NET.3.3: VPN

1 Beschreibung

1.1 Einleitung

Mithilfe von Virtuellen Privaten Netzen (VPNs) können schutzbedürftige Daten über nicht-vertrauenswürdige Netze wie das Internet übertragen werden. Ein VPN ist ein Netz, das physisch innerhalb eines anderen Netzes betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs können mithilfe kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten schützen. Die sichere Authentisierung der Kommunikationspartner ist auch dann möglich, wenn mehrere Netze oder IT-Systeme über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

1.2 Zielsetzung

Der Baustein definiert Anforderungen, mit denen sich ein VPN zielgerichtet und sicher planen, umsetzen und betreiben lässt.

1.3 Abgrenzung und Modellierung

Der vorliegende Baustein ist für jede Art von Fernzugriffen auf den Informationsverbund auf jeden VPN-Endpunkt anzuwenden.

In diesem Baustein werden nur VPN-Systeme für die Schichten 2 (Sicherungsschicht) bis 4 (Transportschicht) des Open-Systems-Interconnection (OSI)-Modells abgedeckt. Der Baustein geht nicht auf Grundlagen für sichere Netze ein (siehe dazu NET.1.1 *Netzarchitektur und -design*). Auch deckt dieser Baustein nicht alle mit dem Betrieb eines VPN zusammenhängenden Prozesse ab. So müssen zusätzlich vor allem die Bausteine CON.1 *Kryptokonzept* und OPS.1.2.5 *Fernwartung* beachtet werden.

Empfehlungen, wie die Betriebssysteme der VPN-Endpunkte konfiguriert werden können, sind ebenfalls nicht Bestandteil dieses Bausteins. Entsprechende Anforderungen sind im Baustein SYS.1.1 *Allgemeiner Server* beziehungsweise SYS.2.1 *Allgemeiner Client* sowie in den jeweiligen betriebssystemspezifischen Bausteinen des IT-Grundschutz-Kompendiums zu finden.

2 Gefährdungslage

Folgende spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.3 *VPN* von besonderer Bedeutung:

2.1 Fehlende oder unzureichende Planung des VPN-Einsatzes

Bei einem nicht sorgfältig geplanten, aufgebauten oder konfigurierten VPN können Sicherheitslücken entstehen, die alle IT-Systeme betreffen könnten, die mit dem VPN verbunden sind. Angreifern kann es

so möglich sein, auf vertrauliche Informationen der Institution zuzugreifen.

So ist es durch eine unzureichende VPN-Planung beispielsweise möglich, dass die Benutzer nicht ordnungsgemäß geschult wurden. Dadurch könnten sie das VPN in einer unsicheren Umgebung benutzen oder sich von unsicheren Clients aus einwählen. Dies ermöglicht es Angreifern eventuell, auf das gesamte Institutionsnetz zuzugreifen.

Auch wenn die regelmäßige Kontrolle der Zugriffe auf das VPN unzureichend geplant wurde, könnten Angriffe nicht rechtzeitig erkannt werden. Somit kann nicht zeitnah reagiert werden und ein Angreifer kann unbemerkt Daten stehlen oder ganze Prozesse sabotieren.

2.2 Unsichere VPN-Dienstleister

Hat eine Institution einen VPN-Dienstleister nicht sorgfältig ausgewählt, könnte dadurch das gesamte Netz der Institution unsicher werden. So könnte beispielsweise ein vom Dienstleister unsicher angebotener VPN-Zugang von Angreifern genutzt werden, um gezielt Informationen zu stehlen.

2.3 Probleme bei der lokalen Speicherung der Authentisierungsdaten für VPNs

Viele VPN-Clients erlauben es, die zur Authentisierung notwendigen Daten für den Fernzugriff lokal zu speichern, sodass der Benutzer sie beim erneuten Verbindungsaufbau nicht noch einmal eingeben muss. Gelingt es einem Angreifer auf den VPN-Client zuzugreifen, kann er eventuell so die Zugangsdaten auslesen und sich als legitimer Benutzer am Netz der Institution anmelden. Somit kann er auf die lokalen Netze und die darin enthaltenen Informationen und erreichbaren Dienste zugreifen.

2.4 Unsichere Konfiguration der VPN-Clients für den Fernzugriff

Wird ein VPN-Client nicht sicher konfiguriert, könnten die Benutzer dessen Sicherheitsmechanismen falsch oder gar nicht benutzen. Auch verändern sie eventuell die Konfiguration des VPN-Clients. Ebenso ist es durch eine unsichere Konfiguration möglich, dass vom Benutzer installierte Software auch die Sicherheit des VPN-Clients gefährdet.

