Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.6 Virtual Desktop Infrastructure

1. Beschreibung

1.1. Einleitung

Eine Virtual Desktop Infrastructure (VDI) steuert und verwaltet standardisierte virtuelle Clients. Hierdurch können zentralisiert einzelne Anwendungen (z. B. Office-Programme) oder ganze Desktops zur Verfügung gestellt werden. Virtuelle Clients sind dabei virtualisierte IT-Systeme, auf die über Terminalserver-Protokolle zugegriffen werden kann. Die virtuellen Clients werden auf Virtualisierungsservern ausgeführt, die mit einem Managementsystem zu einer Virtualisierungsinfrastruktur zusammengefasst werden (siehe Bausteine SYS.1.5 *Virtualisierung* und SYS.2.5 *Client-Virtualisierung*).

Je nachdem, welches Produkt eingesetzt wird, besteht eine VDI typischerweise aus Zugangs-, Steuerungs- und Managementkomponenten, die auf einem oder auf mehreren IT-Systemen verteilt betrieben werden. Diese zentralen VDI-Komponenten verwalten unter anderem die Virtualisierungsinfrastruktur und stellen die Verbindungen zwischen zugreifenden und virtuellen Clients her. Daher sind die Virtualisierungsinfrastruktur, die angebundenen Storage-Systeme sowie die virtuellen und zugreifenden Clients ebenfalls impliziter Teil der VDI. In diesem Baustein sind jedoch mit „VDI-Komponenten“ immer die folgenden drei zentralen Komponenten einer VDI gemeint:

- Die VDI-Zugangskomponenten authentisieren die Benutzenden und entscheiden anhand ihrer Berechtigungen, ob Zugriffe erlaubt oder nicht erlaubt sowie für welchen Typ von virtuellem Client die Benutzenden autorisiert sind.
- Die VDI-Steuerungskomponenten wählen für die erlaubten Zugänge die entsprechenden virtuellen Clients aus und stellen die Verbindung zwischen zugreifendem und virtuellem Client her.
- Die VDI-Managementkomponenten verwalten die Regeln (z. B. die Zuordnung von Benutzenden zu Clienttypen) und Einstellungen (z. B. die zu nutzenden Protokolle). Außerdem verwalten sie die virtuellen Clients (gemäß SYS.2.5 *Client-Virtualisierung*). Dies umfasst auch die zugewiesenen Ressourcen und deren Provisionierung sowie die Terminalserver-spezifischen Einstellungen der virtuellen Clients.

Außerdem kann es zusätzlich erforderlich sein, dass weitere Infrastrukturdienste angebunden werden, die nicht zur VDI-Lösung selbst gehören (z. B. Verzeichnisdienste, Namensauflösung oder IP-Adress-Management).

VDIs werden in der Regel eingesetzt, um zentral administrierbare standardisierte Arbeitsplätze effizient zur Verfügung zu stellen. Dies wird beispielsweise genutzt, um klassische physische Clients durch Thin Clients zu ersetzen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die beim Einsatz einer VDI gespeichert, verarbeitet und übertragen werden. Hierzu werden spezielle Anforderungen an die in der Einleitung beschriebenen Komponenten einer VDI gestellt.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.6 *Virtual Desktop Infrastructure* ist auf jedes IT-System anzuwenden, das als Teil einer VDI-Lösung eingesetzt wird.

Dieser Baustein behandelt die folgenden Inhalte:

Der Baustein SYS.2.6 *Virtual Desktop Infrastructure* behandelt den sicheren Einsatz einer VDI. Dabei wird der Fokus auf die drei zentralen Komponenten einer VDI gelegt.

Dieser Baustein beinhaltet spezifische Anforderungen an die verwendeten Netze, um die Kommunikation zwischen zugreifendem Client und Virtualisierungsinfrastruktur abzusichern.

