Michael Doß

SYS: Dezentrale Systeme

SYS.5.1 Blockchain und Distributed Ledger Technologien

1. Beschreibung

1.1 Einleitung

Die Blockchain in Verbindung mit Distributed Ledger Technologien (DLT) ist ein dezentraler Ansatz für eine fälschungssichere, unveränderliche, redundante und nachvollziehbare Bereitstellung von Informationen in einem Netzwerk gleichberechtigter Peers ohne zentrale Instanz.

Das fälschungssichere und unveränderliche Speichern von Informationen findet in der Blockchain mittels kryptografischer Verfahren wie bspw. digitale Signaturen und kryptografische Hashfunktionen statt. Nachvollziehbarkeit erreicht die Blockchain über die Verkettung ihrer Hashblöcke, wodurch Änderungen an jeder Position auffallen.

Distributed Ledger Technologien sorgen mit Hilfe von Public Key Verfahren, verteilte Peer-to-Peer-Netzwerke (P2P) sowie einem Konsensalgorithmus für Redundanz und Einheitlichkeit unter den verteilten Datenstrukturen und sorgen damit für Dezentralität ohne die Einbindung einer zentralen Autorität. Der Konsensalgorithmus stellt in diesem Rahmen sicher, dass sich alle Teilnehmenden im Netzwerk über den aktuellen Status der Blockchain einig sind.

Eine weitere Fähigkeit ist die Fault Toleranz. In Bezug auf Blockchain und DLT besteht sie darin, dass das Netzwerk robust gegenüber ausfallenden oder fehlerhaften Knoten ist, um Integrität, Verfügbarkeit, Authentizität und Nichtabstreitbarkeit zu gewährleisten.

Zur Automatisierung existiert, in vielen Blockchains, die Möglichkeit Smart Contracts (intelligente selbstausführende Verträge) zu verwenden. Diese sind automatisierte Programme bzw. eine Form von Software, die auf einer Blockchain-Plattform automatisch Aktionen ausführt, sobald bestimmte Bedingungen erfüllt sind.

Um möglichst allgemeingültig zu bleiben, wurden die Blockchains und DLT, in Abhängigkeit der Ähnlichkeit ihrer Merkmale, in Geltungsbereiche bzw. Cluster eingeteilt. Diese sind mit Cluster0 bis Cluster4 durchnummeriert, da eine Benamung über prägende Merkmale nicht möglich ist.

1.2 Zielsetzung

Ziel dieses Bausteines ist es, den Einsatz einer Blockchain und DLT abzusichern und zu erleichtern, um Integrität, Verfügbarkeit, Authentizität, Vertraulichkeit und die Unveränderlichkeit aufgrund der Verkettung der Blöcke unter Verwendung des Hash-Wertes zu gewährleisten. Dazu stellt dieser Baustein Anforderungen bereit, um spezifischen Gefährdungen entgegenzuwirken und die Blockchain und DLT sicher zu betreiben. Er richtet sich zentral an

Informationssicherheitsbeauftragte (ISB) der jeweiligen Institutionen sowie dezentral an Administrierende von Blockchains und DLT, wodurch Sicherheitsanforderungen gemäß dem Security By Design Ansatz so früh wie möglich bereits bei der Planung und der Entwicklung berücksichtigt werden können.

1.3 Abgrenzung und Modellierung

Der Baustein **SYS.5.1** *Blockchain und Distributed Ledger Technologien* ist einmal auf jedem Knoten im Peer-to-Peer-Netzwerk (P2P) der Distributed Ledger Technologie anzuwenden, auf dem eine dezentrale Kopie einer Blockchain vorhanden ist.

Der Baustein **SYS.5.1** *Blockchain und Distributed Ledger Technologien* ist immer anzuwenden, sobald eine Blockchain und Distributed Ledger Technologien unabhängig vom Typ oder Cluster zum Einsatz kommen.

