Risikobericht

Managementsystem: ISMS Reporting

Das gegenständliche Dokument gilt als vertraulich und ist ausschließlich für den internen Gebrauch bestimmt. Es ist nicht gestattet, dieses Dokument oder Teile daraus in irgendeiner Form zum Gebrauch durch Dritte zu vervielfältigen und/oder ganz bzw. auszugsweise zu veröffentlichen.

© TogetherSecure

Inhaltsverzeichis

Bauliche Risiken (FM_Risk) 2

Offene Maßnahmen 2

Brandschutztüre wechseln (ToSec_005) 2

Temp. - und Feuchtigkeitssensor in Serverraum einbauen (ToSec_006) 2

Aktive Kontrollen 3

Feuerlöscher überprüfen (ToSec_FM_01) 3

Wöchentl. Serverraum-Kontrolle (ToSec_FM_02) 4

Zeitliche Entwicklung 6

Zugriffsrisiko für SAP (APP_Risk) 8

Offene Maßnahmen 8

Passwort Komplexität erhöhen (ToSec_007) 8

Zeitliche Entwicklung 8

Risiko Windows Server 2012 (Srv2012_Risk) 9

Offene Maßnahmen 10

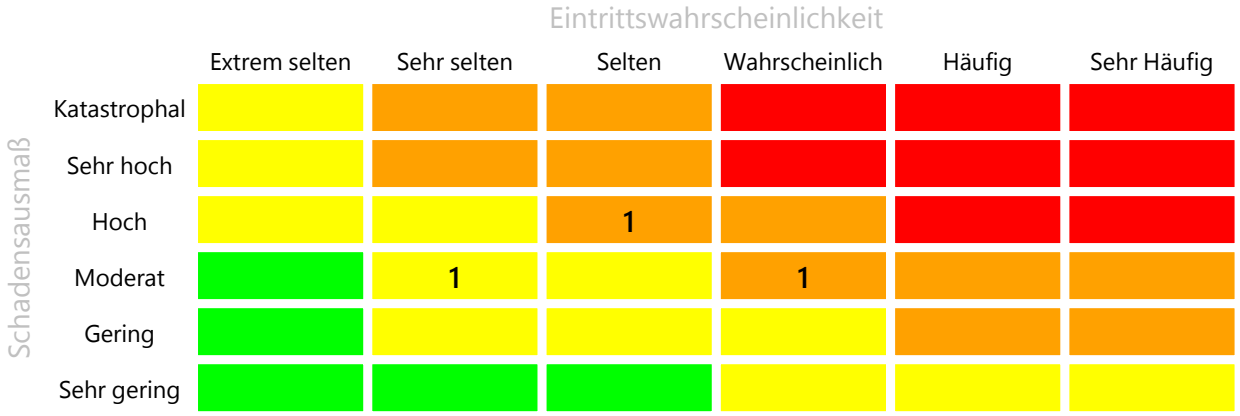
Sichere Installation von Windows Server 2012 (SYS.1.2.2.M2) 10

Planung von Windows Server 2012 (SYS.1.2.2.M1) 11

Sichere Authentisierung und Autorisierung in Windows Server 2012 (SYS.1.2.2.M6) 13

Gefährdungslagen im Überblick

Verwendete Schadensausmaßklassifikation: Standard



RKZ	Kürzel	Beschreibung	Status
12	APP_Risk	Zugriffsrisiko für SAP	Aktiv
12	Srv2012_Risk	Risiko Windows Server 2012	Aktiv
6	FM_Risk	Bauliche Risiken	Aktiv

Bauliche Risiken (FM_Risk)

Identifiziert am:	13.02.2019	Letzte Änderung:	07.10.2020 10:42
Eintrittswahrscheinlichkeit:	Sehr selten	Schadensausmaß:	Moderat
Verantwortliche(r):	Max Mustermann		
Managementsystem:	ISMS Reporting		
Beschreibung:	die Erkenntnisse wurden bei einer Begehung durch die Brandschutzbehörde erkannt. Der Auditbericht liegt seit Ende 2018 vor: Die Brandschutzmaßnahmen sind nicht ausreichend gut umgesetzt und müssen dringend nachgebessert werden.		
Schutzziele:	Vertraulichkeit Verfügbarkeit Integrität		
Zugewiesene Entitäten:	Gebäude B (Ressource)		

Offene Maßnahmen:

Brandschutztüre wechseln (ToSec_005)

