Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.4 Network Access Control

1. Beschreibung

1.1. Einleitung

Eine Netzzugangskontrolle (engl. Network Access Control, NAC) sichert Netzzugänge im Endgerätebereich durch Identitätsprüfung (Authentisierung) und Reglementierung (Autorisierung) ab. Unter Endgeräten werden in diesem Baustein alle IT-Systeme verstanden, die am Access Layer eines Campus-Netzes angeschlossen werden. NAC kann sowohl in kabelgebundenen als auch in drahtlosen Netzen eingesetzt werden. Eine Identität kann zum Beispiel über Konten mit Zertifikaten sicher geprüft werden. Durch die folgende Autorisierung werden den Endgeräten über Autorisierungsregeln passende Netzsegmente und Berechtigungen zugewiesen und damit Zugriffsregeln festgelegt. Ebenso kann Endgeräten der Netzzugang verweigert werden.

Beispielsweise kann ein Drucker über NAC als solcher identifiziert und mit einem validen Zertifikat sicher authentisiert werden. Wurde der Drucker erfolgreich authentisiert, wird er dann mittels NAC-Autorisierung dem für den Drucker vorgesehenen Netzsegment zugewiesen.

NAC-Lösungen nutzen dabei entweder die im Standard IEEE 802.1X (Port Based Network Access Control) beschriebenen Techniken oder die sogenannte MAC-Adress-Authentisierung. Bei IEEE 802.1X erfolgt die Authentisierung über das Extensible Authentication Protocol (EAP) zwischen einer Software auf dem Endgerät, dem sogenannten Supplicant, und dem sogenannten Authenticator, der von einem Access-Switch, WLAN Access Point oder WLAN Controller realisiert wird. Für die Authentisierung wird zusätzlich ein zentraler RADIUS-Server (Remote Authentication Dial-In User Service) genutzt. Der RADIUS-Server wird auch als Authentication Server oder AAA-Server (Authentication, Authorization, Accounting) bezeichnet. Bei der MAC-Adress-Authentisierung wird das Endgerät über seine MAC-Adresse authentisiert.

Eine NAC-Lösung nach IEEE 802.1X umfasst also folgende Komponenten:

- Authentication Server oder RADIUS-Server
- Supplicant auf einem Endgerät
- Authenticator auf einem Access-Switch oder einer WLAN-Komponente (WLAN Access Point oder WLAN Controller)
- zentrale NAC-Identitätsverwaltung, die als integrierte Identitätsverwaltung auf dem Server realisiert sein kann oder auf bestehende Verzeichnisdienste zurückgreift

Eine NAC-Lösung umfasst in diesem Baustein alle zuvor beschriebenen Komponenten. Ist eine einzelne Komponente der NAC-Lösung gemeint, z. B. der RADIUS-Server, dann wird diese

Komponente tatsächlich auch als solche benannt. Als zentrale Komponenten einer NAC-Lösung gelten in diesem Baustein der RADIUS-Server und die NAC-Identitätsverwaltung.

Damit eine NAC-Lösung sinnvoll eingesetzt werden kann und die Netzzugänge geeignet abgesichert werden können, müssen viele Punkte festgelegt und die genannten Komponenten der Lösung aufeinander abgestimmt werden. Weiterhin sind NAC-spezifische Prozesse (z. B. Maßnahmen, um Störungen zu beheben) zu definieren und bestehende Prozesse (z. B. Inbetriebnahme von Endgeräten) anzupassen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei NAC zu etablieren. Eine NAC-Lösung soll sicherstellen, dass der Zugang zum Netz durch identitätsabhängige Autorisierungsregeln reglementiert wird. Dadurch werden Informationen geschützt, die über Netze verarbeitet, gespeichert und übertragen werden.

1.3. Abgrenzung und Modellierung

Der Baustein NET.3.4 *Network Access Control* ist auf die Elemente einer NAC-Lösung anzuwenden. Dies beinhaltet betroffene Netze, Clients und zentrale Komponenten.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt NAC-Lösungen, die auf dem Standard IEEE 802.1X und MAC-Adress-Authentisierung via RADIUS basieren. Dabei liegt der Fokus auf folgende Teilaspekte einer NAC-Lösung:

- allgemeine Festlegungen für NAC sowohl für die zentralen Komponenten als auch für die Endgeräte
- Anforderungen an Authentisierung und Autorisierung
- Festlegungen für Management und Betrieb einer NAC-Lösung

