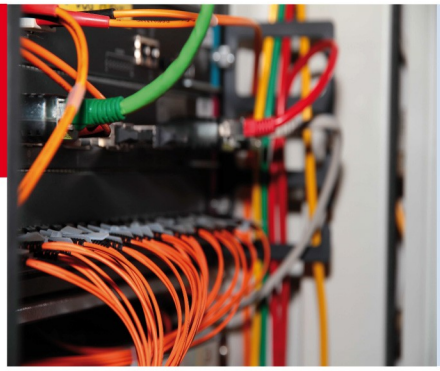
Bundesamt
für Sicherheit in der
Informationstechnik

# Überblickspapier

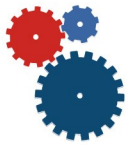
## Netzzugangskontrolle



IT-Grundschutz aktuell

## Was ist Netzzugangskontrolle?

Netzzugangskontrolle ist ein Sammelbegriff für diverse Techniken und Strategien, um den berechtigten Zugriff zu lokalen Netzen zu steuern. Daneben gibt es weitere Begriffe, die für Konzepte und Techniken von Produktherstellern oder Gremien rund um die Netzzugangskontrolle benutzt werden, wie beispielsweise: „Network Admission Control“ (Cisco), „Trusted Network Connect“ (Trusted Computing Group) und dem seit 2008 von Microsoft herausgebrachten „Network Access Protection“. Als plattformunabhängiger Begriff scheint sich „Network Access Control“ (NAC) durchzusetzen. Eine einfache Form der Netzzugangskontrolle sind White-List-Prüfungen, die an Netzübergängen durchgeführt werden, bei denen lediglich abgefragt wird, ob Geräte, die Zugriff auf das Netz nehmen wollen, eine in der White-List enthaltene MAC- bzw. IP-Adresse haben. Abgesehen davon, dass ohne zertifikatsgestützte Authentisierung wie MACSec oder IPSec MAC- und IP-Adressen leicht gefälscht werden können, kann durch diese Form der Überprüfung nicht festgestellt werden, welches Betriebssystem diese Geräte verwenden, welche Anwendungen darauf installiert sind, welche Verbindungsarten (z. B. IP oder IPSec) verwendet werden, ob deren Antivirenprogramme aktuell sind, ob alle Patches eingespielt sind und dergleichen Dinge mehr. Das Ziel von Netzzugangskontrolle ist es, auch diese Sicherheitsrisiken zu minimieren.

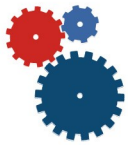


## Vorstufe zu NAC: IEEE 802.1X

Das „Institute of Electrical and Electronics Engineers“ (IEEE) hat 2004 den Standard IEEE 802.1X „Port Based Network Access Control“ verabschiedet, der die Authentisierung in Rechnernetzen standardisiert. Inzwischen unterstützen nahezu alle Netzkomponenten (Switches, Netzwerkkarten, Netzdrucker, etc.) und Betriebssysteme auf dem Markt diesen Standard. Der Standard ist für physische LANs, virtuelle LANs und WLANs anwendbar.

Bevor einem IT-System Zugang zu einem nach dem IEEE-Standard 802.1X-konfiguriertem Netz gewährt wird, muss sich das neue Gerät (im Standard „Supplicant“ genannt) an einem Authentikator anmelden. Dieser Authentikator ist für gewöhnlich ein Netzkoppelelement, also z. B. ein Switch, Router oder WLAN Access Point. Der Authentikator überprüft die übermittelten Authentisierungsdaten mit Hilfe eines Authentisierungsservers und gibt je nach Ausgang dieser Überprüfung den Zugriff auf das Netz frei oder verwehrt ihn. Für die Anmeldungsprozedur empfiehlt der Standard das „Extensible Authentication Protocol“ (EAP). Dieses Protokoll wurde von der „Internet Engineering Task Force“ im „Request for Comments“ (RFC) 3748 beschrieben. Es wird empfohlen, die Kommunikation zwischen Authentikator und Authentisierungsserver mittels kryptographischer Verfahren (z. B. SSL/TLS) abzusichern. In den allermeisten Fällen wird als Authentisierungsserver ein „Remote Authentication Dial-In User Service“-Server (RADIUS-Server) im Netz eingesetzt.

