Regelungen für Lieferanten

Inhaltsverzeichnis

1. Anwendungsbereich

Die Regelungen für Lieferanten gelten für Lieferanten der HDT Veritas Hessen GmbH, die im Rahmen eines Vertragsverhältnisses Zugang oder Zugriff auf IT-Systeme, -Applikationen, -Netze oder firmenvertrauliche Informationen haben.

Die hierin definierten Regeln und Grundsätze gelten unabhängig davon, ob der Lieferant IT-Systeme der HDT Veritas oder eigene IT-Systeme nutzt, der Lieferant in Räumlichkeiten der HDT Veritas arbeitet oder nicht, oder ein Anschluss zu IT-Ressourcen der HDT Veritas erfolgt (z.B. zu einem IT-System oder einer IT-Applikation).

1.1. Verantwortlichkeiten

Dem Lieferanten der HDT Veritas Hessen GmbH wird zur Erfüllung vertraglicher Verpflichtungen und zur Steigerung der Effizienz der Geschäftsabwicklung Zugang und Zugriff auf Informationen bzw. IT-Systeme, -Applikationen und-Netze oder firmenvertrauliche Informationen ermöglicht.

Dies bedarf Maßnahmen zum Schutz der IT-Systeme, -Applikationen, -Netze und firmenvertraulichen Informationen vor ungewollter Offenlegung, unberechtigten Zugriff, Manipulation, Computerviren, Hacking, Cyberangriffen und anderer Bedrohungen. Dazu ist es erforderlich, dass alle Lieferanten der HDT Veritas die nachfolgenden Regeln und Grundsätze einhalten und Schutzmaßnahmen weder außer Betrieb nehmen, umgehen oder in sonstiger Weise verändern.

Der Lieferant verpflichtet sich zusätzlich zu den sonstigen vertraglichen Vereinbarungen, die hierin definierten Regeln und Grundsätze zu beachten sowie diese Unterlage seinen Mitarbeitern, die Zugang oder Zugriff auf IT-Systeme, -Applikationen und -Netze der HDT Veritas oder firmenvertrauliche Informationen erhalten, zur Kenntnis zu bringen, sie auf die Einhaltung zu verpflichten und die Einhaltung in geeigneter Weise zu überprüfen.

Im Weiteren werden Lieferanten und dessen Mitarbeiter zusammenfassend als Lieferant/Lieferanten bezeichnet.

2. Regeln und Grundsätze

2.1. Umgang und Informationen

Grundsätzlich sind alle Informationen der HDT Veritas Hessen GmbH unabhängig von ihrer Erscheinungsform und ihrem Informationsträger gemäß ihrer Einstufung vor Verlust der Vertraulichkeit, Integrität und Verfügbarkeit zu schützen.

Firmenvertrauliche Informationen der HDT Veritas sind alle Informationen, die nicht öffentlich sind. Für firmenvertrauliche Informationen sind zwei Schutzklassen vorgesehen: „Innerbetrieblich" und "Vertraulich". Entsprechend der Schutzklasse sind bei der Kennzeichnung/Erstellung, Verteilung, dem Versand und der Übertragung, Aufbewahrung und Speicherung sowie bei der Entsorgung/Vernichtung/Löschung Schutzmaßnahmen erforderlich, die mit zunehmendem Schutzbedarf höher werden.

Der Lieferant legt in Absprache mit dem Ansprechpartner seitens der HDT Veritas GmbH den Vertraulichkeitsgrad der von ihm erstellten Informationen fest. Bei überlassenen Informationen ist der Lieferant verpflichtet, die von HDT Veritas definierten Schutzmaßnahmen einzuhalten.

Firmenvertrauliche Informationen dürfen nur auf IT-Systemen, -Applikationen und Dateiablagesystemen gespeichert und verarbeitet werden, die einen adäquaten Schutz dieser Informationen gewährleisten.

