- Leitlinie -

Informationssicherheits-anforderungen für Vertragspartner

Herausgeber: IT

Inhaltsverzeichnis

1 Ziel und Zweck

Dieses Dokument legt die Erwartungen der WEBER-HYDRAULIK zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von deren Daten und Vermögenswerten fest.

Der Verstoß bzw. die Missachtung dieser Regelungen kann rechtliche Konsequenzen nach sich ziehen.

2 Geltungsbereich

Diese Handlungsleitlinie gilt für Vertragspartner, die auf Basis vertraglicher Regelungen Lieferungen und Leistungen für die WEBER-HYDRAULIK erbringen.

Die in der Handlungsleitlinie festgelegten Regelungen sind einzuhalten. Abweichungen sind nur durch Freigabe des Auftraggebers möglich.

3 Auditrecht

WEBER-HYDRAULIK ist berechtigt, Vertragspartner auf der Grundlage der Leitlinie mindestens einmal im Jahr zu auditieren.

4 IT-Sicherheitspolicy und Standards

Vertragspartner mit Zugang zu Informationen der WEBER-HYDRAULIK müssen deren Informationssicherheitsrichtlinien und die damit verbundenen Dokumente einhalten.

Ferner müssen Vertragspartner über geeignete Cyber-Risiko-Governance-Prozesse verfügen, um das Risiko für die ihrerseits eingesetzten IT-Systeme in Bezug auf die Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität der WEBER-HYDRAULIK zu gewährleisten.

Es müssen von der Unternehmensleitung des Vertragspartners genehmigte Richtlinien und Standards zur Steuerung des Cyber-Risikos etabliert sein. Diese sind nachweislich mindestens einmal jährlich zu überprüfen.

5 Informationssicherheitsinformation für Vertragspartner

Im Rahmen bestehender Vertrags- und Lieferbeziehungen ist es von größter Bedeutung, dass Vertragspartner den Sicherheitsinteressen und Anforderungen an die Informationssicherheit der WEBER-HYDRAULIK sowie deren Kunden entsprechen. Deshalb sind sämtliche mit entsprechender Klassifizierung eingestufte Umfänge (wie z. B. Design- und Entwicklungsdaten sowie andere entsprechend kritische Informationen) in geeigneter Weise zu verarbeiten und zu schützen.

Mit TISAX (Trusted Information Security Assessment Exchange - www.tisax.org) und TPISR (Third Party Information Security Requirements - https://www.aiag.org/supplychain-management/cybersecurity) werden Branchenstandards für den Informationsschutz definiert und Bewertungsanforderungen festgelegt, die innerhalb der Lieferkette zu gewährleisten sind.

Der Vertragspartner ist angehalten, aktiv dafür zu sorgen, dass seine Lieferungen und Leistungen (dies beinhaltet insbesondere Daten und kritische Informationen) eine entsprechende Klassifizierung erfahren haben und ein zertifiziertes Informationssicherheitsmanagementsystem (z.B. ISO 27001) betrieben wird. Vertragspartner, die Lieferungen und Leistungen im Zusammenhang mit dem Automotive Geschäftsfeld der WEBER-HYDRAULIK erbringen, müssen auf Verlangen ein gültiges TISAX-Label vorweisen.

Im Sinne der Informationssicherheitsanforderungen der WEBER-HYDRAULIK hat der Vertragspartner die Verpflichtung, sämtliche Lieferungen und Leistungen, sowie den gesamten im Zusammenhang stehenden Datenbestand der WEBER-HYDRAULIK, nach dem Stand der Technik gegen unberechtigten Zugriff, Veränderung, Zerstörung und sonstigen Missbrauch zu sichern. Ferner sind Daten der WEBER-HYDRAULIK strikt von Daten anderer Kunden des Vertragspartners zu trennen.

Ist ein identifizierter, signifikanter Fall der Verletzung der Informationssicherheit eingetreten, ist die Informationssicherheitsbeauftragte der WEBER-HYDRAULIK unverzüglich zu informieren.

Kontaktdaten:

Ruth-Maria Gerlach
Data-Security@weber-hydraulik.com
Telefon: +49 7161 / 65 393 30

Ferner hat der Vertragspartner zu gewährleisten, dass seine Unterauftragnehmer durch geeignete vertragliche Regelungen den beschriebenen Anforderungen an die Informationssicherheit genügen.

