

Vereinbarung zur Informationssicherheit

zwischen

VAG Verkehrs-Aktiengesellschaft

Am Plärrer 43

90429 Nürnberg

(nachfolgend Auftraggeber genannt)

und

<Firma>

<Straße>

<PLZ> <Ort>

(nachfolgend Auftragnehmer genannt)

Inhalt

1	Vulnerability-Management.....	3
1.1	Methodik und Umfang	3
1.2	Vulnerability-Assessment	3
1.3	Behebung von Schwachstellen	4
1.4	Kommunikation	4
2	Patch-Management	4
2.1	Umfang des Patchings	4
2.2	Patch-Level während der Systemabnahme	5
2.3	Patch-Management nach der Systemabnahme.....	5
2.3.1	Patch-Management-Lifecycle	5
2.3.2	Ende des Lifecycle	5
2.3.3	Ausnahmen bei Konflikten.....	5
2.4	Dokumentation und Nachweis	5
3	Systemhärtung	5
3.1	Minimale Installationsprinzipien	6
3.2	Netzwerkdienste (Netzwerkzugänge)	6
3.3	Konfigurationsstandards.....	6
3.4	Standardpasswörter	6
3.5	Backdoors	6
3.6	Kontrolle und Audit der in diesem Kapitel genannten Konditionen.....	6
4	Benachrichtigung über sicherheitsrelevante Vorfälle	6
5	Sicherheitsanforderungen für den IT-Betrieb	7
5.1	Security-Incident-Management.....	7
5.2	Sicherheit in Auslagerungsprozessen	7
6	Nicht-technische Sicherheit	7
6.1	Externe Systemzugriffe	7
7	Ansprechpartner Informationssicherheit	8

Der Auftraggeber betreibt ein Informationssicherheitsmanagementsystem (ISMS) mit dem Ziel die Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Daten bzw. der relevanten Systeme sicherzustellen.

Auch Lieferanten leisten mit ihren Dienstleistungen und Produkten einen wichtigen Beitrag zur Informationssicherheit, weshalb mit dieser Vereinbarung entsprechende Regelungen definiert werden.

1 Vulnerability-Management

Der Auftragnehmer 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 24 Monate zurück liegen, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren. Das Vulnerability-Management 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.

Sind vom Auftragnehmer bereitgestellte Software-, Firmware- oder Hardware-Komponenten betroffen, ist der Auftragnehmer verpflichtet, umgehend die Schwachstellen an den Auftraggeber zu melden.

1.1 Methodik und Umfang

Jede Schwachstelle muss vom Auftragnehmer an den Auftraggeber 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 Vulnerability-Managements umfasst jede Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität oder Vertraulichkeit der Vermögenswerte (materielle oder immaterielle) oder auf eine beim Auftraggeber operierende Dienstleistung des Auftragnehmers 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:

CVSS2-Score	CVSS3-Score	Kritikalitätsstufe
10	9.0-10.0	kritisch
7.0-9.9	7.0-8.9	hoch
4.0-6.9	4.0-6.9	mittel
0.0-3.9	0.0-3.9	niedrig

1.2 Vulnerability-Assessment

Der Auftragnehmer ist angehalten, kontinuierlich Quellen für Sicherheitsempfehlungen zu sichten und diese in Bezug auf die dem Auftraggeber zur Verfügung gestellten Assets zu bewerten. Sollte eine Komponente von der Sicherheitslücke betroffenen sein, wird von dem

¹ <https://nvd.nist.gov/cvss.cfm>

Auftragnehmer erwartet, die Einstufung der Kritikalität nach CVSS2/CVSS3 und die „zeitliche“ Bewertung durchzuführen.

Es können mit dem Auftragnehmer weitere Kriterien für Schwachstellen vereinbart werden, bei denen der Auftraggeber vom Auftragnehmer oder Hersteller informiert werden muss und wie dieses erfolgen sollte.

1.3 Behebung von Schwachstellen

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 Auftragnehmer wird erwartet, dass eine Lösung mit einem Best-Effort-Ansatz und nach bestem Wissen erarbeitet wird. Die Zeitzählung beginnt mit der Benachrichtigung des Auftragnehmers über die Schwachstelle.

Priorität	Kritikalitätsstufe	Finale Lösungszeit	Zeit zur Neutralisierung
1	kritisch	1 Monat	7 Tage
2	hoch	3 Monate	14 Tage
3	mittel	12 Monate	2 Monate
4	niedrig	Nach Absprache	Nach Absprache

1.4 Kommunikation

Der Auftraggeber muss über identifizierte Schwachstellen ab der Kritikalitätsstufe „hoch“ unmittelbar informiert werden. Bei Schwachstellen mittlerer und niedriger Kritikalität genügt eine Sammelmeldung nach 90 Tagen.

