BITMARCK®

Sicherheitsstandards für Systeme im BITMARCK Verbund

Fachkonzept

Version: 2

Stand: 06.11.2025

Klassifizierung: A1 - Eingeschränkte Weitergabe

Dokumentenverantwortliche(r):

Ahmadi, Tareq;Eller, Martin;

Codierung: BMH_FK_EW_Sicherheitsstandards für Systeme im BITMARCK Verbund

Dokumentinformationen

Klassifizierung	A1 - Eingeschränkte Weitergabe	**Gültig bis**	06.11.2027
		Status	Gültig
Dateiname	BMH_FK_EW_Sicherheitsstandards für Systeme im BITMARCK Verbund		
Mitgeltende Dokumente	[Mitgeltende Dokumente]		

Zielsetzung und Einordnung des Dokumentes

Dieses Dokument behandelt **verbindliche Vereinbarungen** zu **sicherheitsrelevanten Mindestanforderungen** für Systeme im BITMARCK-Verbund.

Unabhängig der Lokalität und den vereinbarten Zuständigkeiten über ein System können die Risiken eines Cyberangriffs nur mit gleichwertigen Sicherheitsstandards effektiv begegnet werden. Das schwächste Glied in der Lieferkette bestimmt die Sicherheit des BITMARCK-Verbunds. Daher ist es erforderlich, dass alle beteiligten Parteien geeignete Sicherheitsmaßnahmen umsetzen. Die **Anbindung der Systeme bestimmt** die möglichen Angriffsvektoren und damit **die Notwendigkeit für die abgestimmten Gegenmaßnahmen**.

Begriffe und Abkürzungen

Einem System im Sinne dieses Dokuments entspricht jegliche informationsverarbeitende Einheit. Dies bezieht sich sowohl auf Hardware als auch Software (Anwendungen) in allen Kombinationen und Ausprägungen.

© BITMARCK

Zielgruppe und Geltungsbereich

Diese Sicherheitsanforderungen gelten für folgende System-Kategorien und -Konstellationen:

1. **Systeme im Eigenbetrieb des Kunden oder Dienstleistungen Dritter**

   In diese Kategorie gehören alle Systeme der Kundinnen und Kunden bzw. Dienstleistenden, die

   - [S1] außerhalb des BITMARCK-Rechenzentrums als Server beim Kunden vor Ort und/oder von anderen Dienstleistern betrieben werden [externe Kundensysteme im Eigenbetrieb] und in irgendeiner Weise auf von BITMARCK verantwortete Systeme zugreifen,
   - [S2] sich im BITMARCK-Rechenzentrum befinden, aber als Server von anderen Dienstleistenden oder den Kunden selbst betreut und teilweise (z. B. Applikation) betrieben werden [interne Kundensysteme im Eigenbetrieb] und in irgendeiner Weise auf von BITMARCK verantwortete Systeme zugreifen,
   - [C] als Clients für den Zugriff auf BITMARCK-Dienste ausgelegt sind und von anderen Dienstleistenden oder den Kunden selbst betreut und betrieben werden (Kundenclients im Eigenbetrieb).

2. **Systeme im Betrieb durch BITMARCK**

   In diese Kategorie gehören alle BITMARCK-Systeme, welche für die Kundinnen und Kunden im Rahmen der Serviceerbringung betrieben oder ihnen zur Verfügung gestellt werden und BITMARCK dabei die Verantwortung im Sinne der Serviceverein-barung trägt (IaaS, PaaS oder SaaS).

© BITMARCK

Inhaltsverzeichnis

Dokumentinformationen **2**
Zielsetzung und Einordnung des Dokumentes **2**
Begriffe und Abkürzungen **2**
Zielgruppe und Geltungsbereich **3**
1 Sicherheitsanforderungen **5**
1.1 Technische Maßnahmen (T1-T9) **5**
1.2 Organisatorische Maßnahmen (O1-O12) **8**
2 Anhang A **10**
2.1 Erläuterungen zu den technischen Maßnahmen (T1-T9) **10**
2.2 Erläuterungen zu den organisatorischen Maßnahmen (O1-O12) **14**
3 Anhang B **19**
3.1 Anwendungsszenarien für den Einsatz der Security-Anforderungen bei Dienstleistenden **19**
4 Anhang C **21**
4.1 Verantwortlicheit für die Anwendung der Sicherheitsmaßnahmen **21**

© BITMARCK

1 Sicherheitsanforderungen

Die Mindestanforderungen definieren die Sicherheitsstandards für Systeme im Verantwortungsbereich von BITMARCK. Sie sind darauf ausgelegt, bei Anwendung auch für Systeme im Eigenbetrieb der Kundinnen und Kunden oder bei Drittanbietern ein gleichwertiges Sicherheitsniveau sicherzustellen. Diese Mindestanforderungen wurden unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der entstehenden Risiken ausformuliert.

Ziel ist es, das Schutzniveau im gesamten Verbund nachhaltig zu stärken.

Die Anbindung der genannten Systeme an die BITMARCK-Infrastruktur (z. B. AD, Filer, Exchange) sowie die Freigabe für die Kommunikation und Interaktion mit weiteren Kundensystemen (z. B. BITMARCK_21c|ng, bitAnalytics) im Verantwortungsbereich von BITMARCK erfolgt ausschließlich bei vollständiger Erfüllung der definierten Sicherheitsanforderungen.

Die konkreten Anwendungsbereiche dieser Anforderungen sind im Abschnitt „Zielgruppe und Geltungsbereich“ auf Seite 4 definiert. Beispiele zu besserer Einordnung der Anwendbarkeit werden im Anhang B ausgeführt.

