Bundesamt
für Sicherheit in der
Informationstechnik

SYS.1.9 Terminalserver

1. Beschreibung

1.1. Einleitung

Ein Terminalserver ist ein Server, auf dem Client-Anwendungen (kurz Anwendungen) direkt ausgeführt werden und der nur deren grafische Oberfläche (Bedienoberfläche) an die Clients weiterleitet. Hierfür wird eine Terminalserver-Software verwendet. Der Terminalserver ist dann das zugrundeliegende IT-System, auf dem diese Software ausgeführt wird. Die Eingaben am Client, z. B. über Tastatur und Maus, werden an die Terminalserver-Software übertragen, die diese Eingaben dann dem Terminalserver übergibt. In der bereitgestellten Anwendung auf dem Terminalserver werden daraufhin die Aktionen ausgeführt, die gegebenenfalls durch die Eingaben ausgelöst werden und der Terminalserver ermittelt die neue (möglicherweise geänderte) Bedienoberfläche. Diese Bedienoberfläche wird dann von der Terminalserver-Software an den Client übertragen.

In einer Terminalserver-gestützten Umgebung verbinden sich typischerweise Clients mithilfe einer entsprechenden Terminal-Client-Software mit der Terminalserver-Software auf dem Terminalserver. Hierfür wird über Terminalserver-Protokolle kommuniziert, über die die Ein- und Ausgaben übertragen werden. Beispiele hierfür sind das Remote Desktop Protocol (RDP), Independent Computing Architecture (ICA), PC-over-IP (PCoIP) oder Virtual Network Computing (VNC).

Die Art der auf diese Weise bereitgestellten Anwendungen ist dabei prinzipiell nicht eingeschränkt und kann beispielsweise produktive Anwendungen wie Webbrowser, Office-Anwendungen oder Finanzsoftware, aber auch Administrationswerkzeuge wie SSH-Clients oder Management-Tools umfassen.

In einem typischen Einsatzszenario stellt ein Terminalserver mehreren Clients zentralisiert Anwendungen bereit, die aus organisatorischen oder technischen Gründen nicht lokal auf diesen Clients ausgeführt werden sollen oder können. Ein Beispiel hierfür sind Administrationstools, die nicht direkt auf den Clients der Administrierenden ausgeführt werden sollen. Ein weiteres Beispiel ist Software mit speziellen technischen Anforderungen an die zugrundeliegende Hardware der Clients, wie beispielsweise bestimmte Grafikkarten, die nicht auf allen Clients vorhanden sind.

In einer Terminalserver-gestützten Umgebung können die Clients sogenannte Fat Clients oder Thin Clients sein. Fat Clients sind mit einem vollwertigen Client-Betriebssystem ausgestattet. Thin Clients können dagegen nur genutzt werden, um sich mit dem Terminalserver zu verbinden und diesen zu bedienen.

Auf einem Terminalserver können mehrere Personen gleichzeitig auf demselben Betriebssystem arbeiten und dieselbe oder mehrere unterschiedliche Anwendungen parallel benutzen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die beim Einsatz von Terminalservern gespeichert, verarbeitet und übertragen werden. Hierzu werden spezielle Anforderungen an die beteiligten Anwendungen, IT-Systeme und Netze gestellt.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.9 *Terminalserver* ist sowohl auf den Terminalserver selbst als auch auf die zugreifenden Fat Clients und Thin Clients mit Terminal-Client-Software anzuwenden. Hierbei sind für Server und Clients jeweils sowohl die Soft- als auch die Hardwarekomponenten zu berücksichtigen.

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 die folgenden Inhalte:

- Ein Terminalserver im Sinne dieses Bausteins ist jedes IT-System, auf dem Anwendungen auf die oben beschriebene Weise zentral zur Verfügung gestellt werden. Hierbei muss die Verbindung vom Client aus direkt initiiert werden.
- Der Baustein SYS.1.9 *Terminalserver* ist anzuwenden, wenn durch eine Terminal-Client-Software ausschließlich Eingaben der Benutzenden an den Terminalserver übermittelt werden.
- Dieser Baustein beinhaltet spezifische Anforderungen an die verwendeten Netze, um die Kommunikation zwischen Clients und Terminalserver abzusichern.

