Cyber-Sicherheitsstandards für Lieferanten

Abschnitt A –alle Lieferanten

ALLE Lieferanten müssen die nachfolgend beschriebenen Cyber-Sicherheitsstandards erfüllen.

1. Lieferanten müssen aufzeigen können, dass in ihrem Unternehmen ein Bewusstsein für Cyber-Sicherheit vorherrscht. Dies umfasst, ist jedoch nicht begrenzt auf:
   I. Belege für eine Registrierung gemäß einem anerkannten Cyber-Sicherheitsstandard (z.B. den in Cyber Essentials aufgeführten Standards);
   II. Cyber-Sicherheitsschulungen für Mitarbeiter, einschließlich ein laufendes Programm für Verbesserung;
   III. robuste Backups; Richtlinien zur Reaktion auf Vorfälle; und Notfall-Wiederherstellungspläne usw.

2. Oft sind beeinträchtigte Lieferanten der Ursprung für Phishing- und Malware-Angriffe. Deswegen müssen Lieferanten robuste Cyber-Sicherheitssysteme nachweisen. Dazu gehören:
   I. E-Mail-Systeme mit Multifaktor-Authentifizierung oder anderen Schutzmaßnahmen, z.B. DMARC;
   II. Verfahren, die sicherstellen, dass frühestmöglich aktive Benachrichtigungen versandt werden, wenn der Lieferant bemerkt, dass seine Systeme beeinträchtigt sind oder für Phishing-Angriffe gedient haben.

3. Falls INEOS Inovyn Phishing- oder Malware-Angriffe erkennt und der Lieferant die Ursache dafür war, muss es eine klare Eskalationsstrecke zum Lieferanten geben.

4. Versuche für Finanzbetrug finden oft statt, indem in abgefangenen E-Mails dazu aufgerufen wird, die hinterlegte Bankverbindung zu ändern. Laut der INEOS Inovyn Betrugsbekämpfungsrichtlinie müssen Lieferanten klar ein Verfahren beschreiben, wie sie INEOS Inovyn über rechtmäßige Änderungen informieren wollen. Darin müssen benannte Kontaktpersonen für INEOS Inovyn aufgeführt sein, bei denen die Gültigkeit unabhängig nachgefragt werden kann.

5. Lieferanten, die Daten mit Bezug zu INEOS Inovyn speichern, müssen sicherstellen, dass diese Datenspeicher den rechtlichen Datenschutzbestimmungen des jeweiligen Landes entsprechen, einschließlich:
   I. Einhaltung der Datenschutz-Grundverordnung (DSGVO) oder entsprechenden Bestimmungen;
   II. INEOS Inovyn-Daten, die auf tragbaren Geräten (z.B. Laptops) gespeichert sind, sollten eine vollständige Festplattenverschlüsselung aufweisen.

6. Jegliche Methode zum Transfer von Software oder Daten im Rahmen der Arbeitsleistung des Lieferanten muss geeignete sichere Mechanismen nutzen, zum Beispiel:
    I. eine gesicherte, von INEOS Inovyn gehostete SharePoint-Site;
    II. eine sichere Website zum Dateitransfer, die der Lieferant bereitstellt und die INEOS Inovyn zertifiziert hat.

7. Massentransfergeräte wie USB-Sticks/-Laufwerke sind nur dann zu verwenden, wenn kein anderes praktisches Medium existiert. Auf jeden Fall müssen die Massenspeichergeräte zum Zeitpunkt der Nutzung den INEOS Inovyn-Richtlinien und -Prüfungen entsprechen.

Abschnitt B –Lieferanten von Systemen und Ressourcen, die auf INEOS Inovyn-Systemen laufen sollen

Neben den Bestimmungen in Abschnitt A müssen ALLE Lieferanten von Systemen, Ausstattung und Ressourcen, die auf INEOS Inovyn-Systemen laufen sollen, sicherstellen, die folgenden zusätzlichen Anforderungen zu erfüllen.

8. Gelieferte Systeme und umetikettierte Ausstattung müssen vom Anbieter unterstützte Plattformen mit einer Mindestlebensdauer von fünf Jahren nutzen. Dies umfasst Aspekte wie:
    I. Betriebssysteme (OS);
    II. Firmware;
    III. Abhängigkeit von Dritt-Anwendungen, -Komponenten und -Webbrowsern.

9. Die gelieferten Systeme müssen zu **Updates gegen zukünftige Schwachstellen** in der Lage sein, zum Beispiel:
    I. Durchführung regelmäßiger Betriebssystem-Patches;
    II. Durchführung von Versionsupdates des Betriebssystems;
    III. der Lieferant muss sein Verfahren zur Prüfung und Genehmigung von Patches angeben, z.B. Dauer der Genehmigungsphase des Lieferanten, besondere Vorgehensweisen bei besonders kritischen Patches.

10. Gelieferte Systeme müssen in der Lage sein zu Cyber-Schutzmaßnahmen, einschließlich Maßnahmen wie:
    I. grundlegender Virusschutz;
    II. Schutz durch Anwendungs-Positivliste (Whitelist);
    III. fortschrittlicher Malware-Schutz;
    IV. Netzwerkschutz durch Firewall-Vorkehrungen;
    V. der Lieferant darf für Behörden nicht als grundsätzlich ungeschützt im Cyber-Bereich gelten und daher Beschränkungen unterliegen.

11. Falls einem Lieferanten der Fernzugriff auf INEOS Inovyn-Systeme gewährt wird, so dürfen diese Zugriffsrechte ausschließlich für den vorgesehenen Zweck und nur an den in der Support-und Dienstleistungsvereinbarung (SLA) genannten Systemen genutzt werden usw.:
    I. INEOS Inovyn muss dem gesamten Arbeitsumfang vor der Durchführung zustimmen und die Arbeiten sind regelmäßig zu überprüfen (mindestens einmal pro Jahr).

12. Falls zu irgendeinem Teil der INEOS Inovyn-Systeme Fernzugriffgewährt wird, können zusätzliche Bedingungen gelten, wie z.B.:
    I. ausschließlich benannte Personen –einschließlich möglicher Hintergrundchecks, Schulungsbelege, vereinbarte benannte Stellvertreter usw.;
    II. Zweifaktorauthentifizierung, abgehalten von INEOS Inovyn.

13. Wenn Lieferanten INEOS Inovyn vielmehr Ressourcen anstatt Systeme bereitstellen, dann wird erwartet, dass alle Ressourcen den INEOS Inovyn-Richtlinien für Cyber-Sicherheit entsprechen, sowohl an unseren Standorten als auch andernorts sofern eine Verbindung zu INEOS Inovyn-bezogener Arbeit besteht. Derartige Richtlinien sind normalerweise Bestandteil des INEOS Inovyn-Einführungsverfahrens.

ENDE DES DOKUMENTS

V1. August 2020