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

2 Patch-Management

Der Auftragnehmer 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 Auftragnehmers durch Updates behoben werden.

2.1 Umfang des Patchings

Der Umfang des Patchings muss jede Komponente des Systems, wie vom Auftraggeber 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

2.2 Patch-Level während der Systemabnahme

Der Auftragnehmer hat sicherzustellen, dass alle Systeme vor der Abnahme gepatcht werden. Der Patch-Level darf dabei nicht älter als 6 Monate ab dem Tag der Systemabnahmeerklärung sein. Der Auftragnehmer muss alle öffentlich verfügbaren Patches als Teil der Lieferung installieren.

2.3 Patch-Management nach der Systemabnahme

2.3.1 Patch-Management-Lifecycle

Der Auftragnehmer verpflichtet sich, bei Bedarf Updates und Patches einzuspielen. Für die Bereitstellung sicherheitsrelevanter Patches durch den Auftragnehmer gelten hiervon unabhängig die in Abschnitt 1.3 festgelegten Zeitrahmen.

2.3.2 Ende des Lifecycle

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 Auftragnehmer 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.

2.3.3 Ausnahmen bei Konflikten

Sollte zwingend notwendige Funktionalität durch eine verfügbare Aktualisierung deaktiviert oder eingeschränkt werden, so ist das weitere Vorgehen mit dem Auftraggeber 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 Auftragnehmer aufzuzeigen.

2.4 Dokumentation und Nachweis

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

3 Systemhärtung

Der Auftragnehmer verpflichtet sich, die von ihm für die Erbringung der Dienste verwendeten Systeme zu härten, um die Auswirkungen potentieller Sicherheitsrisiken zu minimieren. Dies muss vor der Deklaration einer Systemabnahme durch den Auftraggeber geschehen sein. Der Auftragnehmer 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.

3.1 Minimale Installationsprinzipien

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

A) Jede Softwarekomponente, die für die Anwendung oder nach der Logik des Dienstes benötigt wird

B) Jede aus der Integration mit anderen Services resultierende andere Anwendung oder Softwarekomponente

C) Jede aus Betriebs- und Wartungsanforderungen resultierende Softwarekomponente

Jede andere Software darf nicht installiert werden, außer der Auftragnehmer und der Auftraggeber 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.

3.2 Netzwerkdienste (Netzwerkzugänge)

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

3.3 Konfigurationsstandards

Der Auftragnehmer stellt sicher, dass die vom Auftraggeber vorgegebenen allgemeinen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden.

3.4 Standardpasswörter

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

3.5 Backdoors

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

3.6 Kontrolle und Audit der in diesem Kapitel genannten Konditionen

Der Auftragnehmer verpflichtet sich, dass er hinsichtlich seiner Produkte mit geeigneten Maßnahmen und Protokollen, die mit dem Auftraggeber abzustimmen sind, nachweist, dass alle in diesem Kapitel genannten Anforderungen eingehalten werden.

4 Benachrichtigung über sicherheitsrelevante Vorfälle

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potentiell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben können, umgehend ohne Zeitverzug dem Auftraggeber zu melden. Dies könnte z.B. auch Industriespionage oder eine Sicherheitslücke im Source-Code sein.

Der Auftragnehmer wird im Falle eines Vorfalles auf Nachfrage des Auftraggebers Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitstellen.

5 Sicherheitsanforderungen für den IT-Betrieb

5.1 Security-Incident-Management

Der Auftragnehmer 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. Zur Meldung der Sicherheitsvorfälle s. den Abschnitt „Benachrichtigung über sicherheitsrelevante Vorfälle“.

5.2 Sicherheit in Auslagerungsprozessen

Wenn der Auftragnehmer Teile der Betriebsleistung oder anderer Dienstleistungen für den Auftraggeber an weitere Dienstleister auslagert, müssen die vom Auftraggeber 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 des Auftraggebers und Leistungen für den Auftraggeber in jedem Fall eingehalten werden und dass der Auftragnehmer in der Lage ist, eigene Verpflichtungen zur Sicherheit gegenüber dem Auftraggeber vollumfassend zu erfüllen. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich Subunternehmer ist gegenüber dem Auftraggeber nachzuweisen. Der Auftragnehmer muss den Auftraggeber im Vorfeld von Entscheidungen über die Auslagerung von Betriebs- oder Dienstleistungen informieren.

6 Nicht-technische Sicherheit

6.1 Externe Systemzugriffe

Einfügen falls relevant

Die vom Auftraggeber zur Verfügung gestellten externen Systemzugriffe müssen vom Auftragnehmer protokolliert werden. Hierfür muss wenigstens festgehalten werden:

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

