PUBLIC
ÖFFENTLICH

ANLAGE 17-H
SORGFALTSPFLICHT FÜR INFORMATIONSSICHERHEIT BEI PARTNERN, DIENSTLEISTERN UND LIEFERANTEN

November 2024

PUBLIC
ÖFFENTLICH

Richtlinien für den Anbieter

Dieses Dokument enthält spezifische Informationen, die MAN den Anbietern für die Beantwortung der Ausschreibung zur Verfügung stellt.

Anweisungen für den Anbieter

1. Der Anbieter verpflichtet sich, keine Änderungen oder Modifikationen an diesem Dokument vorzunehmen.
2. Die Antwort des Anbieters auf diese Ausschreibung sollte die Informationen in diesem Dokument widerspiegeln und diesen Angaben entsprechen.
3. Einwände oder Probleme in Verbindung mit den in den Dokumenten enthaltenen Definitionen machen die Anforderungen dieses Dokuments oder der Ausschreibung weder ungültig noch bewirken sie eine Modifizierung der Anforderungen. Von einer Aufnahme der vorgeschlagenen Änderungen des Anbieters kann der Anbieter nur ausgehen, sofern die MAN diese dem Anbieter gegenüber ausdrücklich schriftlich bestätigt hat.

Inhalt

EINLEITUNG

In der heutigen Geschäftswelt ist vorausschauendes Handeln Pflicht. Daher ist der Nachweis der Sorgfaltspflicht und der gebotenen Sorgfalt die einzige Möglichkeit, Fahrlässigkeit bei einem möglichen Schadensfall zu widerlegen.

In diesem Dokument werden die MAN Anforderungen zur Sicherstellung einer ausreichenden Verfügbarkeit und Leistung bei der Bereitstellung von Produkten und Diensten dargelegt, indem aktuelle Bedrohungen der Cybersicherheit berücksichtigt werden und angemessen auf diese reagiert wird.

Im weiteren Verlauf des Dokuments finden sich Informationen über die Meldekanäle für Cybervorfälle, die wichtigsten Verhaltens- und Sensibilisierungsgrundsätze sowie über den fairen Wettbewerb.

Die Sorgfaltspflichten im Bereich der Informationssicherheit und der Verhaltenskodex für die Informationssicherheit sind integraler Bestandteil des Dienstleistungsvertrags.

Es ist sicherzustellen, dass es sich bei allen Partnern oder Gliedern der Lieferkette um zuverlässige, vertrauenswürdige und seriöse Organisationen handelt, die ihre Praktiken und Sicherheitsanforderungen gegenüber ihren Geschäftspartnern offenlegen.

1. Sorgfaltspflichten für Partner, Dienstleister und Lieferanten

Da die Bereitstellung und Verfügbarkeit kritischer Dienste ständig einer Vielzahl von Bedrohungen ausgesetzt ist, wie z. B.:

- Zerstörung von Informationen durch Computerviren
- Böswillige Verschlüsselung wichtiger Daten durch Ransomware-Angriffe
- Diebstahl von Informationen durch Social-Engineering-Angriffe - Ausspähen von Passwörtern, Phishing
- Verlust oder Diebstahl von Datenträgern oder Computern
- Ausfall von Systemen aufgrund von Stromausfällen, Sabotage, Vandalismus, Naturkatastrophen,

müssen Partner, Dienstleister und Lieferanten von MAN Truck & Bus (MTB) proaktive Maßnahmen zu ihrem Schutz dringend umsetzen, um das vertraglich vereinbarte Verfügbarkeits- und Leistungsniveau für MTB zu gewährleisten.

Der Schutz ist nur dann wirksam, wenn er auf einer Vielzahl von miteinander verbundenen Maßnahmen und Schutzvorkehrungen beruht. Zu den erforderlichen Mindestsicherheitsmaßnahmen, die von Partnern, Dienstleistern und Lieferanten von MTB umzusetzen sind, gehören unter anderem insbesondere:

- Wirksame Absicherung der IT Systeme gegen Angriffe von Aussen durch regelmäßige Schwachstellenanalyse und zeitnahes security patch management
- Kontinuierliche Schärfung des Sicherheitsbewusstseins aller Mitarbeiter, insbesondere in Bezug auf Social-Engineering-Angriffe wie Phishing sowie die Kanäle zur Meldung von Ereignissen und Vorfällen / siehe Ethikkodex.
- Einhaltung von definierten Prozessen und Verfahren sowohl intern als auch extern von nationalen und internationalen Gesetzen, Standards und Vorschriften.
- Angemessene und regelmäßige risikoorientierte Berichterstattung über die Gestaltung und Wirksamkeit der Informationssicherheit und der betrieblichen Prozesse - sicherheitsbezogene Berichte, Compliance-Berichte, Bedrohungsanalyse der aktuellen Landschaft.
- Ernennung einer für die Informationssicherheit verantwortlichen Person, insbesondere einer Funktion, die für Informationssicherheitsvorfälle und deren Behandlung und Meldung an MTB und die kompetenten Behörden zuständig ist.

2. Ethikkodex für Informationssicherheit

Die unternehmerische Verantwortung beinhaltet die Verpflichtung, alle geltenden Vorschriften und Regeln einzuhalten. Daher erwartet MTB von seinen Lieferanten und Geschäftspartnern, dass sie insbesondere die in diesem Abschnitt aufgeführten Grundprinzipien beachten.

Dieser Ethikkodex für Informationssicherheit legt den Nutzen ethischer Werte für das Verhalten der Organisation dar, aber auch die Erwartungen, die MTB an seine Lieferanten und Partner stellt, wie sie sich in kritischen Situationen verhalten sollen, sowie die Grundprinzipien, die ihre Aktivitäten und Entscheidungen leiten sollen.