OrgEH:	TogetherSecure Holding AG (ToSec)
Beschreibung:	Brandschutztüre bei Abgang C entspricht nicht der Norm und muss ausgetauscht werden
Fortschritt:	0% gemeldet am 30.09.2020 16:19
Fortschrittsmeldung:	

Temp. - und Feuchtigkeitssensor in Serverraum einbauen (ToSec_006)

OrgEH:	TogetherSecure Holding AG (ToSec)
Beschreibung:	Ein Temperatur- bzw. Feuchtigkeitssensor sollte im Serverraum vorgesehen werden.
Fortschritt:	0%

Aktive Kontrollen:

Feuerlöscher überprüfen (ToSec_FM_01)

OrgEH:	TogetherSecure Holding AG (ToSec)
Umsetzer:	Marcel Habel
Prüfverhalten:	Alle müssen akzeptieren
Erstmalig:	17.02.2017 14:00
Wiederkehrend:	☒ Alle 1 Quartal(e)
Deadline:	☐
Eskaliert zu:	Marcel Habel
Beschreibung:	regelmäßige Überprüfung der Feuerlöscher
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 17.12.2018 12:00 Status: Abgeschlossen am 13.02.2019 10:37
Geprüft von: Max Mustermann (Akzeptiert) am 13.02.2019 10:37
Begründung: ok

2. Kontrolle ausgelöst am 17.01.2019 12:00 Status: Abgeschlossen am 13.02.2019 10:37
Geprüft von: Max Mustermann (Akzeptiert) am 13.02.2019 10:37
Begründung: ok

3. Kontrolle ausgelöst am 17.04.2019 12:00 Status: **Fehlgeschlagen** (Deadline überschritten)
4. Kontrolle ausgelöst am 17.07.2019 12:00 Status: **Fehlgeschlagen** (Deadline überschritten)
5. Kontrolle ausgelöst am 17.02.2017 14:00 Status: Ausstehend
6. Kontrolle ausgelöst am 17.05.2017 14:00 Status: Ausstehend
7. Kontrolle ausgelöst am 17.08.2017 14:00 Status: Ausstehend
8. Kontrolle ausgelöst am 17.11.2017 14:00 Status: Ausstehend
9. Kontrolle ausgelöst am 17.02.2018 14:00 Status: Ausstehend
10. Kontrolle ausgelöst am 17.05.2018 14:00 Status: Ausstehend
11. Kontrolle ausgelöst am 17.08.2018 14:00 Status: Ausstehend
12. Kontrolle ausgelöst am 17.11.2018 14:00 Status: Ausstehend
13. Kontrolle ausgelöst am 17.02.2019 14:00 Status: Ausstehend
14. Kontrolle ausgelöst am 17.05.2019 14:00 Status: Ausstehend
15. Kontrolle ausgelöst am 17.08.2019 14:00 Status: Ausstehend
16. Kontrolle ausgelöst am 17.11.2019 14:00 Status: Ausstehend
17. Kontrolle ausgelöst am 17.02.2020 14:00 Status: Ausstehend
18. Kontrolle ausgelöst am 17.05.2020 14:00 Status: Ausstehend
19. Kontrolle ausgelöst am 17.08.2020 14:00 Status: Ausstehend

Wöchentl. Serverraum-Kontrolle (ToSec_FM_02)

OrgEH:	TogetherSecure Holding AG (ToSec)
Umsetzer:	Max Mustermann
Prüfverhalten:	Alle müssen akzeptieren
Erstmalig:	14.01.2019 12:00
Wiederkehrend:	☒ Alle 1 Woche(n)
Deadline:	☐
Eskaliert zu:	Lisa Musterfrau
Beschreibung:	regelmäßige Kontrolle des Serverraums bzgl. Temperatur und Feuchtigkeit
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 14.01.2019 12:00	Status:	Abgeschlossen am 13.02.2019 10:35
Geprüft von:	Daniel Mustermann (Akzeptiert) am 13.02.2019 10:35	
	Begründung: passt	
2. Kontrolle ausgelöst am 21.01.2019 12:00	Status:	**Fehlgeschlagen** (Abgelehnt)
3. Kontrolle ausgelöst am 28.01.2019 12:00	Status:	Abgeschlossen am 13.02.2019 10:35
Geprüft von:	Daniel Mustermann (Akzeptiert) am 13.02.2019 10:35	
	Begründung: passt	
4. Kontrolle ausgelöst am 04.02.2019 12:00	Status:	Abgeschlossen am 13.02.2019 10:35
Geprüft von:	Daniel Mustermann (Akzeptiert) am 13.02.2019 10:35	
	Begründung: passt	
5. Kontrolle ausgelöst am 11.02.2019 12:00	Status:	Abgeschlossen am 13.02.2019 10:37
Geprüft von:	Daniel Mustermann (Akzeptiert) am 13.02.2019 10:37	
	Begründung: ok	
6. Kontrolle ausgelöst am 18.02.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
7. Kontrolle ausgelöst am 25.02.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
8. Kontrolle ausgelöst am 04.03.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
9. Kontrolle ausgelöst am 11.03.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
10. Kontrolle ausgelöst am 18.03.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
11. Kontrolle ausgelöst am 25.03.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
12. Kontrolle ausgelöst am 01.04.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
13. Kontrolle ausgelöst am 08.04.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
14. Kontrolle ausgelöst am 15.04.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
15. Kontrolle ausgelöst am 22.04.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
16. Kontrolle ausgelöst am 29.04.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
17. Kontrolle ausgelöst am 06.05.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
18. Kontrolle ausgelöst am 13.05.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
19. Kontrolle ausgelöst am 20.05.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
20. Kontrolle ausgelöst am 27.05.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)