Der Lieferant ist verpflichtet, die verschlüsselte Übertragung von E-Mails mit vertraulichem Inhalt und die Entschlüsselung empfangener verschlüsselter E-Mails zu ermöglichen.

Die automatische Weiterleitung empfangener E-Mails an externe Postfächer ist ebenso untersagt wie der Faxversand von vertraulichen Informationen.

HDT Veritas benennt einen Ansprechpartner, der in Angelegenheiten der Informationssicherheit vom Lieferant kontaktiert werden kann. An ihn müssen auch sämtliche sicherheitsrelevanten Vorfälle gemeldet werden. Der Lieferant benennt ebenfalls einen qualifizierten Ansprechpartner für Informationssicherheit.

Informationen der HDT Veritas, die für die Erbringung der vertraglich vereinbarten Aufgaben und Tätigkeiten nicht mehr erforderlich sind und nicht aufgrund gesetzlicher oder vertraglicher Aufbewahrungspflichten vorgehalten werden müssen, sind vom Lieferanten zuverlässig von allen seinen Informationsträgern zu löschen. Während eines normalen Arbeitsablaufes dürfen auf IT-Systemen gespeicherte elektronische Informationen mit den vom IT System standardmäßig angebotenen Löschfunktionen gelöscht werden, wenn eine Verschlüsselung eingerichtet ist.

Papierdokumente sind mit Hilfe eines geeigneten Aktenvernichters oder durch einen Entsorgungsdienst zu vernichten. Wenn der Lieferant keine geeigneten Entsorgungsmöglichkeiten bzw. Aktenvernichter hat, muss das weitere Vorgehen mit dem Ansprechpartner der HDT Veritas abgesprochen werden.

2.2. Zugangs- und Zutrittsberechtigungen

Soweit der Lieferant Zugangs- und/oder Zutrittsberechtigungen (z.B. Passwort oder Zugangskarten) erhält, sind diese nur in dem Umfang zu nutzen, wie dies zur Erfüllung seiner vertraglich vereinbarten Aufgaben und Tätigkeiten notwendig ist. Diese sind vertraulich zu behandeln und dürfen weder an Dritte weitergegeben noch offengelegt werden.

2.3. Zugangs- und Zugriffsschutz

Die vom Lieferanten für die Erfüllung der Aufgaben benutzten IT-Systeme und Informationsträger sowie alle von der HDT Veritas an den Lieferanten übergegebenen IT-Systeme und Informationsträger sind nach aktuellem Stand der Technik wirksam gegen den Zugang und Zugriff durch Unbefugte zu schützen. Folgende Maßnahmen gelten aus heutiger Sicht zum Mindestschutz für IT-Systeme und Informationsträger:

- BIOS/UEFI-Passwort.
- Bildschirmschoner mit Passwortschutz des Betriebssystems (als Systemsperre bei unbeaufsichtigten IT-Systemen).
- Diebstahlschutz bei Mobilsystemen.
- Festplatten- und Dateiverschlüsselung.
- Schutz vor Viren und ähnlicher Schadsoftware nach aktuellem Stand der Technik, soweit die IT-Systeme oder Informationsträger solchen Risiken unterliegen. Für PC-Systeme sind aktuelle, permanent wirkende Virenwächter einzusetzen.
- Absicherung von Netzzugängen mindestens durch Passwort.
- Keine Zugriffsmöglichkeiten Unbefugter durch Ressourcen-Sharing.
- Verwendung eines eigenen unterschiedlichen Passworts je Benutzerkonto.
- Keine Verwendung von Standardpasswörtern. Löschung von Initialpasswörtern sofort nach deren Erhalt.
- Passwörter müssen aus einer Kombination von Klein- und Großbuchstaben, Zahlen und Sonderzeichen gebildet werden. Passwörter müssen mindestens 10 Zeichen (bei administrativen Kennungen 14 Zeichen) enthalten. Für PINs müssen Zufallszahlen verwendet werden. Passwortwechsel sind mindestens alle 90 Tage (bei administrativen Kennungen 30 Tage) vorzunehmen. Die letzten 10 Passwörter sind nicht wieder zu verwenden.

