Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.5 Client-Virtualisierung

1. Beschreibung

1.1. Einleitung

Client-Virtualisierung bezeichnet die virtualisierte Bereitstellung von Clients. Sowohl lokal auf einem physischen Client als auch mittels einer (zentralen) Virtualisierungsinfrastruktur können Clients virtualisiert werden. Virtualisierungsinfrastrukturen können genutzt werden, um virtuelle Clients von einem entfernten Arbeitsplatz aus zu bedienen.

Dieser Baustein behandelt den sicheren Einsatz von Client-Virtualisierung mittels einer Virtualisierungsinfrastruktur. Eine Virtualisierungsinfrastruktur umfasst dabei einen oder mehrere physische Virtualisierungsserver gemäß des Bausteins SYS.1.5 *Virtualisierung*. Die einzelnen virtuellen Clients werden auf den jeweiligen Virtualisierungsservern ausgeführt und setzen sich dabei aus den hierfür festgelegten virtuellen Hardware-Ressourcen wie CPU, Arbeitsspeicher und dem zugehörigen Festplatten-Abbild (Image) zusammen. Diese Abbilder werden üblicherweise anhand von Vorlagen (Templates) erzeugt.

Die Benutzenden interagieren hierbei über physische Clients, die sich mittels Terminalserver-Techniken und -Protokollen mit den virtuellen Clients verbinden. Somit ist der virtuelle Client auch ein Terminalserver im Sinne des Bausteins SYS.1.9 *Terminalserver*.

Virtuelle Clients, die auf einer Virtualisierungsinfrastruktur ausgeführt werden, sind in der Regel leichter zu administrieren als physische Clients, die geographisch über die Institution verteilt sind. Weiterhin können virtuelle Clients anhand von Templates einfacher als physische Clients provisioniert werden. Zudem können virtuelle Clients über Snapshots oder geklonte virtuelle Maschinen einfacher aktualisiert werden. Ein anderer typischer Einsatzfall sind virtuelle Clients, die erzeugt werden, um bestimmte Anwendungen zu testen und daher nur für einen kurzen Zeitraum benötigt werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die bei der Client-Virtualisierung verarbeitet und übertragen werden. Hierzu werden spezielle Anforderungen an die virtuellen Clients und die zugrundeliegende Virtualisierungsinfrastruktur sowie an die verwendeten Netze gestellt.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.5 *Client-Virtualisierung* ist auf die Virtualisierungsinfrastruktur sowie alle virtuellen Clients anzuwenden, sofern diese wie oben beschrieben zentral bereitgestellt werden.

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:

- Der Baustein SYS.2.5 *Client-Virtualisierung* thematisiert diejenigen Teile einer Client-Virtualisierung, die spezifisch für die Bereitstellung und den Einsatz von virtuellen Clients sind.
- 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:

- Zugreifende und virtuelle Clients kommunizieren über eine Terminalserver-Software, die auf den virtuellen Clients ausgeführt wird. Daher ist der Baustein SYS.1.9 *Terminalserver* sowohl auf die virtuellen Clients als auch auf die zugreifenden Clients anzuwenden.
- Um die allgemeinen Aspekte von virtuellen Clients zu adressieren, ist der Baustein SYS.2.1 *Allgemeiner Client* anzuwenden. Weiterhin sind gegebenenfalls die betriebssystemspezifischen Bausteine der Schicht *SYS* anzuwenden.
- Die allgemeinen Aspekte der Virtualisierung, zum Beispiel die Isolation über den Virtualisierungsserver, werden im Baustein SYS.1.5 *Virtualisierung* adressiert.
- Der Baustein NET.1.1 *Netzarchitektur und -design* muss angewendet werden, um die Netze abzusichern, die für die Kommunikation zwischen zugreifendem Client und Virtualisierungsinfrastruktur genutzt werden.

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

- Die lokale Bereitstellung von virtuellen Clients auf physischen Clients.

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.2.5 *Client-Virtualisierung* von besonderer Bedeutung.