Diese Sicherheitsanforderungen werden als technische und organisatorische Maßnahmen aufgeführt und sind sowohl für BITMARCK als auch für weitere Drittdienstleistende und für die Kunden von BITMARCK mit Systemen im Eigenbetrieb verpflichtend umzusetzen.

1.1 Technische Maßnahmen (T1-T9)

T1. Nutzung eines EDR-/XDR-Systems, welches neben Virensignaturen zusätzlich Angriffsverhalten erkennt und unterbindet.

- Das Fremdsystem kann diesbezüglich an das BITMARCK EDR-/XDR-System (nach passender vertraglicher Vereinbarung) angebunden werden.
- Falls kundenseitig – oder über Dritte – bereits eigene Systeme betrieben werden, wäre es ausreichend, die Alarmierungen des Systems an BITMARCK in geeigneter Form weiterzuleiten.

#Anwendungsbereich: S1, S2, C

T2. Nutzung eines SIEM-Systems, welches korrelierte Systemmeldungen nach Angriffsmustern untersucht und bei erkannten Angriffen alarmiert.

- Das Fremdsystem kann diesbezüglich an das BITMARCK-SIEM-System (nach passender vertraglicher Vereinbarung) angebunden werden.
- Falls kundenseitig – oder über Dritte – bereits eigene Systeme betrieben werden, sollen die Alarmierungen des Systems an BITMARCK in geeigneter Form weitergeleitet werden.

#Anwendungsbereich: S1, S2

T3. Regelmäßige Durchführung von technischen Sicherheitsprüfungen (z. B. Schwachstellen-Scans, Penetrationstests) und Behebung der erkannten Schwachstellen in angemessenem Zeitrahmen, abhängig von der Kritikalität.

- Das Fremdsystem kann diesbezüglich an den BITMARCK-Schwachstellen-Scanner (nach vertraglicher Vereinbarung) angebunden werden.
- Penetrationstests können vorbehaltlich einer vertraglichen Vereinbarung durch Mitarbeitende des Cyber Defence Teams von BITMARCK durchgeführt werden.
- Falls kundenseitig – oder über Dritte – bereits eigene Systeme betrieben werden, wäre es ausreichend, die Ergebnisse der Scans und die rechtzeitige Behebung von erkannten Schwachstellen regelmäßig an BITMARCK in geeigneter Form weiterzuleiten.

#Anwendungsbereich: S1, S2

T4. Für Kundensysteme im Eigenbetrieb müssen Härtungsmaßnahmen getroffen werden. Der BITMARCK müssen dazu grundlegende Informationen bereitgestellt werden.

- Grundlegende Mindestanforderungen sind in den nächsten Abschnitten (Details) zwecks Orientierung angegeben.
- Solche Maßnahmen und insbesondere deren Umfang hängen vom jeweiligen System und Nutzungsszenario ab, daher sind die Hersteller (z. B. Microsoft, Citrix, Cisco etc.) „Best Practice" bzw. „Hardening Guides" anzuwenden.

#Anwendungsbereich: S1, S2, C

T5. Segmentierung und Kontrolle des Netzwerks innerhalb und außerhalb vom BITMARCK Rechenzentrum (einschließlich Richtlinienkonformität der Endgeräte)

- Trennung von Netzwerksegmenten nach angebotener Angriffsfläche (z. B. zwischen Netzen mit Endbenutzersystemen und Servern für die Bereitstellung von lokalen Diensten), sodass Netzwerkzugriffe kontrolliert werden können.

#Anwendungsbereich: S1, S2, C

T6. Absicherung der administrativen Accounts auf BITMARCK- und Kunden-Systemen

- Verwaltung von privilegierten Zugängen gemäß gängigen Praktiken (z. B. Protokollierung der Aktionen, sichere Ablage von Anmeldedaten, Abkopplung von Endbenutzer-Systemen mittels Sprungserver).
- Einbindung der administrativen Kunden-Accounts auf BITMARCK-Systemen in das PAM-Modell von BITMARCK.

#Anwendungsbereich: S1, S2, C

T7. Verschlüsselung von Daten bei der Übertragung und bei der Speicherung (gemäß Schutzbedarf und technische Umsetzbarkeit).

- Die verschlüsselte Übertragung (Encryption in Transit) erschwert die Entwendung von Daten und Ausbreitung von Angreifenden im Netz.

© BITMARCK

- Die Verschlüsselung gespeicherter Daten (Encryption at Rest) soll dann erfolgen, wenn es sicherheitstechnisch einen Mehrwert bietet. Bei Clients ist eine Festplatten-Vollverschlüsselung (z.B. BitLocker) erforderlich.
- Der Schutzbedarf der verarbeiteten Daten und die Art des Zugriffs bestimmen die Verschlüsselungsvorgaben
- Die Verschlüsselung muss dem aktuellen Stand der Technik entsprechen

#Anwendungsbereich: S1, S2, C

T8. Die physischen Lokationen, in denen Server untergebracht sind, sind durch geeignete Maßnahmen vor dem Zugriff durch nicht autorisierte Dritte geschützt (Perimeterschutz).

- Server sind vom direkten physischen Zugriff geschützt.

#Anwendungsbereich: S1

T9. Der Zugriff auf Internet-Ressourcen ist über geeignete Maßnahmen unter Berücksichtigung des jeweiligen Zonenkonzepts abgesichert. Zum Beispiel:

- Es dürfen keine unreglementierten bzw. direkten Zugriffe ins Internet stattfinden.
- Verbindungen und Übertragungen müssen erst nach passenden Prüfungen von Inhalten und Legitimität erfolgen.

