Leitlinien für Betriebssicherheit für Auftragnehmer/Lieferanten

A. Aktualität der bereitgestellten Sicherheitsaktualisierungen

Der Lieferant verpflichtet sich, von ihm ausgelieferte Soft- und Hardware stets auf dem aktuell sicheren Versionsstand zu halten oder solche Komponenten seiner aktuellen Software unverzüglich unaufgefordert zu ersetzen, deren offizieller End-of-Service Status erreicht ist. Damit sind insbesondere Softwarebibliotheken und Laufzeitumgebungen gemeint, die zum bestimmungsgemäßen Ablauf der Software bestimmt oder erforderlich sind und die vom Lieferanten mit ausgeliefert werden. Dazu hat der Lieferant Sicherheitsaktualisierungen, die von einem Hersteller bereitgestellt werden, unverzüglich zu installieren oder bereit zu stellen oder für den Fall, dass der Lieferant zugleich der Hersteller ist, Sicherheitslücken aus CVE und BSI Bekanntmachungen in angemessener Zeit zu schließen, indem er die notwendigen Sicherheitsaktualisierungen bereitstellt.

Sofern dazu ein gesonderter Servicevertrag erforderlich ist, hat der Lieferant darauf spätestens bei Angebotsabgabe hinzuweisen. Unterlässt er dies, so entsteht ihm bei Rücktritt oder Irrtumsanfechtung durch KDO kein Schadensersatzanspruch, wenn die Anfechtung oder der Rücktritt auf diesem Grund beruht, dies schadet nicht der Geltendmachung weiterer Ansprüche gegen den Lieferanten.

B. Sichere Übergabe

Personenbezogene und sensible Daten

Personenbezogene oder sensible Daten wie z.B. Datenbankdumps, Passwörter oder kryptografische Schlüssel sind stets verschlüsselt nach dem Stand der Technik zwischen KDO und Lieferant zu übertragen. Hierzu eignen sich beispielsweise PGP oder S-MIME verschlüsselte Mails oder die Bereitstellung in einem verschlüsselten Archiv unter Beachtung der Sicherheit des eingesetzten Verschlüsselungsalgorithmus.

Eine telefonische Übertragung ist bei kurzen Informationen wie z. B. Benutzernamen und Passwörtern ebenfalls zulässig.

Ebenfalls zulässig ist der Einsatz der KDO Owncloud/Nextcloud für die Datenübermittlung, die zwingend mit einem Passwort gesichert werden muss, oder einer vergleichbaren, sicheren Lösung. Dabei ist das Passwort auf einem anderen Kanal zu übermitteln als per E-Mail oder in der Owncloud/Nextcloud selbst.

C. Übertragung von Software und Konfigurationen

1. Manuelle Übertragung

Software, Source-Code oder Konfigurationsdateien, die keine sensiblen Daten enthalten, müssen nicht verschlüsselt übertragen werden. Die Integrität der übertragenen Daten sollte jedoch mittels eines Hash-Verfahrens nach dem Stand der Technik sichergestellt werden. So könnten Daten bspw. in einem Archiv, dessen Hashwert telefonisch verglichen wird, übertragen werden.

Vor der Übertragung von Binärdateien (z. B. kompilierte Programmdateien oder Bibliotheken) sind diese mit einem aktuellen Antivirenprogramm zu prüfen, das Ergebnisprotokoll ist zusammen mit den Dateien zu übertragen.

2. Automatische Übertragung mittels Repositories

Erfolgt die Bereitstellung von Software, Source-Code oder Konfigurationsdateien mittels eines Repositories, sind auch hier die Funktionen zur Prüfung der Integrität der übertragenen Daten zu nutzen und wenn möglich ein verschlüsselter Übertragungsweg zu verwenden. Zudem ist sicherzustellen, dass Änderungen am Repository-Inhalt nur durch einen eingeschränkten, autorisierten Personenkreis durchgeführt und dokumentiert werden. Die vorgenommenen Änderungen müssen personenbezogen nachvollziehbar sein.

Die Inhalte der bereitgestellten Repositories sind durch den Anbieter regelmäßig, vorzugsweise automatisch, mit einem Antivirenprogramm zu prüfen.

D. Sichere Software-Konfiguration

1. Einsatz von Verschlüsselung

Die Schnittstellen und Dienste der zu betreibenden Software müssen zur Datenübertragung Verschlüsselungsverfahren gemäß dem Stand der Technik anbieten. Werden keine Verschlüsselungsverfahren angeboten oder entsprechen diese nicht dem Stand der Empfehlungen des BSI, muss dieses bei Angebotsabgabe und vor Auftragserteilung mitgeteilt werden. Das Fehlen eines entsprechenden Hinweises berechtigt KDO zum Rücktritt, es sei denn, die Kenntnis von KDO zum Zeitpunkt der Angebotsabgabe/Auftragserteilung kann nachgewiesen werden.

