Einsatz von Network Access Control als wesentlicher Bestandteil eines Konzeptes zur Netzsicherheit

Dave Lenth*, Andreas Hanemann

Fachbereich Elektrotechnik und Informatik
Kompetenzzentrum CoSA
Fachhochschule Lübeck
Mönkhofer Weg 239
23562 Lübeck
dave.lenth@stud.fh-luebeck.de
andreas.hanemann@fh-luebeck.de

Abstract: Im Rahmen einer Modernisierung der Switch-Infrastruktur einer Landesverwaltung wurde ein verbessertes Sicherheits- und Organisationskonzept eingeführt, das in diesem Beitrag vorgestellt wird. Das Konzept sieht dabei neben der Verwendung von VLANs den Einsatz von Network Access Control (NAC) vor. Mit NAC ist gemeint, dass neu an das Netzwerk angeschlossene Geräte zunächst einer Überprüfung unterzogen werden, ehe die vollen Kommunikationsmöglichkeiten zur Verfügung stehen. Damit soll verhindert werden, dass fremde Geräte unerkannt an das Netz angeschlossen werden oder dass von Schadsoftware betroffene Geräte diese innerhalb des Netzes weiter verbreiten. NAC ist ein Konzept, das von Hersteller zu Hersteller unterschiedlich betrachtet wird. Daher wird in diesen Beitrag ein Überblick der Konfigurationsmöglichkeiten gegeben und das vorliegende Konzept in diesen Zusammenhang gestellt. Zum Abschluss wird die Übertragbarkeit des Konzeptes auf Hochschulen diskutiert.

1 Einleitung

Die Netze von öffentlichen Institutionen wie Hochschulen oder Landesbehörden sind einer zunehmenden Anzahl von Angriffen ausgesetzt, so dass die Überprüfung und Verbesserung von Sicherheitsvorkehrungen eine ständige Aufgabe ist. Hierbei stellen mobile Geräte eine besondere Herausforderung dar, da diese im Netz der Organisation, aber auch außerhalb verwendet werden können. Selbst wenn der Schutz des Netzes am Übergang zum Internet sehr gut funktioniert, kann durch den Anschluss dieser Geräte Schadsoftware in das Netz eindringen.

Es ist daher wünschenswert, eine Überprüfung von Geräten durchführen zu können, wenn diese neu an das Netz angeschlossen werden. Hierbei soll sichergestellt werden, dass die

*Dave Lenth ist in der IT-Abteilung der Verwaltung eines Bundeslandes tätig und studiert Medieninformatik an der FH Lübeck. Dieser Beitrag basiert auf seiner Bachelorarbeit.

Geräte vom Softwarestand her aktuell sind und auf Schadsoftware getestet werden, indem ein Abgleich mit dem installierten Virenscanner und der Personal Firewall erfolgt. Diese Methode wird Network Access Control (NAC) genannt. Ihre Umsetzung muss die Datenschutzbedürfnisse des Nutzers beachten und darf nicht zu einer Verhaltensüberwachung werden.

In den folgenden Abschnitten dieses Beitrags wird der Einsatz von NAC diskutiert. Zunächst wird im Abschnitt 2 die Situation einer Landesbehörde in verallgemeinerter Form dargestellt. Danach werden im Abschnitt 3 Konfigurationsmöglichkeiten für NAC und relevante Technologien wie VLANs, IPsec, MACsec, 802.1X und SNMP dargestellt, die für das Verständnis des in diesem Netzwerk eingesetzten Konzepts wichtig sind. Ergänzend zur Konzeptvorstellung in Abschnitt 4 wird ein Einblick in die Umsetzung gegeben (Abschnitt 5), ehe die Übertragbarkeit auf den Hochschulbereich diskutiert wird. Am Ende des Beitrags folgt eine kurze Zusammenfassung der Erfahrungen aus der Praxis der letzten Monate.

2 Bisherige Netzwerkstruktur und Sicherheitskonzept

In diesem Abschnitt werden die Netze der Behörde in verallgemeinerter Form vorgestellt und Einblick in bestehende Schwierigkeiten gegeben, die zur Einführung des verbesserten Sicherheitskonzeptes geführt haben.

