Standard för Cybersäkerhet –Leverantörer

Avsnitt A –alla leverantörer

ALLA leverantörer förväntas att uppfylla de standarder för cybersäkerhet som beskrivs nedan.

1. Leverantören måste kunna visa att det finns stark medvetenhet om cybersäkerhet inom organisationen. Detta omfattar, men är inte begränsat till:
   I. bevis om registrering av en erkänd standard för cybersäkerhet (t.ex. de som beskrivs i Cyber Essentials),
   II. utbildning av medarbetare i cybersäkerhet, inklusive ett pågående förbättringsprogram,
   III. stabil säkerhetskopiering, policyer om incidenthantering och planer för återhämtning efter haverier etc.

2. Nätfiske och skadlig programvara härstammar ofta från komprometterade källor hos leverantörer. Leverantörer måste därför demonstrera att de har stabila system för cybersäkerhet. Detta omfattar:
   I. e-postsystem som använder multifaktorautentisering eller andra skyddsåtgärder, t.ex. DMARC,
   II. processer som säkerställer att aktiv anmälan kan ske så snart som möjligt efter att leverantören upptäcker att dess system har komprometterats eller utsatts för nätfiske.

3. Om INEOS Inovyn upptäcker att systemet har komprometterats till följd av nätfiske eller skadlig programvara som härstammar från leverantören, måste det finnas en tydlig eskaleringsväg till leverantören.

4. Ekonomiskt bedrägeri sker ofta genom att genskjuta e-postmeddelanden och begära att mottagaren ska ändra sina bankuppgifter. Som en del av INEOS Inovyn:s policy om förebyggande av bedrägerier ska leverantören ha tydliga processer för att underrätta INEOS Inovyn om eventuella rimliga ändringar. De ska tillhandahålla kontaktuppgifter så att INEOS Inovyn kan utföra oberoende kontroller för att bekräfta giltigheten.

5. Leverantörer som lagrar data relaterad till INEOS Inovyn måste säkerställa att informationen lagras på ett sätt som överensstämmer med respektive lands lagstiftning om dataskydd, inklusive:
   I. efterlevnad av den Allmänna dataskyddsförordningen (GDPR) eller motsvarande,
   II. fullständig diskkryptering av all INEOS Inovyn-data som lagras på bärbara enheter, t.ex. bärbara datorer.

6. All överföring av programvara eller data som utgör en del av leverantörens verksamhet måste använda lämpliga säkerhetsmetoder, såsom:
   I. en säker SharePoint-plats som sköts av INEOS Inovyn,

II. en säker filöverföringsplats som tillhandahålls av leverantören och har godkänts av INEOS Inovyn.

7. Massöverföring via USB-minnen/USB-drivenheter ska endast användas i brist på någon annan praktisk metod och måste då alltid uppfylla INEOS Inovyn:s policyer och andra kontroller vid användningen.

Avsnitt B –leverantörer av system och resurseravsedda för INEOS Inovyn:s system

Utöver vad som anges i avsnitt A måste ALLA leverantörer av system, utrustning och resurser som utför arbete på INEOS Inovyn:s system säkerställa att de ytterligare kraven nedan uppfylls.

8. Alla system som tillhandahålls och eventuell utrustning under nytt namn måste använda plattformar som stöds av säljaren med en förväntad livslängd på minst 5år. Detta inbegriper följande faktorer:
   I. operativsystem (OS),
   II. fast programvara,
   III. förlitande på program, komponenter och webbläsare från tredje part.

9. Alla system som tillhandahålls måste kunna uppdateras för att skydda mot framtida sårbarheter, t.ex.:
   I. regelbundna korrigeringar för operativsystemet,
   II. uppdateringar av operativsystemets version,
   III. leverantören måste ange hur de kommer att testa och godkänna korrigeringar, t.ex. godkännandefasens varaktighet och särskilda bestämmelser för korrigeringar som är särskilt kritiska.

10. Alla system som tillhandahålls måste ha kapacitet för cyberskydd, inklusive åtgärder såsom:
    I. grundläggande antivirusskydd,
    II. skydd genom att skapa vitlistor för applikationer,
    III. avancerat skydd mot skadlig programvara,
    IV. nätverksskydd via brandväggsenheter,
    V. en leverantör får inte vara föremål för restriktioner från regeringen på grund av bristande kompetens inom cybersäkerheten.

11. Fjärråtkomst till INEOS Inovyn:s system som beviljas en leverantör får endast användas för avsedda ändamål och ska begränsas till de system som har identifieras inom ramen för supportarbetet, servicenivåavtalet (SLA) etc.:
    I. arbetet måste avtalas med INEOS Inovyn innan det äger rum och vara föremål för regelbunden granskning (minst årligen).

12. När fjärråtkomst till någon del av INEOS Inovyn:s system beviljas kan det vara nödvändigt att lägga till ytterligare krav såsom:

I. endast namngivna personer –inklusive eventuella bakgrundskontroller, utbildningsbevis, godkända namngivna representanter etc.,
II. tvåfaktorsautentisering ska utföras av INEOS Inovyn.

13. Då leverantörer tillhandahåller resurser snarare än system till INEOS Inovyn, förväntas det att alla dessa resurser ska fungera inom INEOS Inovyn:s riktlinjer för cybersäkerhet, både på våra anläggningar och på andra platser där arbete relaterat till INEOS Inovyn utförs. Riktlinjerna utgör normalt en del av INEOS Inovyn:s introduktionsprocess.

SLUT PÅ DOKUMENTET

V1. Augusti 2020