Vejledning til anvendelse af sikkerhedsbilaget 02.14 It-konsulenter (DIS) (2024)

Kunden skal enten benytte Bilag 6 Sikkerhedskrav (SKI´s Sikkerhedskrav til it-konsulentaftaler), eller kunden erstatter indholdet af Bilag 6 med egne sikkerhedskrav.

Nærværende vejledning er alene målrettet Bilag 6 Sikkerhedskrav SKI´s Sikkerhedskrav til It-konsulentaftaler).

Kundens korrekte anvendelse af bilaget forudsætter, at Kunden kender sine risici, sine kritiske systemer og data.

Manglende kendskab til sine risici, nedbrud af kritiske it-systemer og databrud kan medføre store konsekvenser for kunder/myndigheder, borgere og samfund.

Hvis en konsulent skal have adgang til Kundens systemer og/eller data skal Kunden således vurdere omfanget heraf i forbindelse med udarbejdelse af et konkret indkøb i DIMS forud for indgåelse af en Leveringskontrakt og på den baggrund vurdere, hvilke sikkerhedspakker der er passende og nødvendige ved konsulentens opgaveløsning.

Sikkerhedskravene/-foranstaltninger er inddelt i pakkerne; B, 1, 2 og 3 samt en række tillægsforanstaltninger inddelt i tillægspakkerne: Fjernadgang, Mobile, BYOD, Udvikl, Projekt.

Om B (Basis):
Hvis konsulenten ikke skal have adgang til nogen former for følsomme/fortrolige eller kritiske data/systemer og konsulenten alene arbejder hos Kunden og med Kundens udstyr, så gælder B (Basis). Her kræves alene, at medarbejderen underskriver Kundens Fortrolighedsaftale (NDA) og Kundens Acceptabel Brug af Udstyr Politik (AUP). Det vil her være Kundens egen sikkerhedspolitik og -retningslinjer, der er gældende.

Om sikkerhedspakkerne 1,2 og 3:
Adgangen til Kundens systemer og/eller data er i sikkerhedsbilaget inddelt i tre kategorier/tre sikkerhedspakker:

1: krav ved få almindelige personoplysninger, få forretningskritiske data samt adgang til ikke-kritiske systemer og applikationer
2: krav ved nogle (omfang vurderes af Kunden) almindelige personoplysninger, nogle forretningskritiske data og adgang til enkelte kritiske systemer
3: krav ved adgang til følsomme personoplysninger, mange almindelige personoplysninger, fortrolige data, mange forretningskritisk data samt flere kritiske systemer

Om tillægspakkerne:
Derudover er der krav til sikkerhed i tillægsforanstaltninger inddelt i tillægspakkerne: Fjernadgang, Mobile, BYOD, Udvikl, Projekt. Højre kolonne, i skemaet nedenfor, angiver hvornår den enkelte tillægspakke finder anvendelse.

Tillægspakke	Relevant, hvis
Fjernadgang	Leverandørens medarbejdere arbejder på Leverandørens udstyr fra Leverandørens lokationer

	Leverandørens medarbejdere arbejder på Leverandørens udstyr hjemme-fra
Mobile	Leverandørens medarbejdere arbejder på Leverandørens udstyr, dvs. Leverandørens bærbare PC'er, tablets og smartphones
BYOD (bring your own device)	Medarbejderen benytter eget udstyr, dvs. medarbejderens eget udstyr
Udvikl	Leverandøren skal rette/ændre/tilpasse kode eller konfigurationer i kritiske systemer og applikationer, jf. bilag 6 Sikkerhed.
Projekt	Leverandøren har projektledelsesansvar jf. bilag 1 Kundens behovsopgørelse

Hvilken sikkerhedspakke er relevant for kunden at vælge?

Kravene er inddelt i fire niveauer/kategorier. Niveauerne er B (Basis), pakke 1, pakke 2 og pakke 3, hvor laveveste niveau, niveau B, ikke indeholder andre krav end Kundens egen sikkerhedspolitik og -retningslinjer og pakke 3 indeholder de mest skærpede krav. Kravene i pakke 1 er indeholdt i pakke 2. Kravene i pakke 1 og 2 er indeholdt i pakke 3.