2.1 Netzstruktur

In der Abbildung 1 ist ein abstrahierter Netzplan der Behörde dargestellt, in dem die zum Verständnis des Konzepts wichtigen Geräte enthalten sind. Die Netzinfrastruktur besteht aus einer aus Switches aufgebauten Baumstruktur, wobei die Endgeräte der Mitarbeiter sowie Netzwerkdrucker an die untere Ebene angeschlossen sind. Für verschiedene Dienste gibt es im Netz spezialisierte Server wie den DHCP-Server, den Server für Updates des Betriebssystems sowie für Updates der Antivirensoftware. In der Abbildung ist außerdem bereits der NAC-Server verzeichnet. Eine Firewall reguliert die Kommunikation mit der Außenwelt.

Was man in der Abbildung nicht direkt erkennen kann, ist zum einen die Virtualisierung der Server und deren redundante Realisierung. Außerdem wurden im Rahmen der Implementierung des Konzepts inzwischen VLAN-Strukturen (wie bei Endgeräten angedeutet) eingeführt, mit denen die Kommunikation zwischen den VLANs nur eingeschränkt über die Firewall möglich ist. Bei der Kommunikation zwischen einigen Netzbereichen werden zusätzlich Application Level Gateways verwendet.

Beim Netz der Behörde muss man zwischen verschiedenen Nutzergruppen unterscheiden. Einmal gibt es die interne Verwaltung, zu der die IT-Abteilung gehört, und weitere Behördenmitarbeiter, deren IT-Versorgung durch die interne Verwaltung sichergestellt wird. Diese Personengruppen erhalten standardisierte Computermodelle und dürfen auf

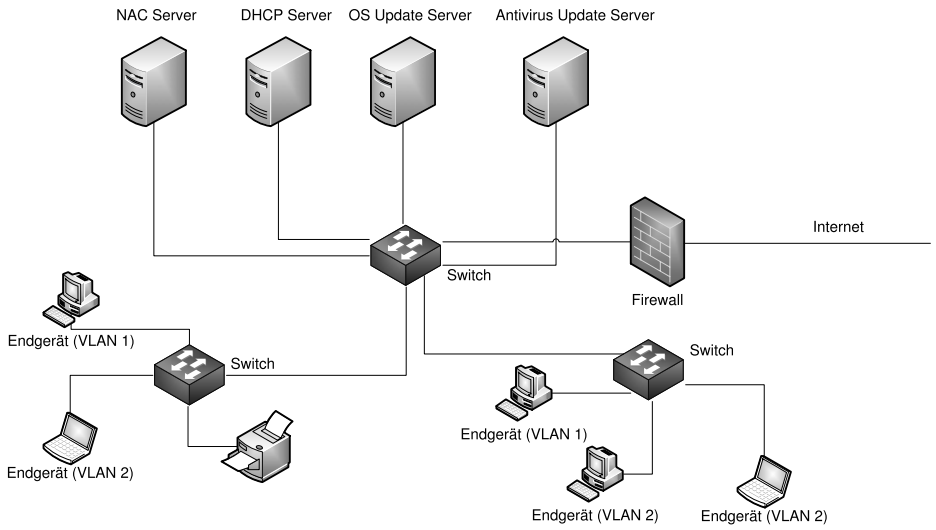

Abbildung 1: Netzstruktur der Behörde

diesen nur Anwendungen nutzen, die explizit erlaubt sind. Daneben soll auch Besuchern ein Internetzugang ermöglicht werden.

2.2 Bisherige Schwierigkeiten und Anforderungen für die Zukunft

Die Netzwerkinfrastruktur der Behörde ist über mehrere Gebäude in einer Stadt verteilt. Zwischen den Gebäuden, die alle in etwa 300 m voneinander entfernt sind, wurden eigenständig Lichtwellenleiter verlegt. Die Abteilungen der Behörde wurden auf physikalischen Wege voneinander abgeschottet und in unterschiedliche Netze aufgeteilt. Dabei erhielten die einzelnen Abteilungen jeweils eigene Switches, was jedoch im Laufe der Zeit zu einer unwirtschaftlichen Situation geführt hat, bei der es viele Switches gab, die oftmals nur wenig ausgelastet waren. Außerdem bestanden in mehreren Räumen Schwierigkeiten mit der Klimatisierung der Switches, wenn die Außentemperaturen hoch waren. Daher sollten bei einer Modernisierung der Infrastruktur wenige neue Switches angeschafft werden, die neben höheren Bitraten bessere Managementfunktionen und viele Anschlussports bieten. Die besseren Managementfunktionen sollten die flexible Konfiguration von VLANs ermöglichen, so dass trotz der Aufgabe einer physikalischen Trennung zwischen Bereichen das Sicherheitsniveau nicht gefährdet wird.