Mit der Überarbeitung des IEEE 802.1X-Standards zum Standard 802.1X-2010 im Jahre 2010 wurden einige Schwachstellen des Verfahrens nach dem bisherigen Standard behoben. Nach dem 802.1X-Standard war es beispielsweise möglich, dass ein berechtigtes Gerät über einen Hub, der noch offene Netzsteckplätze besitzt, mit dem lokalen Netz verbunden wurde und dass nach der Authentisierung beliebige weitere Geräte die noch offenen Ports zum unberechtigten Zugang zum lokalen Netz nutzen konnten. Der überarbeitete IEEE-Standard 802.1X-2010 begegnet dieser Schwachstelle durch ein kryptographisches Authentisierungsverfahren der MAC-Adressen aller mit dem lokalen Netz verbundenen Geräte. Dieses Verfahren heißt „MACSec“ und ist im IEEE-Standard 802.1AE beschrieben. Ferner beschreibt der überarbeitete IEEE 802.1X-2010-Standard mit dem MACSec Key Agreement (MKA) Protokoll ein Verfahren zur sicheren MACSec-Schlüsselverteilung. Neben der kryptographischen Authentisierung aller Netzteilnehmer zu Beginn der Netzverbindung wird mit dem MACSec-Verfahren alle Kommunikation im Netz auf OSI-Ebene 2 verschlüsselt. Während die meisten Router und Switches den IEEE 802.1X-Standard unterstützen, werden die Erweiterungen MACSec und MKA nur von Switches und Routern unterstützt, die bei hohem bis sehr hohem Schutzbedarf eingesetzt werden und entsprechend teurer in der Anschaffung sind.

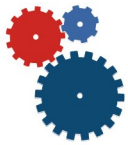


# Überblick über Funktionen und Arten von Netzzugangskontrollsystemen

Systeme für die Netzzugangskontrolle (Network Access Control, NAC) bauen entweder auf dem IEEE 802.1X-Standard von 2004 auf oder bedienen sich seines Konzepts. In einem 802.1X-Netz ist zwar der Zugang zum lokalen Netz auf zugelassene Benutzer beschränkt, aber ob von diesen legitimen Benutzern eine Gefahr für andere Netzteilnehmer oder der Informationssicherheit der Institution insgesamt ausgeht, beispielsweise durch Schadsoftware oder unverschlüsselte Kommunikation, wird nicht überprüft. Wird der 802.1X-Standard zur Absicherung von Rechnernetzen auf die Zugangssicherung eines Gebäudes übertragen, so ist der 802.1X-Standard mit einer Ausweiskontrolle am Eingang vergleichbar, die dafür sorgt, dass nur noch Personen mit einem gültigen Ausweis Zugang erhalten. Ob diese Personen Waffen, Kameras oder Mikrofone dabei haben oder mit einem Grippevirus infiziert sind und damit eine Gefährdung für andere Personen im Gebäude darstellen, wird durch diese Zugangskontrolle nicht überprüft. Solche erweiterten Überprüfungen werden in Teilaspekten beispielsweise vor dem Betreten von Krankenhaus-Intensivstationen, Flugzeugen oder Sicherheitsbehörden durchgeführt. Vergleichbare Funktionalitäten können für das lokale Rechnernetz von einem NAC übernommen werden. Ein NAC überprüft bei jedem neuen Netzteilnehmer, ob gewisse Sicherheitssoftware vorhanden ist, die aktuellen Betriebssystempatches eingespielt sind und vordefinierte Sicherheitsleitlinien eingehalten werden. Die jeweilige Ausprägung und Detailtiefe dieser Überprüfung hängt vom jeweiligen NAC-Anbieter ab.

Typischerweise überprüfen NACs, ob die Virensignaturdatenbank aktuell ist, ob eine Personal-Firewall eingeschaltet ist und ob vorhandene Betriebssystemaktualisierungen installiert sind. Die Sicherheitsleitlinie der Institution kann vorschreiben, dass die gesamte Kommunikation im LAN kryptographisch – z. B. mit MACSec oder IPSec – abgesichert sein soll. Ein NAC kann überprüfen, ob das entsprechende kryptographische Verfahren vom neuen Client unterstützt wird und alle nötigen Initiierungsmaßnahmen veranlassen, wie beispielsweise die Einigung auf Verfahren, der Schlüsselaustausch und so weiter.

NACs spalten das LAN in verschiedene virtuelle LANs (VLANs) auf und gewähren je nach Ergebnis der Überprüfung zu Beginn Zugang zum jeweiligen VLAN. Sollte beispielsweise eine Überprüfung ergeben, dass noch nicht die neuesten Virendefinitionen installiert sind, so kann das NAC zuerst den Zugang zu einem Quarantäne-Netz gewähren, wo die entsprechenden Aktualisierungen aus dem Internet oder lokalen Quellen installiert werden.