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

- Für den Terminalserver und die Clients müssen die Bausteine SYS.1.1 *Allgemeiner Server* bzw. SYS.2.1 *Allgemeiner Client* sowie gegebenenfalls die spezifischen Bausteine für die Server- bzw. Client-Betriebssysteme angewendet werden.
- Auf die Terminalserver-Software müssen der Baustein APP.6 *Allgemeine Anwendung* sowie gegebenenfalls entsprechende weitere Bausteine der Schicht APP *Anwendungen* angewendet werden.
- Für die Anwendungen, die über den Terminalserver bereitgestellt werden, müssen zusätzlich der Baustein APP.6 *Allgemeine Anwendung* sowie gegebenenfalls die entsprechenden spezifischen Bausteine der Schicht APP *Anwendungen* angewendet werden.
- Der Baustein NET.1.1 *Netzarchitektur und -design* muss angewendet werden, um die für die Kommunikation zwischen Clients und Terminalserver verwendeten Netze abzusichern.

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

- Fernwartungswerkzeuge sind keine Terminalserver im Sinne dieses Bausteins. Um diese Werkzeuge abzusichern, ist der Baustein OPS.1.2.5 *Fernwartung* umzusetzen.
- Wenn ein zu administrierendes IT-System über Terminalserver-Protokolle angesprochen wird, stellt dies keine Nutzung des Terminalservers im Sinne dieses Bausteins dar.
- Dieser Baustein adressiert nicht den Fall, dass Clients direkt auf andere Clients über Terminalserver-Protokolle oder Kollaborationswerkzeuge zugreifen.
- Falls der Terminalserver-Dienst über zusätzliche Sicherheitskomponenten wie Application Delivery Controller (ADC, siehe Kapitel 4 *Weiterführende Informationen*) zur Verfügung gestellt wird, sind diese zusätzlichen Komponenten gesondert zu betrachten.

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 SYS.1.9 *Terminalserver* von besonderer Bedeutung.

2.1. Qualitätsverlust der Anwendungsbereitstellung

Eine vom Terminalserver bereitgestellte Anwendung wird in Echtzeit genutzt. Da die Bedienoberfläche auf dem Terminalserver vorbereitet und an die Clients übertragen wird, kann nur reibungslos gearbeitet werden, wenn die Antwort des Terminalservers auf eine Eingabe ohne merkliche Zeitverzögerung und klar erkennbar bei den Clients ankommt. Empfangen die Clients die Antworten des Terminalservers zeitlich verzögert, kann die Bedienbarkeit soweit einschränkt sein, dass dies einem Ausfall des Dienstes gleichkommt. Sowohl eine konstant hohe Verzögerung als auch häufig auftretende und nicht vorhersehbare Spitzen können diesen Effekt hervorrufen.

Eine zu hohe Verzögerung kann durch eine zu hohe Latenz der Übertragungsstrecken oder Netzkomponenten hervorgerufen werden. Wird die Kommunikation beispielsweise über weitere Sicherheitskomponenten wie VPN-Gateways abgesichert, die möglicherweise unzureichend dimensioniert sind, kann die Verzögerung weiter erhöht werden. Dies kann dazu führen, dass die Anwendung nur noch eingeschränkt genutzt werden kann.

Ist der Terminalserver stark ausgelastet, kann dieser nur verzögert antworten. Ist beispielsweise die CPU oder der Arbeitsspeicher unzureichend dimensioniert, kann der Terminalserver schnell überlasten und schließlich nur verzögert antworten. Ähnliches gilt, wenn der Terminalserver von zu vielen Personen zeitgleich genutzt wird.

Ist der Bildschirminhalt nicht klar genug erkennbar, kann mit dem Terminalserver nicht mehr effizient gearbeitet werden. Beispielsweise können Schrift oder Mauszeiger aufgrund von Kompressionsartefakten schwer zu erkennen sein, falls nicht genügend Leitungskapazität zur Verfügung steht.

All dies kann dazu führen, dass die Benutzenden entweder nicht oder nur noch stark eingeschränkt den Terminalserver nutzen können.

2.2. Ausfall der Anwendungsbereitstellung

In einer Terminalserver-gestützten Umgebung werden Anwendungen zentral ausgeführt und deren Ausgabe an die entsprechenden Clients übertragen. Ist der Terminalserver nicht verfügbar, können keine Eingaben mehr verarbeitet werden und die von dem Terminalserver bereitgestellten Anwendungen versagen unmittelbar ihren Dienst. Beziehen die Clients ihre gesamte Bedienoberfläche vom Terminalserver, fällt aus der Perspektive der Benutzenden das IT-System vollständig aus.