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Verzeichnisdienste (siehe APP.2.1 *Allgemeiner Verzeichnisdienst*)
- Netzarchitektur und -design (siehe NET.1.1 *Netzarchitektur und -design*)
- WLAN-spezifische Aspekte (siehe NET.2.1 *WLAN-Betrieb* und NET.2.2 *WLAN-Nutzung*)
- allgemeine Betriebsaspekte (siehe Bausteine der Schicht OPS *Betrieb*)

Dieser Baustein behandelt **nicht** die folgenden Inhalte:

- Port Security sowie allgemeine Aspekte für Netzkomponenten (siehe NET.3.1 *Router und Switches*)
- proprietäre NAC-Implementierungen, die nicht auf IEEE 802.1X basieren
- die Implementierung eines RADIUS-Servers auf Netzkomponenten (Access-Switch, WLAN Access Point oder WLAN Controller)
- administrative Authentisierung an Netzkomponenten mittels RADIUS
- allgemeine Aspekte für Endgeräte (siehe Bausteine der Schichten SYS.2 *Desktop-Systeme*, SYS.3 *Mobile Devices* und SYS.4 *Sonstige Systeme*)
- allgemeine Aspekte für Server (siehe SYS.1.1 *Allgemeiner Server*) und Virtualisierung (siehe SYS.1.5 *Virtualisierung*)

- allgemeine Aspekte für Identitäts- und Berechtigungsmanagement (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*)

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.4 *Network Access Control* von besonderer Bedeutung.

2.1. Unzureichende Planung der NAC-Lösung

Sind nicht alle für NAC relevanten IT-Systeme und Informationen in einem IT-Asset-Management erfasst, kann eine NAC-Lösung nicht ausreichend geplant werden. Endgeräte erhalten dann gegebenenfalls keinen Zugang zum Netz oder einen Zugang zu einem falschen Netzsegment.

Wurden die Anforderungen an die NAC-Lösung nicht ausreichend erfasst und analysiert, kann auch dies zu einer unzureichenden Planung führen. Beispielsweise ist es dann möglich, dass eingesetzte Switches die Anforderungen an die geplante NAC-Lösung nicht erfüllen können oder der geplante RADIUS-Server falsch dimensioniert wird. Eine weitere Folge könnten auch zu harte oder zu weiche Vorgaben für die genutzten Authentisierungs- und Autorisierungsverfahren sein. Dadurch könnte Endgeräten entweder der Zugang zum Netz verweigert oder unsichere Authentisierungsverfahren könnten genutzt werden, obwohl sichere Verfahren möglich wären. Möglicherweise könnten dadurch auch zu weitreichende Kommunikationsberechtigungen erlangt werden.

2.2. Unzureichend abgestimmte Integration von Endgeräten in die NAC-Lösung

Fehlende oder unzureichend umgesetzte Orchestrierungswerkzeuge, Sicherheitsrichtlinien, Anforderungskataloge und Ressourcen für die Erfassung aller Endgeräte können dazu führen, dass Endgeräte unzureichend abgestimmt in die NAC-Lösung integriert werden. Dies erschwert es, ein sicheres und betriebsfreundliches Authentisierungsverfahren je Endgerätegruppe umzusetzen und ein entsprechendes Inbetriebnahmeverfahren zu konzipieren. Dadurch könnten die Kommunikationsmöglichkeiten der Endgeräte negativ beeinträchtigt werden. Außerdem kann es sein, dass zu schützende Geräte versehentlich in falschen Netzsegmenten positioniert werden.

Sind die Endgeräte unzureichend standardisiert oder werden NAC-spezifische Endgeräteanforderungen unzureichend unterstützt, kann dies auch dazu führen, dass unsichere Authentisierungsverfahren eingesetzt werden, obwohl eine starke Authentisierung grundsätzlich möglich wäre.

2.3. Nutzung unzureichend sicherer Protokolle bei NAC

Werden sichere EAP-Authentisierungsverfahren technisch nicht unterstützt, kann es passieren, dass unsichere Authentisierungsprotokolle wie EAP-MD5 oder MAC-Authentisierung eingesetzt werden müssen. In diesem Fall sind Spoofing-, Replay- oder Man-in-the-Middle-Angriffe leichter möglich und es kann nicht ausgeschlossen werden, dass unberechtigte IT-Systeme in das Netz gelangen. Wird für Endgeräte mit schwachen Authentisierungsprotokollen nicht eingeschränkt, mit welchen Zielen und über welche Protokolle sie kommunizieren dürfen, können auch unberechtigte IT-Systeme, die durch einen der oben genannten Angriffe Zugang erhalten, weitreichende Kommunikationsmöglichkeiten erlangen.