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

- Die grundlegende Funktionalität der Kommunikation zwischen einem zugreifenden und einem virtuellen Client in einer VDI-Lösung wird mithilfe von Terminalserver-Techniken erfüllt. Daher ist der Baustein SYS.1.9 *Terminalserver* ebenfalls auf die VDI-Lösung anzuwenden, wobei die einzelnen virtuellen Clients die eigentlichen Terminalserver sind.
- Ebenfalls sind die Bausteine SYS.2.5 *Client-Virtualisierung* und SYS.1.5 *Virtualisierung* für die einzelnen virtuellen Clients bzw. die Virtualisierungsinfrastruktur anzuwenden, speziell für die Isolation der virtuellen Clients über den Virtualisierungsserver.
- Grundsätzliche Anforderungen an die einzelnen Server-Komponenten sowie die zugreifenden und virtuellen Clients sind dem Baustein SYS.1.1 *Allgemeiner Server* bzw. SYS.2.1 *Allgemeiner Client* zu entnehmen. Außerdem sind gegebenenfalls betriebssystemspezifische Bausteine anzuwenden.
- Der Baustein NET.1.1 *Netzarchitektur und -design* muss angewendet werden, um die Netze abzusichern, die für die VDI genutzt werden.

Dieser Baustein behandelt **nicht**

- diejenigen IT-Systeme, die im Kontext der VDI zusätzlich zu den oben beschriebenen VDI-Komponenten verwendet werden (z. B. Storage Systeme) sowie
- die Techniken, die bei der Virtualisierung oder für die Kommunikation zwischen zugreifenden und virtuellen Clients eingesetzt werden.

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.2.6 *Virtual Desktop Infrastructure* von besonderer Bedeutung.

2.1. Qualitätsverlust der Bereitstellung virtueller Clients

Eine VDI wird in vielen Fällen dazu eingesetzt, um Ressourcen zu optimieren. Werden jedoch viele virtuelle Clients auf einzelnen Virtualisierungsservern platziert, können die verfügbaren Ressourcen überbucht werden. Auch wenn die geplante Anzahl der Benutzenden unzutreffend eingeschätzt wurde, können die Ressourcen überbucht werden.

Hierdurch können virtuelle Clients in der VDI stark um Ressourcen konkurrieren und die Leistung kann unvorhersehbar einbrechen. Das kann dazu führen, dass die virtuellen Clients temporär nicht mehr verfügbar sind.

Die Leistungseinbrüche sind für die Benutzenden meist intransparent, so dass Daten verloren gehen oder ungewollt geändert werden.

2.2. Falsche Zuweisung von virtuellen Clients zu Benutzenden

Den Benutzenden werden virtuelle Clients und deren Ressourcen anhand von Profilen von der VDI zentralisiert zugewiesen. Sollte eine solche Zuweisung fehlerhaft sein, können hierdurch

- hohe Kosten entstehen, wenn leistungsstarke virtuelle Clients an Benutzende ohne großen Ressourcenbedarf zugewiesen werden,
- virtuelle Clients mit geringer Leistung an Benutzende mit hohem Ressourcenbedarf oder besonderen Hardwareanforderungen, z. B. für CAD-Aufgaben, zugewiesen werden,
- Benutzende auf IT-Systeme und Informationen unberechtigt zugreifen oder
- externe USB-Geräte angebunden und Informationen an nicht dafür vorgesehene virtuelle Clients übertragen werden.

2.3. Unzureichende Netztrennung durch Fehlkonfiguration in der VDI

Typischerweise werden in einer VDI-Lösung unterschiedliche virtuelle Clients betrieben, die sich stark in ihren Anwendungsbereichen unterscheiden und entsprechend auch unterschiedlichen Netzen zugeordnet sein können. Die VDI-Managementkomponente verwaltet alle diese Clients. Ist die VDI-Managementkomponente fehlerhaft konfiguriert, kann eine notwendige Netztrennung aufgehoben werden. Unter Umständen können hierdurch virtuelle Clients unerlaubt miteinander kommunizieren.

Diese Situation ergibt sich beispielsweise, wenn die virtuellen Clients den Benutzenden auf Basis von Eigenschaften wie Gruppenzugehörigkeiten zugewiesen und falsch zugeordnet werden. In diesem Fall kann eine Netztrennung umgangen werden, die eigentlich zwischen Clients verschiedener Gruppen bestehen sollte.