Wenn der Client ausfällt, kann hierüber nicht auf die vom Terminalserver bereitgestellten Anwendungen zugriffen werden, auch wenn diese dort verfügbar sind. Ähnliches gilt, wenn die Verbindung zwischen Client und Terminalserver gestört ist.

Von Ausfällen des Netzes oder des Terminalservers sind in der Regel nicht nur einzelne Clients betroffen. In vielen Fällen sind zahlreiche oder sogar alle Clients einer Institution auf den Terminalserver angewiesen. Fällt der Terminalserver aus, ist in diesem Fall eine große Anzahl von Clients gleichzeitig betroffen.

2.3. Unzureichende Netztrennung für Terminalserver

Auf Terminalservern werden meist Anwendungen bereitgestellt, die als Client fungieren. Hierdurch ähnelt ein Terminalserver von der Vertrauenswürdigkeit her eher einem Client als einem Server.

Wird dies bei der Netztrennung nicht geeignet berücksichtigt, kann unter Umständen über den Terminalserver unberechtigterweise auf weitere Serveranwendungen zugegriffen werden, beispielsweise über einen Webbrowser. Hierdurch kann der Terminalserver als Ausgangspunkt für Angriffe auf weitere IT-Systeme und Anwendungen missbraucht werden.

Durch die Eingaben am Client ist ein hoher Grad an Interaktion mit dem Terminalserver zu erwarten. Hierdurch können mögliche Schwachstellen leichter ausgenutzt werden. Dies ist insbesondere dann relevant, wenn ein Terminalserver Anwendungen für Benutzendengruppen bereitstellt, die unterschiedlichen Netzsegmenten zugeordnet sind. In diesem Fall könnte vom Terminalserver aus unautorisiert auf weitere Anwendungen in diesen Netzsegmenten zugegriffen werden.

2.4. Unzureichende Absicherung von Sitzungen auf dem Terminalserver

Terminalserver können unterschiedlichen Clients dedizierte Anwendungsinstanzen bereitstellen, die auf demselben Betriebssystem ausgeführt werden. Dabei teilen sich die Anwendungen unter anderem gemeinsam genutzte Bibliotheken, den Kernel und die benötigten Ressourcen des Terminalservers (z. B. CPU oder RAM).

Aufgrund von Fehlkonfigurationen oder Software-Schwachstellen können einzelne Anwendungsinstanzen gegebenenfalls miteinander kommunizieren, ohne dass dies ursprünglich vorgesehen war. Werden beispielsweise Sitzungen auf Terminalservern mit zu weitreichenden Berechtigungen ausgeführt, kann unter Umständen aus einer Anwendung heraus auf beliebige Teile des Dateisystems zugegriffen werden. Dies kann beispielsweise über Programmdialoge zum Speichern oder Öffnen von Dateien ausgenutzt werden, über die nicht vorgesehene Bereiche der Festplatte beschrieben oder gelesen werden.

Ein weiteres Beispiel ist das sogenannte RDP Session Hijacking, das auf den Sitzungen des Terminalservers selbst beruht. Bleiben Benutzende weiterhin angemeldet, nachdem ihre Sitzungen am Terminalserver beendet sind, kann dies zu Problemen führen. Sind Angreifende mit entsprechenden Rechten ausgestattet, die sie beispielsweise durch ein unzureichendes Rechtemanagement oder durch Ausnutzen von Software-Schwachstellen zuvor erhalten haben, können sie unter Umständen aus einer anderen Sitzung heraus eine bestehende Sitzung übernehmen. In diesem Fall können Angreifende die Sitzung im Kontext des oder der Benutzenden fortsetzen.

Wird das Betriebssystem von mehreren Anwendungen oder Anwendungsinstanzen gemeinsam genutzt, können gegebenenfalls Sitzungen anderer Benutzenden über CPU oder RAM beeinflusst werden. Hierfür müssen in den entsprechenden Anwendungen entsprechende Sicherheitslücken vorhanden sein, über die die benötigte Schadsoftware ausgeführt werden kann. Beispielsweise kann dann eine spezielle Schadsoftware Passwörter aus dem RAM auslesen. Auch ohne Sicherheitslücken in der Software können durch Sicherheitslücken in der Hardware (z. B. Meltdown) Angreifende beliebige schützenswerte Daten anderer Sitzungen auslesen.