21. Kontrolle ausgelöst am 03.06.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
22. Kontrolle ausgelöst am 10.06.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
23. Kontrolle ausgelöst am 17.06.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
24. Kontrolle ausgelöst am 24.06.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
25. Kontrolle ausgelöst am 01.07.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
26. Kontrolle ausgelöst am 08.07.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
27. Kontrolle ausgelöst am 15.07.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
28. Kontrolle ausgelöst am 22.07.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
29. Kontrolle ausgelöst am 29.07.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
30. Kontrolle ausgelöst am 05.08.2019 12:00	Status:	**Fehlgeschlagen** (Deadline überschritten)
31. Kontrolle ausgelöst am 12.08.2019 12:00	Status:	Ausstehend
32. Kontrolle ausgelöst am 19.08.2019 12:00	Status:	Ausstehend
33. Kontrolle ausgelöst am 26.08.2019 12:00	Status:	Ausstehend
34. Kontrolle ausgelöst am 02.09.2019 12:00	Status:	Ausstehend
35. Kontrolle ausgelöst am 09.09.2019 12:00	Status:	Ausstehend
36. Kontrolle ausgelöst am 16.09.2019 12:00	Status:	Ausstehend
37. Kontrolle ausgelöst am 23.09.2019 12:00	Status:	Ausstehend
38. Kontrolle ausgelöst am 30.09.2019 12:00	Status:	Ausstehend
39. Kontrolle ausgelöst am 07.10.2019 12:00	Status:	Ausstehend
40. Kontrolle ausgelöst am 14.10.2019 12:00	Status:	Ausstehend
41. Kontrolle ausgelöst am 21.10.2019 12:00	Status:	Ausstehend
42. Kontrolle ausgelöst am 28.10.2019 12:00	Status:	Ausstehend
43. Kontrolle ausgelöst am 04.11.2019 12:00	Status:	Ausstehend
44. Kontrolle ausgelöst am 11.11.2019 12:00	Status:	Ausstehend
45. Kontrolle ausgelöst am 18.11.2019 12:00	Status:	Ausstehend
46. Kontrolle ausgelöst am 25.11.2019 12:00	Status:	Ausstehend
47. Kontrolle ausgelöst am 02.12.2019 12:00	Status:	Ausstehend
48. Kontrolle ausgelöst am 09.12.2019 12:00	Status:	Ausstehend
49. Kontrolle ausgelöst am 16.12.2019 12:00	Status:	Ausstehend
50. Kontrolle ausgelöst am 23.12.2019 12:00	Status:	Ausstehend
51. Kontrolle ausgelöst am 30.12.2019 12:00	Status:	Ausstehend
52. Kontrolle ausgelöst am 06.01.2020 12:00	Status:	Ausstehend
53. Kontrolle ausgelöst am 13.01.2020 12:00	Status:	Ausstehend
54. Kontrolle ausgelöst am 20.01.2020 12:00	Status:	Ausstehend
55. Kontrolle ausgelöst am 27.01.2020 12:00	Status:	Ausstehend
56. Kontrolle ausgelöst am 03.02.2020 12:00	Status:	Ausstehend
57. Kontrolle ausgelöst am 10.02.2020 12:00	Status:	Ausstehend
58. Kontrolle ausgelöst am 17.02.2020 12:00	Status:	Ausstehend
59. Kontrolle ausgelöst am 24.02.2020 12:00	Status:	Ausstehend
60. Kontrolle ausgelöst am 02.03.2020 12:00	Status:	Ausstehend
61. Kontrolle ausgelöst am 09.03.2020 12:00	Status:	Ausstehend