2.5 Unsichere Standard-Einstellungen auf VPN-Komponenten

In der Standard-Einstellung sind VPN-Komponenten meist ohne oder nur mit unzureichenden Sicherheitsmechanismen vorkonfiguriert. Oft wird mehr auf Benutzerfreundlichkeit und problemlose Integration in bestehende IT-Systeme als auf Sicherheit geachtet. Werden VPN-Komponenten nicht oder nur mangelhaft an die konkreten Sicherheitsbedürfnisse der Institution angepasst, können Schwachstellen und somit gefährliche Angriffspunkte entstehen. Werden beispielsweise vom Hersteller voreingestellte Passwörter nicht geändert, könnte das gesamte VPN und damit das interne Netz der Institution angegriffen werden.

2.6 Diebstahl von mobilen Endgeräten mit VPN-Client

Mobile Endgeräte werden öfter gestohlen oder gehen anderweitig verloren. Dadurch kann es passieren, dass Angreifer über die dort eingerichtete VPN-Verbindung auf das interne Netz der Institution zugreifen können. Oftmals fehlen auch Verlustmeldeprozesse, sodass z. B. ein gestohlener Laptop nicht zeitnah der richtigen Stelle in der Institution gemeldet wird. Dadurch kann sich der Angreifer möglicherweise lange unbemerkt im internen Netz aufhalten und zahlreiche schützenswerte Informationen stehlen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen für den Baustein NET.3.3 *VPN* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten

Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt

Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Informationssicherheitsbeauftragter (ISB)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein NET.3.3 *VPN* vorrangig umgesetzt werden:

NET.3.3.A1 Planung des VPN-Einsatzes (B)

Die Einführung eines VPN MUSS sorgfältig geplant werden. Dabei MÜSSEN die Verantwortlichkeiten für den VPN-Betrieb festgelegt werden. Es MÜSSEN für das VPN zudem Benutzergruppen und deren Berechtigungen geplant werden. Ebenso MUSS definiert werden, wie erteilte, geänderte oder entzogene Zugriffsberechtigungen zu dokumentieren sind.

NET.3.3.A2 Auswahl eines VPN-Dienstleisters [Informationssicherheitsbeauftragter (ISB)] (B)

Mit einem VPN-Dienstleister MÜSSEN Service Level Agreements (SLAs) ausgehandelt und schriftlich dokumentiert werden. Es MUSS regelmäßig kontrolliert werden, ob der VPN-Dienstleister die vereinbarten SLAs einhält.

NET.3.3.A3 Sichere Installation von VPN-Endgeräten (B)

Das zugrundeliegende Betriebssystem der VPN-Plattform MUSS sicher konfiguriert werden. Wird eine Appliance eingesetzt, MUSS es dafür einen gültigen Wartungsvertrag geben. Es MUSS sichergestellt werden, dass nur qualifiziertes Personal VPN-Komponenten installiert. Die Installation der VPN-Komponenten sowie eventuelle Abweichungen von den Planungsvorgaben SOLLTEN dokumentiert werden. Die Funktionalität und die gewählten Sicherheitsmechanismen des VPN MÜSSEN vor Inbetriebnahme geprüft werden.

NET.3.3.A4 Sichere Konfiguration eines VPN (B)

Für alle VPN-Komponenten MUSS eine sichere Konfiguration festgelegt werden. Diese SOLLTE geeignet dokumentiert werden. Auch MUSS der zuständige Administrator regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

NET.3.3.A5 Sperrung nicht mehr benötigter VPN-Zugänge (B)

Es MUSS regelmäßig geprüft werden, ob ausschließlich berechtigte IT-Systeme und Benutzer auf das VPN zugreifen können. Nicht mehr benötigte VPN-Zugänge MÜSSEN zeitnah deaktiviert werden. Der VPN-Zugriff MUSS auf die benötigten Benutzungszeiten beschränkt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein NET.3.3 *VPN*. Sie SOLLTEN grundsätzlich umgesetzt werden.

NET.3.3.A6 Durchführung einer VPN-Anforderungsanalyse (S)

Es SOLLTE eine Anforderungsanalyse durchgeführt werden, um für das jeweilige VPN die Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigten Hard- und Software-Komponenten ableiten zu können. In der Anforderungsanalyse SOLLTEN folgende Punkte betrachtet werden:

- Geschäftsprozesse beziehungsweise Fachaufgaben,
- Zugriffswege,

- Identifikations- und Authentisierungsverfahren,
- Benutzer und Benutzerberechtigungen,
- Zuständigkeiten und
- Meldewege.