2.4. Fehlerhafte Konfiguration der NAC-Lösung

Durch menschliche Fehler, unzureichende Prozesse oder unzureichende Personalkapazitäten und den dadurch bedingten Zeitmangel kann es passieren, dass die NAC-spezifischen Parameter an Endgeräten, Access-Switches oder RADIUS-Servern (NAC-Regelwerk) fehlerhaft konfiguriert werden. Dies kann dazu führen, dass sich die gesamte NAC-Lösung ungewollt falsch verhält, wodurch z. B. Endgeräte benötigte Ressourcen nicht erreichen können oder keinen Netzzugang erhalten.

Werden MAC-Adressen bewusst falsch registriert, können dadurch zu viele Ressourcen freigeschaltet werden, indem falsche Netzsegmente oder andere falsche Autorisierungsparameter zugewiesen werden.

2.5. Unzureichende Validierung von Konfigurationsänderungen

Unzureichende Änderungsprozesse, die Konfigurationsänderungen nicht oder nur unzureichend validieren, begünstigen Fehler in der Konfiguration. Hierdurch kann es passieren, dass für Endgeräte zu viel oder zu wenig schützenswerte Ressourcen erreichbar sind oder es ihnen gänzlich verwehrt wird, auf das Netz zuzugreifen. Wird z. B. NAC an Switch-Ports ohne zwingenden Grund abgeschaltet, können gegebenenfalls unberechtigte Endgeräte uneingeschränkt auf das Netz zugreifen. Wird neue Software auf Endgeräten unzureichend validiert, kann dies z. B. zu Interferenzen zwischen Software-Komponenten führen und die Funktionalität des Supplicants beeinflussen.

2.6. Unzureichend geschützter Netzzugang

Wird NAC an Switch-Ports temporär oder dauerhaft abgeschaltet, ist der Netzzugang unzureichend geschützt. Dadurch ist es möglich, dass unautorisierte Personen auf das Netz zugreifen können oder unsichere IT-Systeme zu weitgehende Kommunikationsberechtigungen erhalten. In der Folge kann unberechtigt auf Informationen zugegriffen und Informationen können manipuliert oder gelöscht werden. Außerdem kann auf diese Weise Schadsoftware eingeschleust werden.

Wird die Endgeräte-Compliance unzureichend geprüft, kann dies auch zu einem unzureichend geschützten Netzzugang führen, wenn das Endgerät z. B. über unzureichenden Virenschutz verfügt und dadurch Schadsoftware eingeschleust wird.

2.7. Ausfall oder unzureichende Erreichbarkeit der zentralen NAC-Komponenten

Ein unzureichendes oder unzureichend umgesetztes NAC-Konzept, gestörte NAC-Komponenten oder ein gestörtes Netz, unzureichende Anforderungsanalyse, mangelnde Prozesse oder Denial-of-Service-Angriffe (DoS-Angriffe) können dazu führen, dass die zentralen NAC-Komponenten ausfallen oder nicht erreichbar sind. Dies hat Auswirkungen auf die Fähigkeit der Endgeräte zu kommunizieren. Zum Beispiel haben, abhängig von der Switch-Konfiguration, Endgeräte bei Ausfall aller RADIUS-Server entweder keinen oder einen uneingeschränkten Netzzugang.

2.8. Nachverfolgung von Benutzenden

Ein unzureichendes Administrationskonzept, eine unzureichende Umsetzung der Konzeptionierung, zu lange Speicherzeiten oder eine mangelnde Abstimmung mit Betriebsrat und Datenschutzbeauftragten könnten dazu führen, dass personenrelevante Log-Daten unzureichend geschützt sind. Dadurch könnten Benutzendenprofile erstellt werden, die es ermöglichen, dass Mitarbeitende zeitlich nachverfolgt werden können.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.4 *Network Access Control* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Institution

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.3.4.A1 Begründete Entscheidung für den Einsatz von NAC (B) [Institution]

Die Institution MUSS grundsätzlich entscheiden, ob und in welchem Umfang NAC eingesetzt wird. Die getroffene Entscheidung MUSS zusammen mit einer Begründung an geeigneter Stelle dokumentiert werden.

