Tanz auf der Rasierklinge

Wie lässt sich die Gerätevielfalt in Unternehmen managen?

Kai-Oliver Detken

IT-Administratoren sehen sich immer mehr einer Gerätevielfalt durch die Anwender ausgesetzt, die mannigfaltige Absicherungen des Unternehmensnetzes nach sich ziehen. Der Trend zum Smartphone verschärft dabei zusätzlich die Situation, da nun auch private Endgeräte in die IT-Umgebung eines Unternehmens gelangen. Um sich dagegen abzusichern und einen geringen Administrationsaufwand zu haben, kann ein IT-Leiter letztendlich nur eine bestimmte Geräteanzahl zulassen und müsste den Rest verbieten. Hier macht ihm allerdings oft die Geschäftsleitung selbst einen Strich durch die Rechnung.
Wie nun kann der Administrator die Endgeräte testen, bevor sie in die Produktivumgebung gelangen? Wie kann er der Gerätevielfalt Herr werden?

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Die Problematik mit der Gerätevielfalt ist nicht neu. Verschiedene Hersteller versuchen sie bereits seit Jahren durch sog. NAC-Lösungen (Network Access Control) zu lösen. Dieser Ansatz sieht die Schaffung einer Quarantänezone für unsichere Endgeräte vor, die nicht den aktuellen Patch-Level besitzen. D.h., durch NAC werden die Endgeräte während der Authentifizierungsphase auf die Konformität der IT-Sicherheitsrichtlinien des Unternehmens überprüft. Werden diese durch ein Endgerät nicht erfüllt, steht unweigerlich der Gang in die Quarantänezone bevor. Hier muss es sich erst einmal um neue Updates von z.B. einer Antivirensoftware oder Betriebssystem-Patches kümmern, bis es für das interne Unternehmensnetz zugelassen wird. Die Kernaufgaben einer NAC-Lösung sind daher:

- Identifizierung und Rollenverteilung von Teilnehmern und Endgeräten;
- Überprüfung der definierten Sicherheitsrichtlinien (Compliance);
- Quarantäne nichtkonformer Endgeräte und ggf. automatische Wiederherstellung;
- Verwaltung zentraler Richtlinien für unterschiedliche Nutzerrollen.

Damit die Endgeräte ihren Status melden können, ist allerdings ein sog. Agent (Posture Collector) auf den Systemen notwendig. Er überprüft die aktuellen Einstellungen und Patch-Level und gibt sie an den Client Broker weiter. Dieser stellt die Informationen dem Network Access Requestor (NAR) zur Verfügung, der neben der Authentifizierung auch den Sicherheitsstatus an die Serverseite weiterleitet und typischerweise einen 802.1x-Supplicant enthält. Der Network Enforcement Point (NEP) hingegen ist in Switchen, Routern, WLAN-APs und VPN-Gateways untergebracht. Bei Einsatz eines Intrusion-Detection/Prevention-Systems ist er zur Durchsetzung bestimmter Regeln durchaus sinnvoll. An zentraler Stelle ist dann noch ein Radius-Server notwendig, der die Entscheidung treffen muss, ob eine Verbindungsanfrage überhaupt berücksichtigt werden darf, und die Profile der mobilen Mitarbeiter enthält. Er steuert das Network Enforcement und den Server Broker. Letzterer liegt als Middleware auf dem Server, da über ihn verschiedene Posture-Validatoren angesprochen werden. *Bild 1* zeigt eine vereinfachte Darstellung der und den Einwahlvorgang eines mobilen Teilnehmers.

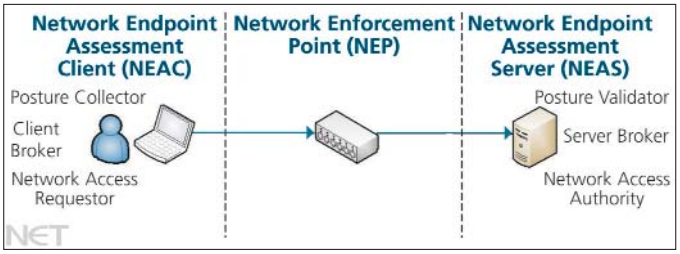

Bild 1: NAC-Bereiche nach IETF

Um eine herstellerübergreifende Lösung herbeizuführen, entwickelte eine Untergruppe der Trusted Computing Group (TCG) die Spezifikation Trusted Network Connect (TNC), mit der sich auch geänderte Komponentenbezeichnungen ergaben. Posture Collector und Validator entsprechen jetzt dem Integrity Measurement Collector (IMC) und dem Integrity Measurement Verifier (IMV), während die Client- und Server-Broker als TNC-Clients/-Server bezeichnet werden. Alle anderen Namen sind identisch.