2.4. Verlust von virtuellen Clients durch Fehlkonfiguration in der VDI

Eine Stärke von VDI ist es, dass viele verschiedene virtuelle Clients über wenige Vorlagen (Templates) einfach verwaltet werden können. Damit können neue Desktops schnell provisioniert sowie fehlerhafte Desktops repariert oder ausgetauscht werden.

Durch diese zentralisierte Verwaltung können aber durch gelöschte oder korrumpierte Templates virtuelle Clients verloren gehen. Werden bestimmte Daten von Benutzenden ausschließlich auf dem Speicher der virtuellen Clients abgelegt, führt der Verlust eines virtuellen Clients auch zu einem Verlust dieser Daten.

Auch von den Benutzenden geänderte Konfigurationen werden unwiederbringlich gelöscht, wenn der virtuelle Client zurückgesetzt wird.

2.5. Ausfall von VDI-Komponenten

Eine VDI besteht typischerweise aus mehreren Komponenten, die voneinander abhängen. Fällt auch nur eine dieser Komponenten aus, beispielsweise aufgrund von Hard- oder Software-Fehlern oder aufgrund von Fehlkonfigurationen, kann dies die Verfügbarkeit der gesamten VDI-Lösung und damit die Arbeitsfähigkeit der Benutzenden beeinträchtigen.

Ein Ausfall einer oder mehrerer Komponenten kann sehr unterschiedliche Auswirkungen haben. Beispielsweise ist beim Ausfall der VDI-Managementkomponente prinzipiell ein normaler Arbeitsbetrieb möglich, aber es können keine Anpassungen vorgenommen werden. Dies kann unter anderem dazu führen, dass

- neue virtuelle Clients nicht bereitgestellt werden können,
- virtuelle Clients nach Fehlern nicht in einen funktionsfähigen Basiszustand zurückgesetzt werden können,
- das Troubleshooting erschwert wird, da die gesammelten Informationen der Managementfunktionen nicht verfügbar sind oder
- die Ressourcen eines virtuellen Clients nicht angepasst werden können, falls diese für Einzelne nicht ausreichen.

Die Zugangs- oder Steuerungskomponenten mancher VDI-Produkte bieten ohne die Managementkomponente nicht ihren vollen Funktionsumfang.

2.6. Unberechtigter Zugriff auf virtuelle Clients

Eine VDI-Managementkomponente verwaltet alle zugehörigen Clients. Wird die VDI-Managementkomponente kompromittiert (beispielsweise aufgrund ausgenutzter Schwachstellen oder Fehlkonfiguration), kann von dort aus auf die virtuellen Clients zugegriffen werden. In diesem Fall können Verfügbarkeit, Vertraulichkeit oder Integrität der virtuellen Clients beeinträchtigt werden.

Einige VDI-Lösungen bringen eine Agentensoftware mit sich, die innerhalb der virtuellen Clients genutzt und für bestimmte VDI-Funktionen (z. B. Verbindungsaufbau, 3D-Beschleunigung, Optimierung des Speicherverbrauchs) benötigt wird. Wirkt sich eine Fehlkonfiguration auf diese Agentensoftware aus, können die virtuellen Clients gefährdet sein.

Die Agentensoftware und die Managementkomponente der VDI steuern je nach Größe der Umgebung viele Clients. In diesen Fällen kann auf viele verschiedene virtuelle Clients zugegriffen werden.

2.7. Nutzung von Templates mit Software-Schwachstellen

In einer VDI können schnell und zentralisiert virtuelle Clients aus einer definierten Menge von Templates erzeugt werden. Wenn diese Templates erzeugt werden, sind sie in der Regel auf einem aktuellen Software-Stand ohne bekannte Schwachstellen.

Ohne eine regelmäßige Aktualisierung dieser Templates ist es jedoch möglich, dass ein neu erzeugter virtueller Client Schwachstellen aufweist, die bekannt wurden, nachdem das Template erzeugt wurde. Können andere IT-Systeme auf diesen virtuellen Client zugreifen, kann die bekannte Schwachstelle ausgenutzt werden und somit der virtuelle Client kompromittiert werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.6 *Virtual Desktop Infrastructure* 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.2.6.A1 Planung des Einsatzes einer VDI (B)

Die Leistungsanforderungen und Anzahl der benötigten virtuellen Clients sowie die daraus resultierenden Anforderungen an die Dimensionierung der VDI MÜSSEN identifiziert werden. Die VDI-Komponenten MÜSSEN anhand dieser Dimensionierungsanforderungen bedarfsgerecht geplant werden. Die VDI-Komponenten und die genutzte Virtualisierungsinfrastruktur MÜSSEN aufeinander abgestimmt geplant werden.

