Standarder for cybersikkerhet for leverandører

Del A –alle leverandører

ALLE leverandører forventes å overholde standardene for cybersikkerhet som er beskrevet nedenfor.

1. Leverandører må kunne vise at de har en kultur for cybersikkerhet innenfor sine organisasjoner. Dette inkluderer, men er ikke begrenset til:
   I. bevis på registrering mot en anerkjent standard for cybersikkerhet (f.eks. de som er beskrevet i Cyber Essentials (grunnleggende om cybersikkerhet)),
   II. opplæring i cybersikkerhet av ansatte, inkludert et pågående forbedringsprogram,
   III. robuste sikkerhetskopier, policyer for svar på hendelser, planer for katastrofegjenoppretting osv.

2. Phishing og skadelig programvare kan ofte komme fra kompromitterte leverandører. Derfor må leverandører vise robuste systemer for cybersikkerhet. Dette inkluderer:
   I. e-postsystemer som bruker godkjenning med flere faktorer eller andre beskyttende tiltak, f.eks. DMARC,
   II. prosesser på plass for å sikre aktiv varsling ved tidligste mulighet hvis leverandøren oppdager at systemet er kompromittert eller involvert i phishing.

3. I tilfelle phishing eller kompromittering knyttet til skadelig programvare, som er kommet fra leverandøren og blir oppdaget av INEOS Inovyn, må det finnes en tydelig definert måte å eskalere dette til leverandøren på.

4. Forsøk på økonomisk svindel skjer ofte med e-post-meldinger som fanges opp, som ber mottakeren om å endre bankdetaljer. Som en del av INEOS Inovyns policy mot svindel, må leverandører ha en tydelig oppgitt prosess for hvordan de varsler INEOS Inovyn om legitime endringer, med navngitte kontakter som INEOS Inovyn kan bruke til uavhengige kontroller for å bekrefte validitet.

5. Leverandører som lagrer data knyttet til INEOS Inovyn, må sikre at slik lagring er i overensstemmelse med lovlige databeskyttelseskrav som avhenger av hvert land, inkludert:
   I. overholdelse av EUs personvernforordning (GDPR) eller tilsvarende,
   II. INEOS Inovyn-data som er lagret på bærbare enheter, f.eks. bærbare datamaskiner, bør bruke fullstendig diskkryptering.

6. Alle metoder som brukes for overføring av programvare eller data som en del av leverandørens arbeid, må bruke tilstrekkelig sikrede mekanismer, for eksempel:
   I. et INEOS Inovyn-driftet sikkert SharePoint-område,
   II. et sikkert filoverføringsområde fra leverandøren som er sertifisert av INEOS Inovyn

7. Masseoverføringsenheter, for eksempel USB-pinner/-stasjoner, skal kun brukes når det ikke finnes en annen praktisk mekanisme, og må i alle slike tilfeller være i overensstemmelse med INEOS Inovyn-policyer og -kontroller på brukstidspunktet.

Del B –leverandører av systemer og ressurser som skal arbeide på INEOS Inovyn-systemer

I tillegg til Del A, må ALLE leverandører av systemer, utstyr og ressurser som skal arbeide på INEOS Inovyn-systemer, kontrollere at følgende tilleggskrav oppfylles.

8. Leverte systemer og utstyr som eventuelt er merket på nytt, må bruke leverandørstøttede plattformer med en forventet levetid på minst 5 år. Dette inkluderer aspekter som for eksempel:
    I. Operativsystemer (OS);
    II. fastvare,
    III. tillit til eventuelle tredjeparts-programmer, -komponenter og nettlesere.

9. Leverte systemer må **kunne oppdateres mot fremtidige sårbarheter**, for eksempel:
    I. bruk av vanlige operativsystemoppdateringer,
    II. bruk av versjonsoppdateringer for operativsystemer,
    III. leverandøren må oppgi prosessen de bruker til testing og godkjenning av oppdatering, f.eks. varigheten til fasen for godkjenning av leverandører og spesielle avtaler for spesielt kritiske oppdateringer.

10. Leverte systemer må ha kapasitet til cyberbeskyttelse, inkludert tiltak som for eksempel:
    I. grunnleggende antivirusbeskyttelse,
    II. beskyttelse med hvitelisting av program,
    III. avansert beskyttelse mot skadelig programvare,
    IV. nettverksbeskyttelse av brannmurenheter,
    V. leverandøren må ikke bli identifisert av myndighetene som cyberusikker og derfor bli underlagt restriksjoner.

11. Hvis en leverandør har fått ekstern tilgang til INEOS Inovyn-systemer, må slik tilgang kun brukes til sitt intenderte formål, og kun til systemene som identifiseres i støtteomfanget, tjenestenivåavtalen (SLA) osv.:
    I. alt slikt arbeid må avtales med INEOS Inovyn før det finner sted, og må være underlagt vanlig gjennomgang (minst årlig).

12. I tilfeller der det gis ekstern tilgang til en del av INEOS Inovyn-systemer, kan tilleggskrav kreves, for eksempel:
    I. kun navngitte personer –inkludert eventuelle bakgrunnssjekker, bevis på opplæring, avtalte navngitte representanter osv.,
    II. tofaktorgodkjenning av INEOS Inovyn.

13. Der leverandører tilbyr ressurser i stedet for systemer til INEOS Inovyn, forventes det at alle ressurser fungerer innenfor INEOS Inovyns retningslinjer for cybersikkerhet, både på våre områder eller andre steder der de tar del i INEOS Inovyn-relatert arbeid. Slike retningslinjer ville vanligvis bli kommunisert som en del av INEOS Inovyns induksjonsprosess.

SLUTT PÅ DOKUMENTET

V1. August 2020