Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.2 Ordnungsgemäße IT-Administration

1. Beschreibung

1.1. Einleitung

Unter IT-Administration werden Tätigkeiten hauptsächlich innerhalb des IT-Betriebs verstanden, für die administrative Rechte benötigt werden und die die Konfiguration von IT-Komponenten verändern. Administrierende sorgen nicht nur dafür, dass die IT-Komponenten verfügbar bleiben, sondern setzen auch Maßnahmen für die Informationssicherheit um und überprüfen, ob diese wirksam sind.

Zu den Tätigkeitsbereichen der Administrierenden gehört es unter anderem, die IT einer Institution einzurichten, zu konfigurieren, zu überprüfen und bestehende IT zu ändern. Hierzu zählt ebenfalls die Fachadministration, also die IT-Administration von Anwendungen, für deren Betrieb der entsprechende Fachbereich statt der Organisationseinheit IT-Betrieb zuständig ist.

Administrative Rechte für IT-Komponenten (also insbesondere für IT-Systeme, IT-Dienste, Anwendungen, IT-Plattformen und Netze) sind privilegierte Rechte, die neben den Zugängen auch Zugriffe über das Netz sowie physikalische Zutritte umfassen können. Daher sind sowohl die administrativen Rechte auf organisatorischer Ebene als auch die Administrationswerkzeuge selber ein attraktives Ziel für Angreifer. Wesentlich für die Sicherheit der IT-Administration sind die ordnungsgemäße und nachvollziehbare Durchführung aller administrativen Tätigkeiten und die Absicherung der dafür benötigten Hilfsmittel.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei der ordnungsgemäßen IT-Administration zu etablieren. Mit der Umsetzung dieses Bausteins sorgt die Institution einerseits dafür, dass die für die Sicherheit des Informationsverbunds erforderlichen Tätigkeiten der IT-Administration ordnungsgemäß und systematisch durchgeführt werden. Andererseits reagiert die Institution damit auch auf die besonderen Gefährdungen, die sich aus dem Umgang mit privilegierten Rechten und aus dem Zugang zu schützenswerten Bereichen der Institution zwangsläufig ergeben.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* ist einmal auf den gesamten Informationsverbund anzuwenden.

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

- übergreifende Anforderungen an den Administrationsprozess, sowohl für den IT-Betrieb als auch in der Fachadministration,
- Anforderungen an administrative Tätigkeiten sowie
- Anforderungen an den Umgang mit administrativen Berechtigungen, also privilegierten Zutritten, Zugängen und Zugriffen.

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

- Fernadministration von IT-Systemen über externe Schnittstellen sowie Fernwartung von Geräten und Komponenten durch die Herstellungs- oder Zulieferunternehmen (siehe OPS.1.2.5 *Fernwartung*)
- Patch- und Änderungsmanagement (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*)
- die Absicherung von Administrationswerkzeugen (siehe NET.1.2 *Netzmanagement* und OPS.1.1.7 *Systemmanagement*)
- die ordnungsgemäße Verwaltung von Benutzenden und Berechtigungen (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*)
- besondere Anforderungen für den Fall, dass die IT-Administration durch Dritte erfolgt (siehe OPS.2.3 *Nutzung von Outsourcing* und OPS.3.2 *Anbieten von Outsourcing*)
- Aspekte für die IT-Administration von industrieller IT (siehe Bausteine aus dem Bereich IND *Industrielle IT*)

Dieser Baustein behandelt **nicht**

- die allgemeinen Aspekte des IT-Betriebs wie Inventarisierung, In- und Außerbetriebnahme von IT-Komponenten sowie die grundsätzlichen Rahmenbedingungen für Administrierende (siehe OPS.1.1.1 *Allgemeiner IT-Betrieb*)
- die Einweisung des Personals in einzuhaltende allgemeine Sicherheitsbestimmungen der IT (siehe ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*)
- die kontinuierliche Schulung des Personals sowie die damit einhergehende Sensibilisierung für Gefährdungen und Sicherheitsmaßnahmen (siehe ORP.2 *Personal* und ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*)

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 OPS.1.1.2 *Ordnungsgemäße IT-Administration* von besonderer Bedeutung.