NET.3.3.A7 Planung der technischen VPN-Realisierung (S)

Neben der allgemeinen Planung (siehe NET.3.3.A1 *Planung des VPN-Einsatzes*) SOLLTEN die technischen Aspekte eines VPN sorgfältig geplant werden. So SOLLTEN für das VPN die Verschlüsselungsverfahren, VPN-Endpunkte, erlaubten Zugangsprotokolle, Dienste und Ressourcen festgelegt werden. Zudem SOLLTEN die Teilnetze definiert werden, die über das VPN erreichbar sind (siehe NET.1.1 *Netzarchitektur und -design*).

NET.3.3.A8 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung (S)

Es SOLLTE eine Sicherheitsrichtlinie zur VPN-Nutzung erstellt werden. Diese SOLLTE allen Mitarbeitern bekannt gegeben werden. Die in der Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen SOLLTEN im Rahmen von Schulungen erläutert werden. Wird einem Mitarbeiter ein VPN-Zugang eingerichtet, SOLLTE ihm ein Merkblatt mit den wichtigsten VPN-Sicherheitsmechanismen ausgehändigt werden. Alle VPN-Benutzer SOLLTEN verpflichtet werden, die Sicherheitsrichtlinien einzuhalten.

NET.3.3.A9 Geeignete Auswahl von VPN-Produkten (S)

Bei der Auswahl von VPN-Produkten SOLLTEN die Anforderungen der Institutionen an die Vernetzung unterschiedlicher Standorte und die Anbindung mobiler Mitarbeiter oder Telearbeiter berücksichtigt werden.

NET.3.3.A10 Sicherer Betrieb eines VPN (S)

Für VPNs SOLLTE ein Betriebskonzept erstellt werden. Darin SOLLTEN die Aspekte Qualitätsmanagement, Überwachung, Wartung, Schulung und Autorisierung beachtet werden.

NET.3.3.A11 Sichere Anbindung eines externen Netzes (S)

Wird ein VPN benutzt, um ein externes Netz anzubinden, SOLLTEN dabei als sicher geltende Authentisierungs- und Verschlüsselungsverfahren mit ausreichender Schlüssellänge verwendet werden. Auch das gewählte Verfahren zum Schlüsselaustausch SOLLTE als sicher gelten. Es SOLLTE sichergestellt werden, dass VPN-Verbindungen NUR zwischen den dafür vorgesehenen IT-Systemen und Diensten aufgebaut werden. Die dabei eingesetzten Tunnel-Protokolle SOLLTEN für den Einsatz geeignet sein.

NET.3.3.A12 Benutzer- und Zugriffsverwaltung bei Fernzugriff-VPNs (S)

Für Fernzugriff-VPNs SOLLTE eine zentrale und konsistente Benutzer- und Zugriffsverwaltung gewährleistet werden. Die genutzten Authentisierungsverfahren SOLLTEN die Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* erfüllen.

Werden eigenständige Server für die Benutzer- und Zugriffsverwaltung eingesetzt, SOLLTE sichergestellt sein, dass diese sicher und konsistent zu den Anforderungen des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* eingerichtet und betrieben werden. Weiterhin SOLLTEN die eingesetzten Server vor unbefugten Zugriffen geschützt sein.

NET.3.3.A13 Integration von VPN-Komponenten in eine Firewall (S)

Die VPN-Komponenten SOLLTEN in die Firewall integriert werden. Es SOLLTE dokumentiert werden, wie die VPN-Komponenten in die Firewall integriert sind.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Für den Baustein NET.3.3 *VPN* sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI hat das weiterführende Dokument „Virtuelles Privates Netz (ISi-VPN): BSI-Leitlinie zur Internet Sicherheit (ISi-L)“ zum Themenfeld VPN veröffentlicht.

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27033-5:2013 „Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)“ Vorgaben für den Einsatz von VPNs.

Das National Institute of Standards and Technology (NIST) macht in seiner Special Publication 800-77 „Guide to IPsec VPNs“ generelle Vorgaben zum Einsatz von VPNs.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein NET.3.3 *VPN* von Bedeutung.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.32 Missbrauch von Berechtigungen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	CIA	G 0.11	G 0.14	G 0.18	G 0.19	G 0.22	G 0.23	G 0.28	G 0.32	G 0.40	G 0.43	G 0.46
NET.3.3.A1				X					X			
NET.3.3.A2		X										
NET.3.3.A3				X								
NET.3.3.A4			X		X	X	X		X			
NET.3.3.A5								X				
NET.3.3.A6				X			X		X			
NET.3.3.A7			X		X	X	X				X	X
NET.3.3.A8				X								
NET.3.3.A9		X								X		
NET.3.3.A10			X		X	X					X	X
NET.3.3.A11		X								X		
NET.3.3.A12									X			
NET.3.3.A13			X		X	X					X	X