2.5. Unzureichende Absicherung des Terminalserver-Protokolls

Viele Terminalserver-Protokolle bieten die Möglichkeit einer authentisierten und verschlüsselten Kommunikation. Diese Möglichkeit ist jedoch nicht immer ausreichend, um die Kommunikation abzusichern. Nutzt das Terminalserver-Protokoll veraltete und angreifbare Mechanismen oder werden durch Fehlkonfigurationen wichtige Sicherheitsfunktionen abgeschaltet, kann die Kommunikation zwischen Clients und Terminalserver abgehört werden. Informationen, die zwischen dem Terminalserver und den Clients übertragen werden und unter Umständen abgehört oder verändert werden, sind insbesondere:

- Authentisierungsinformationen und Eingaben von Benutzenden, die von den Clients zu den Terminalservern gesendet werden,
- Bildschirminformationen, die auf den Clients ausgegeben werden,

- Daten aus der Zwischenablage,
- Dateitransfers zwischen den lokalen Laufwerken des Clients und dem Server sowie
- Informationen von umgeleiteten Geräten des Clients (z. B. Audiogeräte, serielle- oder parallele Schnittstellen, USB-Geräte und Drucker).

Aber auch wenn die Protokollmechanismen die Kommunikation grundsätzlich stark genug absichern, kann die Implementierung des Protokolls innerhalb eines Terminalservers oder einer Terminal-Client-Software Schwachstellen beinhalten. Dies kann dazu führen, dass der Terminalserver direkt angreifbar wird, ohne dass die Kommunikation ausgespäht werden muss.

2.6. Unberechtigte Nutzung von Sammelkonten

Falls mehrere Personen eine Anwendung auf einem Terminalserver zu unterschiedlichen Zeiten nutzen wollen, werden oft Sammelkonten eingerichtet. Dies kann jedoch internen Regelungen oder den Lizenzbedingungen der über den Terminalserver bereitgestellten Software widersprechen.

Werden Sammelkonten verwendet, verhindert dies auch, dass die auf dem Terminalserver ausgeführten Aktionen konkreten Personen zugeordnet werden können. Hierdurch kann nicht mehr nachvollzogen werden, wer was getan hat. Dies kann insbesondere ein rechtliches Risiko bedeuten, wenn es gesetzliche Anforderungen an die Nachvollziehbarkeit gibt, z. B. falls auf dem Terminalserver personenbezogene Daten verarbeitet werden.

2.7. Ungeeignete Einschränkung der Zugriffsrechte der Benutzenden

Ein Terminalserver kann zeitgleich sowohl als Server und bezogen auf die auf ihm ausgeführten Anwendungen auch als Client fungieren. Dies kann zu Fehlern in der Vergabe der Zugriffsrechte führen.

Sichere Konfigurationen von IT-Systemen und Anwendungen sehen zumeist eine möglichst restriktive Rechtevergabe vor. Dies gilt insbesondere auch für Terminalserver. Werden die Berechtigungen für die Benutzung eines Terminalservers jedoch zu weit eingeschränkt, können die Benutzenden die bereitgestellten Anwendungen nur noch stark eingeschränkt nutzen. Dies kann sowohl aus einer zu strengen Richtlinie als auch aus einer Fehlkonfiguration resultieren.

Wird die Arbeit durch solche Einschränkungen zu sehr erschwert, indem beispielsweise der Schreibzugriff auf lokale Laufwerke komplett verboten wird, kann dies unerwünschte Auswirkungen haben. Beispielsweise könnten Benutzende auf nicht vorgesehene Workarounds ausweichen und Daten z. B. nach einem Export über Datenaustauschplattformen an ungeeigneter Stelle verarbeiten.

2.8. Ungeeignete Anwendungen für den Einsatz auf Terminalservern

Nicht alle Anwendungen lassen sich auf beliebigen Terminalservern bereitstellen. Werden beispielsweise notwendige Funktionen der Graphics Processing Unit (GPU) in der emulierten Grafikeinheit nicht unterstützt, können 3D-Anwendungen über einen Terminalserver nicht oder nur eingeschränkt genutzt werden. Ähnliches gilt, wenn Eingaben von anwendungs- oder branchenspezifischen Peripheriegeräten vom Terminalserver, der Terminal-Client-Software oder dem Terminalserver-Protokoll nicht unterstützt werden.