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

- allgemeine Sicherheitsaspekte von Blockchain und Distributed Ledger Technologien,
- Anforderungen zur Abdeckung der wichtigsten Angriffsvektoren,
- eine Betrachtung der Blockchain und Distributed Ledger Technologien in Cluster unabhängig vom eingesetzten Produkt.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:
(In den aufgelisteten IT-Grundschutz-Bausteinen sind Anforderungen vorhanden auf denen der Baustein **SYS.5.1** *Blockchain und Distributed Ledger Technologien* aufbaut.)

- Absicherung und Umgang mit Hardware (siehe:
- **INF.1** Allgemeines Gebäude, **INF.2** Rechenzentrum sowie Serverraum,
  INF.2 Raum sowie Schrank für technische Infrastruktur,
- **SYS.1.1** Allgemeiner Server,
- **NET.1.1** Netzarchitektur und -design, **NET.3.1** Router und Switches, **NET.3.2** Firewall,
- **OPS.1.1.1** Allgemeiner IT-Betrieb, **OPS.1.1.2** Ordnungsgemäße IT-Administration,
  OPS.1.1.4 Schutz vor Schadprogrammen),
- Kryptographie und Datensicherheit (siehe:
- **CON.1** Kryptokonzept, **CON.3** Datensicherungskonzept),
- Software (siehe:
- **APP.6** Allgemeine Software, **APP.7** Entwicklung von Individualsoftware,
- **CON.8** Software-Entwicklung
- **OPS.1.1.3** Patch- und Änderungsmanagement, **OPS.1.1.6** Software-Tests und – Freigaben),
- Konfiguration (siehe:
- **APP.3.6** DNS-Server,
- **ORP.4** Identitäts- und Berechtigungsmanagement,
- **NET.3.1** Router und Switches),
- Personelle Aspekte (siehe:
- **ORP.2** Personal,
- **SYS.3.3** Mobiltelefon).

Dieser Baustein behandelt nicht

- Produktspezifische Sicherheitsaspekte und Lösungen, die auf einer DLT als weiterer nicht DLT-spezifischer-Layer aufsetzen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein **SYS.5.1** *Blockchain und Distributed Ledger Technologien* von besonderer Bedeutung.

2.1 Verlust der Mehrheit

Sollte eine Gruppe von Teilnehmenden über die Mehrheit an Knoten im Netzwerk verfügen und diese dazu verwenden, die Blockchain zu manipulieren, kann dies zu schwerwiegenden Gefährdungen der Integrität führen. Ein solcher Mehrheitsverlust kann auf verschiedene Weise auftreten, wie bspw. durch 51%-, Sybil- oder Fork-Angriffe.

2.2 Ausfall oder Manipulation des Netzwerkes

Da in einer DLT zur Konsensbildung der Blockchains die Kommunikation der Knoten elementar ist, stellt der Ausfall oder auch die Manipulation eine große Gefahr dar. Dabei können Teile des Netzwerkes abgespalten (Partitionierungen) oder Kommunikation umgeleitet werden (Routing-Angriffe). Ein Ausfall des Netzwerkes würde eine Konsensbildung der Blockchains unmöglich machen.

2.3 Unsichere oder fehlerhafte Smart Contracts (SC)

Da Smart Contracts bei bestimmten Blockchain Frameworks zum Einsatz kommen, um komplexe Verträge und Transaktionen abzuschließen, können diese wie bei jeder Software fehleranfällig sein. Dies könnte möglicherweise zu gefährlichen Situationen führen, wenn sie fehlerhaft sind oder von bösartigen Akteuren manipuliert werden.

2.4 Gefahren durch Social Engineering (SE)

Social Engineering ist eine Taktik, bei der Angreifende versuchen, menschliche Schwächen auszunutzen, um Informationen oder Zugang zu sensiblen Daten oder Systemen zu erhalten. In Blockchains können Social Engineering-Angriffe zu erheblichen Gefährdungen führen. Netzwerkteilnehmenden, die Opfer solcher Angriffe werden, wird vorgespielt, der Angreifende sei vertrauenswürdig, um so bspw. an Passwörter und private Schlüssel zu gelangen, mit denen nicht rückgängig zu machende Transaktionen oder Manipulationen an der Blockchain durchgeführt werden und in der Folge dazu führen, dass eine Blockchain bzw. eine DLT in Teilen oder im Ganzen neu aufgesetzt werden muss, welches in der Konsequenz zu ungewollt sehr hohen Aufwänden und Reputationsverlusten führen kann.