2.1. Unzureichend geregelte Zuständigkeiten

Die IT-Administration umfasst diverse Aufgaben auf verschiedensten Komponenten unterschiedlicher Bereiche. Fehlen Regelungen über Zuständigkeiten oder Prozesse oder sind die Regelungen und Prozesse den Zuständigen nicht bekannt, kann dies verschiedene mögliche Folgen haben. Gegebenenfalls werden erforderliche Administrationsaufgaben gar nicht oder durch den falschen Bereich erledigt, der gegebenenfalls nicht alle zu beachtenden Einzelheiten kennt. Womöglich werden auch gegenwirkende Maßnahmen von verschiedenen Bereichen durchgeführt. Dies kann bewirken, dass IT-Systeme nur eingeschränkt oder gar nicht mehr verfügbar sind.

Wird bei der Festlegung von Zuständigkeiten nicht beachtet, dass verschiedene IT-Administrationstätigkeiten, z. B. zwischen Applikationsbetrieb und Systembetrieb, untrennbar miteinander verbunden sind, können zusammengehörende Aufgaben gegebenenfalls nicht ordnungsgemäß durchgeführt werden.

Erhalten Administrierende zu viele Rechte, weil Zuständigkeiten nicht geregelt sind, können sie eventuell vertrauliche Informationen einsehen, die sie nicht einsehen dürfen. Dies ist insbesondere der Fall, wenn aus Bequemlichkeit zu viele administrative Konten mit zu weitreichenden Rechten eingerichtet sind, im schlimmsten Fall sogar über Organisationseinheiten hinweg.

Außerdem kann eine zu hohe Anzahl Administrierender zu einem Kontrollverlust führen, wenn nicht klar geregelt ist, wer für welche Aufgaben zuständig ist. In diesem Fall sind alle Schutzziele der Informationssicherheit gefährdet.

2.2. Unzureichende Dokumentation

Die Dokumentation kann unzureichend sein, wenn Informationen über IT-Komponenten (z. B. über Konfiguration oder Zugriffsrechte) nicht oder nur unvollständig erfasst wurden. Auch wenn die Dokumentation im Rahmen von IT-Administrationstätigkeiten nicht aktualisiert wird, ist die Dokumentation unzureichend, weil sie nicht mehr dem Ist-Zustand entspricht.

Unzureichende Dokumentation kann zu Fehlkonfigurationen oder allgemein fehlerhafter IT-Administration führen. Dadurch können alle Schutzziele der Informationssicherheit erheblich gefährdet werden.

Außerdem kann auch das Notfallmanagement erheblich beeinträchtigt werden, weil für zeitkritische Aufgaben erst Informationen gesammelt werden müssen oder die Aufgaben aufgrund der Diskrepanz zwischen Dokumentation und Ist-Zustand nicht wie geplant durchgeführt werden können. Dies kann dazu führen, dass ein Notfall nicht schnell genug behandelt und die Verfügbarkeit von IT-Komponenten länger beeinträchtigt wird.

2.3. Missbrauch von privilegierten Berechtigungen durch Administrierende

Zu weit gefasste administrative Berechtigungen können genutzt werden, um zu sabotieren oder Informationen auszuspähen, die als Ausgangspunkt für Angriffe verwendet werden können. Dadurch werden alle Schutzziele der Informationssicherheit gefährdet.

Privilegierte Zutritte, Zugänge und Zugriffe können auch missbraucht werden, wenn die Prozesse beim Ausscheiden von internen oder externen Administrierenden unzureichend sind und dadurch ausgeschiedene Personen weiterhin auf IT-Komponenten zugreifen können. Auch in diesem Fall sind alle Schutzziele der Informationssicherheit gefährdet.

2.4. Preisgabe von schützenswerten Informationen an unberechtigte Personen

Über Zugänge der IT-Administration kann auf schützenswerte Informationen zugegriffen werden, z. B. auf die Dokumentation, die für die IT-Administration benötigt wird, oder auf die Konfigurationen von IT-Systemen. Werden die Zugänge der IT-Administration unzureichend abgesichert, können auch unberechtigte Personen an schützenswerte Informationen gelangen. Über den Verlust der Vertraulichkeit hinaus können diese Informationen auch manipuliert oder für weitergehende Angriffe genutzt werden, wodurch alle Schutzziele der Informationssicherheit erheblich gefährdet sind.