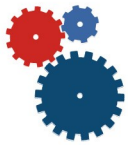
Sind diese Aktualisierungen installiert, so wird der Zugang zum gewünschten Netz gewährt. Dabei ist zu bedenken, dass das NAC die Einteilung in die verschiedenen VLANs nur konfiguriert, die VLANs aber auf den jeweiligen Switches und Routern umgesetzt sind. Die Stärke der Abschottung zwischen den einzelnen VLANs hängt daher sowohl von der einwandfreien Konfiguration des NACs als auch von der einwandfreien Konfiguration der VLANs auf Switches und Routern ab. Zudem muss sichergestellt sein, dass das NAC mit den vorhandenen Switches und Routern funktioniert und alle deren Funktionalitäten unterstützt.

NACs werden danach klassifiziert, ob sie sogenannte „In-Line NACs“ oder „Out-of-Band NACs“ sind und ob sie agentenbasiert oder agentenlos sind. Bei den agentenbasierten NACs kann zusätzlich noch zwischen Varianten mit permanenten und temporären Agenten unterschieden werden. Letztere Variante wird häufig auch „auflösender Agent“ (dissolvable Agent) genannt, da sich ein „auflösender Agent“ nur für die Dauer der Netzteilnahme auf dem Endgerät befindet und sich danach komplett deinstalliert. Es gibt außerdem Kombinationen von agentenbasierten und agentenlosen NACs.

Je nach Art des NACs (und in Abhängigkeit vom NAC-Anbieter) unterscheiden sich die umsetzbaren Sicherungsfunktionalitäten, Einsatzmöglichkeiten und der Installationsaufwand. Diese Unterschiede bieten diverse damit verbundene Vor- und Nachteile. Jede Institution sollte daher vorab überlegen, welche Systeme von welchen Anbietern eingesetzt werden sollen.

## In-Line NACs

In-Line NACs werden an den Rändern eines Netzes installiert, z. B. in Form eines Switches oder einer Appliance. Dies bedeutet, dass der vollständige Netzverkehr durch diese NAC-Appliances fließt, was gewisse Einschränkungen bezüglich der Netzgröße mit sich bringt, da durch eine NAC-Appliance kein beliebig großer Datenstrom fließen kann. Ferner verändert sich bei der Einführung eines In-Line NAC die komplette Netzstruktur. Daher muss für die Installation des NACs das gesamte Netz abgeschaltet werden. Aus diesem Grund werden In-Line NACs eher für kleinere Netze eingesetzt, die gerade erst geplant werden und noch nicht im produktiven Betrieb sind. Der Vorteil von In-Line NACs liegt in der umfassenden Überwachungsmöglichkeit des Netzverkehrs, da alle Kommunikation über die NAC-Appliances erfolgt.



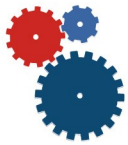
## Out-of-Band NACs

Im Gegensatz zu In-Line NACs werden Out-of-Band NACs wie jede beliebige andere Netzkomponente in ein Rechnernetz eingebaut. Sie übernehmen die Rolle des Authentisierungsservers eines 802.1X-kompatiblen Netzes und konfigurieren zentral die VLANs des Netzes. Auf der einen Seite können Out-of-Band NACs den Netzverkehr prinzipiell nicht so gut überwachen wie In-Line NACs, da der Netzverkehr nicht durch sie durchfließt. Dadurch gibt es aber bei Out-of-Band NACs keine Bandbreitenbeschränkung, so dass sie auch in größeren Netzen eingesetzt werden können. Durch die Installation eines Out-of-Band NACs ändert sich außerdem lediglich die logische Netzstruktur, nicht aber die physische Netzstruktur, was mit einer geringeren Ausfallzeit zur Installation des NACs einhergeht.

