nicht nur wissen, wer sich wann mit welchem Gerät einloggt, sondern auch von welchem Standort aus.

Ganz selbstverständlich loggen sich Mitarbeiter heute von zu Hause aus ins Firmennetz ein und greifen auf Geschäftsreise via Hot Spot im Hotel oder am Flughafen auf unternehmenskritische Informationen zu. Besuchern bietet der Netzanschluss im Konferenzraum willkommene Gelegenheit, um sich sicher mit dem eigenen Firmennetzwerk zu verbinden. Und immer öfter erhalten Geschäftspartner per VPN (Virtual Private Network) Zugang zu Anwendungen und Datenbanken. Die Grenze zwischen Inter- und Intranet verschwimmt. Hinzu kommt, dass Gebäudemauern keine Grenze mehr für Netzwerke darstellen, denn Funkwellen drahtloser Netze durchdringen auch Stein und Beton und sind bestens auf dem Parkplatz zu empfangen.

Um die Sicherheit im Unternehmensnetz zu gewährleisten sind deshalb zwei Problembereiche zu adressieren:

1. Welche Geräte befinden sich im internen Netzwerk – drahtlos und drahtgebunden – und in welchem Sicherheitszustand sind diese?
2. Und natürlich die umgekehrte Betrachtung – in welchem Netzwerkkontext befindet sich ein Endgerät und kann ich dort die entsprechende Sicherheitsrichtlinie durchsetzen?

Ja wen haben wir den da? – Lokalisierung nicht Richtlinienkonformer Endgeräte

Endgeräte deren Antivirus-, Host-based-Intrusion-Detection-, oder Personal-Firewall-Produkte oder deren Betriebssystem- und Anwendungssoftware nicht auf dem aktuellen Stand sind, stellen ein Risiko für die Unternehmenssicherheit dar. Ein solches Gerät kann die Ursache für eine Neuinfektion mit einem Wurm oder Virus sein, den der PC-Betrieb zwar gerade mühsam beseitigt hatte, aber nicht auf dem Rechner des mobilen Mitarbeiters, weil dieser zu dem Zeitpunkt nicht im Haus war. Nicht konforme oder gar infizierte Endgeräte lassen sich bisher nur sehr schwer identifizieren. Meist erfolgt die Prüfung von Endgeräten während des Logins. Zu diesem Zeitpunkt hat das Endgerät jedoch vollen Netzwerkzugang, das heißt DHCP ist bereits erfolgreich gelaufen, uneingeschränkter IP-Zugang zum lokalen Firmennetzwerk besteht und ein netzbasierter Schädling kann sich weiterverbreiten, ohne dass es eine Möglichkeit gibt ihn zu stoppen – bisher jedenfalls.

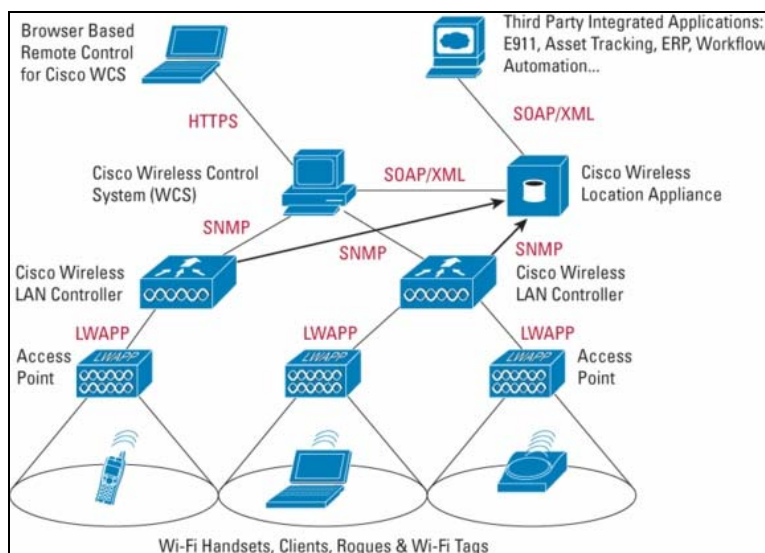
Wie sieht es überhaupt damit aus, Endgeräte im Unternehmen zu lokalisieren? Im LAN kann man hierzu auf die Statusinformationen der Ethernet-Infrastruktur zurückgreifen, diese mit den Verkabelungsinformationen verknüpfen und erhält so die Position des aktiven Gerätes. Dies liefert jedoch nur wenig Informationen darüber, wer den aktiven Port wirklich nutzt und ist mit ein Grund dafür, dass dieses Verfahren keine Anwendung findet. Führt man Port-basierte Authentifizierung ein, beispielsweise mit Hilfe von 802.1X, erhält man weitere Details, wie beispielsweise die Geräte- oder die Benutzer-Identifikation, je nachdem welches Merkmal verwendet wurde; über den Sicherheitszustand sagt dies jedoch immer noch nichts aus.