2.5. Personalausfall von Kernkompetenzträgern

Sind die benötigten Kenntnisse bei den Administrierenden nicht auf allen Gebieten redundant vorhanden, könnte eine entsprechende IT-Administrationstätigkeit nicht durchgeführt werden, wenn Kernkompetenztragende ausfallen. Wenn zusätzlich die Dokumentation für durchzuführende Arbeitsschritte unzureichend ist, kann die IT-Administrationstätigkeit nicht von anderen Administrierenden ohne weitere Risiken durchgeführt werden. Dies kann dazu führen, dass Fehlfunktionen nicht behoben werden können. In der Folge ist die Verfügbarkeit von IT-Systemen nicht (ausreichend) gewährleistet und Schwachstellen können nicht behoben werden, wodurch Angriffe begünstigt werden.

Diese Situation kann auch dadurch entstehen, dass es für IT-Administrationstätigkeiten keine festgelegten Vertretenden mit entsprechenden Berechtigungen gibt oder dass festgelegte Vertretende oder sogar der Notfallzugang nicht über die erforderlichen administrativen Berechtigungen verfügen.

2.6. Unzureichende Verfügbarkeit von Administrierenden

Herrscht bei den Administrierenden Personalmangel, z. B. durch unzureichende Personalplanung, Überbuchung oder Pandemie, können gegebenenfalls erforderliche Administrationsaufgaben nicht durchgeführt werden, falls dazu keine Zeit ist. Unter Umständen werden aufgrund von Zeitmangel auch Fehler bei der IT-Administration gemacht. Beides kann zu unzureichender Verfügbarkeit von IT-Systemen oder zu einer erhöhten Angriffsfläche und damit zur Gefährdung aller Schutzziele der Informationssicherheit führen.

Personalmangel kann zusätzlich zur Folge haben, dass Administrierende aus Zeitmangel für ihre Aufgaben unzureichend geschult werden, was ebenfalls dazu führen kann, dass im Bedarfsfall bzw. im Notfall bestimmte IT-Administrationstätigkeiten nicht korrekt durchgeführt werden.

2.7. Unzureichende Absicherung von Administrationswerkzeugen

Administrationswerkzeuge ermöglichen einen weitreichenden Zugriff auf die IT einer Institution. Werden diese Werkzeuge unzureichend abgesichert, kann das dazu führen, dass die Administrationswerkzeuge als solche bezüglich aller Schutzziele der Informationssicherheit gefährdet sind. Über sie kann die IT-Administration sabotiert werden oder es kann eine unberechtigte IT-Administration ermöglicht werden.

Wird bei einem Angriff Zugriff auf Administrationswerkzeuge erlangt, können weitreichende Berechtigungen erhalten werden. Diese Berechtigungen können für Angriffe aller Art missbraucht werden, wodurch ebenfalls alle Schutzziele der Informationssicherheit gefährdet sind.

Eine Ursache für die unzureichende Absicherung von Administrationswerkzeugen kann z. B. dadurch entstehen, dass sie unzureichend von anderen Anwendungen getrennt sind. Diese unzureichende Trennung ist auf allen Ebenen möglich. Sie kann z. B. dadurch entstehen, dass Texteditoren oder SSH-Clients zur IT-Administration genutzt werden, die auch im nicht-administrativen Kontext verwendet werden.

2.8. Ausfall der Administrationsmöglichkeit

Wenn Administrationsmöglichkeiten ausfallen und es aufgrund von Fehlplanungen keine Redundanz oder andere Alternativen gibt, können IT-Administrationstätigkeiten dieser Art nicht durchgeführt werden, bis der Ausfall behoben ist. Dadurch ist im schlimmsten Fall die gesamte IT eingeschränkt oder nicht verfügbar bzw. funktionstüchtig.

Administrationswerkzeuge können auch durch die Administration des Werkzeuges selbst ausfallen, z. B. durch eine Fehladministration, durch einen eingespielten Patch oder eine Änderung, die durch eine IT-Administrationstätigkeit herbeigeführt wird.