Werden einzelne Anwendungsfunktionen oder die Anbindung von Peripheriegeräten vor der Beschaffung nicht oder nur unzureichend getestet, werden diese Einschränkungen möglicherweise erst im laufenden Betrieb festgestellt. Dadurch kann die Verfügbarkeit der Anwendung erheblich eingeschränkt sein und der Terminalserver kann möglicherweise nicht wie vorgesehen eingesetzt werden. Gegebenenfalls muss er sogar komplett ersetzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.9 *Terminalserver* 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	Planende

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.

SYS.1.9.A1 Erstellung einer Sicherheitsrichtlinie für den Einsatz von Terminalservern (B)

Für den Einsatz von Terminalservern MUSS eine Sicherheitsrichtlinie erstellt werden. Bei der Erstellung der Sicherheitsrichtlinie MÜSSEN mindestens folgende Punkte berücksichtigt werden:

- Anwendungen, die auf Terminalservern bereitgestellt werden dürfen,
- Anwendungen, die gemeinsam auf Terminalservern bereitgestellt werden dürfen,
- Anforderungen an die Sicherheit von Clients, auf denen die Terminal-Client-Software ausgeführt wird,
- physisches Umfeld, in dem die Clients eingesetzt werden dürfen,
- Netze, aus denen heraus Kommunikationsverbindungen zu den Terminalservern initiiert werden dürfen,
- Netze, in die Anwendungen auf den Terminalservern kommunizieren dürfen,
- Kommunikationsprotokolle, die zwischen Clients und Terminalservern erlaubt sind,
- Verschlüsselungsmechanismen und Authentisierungsmethoden, die zwischen Clients und Terminalservern zu benutzen sind,
- Möglichkeiten, wie Dateien und Anwendungsdaten zusätzlich zur Bildschirmausgabe über das Terminalserver-Protokoll übertragen werden dürfen sowie
- Peripheriegeräte, die neben Ein- und Ausgabegeräten zusätzlich an den Client angebunden werden dürfen.

SYS.1.9.A2 Planung des Einsatzes von Terminalservern (B)

Für die Anwendungen, die auf einem Terminalserver bereitgestellt werden sollen, MÜSSEN die Anforderungen an die Funktionalität (Anforderungsprofil) ermittelt werden. Für alle benötigten Funktionen MUSS sichergestellt werden, dass diese tatsächlich auch über den Terminalserver abgerufen werden können. Darüber hinaus MUSS getestet werden, ob die Anwendungen die Anforderungen bei der Bereitstellung über den Terminalserver grundlegend erfüllen.

Die Gesamtzahl der einzurichtenden Benutzenden MUSS prognostiziert werden. Dabei MÜSSEN alle Anwendungen mitgezählt werden, die auf dem Terminalserver bereitgestellt werden.

Die Anzahl der Benutzenden, die den Terminalserver potenziell gleichzeitig benutzen, MUSS prognostiziert werden. Diese Prognosen MÜSSEN den Einsatzzeitraum des Terminalservers abdecken.

Abhängig von der prognostizierten Anzahl der Benutzenden und den Anforderungen der bereitgestellten Anwendungen MÜSSEN die Leistungsanforderungen (z. B. hinsichtlich CPU und Arbeitsspeicher) an den Terminalserver ermittelt werden. Der Terminalserver MUSS anhand dieser Leistungsanforderungen dimensioniert und ausgestattet werden.

Das Lizenzschema der eingesetzten Anwendungen MUSS daraufhin geprüft werden, ob es dafür geeignet ist, diese Anwendungen auf Terminalservern einzusetzen.

SYS.1.9.A3 Festlegung der Rollen und Berechtigungen für den Terminalserver (B)

Auf Terminalservern DÜRFEN KEINE Sammelkonten verwendet werden, wenn dies gegen interne Regelungen oder Lizenzbedingungen verstößt. Bei der Festlegung von Rollen und Berechtigungen für die Benutzung des Terminalservers MÜSSEN alle auf dem Terminalserver bereitgestellten Anwendungen und deren Anforderungen mit ausreichenden Berechtigungen ausgestattet werden.