Da die Mitarbeiter der Behörde mittlerweile überwiegend Notebooks verwenden und diese auch bei Auswärtsterminen oder zu Hause nutzen, besteht ein erhöhtes Risiko einer Infektion der Geräte durch Schadsoftware, zumal Schadsoftware immer vielfältiger wird.

Daher könnten infizierte Geräte an das Netzwerk angeschlossen werden und damit das Einfallstor, zumindest zum Netzwerk einer Abteilung, sein.

Durch die einheitliche Hardware- und Softwarekonfiguration wird zwar eine vereinfachte Verwaltung der IT-Landschaft ermöglicht, bei Schadsoftware ist jedoch davon auszugehen, dass vorhandene Schwachstellen gegebenenfalls alle Geräte eines Typs betreffen.

Nachdem es in der Vergangenheit möglich war, fremde Geräte anzuschließen oder Geräte mittels Anschluss an einem anderen Switch Zugang zu einem anderen Netz zu verschaffen, soll dieses in Zukunft ausgeschlossen werden. In diesem Zusammenhang sind die Angriffstechniken *MAC-Spoofing* und *ARP-Spoofing* relevant, wobei beide Methoden verhindert werden sollen. Mit MAC- (Medium Access Control) Spoofing ist gemeint, dass auf einem Endgerät per Software die MAC-Adresse manipuliert und so die Adresse eines zugangsberechtigten Gerätes vorgegeben wird. Damit wird ein solches Endgerät beim Verbinden mit einem Switch zur Kommunikation mit dem Netz zugelassen, falls die Authentifizierung nur über die MAC-Adresse erfolgt. Beim ARP- (Address Resolution Protocol) Spoofing werden falsche ARP-Replies gesendet, die eine Zuordnung von IP-Adressen im Netz zu einer MAC-Adresse des Angreifers enthalten. Auf diese Weise kann ein Angreifer Datenverkehr zu sich umleiten.

3 Relevante Technologien

Für die Verbesserung der Sicherheit auf den Endgeräten und im Netzwerk kann NAC verwendet werden, wobei sich seit der ersten Verwendung des Begriffs und dem Erscheinen der ersten Produkte im Jahr 2005 kein einheitliches Begriffsverständnis etabliert hat. Es gibt stattdessen einige Konfigurationsmöglichkeiten, die jedoch auch herstellerabhängig sind. Wie eine Untersuchung der am Markt angebotenen Lösungen zeigte [Sny10], implementieren die Hersteller NAC entsprechend ihrer eigenen Herkunft als Netzkomponenten- oder Antivirenprogrammanbieter, d.h. mit dem Schwerpunkt auf Authentifizierung, Endgerätesicherheit oder Zugriffskontrolle.

In den IT-Grundschutzkatalogen des BSI [Bun13] wird NAC nicht direkt empfohlen. In der organisatorischen Maßnahme 2.204 (Verhinderung ungesicherter Netzzugänge) wird gefordert, dass es keine unkontrollierten Netzzugänge geben soll. Die Verwendung von 802.1X mit Auswahl einer sicheren EAP-Variante wird in Maßnahme 4.206 (Sicherung von Switch-Ports) empfohlen. Dagegen beschäftigt sich ein Überblickspapier des BSI [Bun11], welches Ende 2011 als Ergänzung zu den IT-Grundschutzkatalogen herausgegeben wurde, mit NAC und unterscheidet verschiedene Arten, wobei diese Klassifikation im Folgenden verwendet wird.