2.9. Fehlgeleitete Administration

Wird die IT-Administration fehlgeleitet, indem z. B. falsche Informationen eingeschleust werden, kann die IT-Administration zu falschen Reaktionen verleitet werden. Beispielsweise können Administrierende außerhalb des geregelten Prozesses fälschlicherweise darüber informiert werden, dass ein IT-System ausgefallen ist, was sie zu einem Neustart verleitet. Hierdurch können Informationen, Hard- oder Software manipuliert werden, wodurch deren Verfügbarkeit und Integrität nicht mehr gewährleistet ist. Zudem können auf diese Weise auch schützenswerte Informationen offengelegt werden.

2.10. Fehlerhafte Administration

Menschliche Fehler können nie ausgeschlossen werden und können bei der IT-Administration weitreichende Folgen haben. Zusätzlich werden sie durch einige der bisher genannten Gefährdungen begünstigt.

Die in der IT-Administration verwendeten Werkzeuge erlauben mit wenig Aufwand sehr weitreichende Änderungen an IT-Komponenten. Je nach Fehler können damit alle Schutzziele der Informationssicherheit erheblich gefährdet sein. Fehler werden insbesondere durch parallele Arbeiten an unterschiedlichen Themen begünstigt, bei denen beispielsweise unterschiedliche Eingabefenster oder Konsolenausgaben verwechselt werden können.

2.11. Störung der IT durch IT-Administrationstätigkeiten

Selbst wenn IT-Administrationstätigkeiten fehlerfrei durchgeführt werden, kann dabei trotzdem die IT der Institution gestört werden. Werden z. B. vorgegebene Wartungsfenster für IT-Administrationstätigkeiten nicht eingehalten, kann die Verfügbarkeit der administrierten IT gestört werden. Zudem können auch korrekt im Wartungsfenster durchgeführte IT-Administrationstätigkeiten später zu Störungen führen, z. B. wenn die Administrierbarkeit der entsprechenden Komponenten durch nicht vorhergesehene Wechselwirkungen beeinträchtigt wird.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.2 *Ordnungsgemäße IT-Administration* 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	Keine

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.

OPS.1.1.2.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.2.A2 Vertretungsregelungen (B)

Für jede Administrationsaufgabe MUSS eine Vertretung benannt werden. Die Vertretung MUSS über die notwendigen administrativen Berechtigungen (organisatorisch und technisch) verfügen, um die Tätigkeit durchführen zu können. Eine benannte Vertretung MUSS über die im Kontext der Administrationsaufgabe notwendigen Kenntnisse verfügen.

Die Regelung der Vertretung MUSS Mangel- und Notfallsituationen berücksichtigen.

OPS.1.1.2.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.2.A4 Beendigung der Tätigkeit in der IT-Administration (B)

Falls eine Person von Administrationsaufgaben entbunden wird, MÜSSEN ihr alle damit zusammenhängenden privilegierten Berechtigungen auf organisatorischer und technischer Ebene entzogen werden. Insbesondere MÜSSEN persönliche administrative Konten gesperrt und Passwörter aller administrativer Konten geändert werden, die der Person bekannt sind. Weiterhin MÜSSEN alle betroffenen Parteien darauf hingewiesen werden, dass diese Person von den entsprechenden Aufgaben entbunden ist und daher keine administrativen Berechtigungen mehr haben darf.

Es MUSS geregelt werden unter welchen Rahmenbedingungen geprüft wird, ob sich zusätzliche nicht dokumentierte administrative Rechte verschafft wurden. Diese Prüfung SOLLTE insbesondere erfolgen, falls die Entscheidung eine Person von Administrationsaufgaben zu entbinden nicht im Einvernehmen mit der entsprechenden Person getroffen wurde. Falls solche administrativen Rechte gefunden wurden, MÜSSEN diese wieder entzogen werden.

OPS.1.1.2.A5 Nachweisbarkeit von administrativen Tätigkeiten (B)

Administrative Tätigkeiten MÜSSEN nachweisbar sein. Dafür MUSS mindestens festgehalten werden,

- welche Änderung bei einer Tätigkeit durchgeführt wurde,
- wer eine Tätigkeit durchgeführt hat und
- wann eine Tätigkeit durchgeführt wurde.

Die Institution MUSS jederzeit nachweisen können, welche Person welche administrativen Tätigkeiten durchgeführt hat. Dazu SOLLTEN alle Administrierenden über eine eigene Zugangskennung verfügen. Auch Vertretungen von Administrierenden SOLLTEN eigene Zugangskennungen erhalten. Jeder Anmeldevorgang (Login) über eine Administrationskennung MUSS protokolliert werden.