6 Asset Management

Der Vertragspartner hat von WEBER-HYDRAULIK zur Verfügung gestellte Informationen gemäß der seitens WEBER-HYDRAULIK angegebenen Klassifizierung, jedoch mindestens als vertrauliche Information, zu behandeln.

Es sind regelmäßig Inventuren der Assets zu erstellen und zu aktualisieren.

Für die Übertragung von Informationen ist eine starke Verschlüsselung zu verwenden.

Die Weitergabe sowie Vervielfältigung von vertraulichen Unterlagen sowie die Verwertung und Mitteilung ihres Inhalts ist nicht ohne vorherige schriftliche Genehmigung der WEBER-HYDRAULIK gestattet.

WEBER-HYDRAULIK Informationen dürfen außerhalb des vertraglich vereinbarten Verwendungszwecks nicht gespeichert, gedruckt, kopiert, weitergegeben oder auf andere Weise verarbeitet werden.

Zuwiderhandlungen werden entsprechend verfolgt.

7 Benutzer-Authentifizierung

Der Zugang zu IT-Systemen des Vertragspartners bzw. auf dort befindliche Daten der WEBER-HYDRAULIK, soll nur sicher identifizierten (authentifizierten) Benutzern möglich sein. Dafür muss die Identität eines Benutzers durch geeignete Verfahren sicher festgestellt sein.

Es müssen Zugriffskontrollen für Informationssysteme, Netzwerke und Anwendungen implementiert sein, die

- die Identität aller Benutzer prüfen und
- den Zugriff ausschließlich auf autorisierte Benutzer beschränken.

Zugriffskontrollen müssen auf einem rollenbasierten Zugriffsmodell basieren. Es müssen differenzierte Zugriffsebenen für Endbenutzer und privilegierte Zugriffe (z. B. Systemadministratoren) vorhanden sein.

Der Vergabeprozess (Zuweisung/Änderung/Löschung) für privilegierte Benutzerkennungen muss begründet und dokumentiert sein. Privilegierte Rechte werden nur nach Genehmigung vergeben.

Zugriffe für Informationssysteme, Netzwerkgeräte und Anwendungen müssen regelmäßig überprüft werden. Sofern nicht mehr benötigt, sind Zugriffe zu widerrufen.

8 Passwort-Richtlinie

Bei der Passwortgenerierung müssen folgende Mindestanforderungen eingehalten werden:

- Passwortwechsel: Änderung alle 180 Tage
- Passwortkomplexitätskriterien:
  - Mindestlänge: 10 Zeichen bestehend aus
    - mind. 1 Zahl
    - mind. 1 Sonderzeichen
    - mind. 1 Großbuchstabe
    - mind. 1 Kleinbuchstabe
- Keine Wiederverwendbarkeit der letzten 10 Passwörter
- Frühestens nach einer Woche kann das Kennwort erneut geändert werden
- Falls ein Nutzer fünfmal in Folge ein falsches Passwort eingibt, wird das betreffende Benutzerkonto gesperrt

9 Incident Management

Der Vertragspartner muss über einen dokumentierten Prozess für das Management von Sicherheitsvorfällen verfügen, um Vorfälle zu erkennen und zu behandeln.

Gemeldete Sicherheitsvorfälle müssen überprüft und anschließend analysiert werden, um ihre Auswirkungen zu bestimmen. Sämtliche bestätigten Vorfälle müssen klassifiziert, nach Prioritäten geordnet und protokolliert werden. Jeder Sicherheitsvorfall muss an die WEBER-HYDRAULIK gemeldet werden.

Kontaktdaten der Informationssicherheitsbeauftragten:

Ruth-Maria Gerlach
Data-Security@weber-hydraulik.com
Telefon: +49 7161 / 65 393 30

Sicherheitsvorfälle müssen von Personal bearbeitet werden, das in der Behandlung und Bewertung von Sicherheitsvorfällen geschult ist. Es muss sichergestellt sein, dass geeignete Verfahren für die Identifizierung, Erfassung, Beschaffung und Bewahrung von Informationen, deren Weitergabe sowie Vervielfältigung nicht ohne vorherige schriftliche Genehmigung der WEBER-HYDRAULIK erfolgt.

Der Vertragspartner ist gehalten, bei der Bearbeitung dieser Meldungen mit der WEBER-HYDRAULIK zusammenzuarbeiten.