2.1. Unzureichende Dimensionierung der Netzanbindung virtueller Clients

Werden bei der Planung der virtuellen Clients die Leistungsanforderungen an deren Netzanbindung nicht oder nur unzureichend berücksichtigt, könnten die virtuellen Clients nicht richtig funktionieren. Ist beispielsweise die Netzanbindung an nachgelagerte Dienste (z. B. Videokonferenzlösungen oder Dateiablagen) nicht leistungsfähig genug, können die virtuellen Clients unter Umständen nur noch eingeschränkt auf Informationen zugreifen, z. B. bei latenzkritischen Anwendungen. Ähnliches gilt, wenn die virtuellen Clients nicht mit hinreichender Netzkapazität an die zugreifenden Clients angebunden sind.

2.2. Unzureichende Leistung der virtuellen Clients durch Ressourcenknappheit

Um auf virtuellen Clients möglichst reibungslos arbeiten zu können, ist es wichtig, dass sie leistungsfähig sind. Werden einem virtuellen Client nur unzureichende Ressourcen (z. B. CPU, Arbeitsspeicher oder Grafikleistung) zugewiesen, kann die Verfügbarkeit der auf dem virtuellen Client installierten Anwendungen beeinträchtigt werden. Beispielsweise können bestimmte grafisch

anspruchsvolle Programme nicht ohne dedizierte Grafikprozessoren auf dem virtuellen Client ausgeführt werden. Auch ein zu niedriger Prozessortakt führt zu einer langsamen Verarbeitungsgeschwindigkeit.

Verhalten sich die virtuellen Clients unterschiedlich, können hierdurch Ressourcen knapp werden. Führen Benutzende beispielsweise viele Anwendungen dauerhaft und parallel aus, können die virtuellen Clients unter Umständen die erforderliche Leistung nicht mehr erbringen.

2.3. Gegenseitiges Stören der virtuellen Clients

Die Dimensionierung der zugrundeliegenden Virtualisierungsinfrastruktur ist maßgeblich für die tatsächlich abrufbare Leistung mehrerer parallel ausgeführter virtueller Clients. Werden auf einem Virtualisierungsserver zusätzlich zu einem virtuellen Client viele andere virtuelle IT-Systeme gleichzeitig ausgeführt, könnte der Virtualisierungsserver den Ressourcenbedarf nicht mehr decken. Dies wiederum kann dazu führen, dass die tatsächliche Leistung des virtuellen Clients begrenzt und nicht mehr vorhersehbar wird. Prozessorleistung und Arbeitsspeicher spielen dabei die größte Rolle, wenn sie dynamisch zugewiesen werden. Rufen nun zu viele verschiedene Personen zeitgleich Leistung ab, konkurrieren sie um diese.

Besonders wenn virtuelle Clients unsachgemäß benutzt werden und die bereitgestellten Ressourcen stark ausgelastet sind, können andere virtuelle Clients beeinträchtigt werden. Im Extremfall kann der zugrundeliegende Virtualisierungsserver ein virtuelles IT-System aus Ressourcenmangel beenden oder sogar selbst vollständig ausfallen.

2.4. Unzureichende Trennung der virtuellen Clients auf Netzebene

Bei den virtuellen Clients handelt es sich um Clients im Sinne des Bausteins SYS.2.1 *Allgemeiner Client*, die gegebenenfalls einen unterschiedlichen Schutzbedarf haben können. Werden diese Clients auf einer gemeinsamen Virtualisierungsinfrastruktur betrieben, könnte eine bestehende Trennung auf Port-Ebene durch den eingesetzten Virtualisierungsserver aufgehoben werden (auf Ebene der virtuellen Switches).

Werden die virtuellen Clients, z. B. durch Konfigurationsfehler, auf Ebene der virtuellen Switches, VLANs oder physischen Schnittstellen nicht den vorgesehenen Netzsegmenten zugeordnet, könnten diese auf schützenswerte Netze und dort befindliche Informationen zugreifen, für die sie nicht berechtigt sind.