Bei NAC gibt es zunächst den Unterschied zwischen In-Line-NAC und Out-of-Band-NAC. Bei In-Line-NAC wird eine Hardware für NAC so in das Netzwerk eingebunden, dass anschließend der komplette Datenverkehr von angeschlossenen Geräten über diese zusätzliche Hardware geleitet wird, was umfangreiche Kontrollmöglichkeiten erlaubt. Out-of-Band-NAC bezeichnet zwar ebenfalls eine spezielle Hardware (Appliance), aber diese wird nur am Anfang verwendet, wenn ein Gerät neu mit dem Netzwerk verbunden wird.

Durch diese Hardware werden dann Überprüfungen des Endgerätes gesteuert. Nachdem ein Gerät zur Kommunikation mit dem Netz zugelassen wurde, fließt der Datenverkehr des Endgerätes nicht mehr über die NAC-Hardware. Die Kontrollmöglichkeiten sind dadurch eingeschränkt. Auf der anderen Seite ist diese Möglichkeit deutlich preiswerter realisierbar, da nicht der Datenverkehr von (ggf. vielen) Anwendern fortlaufend überprüft wird.

Weiterhin kann man unterscheiden, ob durch die NAC-Lösung ein Agent auf dem Endgerät des Nutzers platziert wird oder nicht. Mit dem Begriff *Agent* ist eine Softwarekomponente gemeint, die Informationen über die Konfiguration des Endgerätes aus diesem ausliest und an die NAC-Hardware im Netz schickt. Bei den Agenten kann man unterscheiden, ob diese nur temporär (das kann technisch eine Ausführung von JavaScript-Code in einer Webseite sein, die standardmäßig ausgeliefert wird) oder permanent installiert werden. Bei einer permanenten Installation ist eine tiefere Einbettung in das System möglich, insbesondere mit Zugriff auf Personal-Firewall-Einstellungen und die Konfiguration des Antivirenprogramms. Wenn kein Agent installiert wird, kann man das System nur von außen untersuchen. Hierbei bieten Tools wie nmap [Lyo09] die Möglichkeit, das Betriebssystem, dessen Version sowie die Art des Endgerätes zu erkennen. Diese Erkennung stützt sich auf die Reaktion des Betriebssystems auf falsche Pakete (z.B. mit nicht gültigen Kombinationen von TCP Flags), bei denen die Antworten nicht in RFCs festgelegt sind und somit unterschiedlich implementiert werden. nmap gleicht die Reaktionen mit einer Datenbank ab und gibt für die angenommene Betriebssystemversion einen Grad der Übereinstimmung an.

NAC wird oftmals im Zusammenhang mit BYOD (Bring Your Own Device) gesehen, d.h., wie man trotz der Erlaubnis an die Mitarbeiter, auch ihre privaten Geräte für den Dienstgebrauch zu nutzen, die Sicherheit des Netzes der Organisation gewährleisten kann [SAN14].

Neben NAC ist zum Verständnis des Konzeptes in der Behörde die Kenntnis über weitere Technologien notwendig. Diese sollen an dieser Stelle nur kurz, bezogen auf die relevanten Aspekte, dargestellt werden.

Mit VLANs ist eine Unterscheidung zwischen der physikalischen und der logischen Netzinfrastruktur möglich, d.h., die Zugehörigkeit zu einem Schicht-2-Netz hängt nicht mehr ausschließlich davon ab, mit welchem Switch das Endgerät verbunden ist. Man unterscheidet zwischen den Varianten Port-based, MAC-based und IP-based, um bei einem Endgerät über die Zugehörigkeit zum VLAN zu entscheiden. Port-based bedeutet, dass statisch festgelegt wird, zu welchem VLAN ein bestimmter Switchport gehört. Beim MAC-based- bzw. IP-based-VLAN hängt die Zugehörigkeit von der MAC- bzw. IP-Adresse des Endgerätes ab. Vom Netz wird diese Adresse zunächst abgefragt und der Switchport dann dynamisch dem jeweiligen VLAN zugeordnet. Vom Prinzip her sind jedoch sowohl MAC- als auch IP-Adressen nicht fälschungssicher und können leicht anders im Endgerät eingetragen werden. Gegen die Manipulation von IP-Adressen sowie zum Schutz der Vertraulichkeit und Integrität kann die für Bereiche mit hohen Sicherheitsanforderungen etablierte (aber nicht einfach zu konfigurierende) IP-Erweiterung IPsec genutzt werden. Auch bei den MAC-Adressen besteht eine Schutzmöglichkeit mit ähnlichen Eigenschaften namens MACsec (IEEE 802.1AE). Im Gegensatz zur bekannten Netzwerkauthentifizierung mittels 802.1X wird MACsec jedoch selten eingesetzt.