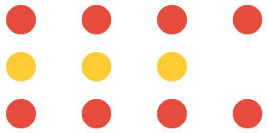
62. Kontrolle ausgelöst am 16.03.2020 12:00	Status:	Ausstehend
63. Kontrolle ausgelöst am 23.03.2020 12:00	Status:	Ausstehend
64. Kontrolle ausgelöst am 30.03.2020 12:00	Status:	Ausstehend
65. Kontrolle ausgelöst am 06.04.2020 12:00	Status:	Ausstehend
66. Kontrolle ausgelöst am 13.04.2020 12:00	Status:	Ausstehend
67. Kontrolle ausgelöst am 20.04.2020 12:00	Status:	Ausstehend
68. Kontrolle ausgelöst am 27.04.2020 12:00	Status:	Ausstehend
69. Kontrolle ausgelöst am 04.05.2020 12:00	Status:	Ausstehend
70. Kontrolle ausgelöst am 11.05.2020 12:00	Status:	Ausstehend
71. Kontrolle ausgelöst am 18.05.2020 12:00	Status:	Ausstehend
72. Kontrolle ausgelöst am 25.05.2020 12:00	Status:	Ausstehend
73. Kontrolle ausgelöst am 01.06.2020 12:00	Status:	Ausstehend
74. Kontrolle ausgelöst am 08.06.2020 12:00	Status:	Ausstehend
75. Kontrolle ausgelöst am 15.06.2020 12:00	Status:	Ausstehend
76. Kontrolle ausgelöst am 22.06.2020 12:00	Status:	Ausstehend
77. Kontrolle ausgelöst am 29.06.2020 12:00	Status:	Ausstehend
78. Kontrolle ausgelöst am 06.07.2020 12:00	Status:	Ausstehend
79. Kontrolle ausgelöst am 13.07.2020 12:00	Status:	Ausstehend
80. Kontrolle ausgelöst am 20.07.2020 12:00	Status:	Ausstehend
81. Kontrolle ausgelöst am 27.07.2020 12:00	Status:	Ausstehend
82. Kontrolle ausgelöst am 03.08.2020 12:00	Status:	Ausstehend
83. Kontrolle ausgelöst am 10.08.2020 12:00	Status:	Ausstehend
84. Kontrolle ausgelöst am 17.08.2020 12:00	Status:	Ausstehend
85. Kontrolle ausgelöst am 24.08.2020 12:00	Status:	Ausstehend
86. Kontrolle ausgelöst am 31.08.2020 12:00	Status:	Ausstehend
87. Kontrolle ausgelöst am 07.09.2020 12:00	Status:	Ausstehend
88. Kontrolle ausgelöst am 14.09.2020 12:00	Status:	Ausstehend
89. Kontrolle ausgelöst am 21.09.2020 12:00	Status:	Ausstehend
90. Kontrolle ausgelöst am 28.09.2020 12:00	Status:	Ausstehend
91. Kontrolle ausgelöst am 05.10.2020 12:00	Status:	Ausstehend

Zeitliche Entwicklung:

	Datum	Änderungen	Status	Eintrittswahrscheinlichkeit	Schadensausmaß
	30.09.2020 09:16	Schadensausmaß, Eintrittswahrscheinlichkeit	Aktiv	Sehr selten	Moderat
	Begründung:	Bewertung durch Brandschutzprüfer			
	30.09.2020 09:13	Eintrittswahrscheinlichkeit	Aktiv	Selten	Hoch
	Begründung:	Deckensprinkler monitert			

Datum	Änderungen	Status	Eintrittswahrscheinlichkeit	Schadensausmaß
30.09.2020 09:12	Schadensausmaß	Aktiv	Wahrscheinlich	Hoch
Begründung:	Neue Brandschutztüren installiert die Feuer eindämmen würden.			