10 Netzwerksicherheit

Der Vertragspartner muss eine geeignete Netzwerksicherheitsinfrastruktur nachweisen können. Dazu gehören u.a. Erkennungs-/Präventionssysteme (IDS/IPS) und andere Sicherheitskontrollen, die kontinuierliche Sicherheit bieten und die die Fähigkeit haben, nicht autorisierten Netzwerkverkehr einzuschränken und Angriffe einschließlich deren Auswirkungen zu erkennen und zumindest zu begrenzen.

Der Fernzugriff auf das Netzwerk des Vertragspartners muss genehmigt und auf autorisiertes Personal beschränkt werden. Ferner muss der Fernzugriff durch sichere Zugriffskontrollprotokolle, und geeignete Verschlüsselung gesichert sein.

Ungenutzte Ports und Protokolle müssen auf Servern deaktiviert werden, um die Angriffsfläche einzuschränken.

Netzwerkverbindungen, die zur Übertragung vertraulicher und streng vertraulicher Daten verwendet werden, müssen verschlüsselt sein.

Der Vertragspartner muss ein formelles Verfahren zur Genehmigung, Prüfung und Dokumentation des gesamten Netzwerks unterhalten.

11 Verschlüsselung von Laptops und mobilen Speichermedien

Geräte des Vertragspartners, auf denen sich Daten der WEBER-HYDRAULIK befinden, sind angemessen zu verschlüsseln und die Implementierung der Verschlüsselung muss kontinuierlich validiert werden. Eine entsprechende Schlüsselverwaltung muss vorhanden sein.

Zum Schutz von vertraulichen Informationen sind während der Übertragung über offene öffentliche Netze starke Kryptographie und Sicherheitsprotokolle (z. B. TLS, IPSEC, SSH usw.) zu verwenden.

Massenspeicher in Mobilgeräten (Laptops, Tablets, Smartphones) müssen verschlüsselt werden.

12 Vulnerability Management

Der Vertragspartner muss Informationen von Technologieanbietern und anderen Quellen in Bezug auf technische Schwachstellen von Betriebssystemen, Anwendungen und Netzwerkgeräten unmittelbar verfolgen. Um sicherzustellen, dass geeignete Maßnahmen ergriffen werden und um potenziellen Risiken zu begegnen, sind Schwachstellen unverzüglich zu bewerten.

Ferner muss der Vertragspartner ein Patch-Management betreiben, zur Verfügung stehende Patches umgehend anwenden und Betriebssysteme, Anwendungen und Netzwerkgeräte einheitlich, standardisiert und priorisiert patchen. Sofern ein Sicherheitspatch nicht zeitnah angewendet werden kann, müssen Maßnahmen zum Schutz des jeweiligen Systems getroffen werden.

13 Change Management

Die sicherheitsrelevanten Anforderungen an Veränderungen innerhalb der Organisation, der Geschäftsprozesse, der Informationsverarbeitung und -systeme sind kontinuierlich zu ermitteln und umzusetzen.

Änderungen mit Auswirkungen auf die IT-Sicherheit müssen entsprechend geplant und überprüft werden. Es muss ein formelles Verfahren zur Genehmigung von Änderungen etabliert sein.

14 Backup

Sämtliche Sicherungsmedien sind während des Transports und der Lagerung zu sichern. Backup-Medien, welche die Räumlichkeiten des Vertragspartners verlassen, müssen während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt werden.

Medien sollten katalogisiert sein, damit eine fehlende Speichereinheit leicht identifiziert werden kann. Medien sind so zu kennzeichnen, dass sie von Außenstehenden nicht dem jeweiligen Kunden zugeordnet werden können.

System- und Anwendungssicherungen sind so zu gestalten, dass die vollständige Systemwiederherstellung für einen Zeitraum von mindestens 30 Tagen gegeben ist. Sicherungsmedien müssen sich auf separaten Systemen befinden. Sämtliche vertraulichen Daten sind innerhalb von 30 Tagen nach Beendigung des Vertragsverhältnisses zu vernichten. WEBER-HYDRAULIK-Daten, die auf Sicherungsmedien gespeichert werden, müssen verschlüsselt werden.

15 Client-Systeme

Der Einsatz von EDR/XDR- sowie Anti-Spyware-Werkzeugen auf Client-Systemen des Vertragspartners wird vorausgesetzt.