Der Einsatz von NAC muss auch auf das Netzwerkmanagement, d.h. auf die SNMP-Konfiguration, abgestimmt werden. Hierbei ist eine klare Unterscheidung zwischen den ersten beiden SNMP-Versionen mit dem unzureichenden Sicherheitskonzept des „Community Strings“ und SNMPv3, welches ein geeignetes Sicherheitskonzept zur Sicherstellung von Vertraulichkeit, Integrität und Authentizität vorsieht, notwendig. Die Netzwerkinfrastruktur sollte auf Basis von SNMPv3 verwaltet werden, auch wenn der Aufwand hierfür größer ist.

4 Konzeption des Einsatzes von Network Access Control

Bei der Auswahl der NAC-Lösung für die Behörde sollte eine kommerzielle Lösung mit zuverlässigem Support ausgewählt werden. Ein weiteres Kriterium war, weitgehende Herstellerabhängigkeiten zu vermeiden. Daher sollte die Kommunikation mit Switches, DHCP-Server und Antivirenprogramm gemäß offenen Protokollen erfolgen. Zusätzlich wurde es positiv gewertet, dass die schließlich gewählte Lösung ein Zertifizierungsverfahren des BSI durchläuft. Aufgrund der eingeschränkten Möglichkeiten in der Behörde zur Anpassung von Software wurde keine freie Software in Betracht gezogen.

Die NAC-Lösung realisiert die Out-of-Band-Variante, d.h., es gibt einen NAC-Server, der beim Anschluss eines Gerätes ans Netz die Kontrolle des Zugangs realisiert (siehe Details im Abschnitt 4.1). Die Zugangskontrolle muss nach jeweils 60 Minuten erneut durchlaufen werden. Erst nach bestandener Kontrolle wird das Endgerät für die Verwendung des VLANs zugelassen. Wird die Kontrolle nicht bestanden, werden die Kommunikationsmöglichkeiten des Endgerätes beschränkt, indem es einem Quarantäne-VLAN zugeordnet wird. Im Quarantäne-VLAN hat das Endgerät lediglich die Möglichkeit, den Software-Update-Server sowie Server für das Antivirenprogramm zu erreichen. Der Fall mit dem Quarantäne-VLAN wird verwendet, wenn das Endgerät grundsätzlich erkannt werden kann, d.h., dass es eines der Geräte der Organisation ist. Ist dieses auch nicht der Fall, dann wird angenommen, dass ein Gast sein Endgerät eingesteckt hat. Dieses erhält dann lediglich Zugriff auf das Internet mittels eines Gäste-VLANs. Die Auswahl der Out-of-Band-Variante erfolgte im Hinblick auf eine Kosten/Nutzen-Abwägung. Die Verwendung von In-Line-NAC hätte zu deutlich höheren Kosten geführt, wenn sämtlicher Datenverkehr durch den NAC-Server (oder dann ein Cluster von NAC-Servern) geleitet würde. Der Sicherheitsgewinn, der in einer Identifikation von Geräten, die während ihrer Verwendung Auffälligkeiten zeigen, besteht, wird dagegen als nicht bedeutend genug angesehen.

Mit der Beschaffung von neuen Switches wurde in der Behörde parallel eine VLAN-Struktur realisiert, durch die die einzelnen Bereiche logisch voneinander getrennt sind. Eine Kommunikation zwischen den Bereichen ist prinzipiell über die Schicht 3 möglich, wobei an dieser Stelle die Kommunikationsmöglichkeiten über eine Firewall eingeschränkt werden. Von den drei Möglichkeiten zur VLAN-Konfiguration entspricht die gewählte Realisierung sowohl der MAC- als auch der IP-based Variante. Dabei erfolgt der Zugang zunächst anhand der MAC-Adresse. Da der NAC-Server jedoch auch Zugriff auf den DHCP-Server und die dort hinterlegten Zuordnungen von MAC- zu IP-Adressen hat, wird

zudem die Richtigkeit der (fest vergebenen) IP-Adresse überprüft. Diese Überprüfung der Kombination in Zusammenhang mit einem permanenten NAC-Agenten wird verwendet, um das für sich betrachtet relativ einfache Fälschen von MAC- und IP-Adressen zu verhindern. Die ARP-Tabellen auf den Endgeräten werden dabei nicht geprüft. Stattdessen wird jede IP-Adresse im Netzbereich alle 15 Minuten mit einem ping angesprochen, was zu ARP-Requests und entsprechenden Replies führt, deren Adresszuordnungen überprüft werden.