Zugriffsrisiko für SAP (APP_Risk)

Identifiziert am:	13.02.2019	Letzte Änderung:	07.10.2020 10:44
Eintrittswahrscheinlichkeit:	Wahrscheinlich	Schadensausmaß:	Moderat
Verantwortliche(r):	Daniel Mustermann		
Managementsystem:	ISMS Reporting		
Beschreibung:	dies wurde vom Wirtschaftsprüfer für alle SAP Applikationen erkannt und dokumentiert		
Schutzziele:	Vertraulichkeit Verfügbarkeit Integrität		

Offene Maßnahmen:

Passwort Komplexität erhöhen (ToSec_007)

OrgEH:	TogetherSecure Holding AG (ToSec)
Beschreibung:	Passwort Komplexität erhöhen: - längere PWD - Historie erhöhen
Fortschritt:	70% gemeldet am 30.09.2020 11: 9
Fortschrittsmeldung:	sss

Zeitliche Entwicklung:

Datum	Änderungen	Status	Eintrittswahrscheinlichkeit	Schadensausmaß
01.09.2020 10:43	Schadensausmaß, Eintrittswahrscheinlichkeit	Aktiv	Wahrscheinlich	Moderat
Begründung:	Risiko erstellt			

Risiko Windows Server 2012 (Srv2012_Risk)

Identifiziert am:	19.07.2019	Letzte Änderung:	07.10.2020 10:42
Eintrittswahrscheinlichkeit:	Selten	Schadensausmaß:	Hoch
Verantwortliche(r):	Daniel Mustermann		
Managementsystem:	ISMS Reporting		
Beschreibung:	Risiken durch den Einsatz von Windows Server 2012		
Schutzziele:	Vertraulichkeit Verfügbarkeit Integrität		
Zugewiesene Entitäten:	SRV_DB_01 (Ressource) SRV_APP_001 (Ressource) SRV_APP_MED (Ressource)		

Offene Maßnahmen:

Sichere Installation von Windows Server 2012 (SYS.1.2.2.M2)

OrgEH:	TogetherSecure Holding AG (ToSec)
Beschreibung:	Grundlegende Funktionen von Windows Server 2012 (R2) werden durch Serverrollen, Rollendienste und Features gesteuert. **Serverrollen** Eine Serverrolle ist eine Gruppe von Programmen, mittels derer eine bestimmte Funktion für mehrere Benutzer oder für andere IT-Systeme in einem Netz ausgeführt werden kann. Mit ihr wird häufig die Hauptfunktion eines Servers beschrieben. Ein Server könnte jedoch auch mehrere Rollen ausführen, wenn diese nur selten verwendet werden. Sind Rollen korrekt installiert und konfiguriert, werden sie automatisch ausgeführt. **Rollendienste** Rollendienste sind Programme, die die Funktionalität einer Rolle bereitstellen. Eine Rolle kann als Satz zusammenhängender, sich ergänzender Rollendienste betrachtet werden, wobei in der Regel die Installation einer Rolle die Einrichtung mindestens eines zugehörigen Rollendienstes bedingt. Je Rolle kann festgelegt werden, welche Rollendienste für andere Benutzer und IT-Systeme mit der Rolle bereitgestellt werden. Einige Rollen (z. B. DNS-Server) haben nur eine Funktion, daher stehen für sie keine Rollendienste zur Verfügung. Andere Rollen (z. B. Remotedesktopdienste) verfügen über mehrere Rollendienste, die je nach Anforderungen installiert werden können. **Features** Features sind Programme, die die Funktionalität des Servers oder aber einer oder mehrerer Rollen unterstützen oder verbessern. Z. B. wird mit dem Feature Failover-Clusterunterstützung die Funktionalität weiterer Rollen (u. a. Dateidienste und DHCP-Server) verbessert, da Servercluster für eine höhere Redundanz und bessere Leistung zusammengeführt werden können. Das Feature Telnet-Client hingegen ermöglicht die Fernkommunikation über das Telnet-Protokoll. Rollen, Rollendienste und Features müssen immer so sparsam wie möglich installiert werden, um die Komplexität und Angriffsoberfläche klein zu halten. Die Regel "ein Dienst pro Server" gilt auch hier sinngemäß, es sollte in der Regel nur eine für die Institution wesentliche Serverrolle pro Server installiert sein. Die Auswahl der zu installierenden Rollen, Rollendienste und Features sollte begründet und dokumentiert werden. **Server Core** Server Core ist eine minimale Installationsoption für Windows Server (inkl. 2012 und 2012 R2), die eine Serverumgebung mit beschränkter Funktionalität und geringerem Wartungsbedarf bereitstellt. Seit Windows Server 2012 ist ein Wechsel zwischen Full Server und Server Core ohne Neuinstallation möglich. Hauptunterschiede sind das Fehlen der vollständigen Windows-Shell und eine extrem begrenzte grafische Oberfläche (GUI), die sich auf ein Kommandoprompt mit PowerShell-Unterstützung beschränkt. Verwalten lässt sich Server Core folgendermaßen: • per PowerShell (lokal und remote) • über eine Terminal-Server-Verbindung von einer Kommandozeile • aus der Ferne über die Microsoft Management Console (MMC) • aus der Ferne mit anderen Kommandozeilentools, die Fernverwaltung unterstützen Da Server Core bezüglich der Angriffsfläche das Minimum und damit Optimum darstellt, sollte, wo immer möglich, die Server Core-Variante genutzt werden. Abweichungen sollten begründet sein. Dies fördert zudem die Zentralisierung der Verwaltung.
Fortschritt:	0% gemeldet am 29.09.2020 22:19
Fortschrittsmeldung:	