Virtualisierungsserver werden in der Regel in zentralen IT-Betriebsbereichen (Rechenzentren) betrieben, in denen auch weitere zentrale Server positioniert sind. Sind virtuelle Clients und zentrale Server nicht in Netzsegmenten positioniert, die voneinander getrennt sind, können virtuelle Clients unberechtigt oder unbeabsichtigt auf Server zugreifen. Sind in diesen Netzsegmenten virtuelle Clients enthalten, die auf das Internet zugreifen dürfen, vergrößert dies die Angriffsfläche.

2.5. Verlust von virtuellen Clients und darauf gespeicherten Daten

Bei der Client-Virtualisierung werden die Images der virtuellen Clients an zentraler Stelle gespeichert und verwaltet. Durch fehlerhafte Administration oder Fehlbedienung von virtuellen Clients können diese beschädigt oder gelöscht werden. Der Verlust virtueller Clients im laufenden Betrieb kann dazu führen, dass auch Informationen gelöscht werden, die auf diesen virtuellen Clients gespeichert sind. Zusätzlich bedeutet der Verlust virtueller Clients, dass Informationen, die auf diesen virtuellen Clients verarbeitet werden, nicht mehr verfügbar sind.

2.6. Nicht-Erreichbarkeit von virtuellen Clients und darauf gespeicherten Daten

In der Regel können virtuelle Clients nicht von den Benutzenden selber eingeschaltet werden, sondern nur vom IT-Betrieb, der auch die Virtualisierungsinfrastruktur administriert. Bei Updates oder generell Wartungsarbeiten an der Virtualisierungsinfrastruktur ist es üblich, dass virtuelle Clients ausgeschaltet werden. Wird vergessen, sie hinterher wieder einzuschalten, bleiben sie ausgeschaltet und sind somit nicht erreichbar.

Ebenso kann ein Ausfall des zugrundeliegenden Virtualisierungsservers dazu führen, dass virtuelle Clients temporär nicht erreichbar sind. In diesem Fall können die Benutzenden nicht mehr auf den jeweiligen virtuellen Client und die darauf gespeicherten Daten zugreifen.

2.7. Software-Schwachstellen auf den virtuellen Clients

Virtuelle Clients setzen sich aus den festgelegten virtuellen Hardware-Ressourcen wie CPU und Arbeitsspeicher und dem zugehörigen Festplatten-Abbild zusammen. Diese Abbilder werden üblicherweise anhand von Vorlagen erzeugt. Wenn diese Vorlagen erzeugt werden, sind sie in der Regel auf einem aktuellen Software-Stand ohne bekannte Schwachstellen.

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

Auch kann es notwendig sein, virtuelle Clients mit bekannten Schwachstellen zu provisionieren, z. B. für Kompatibilitätstests oder für benötigte Software, die nur auf veralteten Betriebssystemen lauffähig ist. Diese Schwachstellen können vorhersehbar auftreten und so leichter ausgenutzt werden.

2.8. Umgehen der Isolation zwischen einem virtuellen Client und anderen virtualisierten IT-Systemen

Virtuelle IT-Systeme werden oft auf einer gemeinsam genutzten Virtualisierungsinfrastruktur eingesetzt, um Ressourcen effizienter zu nutzen und flexibler bereitzustellen. Dadurch können sich die verschiedenen virtualisierten IT-Systeme gegenseitig beeinflussen. Im Gegensatz zu einem virtuellen Server können virtuelle Clients einfacher kompromittiert werden, da die auf den virtuellen Clients ausgeführten Anwendungen vielfältiger und interaktiver sind.