OPS.1.1.2.A6 Schutz administrativer Tätigkeiten (B)

Administrative Schnittstellen und Funktionen DÜRFEN NUR berechtigten Personen zur Verfügung stehen. Für diese Schnittstellen und Funktionen MÜSSEN geeignete Verfahren zur Authentisierung

festgelegt werden. Es MUSS sichergestellt sein, dass IT-Administrationstätigkeiten nur durchgeführt werden können, falls vorher eine dementsprechende Authentisierung erfolgt ist.

Es MUSS festgelegt werden, welche Protokolle für Administrationsschnittstellen verwendet werden dürfen, so dass die bei der Administration stattfindende Kommunikation abgesichert ist.

OPS.1.1.2.A21 Regelung der IT-Administrationsrollen (B)

Es MÜSSEN Rollen definiert werden, die ausschließlich zur IT-Administration vergeben werden. Administrationsrollen MÜSSEN aufgrund des tatsächlichen Bedarfs im Aufgabenbereich der IT-Administration nachvollziehbar vergeben werden. Alle notwendigen IT-Administrationstätigkeiten MÜSSEN durch Berechtigungen in den Administrationsrollen nach dem Minimalprinzip abgedeckt sein.

Die IT-Administration unterschiedlicher Ebenen der IT-Komponenten, z. B. die Trennung von Betriebssystem- und Anwendungsadministration, MUSS bei der Konzeption der Administrationsrollen berücksichtigt werden.

OPS.1.1.2.A22 Trennung von administrativen und anderen Tätigkeiten (B)

Die durchführende Person MUSS wissen, bei welchem Teil ihrer Aufgabe es sich um administrative Tätigkeiten handelt. Aufgaben, die keine Administrationsrechte benötigen, DÜRFEN NICHT mit Administrationsrechten ausgeführt werden.

Es MUSS sichergestellt werden, dass Administrationswerkzeuge klar als solche erkennbar sind. Wenn eine Anwendung zur Erfüllung einer Administrationsaufgabe benutzt wird, DARF NICHT dieselbe Instanz dieser Anwendung für andere Aufgaben verwendet werden. Dies SOLLTE auf technischer Ebene sichergestellt werden. Die Zugangskennungen, die zur IT-Administration genutzt werden, SOLLTEN sich von Zugangskennungen unterscheiden, die in anderem Kontext genutzt 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.

OPS.1.1.2.A7 Regelung der IT-Administrationstätigkeit (S)

Jede IT-Administrationstätigkeit SOLLTE einer klar definierten Aufgabe zugeordnet sein. Für diese Aufgaben SOLLTE geregelt werden,

- durch wen diese Aufgabe ausgeführt werden darf und
- durch wen diese Aufgabe beauftragt werden darf.

Es SOLLTE nachvollziehbar sein, in welchen Prozessen sich Administrationsaufgaben einfügen. IT-Administrationstätigkeiten SOLLTEN nur mit denjenigen Berechtigungen durchgeführt werden, die zur Erfüllung der entsprechenden Aufgabe notwendig sind. Es SOLLTE festgelegt werden, wie IT-Administrationstätigkeiten auszuführen sind.

Die Regelungen für IT-Administrationstätigkeiten SOLLTEN regelmäßig und anlassbezogen überprüft und aktualisiert werden.

Für jede IT-Administrationstätigkeit SOLLTE sichergestellt werden, dass diese bei Bedarf auch im Notfall ausgeführt werden kann.

OPS.1.1.2.A8 Administration von Fachanwendungen (S)

Es SOLLTE geregelt und dokumentiert werden, welche Administrationsaufgaben für Fachanwendungen vom IT-Betrieb und welche durch die Fachadministration durchgeführt werden.

Für Fachanwendungen SOLLTE identifiziert werden, welche Zugriffe der IT-Betrieb auf Systemebene benötigt.

Alle Schnittstellen und Abhängigkeiten zwischen der Fachadministration und der Administration durch den IT-Betrieb SOLLTEN identifiziert werden. Immer wenn Administrationsprozesse erstellt und gepflegt werden, SOLLTEN die Zuständigkeiten und Abhängigkeiten dieser Schnittstellen berücksichtigt werden.