Planung von Windows Server 2012 (SYS.1.2.2.M1)

OrgEH:	TogetherSecure Holding AG (ToSec)
Beschreibung:	Da Windows Server 2012 (R2) ein komplexes Betriebssystem mit einer Vielzahl von Funktionen und Konfigurationsoptionen darstellt, muss der Einsatz sorgfältig und systematisch geplant werden. Eine Dokumentation der Entscheidungen samt kurzer Begründung sollte dabei angelegt werden, etwa in Form eines Betriebskonzepts oder eines Serverhandbuchs. **Editionen** Windows Server 2012 ist in vier Editionen verfügbar, die für unterschiedliche Einsatzgebiete vorgesehen und optimiert sind: ● Foundation ○ Grundlegende Server-Funktionen ○ keine Virtualisierung ● Essentials ○ einfache Benutzeroberfläche ○ voreingestellte Konnektivität zu Cloud-Diensten ○ keine Virtualisierung ● Standard ○ Voller Funktionsumfang ○ max. zwei virtuelle Instanzen ● Datacenter ○ wie Standard ○ mit unbegrenzten virtuellen Instanzen Weitere Beschränkungen existieren bei Foundation bzw. Essentials bezüglich Speicher (max. 32/64 GB RAM) und Lizenzierung (max. 15/25 Benutzerkonten) sowie in den installierbaren Rollen und Funktionalitäten. Über weitere Details der Unterschiede bzgl. Beschränkungen, Rollen und Funktionen informiert Microsoft auf seiner Website. Der Server-Core-Modus etwa ist erst ab Edition Standard verfügbar, die Nutzung von WSUS erst ab Essentials. Zumindest Foundation ist daher nur in sehr begrenzten Szenarien für den professionellen Einsatz im Unternehmen oder in der Behörde zu empfehlen und wird in diesem Baustein nicht näher betrachtet. Die Editionen Standard und Datacenter sind aus Sicherheitssicht gleichwertig und unterscheiden sich im Wesentlichen in Hinsicht auf das Lizenzmodell. Es bleibt also die Frage nach der Entscheidung zwischen Essentials und Standard bzw. Datacenter. **Eigenschaften der Essentials-Edition** Foundation und Essentials in Windows 2012 sind nicht dafür gedacht, innerhalb einer vollwertigen Domäne betrieben zu werden. Zwar ist dies für Essentials mit Windows Server 2012 R2 mittlerweile technisch möglich, jedoch richtet sich diese mit ihren Funktionen hauptsächlich an kleinere Institutionen, die nur einen einzigen Server zum Betrieb sämtlicher Funktionen einsetzen. Dies steht im Widerspruch zur etablierten Praxis in größeren IT-Umgebungen, möglichst wenige Dienste pro Server zu betreiben, um Abhängigkeiten aufzulösen und Risiken zu streuen, ein Trend, der durch zunehmende Virtualisierung weitere Verbreitung findet. Die Essentials-Edition bietet ohne weitere Konfiguration eine Reihe von Funktionen, welche die Einrichtung erleichtern können: ● Hinzufügen zur Domäne Mit Essentials ist es einfach möglich, Rechner zur Domäne hinzuzufügen, die sich an einem entfernten Standort befinden. Es genügt, dass ein neuer Mitarbeiter auf den Pfad "/connect" der Essentials-Fernzugriffswebsite zugreifen kann. ● Vorkonfiguriertes VPN Es ist ein vorkonfigurierter VPN-Client verfügbar. Der Benutzer kann zudem die Autoeinwahl aktivieren, sodass er immer mit dem Firmen- bzw. Behördennetz verbunden ist. ● Server-SpeicherFür Speicherorte wie etwa die Heimatverzeichnisse der Benutzer können einfach Shared Folder auf einem weiteren Server im selben Netz angelegt werden. Dabei kann eine automatische Alarmierung erfolgen, wenn die Verzeichnisse eine bestimmte Größe überschreiten. ● Health Report Ein grundlegender "Gesundheitscheck" der Windows Server 2012 R2 Essentials-Umgebung ist bereits

integriert und muss nicht erst als Add-in installiert werden. Es lassen sich verschiedene Werte konfigurieren, die über unterschiedliche Medien angezeigt werden, etwa auch auf dem Smartphone.