2.5 Missbrauch von Berechtigungen autorisierter Benutzer

Der Missbrauch durch autorisierte Benutzer besteht darin, dass „Insider“ z.B. unbefugt auf private Schlüssel zugreifen können, die zur Verwaltung von Vermögenswerten oder anderen vertraulichen Informationen in der Blockchain verwendet werden können. Wenn ein solcher Schlüssel in die falschen Hände gerät, kann der Angreifende alle mit ihm verbundenen Privilegien nutzen und bspw. Transaktionen autorisieren. Sie könnten ihre Berechtigungen ebenfalls dazu verwenden, in der Blockchain gespeicherte Informationen zu manipulieren oder zu löschen. Auch die Funktionsfähigkeit der Blockchain bzw. DLT könnte beeinträchtigt werden bspw. durch Denial-of-Service-Angriffe.

2.6 Unsachgemäßer Umgang mit privaten Schlüsseln

Der private Schlüssel dient in einer Blockchain als Identitätsnachweis und kommt einer digitalen Identität gleich. Sollten Personen, die mit der Blockchain einer Institution agieren, nicht ausreichend im Umgang mit privaten Schlüsseln und deren Passwörtern sensibilisiert und geschult sein, kann es zu einem erhöhten Risiko des Verlustes, der Weitergabe oder des Missbrauches eines solchen kommen. Dies kann dazu führen, dass Angreifende vollen Zugriff auf ein Wallet oder Vermögenswerte bekommen und Transaktionen ausführen, Zugriff auf persönliche Informationen haben und somit komplett im Namen des Opfers handeln. Durch den Einsatz von kryptografischen Hashfunktionen ist es unmöglich, bereits gespeicherte Informationen rückgängig zu machen.

2.7 Angriffe durch Schadsoftware

Angriffe durch Schadsoftware wie Malware (Malicious Software) oder Ransomware können trotz der dezentralen Natur der Blockchain und DLT besonders schwerwiegend sein und sich von einem kompromittierten Knoten schnell im gesamten Netzwerk verbreiten. Schadsoftware kann auf verschiedene Arten auf eine Blockchain gelangen, z.B. durch infizierte Transaktionen oder Smart Contracts. Im Fokus eines solchen Angriffes stehen i.d.R. private Schlüssel, ähnlich wie beim Phishing.

Erfolgreiche Angriffe könnten das Vertrauen und die Integrität der Blockchain untergraben und das gesamte System gefährden, indem endgültige Transaktionen autorisiert oder manipuliert werden.

2.8 Unsichere kryptografische Verfahren

Kommen kryptografische Hashverfahren zur Anwendung, die nicht dem Stand der Technik entsprechen bzw. als unsicher gelten, kann die Integrität und Vertraulichkeit der Blockchain untergraben werden, da sie zum Signieren und Autorisieren von Transaktionen verwendet werden. Wenn ein Angreifer auf Grund schwacher kryptografischer Verfahren das Urbild oder ein zweites passendes Urbild zu einer mit dem privaten Schlüssel signierten Transaktion errechnen kann, so kann er auch den privaten Schlüssel selbst errechnen bzw. dechiffrieren. Somit können Transaktionen im Namen anderer Teilnehmenden ausgeführt werden, welche durch die Unveränderlichkeit der Blockchain nicht mehr rückgängig zu machen sind. Zusätzlich können auch ältere Transaktionen der Kette manipuliert werden.

2.9 Unzureichendes Identitäts- und Berechtigungsmanagement

Durch ein Identitätsmanagement, welches in einer Blockchain bzw. DLT sicherstellt, dass nur berechtigte Teilnehmende oder Entitäten auf das Netzwerk zugreifen und Transaktionen durchführen dürfen, können diese überprüft und verwaltet werden. Durch eine unzureichende Identitätsüberprüfung oder schwache Authentifizierung kann es zu unbefugtem Zugriff oder Missbrauch kommen.