Die Verwendung des NAC-Servers führt auch zu einer Änderung des Managements der Switches. Diese werden nun vom NAC-Server konfiguriert, wobei SNMPv3 zum Einsatz kommt. Hierbei erfolgt die Absicherung der Kommunikation zertifikatsbasiert, d.h., alle Switches erhalten Zertifikate. An dieser Stelle kommt ein selbstgeschriebenes Skript für die Verteilung zum Einsatz. Mit dem Zugriff auf die Switches wird ein Port dynamisch einem entsprechenden VLAN zugewiesen, wenn die Authentifizierung erfolgreich war. Die Netzwerktopologie wird automatisch verwaltet, wobei CDP (Cisco Discovery Protocol) bzw. LLDP (Link Layer Discovery Protocol) zur Topologieerkennung zur Verfügung stehen.

Die NAC-Lösung wurde nicht als Appliance eingekauft, sondern wird als virtuelle Appliance betrieben. Sie kann damit in eine existierende Backup-Strategie für virtuelle Server einbezogen werden, bei der insbesondere Snapshots des kompletten Systems erstellt werden. Sollte der virtuelle NAC-Server dennoch ausfallen, würde das bedeuten, dass alle angeschlossenen Geräte in den aktuell verwendeten VLANs bleiben. Es ist also kein Wechsel, z.B. vom Quarantäne-VLAN in ein reguläres VLAN durchführbar. Während die schon angemeldeten Geräte weiter kommunizieren können, wäre beim Ausfall des NAC-Servers keine Neuanmeldung mehr möglich.

Das Konzept wird zunächst nur für Windows-PCs und Windows-Notebooks angewendet, die von der Behörde vorkonfiguriert werden und damit permanente NAC-Agenten installiert bekommen, für die zentral SSL-Zertifikate ausgestellt werden. Die Nutzer haben auf diesen Geräten keine Administratorrechte. Es wird zentral verwaltet, welcher Mitarbeiter welche Applikationen nutzen darf, so dass eine zentralisierte Verteilung der Software und deren Aktualisierung möglich ist. Die Applikationen sind soweit möglich so konfiguriert, dass die zu verarbeitenden Daten primär nicht auf den Endgeräten, sondern auf Servern im Netzwerk gespeichert werden. Dennoch ist es wichtig, die Endgeräte vor Datendiebstahl zu sichern. Daher wird für jedes Gerät eine Festplattenverschlüsselung durchgeführt, deren Verwaltung ebenfalls zentralisiert gesteuert wird.

Da die Informationen, die die NAC-Lösung verarbeitet, gerätebezogen und nicht direkt personenbezogen sind, wurde die Situation hinsichtlich des Datenschutzes nicht anders bewertet als vor der NAC-Einführung.

4.1 Authentifizierung

Wenn Geräte in der Behörde neu beschafft werden, werden bei der Inventarisierung umfangreiche Details in einer Datenbank erfasst, von denen hier insbesondere die MAC-

Adressen interessant sind. Daneben gibt es, wie oben schon dargestellt, agentenloses und auf Agenten basierendes NAC. Zur Identifikation von Geräten ohne Agent kann man ein sog. Protokollprofil erstellen, d.h., wie das Endgerät auf Dateneinheiten von verschiedenen Protokollen reagiert. Es zeigt an, welche Dienste gerade aktiv sind. Mit einem Agenten kann zusätzlich ein sog. Geräteprofil mit weiteren Informationen erstellt werden. Dieses ist aber recht allgemein und zeigt einen ID-Hash und die Betriebssystemversion (z.B. Windows 7, 64 Bit). Wie die Tabelle 1 zeigt, funktioniert diese Methode nicht bei den Netzwerkdruckern und sonstigen einfachen netzwerkfähigen Geräten wie beispielsweise Temperaturfühlern.