#Anwendungsbereich: S1, S2, C

© BITMARCK

1.2 Organisatorische Maßnahmen (O1-O12)

O1. Die vertragliche Basis für die Anbindung der Systeme enthält Regelungen zu folgenden Punkten:

- SLAs
- Betriebs- und Servicezeiten
- Mitwirkungspflichten
- RTO/RPO
- Verantwortlichkeiten gemäß einer RACI-Matrix
- Kommunikationskanäle/Eskalationsmatrix

#Anwendungsbereich: S1, S2, C

O2. Für „Technische Maßnahmen" 1 und 2 sind kundenseitig bzw. vom Dienstleister zuständige Personen und Rufbereitschaften (24/7) notwendig, welche bei Alarmierungen zur Klärung des Sachverhalts unterstützen und fachlich eingreifen können. Diese Personen benötigen geeignete technische Skills, da BITMARCK-Mitarbeitende das Fremdsystem weder kennen noch im Zugriff haben.
#Anwendungsbereich: S1, S2

O3. Es müssen Vereinbarungen über die Prüfung und die Behebung erkannter Schwachstellen getroffen werden. Anhand der Kritikalität der Schwachstelle schreiben diese zeitlichen Vorgaben zu deren Behebung vor und konkretisiert weitere Maßnahmen. Die Frequenz der Scans/Tests hängt dabei vom Schutzbedarf der verarbeiteten Daten ab.

#Anwendungsbereich: S1, S2, C

O4. Es müssen systembedingte Vereinbarungen über das Patch-Management getroffen werden (Mindestanforderungen in Anhang A zu O3 und O4). Der Patch-Zyklus muss dabei End-of-Life bzw. End-of-Support von verwendeten Systemen und/oder Softwarekomponenten respektieren.

#Anwendungsbereich: S1, S2, C

O5. Es existiert ein dokumentierter Change-Management-Prozess.

#Anwendungsbereich: S1, S2

O6. Es existiert ein dokumentierter Konfigurationsmanagement-Prozess, gestützt von geeigneten Tools.

#Anwendungsbereich: S1, S2

O7. Die Kundinnen und Kunden bzw. Dienstleistende unterhalten Richtlinien zur Informationssicherheit für die relevanten Bereiche, z. B. Netzwerksicherheit, Kryptografie, Identitäts- und Rechtemanagement, Protokollierung und physische Sicherheit. Der Inhalt orientiert sich dabei am Stand der Technik in Form anerkannter Standards (ISO27001, BSI, B3S, usw.).

© BITMARCK

#Anwendungsbereich: S1, S2, C

O8. Es besteht ein Identitäts- und Rechtemanagement (Access Management) nach dem Least-Privilege- bzw. Need-to-Know-Prinzip.

#Anwendungsbereich: S1, S2, C

O9. Auf Seiten der Kundinnen und Kunden bzw. des Dienstleistenden ist eine geeignete Rolle (z. B. eine beauftragte Person für Informationssicherheit) vorhanden, welche grundlegende Themen der Informationssicherheit bedienen kann.

#Anwendungsbereich: S1, S2, C

O10. Es existiert ein Business Continuity Management inkl. Notfallhandbuch und Desaster-Recovery-Pläne.

#Anwendungsbereich: S1, S2

O11. Alle genannten Anforderungen gelten uneingeschränkt für alle weiteren untergeordneten Dienstleistenden, die für die Erbringung des jeweiligen Services involviert sind.

#Anwendungsbereich: S1, S2, C

O12. BITMARCK behält sich das Recht vor, Systeme, welche direkt mit der Infrastruktur in den BITMARCK-Rechenzentren verbunden sind, auf die Einhaltung der oben genannten Anforderungen zu prüfen bzw. prüfen zu lassen. Die Prüfung wird in der Regel anlassbezogen erfolgen.

Bei Nicht-Einhaltung der Sicherheitsanforderungen und erhöhtem Risiko darf die Verbindung dieser Systeme zur BITMARCK-Infrastruktur ausgeschlossen bzw. unterbrochen werden.

#Anwendungsbereich: S1, S2, C

© BITMARCK

2 Anhang A

Details zu besserer Einordnung der oben aufgeführten technischen und organisatorischen Maßnahmen.

2.1 Erläuterungen zu den technischen Maßnahmen (T1-T9)

T1. EDR-/XDR-System

- Ein EDR-System ist die Mindestanforderung für Server und Client.
- Im Falle der Nutzung des BITMARCK-EDR-Systems müssen die erforderlichen Lizenzen durch BITMARCK beschafft werden.
    - Die Kundinnen und Kunden verpflichten sich, die benötigte Anzahl an Lizenzen zu ermitteln und BITMARCK mitzuteilen.
    - Im Falle einer Unterlizensierung basierend auf den kundenseitig genannten Zahlen behält sich BITMARCK das Recht vor, die zusätzlich nötigen Lizenzen zu beschaffen und dem Kunden in Rechnung zu stellen.
    - Die Installation des Agenten auf dem Kundensystem obliegt den Kundinnen und Kunden oder seinen Dienstleistenden, sofern nicht anders vereinbart.
    - Die Anbindung an die passende Infrastruktur erfolgt durch BITMARCK.
- Falls kundenseitig – oder über Dritte – bereits solche Systeme betrieben werden und eine Integration stattfinden soll, müssen unter Mitwirkung beider Seiten
    - die meldepflichtigen Ereignisse festgelegt werden,
    - die passende Form der Weiterleitung der sicherheitsrelevanten Ereignisse festgelegt werden (u. a. Übertragungsprotokoll, Format der Daten).