Ein kompromittierter virtueller Client kann die gemeinsam genutzte Virtualisierungsinfrastruktur gefährden, da nicht nur über das Netz erreichbare IT-Systeme, sondern auch andere virtuelle IT-Systeme auf dem Virtualisierungsserver angegriffen werden können. Da das physische IT-System gemeinsam genutzt wird, können beispielsweise Seitenkanalangriffe wie Spectre oder Meltdown durchgeführt oder es kann aus der virtuellen Maschine ausgebrochen werden, um anschließend den zugrundeliegenden Hypervisor oder das zugrundeliegende Betriebssystem zu kompromittieren. In diesem Fall können virtuelle IT-Systeme außer Betrieb genommen oder auch die in ihnen verarbeiteten Daten ausgelesen oder modifiziert werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.5 *Client-Virtualisierung* 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.2.5.A1 Planung des Einsatzes virtueller Clients (B)

Es MUSS festgelegt werden, welche Anwendungen auf den virtuellen Clients eingesetzt werden sollen. Die Aufgaben, die mit diesen Anwendungen gelöst werden sollen, MÜSSEN festgelegt werden. Für diese Anwendungen MUSS überprüft und dokumentiert werden, welche Anforderungen an die Virtualisierungsinfrastruktur und deren etwaige Zusatzhardware (z. B. Grafikkarten) gestellt werden. Der genutzte Virtualisierungsserver MUSS die notwendigen Ressourcen hinsichtlich CPU, Arbeitsspeicher und Datenspeicher bereitstellen.

SYS.2.5.A2 Planung der verwendeten Netze für virtuelle Clients (B) [Planende]

Die Netze für die Verbindung zwischen zugreifenden Clients und virtuellen Clients sowie die Netze zur Anbindung nachgelagerter Dienste an die virtuellen Clients (z. B. Verzeichnisdienst, E-Mail oder Internetzugriff) MÜSSEN ausreichend leistungsfähig ausgelegt werden.

Es MUSS geplant werden, welche Netzsegmente für die virtuellen Clients verwendet werden sollen. Die Netzsegmente für virtuelle Clients MÜSSEN von Netzsegmenten für Server getrennt sein. Eine bestehende Netztrennung DARF NICHT mithilfe eines virtuellen Clients oder eines Virtualisierungsservers umgangen werden.

Für virtuelle Clients MUSS festgelegt werden, ob und in welchem Ausmaß die Kommunikation in nicht vertrauenswürdige Netze eingeschränkt werden soll.

SYS.2.5.A3 Schutz vor Schadsoftware auf den virtuellen Clients (B)

Für die virtuellen Clients MUSS ein Schutz vor Schadsoftware gemäß den Bausteinen OPS.1.1.4 *Schutz vor Schadprogrammen* und SYS.2.1 *Allgemeiner Client* sowie unter Berücksichtigung der betriebssystemspezifischen Bausteine umgesetzt werden. Wird ein Virenschutzprogramm eingesetzt, MUSS festgelegt und dokumentiert werden, ob dieser Schutz zentralisiert in der Virtualisierungsinfrastruktur, dezentralisiert auf den virtuellen Clients oder in Mischformen umgesetzt wird. Falls die virtuellen Clients mit zentralen Komponenten geschützt werden sollen, MÜSSEN diese zentralen Komponenten über eine ausreichende Leistung verfügen.

Falls ein Virenschutzprogramm auf den virtuellen Clients ausgeführt wird, MUSS sichergestellt werden, dass die Leistung der Virtualisierungsinfrastruktur ausreicht.

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.2.5.A4 Verwendung einer dedizierten Virtualisierungsinfrastruktur für die virtuellen Clients (S)

Die virtuellen Clients SOLLTEN auf einer dedizierten Virtualisierungsinfrastruktur betrieben werden. Virtuelle Server SOLLTEN NICHT auf derselben Virtualisierungsinfrastruktur ausgeführt werden.

SYS.2.5.A5 Zusätzliche Netzsegmentierung für virtuelle Clients (S)

Folgende Kriterien SOLLTEN für eine zusätzliche Netztrennung der virtuellen Clients berücksichtigt werden:

- Nutzungsszenario für die virtuellen Clients und Gruppenzugehörigkeit der Benutzenden
- aus der Gruppenzugehörigkeit abgeleitete Berechtigungen der Benutzenden
- auf den virtuellen Clients installierte und den Benutzenden zur Verfügung gestellte Anwendungen
- Schutzbedarf der auf den virtuellen Clients verarbeiteten Informationen
- Vertrauenswürdigkeit der virtuellen Clients
- für die Funktionsfähigkeit der virtuellen Clients notwendige Netzanbindungen

SYS.2.5.A6 Keine lokale Datenablage auf virtuellen Clients (S)

Durch die Benutzenden erstellte oder verarbeitete Daten SOLLTEN zentral gespeichert werden. Die Daten SOLLTEN NICHT dauerhaft auf den virtuellen Clients abgelegt werden.