SKI har således identificeret risici som er relevante at overveje og har struktureret relevante krav i forskellige sikkerhedspakker der er udtryk for sikkerhedsforanstaltninger der kan håndtere kundens risici.

Kunden skal læse alle sikkerhedskravene og på den måde få en hjælp til at danne sig en et overblik over hvilke risici der er relevante at overveje i forhold til Kundens situation og indkøbsbehovet.

Kunden kan, ved at læse sikkerhedskravene, sammenholdt med deres rangering, dvs. pakkerne 1 til 3, og med sit eget estimat af sandsynlighed og konsekvens af identificerede risici, vælge den sikkerhedspakke med krav, som indeholder passende og nødvendige foranstaltninger til at håndtere Kundens risici.

Det bemærkes at tillægspakkerne (Fjernadgang, Mobile, BYOD, Udvikl, Projekt) ikke indeholder rangerede krav (som det er tilfældet for pakkerne 1-3). Kravene i tillægspakkerne er gældende, når konsulenten ved sin adfærd eller ved udtrykkelig aftale med kunden har gjort kravene relevante i forbindelse med opgavens løsning.

På baggrund af kravene i sikkerhedspakkerne 1-3 og sammen med Kundens egen risikovurdering af den opgave, som det konkrete indkøb vedrører, forud for indgåelse af den konkrete Leveringskontrakt, skal Kunden stille krav om de relevante sikkerhedspakker Dvs. B, eller,1, eller 2 eller 3. Tillægspakkerne aktiveres blot automatisk, hvor de er relevante for opgavens udførelse.

Kontraktstyring og sikkerhed

Det er vigtigt, at kunden vurderer og vælger den passende og nødvendige sikkerhedspakke i forbindelse med oprettelse af deres indkøb, så konsulenten er bedst muligt oplyst om de sikkerhedskrav der gælder for den konkrete leveringskontrakt. Derfor er det relevant for kunden at tænke sikkerhedskravene ind i sin behovsopgørelse som danner grundlag for opgavens udførelse.

Kunden bør desuden ved sin oprettelse af indkøbet oplyse, såfremt der er situationer, (som tillægspakkerne er relevante for), som kunden ikke kan acceptere. Se hvad tillægspakkerne regulerer i skemaet ovenfor og de nærmere krav i selve sikkerhedsbilaget.

Hvis kunden vurderer, at der er forhold der fører til en ændret risikovurdering, der indebærer, at kravene til sikkerhed skærpes, skal kunden håndtere dette ved en ændringsanmodning til sin leverandør. Det påhviler kunden, førend ændringsanmodningen kan gennemføres, at vurdere, hvorvidt ændringen kan foretages indenfor udbudslovens regler. Dette kunne fx tilfældet, hvis kunden i forbindelse med at de udbød deres indkøb og inden kontraktunderskrift har vurderet at sikkerhedspakke 2 indeholder de nødvendige og passende sikkerhedsforanstaltninger, men det senere viser sig, at leverandøren skal behandle følsomme persondata, hvor kundens nye og dermed revurderede risikovurdering fører til, at også sikkerhedskravene fra sikkerhedspakke 3 (som er skærpet i forhold til sikkerhedspakke 2), er nødvendige for kunden at gøre gældende.]

Leverandøren og dennes underleverandører, herunder medarbejdere, der medvirker til at opfylde Leveringskontrakten, er forpligtede til at respektere og samarbejde loyalt med Kunden om dennes forpligtelser vedrørende informationssikkerhed.

Det indebærer bl.a. at medvirke til, at Kunden kan opfylde sine forpligtelser i henhold til ISO 27001 eller tilsvarende, når dette er er nødvendigt for at opfylde Leveringskontrakten, og i fornødent omfang ved at implementere processer, der understøtter det sikkerhedsniveau som Kundens forpligtelser og risikoprofil forudsætter.

Leverandøren er dog ikke forpligtet til at medvirke i et omfang, der rækker videre end de til enhver tid gældende forpligtelser og bestemmelser, som Kunden er omfattet af.