T2. SIEM-System

- Die Anbindung an das SIEM-System ist für Server die Mindestanforderung. Für Clients dagegen ist die Anbindung optional.
- Protokolldateien müssen durch technische Maßnahmen vor Manipulation geschützt werden.
- Falls das BITMARCK-SIEM-System genutzt werden sollte, müssen die erforderlichen Lizenzen beauftragt werden.
    - Die beauftragende Person verpflichtet sich, die benötigte Anzahl an Lizenzen eigenständig zu ermitteln und BITMARCK mitzuteilen.
    - Im Falle einer Unterlizensierung basierend auf den kundenseitig genannten Zahlen behält sich BITMARCK das Recht vor, die zusätzlich nötigen Lizenzen zu beschaffen und dem Kunden in Rechnung zu stellen.

© BITMARCK

    - Die Konfiguration am Kundensystem für die Weiterleitung der passenden Meldungen obliegt den Kundinnen und Kunden oder deren Dienstleistenden in Abstimmung mit und unter Hilfestellung von BITMARCK.
    - Die Anbindung an die passende Infrastruktur erfolgt durch BITMARCK.
- Falls kundenseitig – oder über Dritte – bereits solche Systeme betrieben werden und eine Integration stattfinden soll, müssen unter Mitwirkung beider Seiten
    - die meldepflichtigen Ereignisse festgelegt werden,
    - die passende Form der Weiterleitung der sicherheitsrelevanten Ereignisse festgelegt werden (u. a. Übertragungsprotokoll, Format der Daten).

T3. Technische Sicherheitsprüfung

- Regelmäßige Schwachstellen-Scans sind die Mindestanforderung für Server und Client (mindestens monatliches Intervall).
- Bei besonders kritischen oder exponierten Systemen sind regelmäßige Penetrationstests für die betroffene Software durchzuführen (mindestens jährliches Intervall).
- Bei besonders exponierten oder kritischen Services muss eine Angriffssimulation (Red-Teaming) erfolgen.
    - BITMARCK behält sich vor, bei besonders kritischen Systemen eine derartige Überprüfung einzufordern.
- Falls der BITMARCK-Schwachstellen-Scanner genutzt werden sollte, müssen die erforderlichen Lizenzen beauftragt werden.
    - Die Kundinnen und Kunden verpflichten sich dazu, die benötigte Anzahl an Lizenzen eigenständig zu ermitteln und diese BITMARCK mitzuteilen.
    - Im Falle einer Unterlizensierung basierend auf den kundenseitig genannten Zahlen behält sich BITMARCK das Recht vor, die zusätzlich nötigen Lizenzen zu beschaffen und in Rechnung zu stellen.
    - Die Konfiguration von passenden Kennungen für den Scanner auf dem Kundensystem – sofern notwendig – obliegt den Kundinnen und Kunden oder deren Dienstleistenden.
    - Die Berichte der Schwachstellen-Scans werden durch BITMARCK bereitgestellt.
- Falls kundenseitig – oder über Dritte – bereits solche Systeme betrieben werden, müssen nur die Berichte regelmäßig bereitgestellt werden.
    - Die Form dieser Berichte muss einmalig festgelegt werden.

T4. Härtung

Die Härtung ist eine Mindestanforderung für Server und Clients. Es sollten die von jeweiligem Hersteller bereitgestellte Hardening Guides und Sicherheitsempfehlungen von anerkannten Institutionen (z.B. BSI, NIST) zur Anwendung kommen.

Zum Beispiel:

- Verwendung von Netzwerkprotokollen nach dem jeweils geltenden Stand der Technik
- Die ausschließliche Verwendung von für den Unternehmensbereich geeigneter Dienste, Technologien und Anwendungen im Sinne des Services
- Deinstallation bzw. Deaktivierung von irrelevanten Komponenten

- Es sind nur die absolut notwendigen Dienste über das Netzwerk erreichbar.
- Netzwerkverbindungen müssen einer risikobasierten Bewertung unterzogen werden und besonders riskante Verbindungen müssen abgestellt oder mit wirksamen Maßnahmen abgesichert werden.
- Netzwerkprotokolle müssen in der jeweils sichersten Variante (Stand der Technik) eingesetzt werden.

- Passwortrichtlinien und Bildschirmsperren sind technisch zu erzwingen.

- Technische Accounts (z. B. Datenbankanbindung, Software-Schnittstellen, Automatisierungszugänge) sind mit hinreichend starken Passwörtern zu sichern und sofern möglich deren interaktive Nutzung bzw. der Remote-Zugriff zu verhindern.

<u>T5. Netzwerksegmentierung</u>

- Das Client-Netz ist wohldefiniert und von Server-Netzen mittels Firewalls getrennt.

- Produktionssysteme stehen in einem abgetrennten Netz.

- Die Firewall-Konfiguration ist nur auf die notwendigste Kommunikation beschränkt, d. h. die Standardeinstellung lautet „Deny All“.

- Aus dem Internet erreichbare Systeme sind in dedizierte Netzwerksegmente (DMZ) abgeschottet. Aus der DMZ sind nur nach zusätzlichen Absicherungsmaßnahmen die absolut notwendigsten Verbindungen ins interne Netz erlaubt.
- Die Zugriffe vom internen Netz (Endbenutzersysteme) ins Internet sind durch passende Maßnahmen abgesichert.
- Aus Admin-Sprungservern dürfen keine Verbindungen in das Internet oder aus dem Internet heraus erfolgen.

- Als **intern** gekennzeichnete Systeme dürfen **keine direkte** Verbindung (weder ein- noch ausgehend) zum Internet haben.

<u>T6. Tiering-Modell und PAM</u>

- Administrative Aufgaben werden nur von einem für diesem Zweck bereitgestellten Admin-Sprungserver ausgeübt.

- Nur dedizierte administrative Kennungen werden passend zum jeweiligen Security-Tier für administrative Aufgaben genutzt und mittels MFA abgesichert.
- Der Zugriff auf den Sprungserver bzw. auf ein Zielsystem im BITMARCK-Rechenzentrum für die Ausübung administrativer Tätigkeiten wird durch ein von BITMARCK bereitgestelltes PAM-System reglementiert.

T7. Verschlüsselung

- Die Netzwerkkommunikation hat ausschließlich verschlüsselt zu erfolgen. Zum Beispiel ist nur die Verwendung von TLS1.2 oder höher zulässig (Stand 2025).
- Die Verschlüsselung von ruhenden Daten hat mindestens über eine Festplattenverschlüsselung oder eine Dateiverschlüsselung zu erfolgen.
- Für die Verschlüsselung sind nur zeitgemäße und als sicher eingestufte Verschlüsselungsalgorithmen (Ciphers) zu verwenden (z. B. AES gilt, als sicher vs. RC4 oder DES gelten als unsicher). Die BSI-Empfehlungen zur Kryptographie gelten als Maßgabe für die Auswahl von sicheren Verschlüsselungsalgorithmen.
- Auf Clients mit Anbindung an das BITMARCK AD (Active Directory) sind für die sichere Authentifizierung BITMARCK-Maschinen-Zertifikate zu installieren.

T8. Perimeterschutz für Serverräume

- Abgeschlossene Serverräume mit eingeschränktem Kreis der Zutrittsberechtigten sind Pflicht.
- Zutrittskontrolle mit mehreren Faktoren (z. B. Smartcard, PIN) und/oder Videoüberwachung sind wünschenswert

T9. Internet-Zugriff

Im Rahmen eines Netzwerkzonenkonzepts (standardisierter Internetzugang von BITMARCK) müssen passende Vorkehrungen getroffen werden.

Zum Beispiel:

- Der Zugriff auf Internet-Ressourcen wird über geeignete Security-Systeme abgesichert (z. B. Safe-Browsing, NGFW-Security-Gateways, Proxy).
- Es findet eine Überprüfung von bekannten Angriffsmustern statt (z. B. IPS-Regeln für die jeweils passende Kommunikation, DNS-Tunneling).
- Bekannte Malware-Domains werden geblockt (setzt kontinuierlich aktualisierte Block Listen voraus).
- Datei-Downloads werden nach bekannter Malware überprüft (Malware-Signaturen müssen ständig aktuell gehalten werden).
- Besonders sicherheitsanfällige bzw. unsichere Netzwerk-Protokolle müssen unterbunden werden.

© BITMARCK

2.2 Erläuterungen zu den organisatorischen Maßnahmen (O1-O12)

O1. Vertragsunterlagen

- SLAs beschreiben die Reaktions- und Lösungszeiten von Vorfällen und Problemen.
- Betriebszeiten beschreiben, in welchen Zeiträumen der jeweilige Service betrieben wird.
- Servicezeiten beschreiben, in welchen Zeiträumen der Regelbetrieb erfolgt.
- Mitwirkungspflichten klären Verantwortlichkeiten, ohne die z. B. eine Entstörung nicht erfolgen kann.
- RTO/RPO beschreiben den vorgesehenen Zeitraum bis zur Entstörung eines Dienstes nach Totalausfall und den maximalen Verlustzeitraum von Daten (bspw. relevant für Backupintervall).
- Eine RACI-Matrix stellt Verantwortlichkeiten auf verschiedenen Ebenen zwischen den Parteien dar und bestimmt so u.a. die Kommunikationswege.
- Kommunikationswege und insbesondere Eskalationsmatrizen helfen bei der schnellen und reibungslosen Kommunikation insbesondere in Ausnahmesituationen.

O2. Ansprechpersonen und Rufbereitschaften

In Abstimmung und Mitwirkung beider Parteien müssen mindestens folgende Meldewege und der Umgang mit sicherheitsrelevanten Ereignissen festgehalten werden:

- Festlegung eines Meldeprozesses
    - Wer kontaktiert unter welchen Voraussetzungen (z. B. betroffenes System, Kritikalität) welche Ansprechperson?
    - Festlegung von 24/7-Rufbereitschaften
- Erstellung einer Kommunikationsmatrix
    - Auflistung der geeigneten Kontakte anhand der technischen Skills zu den Ereignissen und der dazu benötigten Kommunikationskanäle
- Ausarbeitung eines Eskalationsplans
    - Vereinbarung von Reaktionszeiten und der nächsthöheren Stufe für die Meldung eines Ereignisses, falls Reaktionen ausbleiben oder die Kritikalität sich erhöht hat.
    - Standardmaßnahmen bei leichtgewichtigen Ereignissen
    - Notfall-Handlungen bei schwerwiegenden Vorkommnissen

Diese organisatorische Maßnahme ist von immenser Bedeutung, da ohne Unterstützung von den Fachpersonen des jeweiligen Systems nur die Abtrennung (Netz) dieses Systems als „Ultima Ratio"-Reaktion auf eine Alarmierung bleibt.

O3. Umgang mit Schwachstellen

- Die Erfassung von Schwachstellen darf nicht nur durch automatisierte Verfahren (z. B. Schwachstellen-Scanner) erfolgen, sondern muss auch durch die zuständige Fachabteilung (z. B. aus Hersteller-Meldungen) aktiv überwacht werden.
- Schwachstellen von Systemen, welche **nicht** von BITMARCK betreut und verantwortet werden (z. B. Applikationen auf Hosting-Server), müssen der BITMARCK von der zuständigen Fachabteilung der Kundinnen und Kunden oder deren Dienstleistenden gemeldet werden.
- Schwachstellen müssen zeitnah bewertet werden, sodass diese nach Kritikalität behandelt werden können.
- Der CVSS-Score (Kritikalitätsbewertung) wird durch Herstellerangaben und vertrauenswürdige Instanzen (z. B. BSI, NIST), aber auch durch internes Wissen über den Einsatzzweck und die Konfiguration eines Systems festgelegt.
- Die Behebung von Schwachstellen anhand deren Kritikalität muss in den vom BSI empfohlenen Fristen erfolgen (z. B. UP KRITIS: Best-Practice-Empfehlungen für Anforderungen an Lieferanten). Innerhalb dieser Fristen muss eine Aktualisierung mit vom Hersteller gelieferten Patches oder Hotfixes stattfinden oder ein wirksamer Workaround implementiert werden.
- Bei langanhaltenden Arbeiten zur Behebung von Schwachstellen müssen passende Gegenmaßnahmen (z. B. Isolation von Systemen und/oder Netzen) für einen bestimmten Zeitraum festgelegt werden.

O4. Patch-Management und Umgang mit End-of-Life-Systemen

- Das regelmäßige Patch-Management ist verpflichtend.
    - Mindestens monatliche Aktualisierungen sind bei den meisten Systemen gängige Praxis. Eine Patch-Management Richtlinie nach BSI-Empfehlungen muss die geltenden Vorgaben festlegen.
    - Applikationen mit abweichenden, aber festgelegten Release-Plänen müssen passend erfasst und bekannt gemacht werden.
- End-of-Life-Systeme und -Anwendungen müssen rechtzeitig auf eine vom Hersteller unterstützte und gepflegte Version (mit Security-Patches) aktualisiert werden.
- Die Hersteller-Meldungen über End-of-Life müssen von der zuständigen Fachabteilung überwacht werden, sodass rechtzeitig eine Umstellung möglich ist.
- Spätestens einen Monat nach End-of-Life eines Systems bzw. einer Anwendung – oder früher falls eine schwerwiegende Schwachstelle bekannt wurde – muss dieses System bzw. diese Anwendung außer Betrieb genommen werden.

O5. Change-Management

- Prozesse zur Änderung von IT-Systemen sind abhängig von Art, Umfang, Komplexität und Risiko gestaltet und umgesetzt.

- Der Prozess deckt u. a. folgende Vorgänge ab:
    - Funktionserweiterung oder Fehlerbehebung von Softwarekomponenten
    - Datenmigrationen
    - Änderungen an Konfigurationseinstellungen
    - Austausch von Hardwarekomponenten
    - Physischer Umzug von Systemen

O6. Konfigurationsmanagement

- Die Klassifizierung der Systeme muss anhand deren Kritikalität für die involvierten Geschäftsprozesse und Sensibilität der verarbeiteten Daten erfolgen.
- Die CMDB listet alle IT-Systeme und deren Beziehung untereinander auf.
- Es werden dort mindestens folgende Informationen dokumentiert:
    - Konfigurationsangaben der Systeme (z. B. Patchlevel)
    - Eigentümer der Systeme
    - Standort der Systeme
    - Angaben zu Gewährleistungen und sonstigen Supportverträgen
    - Angaben zum Ablaufdatum des Supports
    - Schutzbedarfsklasse
    - RTO/RPO
- Die CMDB wird regelmäßig sowie anlassbezogen aktualisiert.

O7. Informationssicherheitsrichtlinien

- Die Existenz dieser Richtlinien dient in erster Linie dazu, Prozesse zu definieren, um die Einhaltung vereinbarter Schutzziele (z. B. Vorbeugung von Informationssicherheitsvorfällen) zu erreichen.
- Diese Richtlinien definieren die Vorgaben zu Netzwerksicherheit, den Einsatz von Kryptografie, die Regelungen zu Passwortbeschaffenheit, die Vorgaben zu Identitäts- und Rechtemanagement, die Pflichten und Umfang der Protokollierung, usw. und müssen anerkannte Standards und Best Practices entsprechen.
- Es ist wichtig bei der Erstellung solcher Richtlinien den aktuellen Stand der Technik zu berücksichtigen und dementsprechend regelmäßig zu aktualisieren.
- Zur Ermittlung der benötigten Richtlinien kann man sich an Vorgaben von der ISO 27001 (inkl. den Erläuterung der ISO27002), BSI-Grundschutz, B3S, usw. orientieren.

O8. Access Management

- Berechtigungen werden nach dem Minimalprinzip vergeben.