So schön diese Möglichkeit klingt, so wenig ist sie heute in den Unternehmen umgesetzt. Das liegt zum einen daran, dass der IT-Administrator eine weitere Sicherheitskomponente managen und sich mit Teilnehmern beschäftigen müsste, die gerade aus ir-

gendwelchen Gründen nicht ins Netz kommen können. Zum anderen kann auch ein notwendiges Update in der Quarantänezone Probleme hervorrufen, die den Zugang zum Unternehmen verhindern bzw. erst mit großen Verzögerungen zulassen. Weiterhin ließen sich bisher nicht alle Endgeräte gleichermaßen in eine NAC-Lösung einbinden, wodurch man wieder unterschiedliche Sicherheitsniveaus hätte. Erschwerend kommt hinzu, dass die NAC-Varianten stark vom jeweiligen Hersteller abhängen und sich nicht unbedingt kompatibel zueinander verhalten.

Herstellerlösungen

Kam der NAC-Ansatz ursprünglich aus dem Lager der Netzhersteller und wurde für Router und Switche vorgesehen, sind heute auch immer mehr Softwareanbieter mit eigenen Lösungen am Markt vorhanden. Einer der ersten Netzhersteller, die NAC anboten, war Enterasys Networks. Dabei achtete man von Anfang an auf eine zentrale Managementoberfläche, um die Switche des Netzes einheitlich verwalten zu können. Der Enterasys NAC Manager und Controller kommt als Inband-Lösung zum Einsatz, während das NAC-Gateway für den Out-of-Band-Betrieb zuständig ist. Dabei unterzieht man nicht nur Endgeräte, die sich in das Unternehmensnetz temporär einwählen wollen, einer regelmäßigen Kontrolle, sondern auch Geräte, die permanent mit dem Netz verbunden sind. Man möchte daher Geräte mit gemeinsamen Eigenschaften im Netz identifizieren und diesen eine bestimmte Rolle zuweisen. So lassen sich z.B. identifizierte IP-Telefone an verschiedenen Stellen des Unternehmens automatisch an eine passende Benutzeroberfläche oder Softwareversion zuweisen. Über NAC wird dann das jeweilige Gerät erkannt, lokalisiert und ggf. umkonfiguriert.

Neben Enterasys Networks war auch Cisco Systems ein NAC-Vorreiter. Wie so häufig scherte man aber erst einmal aus gemeinsamen Ansätzen aus, um dann in der Network Endpoint Assessment (NEA) Group der IETF an einem interoperablen Ansatz zu arbeiten. Allerdings arbeitet Cisco Systems nicht in der Trusted Computing Group (TCG) am TNC-Standard mit, was wieder die Frage der Kompatibilität aufwirft. Cisco liefert mit seiner Lösung einen CTA-Client (Cisco Trust Agent) aus, der auf den Endgeräten installiert werden muss. Die Software sammelt alle Daten zum Sicherheitsstatus und sendet diese an die Switche sowie an andere Netzgeräte, die darüber entscheiden, ob das Endgerät zugelassen wird.

Microsoft nannte NAC Network Access Protection (NAP) und versuchte zuerst, die eigene Lösung durchzusetzen, bevor man sich im Nachhinein der TCG mit dem TNC-Standard anschloss. NAP ist mittels Windows 2008 Server heute umsetzbar, NAP-Clients können ab Windows XP mit Service Pack 3 eingesetzt werden. Der NAP-Client unterstützt DHCP, VPN-Funktionalität und 802.1x Enforcement. Der Enforcement Point kann allerdings auch in der Netzinfrastruktur vorhanden sein, wenn die Steuerung über einen Radius-Server erfolgt. Andere Betriebssysteme werden nicht unterstützt, weshalb der NAP-Ansatz auch nur in homogener Microsoft-Umgebung sinnvoll ist.

Aus dem Antivirenlager kann z.B.. McAfee genannt werden, obwohl auch Symantec und F-Secure hier aktiv sind. McAfee hat den NAC-Ansatz in die zentrale Managementkonsole ePolicy Orchectra (e-PO) integriert, was das Durchsetzen von Richtlinien vereinfachen soll. Im ersten Schritt werden die Richtlinien definiert, anschließend die Endgeräte gescannt und erkannt. Dann wird darüber entschieden, ob die Geräte auf die Netzebene weitergereicht werden, und es findet eine automatische Bereinigung statt. Zuletzt kann jedes Endgerät inkl. Netzverkehr überwacht werden. Neben dem Patch-Level-Zustand wird auch überprüft, ob die Endgeräte korrekt konfiguriert wurden. Entsprechende Reports können zur Analyse und Dokumentation generiert werden. Für die Lösung ist neben der ePO-Konsole ein McAfee-Agent notwendig. Es wird aber auch Microsoft NAP unterstützt. Zusätzlich werden auch unbekannte Geräte durch Rogue System Detection im Netz erkannt.