- Papierdokumente und mit vertraulichen oder streng vertraulichen Dokumenten dürfen nicht offen zugänglich und unbeaufsichtigt sein. Diese müssen mit geeigneten Schutzmechanismen weggeschlossen werden.

Die von der HDT Veritas GmbH zur Verfügung gestellten externen Systemzugriffe müssen vom Lieferanten protokolliert werden. Hierfür muss wenigstens festgehalten werden:

- wer (Name des Mitarbeiters)
- wann und wie lange
- über welchen Zugang
- zu welchem Zweck
- auf welches System

2.4. Mandanten Trennung

Es wird für eine Mandanten Trennung folgende Punkte vorausgesetzt:

- 1 Datenisolation: Die Mandanten müssen strikt voneinander getrennt sein, sodass es keine Möglichkeit gibt, dass Daten zwischen verschiedenen Mandanten vermischt werden. Es muss systemisch verhindert werden, dass andere Mandant auf die Daten zugreifen können.
- 2. Authentifizierung und Zugriffskontrolle: Das Konzept muss eine robuste Authentifizierungs- und Zugriffskontrollmechanismen bieten, zur Sicherzustellung, dass nur autorisierte Benutzer auf hinterlegten Daten zugreifen können. Jeder Benutzer sollte nur Zugriff auf die Informationen haben, für die er berechtigt ist.
- 3. Verschlüsselung: Alle Daten, die übertragen werden, müssen verschlüsselt sein, um die Vertraulichkeit während der Datenübertragung zu gewährleisten. Zusätzlich sollten die Daten in der Datenbank und im Speicher verschlüsselt sein, um die Sicherheit in Ruhe zu gewährleisten.
- 4. Ressourcenisolierung: Die Ressourcen (z. B. Rechenleistung, Speicher, Netzwerkbandbreite) müssen isoliert sein, um sicherzustellen, dass keine Ressourcen anderer Mandanten beeinträchtigt werden können. Das Konzept sollte sicherstellen, dass ein hoher Ressourcenbedarf eines Mandanten keine negativen Auswirkungen auf die Leistung hat.
- 5. Audit-Trail und Protokollierung: Es ist wichtig, dass das Konzept eine umfassende Protokollierung und einen Audit-Trail bietet. Alle Aktionen, die von Benutzern oder Systemen durchgeführt werden, sollten aufgezeichnet werden, um eine lückenlose Nachvollziehbarkeit von Aktivitäten zu gewährleisten.
- 6. Software-Updates und Patch-Management: Der IT-Dienstleister muss ein wirksames Software-Update- und Patch-Management implementieren, um Sicherheitslücken zu schließen und Schwachstellen zu beheben, bevor diese von Angreifern ausgenutzt werden können.
- 7. Notfallwiederherstellung und Backup: Das Mandantenrennungskonzept sollte eine solide Notfallwiederherstellungsstrategie und regelmäßige Backups enthalten, um Datenverlust und Ausfallzeiten zu minimieren und die Geschäftskontinuität sicherzustellen.
- 8. Datenschutz und Compliance: Das Konzept muss den geltenden Datenschutzbestimmungen und branchenspezifischen Compliance-Anforderungen entsprechen, um sicherzustellen, dass personenbezogene Daten angemessen geschützt werden.
- 9. Monitoring und Frühwarnsystem: Es sollte ein kontinuierliches Überwachungssystem eingerichtet werden, das verdächtige Aktivitäten frühzeitig erkennt und auf mögliche Sicherheitsverletzungen hinweist.

Ein vorhandenes Konzept gilt vorzulegen, anderenfalls gelten die hier vertraglich festgelegten Regelungen zur Gewährleistung.