- Die Least-Privilege-Berechtigungen sind nicht nur für personalisierte, sondern auch für technische Benutzende sowie auf unterschiedlichen Ebenen (z. B. Betriebssystem, Anwendung, Datenbank) durchzusetzen.
- Automatisierte Aktivitäten müssen verantwortlichen natürlichen Personen zugeordnet werden können, auch wenn diese von technischen Nutzenden durchgeführt werden.
- Einrichtung, Änderung und Deaktivierung oder Löschung von Berechtigungen und Zugängen müssen zeitnah und unverzüglich erfolgen.
- Berechtigungen und Zugänge werden mindestens jährlich überprüft und festgestellte Abweichungen zeitnah bereinigt.
- Administrative Berechtigungen dürfen **nicht** regulären Kennungen zugeordnet sein. Für administrative Aufgaben werden ausschließlich dedizierte Kennungen genutzt.
- Die interaktive Nutzung einer administrativen Kennung hat über personalisierte Accounts zu erfolgen.
- Administrative Aufgaben dürfen nur über dedizierte Admin-Sprungserver erfolgen.
- Der Zugang zu den Admin-Sprungserver wird durch MFA abgesichert.

O9. Informationssicherheit

Der ISB erstellt Informationssicherheitsrichtlinien und steuert die daraus resultierenden Prozesse.

- Ist an der Erstellung und Fortschreibung des Notfallkonzepts beteiligt
- Überwacht die Einhaltung der Informationssicherheit im Unternehmen
- Dient als verantwortliche Ansprechperson für Fragen und Anliegen rund um die Informationssicherheit (insbesondere bei Sicherheitsvorfällen)
- Berät zu Informationssicherheitsaspekten bei der Einführung von neuen Systemen.

O10. Business Continuity Management (BCM)

- Ein Business Continuity Management regelt das Verhalten in Notfällen und den Prozessablauf bis zur Rückkehr in den Normalbetrieb mit dem Ziel, den Ausfall so gering wie möglich zu halten.
- In einem Notfallhandbuch sind konkrete Handlungsanweisungen festgehalten, wie in bestimmten Notfällen (z. B. Cyberangriffe) zu verfahren ist (z.B. wer zu welchem Zeitpunkt informiert werden muss)
- In einem Desaster-Recovery-Plan ist festgelegt, wie ein Notbetrieb erfolgt und welche Schritte unternommen werden, um den Normalbetrieb nach einem Desaster Case wiederherzustellen.

O11. Weiterverlagerung

- Die obenstehenden Regelungen, die zwischen Dienstleistenden, BITMARCK und den Kundinnen und Kunden vereinbart werden, müssen an weitere Dienstleistende

mit Zugriff auf Systeme bzw. mit Systemen in Betreuung/Entwicklung im BITMARCK-Rechenzentrum durch die Kundinnen und Kunden durchgereicht und vertraglich vereinbart werden.

- Für die Rechner eines Dienstleistenden sind die technischen Maßnahmen (T1-T9) nur bei einer vollwertigen Netzwerkverbindung (MPLS/VPN) mit Systemen im BITMARCK-Rechenzentrum notwendig. Bei Dienstleistungen (z. B. Support) ausschließlich über CAG-Verbindungen (Remote Desktop ohne jegliche Dateiübertragungen) würden solche Maßnahmen keinen großen Sicherheitszugewinn bringen und sind daher obsolet. Bespiele zur Anwendbarkeit dieser Sicherheitsanforderungen für Dienstleister sind in Anhang B aufgeführt.

<u>O12. Prüfung</u>

- Die risikobasierte Prüfung erfolgt zusammen mit Bereibenden/Verantwortlichen des Systems.
- Für eine Prüfung ist die Einsicht der Unterlagen/Dokumentationen notwendig.
- Die Prüfung kann auch in Form eines Penetrationtests oder eines Schwachstellenscans erfolgen.
- Der Ausschluss bzw. Trennung der Verbindung mit der BITMARCK-Infrastruktur dient ausschließlich der Risikoreduktion für die übrige Infrastruktur. Damit sollen die Auswirkungen einer Kompromittierung des betroffenen Systems auf die Infrastruktur und damit auf andere Kundenprozesse reduziert werden.

© BITMARCK

3 Anhang B

3.1 Anwendungsszenarien für den Einsatz der Security-Anforderungen bei Dienstleistenden

Nachfolgende exemplarische Szenarien zur besseren Einordnung der Anwendbarkeit der Security-Anforderungen bei Dienstleistenden / Unterauftragsnehmenden / Lieferantinnen und Lieferanten.

Ausschlaggebend für die Anwendung der Security-Anforderungen ist die Art der Anbindung der Fremdsysteme mit Systemen in der Verantwortung von BITMARCK (überwiegend in BITMARCK-Rechenzentren).

Szenarien mit Pflicht zur **vollständigen Anwendung** der Security-Anforderungen bei Dienstleistenden

1. Das Fremdsystem mit dem Zugriff auf Systeme in der Verantwortung von BITMARCK befindet sich **außerhalb** des BITMARCK-Rechenzentrums beim Dienstleistenden und für den Zugriff ist ein vollwertiger Netzwerkzugang (z. B. VPN, MPLS) vorhanden. Hierzu gehören auch Zugriffe über HTTPS auf internen Systemen außerhalb der Internet-DMZ.
2. Das Fremdsystem mit dem Zugriff auf Systeme in der Verantwortung von BITMARCK befindet sich **im** BITMARCK-Rechenzentrum. Es wird aber vom Dienstleistenden **vollumfänglich** (Housing, Full-Service-Dienstleistung) betrieben und betreut. Außerdem besteht eine dauerhafte Netzwerkverbindung mit dem Dienstleistenden (damit ist **nicht** der temporäre CAG-Zugang des Dienstleistenden gemeint).