Wird NAC eingesetzt, MÜSSEN folgende Punkte geeignet thematisiert werden:

- Netzbereiche und Netzkomponenten, für die NAC realisiert werden soll
- Umgang mit internen Endgeräten und Fremdendgeräten
- Berücksichtigung von NAC bei der Beschaffung von neuen IT-Systemen

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.3.4.A2 Planung des Einsatzes von NAC (S)

Der Einsatz von NAC SOLLTE umfassend und detailliert geplant werden. Die Planung SOLLTE dabei mindestens folgende Aspekte beinhalten:

- Erstellung von Anforderungskatalogen für Endgeräte, Access-Switches und RADIUS-Server
- Prüfung und gegebenenfalls Ergänzung des IT-Asset-Managements
- Erstellung eines spezifischen NAC-Konzepts
- Festlegung von Beschaffungs-, Betriebs-, und Incident-Prozessen für NAC-Komponenten
- Migrationsplanung
- Monitoring und Logging der NAC-Lösung

- Anbindung an sicherheitsrelevante Komponenten (z. B. Firewalls, Virenschutz, Schwachstellen-Scanner, System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen)
- Zusatzfunktionen wie Profiling, Endgerätekonformitätsprüfung und Integritätsprüfung sowie Verschlüsselung auf Layer 2 mit MACsec

NET.3.4.A3 Erstellung eines Anforderungskatalogs für NAC (S)

Die Anforderungen an die NAC-Lösung SOLLTEN in einem Anforderungskatalog erhoben werden. Der Anforderungskatalog SOLLTE dabei die grundlegenden funktionalen Anforderungen umfassen und alle NAC-Komponenten (z. B. Endgeräte, Access-Switches und RADIUS-Server) adressieren.

Der Anforderungskatalog SOLLTE mit allen betroffenen Fachabteilungen, den zuständigen Gremien und den Richtlinien der Institution abgestimmt werden. Der Anforderungskatalog SOLLTE regelmäßig und bei Bedarf aktualisiert werden.

Wenn NAC-Komponenten beschafft werden, SOLLTEN zugehörige Anforderungen berücksichtigt werden.

Die NAC-Lösung SOLLTE auf Basis des Anforderungskatalogs getestet werden.

NET.3.4.A4 Erstellung eines NAC-Konzepts (S)

Ausgehend von der Entscheidung aus NET.3.4.A1 *Begründete Entscheidung für den Einsatz von NAC* und den Anforderungen an die NAC-Lösung SOLLTE ein NAC-Konzept erstellt werden. Das NAC-Konzept SOLLTE mit dem Segmentierungskonzept gemäß NET.1.1 *Netzarchitektur und -design* abgestimmt werden. Darüber hinaus SOLLTEN im NAC-Konzept mindestens folgende Aspekte festgelegt werden:

- Netzbereiche, in denen NAC eingeführt wird
- Authentisierung und Autorisierung
- Nutzung von Zusatzfunktionen
- Konfigurationsvorgaben für betroffene Endgerätetypen, Access-Switches und WLAN Access Points sowie WLAN Controller
- Aufbau der RADIUS-Infrastruktur und das grundlegende Regelwerk für NAC
- Anbindung an externe Sicherheitskomponenten wie Firewalls oder Virenschutz
- Anbindung an Verzeichnisdienste

Das NAC-Konzept SOLLTE alle technischen und organisatorischen Vorgaben beschreiben. Insbesondere SOLLTEN alle relevanten Prozesse und die Migration thematisiert werden.

Das NAC-Konzept SOLLTE regelmäßig geprüft und bei Bedarf aktualisiert werden.

NET.3.4.A5 Anpassung von Prozessen für Endgeräte bezüglich NAC (S)

Für die Endgeräte, die in die NAC-Lösung eingebunden werden, SOLLTE NAC in allen relevanten Prozessen angemessen berücksichtigt werden. Insbesondere SOLLTEN die Prozesse zu Inbetriebnahme, Austausch, Änderungen und Störungen angepasst werden.

Für Supplicant-Software, Konfiguration und Identitätsmerkmale (z. B. Zertifikate), die für NAC auf den Endgeräten erforderlich sind, SOLLTE ein Prozess festgelegt werden, um die Endgeräte zentral zu verwalten.

NET.3.4.A6 Festlegung von Notfallprozessen für NAC (S)

Wird die Wirkkette bei NAC gestört, SOLLTE erwogen werden, die Sicherheitsmechanismen von NAC temporär in angemessenem Umfang zu deaktivieren.