2.5. Informationspflichten, Kontrolle

Die von der HDT Veritas Hessen GmbH und dem Lieferanten definierten Ansprechpartner informieren sich gegenseitig und rechtzeitig über relevante Betriebsstörungen, bei Erkennung von Fehlern und Schadensfunktionen in allen innerhalb der Zusammenarbeit genutzten IT-Systemen, -Applikationen, -Netzen oder Software (z.B. Computerviren, Programmfehler).

Sofern der Lieferant Schwachstellen und Vorfälle mit möglicher Auswirkung auf die Informationssicherheit erkennt, z.B. Verdacht eines Missbrauchs oder Offenlegung von PINs/Passwörtern, müssen diese unverzüglich dem Ansprechpartner bei der HDT Veritas gemeldet werden.

Der Lieferant ist zur Einhaltung von Hinweisen und Regelungen seitens der HDT Veritas zur Sicherheit der IT Systeme, -Applikationen und -Netze verpflichtet. Eine personalrechtliche oder disziplinarische Weisungsbefugnis gegenüber dem Lieferanten besteht nicht.

Die Einhaltung dieser Regeln und Grundsätze zur Informationssicherheit wird bei der HDT Veritas kontrolliert. Die an die Netze von der HDT Veritas angeschlossenen IT-Systeme werden gemäß dem Stand der Technik auf Sicherheitsschwachstellen hin überprüft. Identifizierte Schwachstellen müssen vom Lieferanten unverzüglich behoben werden. Von den Herstellern angebotene sicherheitsrelevante patche, Korrekturen und Hotfixe müssen vom Lieferanten installiert werden.

Falls der Lieferant einzelne oder alle der vorliegenden Regeln missachtet, kann dies zur Sperrung von Zugangs- bzw. Zutrittsberechtigungen zu den Räumlichkeiten bzw. von Zugriffsberechtigungen zu den IT-Systemen führen, sowie vertraglich vereinbarte bzw. gesetzlich normierte Konsequenzen nach sich ziehen.

2.6. Beendigung der Zusammenarbeit

Bei Beendigung der Zusammenarbeit mit der HDT Veritas Hessen GmbH werden, sofern nichts anderes vereinbart wurde, vom Lieferanten folgende Tätigkeiten ausgeführt und schriftlich bestätigt:

- Rückgabe aller überlassenen IT-Systeme, Geräte, Informationen, Informationsträger, Papierdokumente und Arbeitsmittel.
- Rückgabe aller erteilten Zutritts- oder Zugangsberechtigungen sowie Nennung aller Zugriffsberechtigungen zwecks Deaktivierung bzw. Löschung (z.B. Zugriffberechtigungen auf Dateiablagen).
- Löschung von Informationen auf allen Informationsträgern und Vernichtung von Papierdokumenten gemäß Kapitel 2.1.

2.7. Zusätzliche Regeln für Lieferanten mit Anschluss an die IT-Systeme, -Applikationen und -Netzen der HDT Veritas

Der Lieferant verpflichtet sich, den Anschluss nur in der vereinbarten technischen Konfiguration und an den dafür vorgesehenen IT-Systemen zu betreiben.
Informationen über Strukturen, Zugangsmöglichkeiten (z.B. Netzadressen) und Sicherheitsvorkehrungen der HDT Veritas IT-Systeme, -Applikationen und -Netze sind firmenvertrauliche Informationen (vgl. Kapitel 2.1) und sind vom Lieferanten dementsprechend zu behandeln.

3. Dokumentation

Der Lieferant stellt der HDT Veritas eine Dokumentation der bereitgestellten Dienste und Systeme zur Verfügung. Die Dokumentation soll insbesondere die folgenden Punkte umfassen:

- Überblick über die Systemarchitektur (kann Teil der Designdokumentation sein)
- Kommunikationsmatrix
- Existierende Benutzerkonten und Rollen sowie deren Berechtigungen
- Beschreibung von proprietären (nicht in der Industrie standardisierten) Sicherheitsmechanismen
- Weitere Dokumentationen, spezifiziert als Teil des Liefergegenstandes oder Auftrages, die die Sicherheit der Lösung gewährleiten

Sollten Änderungen an der bereitgestellten Lösung durchgeführt werden, wird vom Lieferanten erwartet, diese in die Dokumentation einzupflegen und eine aktualisierte Fassung an die HDT Veritas zu übermitteln.

