6a. Cybersecurity due diligence mod nye kunder

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 kunde håndterer cyberrisici, og om der er skjulte trusler eller forpligtelser.
  - Vedlagte procedure hjælper med at identificere potentielle cybersikkerhedsrisici og forpligtelser samt med at forstå, hvordan en kunde – bevidst eller ubevidst – kan udsætte din organisation for cyberrisici.
- **Deltagere**
  - Salg og kundeauditteam.
- **Anvendelse**
  - Ved nye kundeengagementer.

Tema 1/8

Generisk due diligence-procedure for nye kundeforhold

En generel procedure bør som minimum dække de følgende temaer:

Tema 1: Risikoprofilering af kunden

- Virksomhedstype og risikoniveau: Er kunden aktiv i en højrisiko-branche (f.eks. finans, sundhedsvæsen, forsvar eller andre kritiske sektorer)?
- Datasensitivitet: Hvilke typer data vil blive udvekslet eller opbevaret på vegne af kunden?
- Interaktionsomfang: Vil kunden have dyb systemintegration (f.eks. via en form for integration eller direkte adgang), eller blot adgang på brugerniveau?
- Jurisdiktion og lovgivning: Er der regulatoriske eller compliancemæssige hensyn (f.eks. GDPR eller anden lokal databeskyttelseslovgivning)?

Tema 2/8

Tema 2: Adgangs- og integrationskrav

- Hvilke systemer vil kunden få adgang til? (Interne applikationer, databaser, osv.?)
- Hvordan vil adgangen til systemerne blive administreret?
  - Brugerstyring og adgangsrettigheder.
  - Integration med eksisterende identitets- og adgangsstyringssystemer.
  - Rollebaseret adgangskontrol: Tildeling af adgang baseret på brugerens rolle og ansvar.
- Segmentering og isolation: Foranstaltninger til at forhindre risici på tværs af kunder.
- Godkendelse:
  - Skal kunden anvende multifaktorautentificering (MFA)?
  - Er VPN-forbindelse påkrævet?

Tema 3/8

Tema 3: Kundens modenhed for cybersikkerhed

For kunder, der kræver integration ud over et simpelt login, bør følgende kontrolleres:

- Grundlæggende cybersikkerhedspolitikker:
  - Findes der dokumenterede politikker for informationssikkerhed, adgangsstyring, hændelseshåndtering osv.?
- Tredjepartsrisici:
  - Benytter kunden leverandører eller underleverandører, som din organisation også skal kunne stole på?
  - Er der en proces for vurdering og overvågning af disse tredjeparter?
- Sikkerhedsstatus og historik:
  - Har kunden tidligere været udsat for sikkerhedsbrud eller offentlige hændelser?
  - Hvordan har de håndteret tidligere hændelser, og hvilke forbedringer er blevet implementeret?

Tema 4/8

Tema 4: Kontraktuelle beskyttelser

- Databehandlingsklausuler:
  - Hvem ejer dataene?
  - Hvad sker der, hvis data kompromitteres?
  - Er der klare regler for datalagring, overførsel og sletning?
- Politikker for acceptabel brug:
  - Hvordan må kunden anvende dine systemer og tjenester?
  - Er der begrænsninger for automatiseret adgang, datamining eller videredistribution?
- Ansvarsbegrænsninger:
  - Begræns din eksponering, hvis kunden bliver kompromitteret, og det påvirker din organisation.
  - Er der fastsat maksimale erstatningsbeløb?
- Opsigelsesrettigheder:
  - Giver kontrakten mulighed for at opsige samarbejdet i tilfælde af brud på cybersikkerheden eller overtrædelser af sikkerhedspolitikker?

Tema 5/8

Tema 5: Overvågning og løbende kontroller

- Kontinuerlig overvågning:
  - Opsætning af alarmer og notifikationer ved mistænkelig adfærd fra kundekonti.
  - Brug af automatiserede systemer til at opdage uregelmæssigheder i realtid.
- Regelmæssige gennemgange:
  - Særligt vigtigt for store konti eller kunder med høj risikoprofil.
  - Periodisk evaluering af adgangsrettigheder og sikkerhedspolitikker.
- Logning og revision:
  - Sikring af, at alle kunders aktiviteter på platformen bliver logget på en sikker og sporbar måde.
  - Mulighed for at gennemføre audits ved behov eller ved hændelser.

Tema 6/8

Tema 6: Forsikring og finansiel risiko

- Forsikring mod cybersikkerhed:
  - Skal enten du eller kunden have en forsikring af cybersikkerhed, afhængigt af tjenestens følsomhed og risikoprofil?
  - Er der krav om dokumentation for aktiv forsikringsdækning?
- Kompensationsklausuler:
  - Fastlæggelse af økonomisk ansvar, hvis et sikkerhedsbrud opstår som følge af kundens handlinger eller forsømmelser.
  - Klare regler for erstatning og omkostningsdækning i tilfælde af tab eller skade.

Tema 7/8

Tema 7: Overholdelse og lovgivningsmæssige forpligtelser

- Hvis databehandlingen er reguleret af f.eks. GDPR, HIPAA (Health Insurance Portability and Accountability Act), Sarbanes-Oxley Act (SOX) eller lignende, bør følgende sikres:
  - Korrekte databehandleraftaler: Der skal være underskrevne aftaler, der klart definerer roller og ansvar i forhold til databehandling.
  - Nødvendige sikkerhedscertificeringer: Kunden (eller du selv) skal have relevante certificeringer på plads – eller være i gang med at opnå dem – såsom ISO 27001 eller tilsvarende.

Tema 8/8

Tema 8: Forventninger til underretning ved sikkerhedsbrud

- Aftal klare tidsrammer for underretning, hvis en af parterne opdager en sikkerhedshændelse, der kan påvirke den anden part.
  - Hvor hurtigt skal der gives besked? (f.eks. inden for 24 eller 72 timer).
- Hvad skal underretningen indeholde?
  - Beskrivelse af hændelsen?
  - Hvilke data eller systemer er berørt=?
  - Foranstaltninger der er truffet eller planlagt=
- Hvordan skal underretningen ske?
  - Via e-mail, telefon, sikker portal eller andet?
- Hvem skal modtage underretningen?
  - Navngivne kontaktpersoner eller roller hos begge parter?

Advarselsflag – når kunden udgør en potentiel risiko

Det bør betragtes som en advarsel, hvis:

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