Wenn in einem Berechtigungsmanagement die Berechtigungen der Teilnehmenden der Blockchain bzw. DLT in Form von Zuweisung spezifischer Rechte und Zugriffsprivilegien entsprechender Rollen und Verantwortlichkeiten, nicht angemessen oder lückenhaft verwaltet werden, kann dies zu unbefugtem Zugriff, Datenmanipulation und anderen Sicherheitsverletzungen führen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins **SYS.5.1** *Blockchain und Distributed Ledger Technologien* aufgeführt. Informationssicherheitsbeauftragte (ISB) sind dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der 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, Informationssicherheitsbeauftragte (ISB), Applikationsverantwortliche (Betrieb), Validatoren

Genau eine Rolle sollte *grundsätzlich zuständig* sein. Darüber hinaus existieren *Geltungsbereiche bzw. Cluster*. Generell muss vor der Umsetzung betrachtet werden, in welches Cluster die Blockchain oder DLT einzuordnen ist. Die jeweiligen Cluster sind hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Nur die für das Cluster relevanten Anforderungen sind umzusetzen.

Die Cluster ergeben sich aus einer analysierten Menge an unterschiedlichen Blockchains und DLT, die, in Abhängigkeit der Ähnlichkeit der ausgewerteten Merkmale oder Kriterien, zusammengefasst wurden.

Übersicht Geltungsbereiche (Cluster):

Kriterien	**Cluster0**	**Cluster1**	**Cluster2**	**Cluster3**	**Cluster4**
Konsens	PoW	PoS, SCP, YAC	plugable: xBFT, PoET, ...	xPoS	plugable: Raft, PoW
Dezentralität	sehr dezentralisiert	sehr dezentralisiert	sehr dezentralisiert	sehr dezentralisiert	mäßig dezentralisiert
Performance in TPS	sehr langsam	mäßig schnell	sehr langsam	sehr langsam	eher langsam
On/Off BC	Off	On & Off	On & Off	-	On & Off
Sicherheit	sicher	sicher	sicher	mäßig sicher	mäßig sicher
Skalierbarkeit	mäßig skalierbar	mäßig skalierbar	mäßig skalierbar	mäßig skalierbar	mäßig skalierbar
Program-mierung	nein	nein	ja	ja	ja
Token	ja	nein	nein	ja	nein
Geschäfts-modell (?2?)	- B2C C2C	B2B - -	B2B - -	B2B B2C C2C	B2B - C2C
Signatur	synchron & asynchron	- asynchron	- asynchron	- asynchron	synchron & asynchron
Identitäts-management	nein	nein	ja	nein	ja

3.1 Basis-Anforderungen

Die folgenden Anforderungen **MÜSSEN** für diesen Baustein vorrangig erfüllt werden.

SYS.5.1.A1 Festlegen einer Mindestknotenanzahl (B) [alle Cluster]

Vor dem Einsatz einer DLT **MUSS** eine Mindestanzahl an Knoten (Netzwerkteilnehmende oder Peers) festgelegt werden. Dabei **DARF NICHT** der vom Hersteller der DLT vorgegebene Mindestwert an Knoten, um Fault Toleranz zu gewährleisten, unterschritten werden. Zusätzlich **MUSS** ein Puffer über dem Mindestwert zur Erreichung von Fault Toleranz berücksichtigt werden (je höher dieser ist, umso robuster ist die DLT gegenüber Bedrohungen):

$$Knotenanzahl_{min} = Fault\ Toleranz_{min} + Puffer$$

Dieser Puffer **MUSS** bei sehr kleinen DLT (≤ 10) bei 50% liegen und mit steigender Größe des Netzwerkes regressiv fallen. Dabei **MÜSSEN** folgende Faktoren, in Abhängigkeit des jeweiligen Anwendungsfalles der DLT, bei der Bestimmung des Puffers betrachtet werden:

- Sicherheitsanforderungen,
- Verfügbarkeit,
- Skalierbarkeit/Leistungsfähigkeit
- Netzwerktopologie sowie der
- Konsensmechanismus.