Der Lieferanten erfasst und dokumentiert alle relevanten Hard- und Softwarekomponenten. Bei Software sollen die Softwareversion und das jeweilige Patchlevel angegeben werden.

4. Systemhärtung

Der Lieferant verpflichtet sich, die von ihm für die Erbringung der Dienste verwendeten Systeme zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren. Dies muss vor der Deklaration einer Systemabnahme durch die HDT Veritas geschehen sein. Der Lieferant sollte sich hierbei an gängigen Vorgaben, wie z.B. aus dem BSI Grundschutzkatalog oder dem CIS-CAT orientieren. Insbesondere sind die nachfolgend beschriebenen Abschnitte einzuhalten.

4.1. Minimale Installationsprinzipien

Es wird von dem Lieferanten erwartet, folgende Komponenten des Betriebssystems oder anderer Software zu installieren:

- Jede Softwarekomponente, die für die Anwendung oder nach der Logik des Dienstes benötigt wird
- Jede aus der Integration mit anderen Services resultierende andere Anwendung oder Softwarekomponente
- Jede aus Betriebs- und Wartungsanforderungen resultierende Softwarekomponente

Jede andere Software darf nicht installiert werden, außer der Lieferant und die HDT Veritas einigen sich darüber. Software, die nur im Zeitraum der Installation notwendig ist, oder deren Installation nicht zu verhindern ist, ist nach Abschluss dieser zu entfernen. Nicht benötigte Rollen, Dienste und Funktionen sollten deaktiviert werden.

4.2. Netzwerkzugänge

Jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) muss gefiltert werden. Die Nutzung jedes Zugangs muss in der Dokumentation des Lieferanten erläutert werden.

4.3. Konfigurationsstandards

Der Lieferant stellt sicher, dass die von der HDT Veritas GmbH vorgegebenen allgemeinen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden.

4.4. Standardpasswörter

Der Lieferant stellt sicher, dass jedes Standardpasswort in allen möglichen Fällen geändert werden kann und vor Abnahme auch tatsächlich geändert wurde.

4.5. Backdoors

Der Lieferant muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine bereitgestellten Systeme frei von „Backdoors“ sind, die die verwendeten Sicherheitsmechanismen umgehen können.

4.6. Kontrolle der Systemanforderungen

Der Lieferant verpflichtet sich, dass er hinsichtlich seiner Produkte mit geeigneten Maßnahmen und Protokollen, die mit der HDT Veritas abzustimmen sind, nachweist, dass alle in diesem Kapitel genannten Anforderungen eingehalten werden.

5. kryptographischen Lösungen

Um sicherzustellen, dass keine veralteten und als unsicher bekannten Kryptographie Lösungen eingesetzt werden, muss die Auswahl kryptographischer Mechanismen gemäß der jeweils aktuellen Fassung der BSI-Richtlinie TR-021022 erfolgen.

Wenn eine Kryptographie Lösung in der Industrie als nicht mehr sicher bekannt wird und eine solche Kryptographie Lösung in dem bereits bei der HDT Veritas bereitgestellten Dienst bzw. der bereitgestellten Anwendung verwendet wird, muss der Lieferant sie im Rahmen vom Vulnerability-Management-Prozess als Schwachstelle bewerten und melden. Der Lieferant hat Vorschläge zur Behebung der Schwachstelle zu unterbreiten und nach Rücksprache umzusetzen.

Der Lieferant muss sicherstellen, dass der Einsatz der kryptographischen Absicherung der Kommunikation und Ablage überall erfolgt, wo es notwendig ist, um die Grundsätze der sicheren Softwarearchitektur zu unterstützen. Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere notwendig, wenn Daten mit hohem Schutzbedarf (z.B. Authentifizierungsdaten, personenbezogene Daten, Steuerungsdaten aus Prozess-Netzen oder vertrauliche Daten) über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.