OPS.1.1.2.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten (S)

Durchgeführte IT-Administrationstätigkeiten SOLLTEN nachvollziehbar dokumentiert werden. Es SOLLTE geprüft werden, welche grundsätzlichen Anforderungen an die Dokumentation der IT-Administrationstätigkeiten existieren. Es SOLLTE identifiziert werden, welche Ziele mit der Dokumentation erreicht werden sollen. Aufgrund dieser Anforderungen und Ziele SOLLTE verbindlich festgelegt werden, welche Schritte in welchem Detailierungsgrad dokumentiert werden. Aus der Dokumentation SOLLTE mindestens hervorgehen,

- welche Änderungen erfolgten,
- wann die Änderungen erfolgten,
- wer die Änderungen durchgeführt hat,
- auf welcher Grundlage bzw. aus welchem Anlass die Änderungen erfolgt sind und
- inwiefern und aus welchem Grund gegebenenfalls von vorgegebenen Standards oder Konfigurationen abgewichen wurde.

Dokumentation im Kontext einer IT-Administrationstätigkeit SOLLTE in Standard-Arbeitsabläufen enthalten sein. Es SOLLTE geregelt werden, welche Möglichkeiten zu nutzen sind, falls IT-Administrationstätigkeiten außerplanmäßig durchgeführt werden.

Es SOLLTE identifiziert werden, unter welchen Umständen ein Zugriff auf die Dokumentation notwendig ist. Der Zugriff SOLLTE dementsprechend gewährleistet sein.

OPS.1.1.2.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A16 Erweiterte Sicherheitsmaßnahmen für Administrationszugänge (S)

Der Zugang zu administrativen Oberflächen und Schnittstellen SOLLTE auf IT-Systeme, die zur IT-Administration verwendet werden, beschränkt sein. Daher SOLLTEN Netze, die zur IT-Administration verwendet werden, durch Filter- und Segmentierungsmaßnahmen von produktiven Netzen zu administrierender Komponenten getrennt werden (Out-of-Band-Management). Wo kein Out-of-Band-Management möglich ist, SOLLTEN Software-Schnittstellen und physische Schnittstellen zur IT-Administration durch zusätzliche Maßnahmen abgesichert werden und nur für Personen erreichbar sein, die für deren Nutzung berechtigt sind. Hierzu SOLLTE eine Zwei-Faktor-Authentisierung verwendet werden.

OPS.1.1.2.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A23 Rollen- und Berechtigungskonzept für administrative Zugriffe (S)

Es SOLLTE ein angemessenes Rollen- und Berechtigungskonzept für administrative Zugriffe existieren. Darin SOLLTEN grundsätzliche Vorgaben gemacht werden, mindestens darüber,

- wie Administrationsrollen beantragt und zugewiesen werden,
- welche Arten von Administrationsrollen existieren,
- welche Arten von Berechtigungen im Kontext der Administrationsrollen vergeben werden,
- wie für die IT-Administration notwendige Berechtigungen vergeben werden.

OPS.1.1.2.A24 Prüfen von IT-Administrationstätigkeiten (S)

Bevor eine IT-Administrationstätigkeit durchgeführt wird, SOLLTE geprüft werden, ob der Anlass und die Art der Tätigkeit im Kontext der zugrundeliegenden Aufgabe plausibel sind. Nachdem eine IT-Administrationstätigkeit an einer Komponente durchgeführt wurde, SOLLTE geprüft werden, ob die Konfiguration und der Status der Komponente dem gewünschten Zielzustand entspricht.

Falls eine zusätzliche Qualitätssicherung der ausgeführten Administrationsaufgabe notwendig ist, SOLLTE diese nicht durch dieselbe Person durchgeführt werden, die die entsprechenden Tätigkeiten durchgeführt hat.

Für IT-Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTE geprüft werden, ob diese Tätigkeiten die Verfügbarkeit der IT-Administration selbst einschränken könnten. In diesem Fall SOLLTEN entsprechende Vorkehrungen getroffen werden, um einen Rollback der IT-Administrationstätigkeiten zu ermöglichen.