Benutzende, die sich mit virtuellen Clients verbinden, SOLLTEN NICHT in der Lage sein, Daten aus den virtuellen Clients auf ihre lokalen IT-Systeme zu übertragen. Falls eine solche Übertragung nachvollziehbar notwendig ist, SOLLTE sie auf das notwendige Minimum beschränkt werden.

SYS.2.5.A7 Automatische Sperrung von Sitzungen (S)

Nachdem ein zugreifender Client seine Terminalserver-Sitzung beendet hat, SOLLTE die aktive Sitzung auf dem virtuellen Client gesperrt werden. Nach einer definierten Zeit der Inaktivität SOLLTEN Verbindungen zwischen zugreifendem und virtuellem Client beendet werden. Falls der Einsatzzweck des jeweiligen virtuellen Clients dies zulässt, SOLLTEN die virtuellen Clients in einen inaktiven Zustand versetzt werden, nachdem die Verbindung beendet ist.

SYS.2.5.A8 Härtung der virtuellen Clients (S)

Die virtuellen Clients SOLLTEN gehärtet werden. Hierbei SOLLTEN die folgenden Aspekte berücksichtigt werden:

- Einschränkung der Datenübertragung zwischen zugreifenden und virtuellen Clients
- Weiterleitungen von Peripheriegeräten oder externen Datenträgern von zugreifenden an die virtuellen Clients
- Explizite Freigabe der Ausführung von Anwendungen
- Deaktivierung von Netzdiensten, die in der Virtualisierungsinfrastruktur nicht benötigt werden

SYS.2.5.A9 Einbindung der virtuellen Clients in das Patch- und Änderungsmanagement (S)

Die Client-Anwendungen SOLLTEN zentral provisioniert werden. Dazu SOLLTE eine geeignete zentral verwaltbare Lösung eingesetzt werden. Templates für die virtuellen Clients SOLLTEN regelmäßig aktualisiert und getestet werden.

SYS.2.5.A10 Bedarfsgerechte Zuweisung von Ressourcen zu virtuellen Clients und Gruppen (S)

Anhand von Rollen und Tätigkeiten SOLLTEN die Leistungsanforderungen der einzelnen Benutzendengruppen an die virtuellen Clients identifiziert werden. Anhand dieser Anforderungen SOLLTE entschieden werden, wie viele Ressourcen (z. B. Prozessorkerne oder Arbeitsspeicher) den einzelnen virtuellen Clients zur Verfügung gestellt werden.

Zusätzliche Ressourcen wie GPUs (Graphics Processing Units) SOLLTEN den Benutzenden nur bei Bedarf bereitgestellt werden.

SYS.2.5.A11 Vermeidung von verschachtelter Virtualisierung auf virtuellen Clients (S)

Auf virtuellen Clients SOLLTEN keine weiteren virtuellen IT-Systeme eingerichtet werden. Falls technisch möglich, SOLLTEN in der zugrundeliegenden Virtualisierungsinfrastruktur Funktionen aktiviert werden, die eine verschachtelte Virtualisierung erschweren oder unterbinden.

SYS.2.5.A12 Sensibilisierung der Benutzenden (S)

Alle Benutzenden von virtuellen Clients SOLLTEN über den sicheren Umgang mit virtuellen Clients sensibilisiert werden. Falls die Ressourcen dynamisch anhand der abgerufenen Leistung zwischen mehreren virtuellen Clients aufgeteilt werden, SOLLTEN die Benutzenden darüber aufgeklärt werden, dass ihr Verhalten potenziell andere Benutzende beeinflussen kann.