Bei den Notfallmaßnahmen, die im Notfallprozess festgelegt werden, SOLLTEN Produktivität und Informationssicherheit gegeneinander abgewogen werden. Dabei SOLLTEN die folgenden Optionen von Notfallmaßnahmen (RADIUS-down-Policies) betrachtet werden:

- Die bestehenden Verbindungen werden durch Mechanismen wie temporäre Aussetzung der Reauthentisierung beibehalten, jedoch werden alle neuen Anmeldeversuche abgelehnt, so dass das vorgesehene Sicherheitsniveau erhalten bleibt.
- Die dynamische Zuordnung wird für neue Anmeldeversuche ausgesetzt und stattdessen eine feste, vordefinierte Zuweisung von Netzsegmenten durch Access-Switches vorgenommen, so dass zumindest grundlegend kommuniziert werden kann.
- NAC wird auf den Access-Switches oder auf einzelnen Ports eines Access-Switches deaktiviert, so dass weiterhin uneingeschränkt kommuniziert werden kann.

RADIUS-down-Policies SOLLTEN mit den relevanten Sicherheitsrichtlinien der Institution abgestimmt werden.

NET.3.4.A7 Nutzung sicherer Authentisierungsverfahren (S)

Endgeräte SOLLTEN sichere Authentisierungsverfahren nach dem Stand der Technik verwenden. Endgeräte SOLLTEN automatisiert auf Basis von Zertifikaten oder Zugangskonten authentisiert werden.

Unsichere Authentisierungsverfahren SOLLTEN nur in begründeten Ausnahmefällen genutzt und die Entscheidung dokumentiert werden.

NET.3.4.A8 Festlegung der NAC-spezifischen Rollen und Berechtigungen für den RADIUS-Server (S)

Im Rollen- und Berechtigungskonzept für den RADIUS-Server SOLLTEN die verschiedenen Gruppen berücksichtigt werden, die wegen NAC auf einen RADIUS-Server zugreifen müssen, um diesen zu administrieren. Dies SOLLTE insbesondere dann sorgfältig geplant werden, wenn ein zentraler RADIUS-Server für die gesamte Institution bereitgestellt wird. Mindestens SOLLTEN die folgenden Gruppen mit NAC-spezifischem Zugriff auf den RADIUS-Server zusätzlich zum allgemeinen IT-Betrieb berücksichtigt werden:

- die jeweiligen Organisationseinheiten, die Access-Switches (RADIUS-Clients) für ihren Netzbereich administrieren
- die jeweiligen Zuständigen für Endgerätegruppen, die Identitäten (z. B. MAC-Adressen) ihrer entsprechenden Gruppen verwalten
- der First-Level-Support, der fehlerhafte RADIUS-Freigaben analysiert und gegebenenfalls die entsprechenden Freischaltungen anpasst

NET.3.4.A9 Festlegung eines angepassten NAC-Regelwerkes (S)

Für die NAC-Lösung SOLLTE ein NAC-Regelwerk definiert werden, das das NAC-Konzept umsetzt und festlegt, wie die Endgeräte auf das Netz zugreifen dürfen. Hierin SOLLTE für jedes Endgerät bzw. für jede Endgerätegruppe festgelegt werden, ob uneingeschränkt auf das Netz zugegriffen werden darf, ob der Zugriff verweigert wird oder ob nur Segmente mit eingeschränkten Kommunikationsmöglichkeiten erreichbar sind.

Im NAC-Regelwerk SOLLTE auch festgelegt werden, auf welcher Basis die Zugangskontrolle erfolgt. Hierfür SOLLTEN für alle Endgeräte die genutzten Authentisierungsmethoden und die Bedingungen für eine erfolgreiche Authentisierung festgelegt werden.

NET.3.4.A10 Sichere Nutzung von Identitäten (S)

Für die NAC-Authentisierung SOLLTEN individuelle Identitäten genutzt werden. Identitäten, die von mehr als einem Endgerät verwendet werden, SOLLTEN nur in begründeten Ausnahmefällen genutzt werden.

Alle Informationen, die für eine erfolgreiche Authentisierung benötigt werden, SOLLTEN nach aktuellem Stand der Technik vor unberechtigtem Zugriff abgesichert werden.