2. Einsatz aktueller Komponenten

Die Software muss kompatibel zum von der KDO eingesetzten Serverbetriebssystem ausgeliefert werden. Wenn nicht anders vereinbart, muss die Software die Systembibliotheken des Serverbetriebssystems verwenden. Zusätzliche Bibliotheken sind aus den Repositories des Distributors (RedHat, Centos) zu beziehen. Updates der Bibliotheken durch den Distributor sind rechtzeitig zu berücksichtigen und zu testen. Falls hiervon abweichende Bibliotheken oder Komponenten eingesetzt werden, müssen Sicherheitsmeldungen zu den betroffenen Produkten durch den Hersteller/Kunden verfolgt und behandelt werden, die KDO ist entsprechend zu informieren. Wird die Software als Quellcode bereitgestellt, der durch die KDO zu kompilieren ist, sind alle Build-Skripte, Komponenten und eine Anleitung auszuliefern, die zu einer erfolgreichen Kompilation führen.

Es gelten die Bestimmungen für die Bereitstellung von Binärdateien. Die KDO kann eine Frist zur Beseitigung von Sicherheitsproblemen in Komponenten und Bibliotheken setzen, nach deren Ablauf KDO auf den Weiterbetrieb der Software aus Sicherheitsgründen verzichten kann. Der Lieferant gerät dadurch möglicherweise in Leistungsverzug.

3. Sichere Kennwörter

Die Kennworttipps des BSI sind bei der Einrichtung von jeglicher Art von Zugängen innerhalb der Software einzuhalten und wenn möglich technisch durchzusetzen. Die Verwendung von Standardkennwörtern ist nicht erlaubt.

4. Rechtemanagement

Die bereitgestellte Software muss nach dem "Least Privilege"-Prinzip so konfiguriert sein, dass sie nur die für den Betrieb nötigten Rechte erfordert. Begründungen für die Erforderlichkeit erhöhter Rechte sind zu dokumentieren.

E. Sichere Virtuelle Maschinen

Für die Bereitstellung von VMs, die für einen Betrieb bzw. Hosting durch die KDO vorgesehen sind, gelten die folgenden Anforderungen.

1. Format

Virtuelle Maschinen sind im vereinbarten Format bereitzustellen. Es gelten die Regelungen zur Übertragung von Software und Konfigurationen. Das Image darf nur dem an der Bereitstellung beteiligtem Personenkreis zur Verfügung

gestellt werden und ist durch angemessene Maßnahmen (z.B. Verschlüsselung, Zugriffskontrolle) vor unberechtigtem Zugriff zu schützen.

2. Betriebssystem und Software

Das eingesetzte Gast-Betriebssystem und die betriebene Software der virtuellen Maschinen müssen jeweils in der aktuellsten Version vorliegen. Das Betriebssystem und die eingesetzte Software müssen sich im zeitlichen Wartungsrahmen des Herstellers befinden. Gültige Lizenzen müssen für Betriebssystem und Software vorliegen.

Microsoftlizenzen dürfen nicht mit einer virtuellen Maschine ausgeliefert werden. Vorher MUSS ein `sysprep` ausgeführt werden.

Die virtuelle Maschine muss einer Serverhärtung unterworfen worden sein, so dass nur die Dienste und Services gestartet werden und kommunzieren, die erforderlich sind. Die durchgeführten Einstellungen sind als Dokumentation mit zu übergeben.

3. Updates

Die kontinuierliche und zeitnahe Versorgung des Betriebssystems und der installierten Software mit Updates ist sicherzustellen. Vor Auslieferung der VM an die KDO sind die aktuellsten Updates und Sicherheitspatches zu installieren.

4. Software und Updates in Windows-Umgebungen

Softwarepakete müssen kompatibel zu einem Softwareverteilungssystem ausgeliefert werden z. B. MSI Pakete (Microsoft-Installer), damit ein Rollout und Rollback automatisiert erfolgen kann. In Folge eines durchgeführten Rollbacks dürfen keine Anwendungsreste zurückbleiben.

5. Kennwortrichtlinie

Die Kennworttipps des BSI ist bei der Einrichtung von jeglicher Art von Zugängen auf der VM einzuhalten. Sämtliche Kennwörter sind individuell für die VM entsprechend anzupassen. Die Verwendung von Standardkennwörtern, auch beim Einsatz mehrerer VMs, ist nicht erlaubt. Die im übermittelten Image gespeicherten Kennwörter sind als Initialkennwörter zu behandeln und bei Inbetriebnahme der VM — sofern diese durch den Lieferanten erfolgt — so bald wie möglich gemäß der Kennwortrichtlinie zu ändern.