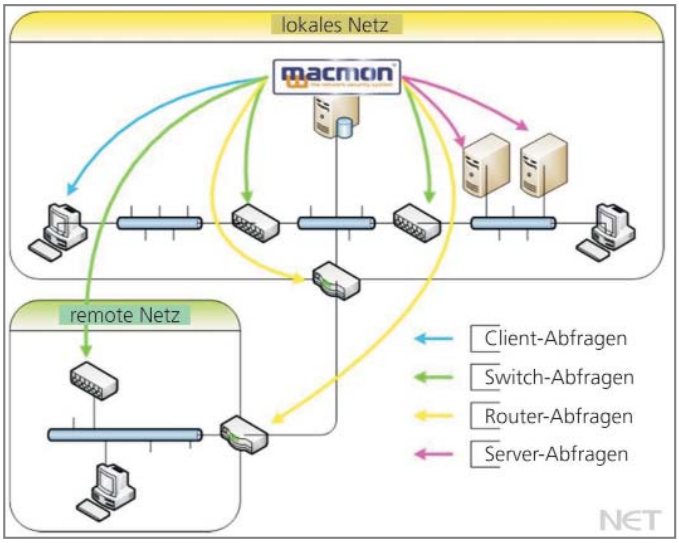

Bild 2: Netz-Monitoring durch Macmon-NAC

Die Mikado Soft Gmbh aus Berlin entwickelte mit Macmon ein System, das die Verwaltung und Überwachung des Netzes und der darin enthaltenen Komponenten und daher auch NAC ermöglicht. Der Macmon-Server wird an zentraler Stelle in das bestehende Netz eingebunden und fragt unterschiedliche Daten von verschiedenen Geräten im Netz ab. Auf deren Grundlage werden die Authentifizierung und Autorisierung von Endgeräten vorgenommen. *Bild 2* zeigt rudimentär die Arbeitsweise von Macmon. Es bietet folgende Kernfunktionen:

- Erkennen und Identifizieren aller aktiven Endgeräte im Netz;
- Authentifizierung der Endgeräte anhand der MAC-Adresse;
- Erfassen weiterer sicherheitsrelevanter Merkmale der Endgeräte;
- manuelle oder regelbasierte Kontrolle des Zugriffs auf das Netz;
- Überwachung des Netzes und der autorisierten Endgeräte zur Laufzeit;
- Erzeugen von Berichten und Statistiken zu Ereignissen im Netz.

Zur Erfassung interner Daten muss auch hier eine Agentensoftware auf

den zu prüfenden Endgeräten im Netz eingesetzt werden. Der Macmon-Agent prüft verschiedene Eigenschaften des Endgerätes und übermittelt die Ergebnisse über eine verschlüsselte Verbindung an den Macmon-Server, der die Daten verarbeitet und für weitere Analysen speichert. Zudem erfasst er die Netzdaten, verarbeitet sie und speichert sie zentral. Die ermittelten Informationen werden auf sicherheitsrelevante Ereignisse im Netz hin analysiert. Die spezifischen Daten eines Ereignisses werden anhand eines Regelwerks überprüft.

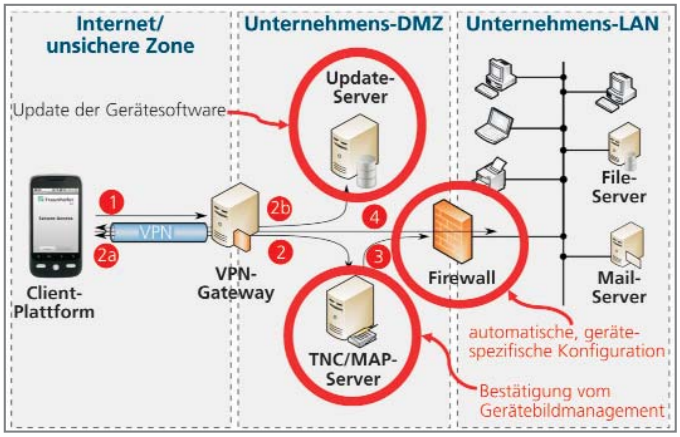

Bild 3: Funktionsweise von BizzTrust (DMZ – demilitarisierte oder Quarantänezone). 1 – Verbindung des Nutzers zum VPN, 2 – Evaluierung der Client-Konfiguration via TNC, 2a – Update-Anfrage und -Bestätigung, 2b – Update der Clientsoftware, 3 – Autorisierung des Nutzers, 4 – Zugang des Nutzers zu den Services

Mikado Soft ist ebenfalls Mitglied der TCG und hat die Erweiterung des TNC-Standards zur Nutzung von Metadaten über die IF-MAP-Schnittstelle in sein Produkt integriert. Diese Erweiterung wird gerade im Forschungsprojekt Esukom (**www.esukom.de**) entwickelt und getestet. Durch bereits vorhandene proprietäre Schnittstellen zu unterschiedlichen Netzkomponenten ist es möglich, Macmon als IF-MAP-Proxy zum Veröffentlichen von Informationen von Netzprotokollen wie DHCP, DNS oder ARP einzusetzen. Zusätzlich können durch die interne Referenzliste von bekannten Geräten und durch die Analyse der erfassten Daten Authentifizierungsinformationen zu Geräten im Netz veröffentlicht werden. Das ermöglicht eine netzweite Reaktion auf sicherheitskritische Geräte im Netz. Man ist daher bestrebt, Interoperabilität mit anderen Lösungen zu erreichen.