Gerätetyp	MAC- u. IP-Adresse	Protokollprofil	Geräteprofil	802.1X
PC, Notebook, Server	ja	ja	ja	ja
Drucker, sonstige Netzgeräte (z.B. USV, Webcam)	ja	ja	nein	nein

Tabelle 1: Authentifizierung von Geräten über verschiedene Merkmale

Die unvollständige Unterstützung durch die Geräte ist auch der Grund, warum 802.1X derzeit nicht genutzt wird. Dessen Einsatz setzt voraus, dass alle Geräte an einem Switch das Protokoll verwenden, was aber oftmals nicht möglich ist. Auch eine Ausweichlösung, bei der bestimmte Geräte gesondert authentifiziert werden (*MAC Authentication Bypass*), wird von den Switches nicht unterstützt.

4.2 Sicherheitswarnungen

Der NAC-Server gibt Warnungen aus, wenn bestimmte Situationen auftreten, in denen eine Manipulation sehr wahrscheinlich vorliegt. Außerdem wird das betroffene Gerät dann einem weiteren speziellen VLAN zugeordnet, das Konflikt-VLAN heißt. Folgende Situationen werden unterschieden.

MAC-Flooding: An einem einzigen Switchport werden Rahmen mit unterschiedlichen Quell-MAC-Adressen empfangen. Es wird vermutet, dass jemand MAC-Adressen ausprobiert, ob eine von diesen den Zugang zum Netz erlaubt.

ARP-Spoofing: Eine MAC-Adresse wird in ARP-Dateneinheiten einer anderen IP-Adresse zugeordnet als das vorher der Fall war. Es wird angenommen, dass jemand dabei eine falsche IP-Adresse, d.h., die ihm nicht zugeordnet ist, angibt, um den Datenverkehr zu sich umzuleiten. Um dieses zu erkennen, werden die ARP-Caches im Netz fortlaufend beobachtet.

MAC-IP-Mismatch: Bei bestimmten MAC-Adressen möchte man nicht, dass diese per DHCP immer eine andere IP-Adresse erhalten, sondern man nimmt eine statische Zuordnung vor. Diese wird aber auch über den DHCP-Server verwaltet. Da der NAC-Server Zugriff auf den DHCP-Server hat, sind ihm diese Zuordnungen bekannt, so dass er Abweichungen feststellen kann.

MAC-Spoofing: Wenn bei einem Gerät die MAC-Adresse gefälscht wird, dann stimmt das Geräteprofil, wie es vom NAC-Agenten übermittelt wird, nicht mit dem gespeicherten Profil überein. Dadurch kann diese Manipulation erkannt werden.

5 Implementierung

In den letzten Monaten wurde das Konzept in der Behörde implementiert. Bei den neuen Switches wurden die VLANs konfiguriert und deren Administration über den NAC-Server eingerichtet.

Bei der Einführung des Quarantäne-VLANs wurde zunächst ein Ansatz gewählt, bei dem die Mitarbeiter nicht unnötigerweise vom Netz ausgeschlossen werden sollten. Die Quarantänefunktion wurde im ersten Schritt nur dann aktiv, wenn ein Gerät über die letzten 90 Tage überhaupt keine Updates erhalten hatte. Nachdem diese Funktion stabil funktionierte, wurde die Toleranzzeit auf 5 Tage verkürzt. An dieser Stelle bleiben jedoch Abwägungen zu treffen, wie restriktiv diese Überprüfung durchgeführt werden soll. Wenn beispielsweise ein Mitarbeiter am gestrigen Tag seinen Computer nicht verwendet hat und gestern neue Virensignaturen verteilt wurden, dann befindet sich der Computer nicht auf dem neuesten Stand. Wenn der Computer heute eingeschaltet wird und sich mit dem Netz verbinden möchte, dann werden zuerst die Überprüfungen durchgeführt, die der Rechner nicht erfüllen würde. Der Rechner würde dann dem Quarantäne-VLAN zugeordnet und erhält die neuen Signaturen. Der Mitarbeiter kann solange nicht das Netz verwenden. Dieses kann in vielen Fällen ungünstig sein, z.B. wenn gerade eine wichtige E-Mail versendet werden soll. An dieser Stelle müssen noch Erfahrungen gesammelt werden, wie viele Tage Toleranz erlaubt sein können und ob man dies von der Schwere der Sicherheitswarnungen bzgl. Schadsoftware (vom BSI, DFN-CERT und anderen) abhängig machen könnte.