6. Personenbezogene Konten

Konten zur Nutzung und Wartung der VM sind personenbezogen zu erstellen. Funktionskonten, die von mehreren Personen genutzt werden, sind nicht gestattet.

F. Sichere Container-Virtualisierung

1. Verwendung sicherer Images

Entsprechend den Regelungen zur sicheren Übertragung von Software muss sichergestellt sein, dass Images nur aus vertrauenswürdigen Registries/Repositories stammen. Sie müssen unverändert und frei von bekannten Schwachstellen sein. Es gelten die Regelungen zur automatischen Übertragung mittels Repositories (siehe oben).

2. Härtung der Software im Container

Alle nicht benötigten Bestandteile der Anwendung bzw. des Dienstes, die bzw. der im Container ausgeführt wird, müssen deinstalliert werden. Die Konfiguration der Anwendung bzw. des Dienstes muss angemessen gehärtet werden, gemäß der entsprechenden BSI IT-Grundschutz Bausteine der beteiligten Komponenten, unter Berücksichtigung der Schutzstufe der verarbeiteten Daten.

3. Persistenz von Nutzdaten

Nutzdaten, auf die durch Anwendungen bzw. Dienste im Container zugegriffen wird oder die sie dauerhaft abspeichern, müssen persistent außerhalb des Containers gespeichert werden.

4. Speicherung von Zugangsdaten

Zugangsdaten müssen so gespeichert und verwaltet werden, dass nur berechtigte Personen und Container hierauf zugreifen können. Insbesondere muss sichergestellt sein, dass Zugangsdaten nur an zugangsgeschützten Orten und nicht in den Images liegen. Die von der Verwaltungssoftware bereitgestellten Verwaltungsmechanismen für Zugangsdaten sollten eingesetzt werden. Folgende Zugangsdaten müssen mindestens berücksichtigt werden:

- Passwörter jeglicher Konten
- API-Keys für von der Anwendung genutzte Dienste
- Private Schlüssel bei Public-Key Authentisierung

5. Rechtevergabe und -verwaltung

Die Konten der Prozesse in den Containern dürfen keine Berechtigungen auf dem Container-Host haben. Wenn dies dennoch notwendig ist, dürfen diese Berechtigungen nur für unbedingt notwendige Daten gelten.

Es muss sichergestellt sein, dass der administrative Fernzugriff nur auf die Cluster-Betriebssoftware oder den Container-Host und nur über diese auf die Container selbst erfolgen kann. Container dürfen selbst keine Dienste für administrativen Fernzugriff enthalten.

Alle Anwendungsdienste in Containern dürfen nur unter einem nicht privilegierten Account gestartet werden. Sie dürfen nicht über erweiterte Privilegien für die Container-Dienste oder die Cluster-Betriebssoftware verfügen.

G. No-Spy-Funktionalität

Es werden keine Daten abgeführt, auf die nicht in der Leistungsbeschreibung ausdrücklich hingewiesen wurde.

H. Tests

Software (auch Patche) müssen zuvor vom Lieferanten getestet worden sein. Nachweisliche, schuldhafte Unterlassung führt unmittelbar zur Verwirkung einer gesondert zu vereinbarenden Vertragsstrafe oder zur Geltendmachung eines Verzugsschadens.

I. Keine Software, die unter Root/Superuser Rechten laufen muss

Software darf nicht zwingend unter ROOT/SUPERUSER Rechten laufen müssen. Ein Ablaufenlassen der Software unter einem nichtprivilegierten Nutzer muss möglich und voreingestellt sein. Sollte das in einem Fall nicht durchführbar sein, so ist KDO zwingend VOR ÜBERGABE oder VOR INBETRIEBNAHME über diese Tatsache zu informieren.

Copyright

Dieses Dokument ist eine Publikation der KDO. Alle Rechte vorbehalten. Reproduktionen jeder Art, z. B. Fotokopie, Mikroverfilmung oder die Erfassung in elektronischen Datenverarbeitungsanlagen, bedürfen der schriftlichen Genehmigung des Herausgebers. Ein Nachdruck, auch auszugsweise, ist verboten. Bitte beachten Sie die Schutzstufe.

Impressum

Herausgeber
Kommunale Datenverarbeitung Oldenburg (KDO)
Elsässer Straße 66 ■ 26121 Oldenburg
Telefon: 0441 9714-0 ■ Fax: 0441 9714-148 ■ E-Mail: info@kdo.de

© Kommunale Datenverarbeitung Oldenburg (KDO) ■ Elsässer Str. 66 ■ 26121 Oldenburg ■ www.kdo.de