Darüber hinaus **MUSS** für jeden Teilnehmenden eine Begrenzung der Anzahl an Knoten festgelegt werden, die von ihm betrieben werden darf, um den Einfluss einzelner Netzwerkteilnehmender zu beschränken.

SYS.5.1.A2 Ausschluss der Speicherung von Daten mit dem Recht auf Vergessenheit (B) [alle Cluster]

In einer Blockchain **DÜRFEN KEINE** Daten gespeichert werden, die aus rechtlichen und gesetzlichen Gründen grundsätzlich das Recht auf Vergessenheit bzw. Löschung besitzen.

SYS.5.1.A3 Persistente Speicherung (B) [alle Cluster]

Zur Erreichung der Persistenz der Daten in einer DLT **MÜSSEN** die Blockchains

- dezentral (wiederherstellbar über andere Knoten),
- konsistent (Konsensalgorithmus und Fault Toleranz),
- unveränderbar ((quantensichere) Hashfunktionen) und
- dauerhaft

gespeichert werden. Dazu **MUSS** der verwendete Speicher

- skalierbar,
- ausfallsicher und
- performant sein.

SYS.5.1.A4 Speicherung von Passwörtern und Schlüsseln (B) [alle Cluster]

Passwörter und Schlüssel für eine Blockchain **MÜSSEN** verschlüsselt gespeichert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie **SOLLTEN** grundsätzlich erfüllt werden.

SYS.5.1.A5 Verteilung der Knoten auf mehrere Standorte (S) [Cluster: 1, 2, 3, 4]

Um eine Verbesserung sowie Erhöhung der Dezentralisierung und Verfügbarkeit zu erreichen, **SOLLTEN** die Knoten über mehrere Standorte verteilt werden. Um eine georedundante Dezentralisierung zu erreichen, **SOLLTEN** die Knoten über mehrere Standorte in verschiedenen Städten oder Staaten verteilt werden.

SYS.5.1.A6 Erstellung von Vorgaben und Richtlinien für Smart Contracts (S) [Cluster: 2, 3, 4]

Für Smart Contracts **SOLLTEN** Vorgaben und Richtlinien festgelegt werden. Die Anforderungen **SOLLTEN** vor der Inbetriebnahme der Blockchain bzw. der DLT aufgestellt werden. Die Anforderungen **SOLLTEN** auf die Besonderheit der dezentralen, unveränderbaren und vertrauenslosen Natur der Blockchain eingehen.

Dabei **SOLLTEN** Merkmale wie

- Determinismus,
- Sicherheit und Verifizierbarkeit,
- Interoperabilität,
- Update-Fähigkeit,
- Transparenz und Durchführbarkeit,
- verteilte Ausführungskosten sowie
- Compliance-Anforderungen betrachtet werden.

Darüber hinaus **SOLLTEN** komplexe Operationen in Smart Contracts vermieden werden, um verteilte Ausführungskosten auf vielen gleichzeitig arbeitenden Knoten zu minimieren. Weiterhin **SOLLTEN** auch Bedingungen und Einschränkungen für die Ausführung und den Betrieb von Smart Contracts festgelegt werden.

Dienste, die in die Blockchain bzw. DLT eingebunden werden, **SOLLTEN** bei der Absicherung mitberücksichtigt werden (auf Netzwerk- und Applikationsebene), um keine potentiellen Bedrohungen über diese zuzulassen.

Die Umsetzung der Vorgaben und Richtlinien **SOLLTE** regelmäßig auditiert werden. Dies **SOLLTE NICHT** durch den Urheber (Entwickler) des Smart Contracts selbst durchgeführt werden.