6 Übertragbarkeit auf Hochschulen

Die dargestellte Sicherheitspolicy der Behörde ist sicherlich als restriktiv zu bezeichnen und zielt auf ein hohes Sicherheitsniveau ab. Sie kann daher nur teilweise direkt auf den Hochschulbereich übertragen werden, wo insbesondere in der Forschung eine viel größere Heterogenität bei Endgeräten und Applikationen vorliegt. Eine vergleichbare Konfiguration kommt jedoch für die Rechner in der Hochschulverwaltung in Frage, insbesondere wenn es um sensible personenbezogene Daten oder um Daten zur Finanzverwaltung geht.

Die gewählte NAC-Software wäre jedoch auch für BYOD-Szenarien verwendbar. Hier könnten die Hochschulmitarbeiter ihre eigenen Geräte über ein Portal verwalten, so dass deren Gerätedaten vor der Verwendung in der Hochschule bekanntgegeben werden. Im Hochschulbereich sollte man auch die Verwendung von Open Source Software wie Packet Fence [Inv15] in Betracht ziehen, da diese keine Lizenzkosten verursacht, an die eigenen Anforderungen angepasst und deren Einsatz nach und nach erweitert werden kann.

7 Fazit und Ausblick

In den letzten Monaten wurde das NAC-Konzept in der Behörde implementiert und wird nun dauerhaft verwendet. Der NAC-Server selbst konnte relativ einfach konfiguriert und in die Virtualisierungsumgebung integriert werden, während ein größerer Aufwand für die passende Konfiguration der Switches notwendig war. Die Verwaltung der Endgeräte konnte auf Basis der bereits existierenden Endgerätedatenbank und den schon vorhandenen Adresszuordnungen im DHCP-Server mit geringem Aufwand erfolgen. Auch wenn bei NAC-Konzepten der Eindruck besteht, dass diese nur für größere Organisationen geeignet sind, hat sich in diesem Projekt gezeigt, dass bei vorausschauender Planung eine schrittweise Einführung auch in mittelgroßen Organisationen möglich ist. Die gewählte Software erwies sich in den letzten Monaten als wartungsarm. Insbesondere konnte eine gute Balance bezüglich der Anzahl der Meldungen gefunden werden, was bei vielen Netzwerkzeugen mit Alarmierungsfunktion oftmals nicht so einfach ist. In der Zukunft soll eine Übertragbarkeit des Konzepts auf WLAN untersucht werden, wobei an dieser Stelle eine Kombination mit 802.1X möglich erscheint.

Literaturverzeichnis

[Bun11] Bundesamt für Sicherheit in der Informationstechnik (BSI). Überblickspapier Netzzugangskontrolle. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html (letzter Zugriff: 21.04.2015), November 2011.

[Bun13] Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutzkataloge, 13. Ergänzungslieferung. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html (letzter Zugriff: 21.04.2015), Juni 2013.

[Inv15] Inverse Inc. Packet Fence. http://www.packetfence.org/ (letzter Zugriff: 21.04.2015), 2015.

[Lyo09] Gordon Fyodor Lyon. NMAP Reference Guide, OS Detection. http://nmap.org/book/osdetect.html (letzter Zugriff: 21.04.2015), Januar 2009.

[SAN14] SANS Institute/ForeScout Technologies. Securing Personal and Mobile Device Use with Next-Gen Network Access Controls. http://www.sans.org/reading-room/whitepapers/analyst/securing-personal-mobile-device-next-gen-network-access-controls-35627 (letzter Zugriff: 21.04.2015), November 2014.

[Sny10] J. Snyder. NAC: What went wrong? http://www.networkworld.com/article/2209345/-security/nac–what-went-wrong-.html (letzter Zugriff: 21.04.2015), Mai 2010.