Positionsbestimmung im Wireless-LAN

Im Wireless-LAN ist es noch wichtiger zu wissen, welche Geräte sich wo genau auf dem Unternehmensgelände befinden. Nicht von der IT-Abteilung installierte und kontrollierte WLAN-AccessPoints können, wenn sie falsch konfiguriert sind, ein Einfallstor für Angreifer darstellen, genauso wie WLAN-NICs, die im „ad-hoc“ Modus arbeiten. Darüber hinaus ist ein Location-Service für Anwendungen wie IP-Telefonie über WLAN absolut notwendig um beispielsweise die Notruf-Funktion

realisieren zu können. Ein weiterer praktischer Nebeneffekt ist, dass mobiles Equipment mit Hilfe von RFID-Tags markiert und jederzeit lokalisierbar ist, wodurch sich Verlust- und Diebstahlraten deutlich reduzieren lassen.

Der effizienteste und kostengünstigste Ansatz zur Client-Ortung im Funknetz nutzt Basisstationen nicht nur für den Traffic, sondern auch als Location Reader. Alle Access Points sammeln Received-Signal-Strength-Indicator-Informationen (RSSI) über die Geräte oder RFID-Tags in ihrer Reichweite und leiten diese via Lightweight Access Point Protocol (LWAPP) an den WLAN Controller weiter. Die zentrale Wireless Location Appliance korreliert diese Informationen, die über verschiedene Schnittstellen (SNMP, SOAP, XML) von den Controllern bereitgestellt werden, und stellt diese grafisch dar.



Liegen in der Appliance auch die kompletten Gebäudepläne nebst Grundriss und funktechnischem Raumprofil vor, können die RSSI-Informationen anhand konkreter Dämpfungs- und Reflexionseigenschaften der Umgebung nachjustiert und entsprechend präzisiert werden. Administratoren haben so jederzeit die aktuelle Verteilung aller Wi-Fi-Quellen im Blick.

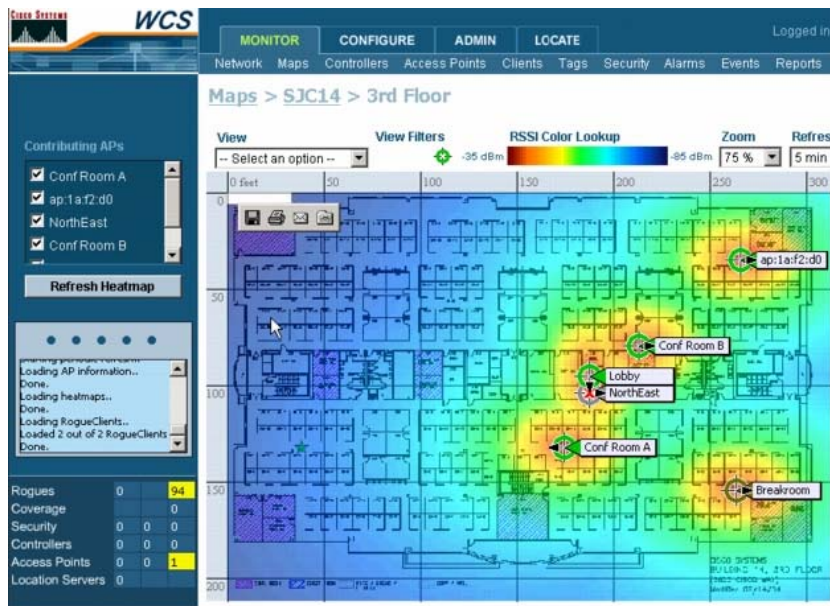


Abb.: Cisco Wireless Location Appliance: Real Time Simultaneous Location Tracking for Thousands of Users, Devices, and Access Points

Neben der Unterstützung der IT-Administration können mithilfe der Location-Information weitere Mehrwertdienste realisiert werden. Über XML oder SOAP lassen sich die Positionsdaten im Assetmanagement, Enterprise Resource Planning oder der Workflow-Automation einsetzen. Verschiedene vertikale Märkte wie Handel, Finanzen, Produktion oder Behörden, hier insbesondere das Gesundheitswesen, können so von Kosteneinsparungen durch Prozessoptimierung profitieren.