Falls die Sicherheitsanforderungen der auf virtuellen Clients ausgeführten Anwendungen besonders sind, SOLLTE kommuniziert werden, wie diese gegenüber physischen Clients abweichen. Es SOLLTE auch kommuniziert werden, welche spezifischen Sicherheitsaspekte zu beachten sind.

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.2.5.A13 Verhinderung der Kommunikation zwischen virtuellen Clients an einem gemeinsam genutzten virtuellen Switch (H)

Mechanismen SOLLTEN aktiviert werden, die eine unkontrollierte Layer-2-Kommunikation zwischen virtuellen Clients an einem gemeinsam genutzten virtuellen Switch unterbinden.

SYS.2.5.A14 Erweiterte Sicherheitsfunktionen für den Einsatz von virtuellen Clients (H)

Die virtuellen Clients SOLLTEN mit zusätzlichen Sicherheitsfunktionen geschützt werden. Dabei SOLLTEN mindestens die folgenden Techniken berücksichtigt werden:

- Mikrosegmentierung für die virtuellen Clients
- Intrusion-Detection- oder Intrusion-Prevention-Systeme, die entweder zentralisiert auf der Virtualisierungsinfrastruktur oder dezentral auf den virtuellen Clients bereitgestellt werden

SYS.2.5.A15 Monitoring der virtuellen Clients (H)

Der Zustand der virtuellen Clients SOLLTE zentral überwacht werden. Folgende Parameter SOLLTEN mindestens überwacht werden:

- Erreichbarkeit der virtuellen Clients über alle vorgesehenen Netzschnittstellen,
- Auslastung von CPU und Arbeitsspeicher der virtuellen Clients,

- freie Festplattenkapazität der virtuellen Clients sowie
- Verfügbarkeit der für den Zugriff eingesetzten Terminalserver-Dienste.

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

SYS.2.5.A16 Erweiterte Protokollierung für virtuelle Clients (H)

Für virtuelle Clients SOLLTEN zusätzliche Ereignisse an eine zentrale Protokollierungsinfrastruktur (siehe OPS.1.1.5 *Protokollierung*) übermittelt werden. Hierbei SOLLTEN mindestens die folgenden Ereignisse protokolliert werden:

- Aktionen, die mit administrativen Rechten ausgeführt werden,
- Konfigurationsänderungen,
- Installation von Software,
- erfolgreiche und fehlgeschlagene Updates und
- alle Ereignisse, die durch den Schutz vor Schadsoftware entstehen.

SYS.2.5.A17 Erweitertes Monitoring der virtuellen Clients (H)

Die virtuellen Clients SOLLTEN kontinuierlich darauf überwacht werden, ob die in SYS.2.5.A16 *Erweiterte Protokollierung für virtuelle Clients* beschriebenen Ereignisse auftreten. Wird ein Security Information and Event Management (SIEM) genutzt, SOLLTEN die virtuellen Clients darin eingebunden werden. Im SIEM SOLLTEN die überwachten Ereignisse auf Anomalien inklusive Angriffsmustern automatisiert analysiert werden.

Die virtuellen Clients SOLLTEN automatisch und regelmäßig auf Schwachstellen überprüft werden.

SYS.2.5.A18 Hochverfügbare Bereitstellung der Virtualisierungsinfrastruktur (H)

Die virtuellen Clients SOLLTEN hochverfügbar bereitgestellt werden. Dies SOLLTE durch die zugrundeliegende Virtualisierungsinfrastruktur sichergestellt werden. Die Virtualisierungsserver SOLLTEN redundant an die relevanten Netze angeschlossen werden. Bei Ressourcenknappheit SOLLTEN die virtuellen Clients automatisch zwischen den Virtualisierungsservern migriert werden. Bei Ausfall eines Virtualisierungsservers SOLLTEN die virtuellen Clients automatisiert auf einem anderen Virtualisierungsserver gestartet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.2.5 *Client-Virtualisierung* sind keine weiterführenden Informationen vorhanden.