SYS.5.1.A7 Verwendung stabiler und aktueller Software-Versionen (S) [alle Cluster]

Zum sicheren Betreiben der Blockchain und DLT **SOLLTEN** nur aktuelle Softwareversionen verwendet werden. Dazu **SOLLTEN** Patches und Updates zeitnah eingespielt werden. Softwareversionen aus Pre-Releases, wie Alpha- oder Beta-Versionen, **SOLLTEN NICHT** verwendet werden.

SYS.5.1.A8 Einführung einer Zugriffskontrolle (S) [Cluster: 1, 2, 3]

Um den Zugriff auf die Blockchain und DLT zu regulieren bzw. nur autorisierten Nutzenden und Administrierenden zu gewähren, **SOLLTE** ein System der Zugriffskontrolle und Authentifizierung implementiert werden. Hierzu **SOLLTE** eine Realisierung über ein Identitätsmanagement, den Konsensalgorithmus oder über Smart Contracts in Betracht gezogen werden.

SYS.5.1.A9 Festlegen von Mindestanforderungen an kryptografische Hashfunktionen (S) [alle Cluster]

Vor der Inbetriebnahme der Blockchain und der DLT **SOLLTE** betrachtet werden, wie lang die voraussichtliche Einsatzdauer sein wird. Bei der Auswahl von Verschlüsselungsverfahren und Schlüssellängen **SOLLTE** die technische Richtlinie „BSI TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI berücksichtigt werden. Die verwendeten kryptografischen Hashfunktionen **SOLTTEN** dem Stand der Technik entsprechen, jedoch mindestens eine Bit- oder Schlüssellänge von 256 besitzen. Bei einer längeren Einsatzdauer **SOLLTEN** die kryptografischen Hashfunktionen mindestens eine Bit- oder Schlüssellänge von 512 besitzen. Sofern sich der Stand der Technik an kryptografischen Hashfunktionen erhöht, **SOLLTEN** diese Anforderungen umgehend umgesetzt werden.

SYS.5.1.A10 Erstellung eines Planes zur Erhaltung der Langlebigkeit (S) [alle Cluster]

Im Vorfeld der Inbetriebnahme der Blockchain und der DLT **SOLLTE** ein Plan erstellt werden, der regelt, wie mit den Daten der Blockchain zu verfahren ist, wenn die Einhaltung der Vertraulichkeit (C) und Integrität (I) in der Zukunft nicht mehr gewährleistet ist. Wenn die Nutzungsdauer der Blockchain und der DLT auf unbestimmte Zeit festgelegt ist, **SOLLTEN** Möglichkeiten existieren, die Sicherheit der Daten zu erhalten. Für den Fall, dass die Blockchain kompromittiert wurde, **SOLLTE** für die Community oder den Hersteller die Möglichkeit bestehen einen Fork der Blockchain zu erstellen.

SYS.5.1.A11 Festlegen von Policies (S) [alle Cluster]

Für die Blockchain und DLT **SOLLTEN** Policies festgelegt werden, die den Betrieb dieser regeln. Diese **SOLLTEN** regeln, welcher Konsensalgorithmus verwendet wird, wie die Transaktionsvalidierung stattfindet und ob und wie eine Zugriffskontrolle und Schlüsselverwaltung stattzufinden hat. Für den Fall, dass Governance-Bestimmungen oder Compliance-Richtlinien (Gesetze, firmeninterne Vorgaben und AGBs) vorliegen, **SOLLTEN** diese umgesetzt werden.

SYS.5.1.A12 Vermeidung von Privileg-Escalation (S) [alle Cluster]

Zur Vermeidung von Privileg-Escalation (Rechteanreicherung) in einer Blockchain oder DLT **SOLLTEN** Sicherheitsmaßnahmen implementiert werden. Dazu **SOLLTE** eine regelmäßige sorgfältige Überprüfung der Smart Contracts zur Erkennung der Schwachstellen erfolgen. Penetrationstests **SOLLTEN** ebenfalls regelmäßig stattfinden. Weiterhin **SOLLTE** ein robuster Konsensalgorithmus verwendet werden, der eine breite Verteilung der Entscheidungsfindung gewährleistet. Darüber hinaus **SOLLTE** eine regelmäßige Aktualisierung der Blockchain-Software stattfinden, um Sicherheitspatches und Updates zu implementieren.

