Normen voor de cyberveiligheid van leveranciers

Sectie A -alle leveranciers

Van ALLE leveranciers wordt verwacht dat ze voldoen aan de onderstaande normen ten aanzien van cyberveiligheid.

1. Leveranciers moeten binnen hun organisatie kunnen aantonen dat er een cultuur heerst waarin men zich bewust is van cyberveiligheid. Dit omvat, maar is niet beperkt tot:
   I. bewijs van registratie ten opzichte van een erkende norm voor cyberveiligheid (bijv. de normen die beschreven staan in Cyber Essentials);
   II. een cyberveiligheidstraining voor werknemers, inclusief een doorlopend verbeterprogramma;
   III. robuuste back-ups; incidentresponsbeleid; en noodherstelplannen enz.

2. Phishing en malware zijn vaak afkomstig van leveranciers die daar zelf slachtoffer van zijn. Daarom moeten leveranciers aantonen dat ze robuuste systemen hebben die bestand zijn tegen cyber-aanvallen. Dit omvat:
   I. e-mailsystemen die meervoudige verificatie of andere beschermende maatregelen gebruiken, bijv. DMARC;
   II. processen om ervoor te zorgen dat er bij de eerste gelegenheid een actieve melding wordt gemaakt als de leverancier detecteert dat zijn systemen geïnfecteerd zijn of betrokken zijn bij phishing.

3. In het geval van phishing of malware, afkomstig van de leverancier en gedetecteerd door INEOS Inovyn, moet er een duidelijke escalatieroute zijn naar de leverancier.

4. Financiële fraude vindt vaak plaats via onderschepte e-mails waarin de ontvanger wordt verzocht de bankgegevens van de verzender te wijzigen. Als onderdeel van het anti-fraudebeleid van INEOS Inovyn moeten leveranciers over een duidelijk omschreven proces beschikken waarmee ze INEOS Inovyn op de hoogte brengen van legitieme wijzigingen, met genoemde contactpersonen die INEOS Inovyn kan gebruiken voor onafhankelijke controles om de geldigheid te bevestigen.

5. Leveranciers die gegevens met betrekking tot INEOS Inovyn opslaan, moeten ervoor zorgen dat dergelijke opslag conform de wettelijke vereisten voor gegevensbescherming is, afhankelijk van elk land, waaronder:
   I. naleving van de algemene verordening gegevensbescherming (AVG) of gelijkwaardig;
   II. INEOS Inovyn-gegevens die zijn opgeslagen op draagbare apparaten, zoals laptops, moeten volledige schijfversleuteling gebruiken.

6. Elke methode die wordt gebruikt voor het overdragen van software of gegevens als onderdeel van het werk van de leverancier, moet gebruikmaken van voldoende beveiligde mechanismen, zoals:
    I. een door INEOS Inovyn gehoste beveiligde SharePoint-site;
    II. een beveiligde site voor bestandsoverdracht die wordt aangeboden door de leverancier en die gecertificeerd is door INEOS Inovyn.

7. Apparaten voor bulkverzendingen, zoals USB-sticks/-schijven, mogen alleen worden gebruikt als er geen ander praktisch mechanisme bestaat en moeten in al deze gevallen voldoen aan het INEOS Inovyn-beleid en de controles op het moment van gebruik.

Sectie B -leveranciers van systemen en middelen om aan INEOS Inovyn-systemen te werken

Naast sectie A moeten ALLE leveranciers van systemen, apparatuur en middelen die aan INEOS Inovyn-systemen werken, ervoor zorgen dat aan de volgende aanvullende vereisten wordt voldaan.

8. Meegeleverde systemen en apparatuur die die van een nieuw kenmerk is voorzien moeten door de leverancier ondersteunde platforms gebruiken met een verwachte minimale levensduur van 5 jaar. Dit omvat aspecten als:
    I. besturingssystemen (OS);
    II. firmware;
    III. afhankelijkheid van applicaties, componenten en webbrowsers van derden.

9. Geleverde systemen moeten **up-to-date kunnen worden gehouden tegen toekomstige kwetsbaarheden**, bijvoorbeeld:
    I. toepassing van regelmatige patches voor het besturingssysteem;
    II. toepassing van updates van de versie van het besturingssysteem;
    III. de leverancier moet zijn proces voor het testen en goedkeuren van patches aangeven, bijv. hoelang de fase duurt waarin de leverancier goedkeuring verleent, speciale regelingen voor in het bijzonder cruciale patches.

10. Geleverde systemen moeten de capaciteit hebben voor cyberbeveiliging, inclusief maatregelen als:
    I. basis anti-virusbescherming;
    II. bescherming door whitelisting van applicaties;
    III. geavanceerde malware-bescherming;
    IV. netwerkbeveiliging door firewall-apparaten;
    V. de leverancier mag niet door de overheid worden geïdentificeerd als inherent cyber-onveilig, en daardoor aan beperkingen onderworpen zijn.

11. Als een leverancier op afstand toegang krijgt tot INEOS Inovyn-systemen, mag dergelijke toegang alleen worden gebruikt voor het beoogde doel, en alleen voor de systemen die worden geïdentificeerd in het toepassingsgebied van de ondersteuning, service-level agreement (SLA) enz.:
    I. al dergelijke werkzaamheden moeten met INEOS Inovyn worden overeengekomen voordat ze worden uitgevoerd en worden regelmatig herzien (minimaal elk jaar).

12. In het geval van toegang op afstand tot enig onderdeel van INEOS Inovyn-systemen, kunnen aanvullende vereisten gelden, zoals:
    I. alleen genoemde personen - inclusief mogelijke antecedentenonderzoeken, bewijs van opleiding, overeengekomen genoemde plaatsvervangers enz.;
    II. twee-factor-authenticatie, gedaan door INEOS Inovyn.

13. Waar leveranciers middelen aan INEOS Inovyn leveren in plaats van systemen, wordt verwacht dat alle middelen zullen werken binnen de INEOS Inovyn-richtlijnen voor cyberveiligheid, zowel op onze locaties als elders wanneer ze betrekking hebben op INEOS Inovyn-gerelateerd werk. Dergelijke richtlijnen worden normaliter gecommuniceerd als onderdeel van het introductieproces van INEOS Inovyn.

EINDE VAN HET DOCUMENT

V1. Augustus 2020