NET.3.4.A11 Sichere Konfiguration der NAC-Lösung (S)

Alle Komponenten der NAC-Lösung SOLLTEN sicher nach dem Stand der Technik konfiguriert werden. Hierfür SOLLTEN entsprechende Standard-Konfigurationen und Betriebshandbücher entwickelt und bereitgestellt werden.

Die vorgegebenen und umgesetzten Konfigurationen für die Komponenten der NAC-Lösung SOLLTEN regelmäßig überprüft und gegebenenfalls angepasst werden.

Auf Endgeräten SOLLTEN die Berechtigungen für die Benutzenden derart eingeschränkt werden, dass diese die Konfigurationsparameter für den Supplicant nicht manipulieren, den Supplicant nicht deaktivieren und die Schlüssel oder Passwörter für NAC nicht auslesen können.

Für Access-Switches oder für einzelne Ports von Access-Switches SOLLTE die NAC-Authentisierung nur in begründeten und zuvor festgelegten Ausnahmefällen deaktiviert werden. Hierfür SOLLTEN technische Maßnahmen genutzt werden, die gegebenenfalls durch organisatorische Maßnahmen ergänzt werden.

NET.3.4.A12 Monitoring der NAC-Lösung (S)

Die zentralen RADIUS-Server und alle Access-Switches mit Authenticator sowie alle weiteren zentralen Dienste, die für die NAC-Lösung essentiell sind, SOLLTEN in ein möglichst umfassendes und einheitliches Monitoring eingebunden werden. Ergänzend zum allgemeinen Monitoring gemäß OPS.1.1.1 *Allgemeiner IT-Betrieb* SOLLTEN alle NAC-spezifischen Parameter überwacht werden, die die Funktionalität der NAC-Lösung oder der entsprechenden Dienste sicherstellen.

Insbesondere SOLLTE die Verfügbarkeit des RADIUS-Protokolls überprüft werden. Hierfür SOLLTEN RADIUS-Anfragen an aktive Konten erzeugt werden, um die gesamte NAC-Wirkkette inklusive der externen Verzeichnisdienste zu prüfen.

Für die Access-Switches SOLLTE der Status von NAC in das Monitoring einbezogen werden, um ein Deaktivieren von NAC zu erkennen.

Abweichungen von definierten Zuständen und Grenzwerten SOLLTEN dem IT-Betrieb gemeldet werden.

NET.3.4.A13 Erstellung von Validierungsvorgaben für die NAC-Konfiguration (S)

Für die NAC-Lösung SOLLTEN Validierungsvorgaben erstellt werden, um sicherzustellen, dass die NAC-Komponenten das NAC-Konzept angemessen umsetzen. Die Validierungsvorgaben SOLLTEN insbesondere die unterschiedlichen Funktionsdetails für die verschiedenen NAC-Komponenten berücksichtigen.

Die Validierung SOLLTE als Soll-Ist-Vergleich regelmäßig sowie bei Bedarf für die zentralen NAC-Komponenten und die Access-Switches durchgeführt werden.

NET.3.4.A14 Umsetzung weiterer Maßnahmen bei Verwendung von MAC-Adress-Authentisierung (S)

Endgeräte, die nicht über eine sichere EAP-Methode authentisiert werden können und anhand ihrer MAC-Adresse identifiziert werden, SOLLTEN NICHT als vertrauenswürdige Endgeräte eingestuft werden. Der Netzzugang SOLLTE auf das notwendige Minimum beschränkt werden.

Hierfür SOLLTEN weitere Maßnahmen wie Nutzung von Kommunikationsbeschränkungen oder nachgelagertes Endgeräte-Profiling der Endgeräte-Aktivitäten umgesetzt werden.

NET.3.4.A15 Anbindung Virenschutz an NAC-Lösung (S)

Jedes Endgerät SOLLTE auf Schadsoftware geprüft werden, bevor es an das Netz der Institution angebunden wird und bevor es auf IT-Systeme der Institution zugreift. Hierfür SOLLTE für die NAC-Endgeräte ein geeigneter Virenschutz mit der NAC-Authentisierung und Autorisierung gekoppelt werden.

Falls das Virenschutzprogramm Schadsoftware meldet, SOLLTE die NAC-Lösung mit geeigneten Maßnahmen reagieren.

NET.3.4.A16 Protokollierung der Ereignisse (S)

Ergänzend zu OPS.1.1.5 *Protokollierung* SOLLTEN Statusänderungen an NAC-Komponenten sowie alle relevanten NAC-spezifischen, gegebenenfalls sicherheitskritischen Ereignisse protokolliert werden. Zusätzlich SOLLTEN alle schreibenden Konfigurationszugriffe auf die zentralen NAC-Komponenten protokolliert werden.

Es SOLLTE festgelegt werden, welche Protokollierungsdaten mit welchen Details erfasst und welche Daten auf einer zentralen Protokollierungsinstanz zusammengeführt werden.

Protokollierungsdaten SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

Sicherheitskritische Ereignisse wie RADIUS-down oder eine ungewöhnliche Anzahl von RADIUS-Anfragen SOLLTEN zu einem automatischen Alarm führen.

NET.3.4.A17 Positionierung des RADIUS-Servers im Management-Bereich (S)

Der RADIUS-Server SOLLTE in einem geschützten Netzsegment innerhalb des Management-Bereichs (siehe NET.1.1 *Netzarchitektur und -design*) positioniert werden. Kommunikationsanfragen an den RADIUS-Server SOLLTEN nur von vertrauenswürdigen Quellen zugelassen werden. Diese SOLLTEN auf ein Minimum eingeschränkt werden.

Der RADIUS-Server SOLLTE NICHT direkt mit Endgeräten kommunizieren, sondern ausschließlich über den Authenticator auf den Access-Switches. Anfragen der Access-Switches SOLLTEN nur aus dem gemeinsamen Management-Netzsegment akzeptiert werden.

NET.3.4.A18 Dokumentation der NAC-Lösung (S)

Die NAC-Lösung mit allen NAC-Komponenten SOLLTE geeignet dokumentiert werden.

Aus der Dokumentation SOLLTE mindestens hervorgehen, auf welchen Komponenten und Endgeräten NAC mit welchen Parametern genutzt wird und welche Abhängigkeiten zwischen den Komponenten existieren. Auch SOLLTE das Regelwerk für Authentisierung und Autorisierung, das in Software-Code vorliegt, ergänzend in vereinfachter, verständlicher Form dokumentiert werden. Darüber hinaus SOLLTE die Konfiguration aller NAC-Komponenten, gegebenenfalls kategorisiert, umfassend dokumentiert werden.

Die Dokumentation SOLLTE bei jeder Änderung fortgeschrieben und stets aktuell gehalten werden. Die Aktualität der Dokumentation SOLLTE regelmäßig und bei Bedarf geprüft werden.

NET.3.4.A19 Ordnungsgemäße Verwaltung von Identitäten zur Authentisierung (S)

Alle Identitäten, die via NAC einen Zugang zum Netz der Institution ermöglichen, SOLLTEN geeignet geschützt und verwaltet werden. Hierzu SOLLTEN mindestens die folgenden Punkte festgelegt werden:

- Handhabung und Schutz von Zertifikaten
- Prüfen, Sperren und Löschen von nicht mehr genutzten Identitäten

- Prozess und Schnittstellen zur Sperrung einer Identität

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.3.4.A20 Einsatz von MACsec (H)

Für jedes Datenpaket SOLLTE die Datenintegrität gewährleistet werden. Darüber hinaus SOLLTE erwogen werden, diese Daten zu verschlüsseln. Hierfür SOLLTE MACsec gemäß IEEE 802.1AE genutzt werden.

Access-Switches und Endgeräte, die MACsec nicht unterstützen oder für die MACsec nicht eingerichtet werden soll, SOLLTEN erfasst werden. Für diese SOLLTE regelmäßig überprüft werden, ob die Ausschlussgründe noch gelten.

NET.3.4.A21 Einsatz von Endgerätekonformitätsprüfung (H)

Bevor ein Endgerät an das Netz der Institution angebunden wird und bevor es auf IT-Systeme der Institution zugreift, SOLLTE geprüft werden, ob es den Konformitätsvorgaben der Institution genügt (Compliance Check).

Für jedes Endgerät SOLLTE festgelegt werden, welche Vorgaben das Endgerät einzuhalten hat. Endgeräte, die nicht den Konformitätsvorgaben der Institution genügen, SOLLTEN nur stark eingeschränkt auf das Netz der Institution zugreifen dürfen.

Die NAC-Lösung SOLLTE mit einem Werkzeug zur Konformitätsprüfung verbunden werden, das eine Bewertung des Zustands der Endgeräte vornimmt und an die NAC-Lösung meldet. Auf dieser Basis SOLLTE die NAC-Lösung steuern, wie die Endgeräte auf das Netz zugreifen dürfen.