SYS.5.1.A13 Erhöhung des Passwortschutzes (S) [alle Cluster]

Zum Speichern von Passwörtern für private Schlüssel oder Wallets **SOLLTEN** Salted Hashverfahren verwendet werden.

SYS.5.1.A14 Erhaltung der Integrität (S) [Cluster: 0, 3]

Es **SOLLTEN** geeignete Maßnahmen getroffen werden, um die Integrität gegen bspw. Double Spending einer Ressource, eines Gutes oder eines Rechtes zu erhalten. Dazu **SOLLTE**

- ein geeigneter Konsensalgorithmus gewählt,
- eine bestimmte Anzahl an Blöcken bis zur Finalität festgelegt,
- nur integere Software in die Blockchain aufgenommen,
- ein Zeitstempel für die chronologische Reihenfolge und als Integritätsnachweis verwendet sowie
- eine Fallback Security implementiert (OFF-Chain Transaktionen)

werden. Wenn Smart Contracts eingesetzt werden, **SOLLTEN** durch diese spezifische Bedingungen für Transaktionen festgelegt werden.

SYS.5.1.A15 Sicherung der Blockchain Business Continuity (S) [Cluster: 1, 2, 3, 4]

Vor der Inbetriebnahme **SOLLTE** zur Erhaltung der Verfügbarkeit und der Integrität ein Notfallplan erstellt werden. Dieser **SOLLTE** klare Anweisungen und Maßnahmen für den Umgang mit Störungen oder Ausfällen in der Blockchain- und DLT-Infrastruktur enthalten. Dabei **SOLLTE** der Notfallplan die Wiederherstellung von

Systemen, Daten und Diensten beschreiben sowie klare Verantwortlichkeiten bei der Durchführung der Maßnahmen festlegen. In diesem Rahmen **SOLLTE** festgelegt werden, wie die Bereitstellung stattzufinden hat und wie groß der Anteil an Netzwerkteilnehmenden sein muss, die dieser zuzustimmen. Darüber hinaus **SOLLTE** ein Monitoring- und Alarmierungssystem implementiert werden, um potenzielle Gefährdungen frühzeitig zu erkennen und geeignete Maßnahmen einleiten zu können.

Im Falle eines Zero-Day Exploit **SOLLTE** für alle Teilnehmenden eine

- maximale Reaktionszeit sowie Maßnahmen bei Nicht-Einhaltung,
- die Art und Weise der Kommunikation und
- notwendige Mindestanzahl an Zustimmungen von Knoten für einen Patch

festgelegt werden.

SYS.5.1.A16 Entwicklung einer Backup-Strategie (S) [Cluster: 1, 2, 4]

Zur Erhöhung der Verfügbarkeit und Wiederherstellbarkeit **SOLLTE** eine Backup-Strategie entwickelt werden. Dieses dezentrale Backup **SOLLTE** als Datensicherung oder Sicherungskopie auf mehrere Knoten verteilt werden. Dazu **SOLLTEN** in Abhängigkeit zur Betriebsumgebung (bspw. Virtualisierung, Containerisierung oder physikalischer Server) folgende Strategien in Betracht gezogen werden:

- vollständige Knotenreplikation (redundant und fehlertolerant)
- inkrementelle Backups
- Datenredundanz durch Sharding
- Off-Chain Backups
- Snapshots

Bei der Implementierung eines Backups **SOLLTEN** bestimmte Aspekte berücksichtigt werden, um das Grundprinzip der Dezentralisierung und Konsensbildung zu wahren:

- Dezentrale Backups (Verteilung auf mehrere Knoten)
- Konsistenz und Integrität (Berücksichtigung kryptografischer Algorithmen)
- Synchronisation (regelmäßiger Abgleich der Backup-Versionen)

SYS.5.1.A17 Mehr-Faktor-Authentifizierung (S) [alle Cluster]

Authentifizierungen und digitale Signaturen von Blockchain bzw. DLT unternehmenskritischer Anwendungen **SOLLTEN** mindestens einen zweiten Weg der Authentifizierung besitzen. Um dies zu ermöglichen, **SOLLTE** eine Mehr-Faktor-Authentifizierung umgesetzt werden, z.B. über Hardware-Token, biometrische Verfahren oder über eine Authenticator APP.

