6b. Cybersecurity due diligence mod nye leverandører

www.cyber-smv.dk

Formål, deltagere og anvendelse

- **Formål**
  - Når man udfører due diligence i relation til cybersikkerhed, er målet at vurdere, hvor godt den pågældende leverandør håndterer cyberrisici, og om der er skjulte trusler eller forpligtelser. Vedlagte procedure hjælper med at identificere potentielle risici mod cybersikkerheden og forpligtelser samt med at forstå, hvordan en leverandør – bevidst eller ubevidst – kan udsætte din organisation for cyberrisici.
- **Deltagere**
  - Sourcing/leverandørteam.
- **Anvendelse**
  - Ved indgåelse af leverandørengagementer.

Tema 1/10

Generisk due diligence-procedure for nye leverandørforhold

En generel procedure bør dække som minimum de følgende temaer:

Tema 1: Sikkerhedsstyring og -politikker

- Har leverandøren dokumenterede informationssikkerhedspolitikker?
- Er de tilpasset anerkendte frameworks (f.eks. ISO 27001, NIST, NIS 2)?
- Er der en ansvarlig på ledelsesniveau for cybersikkerhed?

Tema 2/10

Tema 2: Dataadgang og -håndtering

- Netværkssikkerhed – Firewalls, systemer til indtrængningsdetektion/-forebyggelse (Intrusion Detection/Preventions systems), segmentering, VPN'er.
- Er der datakryptering under overførsel og i hvile?
- Har de endepunktsbeskyttelse (f.eks. antivirus, administration af mobile enheder)?
- Har de sikkerhedspolitikker for cloud-løsninger?
- Anvenders principperne om mindst mulige rettigheder og need-to-know ved adgang?

Tema 3/10

Tema 3: Identitets- og adgangsstyring

- Håndhæver de stærke autentificeringsmetoder, såsom multifaktorautentificering (MFA)? Har de adgangskodepolitikker?
- Hvordan håndteres oprettelse og nedlæggelse af brugere (især for medarbejdere, der fratræder)?
- Hvordan administreres privilegerede konti?

Tema 4/10

Tema 4: Kontraktuelle beskyttelser

Indeholder aftalen:

- Klare databeskyttelsesklausuler?
- Sikkerhedskrav?
- Ret til audit?
- Tidsfrister for brudmeddelelser (f.eks. inden for 24 eller 72 timer)?

- Databehandlingsklausuler: Hvem ejer dataene? Hvad sker der, hvis data kompromitteres? Er der klare regler for datalagring, overførsel og sletning?
- Er der sanktioner eller afhjælpninger i tilfælde af et brud?
- Opsigelsesrettigheder: Hvilke muligheder giver kontrakten for at opsige samarbejdet i tilfælde af brud på cybersikkerheden eller overtrædelser af sikkerhedspolitikker?
- Ansvarsbegrænsninger: Begræns din eksponering, hvis leverandøren bliver kompromitteret, og det påvirker din organisation. Er der fastsat maksimale erstatningsbeløb?

Tema 5/10

Tema 5: Hændelseshåndtering og historik for databrud

- Har de en testet beredskabsplan for sikkerhedshændelser (IRP)?
- Hvad er deres historik med databrud?
- Vil de informere dig med det samme, hvis dine data bliver berørt?
- Opsætning af alarmer og notifikationer ved mistænkelig adfærd fra kundekonti.
- Brug af automatiserede systemer til at opdage uregelmæssigheder i realtid.
- Er der periodisk evaluering af adgangsrettigheder og sikkerhedspolitikker?
- Mulighed for at gennemføre audits ved behov eller ved hændelser.

Tema 6/10

Tema 6: Sikkerhedskontroller og -praksis

- Udfører de regelmæssige sårbarhedsscanninger og patching?
- Har de gennemført nylige sikkerhedsaudits eller opnået certificeringer? (f.eks. ISO 27001 osv.)
- Er systemer og infrastruktur adskilt for hver kunde?
- Har de en backup- og gendannelsesplan?

Tema 7/10

Tema 7: Test og vurdering

- Har de gennemført penetrationstest eller tredjeparts risikovurderinger – og hvornår?
- Vil de acceptere en sikkerhedsspørgeskemaundersøgelse eller teknisk audit?
- Findes der eksterne offentlige eller private sikkerhedsvurderinger?

Tema 8/10

Tema 8: Risiko fra underleverandører (sub-contractors/fjerdeparter)

- Udliciterer de nogen tjenester? Hvis ja, til hvem og hvilke?
- Udfører de cybersikkerhedsmæssig due diligence på deres egne leverandører?
- Bliver du informeret, hvis de skifter kritiske tjenesteudbydere?

Tema 9/10

Tema 9: Sikkerhedsbevidsthed og -uddannelse

- Modtager deres medarbejdere regelmæssig træning i sikkerhedsbevidsthed?
- Gennemføres der phishing-simulationer eller øvelser i social engineering?
- Findes der en politik for indberetning af sikkerhedshændelser?

Tema 10/10

Tema 10: Forsikring mod cyberangreb

- Har de en forsikring mod cyberangreb?
- Er der et krav om dokumentation for aktiv forsikringsdækning?
- Dækker forsikringen krav fra tredjeparter eller kun egne tab (førsteparts)?

Advarselsflag – når leverandøren udgør en potentiel risiko

Det bør betragtes som en **advarsel**, hvis:

- Leverandøren nægter at acceptere sikkerhedsklausuler i kontrakten:
  - F.eks. modstand mod databehandleraftaler, ansvarsbegrænsninger eller brudunderretning.
- Leverandøren anmoder om undtagelser fra grundlæggende sikkerhedspraksis:
  - Eksempel: Ønsker at undgå brug af multifaktorautentificering (MFA).
- Leverandøren insisterer på dyb systemadgang uden tilsyn:
  - F.eks. adgang til backend-systemer, databaser osv. uden logning, kontrol eller begrænsninger.