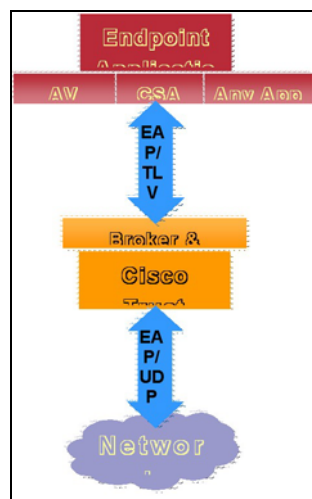
Rouges müssen draußen bleiben

Als „Rouge“ bezeichnet man Access Points, die unbefugt an einem Ethernetport angeschlossen worden sind. Über einen solchen Access Point kann unter Umständen unternehmenskritischer Datenverkehr von und zu jedem beliebigen nicht-autorisierten 802.11-Client weitergeleitet werden.

Die grafischen Gebäudepläne der Appliance verzeichnen auch metergenau den Standort eines Rouge Devices – noch bevor dieses für Angriffsversuche verwendet werden kann. IT-Administratoren können so die Geräte aufspüren und entfernen, bevor Schaden für das Unternehmen entsteht.

Was bedeutet Sicherheitszustand?

Um den Sicherheitszustand eines Endgerätes über die Netzwerkebene abfragen zu können, wird ein vertrauenswürdiger Agent – Cisco Trust Agent (CTA) – auf dem Endgerät benötigt. Um das Konzept so flexibel wie möglich zu halten, ist der eigentliche CTA ein sehr kleines, robustes und nicht tief in das Endgerätebetriebssystem eingreifendes Stück Software, das frei erhältlich ist. Was versteht man unter dem Sicherheitszustand eines Endgerätes und welche Informationen muss der CTA liefern, damit dieser von einem unternehmensweiten Richtlinienmanagement bewertet werden kann? Dies hängt ganz von der im Unternehmen verwendeten Sicherheitsrichtlinie ab. Beispielsweise kann es in einem Unternehmen ausreichend sein, wenn die Personal Firewall auf dem Endgerät installiert und aktiviert ist und das Antivirenprogramm den aktuellsten Signaturfile geladen hat. Für die Überprüfung dieses Zustandes braucht ein Sicherheitsadministrator deshalb folgende Informationen über das Endgerät: Ist die Personal Firewall installiert? Ist sie aktiv? Wurde sie in den letzten Stunden deaktiviert? Ist der Antivirusscanner installiert? Ist er aktiv? Welche Versionsnummer hat die AV-Signaturdatei?

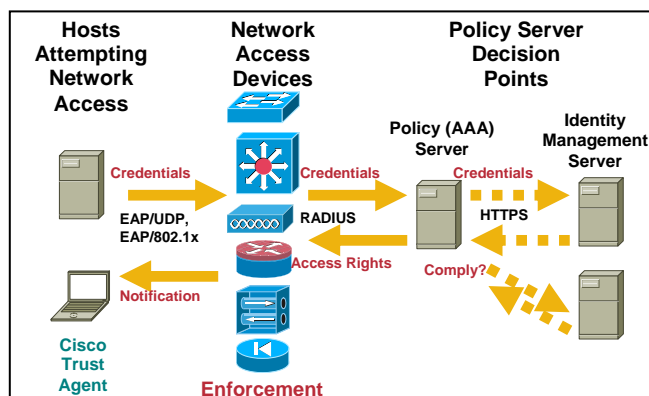


Der CTA selbst liefert nur sehr rudimentäre Informationen über das verwendete Betriebssystem. Die eigentliche Informationssammlung leisten so genannte Posture-Plug-Ins, die herstellerspezifisch und auf die jeweilige Software abgestimmt sind. Diese Plug-Ins werden von den meisten Herstellern mittlerweile gemeinsam mit ihrer

Softwareanwendung ausgeliefert, sodass NAC (Network Admission Control) direkt auf diese Informationen zugreifen kann.