SYS.5.1.A18 Multi-Signatur für administrative Tätigkeiten (H) [alle Cluster]

Die Ausführung von administrativen Tätigkeiten zur Verwaltung und Wartung der Blockchain bzw. der DLT **SOLLTE** erst nach Zustimmung von mehreren Berechtigten erfolgen. Dazu **SOLLTE** eine Multi-Signatur (MultiSig) für administrative Tätigkeiten verwendet werden, bei der mehrere Administrierende diese mit ihrem privaten Schlüssel signieren.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über das Schutzniveau hinausgehen, welches dem Stand der Technik entspricht. Die Vorschläge **SOLLTEN** bei erhöhtem

Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.5.1.A19 Verwendung von quantensicheren Algorithmen (H) [alle Cluster]

Es **SOLLTEN** quantensichere Algorithmen (Post-Quantum-Kryptographie) verwendet werden, wenn eine höhere Sicherheit bei der Verwendung kryptografischer Hashverfahren zu gewährleisten und um eine Entschlüsselung von kryptografischen Hashfunktionen mittels leistungsstarker Systeme, wie z.B. Quantencomputer, zu verhindern (siehe technische Richtlinie BSI-TR-02102-1).

SYS.5.1.A20 Trennung von Management- und Applikationsnetzwerk (H) [alle Cluster]

Als zusätzliche Sicherheitsmaßnahme **SOLLTE** eine Trennung von Management- und Applikationsnetzwerk implementiert werden. Eine effektive Trennung der Netzwerke **SOLLTE** durch physische oder logische Netzwerksegmentierung erreicht werden.

4. Weiterführende Informationen

Das National Institute of Standards and Technology (NIST) gibt in den folgenden Publikationen Hinweise für das Schlüsselmanagement sowie Empfehlungen für Applikationen, die Hashalgorithmen verwenden:

- Special Publication 800-107 *„Recommendation for Applications Using Approved Hash Algorithms“* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf
- und Special Publication 800-*57 „Recommendation for Key Management“*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

Bei der Auswahl von Verschlüsselungsverfahren und Schlüssellängen finden sich weiterführende Informationen in der technischen Richtlinie „BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI wieder:

- BSI-TR-02102-1: *„Kryptographische Verfahren: Empfehlungen und Schlüssellängen“* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=8

Weiterhin sind Informationen zum Business Continuity Management von der ISO (International Organization for Standardization) und dem BSI standardisiert worden:

- ISO 22301:2019 *„Security and resilience - Business continuity management systems – Requirements“* https://www.iso.org/standard/75106.html
- BSI-Standard 200-*4 „Business Continuity Management“* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8

Zusätzliche Informationen zur Herleitung, sowohl zum Clustering als auch zur Bedrohungslage und den Anforderungen, befinden sich in der Masterthesis:

- „Systemorientierte IT-Grundschutz-Bausteine für Blockchain und Distributed Ledger Technologien“.

Weitere Informationen vom BSI und NIST zum Themen Blockchain und DLT sind in folgenden Veröffentlichungen zu finden:

- BSI *„Blockchain sicher gestalten - Konzepte, Anforderungen, Bewertungen“* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=3
- BSI *„Projekt 374 (Studie Blockchain) – Abschlussbericht"* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.pdf?__blob=publicationFile&v=2

- BSI *„Eckpunktepapier für DLT-basierte Kryptowährungen“* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunktepapier_fuer_DLTbasierte_Kryptowaehrungen.pdf?__blob=publicationFile&v=2
- NISTIR 8202 *„Blockchain Technology Overview“* https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf