Delphi

Checklista – Utgångspunkter för att säkerställa säkerhet i leveranskedjan enligt NIS2

1. Leverantörsbedömning

- Säkerhetsbedömning av leverantörer: Utvärdera leverantörernas säkerhetsrutiner, kapacitet och historik innan avtal ingås.
- Kontinuerlig övervakning: Implementera en process för regelbunden övervakning och omvärdering av leverantörernas säkerhetsstatus.
- Riskklassificering: Klassificera leverantörer baserat på den risk de utgör för verksamhetens säkerhet och affärskritiska system. Ställ avtalskrav på leverantören baserat på klassificering.

2. Avtal om säkerhetsåtgärder

- Införande av säkerhetskrav i avtal: Säkerställ att avtal med leverantörer inkluderar specifika säkerhetsåtgärder och krav på informationssäkerhet. Överväg att avtala om servicenivåer och spegla relevanta delar av de obligatoriska säkerhetsåtgärder som verksamheten måste vidta enligt NIS2 och cybersäkerhetslagen.
- Krav på incidentrapportering: Avtala om tydliga processer för hur säkerhetsincidenter ska rapporteras och hanteras av leverantören.
- Åtaganden för kontinuitetsplanering och återställanderutiner: Säkerställ att leverantörer har beredskapsplaner och incidenthanteringsplaner som kan samordnas med verksamhetens egna.
- Processer och standarder: Överväg att kravställa informationssäkerhetssystem och standardisering, till exempel ISO 27000-serien.

3. Kontroll över åtkomskt och information

- Åtkomstkontroll till kritiska system: Begränsa leverantörers tillgång till känsliga system och data. Tillämpa *”the principle of least privilege”*.
- Säker dataöverföring: Implementera krypterade kanaler för all dataöverföring mellan verksamheten och leverantörer.
- Datahanteringspolicy: Säkerställ att leverantörer följer verksamhetens externa policyer för säker datahantering och åtkomstkontroll, särskilt vad gäller känsliga data.

4. Övervakning av leveranskedjan

- Ständigt uppdaterad sårbarhetshantering: Kräv att leverantörer har en robust patchhanterings- och sårbarhetshanteringsprocess.
- Hotövervakning: Implementera övervakningslösningar som kan upptäcka och rapportera om hot eller angrepp inom leveranskedjan.
- Insyn i leverantörens säkerhetsrutiner: Begär rapporter eller revisioner som visar hur leverantören säkerställer sin informationssäkerhet.

5. Kontinuerlig utbildning och säkerhetsmedvetenhet

- Utbildning av leverantörer: Säkerställ att anställda hos leverantörer genomgår regelbunden säkerhetsutbildning, särskilt inom områden som rör cyberhot och nätverkssäkerhet.
- Simulerade angrepp: Samordna och genomför säkerhetsövningar med leverantörer, som till exempel simuleringar av cyberangrepp.

6. Ställ krav på säkerhet i hela leveranskedjan

- Granskning av underleverantörer: Kräv att leverantörer utför liknande säkerhetsbedömningar på sina underleverantörer och rapporterar resultaten.
- Kedjebaserade säkerhetsåtgärder: Säkerställ att kraven på säkerhetsåtgärder följer genom hela leveranskedjan, inklusive underleverantörer och tjänsteleverantörer.

7. Säkerhet vid förändringar i leveranskedjan

- Hantering av förändringar: Inrätta en process för att bedöma och hantera säkerhetsrisker när nya leverantörer tas in eller förändringar sker i den befintliga leveranskedjan.
- Granskning av tekniska uppgraderingar: Se till att säkerhetskontroller görs vid systemuppgraderingar eller förändringar i leverantörers tjänster eller produkter.

8. Kontinuitetsplanering och resiliens

- Beredskap vid leverantörsstörningar: Säkerställ att leverantörer har robusta kontinuitets- och återhämtningsplaner i händelse av störningar eller attacker.
- Diversifiering av leverantörer: Minska beroendet av enskilda leverantörer genom att diversifiera leveranskedjan och därmed stärka verksamhetens resiliens mot leveransstörningar.

9. Incidenthantering och samordning

- Gemensam incidenthantering: Samordna incidenthanteringsplaner med leverantörer så att incidenter snabbt kan identifieras och hanteras över hela leveranskedjan.
- Informationsdelning vid incidenter: Etablera kanaler för snabb och effektiv informationsdelning om potentiella eller pågående cyberattacker mellan verksamheten och leverantörer.

10. Revision och uppföljning

- Årlig revision av leverantörer: Genomför regelbundna revisioner av leverantörernas säkerhetsåtgärder, inklusive granskning av efterlevnaden av avtalade säkerhetskrav.
- Certifiering av leverantörer: Överväg att kräva att leverantören certifierar sig enligt till exempel ISO 27001 och/eller genomför SOC 2 eller andra revisioner, samt delar med sig av relevanta resultat.
- Rapportering av säkerhetsåtgärder: Begär regelbundna rapporter från leverantörer om hur de upprätthåller och utvecklar sin säkerhetspraxis.

Observera att denna sammanställning inte är uttömmande. Checklistan syftar till att ge en översikt över centrala aspekter och ska inte betraktas som fullständig rådgivning.