Die Klassifizierung der Daten ist Aufgabe der HDT Veritas Hessen GmbH und wird dem Lieferanten bei Auftragserteilung zur Verfügung gestellt.

6. Patch-Management

Der Lieferant muss alle eingesetzten Komponenten regelmäßig mit notwendigen Sicherheitsupdates versorgen, um etwaige Schwachstellen schnell zu schließen. Darüber hinaus müssen Bugs und Fehler innerhalb der Komponenten des Lieferanten durch Updates behoben werden.

6.1. Umfang des Patchings

Der Umfang des Patchings muss jede Komponente des Systems, wie von der HDT Veritas akzeptiert, umfassen. Dazu gehören in der Regel:

- Betriebssystem
- Alle Softwarepakete und Services, die Teil des Betriebssystems sind
- Alle Tools und Applikationen, die der Hersteller zu Betriebs- und Wartungszwecken installiert hat
- Zielapplikation (Servicelogik)
- Alle Middleware-Application-Layer, Datenbanken, Access-, Monitoring- oder Applikationsserver, die für den Service genutzt werden
- Netzwerkkomponenten
- Sicherheitskomponenten
- Management-Umgebungen und Clients

6.2. Patch-Level während der Systemabnahme

Der Lieferant hat sicherzustellen, dass alle Systeme vor der Abnahme gepatcht werden. Der Patch-Level darf dabei nicht älter als 3 Monate ab dem Tag der Systemabnahmeerklärung sein. Der Lieferant muss alle öffentlich verfügbaren Patches als Teil der Lieferung installieren.

6.3. Patch-Management nach der Systemabnahme

6.3.1. Patch-Management-Lifecycle

Der Lieferant verpflichtet sich mindestens zweimal pro Jahr Updates und Patches einzuspielen.

Sollte für ein eingesetztes Produkt eines Drittanbieters, z.B. ein Betriebssystem oder eine andere Komponente (Software, Datenbanken, Anwendungen, etc.), das Ende des Lifecycles verkündet werden, muss der Lieferant entweder:

- die Komponente auf die aktualisierte neuere Version migrieren,
- eine adäquate Alternative einsetzen,
- oder den weiteren Support von Sicherheitspatches für die ältere Version vertraglich mit dem Drittanbieter sicherstellen.

6.3.2. Ausnahmen bei Konflikten

Sollte zwingend notwendige Funktionalität durch eine verfügbare Aktualisierung deaktiviert oder eingeschränkt werden, so ist das weitere Vorgehen mit der HDT Veritas abzustimmen. Dasselbe gilt, falls eine bestimmte Version einer Software benötigt wird, um Herstellersupport für ein anderes eingesetztes Produkt zu erhalten. Die jeweiligen Auswirkungen auf die Funktionalität und Sicherheit sind durch den Lieferanten aufzuzeigen.

6.4. Dokumentation und Nachweis

Die Durchführung des Patchens ist im Voraus zu planen und zu dokumentieren. Die HDT Veritas muss sowohl über geplante als auch durchgeführte Patches informiert werden.

7. Softwareentwicklungsprozesse

Die Berücksichtigung der Sicherheit in Entwicklungsprozessen (Security by Design) ist in vielen Fällen ein effizienterer Weg, um ein sicheres Softwareprodukt herzustellen, als das nachträgliche Patching und Ausrollen in der Produktion. Die Softwareentwicklungsprozesse des Lieferanten müssen so ausgelegt sein, dass der Sicherheit der entwickelten Software angemessene Beachtung in allen wichtigen Entwicklungsphasen geschenkt wird und die Prozesse sich an den allgemein anerkannten Industriestandards orientieren. Insbesondere sollen folgende Punkte berücksichtigt werden:

- Etablierte Standards der sicheren Softwarearchitektur
- Die Entwickler müssen sich an etablierte Standards (z.B. OWASP Top 10, BIZEC, etc.) zur sicheren Programmierung halten, um Schwachstellen vorzubeugen. Diese Standards müssen dokumentiert werden und den Entwicklern z.B. in Schulungen bekannt gemacht werden.
- Secure-Code-Reviews als Teil der Qualitätssicherung und Testing.
- Dokumentation und Aktualisierung von verwendeten Fremd-Komponenten (z.B.: Open-Source Bibliotheken)
- Die Testverfahren beim Lieferanten sollen die implementierten Sicherheitsmechanismen und -funktionen (Verschlüsselung, Zugriffskontrollen, Authentisierung und andere) explizit beinhalten.
- Sicherheitsüberprüfungen entsprechend den vorgesehenen Betriebsumgebungen, z.B. unabhängige Penetrationstests für die Systeme, die aus den externen bzw. nicht abgesicherten Netzen erreichbar sein sollen.
- Ergebnisse relevanter Sicherheitsüberprüfungen müssen der HDT Veritas zur Verfügung gestellt werden.

8. Sicherheits- und Schwachstellenmanagement

Der Lieferant muss seine Produkte einer kontinuierlichen Prüfung auf Schwachstellen unterziehen, bspw. in Form eines Schwachstellenscans oder einer Konfigurationsüberprüfung. Die letzte Prüfung darf zu keinem Zeitpunkt länger als 12 Monate zurück liegen, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren. Das Schwachstellenmanagement berücksichtigt alle Komponenten der technischen Architektur einschließlich der Betriebssysteme, Datenbanken, Server (z.B. Web, SSH), Middleware und Bibliotheken. Die Ergebnisse werden verwendet, um neue Schwachstellen in Bezug auf die Kritikalität und die geschäftlichen Auswirkungen zu beurteilen.

8.1. Schwachstellen

Jede Schwachstelle muss vom Lieferant an die HDT Veritas Hessen GmbH gemeldet und bzgl. möglicher funktionaler und sicherheitsrelevanter Auswirkungen bewertet werden. Zusätzlich sollen Schwachstellen auf technischer Ebene zum Beispiel nach CVSS2/CVSS3 oder einem Vergleichbaren System bewertet werden. Der Umfang des Schwachstellenmanagement umfasst jede Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität oder Vertraulichkeit der Vermögenswerte (materielle oder immaterielle) oder auf eine bei der HDT Veritas operierende Dienstleistung des Lieferanten nehmen kann.

Bei Bewertung der Kritikalität nach CVSS2/CVSS3, sollte eine Einstufung der Schwachstellen in die Stufen „kritisch“, „hoch“, „mittel“ und „niedrig“ - angelehnt an die Einstufung des „National Institute of Standards and Technology“1 – erfolgen.

8.1.1. Schwachstellenanalyse

Der Lieferant ist verpflichtet, kontinuierlich Quellen für Sicherheitsempfehlungen zu sichten und diese in Bezug auf die der HDT Veritas zur Verfügung gestellten Assets zu bewerten. Sollte eine Komponente von der Sicherheitslücke betroffenen sein, wird von dem Lieferanten erwartet, die Einstufung der Kritikalität nach CVSS2/CVSS3 und die „zeitliche“ Bewertung durchzuführen.

Es können mit dem Lieferanten weitere Kriterien für Schwachstellen vereinbart werden, bei denen die HDT Veritas vom Lieferanten oder Hersteller informiert werden muss und wie dieses erfolgen sollte.

8.1.2. Schwachstellenbehebung

Finale Lösungszeit = Zeit benötigt für den Patch / die Wartungsfreigabe / die korrekte Installation der Lösung; Zeitraum, in dem auf den Service aus öffentlichen / externen Netzwerken zugegriffen werden kann.