- BranchCache
  Bereits in Essentials kann der Mechanismus BranchCache aktiviert werden, der die Verfügbarkeit von Daten in Außenstellen durch Caching (Zwischenspeicherung) erhöht. Er verringert darüber hinaus gleichzeitig die Bandbreitennutzung über das WAN.
- Remote Web Access
  Viele Funktionen von Windows Server 2012 Essentials lassen sich aus der Ferne über eine Weboberfläche erreichen und bedienen (Remote Web Access), die in R2 zudem modernisiert und für die Nutzung mit Tablets und ähnlichen Geräten optimiert wurde.

Microsoft Azure Online Backup

In Windows Server 2012 ist Microsofts Cloud-Speicherlösung Azure Online Backup bereits in Essentials integriert und kann leicht aktiviert werden. Dafür muss lediglich im Essentials Dashboard das entsprechende Add-in installiert werden und ein (je nach Speichervolumen kostenpflichtiger) Account angelegt werden. In R2 ist nicht mal mehr ein Add-in notwendig, hier kann direkt per Klick die Registrierung bei Azure erfolgen.

Während dies eine sehr einfache Möglichkeit darstellt, regelmäßige Backups der auf dem Server gespeicherten Daten zu erzeugen, sollte diese Funktion keinesfalls leichtfertig aktiviert werden, sondern allenfalls nach einer umfassenden Beschäftigung mit den Themen der Bausteine OPS.2.2 Cloud-Nutzung und OPS.1.16 Datensicherung und einer erfolgten Abwägung zwischen Vertraulichkeit, Verfügbarkeit und verschiedenen Anbietern.

Blockieren von Microsoft-Konten

Der folgende Abschnitt ist nicht anzuwenden, wenn im Rahmen der Beschäftigung mit dem Baustein OPS.2.2 Cloud-Nutzung eine begründete und dokumentierte Entscheidung für die Nutzung von Microsoft Azure in Zusammenhang mit dem Windows Server 2012 (R2)-Serversystem getroffen wurde.

Andernfalls darf während der Einrichtung des Systems kein Microsoft-Konto angelegt werden. Die Erstellung von Microsoft-Konten auf dem Server muss zudem blockiert werden. Am verlässlichsten geschieht dies zentral über das Active Directory und die folgende Sicherheitsrichtlinie:

"Windows Settings/Security Settings/Local Policies/Security Options/Accounts: Block Microsoft Accounts"

Fortschritt:	0%

Sichere Authentisierung und Autorisierung in Windows Server 2012 (SYS.1.2.2.M6)

OrgEH:	TogetherSecure Holding AG (ToSec)

Beschreibung:	Authentisierung und Autorisierung spielen als zwei grundlegende Sicherheitstechniken an verschiedenen Stellen in Windows Server 2012 (R2) wichtige Rollen. Folgende Prinzipien können dabei als allgemeine Leitlinien der Realisierung dienen:
	
	• Beschränkung und Schutz privilegierter Domänenaccounts
	  ○ Getrennte Accounts für Administration und andere Nutzung für Administratoren
	  ○ Spezielle abgesicherte Admin-Workstations
	  ○ Einschränkung der Konten, die sich interaktiv einloggen können
	  ○ Beschränkung von Account Delegation-Rechten für administrative Accounts
	• Beschränkung und Schutz lokaler Adminaccounts
	  ○ Lokale Account-Beschränkungen für Remote-Zugriff
	  ○ Kein Netz-Login für lokale Accounts
	  ○ Individuelle Passwörter für lokale Admin-Accounts
	
	Geschützte Benutzer
	
	Mit R2 kam die domänenbezogene globale Sicherheitsgruppe "Geschützte Benutzer" (Protected Users) hinzu. Die Anmeldeinformationen der Mitglieder dieser Gruppe werden durch standardmäßig restriktivere Sicherheitseinstellungen zusätzlich geschützt.
	
	Der nicht weiter konfigurierbare Schutz gilt für alle Geräten, auf denen Windows Server 2012 R2 und Windows 8.1 ausgeführt wird sowie auf Domänencontrollern in Domänen mit einem primären Windows Server 2012 R2 Domänencontroller.
	