Absicherung von Smartphones

Wie man an den bisherigen Lösungen erkennen konnte, ist der NAC-Ansatz zum Verwalten und Managen verschiedener Endgeräte von dem Einsatz eines Agents abhängig, der auf dem Client installiert wird. Das bedeutet, dass mannigfaltige Betriebssysteme unterstützt werden müssten, was besonders im mobilen Umfeld problematisch ist. Durch die Vielfalt der OS-Versionen und die immer schnelleren Entwicklungszyklen ist dies aber nur eines der Probleme. Ein anderes ist, dass Smartphones, die inzwischen die Leistungsfähigkeit von Rechnersystemen haben, oft sowohl privat als auch beruflich genutzt werden. Damit wird ein Sicherheitsloch in Unternehmen aufgemacht, wenn man nicht alle Smartphones verbieten möchte. Das Fraunhofer SIT hat aus diesem Grund die Lösung BizzTrust (**www.bizztrust.de**) entwickelt. Basierend auf der Arbeit verschiedener Forschungsprojekte (z.B. Vogue, s. NET 9/2010, S. 38), ist ein Android-basiertes Smartphone um eine Sicherheitsfunktionalität erweitert worden, die eine Trennung von vertrauenswürdigen und unsicheren Daten ermöglicht, wodurch der Benutzer beliebige private Apps installieren kann, ohne dass diese den geschützten Unternehmensbereich beeinträchtigen. *Bild 3* zeigt den ganzheitlichen Ansatz, der auch die Schaffung einer Quarantänezone vorsieht, sowie die sichere Einwahl des Endgerätes über TNC.

Während der Nutzung wird farblich angezeigt, in welchem Bereich sich der Anwender befindet. So werden Anrufe z.B. grün markiert, wenn es sich um einen geschäftlichen Kontakt handelt. Eine SMS-Benachrichtigung von einem privaten Kontakt wird dagegen rot angezeigt. Die Lösung wurde auf der diesjährigen Cebit erstmals demonstriert. Nachteilig ist, dass eine Umsetzung nur auf speziell vorbereiteten Smartphones möglich ist, was eine Implementierung erschwert. Vorteilhaft ist, dass das Netz in verschiedene Domains aufgeteilt werden kann, die ein Update des Endgerätes ermöglichen.

Fazit

Der NAC-Ansatz oder der TNC-Standard ist in jedem Fall zur Erhöhung der Unternehmenssicherheit zu empfehlen. Sie werden aber teilweise von den Herstellern unterschiedlich interpretiert und umgesetzt. Bei Desktop-Rechnersystemen wird sicherlich nach wie vor Microsoft den Hauptschwerpunkt ausmachen. Durch den NAP-Ansatz, der sich mit dem TNC-Standard inzwischen verträgt, können zudem Windows-Systeme mit verschiedenen Herstellerlösungen umgesetzt werden. Dadurch ist man in diesem Umfeld flexibler, als bei den mobilen Endgeräten. Eine Integration verschiedener Systeme ist auf Serverseite ebenfalls möglich, wenn intelligente Network-Access-Authority-Server erkennen, ob und welche Clients vorhanden sind. Das heißt, man kann im Grunde heute NAC im Unternehmensnetz für stationäre Systeme einführen, sollte aber auf die standardbasierte Umsetzung achten.

Nicht so einfach ist die Integration mobiler Endgeräte, speziell von Smartphones. Hier muss durch die jeweilige NAC-Lösung der Support sämtlicher Betriebssysteme sichergestellt werden können. Dies wird durch die Vielfalt der möglichen Smartphones erschwert. Daher sollte man sich im Vorfeld genau ansehen, ob die favorisierte NAC-Lösung die vorhandenen Betriebssysteme unterstützt, und den Einsatz von Endgerätetypen begrenzen. Da leider die Smartphone-Hersteller den Massenmarkt anvisieren und bisher keine sicheren Unternehmenslösungen anbieten, ist man in jedem Fall auf NAC- bzw. TNC-basierte Lösungen angewiesen. Dabei kommt man für eine höchstmögliche IT-Sicherheit momentan nicht an Betriebssystemanpassungen vorbei. *(bk)*