Bei der Dimensionierung der VDI MUSS berücksichtigt werden, ob und wie sich die Anforderungen hieran über den geplanten Einsatzzeitraum der VDI-Lösung ändern. Der Support MUSS für den gesamten geplanten Einsatzzeitraum der VDI-Lösung bei der Planung mitberücksichtig werden.

Die Anzahl virtueller Clients und deren benötigte Leistung pro Virtualisierungsserver MUSS festgelegt werden.

SYS.2.6.A2 Sichere Installation und Konfiguration der VDI-Komponenten (B)

Wenn die VDI-Komponenten installiert und konfiguriert werden, MUSS mindestens berücksichtigt werden, wie:

- auf betrieblich und technisch notwendige Funktionen beschränkt wird,
- die Kommunikation zwischen VDI-Komponenten abgesichert wird sowie
- virtuelle Clients sicher den Benutzenden oder Gruppen hiervon zugewiesen werden.

Empfehlungen von dem herstellenden Unternehmen der VDI-Lösung für die sichere Konfiguration MÜSSEN berücksichtigt werden.

Die Konfigurationen der VDI-Komponenten MÜSSEN geeignet dokumentiert werden.

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.2.6.A3 Sichere Installation und Konfiguration der virtuellen Clients mithilfe der VDI (S)

Die VDI-Lösung SOLLTE genutzt werden, um die virtuellen Clients zu installieren und zu konfigurieren. Virtuelle Clients SOLLTEN NICHT manuell in die VDI-Lösung integriert werden. In der für die VDI verwendeten Virtualisierungsinfrastruktur SOLLTEN virtuelle Clients NICHT unabhängig von der VDI erzeugt werden.

SYS.2.6.A4 Netzsegmentierung der VDI-Komponenten (S) [Planende]

Die VDI-Komponenten inklusive der virtuellen Clients SOLLTEN bei der Netzsegmentierung gesondert berücksichtigt werden. Netze SOLLTEN dabei mindestens mit Hilfe der Virtualisierungsinfrastruktur getrennt werden. Dedizierte Netzsegmente SOLLTEN mindestens für das Administrationsnetz der VDI-Komponenten und für die Netze der internen Kommunikation zwischen VDI-Komponenten eingerichtet werden.

SYS.2.6.A5 Standardisierter Zugriff auf virtuelle Clients (S)

Die Mechanismen und Dienste der VDI-Lösung SOLLTEN genutzt werden, um die Zugriffe auf die virtuellen Clients zu steuern und abzusichern. Falls eine zusätzliche Software für diese Zugriffe auf den zugreifenden Clients eingesetzt wird, SOLLTE diese Software standardisiert und zentralisiert bereitgestellt werden.

SYS.2.6.A6 Verwendung einer dedizierten Infrastruktur für virtuelle VDI-Komponenten (S)

Falls die VDI-Komponenten virtualisiert betrieben werden, SOLLTEN sie auf einer dedizierten Virtualisierungsinfrastruktur betrieben werden.

SYS.2.6.A7 Härtung der virtualisierten Clients durch die VDI-Lösung (S)

Die Möglichkeiten der VDI-Lösung SOLLTEN für die Härtung der virtuellen Clients entsprechend den Anforderungen des Bausteins SYS.2.5 *Client-Virtualisierung* genutzt werden. Die Betriebssysteme der Clients SOLLTEN ausschließlich über die Managementkomponente der VDI-Lösung konfiguriert werden. Eine individuelle Konfiguration bestehender virtueller Clients über die Virtualisierungsinfrastruktur SOLLTE mit technischen Mitteln unterbunden werden.

SYS.2.6.A8 Härtung der VDI-Lösung (S)

Eine automatische Anmeldung an der VDI SOLLTE nicht möglich sein. Die Authentisierung SOLLTE nur erfolgen, nachdem die Benutzenden mit der VDI interagiert haben.