	Der Speicherfußabdruck von Anmeldeinformationen wird durch mehrere Einschränkungen signifikant reduziert:
	
	• NTLM, Digestauthentifizierung oder CredSSP sind deaktiviert.
	• Kerberos nutzt in der Vor-Authentifizierung nicht die schwächere DES- oder RC4-Verschlüsselung.
	• Das Konto kann nicht mit der eingeschränkten und uneingeschränkten Kerberos-Delegierung delegiert werden. Das bedeutet, dass frühere Verbindungen mit anderen Systemen fehlschlagen, wenn der Benutzer Mitglied der Gruppe "Geschützte Benutzer" ist.
	• Eine Ticket-Granting-Ticket-Lebensdauer von vier Stunden kann via Active Directory-Verwaltungscenter (ADAC) über Authentifizierungsrichtlinien und Silos konfiguriert werden, sodass sich der Benutzer alle vier Stunden erneut authentifizieren muss.
	
	Alle menschlichen Benutzer sollten möglichst Mitglieder der Gruppe "Geschützte Benutzer" sein.
	
	Achtung: Konten für Dienste und Computer sollten nicht Mitglieder von "Geschützte Benutzer" sein, da die Gruppe keinen lokalen Schutz bietet: Kennwort oder Zertifikat sind immer auf dem System verfügbar.
	
	Gruppe "Managed Service Accounts"
	
	Managed Service Accounts (MSA) sind eines der besonderen Features, die mit Windows Server 2008 R2 und Windows 7 hinzugekommen sind. Es handelt sich hierbei um Konten für Dienste (z. B. SQL Server oder Exchange) im Active Directory, die an einen bestimmten Rechner gebunden sind. Das Konto verfügt über sein eigenes komplexes Passwort und wird automatisch verwaltet. So kann ein MSA einfach und sicher Dienste auf einem bestimmten System ausführen, während die Möglichkeit, als ein bestimmter Benutzer-Principal auf Ressourcen im Netz zuzugreifen, gewahrt bleibt. Die Gruppe "Managed Service Account", die mit Windows Server 2012 geschaffen wurde, bietet dieselbe Funktionalität in der Domäne, jedoch zusätzlich mit der Möglichkeit, diese über mehrere Server zu erstrecken.
	
	Wo immer möglich sollten für Dienstkonten MSA eingesetzt werden, sowie im Sinn einer einheitlichen Konfiguration und Beschränkung der Komplexität möglichst auch die Gruppe "Managed Service Account".
	
	LSA-Schutz in Windows Server 2012 R2
	
	Die Local Security Authority (LSA), die den Local Security Authority Server Service (LSASS)-Prozess umfasst, authentisiert Benutzer bei lokalen und Netzanmeldungen und setzt die lokalen Sicherheitspolicies durch. Windows 8.1 und Windows Server 2012 R2 bieten zusätzliche Schutzmechanismen dafür, die ein Auslesen von Speicher sowie eine Injektion von Code erschweren. Dies erhöht den Schutz für Credentials, die in der LSA

	gespeichert und verwaltet werden, etwa gegenüber Pass-the-Hash-Angriffen. Auch Smartcard-Daten inklusive PINs sind dort abgelegt. Dazu ist in der Registry unter "HKEY_LOCAL MACHINE > SYSTEM > CurrentControlSet > Control > Lsa" ein DWORD (32-bit) des Namens "RunAsPPL" mit Inhalt "1" einzutragen und der Server neu zu starten. Alternativ geht dies auch über eine GPO (Computer Configuration > Windows Settings > Hive > **HKEY_LOCAL_MACHINE > SYSTEM\CurrentControlSet\Control\Lsa)**. Um die erfolgreiche Einrichtung zu überprüfen, sollte im Event Viewer unter Windows Logs > System nach folgendem WinInit-Event Ausschau gehalten werden: "LSASS.exe was started as a protected process with level: 4". In Kombination mit Secure Boot ist der Schutz besonders sicher, da er in dem Fall in UEFI generell aktiviert ist, unabhängig vom Inhalt der Registry. **Dynamische Zugriffsregeln** In Windows Server 2012 wurde die Möglichkeit geschaffen, für die Autorisierung dynamische Zugriffsregeln für Dateien und Ordner zu definieren. Da diese einen wesentlich schlankeren und dadurch leichter zu pflegenden Regelsatz erlauben können, sollte ihr Einsatz geprüft und bevorzugt werden, wenn nicht andere, betriebliche Gründe dagegen sprechen.
Fortschritt:	10% gemeldet am 29.09.2020 22:47
Fortschrittsmeldung:	.