## Agentenbasierte und agentenlose NACs

Bei den agentenbasierten NACs muss auf jedem Netzteilnehmer ein Programm (der Agent) installiert sein, der mit dem NAC-Validator (vergleichbar mit dem RADIUS-Server in reinen 802.1X-Netzen) Informationen über den jeweiligen Teilnehmer austauscht. In der Variante mit auflösendem Agenten wird dieses Programm zu Beginn der Netzteilnahme auf das Gerät des neuen Teilnehmers installiert und nach Verlassen des Netzes wieder gelöscht. Die auflösenden Agenten sind dabei meistens als Java- oder ActiveX-Programm umgesetzt und somit nicht so tief im System verankert wie bei der Variante mit permanentem Agenten. Daher ist der Funktionsumfang der auflösenden Agenten im Vergleich zu den permanenten Agenten geringer – so können die auflösenden Agenten nicht ohne Zutun des Benutzers Firewalls einschalten oder Virensignaturen aktualisieren. Andererseits sind auflösende Agenten vom Betriebssystem unabhängig und damit flexibler einsetzbar. Einige solcher NAC-Agenten gibt es beispielsweise schon für iOS und Android.

Bei agentenbasierten NACs gibt es sowohl Varianten, die diese Überprüfung nur zu Beginn ausführen als auch Varianten, die fortlaufend den Zustand überwachen. Bei agentenlosen NACs scannt der NAC-Validator aktiv das neue Gerät nach offenen Ports, Betriebssystemversion und/oder nach Schwachstellen, wertet die Ergebnisse aus und gewährt bzw. verwehrt daraufhin den Zugang zum Netz. Umfang, Tiefe und damit auch Dauer sowie Aussagekraft dieser Scans hängt vom eingesetzten Scanner des jeweiligen NAC-Anbieters ab. Als Scanner können beispielsweise Nessus- beziehungsweise OpenVAS-Scanner eingesetzt werden. Je nach Art des Port- beziehungsweise Schwachstellenscans kann die Funktionsfähigkeit des gescannten Gerätes beeinträchtigt werden.



Dies sollte daher bei der Abwägung, welche Scans in welcher Tiefe standardmäßig ausgeführt werden, eine Rolle spielen.

Agentenbasierte und agentenlose NACs schließen einander nicht aus und kommen je nach Anbieter auch in Kombination vor; etwa mit dem Ziel, die Informationen des Agenten (z. B. über installierte Patches) zu überprüfen.

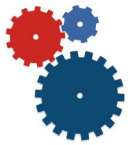
### Kombination mit anderen Sicherheitsprogrammen

Viele NACs sind entweder Teil eines umfassenderen Sicherheitsproduktes eines (oder mehrerer) Anbieter oder lassen sich mit anderen Sicherheitsprodukten kombinieren. Es gibt beispielsweise Anbieter von Antivirenprogrammen, die gleichzeitig NACs vertreiben und damit werben, dass dieses NAC besonders gut mit dem Antivirenprogramm zusammenarbeitet. Einige eher Hardware-orientierte Anbieter wie Cisco werben mit der Kombinierbarkeit ihrer Produkte mit Software-NACs wie beispielsweise Network Access Protection (NAP) von Microsoft. Einige NACs können ferner auch mit dem Simple Network Management Protokoll (SNMP) umgehen und betten sich damit in ein umfassendes Netzmanagementsystem ein. Interoperabilität zwischen Komponenten des Informationsverbundes und die Einbettung vom gewählten NAC in ein umfassendes Sicherheitskonzept sind wichtige Voraussetzungen für einen einwandfreien Betrieb. Daher sollten diese Randbedingungen gründlich erhoben und dokumentiert werden und mit den ermittelten Schutzbedarfen abgeglichen werden.

## Anwendungsszenarien von NACs: Wozu eignen sich NACs und was sind verbleibende Sicherheitsgefährdungen?

Bereits die Vielzahl der verschiedenen NAC-Varianten, -Funktionen und -Anbieter, die es auf dem Markt gibt, sowie die Tiefe des Eingriffs in die Netzstruktur der Institution macht deutlich, dass die Einführung eines NACs umfassend geplant und diverse Für und Wider der jeweiligen Varianten gegeneinander abgewogen werden müssen. Ein Netzzugangskontrollsystem, das als eine Art internes Intrusion Prevention System auftritt, kann dabei nur ein Baustein eines umfassenden Sicherheitssystems sein. Daher ist eine stufenweise Einführung eines NACs zu empfehlen. Es sollte beachtet werden, dass das gewünschte NAC unter Umständen zwar mit allen derzeit vorhandenen Komponenten zusammenarbeitet, aber unflexibel gegenüber weiteren Betriebssystemen und Komponenten sein kann.

Für eine gute Planung ist es wichtig, Anwendungsszenarien und Sicherheitsziele zu formulieren, wobei folgende Fragen hilfreich sein können:



- Durch welche Gefährdungen oder mögliche Szenarien ist die Sicherheit des eigenen Netzes bedroht?
- Kann das gewünschte Maß an Sicherheit mit einem NAC erreicht werden und welches NAC passt am besten dazu?
- Welche neuen Gefährdungen eröffnen sich durch die Einführung des NACs und welche Restrisiken verbleiben?