Die Rollen und Berechtigungen MÜSSEN so vergeben werden, dass zwischen Terminalserver-Sitzungen nur in dem Umfang kommuniziert werden kann, wie es für die Funktionalität der Anwendung erforderlich ist. Mindestens MÜSSEN die Berechtigungen für folgende Tätigkeiten festgelegt werden:

- Ausführen von Anwendungen in fremdem Kontext (insbesondere als „root“),
- Zugriff auf betriebssystemspezifische Funktionen,
- Zugriff auf das Dateisystem des Terminalservers,
- Zugriff auf Schnittstellen und Dateisystem des verwendeten zugreifenden Clients,
- Zugriff der auf dem Terminalserver bereitgestellten Anwendungen auf nachgelagerte Dienste,
- Datei- und Objekttransfer zwischen Clients und Terminalservern (z. B. zum Drucken am Client) sowie
- Anbindung von Peripheriegeräten am Client.

SYS.1.9.A4 Sichere Konfiguration des Terminalservers (B)

Abhängig von den Anforderungen an die Sicherheit und Funktionalität der bereitgestellten Anwendungen MÜSSEN Vorgaben für die Konfiguration von Terminalservern erstellt werden. Diese Vorgaben MÜSSEN vollständig umgesetzt und dokumentiert werden.

Es MUSS geprüft werden, ob das Unternehmen, das den Terminalserver herstellt, Vorgaben oder Empfehlungen zur sicheren Konfiguration oder Härtung bereitstellt. Ist dies der Fall, MÜSSEN diese für die Erstellung der Konfigurationsvorgaben angemessen berücksichtigt werden. Sowohl die Konfigurationsvorgaben als auch deren Umsetzung MÜSSEN regelmäßig geprüft und gegebenenfalls angepasst werden.

Es MÜSSEN mindestens folgende Punkte für die Konfigurationsvorgaben berücksichtigt werden:

- Rollen und Berechtigungen
- Umfang der Verschlüsselung des Terminalserver-Protokolls
- benötigte Authentisierungsfunktionen des Terminalserver-Protokolls
- Möglichkeit zum Anzeigen der Ausgabe fremder Sitzungen

- Kommunikation zwischen Anwendungen in den Terminalserver-Sitzungen und Anwendungen auf anderen Servern
- Kommunikation zwischen Terminalserver und anderen Servern

SYS.1.9.A5 Planung der eingesetzten Clients und Terminal-Client-Software (B)

Es MUSS festgelegt werden, über welche Terminal-Client-Software auf den Terminalserver zugegriffen werden darf. Zusätzlich MUSS festgelegt werden, auf welchen Clients diese Software ausgeführt werden darf, um sich mit dem Terminalserver zu verbinden. Hierbei MÜSSEN mindestens die folgenden Punkte berücksichtigt werden:

- Einsatz von Thin Clients oder Fat Clients,
- Hardware-Konfiguration der zugreifenden Clients sowie
- Betriebssystem der zugreifenden Clients.

Es MUSS festgelegt werden, welche Software neben der Terminal-Client-Software zusätzlich auf den Clients zugelassen ist. Zusätzlich MUSS festgelegt werden, ob ein Client parallel Anwendungen auf unterschiedlichen Terminalservern benutzen darf.

SYS.1.9.A6 Planung der verwendeten Netze (B) [Planende]

Die Netze, über die Clients mit Terminalservern kommunizieren, MÜSSEN anhand der Anforderungen der bereitgestellten Anwendungen geplant und gegebenenfalls angepasst werden. Hierbei MÜSSEN mindestens folgende Punkte berücksichtigt werden:

- zu erwartende Anzahl gleichzeitiger Terminalserver-Sitzungen,
- benötigte Übertragungskapazität,
- maximal vertretbarer Paketverlust,
- maximal vertretbarer Jitter sowie
- maximal tolerierbare Latenzzeit des Netzes.