Durchsetzung von Sicherheitsrichtlinien im Netzwerk

Die eigentliche Durchsetzung der Sicherheitsrichtlinie erfolgt auf dem ersten Netzwerkgerät (NAD), an das sich das Endgerät mit dem CTA für einen Verbindungsaufbau wendet. Das NAD blockt jeglichen Verkehr von diesem Endgerät und antwortet hierauf mit einem EAP Request (Extensible Authentication Protocol) auf der Netzwerkschicht, die vom Endgerät für den Verbindungsaufbau genutzt wird. Im LAN oder WLAN findet dies auf Layer 2 mit Hilfe von EAPoL (EAP over LAN) oder EAPoW (EAP over WAN) statt, also sehr früh im Aufbau der Verbindung, womit sich die eingangs geschilderten Probleme der bisherigen Verfahren umgehen lassen. Besteht bereits eine IP-Verbindung, weil sich das Endgerät beispielsweise per VPN anbindet, findet NAC auf Layer 3 per EAPoUDP statt. Der CTA beantwortet den EAP Request und meldet sich beim NAD zurück. Dieser leitet das Paket an den zentralen Richtlinienserver weiter, der eine sichere PEAP-Verbindung (Protected EAP) zum CTA aufbaut. Über die gesicherte Verbindung kann der Richtlinienserver alle sicherheitsrelevanten Informationen über das Endgerät abfragen und die Entscheidung treffen, ob das Endgerät der aktuellen Sicherheitsrichtlinie entspricht. Das Ergebnis teilt der Richtlinienserver dem CTA und gegebenenfalls über ein Mitteilungsfenster direkt dem Anwender mit. Die PEAP-Verbindung wird terminiert und das NAD ebenfalls über das Ergebnis in Form eines Token und einer Zugangspolicy informiert.



Die Sicherheitsüberprüfung durch den Richtlinienserver kann vier mögliche Zustände als Ergebnis haben, die den erlaubten Netzzugriff beschreiben: ACCES, DENY, RESTRICTED und QUARANTINE. Neben „Alles OK = Vollzugriff“ und „Objekt ist nicht vertrauenswürdig, weil beispielsweise kein CTA installiert oder wichtige Anforderungen der Sicherheitsrichtlinie nicht erfüllt = Kein Zugriff“ ist der Quarantäne-Fall der Schlüssel für eine umfassende Remediation-Lösung. Wurden Abweichungen zur Sicherheitsrichtlinie festgestellt, bekommt der CTA den Token QUARANTINE und der Endanwender kann mit Hilfe eines Pop-Up-Fensters über diesen Zustand informiert werden. Dem NAD wird vom Richtlinienserver ebenfalls der Token und eine entsprechende Accessliste mitgeteilt, die das NAD umsetzt. Im Quarantänefall wird das Endgerät in ein Quarantäne-Netzwerk umgeleitet (VLAN oder auch nur eine einzelne Route/ACL zu einem Remediationserver). Jetzt kann eine externe Sicherheitsüberprüfung oder nur eine Software ausgeführt werden, um das Endgerät wieder Sicherheitsrichtlinien-konform zu machen. Ist dieser Prozeß abgeschlossen, kann das Endgerät erneut einen Zugangsversuch machen, um diesmal den Token ACCESS oder RESTRICTED zu bekommen.

Durchsetzung von Sicherheitsrichtlinien – Offline?

Unternehmen setzen mehr und mehr auf Mobilitätslösungen und müssen daher auch für die Sicherheit der Endgeräte sorgen, wenn diese unterwegs sind und nicht über die Mechanismen im LAN geschützt und kontrolliert werden können. Auch in diesem Fall spielt wieder die Bestimmung des Ortes, diesmal aus Sicht des Endgerätes – wo befinde ich mich, in welchem Netzwerk? – eine Rolle. Je nachdem in welchem Netzwerk-Kontext sich das Gerät befindet, müssen unterschiedliche Sicherheitsregeln umgesetzt werden. Beispielsweise könnte die höchste Sicherheitsstufe vorsehen, dass nur die Anmeldeseite eines Hot-Spots per HTTP erreicht und maximal ein VPN-Tunnel zum Unternehmen aufgebaut werden darf, wenn sich das Gerät offen im Internet befindet. So kann wirkungsvoll verhindert werden, dass das Gerät durch Malicious Code infiziert und dieser zurück in das Unternehmensnetzwerk geschleppt wird. Der Cisco Security Agent, ein Endpoint-Protection-Produkt, bietet die Möglichkeit, solche Location-based Policies zu definieren. Dabei können für die Ortsbestimmung

Layer-3-Informationen herangezogen werden, wie beispielsweise IP-Adresse, Domain, Group oder DNS-Suffix und diese mit dem Layer-2-Zustand kombiniert werden, der über den CTA abgefragt wird. Im Unternehmen können für normale Arbeitsbereiche moderate Richtlinien, für sensitive Bereiche wie Entwicklungs- oder Vorstandsbereich, sehr stringente Regeln eingerichtet werden, die beispielsweise das Kopieren von elektronischen Dokumenten auf lokale Festplatten oder gar externe USB-Devices völlig unterbinden.

12.564 Zeichen inklusive Leerzeichen

Autor: Klaus Lenssen, Business Development Manager Security und Government Affairs, Cisco Systems GmbH

Für redaktionelle Rückfragen:
Fink & Fuchs Public Relations AG
Mathias Gundlach
Tel.: 0611-74 131 52
mathias.gundlach@ffpr.de