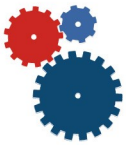
Die Wahl des jeweiligen NAC hängt immer von den individuellen Rahmenbedingungen ab. Die Szenarien und die darin enthaltenen Gefährdungen sind jedoch häufig vergleichbar. Zur Verdeutlichung von Gefährdungen und dem Nutzen von NACs werden hier vier Beispielszenarien betrachtet:

## Beispiel 1: Rückkehr mobiler IT in die Institution

In diesem Szenario besitzt eine Institution mobile IT, die von den Mitarbeitern außerhalb des internen Netzes genutzt wird und sogar außerhalb des internen Netzes an das Internet angeschlossen wird. Dazu gehören unter anderem Laptops von Mitarbeitern, die unterwegs und beim Kunden auf das Firmennetz zugreifen. Hierfür sieht beispielsweise die Maßnahme M 5.122 „Sicherer Anschluss von Laptops an lokale Netze“ aus den IT-Grundschutz-Katalogen vor, dass solche Geräte nach der Rückkehr zuerst auf Viren überprüft werden, bevor sie wieder auf das lokale Netz zugreifen dürfen. Ferner müssten zuerst auch alle Sicherheitsupdates des Betriebssystems und der Anwendungen aufgespielt werden. Eine Lösung dafür könnte sein, dass diese Geräte zuerst in einem, vom übrigen internen Netz abgeschottetem, Netz angeschlossen werden und ihre Sicherheit überprüft wird. Dies ist allerdings ein zeitaufwendiges Unterfangen, so dass die Gefahr besteht, dass die in der Maßnahme M 5.122 aufgeführten Test aus Zeitnot nicht mit der nötigen Sorgfalt durchgeführt werden.

Agentenbasierte NACs können ein Weg sein, die Empfehlungen der Maßnahme M 5.122 elegant umzusetzen, da mit dem NAC mobile Endgeräte zuerst auf ein virtuelles Quarantäne-Netz zugreifen, wo sie die neuesten Patches und Virendefinitionen herunterladen können, nach Viren durchsucht werden, die Einhaltung aller sonstigen Punkte der Sicherheitsleitlinie überprüft wird und nach positivem Ausgang der Prüfung automatisch voller Zugriff zum internen Netz gewährt wird. Dies alles geschieht bei der Variante mit permanentem Agenten automatisch, also ohne Umstecken oder händische Neukonfiguration durch Support-Mitarbeiter.

Ein temporärer Agent könnte die Einstellungen am Client zwar nicht selbständig ausführen, aber er könnte die mobilen Mitarbeiter zumindest mit einer Schritt-für-Schritt-



Anleitung versorgen, um alle notwendigen Veränderungen und Einstellungen durchzuführen.

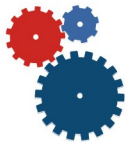
In dieser Zeit sind potentiell sicherheitsgefährdende Endgeräte in einer abgeschotteten Umgebung und stellen – eine sichere VLAN-Trennung vorausgesetzt – für die restlichen Endgeräte der Institution keine Bedrohung dar.

So verlockend dieses Szenario klingen mag, ist jedoch zu bedenken, dass es auf einem einwandfreien Agenten basiert. Ist der auf dem mobilen Endgerät installierte Agent durch Schadsoftware kompromittiert, kann das Endgerät infiziert sein, aber einwandfrei wirken und so Zugang zum Netz erlangen. Der Sicherheitsgewinn durch die Einführung eines NAC liegt dann lediglich darin, dass die Gefährdung des eigenen Netzes Schadsoftware voraussetzt, die auf den Agenten spezialisiert ist. Es ist zu erwarten, dass bei weiterer Verbreitung von NACs die kommerziell erhältlichen Virenbaukästen um diese Funktion erweitert werden. Bei agentenlosen NACs gibt es diesen Nachteil nicht, denn wo kein Agent auf dem Endgerät vorhanden ist, kann dieser auch nicht durch Schadsoftware kompromittiert werden. Ein agentenloses NAC hingegen könnte zwar nach Schwachstellen durch fehlende Patches scannen, nicht unbedingt aber nach der Aktualität der Virendefinitionen. Ferner kann ein agentenloses NAC weder notwendige Einstellungen auf dem Endgerät automatisch vornehmen, noch kann es dem Benutzer mitteilen, welche Sicherheitslücken noch zu schließen sind und diesen Schritt für Schritt durch die notwendigen Aktionen führen, sondern das Endgerät lediglich aus dem geschützten Netz aussperren.

## Beispiel 2: Sicherer Gastzugang für Besucher der Institution

In einem ähnlichen Szenario geht es darum, dass Gäste der Institution (beschränkten) Zugang zum internen Netz und/oder zum Internet gewährt werden soll, die hierdurch entstehenden Risiken für die Institution aber klein gehalten werden sollen. Durch ein NAC kann ein vom internen Netz getrenntes Gäste-VLAN eingerichtet werden. Je nach technischer Ausstattung können Gäste einen permanenten oder temporären NAC-Agenten installieren, der überprüft, ob die mitgebrachten Geräte die festgelegten Sicherheitsstandards erfüllen. Je nach Ergebnis dieser Überprüfung kann dann der Zugang zum Gäste-VLAN frei gegeben werden. Die Trennung zwischen Gäste-VLAN und internem Netz muss dabei ausreichend stark für den Schutzbedarf des internen Netzes sein.

Auch ohne NAC kann ein Gäste-VLAN eingerichtet werden, in das sich Gäste z. B. per VPN einwählen. Der zusätzliche Sicherheitsgewinn durch ein NAC besteht in diesem Fall darin, dass die Gastsysteme einer Sicherheitsüberprüfung unterzogen werden und so das Risiko reduziert wird, dass sich verschiedene Gäste im Gäste-VLAN untereinander mit



Schadsoftware kompromittieren. Eine solche Kompromittierung könnte für den Gastgeber eine Imageschädigung darstellen, denn auch wenn die Infektion faktisch nicht durch ein Endgerät der Institution passiert ist, so ist sie doch innerhalb der Institution passiert.

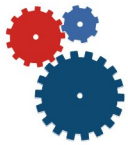
## Beispiel 3: Zugriff privater Endgeräte auf das interne Netz

Viele Mitarbeiter wünschen sich, ihre privaten Endgeräte wie Laptops, Smartphones oder Tablet-PCs auch in der Institution nutzen zu können. Typischerweise haben weder die Institution noch deren Mitarbeiter ein Interesse daran, die privaten Geräte durch die IT-Abteilung konfigurieren zu lassen. Unter diesen Voraussetzungen kann ein NAC mit auflösenden Agenten ein angemessener Kompromiss sein. Der Agent wird dabei nur für die Dauer der Netzteilnahme auf dem Endgerät installiert. Ein temporärer Agent benötigt allerdings für die Einhaltung der Sicherheitsleitlinie noch Unterstützung durch den Benutzer. Das durch das NAC gebildete VLAN für private Endgeräte ist – eine hinreichende Trennung der VLANs vorausgesetzt – vom Netz der Institution abgeschottet und die Mitarbeiter behalten weitestgehend die Kontrolle über ihre Endgeräte. Ein kritischer Punkt kann hier außerdem noch die Frage nach dem Zugriff auf interne Daten durch die privaten Endgeräten sein, was jedoch außerhalb des hier bearbeiteten Themas liegt.

## Beispiel 4: Reaktion auf unerlaubt angeschlossene Netzkomponenten

In einem LAN befinden sich normalerweise nicht nur Server und Clients, sondern auch andere Netzgeräte wie Netzdrucker, Scanner und VoIP-Telefone. In diesem Szenario wird betrachtet, wie verhindert werden kann, dass IT-Systeme im LAN ungenehmigt angeschlossen werden. Ein Gast oder auch ein Mitarbeiter könnte den Wunsch haben, „nur mal kurz“ auf das Internet zuzugreifen, und verbindet ein mobiles Gerät dafür über eine Netzsteckdose mit dem LAN (siehe z. B. in den IT-Grundschutz-Katalogen Gefährdung G 5.136 „Missbrauch frei zugänglicher Telefonanschlüsse“).

Auch ein Angreifer könnte versuchen, über ungeschützte Netzsteckdosen auf das LAN zuzugreifen und sich dafür beispielsweise einen wenig beobachteten Druckerraum suchen. Leider befinden sich Netzdrucker in frei zugänglichen Räumen (auch wenn dies in Maßnahme M 1.32 „Geeignete Aufstellung von Druckern und Kopierern“ anders gefordert wird). Ein Angreifer könnte also statt des Netzdruckers einen Laptop mit dem LAN verbinden. Auch wenn eine MAC-basierte Zugangskontrolle vorhanden ist, ist es leicht, die MAC-Adresse des Druckers herauszufinden und auf dem Laptop einzustellen. Dies trifft in der Regel bei Netzdruckern auch für die Authentisierungsdaten für ein 802.1X-Netz zu, wenn physischer Zugriff auf den Drucker besteht.

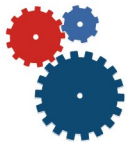


Ein NAC könnte aber sowohl das Umstecken als auch das veränderte Verhalten des Endgerätes bemerken und zeitnah reagieren, wie in Maßnahme M 4.302 „Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten“ empfohlen. Das neue Endgerät verhält sich nicht wie ein Drucker, da es nicht mehr nur auf dem Druckerport empfängt, sondern beispielsweise Samba-Freigaben im Netz sucht. Einige NACs können bei solchen Vorfällen das Gerät automatisch in ein anderes VLAN verlagern und so – eine hinreichende VLAN-Trennung vorausgesetzt – den Angriff abwehren und Alarm auslösen. Ein solches NAC nimmt damit zusätzlich Funktionen eines Intrusion Detection Systems wahr und stellt damit eine weitergehende Trennungsmaßnahme für Netze dar, wie sie in Maßnahme M 2.376 „Trennung des Daten- und VoIP-Netzes“ empfohlen wird.

## Verbleibende Sicherheitsgefährdungen

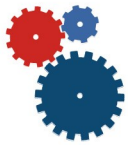
Diese Szenarien zeigen, dass NACs einige Vorteile und Sicherheitsgewinne bringen, aber auch komplexe Systeme sind, deren Einsatz genau durchdacht werden muss. Bei schlechter Planung bringen NACs nicht den erwünschten Sicherheitsgewinn, stattdessen könnten sogar neue Gefährdungen dazu kommen. Es ist zu überprüfen, ob die Sicherheitsgewinne durch ein NAC gegenüber dem Einführungsaufwand überwiegen und ob Anschaffung und Betrieb eines NAC zu diesen Investitionen in einem sinnvollen Verhältnis stehen. Auch wenn die Einführung eines passenden NACs grundsätzlich zu befürworten ist, sind vorab folgende Punkte zu erwägen:

- Sicherheitsleitlinien für den Netzverkehr zu erstellen und ein NAC entsprechend zu konfigurieren, sind komplexe Aufgaben. Werden hierbei Fehler gemacht, kann die Informationssicherheit der Institution gefährdet werden, wenn beispielsweise Zugriffsberechtigungen falsch gesetzt werden und dadurch Unberechtigte Zugang zu einem lokalen Netz erlangen könnten. Entsprechender Arbeits- und Schulungsaufwand muss in die Planung und den Betrieb eines NACs mit einbezogen werden und die entsprechenden Kosten mit dem zu erwartendem Sicherheitsgewinn in sinnvoller Relation stehen.
- Bei allen Varianten von NACs wird das lokale physische Netz in mehrere virtuelle lokale Netze mit dem Ziel aufgespalten, interne Informationen vor unbefugten Zugriffen zu schützen. Die Stärke dieser Trennung hängt nicht nur vom NAC ab, sondern vor allem an den Switches und Routern, die für die VLAN-Trennung sorgen. Bei der Anschaffung eines NACs muss daher überprüft werden, wie diese Trennung umgesetzt ist. Gegebenenfalls muss eine ergänzende Sicherheitsanalyse durchgeführt werden, ob die verwendete Trennung der VLANs dem Schutzbedarf der Informationen angemessen ist. Sollte diese Analyse ergeben, dass die



technischen Möglichkeiten zur Abschottung von VLANs mit unterschiedlichem Schutzbedarf unzureichend sind, scheiden NACs als Lösung aus.

- Durch die Einführung eines NACs werden Sicherheitsprüfungen zu den Validatoren verlagert. Daher muss sichergestellt werden, dass diese weder kompromittiert oder unbeabsichtigt falsch konfiguriert werden (z. B. durch ein Update). Wird z. B. auf einem Validator die Leitlinie von IPSec auf unverschlüsseltes IP umgestellt, so sorgen die permanenten Agenten auf allen Clients für die zeitnahe Umstellung auf unverschlüsselte Kommunikation im gesamten Netz. Wird auf dem Validator ein ungültiges Patchlevel oder Virensignaturdatenbank vorgeschrieben, so könnten in der Folge alle – eigentlich berechtigten – Benutzer in ein Quarantäne-Netz verlagert werden. Die Auswirkung einer fehlerhaften Konfiguration ist daher sehr groß. Daher muss entsprechend große Sorgfalt in die Konfiguration eines NACs gelegt werden. Damit Fehlkonfigurationen im nachhinein nachvollzogen werden können, sollten alle Konfigurationsänderungen an NACs protokolliert werden.
- Aufgrund der zentralen Bedeutung für die Informationssicherheit des Netzes und den weitreichenden Folgen durch Konfigurationseinstellungen des NACs stellen NACs ein lukratives Ziel für externe Angreifer dar. Erhält ein externer Angreifer Zugriff auf ein NAC und stellt dort beispielsweise ein falsches Patchlevel ein oder stellt die Kommunikation auf unverschlüsselten Modus, so werden alle berechtigten Clients aus dem Netz ausgeschlossen beziehungsweise zeitnah im gesamten Netz unverschlüsselt Daten ausgetauscht. Durch solche absichtlichen Fehlkonfigurationen an einem Gerät im Netz kann die Verfügbarkeit und Vertraulichkeit für alle weiteren Netzteilnehmer gefährdet werden. Daher müssen NACs auch vor absichtlichen Fehlhandlungen geschützt werden. So sollten sie nur in einem zutrittsgeschützten Raum aufgestellt sein, zu dem nur Administratoren Zutritt haben. Die Konfiguration eines NACs sollte nur vor Ort und nicht per Fernzugriff möglich sein.
  Bewertet eine Institution das Risiko vor einem internen Angreifer als groß genug, so sollte die oben genannte Protokollierung aller Konfigurationen zusätzlich revisionssicher erfolgen.
- Wichtig bei der Auswahl eines NACs ist die Frage, was bei seinem Ausfall passiert. Eine typische Antwort von NAC-Anbietern ist hier die redundante Auslegung des NACs, aber eventuell ist eine redundante Auslegung des NACs zu teuer. Bricht bei einem Ausfall des NACs also das gesamte Netz zusammen oder bietet das NAC passende Notfallvorsorgefunktionen? Viele NACs frieren bei einem Ausfall den aktuellen Zustand ein: Alle Benutzer verbleiben in ihrem jeweiligen VLAN, neue



Benutzer können sich jedoch nicht anmelden und Teilnehmer des Quarantäne-Netzes können nicht zum internen Netz wechseln. Das NAC könnte jedoch auf die regelmäßige Kommunikation mit dem NAC-Validator angewiesen sein und in diesem Fall die Funktionalität der Clients einschränken bzw. die Arbeit der Benutzer mit regelmäßigen Fehlermeldungen unterbrechen. Solche Auswirkungen müssen vorher analysiert werden und entsprechende Notfallvorsorgemaßnahmen ergriffen werden.

## Fazit

Heutige IT-Netze von Institutionen stehen vor vielen Herausforderungen. So nimmt die Anzahl der verschiedenen Endgeräte, Betriebssysteme und Anwendungen im Netz zu. Außerdem verschwimmen die Netzgrenzen zunehmend, da mobile Mitarbeiter von außerhalb der Institution auf das Netz zugreifen wollen sowie Auftragnehmer und Gäste auch innerhalb der Institution auf das Netz zugreifen sollen. Es stellt vor dem Hintergrund von Kostendruck und Anwenderwünschen nicht unerhebliche Schwierigkeiten dar, in einem solchen Umfeld Informationssicherheitsleitlinien zu überprüfen und für deren Einhaltung zu sorgen, sowie Angriffe auf das Netz und Störungen im Netz zu erkennen und ihnen zu begegnen. Am Markt existierende Systeme zur Netzzugangskontrolle können helfen, diese Herausforderungen und Schwierigkeiten zu bewältigen. Wenn Netzzugangskontrollsysteme in ein umfassendes Informationssicherheitsmanagement eingebettet sind, können sie in vielen Einsatzumgebungen die technischen Anforderungen der Informationssicherheit in IT-Netzen abdecken.

## Weitere BSI-Empfehlungen zu diesem Thema

- IT-Grundschutz-Kataloge, beispielsweise Maßnahme M 5.122 „Sicherer Anschluss von Laptops an lokale Netze“, M 4.302 „Protokollierung bei Druckern, Kopierern und Multifunktionsgeräten“ und M 2.376 „Trennung des Daten- und VoIP-Netzes“