Szenarien **ohne Pflicht zur Anwendung** der Security-Anforderungen bei Dienstleistenden

a. Die bzw. der Dienstleistende ist nur Lieferantin bzw. Lieferant von Soft- und/oder Hardware und hat **keinen** Zugriff auf die Systeme im BITMARCK-Rechenzentrum.
b. Die bzw. der Dienstleistende greift ausschließlich mittels CAG der bzw. des Dienstleistenden auf ein System in BITMARCK-Betrieb und -Betreuung zu, welches sich im BITMARCK-Rechenzentrum befindet. In diesem Fall werden die Security-Anforderungen von BITMARCK geleistet.
c. Die bzw. der Dienstleistende hat außer einer standarisierten Dateiübertragung über BITMARCK-Produkte (z. B. SFTP über Datacenter) keinen weiteren direkten Zugriff auf ein System in der Verantwortung von BITMARCK. Wichtig: SMB- oder NFS-Übertragungen sind wegen der Betriebssystemabhängigkeiten nicht Gegenstand dieses Anwendungsfalls, sondern gehören zum ersten Szenario.
d. Die bzw. der Dienstleistende greift auf öffentliche (ins Internet publizierte) Schnittstellen und Systeme zu. Meistens kommen in diesem Fall HTTPS-Verbindungen zum Einsatz. Hier sind die Security-Anforderungen durch BITMARCK zu leisten.

Szenarien mit Pflicht zur **partiellen Anwendung** der Security-Anforderungen bei Dienstleistenden

Ein Teil dieser Security-Anforderungen werden in dieses Szenario **bereits** durch die **BITMARCK geleistet**

i. Das System befindet sich im BITMARCK-Rechenzentrum. Die Basisdienstleistung (z. B. Betriebssystem) wird von BITMARCK geleistet (Hosting), aber die Applikation wird von Dienstleistenden betrieben und betreut.

ii. Das System befindet sich **außerhalb** des BITMARCK-Rechenzentrums bei Dienstleistenden, wird aber von BITMARCK betrieben und betreut (damit liegt die Verantwortung bei BITMARCK).

Die letzte Kategorie (partielle Anwendung) bedarf im **Einzelfall einer Ermittlung der zutreffenden Security-Anforderungen**.

Der Zugriff von BITMARCK-Systemen auf Systeme von Dienstleistenden sind in diesen Szenarien nicht berücksichtigt, da in diesem Fall BITMARCK diese Security-Anforderungen erfüllen muss.

© BITMARCK

4 Anhang C

Hilfestellung zur besseren Einordnung der Zuständigkeiten für die Anwendung der oben aufgeführten Sicherheitsmaßnahmen.

4.1 Verantwortlicheit für die Anwendung der Sicherheitsmaßnahmen

Verantwortlichkeitsmatrix

Legende:
K = Kunde
B = BITMARCK
K/B = Kunde und BITMARCK

Die Einträge sind im Sinne einer RACI-Matrix als „Accountable/Responsible“ zu verstehen.

	Rechenzentrum der BITMARCK										RZ Kunde	RZ DL
	Housing	Managed Server, bis zum Übergang zur Anwendungsebene	Managed Server, Applikation im Eigenbetrieb des Kunden	BITMARCK Managed Database	Managed Platform, bis zum Übergang zur Anwendungsebene	Managed Platform, Applikation im Eigenbetrieb des Kunden	BITMARCK Managed Application	Webzugriff/Proxy	BITMARCK Managed WAN	BITMARCK Managed VPN	Eigenbetrieb des Kunden	RZ eines Drittdienstleisters
T1 Nutzung eines EDR/XDR-Systems	K	B	K	B	B	K	B	B	B	B	K	K
T2 Nutzung eines SIEM-Systems	K	B	K	B	B	K	B	B	B	B	K	K
T3 Regelmäßige Sicherheitsprüfungen	K	B	K	B	B	K	B	B	B	B	K	K
T4 Hardening-Maßnahmen	K	B	K	B	B	K	B	B	B	B	K	K
T5 Segmentierung und Kontrolle des Netzwerks	K	B	-	B	B	K	B	B	B	B	K	K
T6 Absicherung der administrativen Accounts	K	B	K	K	B	K	K	-	-	-	K	K
T7 Verschlüsselung von Daten	K	B	K	B	B	K	B	B	B	B	K	K
T8 Perimeterschutz	B	B	-	B	B	-	B	B	B	B	K	K
T9 Absicherung des Internet-Zugriffs	K	B	K	B	B	K	B	B	B	B	K	K
O1 Vertragliche Basis schaffen	K/B	K/B	-	K/B	K/B	-	K/B	K/B	K/B	K/B	-	K
O2 Rufbereitschaft und Verantwortung für T1&2	K	B	K	B	B	K	B	B	B	B	K	K
O3 Prüfung und Behebung von Schwachstellen	K	B	K	B	B	K	B	B	B	B	K	K
O4 Patchmanagement	K	B	K	B	B	K	B	B	B	B	K	K
O5 Change Management Prozess	K	B	K	B	B	K	B	B	B	B	K	K
O6 Konfigurationsmanagement Prozess	K	B	K	B	B	K	B	B	B	B	K	K
O7 Richtlinien zur Informationssicherheit	K	B	K	B	B	K	B	K/B	B	B	K	K
O8 Identitäts- und Rechtemanagement	K	B	K	B	B	K	B	B	B	B	K	K
O9 Beauftragter für Informationssicherheit	K	B	K	B	B	K	B	B	B	B	K	K
O10 Business Continuity Management	K	B	K	B	B	K	B	B	B	B	K	K
O11 Geltungsbereich auch für Dienstleister	K	B	K	B	B	K	B	B	B	B	K	K
O12 Prüfungsrecht der BITMARCK	K/B	-	K/B	-	-	K/B	-	-	-	-	K/B	K/B

© BITMARCK