SYS.2.6.A9 Einbindung der virtuellen Clients in das Patch- und Änderungsmanagement (S)

Die virtuellen Clients SOLLTEN, wenn möglich, zentral über die Managementkomponenten der VDI-Lösung verwaltet werden. Die virtuellen Clients SOLLTEN auch im ausgeschalteten Zustand gepatcht werden, falls dies von der VDI-Lösung unterstützt wird. Die Templates, aus denen virtuelle Clients erzeugt werden, SOLLTEN regelmäßig aktualisiert werden.

SYS.2.6.A10 Monitoring von Verfügbarkeit und Nutzungsgrad der VDI (S)

Der Zustand der VDI-Komponenten SOLLTE zentral überwacht werden. Es SOLLTEN mindestens folgende Parameter für jede VDI-Komponente überwacht werden:

- Erreichbarkeit der benötigten Netzschnittstellen
- Verfügbarkeit der von der VDI-Komponente bereitgestellten Dienste
- Auslastung der CPU und des Arbeitsspeichers

SYS.2.6.A11 Monitoring von sicherheitsrelevanten Ereignissen der VDI (S)

Für die VDI-Komponenten SOLLTEN mindestens die folgenden Ereignisse an ein zentrales Monitoring weitergeleitet werden:

- erfolgreiche und fehlgeschlagene Anmeldeversuche
- Konfigurationsänderungen an VDI-Komponenten oder virtuellen Clients
- erfolgreiche und fehlgeschlagene Updates an VDI-Komponenten
- fehlgeschlagene Updates an virtuellen Clients

Die VDI-Komponenten SOLLTEN regelmäßig auf Schwachstellen überprüft werden.

SYS.2.6.A12 Verteilung von virtuellen Clients auf Virtualisierungsservern (S)

Pro Virtualisierungsserver SOLLTE die maximale Leistung festgelegt werden, die dieser für virtuelle Clients zur Verfügung stellen darf. Diese Grenzwerte SOLLTEN in der VDI-Managementkomponente genutzt werden, um bei hoher Auslastung die virtuellen Clients auf verschiedene Virtualisierungsserver zu verteilen.

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.2.6.A13 Verwendung getrennter VDI-Lösungen für unterschiedliche Benutzendengruppen (H)

Es SOLLTE geprüft werden, ob es Benutzendengruppen gibt, die sich in ihren Berechtigungen so stark unterscheiden, dass die Nutzung einer gemeinsamen VDI-Lösung nicht sinnvoll ist. In diesem Fall SOLLTE jeweils eine eigene VDI-Lösung pro Benutzendengruppe verwendet werden.

SYS.2.6.A14 Verwendung von nicht-persistenten virtuellen Clients (H)

Nachdem sie benutzt wurden oder zu einem definierten Zeitpunkt SOLLTEN die virtuellen Clients auf ihren Grundzustand, d. h. auf das zugrundeliegende Template, zurückgesetzt oder bei Bedarf neu provisioniert werden. Diese Zeitfenster SOLLTEN dokumentiert und an die Betroffenen kommuniziert werden. Nicht zurückgesetzte virtuelle Clients SOLLTEN NICHT von mehreren unterschiedlichen Benutzenden verwendet werden.

SYS.2.6.A15 Hochverfügbare Bereitstellung der VDI-Komponenten (H)

Die VDI-Komponenten SOLLTEN redundant ausgelegt werden. Jede Komponente SOLLTE darüber hinaus redundant an die relevanten Netze angeschlossen werden. Falls die VDI-Komponenten auf physischen IT-Systemen betrieben werden, SOLLTEN diese IT-Systeme über redundante Stromversorgung und Datenspeicher verfügen. Falls die VDI-Komponenten virtualisiert betrieben werden, SOLLTEN Mechanismen der Virtualisierungsinfrastruktur für die Hochverfügbarkeit eingesetzt werden.

SYS.2.6.A16 Integration der VDI in ein SIEM (H)

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

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.2.6 *Virtual Desktop Infrastructure* sind keine weiterführenden Informationen vorhanden.