Zeit zur Neutralisierung = Zeit für eine vorläufige Lösung oder einen Workaround für den Fall, dass der Patch nicht innerhalb eines bestimmten Zeitrahmens verfügbar ist. Vom Lieferanten wird erwartet, dass eine Lösung mit einem Best-Effort-Ansatz und nach bestem Wissen erarbeitet wird. Die Zeitzählung beginnt mit der Benachrichtigung des Lieferanten über die Schwachstelle.

8.1.3. Kommunikation

Die HDT Veritas GmbH muss über identifizierte Schwachstellen ab der Kritikalitätsstufe „mittel“ unmittelbar informiert werden. Bei Schwachstellen niedriger Kritikalität genügt eine Sammelmeldung nach 30 Tagen.

Zur Meldung der Schwachstellen an die HDT Veritas müssen kryptographische Verfahren nach dem Stand der Technik zur Geheimhaltung und Integrität der Übermittlung dieser Mitteilung genutzt werden.

8.2. Sicherheitsvorfälle

Der Lieferant ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potenziell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben können, umgehend ohne Zeitverzug der HDT Veritas melden. Dies könnte z.B. auch Industriespionage oder eine Sicherheitslücke im Source-Code sein.
Der Lieferant wird im Falle eines Vorfalls auf Nachfrage der HDT Veritas Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitstellen.

IT-Betrieb:
Der Lieferant muss im Rahmen seiner Möglichkeiten Lösungen etablieren, um sicherheitsrelevante Ereignisse erkennen zu können. Dies umfasst beispielsweise die Auswertung sicherheitsrelevanter Ereignisse und die Verwendung dem Stand der Technik entsprechenden Erkennungsmechanismen. Prozesse zur Reaktion auf Sicherheitsvorfälle, sowie die dazugehörigen Rollen und Verantwortlichkeiten müssen definiert sein.

9. Zusammenarbeit mit Dritten

Wenn der Lieferant Teile der Betriebsleistung oder anderer Dienstleistungen für die HDT Veritas an weitere Dienstleister auslagert, müssen die von der HDT Veritas in diesem Dokument beschriebenen Sicherheitsanforderungen in den Vereinbarungen mit den Dienstleistern berücksichtigt werden. Die Sicherheitsanforderungen mit den Dienstleistern müssen so definiert werden, dass die Sicherheitsstandards für die Daten und Leistungen der HDT Veritas in jedem Fall eingehalten werden und dass der Lieferant in der Lage ist, eigene Verpflichtungen zur Sicherheit gegenüber der HDT Veritas vollumfassend zu erfüllen. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich Subunternehmer ist gegenüber der HDT Veritas nachzuweisen. Der Lieferant muss die HDT Veritas im Vorfeld von Entscheidungen über die Auslagerung von Betriebs- oder Dienstleistungen informieren.

Jeder, der im Namen des Lieferanten agiert, der entfernten oder lokalen Zugriff auf das Informationssystem der HDT Veritas haben muss, muss Informationen zu seiner Identität bereitstellen. Der Lieferant stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt.
Sollte der Lieferant mit Subunternehmern zusammenarbeiten, um den Vertrag mit der HDT Veritas zu erfüllen, muss der Lieferant diesen ausdrücklich als Subunternehmer identifizieren und er muss sicherstellen, dass der Subunternehmer die sicherheitsrelevanten Vorgaben der HDT Veritas umsetzt.
Der Lieferant beauftragt nur Personen, die über entsprechende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung verfügen.

10. Einhaltung der Vorgaben

Der Lieferant stimmt zu, dass die HDT Veritas oder ein anderer beauftragter Dritter im Auftrag der HDT Veritas die relevanten Teile der Organisation, sowie die zum Produkt gehörenden Systeme in Bezug auf die Informationssicherheit des Lieferanten auditieren darf. Diese Überprüfung wird einmalig vor dem Go-Live der Software durchgeführt. Die Prüfungen werden auf der Grundlage der von dem Lieferanten zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden jeweils einvernehmlich vereinbart.

Zusätzlich muss der Lieferant Abweichungen von den vereinbarten Sicherheitsanforderungen melden.