NET.3.4.A22 NAC-Autorisierung mit Mikrosegmenten (H)

Endgeräte mit ähnlichem Anforderungsprofil und identischem Schutzbedarf SOLLTEN via NAC getrennten Netzsegmenten zugewiesen werden.

Darüber hinaus SOLLTE erwogen werden, ob mit NAC eine Mikrosegmentierung der zu autorisierenden Endgeräte umgesetzt wird.

NET.3.4.A23 Einsatz von autarken RADIUS-Servern für unterschiedliche Netzbereiche und Funktionen (H)

Für NAC SOLLTEN dedizierte und autarke RADIUS-Server eingesetzt werden. Weitere Funktionen wie VPN-Zugriffsregelung SOLLTEN NICHT gemeinsam mit NAC-Funktionen auf einem gemeinsamen RADIUS-Server realisiert werden.

Zusätzlich SOLLTE erwogen werden, dedizierte und autarke RADIUS-Server für unterschiedliche Netze bereitzustellen. Hier SOLLTEN insbesondere getrennte RADIUS-Server erwogen werden, um Office- und Produktions-Endgeräte oder LAN- und WLAN-Endgeräte getrennt abzusichern.

Darüber hinaus SOLLTE erwogen werden, für einzelne Netz- oder Funktionsbereiche eigenständige RADIUS-Server einzurichten.

NET.3.4.A24 Nutzung sicherer Protokolle zwischen NAC-Komponenten (H)

Für die Kommunikation zwischen den zentralen NAC-Komponenten SOLLTEN grundsätzlich Protokolle verwendet werden, die nach dem Stand der Technik als sicher gelten. Für die Kommunikation zwischen dem RADIUS-Server und einem gegebenenfalls genutzten Verzeichnisdienst SOLLTEN nur sichere Protokolle eingesetzt werden.

Darüber hinaus SOLLTE auch geprüft werden, ob für die Kommunikation zwischen dem RADIUS-Server und Access-Switches sichere Protokolle eingesetzt werden sollen.

NET.3.4.A25 Einbindung der NAC-Lösung in ein Sicherheitsmonitoring (H)

Die NAC-Lösung SOLLTE in ein Sicherheitsmonitoring eingebunden werden. Dies SOLLTE zumindest für die zentralen NAC-Komponenten und für die weiteren zentralen Dienste, die von der NAC-Lösung genutzt werden, umgesetzt werden.

NAC-spezifische Sicherheitsereignisse (z. B. häufige Zurückweisung von Anfragen oder die Mehrfachverwendung von Identitäten) SOLLTEN in eine Alarmierung übernommen werden.

Wird für die IT der Institution ein System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen eingesetzt, SOLLTEN die zentralen NAC-Komponenten sowie gegebenenfalls die weiteren zentralen Dienste hierin eingebunden werden.

NET.3.4.A26 Hochverfügbarkeit der zentralen NAC-Komponenten (H)

Die zentralen NAC-Komponenten SOLLTEN redundant ausgelegt werden. Alle weiteren zentralen Dienste, die für die Funktionsfähigkeit der NAC-Lösung essentiell sind, SOLLTEN auch hochverfügbar ausgelegt sein.

Die für die Hochverfügbarkeit relevanten Parameter SOLLTEN in Monitoring und Protokollierung integriert werden. Statusänderungen und Warnmeldungen SOLLTEN regelmäßig kontrolliert und gegebenenfalls in eine Alarmierung einbezogen werden.

Die RADIUS-down-Policies, mit denen eine Kommunikation auch bei ausgefallenem RADIUS-Dienst gewährleistet wird, SOLLTEN das Sicherheitsniveau des Netzes NICHT senken.

NET.3.4.A27 Prüfung der Notwendigkeit für MAC-Adress-Authentisierung (H)

Eine Authentisierung über MAC-Adressen SOLLTE nur dort genutzt werden, wo dies technisch unumgänglich ist und die Sicherheitsrichtlinien dies zulassen.

Es SOLLTE im Vorfeld geprüft werden, ob solche Ausnahmefälle notwendig sind. Ist dies der Fall, SOLLTEN die Ausnahmefälle auf den minimalen Einsatzbereich eingeschränkt werden.

Die Begründung und das Ergebnis der Prüfung SOLLTEN dokumentiert werden. Sie SOLLTEN regelmäßig und bei Bedarf nochmals verifiziert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein NET.3.4 *Network Access Control* sind keine weiterführenden Informationen vorhanden.