Die Ziele des Kodex lassen sich wie folgt zusammenfassen:

- Sorgfältige Maßnahmen zum Schutz und zur Sicherstellung der vertraglich vereinbarten Service-Levels und Leistungen ergreifen
- Verantwortung und Kompetenz im Falle von Cyberangriffen zeigen
- Ablehnung von Korruption, Bestechung und ungesetzlichem oder unethischem Verhalten
- Gewährleistung transparenter Geschäftsbeziehungen und eines fairen Wettbewerbs - anhand MAN Code of Conduct für Lieferanten und Business Partner
- Einhaltung der Informationssicherheitsrichtlinien von MTB, die in Anhang 17 und Anlage 17-A aufgeführt sind
- Enhaltung von gesetzlichen Anforderungen, Vorschriften und Normen

3. Pflichten für Partner und Lieferanten

Angemessenes Bewusstsein bei Mitarbeitern und Subunternehmern sicherstellen

Die meisten Angriffe zielen auf den Faktor "Mensch" als vermeintlich schwächstes Glied in der IT-Sicherheitskette.

Unter falscher Identität versuchen Cyberkriminelle, ihre Opfer dazu zu verleiten, sensible Informationen preiszugeben, Schutzmaßnahmen zu umgehen oder selbst Malware auf ihren Systemen zu installieren.

Dies geschieht zunehmend in Form von so genannten Phishing-E-Mails, einer Unterform des "Social Engineering". Sowohl die Phishing-E-Mail selbst als auch die Website, auf die ein Link im Text der Phishing-E-Mail verweist, sehen täuschend echt aus, indem Logos, Farben und Schriftarten der jeweiligen Organisation oder des Unternehmens verwendet werden, das vorgibt, die Phishing-E-Mail verschickt zu haben, um beim Empfänger Vertrauen zu erwecken. Oft wird dem Empfänger vorgegaukelt, dass dringender Handlungsbedarf besteht - zum Beispiel ein aktueller Sicherheitsvorfall oder eine Kreditkarte, die vorsorglich gesperrt worden ist. Die Phishing-E-Mails sind oft mit aktuellen Ereignissen verknüpft.

Phishing-E-Mails stellen nicht nur dann eine große Gefahr dar, wenn sensible Informationen weitergegeben werden, sondern auch, wenn bösartige Anhänge geöffnet werden. Ein erfolgreicher Phishing-Angriff ist oft der Auslöser für einen nachfolgenden Ransomware-Angriff. Dabei werden Daten verschlüsselt, um anschließend vom Empfänger der Phishing-E-Mail ein Lösegeld zu fordern. Es wird damit gedroht, Daten zu löschen oder zu veröffentlichen, wenn die

Lösegeldforderung nicht rechtzeitig erfüllt wird. Auch die Zerstörung von Systemen kann die Folge von Phishing-E-Mails oder eines Ransomware-Angriffs sein.

Im Hinblick auf die immer größer werdende Cybersicherheits- und Bedrohungslage bitten wir Sie, besonders wachsam zu sein und Ihre Mitarbeiter entsprechend zu sensibilisieren. Wir empfehlen Ihnen, bei E-Mails von Vorgesetzten, die Druck aufbauen oder einen scharfen Ton anschlagen, besondere Vorsicht walten zu lassen. Im Zweifelsfall sollten solche E-Mails an entsprechend geschultes Personal zur weiteren Prüfung weitergeleitet werden. Durch das schnelle Erkennen eines "Social Engineering"-Versuchs kann großer Schaden verhindert werden.

Meldung von Cyber-Vorfällen und angemessenes Verhalten im Falle von Cyber-Kriminalität:

Wenn Sie von einem Cyberangriff betroffen sind, melden Sie den Vorfall bitte sofort der MTB Cyber Defense Center mtb-cdc@man.eu.

Wir empfehlen folgendes Verhalten:

- Gehen Sie nicht auf Zahlungsaufforderungen ein.
- Wenden Sie sich an die zentrale Anlaufstelle für Internetkriminalität bei dem für Sie zuständigen Landeskriminalamt.
- Melden Sie den Angriff an das Bundesamt für Sicherheit in der Informationstechnik. Dort erhalten Sie wertvolle Informationen und Hinweise, wie Sie mit dem Vorfall umgehen können.
- Stellen Sie Strafanzeige bei der Polizei. Insbesondere dann, wenn Ihr Unternehmen durch den Einsatz von Verschlüsselungstrojanern erpresst wird.

Einhaltung und Umsetzung grundlegender Sicherheitsgrundsätze:

- Zuständigkeiten: Die Rollen und Verantwortlichkeiten der Personen, die an der beauftragten Dienstleistung beteiligt sind, müssen klar definiert sein und mit den Kompetenzen und Verpflichtungen der Mitarbeiter übereinstimmen.

- Trennung der Aufgaben: Die Privilegien zur Erfüllung kritischer Aufgaben müssen angemessen zwischen den einzelnen Personen aufgeteilt werden, um den Missbrauch von Systemen und die Untergrabung von Prozessen zu verhindern.
- Geringstmögliche Privilegien: Benutzer sollten nur mit den minimalen Zugriffsrechten (oder Berechtigungen) ausgestattet werden, die für die Erfüllung ihrer Aufgaben erforderlich sind.
- Kenntnisnahme erforderlich: Benutzer sollten nur Zugang zu Informationen und Ressourcen erhalten, die zur Erfüllung einer Aufgabe im Rahmen ihrer Funktion erforderlich sind.
- Nachvollziehbarkeit: Wichtige Ereignisse müssen regelmäßig aufgezeichnet und analysiert werden, um böswillige Aktivitäten zu erkennen und vollständig zu untersuchen.