Alle Client-Systeme, die auf vertrauliche Daten zugreifen, müssen unabhängig davon, ob sie verwendet werden oder nicht, physisch gesichert werden. Empfangene Daten und Programme werden vor ihrer Ausführung automatisch auf Schadsoftware untersucht. Ferner wird der gesamte Dateninhalt aller Systeme regelmäßig auf Schadsoftware untersucht. Die Datenübertragung durch zentrale Gateways (z.B. E-Mail, Internet, Drittnetze) wird mit einer Schutzsoftware überprüft (einschließlich verschlüsselter Verbindungen).

Client-Systeme, die von gesicherten Orten aus auf vertrauliche Daten zugreifen, müssen über ein Passwort verfügen. Es wird ein geschützter Bildschirmschoner gefordert bzw. muss nach spätestens 10 Minuten Inaktivität der Kontozugang gesperrt werden. Es werden Maßnahmen festgelegt, die verhindern, dass Schutzsoftware durch Benutzer deaktiviert oder verändert werden kann.

16 Monitoring

Der Login an kritischen Assets (Server, Netzwerk, usw.) muss vor Manipulation und unbefugtem Zugriff geschützt werden. Ereignisprotokolle, die Benutzeraktivitäten, Ausnahmen, Fehler und IT-Sicherheitsereignisse aufzeichnen, müssen implementiert und regelmäßig überprüft werden. Aktivitäten von Systemadministratoren und Systemoperatoren müssen protokolliert und die Protokolle regelmäßig überprüft werden. Protokolle sind mindestens 3 Monate aufzubewahren.

17 Server Security

Alle Produktionsserver müssen sich an einem sicheren, zugriffskontrollierten Standort befinden. Sämtliche Systeme müssen einschließlich des Patchens bekannter Schwachstellen vor dem Produktionseinsatz gehärtet werden.

Gast-, Wartungs- und Standardkonten müssen deaktiviert werden. Testkonten und Benutzerkonten werden, wenn sie nicht mehr benötigt werden, entfernt oder widerrufen.

Entwicklungs- und Testsysteme sind von der Produktionsumgebung und dem Netzwerk zu trennen. Alle nicht benötigten Ports und/oder Dienste auf Serverbetriebssystemen und Firewalls müssen

deaktiviert werden. Das Betriebssystem muss regelmäßig aktualisiert werden. Nicht genutzte Software darf nicht installiert werden. Der Zugriff auf Verzeichnisse muss im Rahmen einer restriktiven Rechtevergabe beschränkt werden. Der gesamte Netzwerkverkehr muss auf ungewöhnliche Aktivitäten/Anomalien überwacht werden.

18 Mobile Geräte

Um auf Mobilgeräten gespeicherte vertrauliche Informationen zu schützen, muss der Vertragspartner eine starke Verschlüsselung verwenden.

Personenbezogene Daten dürfen nur auf Mobilgeräten mit starker Verschlüsselung gespeichert werden. Entsprechend dokumentierte Richtlinien, Verfahren und Standards müssen etabliert sein.

19 Schutz vor Schadcode

Der Vertragspartner muss über Erkennungs- und Präventionsmaßnahmen verfügen, die vor bösartiger Software schützen. Durch Schulungen zur Sensibilisierung der Benutzer ist die entsprechende Awareness zu schaffen. Der ein- und ausgehende Netzwerkverkehr ist zur Erkennung und zum Schutz von bösartigem Code entsprechend in Echtzeit zu scannen und zu filtern (E-Mail, HTTP, FTP u. andere Messaging). Es muss verhindert werden, dass nicht autorisierter mobiler Code ausgeführt wird.

20 Zugang zu Rechenzentren/ Serverräumen

Jeder Zutritt in die Sicherheitszonen des Vertragspartners erfordert eine Zutrittskontrolle (z. B. Wachmann, Ausweisleser, elektronisches Schloss, Videoüberwachung). Zutrittsprotokolle sind für mindestens 90 Tage aufzubewahren. Der Zutritt ist auf autorisiertes Personal zu beschränken. Eine Überprüfung der vergebenen Rechte muss regelmäßig durchgeführt werden.

21 Vernichtung von Speichermedien

Der Vertragspartner muss über Verfahren zur sicheren Vernichtung von Speichermedien verfügen. Die Vernichtung ist zu protokollieren.

22 Schlussbestimmungen

Abweichungen von den oben genannten Anforderungen bedürfen der Schriftform und deren Anerkennung durch WEBER-HYDRAULIK.

23 Änderungshistorie

Rev.	Datum	Bearbeiter	Änderungen
1	09.05.2022	Ruth-Maria Gerlach (ISB), Frank Bissinger	Neuerstellung
2			
3			
4			