OPS.1.1.2.A25 Zeitfenster für schwerwiegende IT-Administrationstätigkeiten (S)

Für IT-Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTEN durch den IT-Betrieb Wartungsfenster abgestimmt werden. Falls der IT-Betrieb für IT-Administrationstätigkeiten Vorgaben zu Zeitfenstern macht, MÜSSEN diese eingehalten werden.

OPS.1.1.2.A26 Backup der Konfiguration (S)

Alle Konfigurationen SOLLTEN durch regelmäßige Backups auf Anwendungsebene und auf IT-Systemebene gesichert werden. Vor IT-Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTE ein zusätzliches Backup gemacht werden. Für Backups SOLLTE gewährleistet sein, dass sie im Fehlerfall wieder eingespielt werden können.

OPS.1.1.2.A27 Ersatz für zentrale IT-Administrationswerkzeuge (S)

Für zentrale IT-Administrationswerkzeuge SOLLTEN Alternativen zur Verfügung stehen, mit denen im Bedarfsfall administriert werden kann. Hierzu SOLLTEN Sprungsysteme mit Zugriff auf entsprechende Administrationsnetze zur Verfügung stehen. Falls solche Alternativen nicht zur Verfügung stehen, SOLLTE zur IT-Administration der Zugang und der direkte Zugriff auf die zu administrierende IT möglich sein.

OPS.1.1.2.A28 Protokollierung administrativer Tätigkeiten (S)

Administrative Tätigkeiten SOLLTEN protokolliert werden. Die Protokolldateien SOLLTEN für eine angemessene Zeitdauer geschützt aufbewahrt werden. Die ausführenden Administrierenden SOLLTEN keine Möglichkeiten haben, die aufgezeichneten Protokolldateien zu verändern oder zu löschen. Protokolldaten SOLLTEN regelmäßig geprüft 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.

OPS.1.1.2.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

OPS.1.1.2.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

OPS.1.1.2.A17 IT-Administration im Vier-Augen-Prinzip (H)

Es SOLLTE geregelt werden, welche Administrationsaufgaben eine zusätzliche Person erfordern, die die Ausführung überwacht. Diese Person SOLLTE im Kontext der durchzuführenden IT-Administrationstätigkeiten auch über die zur Ausführung notwendigen Qualifikationen verfügen.

OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten (H)

Bei IT-Komponenten mit hohem Schutzbedarf SOLLTEN alle administrativen Tätigkeiten in sämtlichen Bereichen protokolliert werden. Dabei SOLLTE jede administrative Aktion vollständig nachvollzogen werden. Die ausführenden Administrierenden SOLLTEN keinen Einfluss auf Art und Umfang der Protokollierung nehmen können.

OPS.1.1.2.A19 Nutzung hochverfügbarer IT-Administrationswerkzeuge (H)

Administrationswerkzeuge SOLLTEN redundant ausgelegt werden. Es SOLLTE sichergestellt werden, dass im Störungsfall weiterhin alle Administrationsaufgaben ohne wesentliche Einschränkungen ausgeführt werden können.

OPS.1.1.2.A29 Monitoring der IT-Administrationswerkzeuge (H)

Für IT-Administrationswerkzeuge SOLLTEN Kenngrößen zur Verfügbarkeit identifiziert werden. Diese Kenngrößen SOLLTEN kontinuierlich überwacht werden. Es SOLLTEN tolerierbare Grenzwerte dieser Kenngrößen festgelegt werden. Werden diese nicht eingehalten, SOLLTEN die zuständigen Teams automatisch benachrichtigt werden.

OPS.1.1.2.A30 Sicherheitsmonitoring administrativer Tätigkeiten (H)

Falls ein IT-System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen genutzt wird, SOLLTEN dort Ereignisdaten zu administrativen Tätigkeiten ausgewertet werden. Hierzu SOLLTEN bestehende Monitoring-Systeme der IT sowie kritische Administrationswerkzeuge in dieses IT-System eingebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) stellt in Anhang A der Norm ISO/IEC 27001:2013 unter anderem im Kontext der Themen Zugangssteuerung (A.9) und IT-Betrieb (A.12) Anforderungen an die ordnungsgemäße IT-Administration.

Das BSI spezifiziert unter anderem für den Bereich der sicheren Administration Anforderungen im Dokument „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen“.