SYS.1.9.A7 Sicherer Zugriff auf den Terminalserver (B)

Es MUSS festgelegt werden, über welche Netze zwischen zugreifendem Client und Terminalserver kommuniziert werden darf. Zusätzlich MUSS festgelegt werden, wie die Kommunikation abgesichert werden soll. Es MUSS festgelegt werden, ob und wie mit dem Terminalserver-Protokoll verschlüsselt werden soll. Falls das Terminalserver-Protokoll in diesem Fall keine ausreichende Verschlüsselung bietet, MUSS die Kommunikation zusätzlich abgesichert werden.

Falls die Clients und der Terminalserver über unzureichend vertrauenswürdige Netze kommunizieren, MÜSSEN sich sowohl die Benutzenden als auch der Terminalserver beim Kommunikationsaufbau authentisieren.

SYS.1.9.A8 Sichere Zuordnung des Terminalservers zu Netzsegmenten (B)

Der Terminalserver MUSS in dedizierten Netzsegmenten oder in Client-Netzsegmenten positioniert werden. Innerhalb von Client-Netzsegmenten MÜSSEN Terminalserver identifizierbar sein.

Eine bestehende Netztrennung DARF NICHT über einen Terminalserver umgangen werden können.

SYS.1.9.A9 Sensibilisierung der Benutzenden (B)

Alle Benutzenden von Terminalservern MÜSSEN über den sicheren Umgang mit Terminalservern sensibilisiert werden. Den Benutzenden MÜSSEN mindestens die folgenden Inhalte vermittelt werden:

- grundsätzliche Funktionsweise und die Auswirkungen von Latenz und verfügbarer Bandbreite auf die Bedienbarkeit
- mögliche und erlaubte Speicherorte von Daten

- zugelassene Austauschmöglichkeiten von Informationen zwischen dem Betriebssystem des Clients und dem Terminalserver (z. B. Zwischenablage)
- Auswirkung des eigenen Ressourcenverbrauchs auf die zur Verfügung stehenden Ressourcen für andere Benutzende
- eingerichtete Rollen und Berechtigungen für Terminalserver-Zugriffe
- genutzte Authentisierung und Autorisierung der Benutzenden für die zur Verfügung gestellten Anwendungen
- maximale Sitzungsdauer und automatische Abmeldevorgänge

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.

SYS.1.9.A10 Einsatz eines zentralen Identitäts- und Berechtigungsmanagements für Terminalserver (S)

Für die Benutzung von Terminalservern SOLLTE ein zentrales System zum Identitäts- und Berechtigungsmanagement eingesetzt werden.

SYS.1.9.A11 Sichere Konfiguration von Profilen (S)

Benutzende SOLLTEN ihre spezifischen Einstellungen (Benutzendenprofile) NICHT derart ändern dürfen, dass die Informationssicherheit oder die Nutzung des Terminalservers eingeschränkt wird. Für die Benutzendenprofile SOLLTE eine geeignete maximale Größe festgelegt werden. Wenn Verbünde aus Terminalservern eingesetzt werden, SOLLTEN die Benutzendenprofile zentral abgelegt werden.

SYS.1.9.A12 Automatisches Beenden inaktiver Sitzungen (S)

Inaktive Sitzungen auf Terminalservern SOLLTEN nach einem vordefinierten Zeitraum beendet werden. Der Zeitraum, während dessen eine Sitzung maximal aktiv bleiben soll, SOLLTE abhängig von der jeweiligen Benutzendengruppe festgelegt werden. Falls eine Sitzung automatisch beendet wird, SOLLTEN die Betroffenen darüber benachrichtigt werden. Wenn eine Sitzung beendet wird, SOLLTE auch der oder die Benutzende automatisch vom Betriebssystem des Terminalservers abgemeldet werden, sofern die Sitzung am Betriebssystem nicht weiterhin für laufende Anwendungen benötigt wird.

SYS.1.9.A13 Protokollierung bei Terminalservern (S)

Für die Terminalserver SOLLTE entschieden werden, welche Ereignisse an eine zentrale Protokollierungsinfrastruktur (siehe OPS.1.1.5 *Protokollierung)* übermittelt werden sollen. Hierbei SOLLTEN mindestens die folgenden spezifischen Ereignisse an Terminalservern protokolliert werden:

- Anbindung von Peripheriegeräten der zugreifenden Clients über das Terminalserver-Protokoll,
- Aktionen auf dem Terminalserver durch zugreifende Clients, die erweiterte Rechte benötigen sowie
- Konfigurationsänderungen mit Auswirkungen auf den Terminalserver-Dienst.

SYS.1.9.A14 Monitoring des Terminalservers (S)

Der Terminalserver SOLLTE zentral überwacht werden. Hierfür SOLLTEN mindestens folgende Parameter überwacht werden:

- Auslastung der Ressourcen des Terminalservers,
- Auslastung der Netzschnittstellen des Terminalservers,

- verfügbare und genutzte Bandbreite der verbundenen Clients sowie
- Latenz an den verbundenen Clients unter Berücksichtigung der jeweiligen Anforderungsprofile.

Für das Monitoring SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining). Diese Schwellwerte SOLLTEN regelmäßig überprüft und bei Bedarf angepasst werden.

SYS.1.9.A15 Härtung des Terminalservers (S)

Nicht benötigte Anwendungen auf dem Terminalserver SOLLTEN entfernt werden. Ist das nicht möglich, SOLLTE deren Ausführung unterbunden werden.

Der Zugriff aus einer Sitzung auf Peripheriegeräte SOLLTE auf die benötigten Geräte eingeschränkt werden.

SYS.1.9.A16 Optimierung der Kompression (S)

Der Grad der Kompression bei der Übertragung der Daten von und zum Terminalserver SOLLTE entsprechend der Anforderungen der jeweiligen Anwendung an die grafische Qualität optimiert werden. Die Anforderungen der bereitgestellten Anwendungen an Genauigkeit von grafischen Elementen, an Farbtreue und die für die Nutzung notwendige Bildrate SOLLTEN berücksichtigt werden.

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.

SYS.1.9.A17 Verschlüsselung der Übertragung (H)

Jegliche Kommunikation zwischen Client und Terminalserver SOLLTE geeignet verschlüsselt werden. Dabei SOLLTEN sichere Protokolle gemäß BSI TR-02102 verwendet werden.

SYS.1.9.A18 Nutzung von Thin Clients (H)

Physische Thin Clients SOLLTEN verwendet werden. Es SOLLTEN NUR Thin Clients eingesetzt werden, die das Unternehmen, das die Terminal-Client-Software herstellt, als kompatibel ausgewiesen hat.

SYS.1.9.A19 Erweitertes Monitoring des Terminalservers (H)

Für den Terminalserver SOLLTE kontinuierlich überwacht werden, ob die in SYS.1.9.A13 *Protokollierung bei Terminalservern* beschriebenen Ereignisse auftreten.

Wird ein Security Information and Event Management (SIEM) genutzt, SOLLTE der Terminalserver darin eingebunden werden. Im SIEM SOLLTEN die überwachten Ereignisse hinsichtlich Anomalien inklusive Angriffsmustern automatisiert analysiert werden.

Der Terminalserver SOLLTE regelmäßig auf Schwachstellen überprüft werden.

SYS.1.9.A20 Unterschiedliche Terminalserver für unterschiedliche Gruppen von Benutzenden oder Geschäftsprozesse (H)

Die Benutzenden von Terminalservern SOLLTEN anhand ähnlicher Berechtigungen und benötigter Anwendungen gruppiert werden. Ein Terminalserver SOLLTE NICHT mehreren Gruppen von Benutzenden zur Verfügung gestellt werden. Ist dies nicht möglich, SOLLTEN dedizierte Terminalserver pro Geschäftsprozess eingesetzt werden.

SYS.1.9.A21 Nutzung hochverfügbarer IT-Systeme (H)

Der Terminalserver SOLLTE hochverfügbar betrieben werden. Dazu SOLLTEN der Terminalserver sowie dessen Netzanbindung redundant ausgelegt werden. Die verwendeten Terminalserver SOLLTEN im Verbund betrieben werden. Für die zugreifenden Clients SOLLTEN Ersatzgeräte bereitgehalten werden.

SYS.1.9.A22 Unterbinden des Transfers von Anwendungsdaten zwischen Client und Terminalserver (H)

Der Transfer von Anwendungsdaten zwischen dem Client und dem Terminalserver SOLLTE deaktiviert werden. Auch der Transfer der Zwischenablage SOLLTE deaktiviert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102“ Hinweise zur Anwendung kryptografischer Verfahren zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Empfehlungen für den sicheren Einsatz von Application Delivery Controllern (ADC)“ Hinweise für den sicheren Einsatz von ADC zur Verfügung.