Rådet for Digital Sikkerheds holdningspapir om styring af leverandørsikkerhed

Rådet for Digital Sikkerhed opfatter sikring af informationssikkerhedsniveauet hos leverandører som en væsentlig del af enhver organisations sikkerhedsarbejde. Opgaven kan opdeles i fem faser. Det er afgørende for succesen, at både kunde og leverandør engagerer sig aktivt i arbejdet.

God sikkerhed hos leverandøren stiller krav til kunden

En organisations informationssikkerhedsniveau er i væsentlig grad afhængig af sikkerheden hos dem, der leverer it-ydelser til den. Derfor er det afgørende for sikkerheden, at organisationer har styr på sikkerhedsniveauet hos deres leverandører.

Det gælder både for private virksomheder og offentlige myndigheder. Således er der et konkret initiativ om styring af leverandørsikkerhed i regeringens "National strategi for cyber- og informationssikkerhed," der blev udgivet i maj 2018. Her står der:

"For at øge it-sikkerheden og forsyningssikkerheden for myndighedernes samfundskritiske it-systemer indføres der skærpede krav til alle offentlige myndigheder om brug af tilstrækkelige sikkerheds- og styringsbestemmelser i fremtidige kontrakter for samfundskritiske it-systemer samt til myndighedernes styring af disse."

I dette holdningspapir kommer Rådet for Digital Sikkerhed med konkrete forslag til, hvordan en virksomhed eller myndighed kan organisere arbejdet med sikkerheden hos leverandører af it-drift og i forbindelse med outsourcing af it-drift.

Udfordringen

Ansvaret for at sikre data ligger hos dataansvarlige. En virksomhed kan lægge driften af et it-system ud til en leverandør, men den kan aldrig outsource sit ansvar.

Hvis leverandørens it-systemer bliver hacket, og personoplysninger dermed kommer i de forkerte hænder, ligger ansvaret som udgangspunkt hos den dataansvarlige, ikke hos databehandleren (leverandøren).

Derfor er det afgørende for informationssikkerheden at have styr på sikkerheden hos leverandører.

Rådet for Digital Sikkerhed
Toldbodgade 12, 1253 København K
Telefon: +45 9137 5600 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Fem trin til styring af leverandørsikkerhed

Rådet for Digital Sikkerhed foreslår, at processen opdeles i fem trin:

1. Skab et ensartet overblik over leverandører og risikovurder dem.
2. Skriv krav til leverandørens sikkerhed ind i kontrakten.
3. Opbyg et rammeværk med roller og rapportering.
4. Mål og overvåg, at leverandøren overholder sikkerhedskravene.
5. Kommuniker løbende om trusler, sårbarheder og risici.

1. Skab et ensartet overblik over leverandører og risikovurder dem

For at få succes med it-sikkerhedsleverandørstyring er det afgørende, at virksomheden skaber sig et fuldt overblik over, hvilke aftaler den har med hvem. Hvad er kontraktens genstand, og hvor stor en risiko er forbundet med den pågældende leverandør? Man kan med fordel overveje at anvende et VRM-system (Vendor Risk Management)[1]. Det er software, der hjælper med at organisere de data, der bruges til at risikovurdere leverandøren.

Virksomheden bør sikre, at der er repeterbare processer, og at den får vurderet, prioriteret og mitigeret risici forbundet med den enkelte leverandør.

2. Skriv krav til leverandørens sikkerhed ind i kontrakten

Informationssikkerhed er så centralt et emne, at det skal skrives ind i kontrakten med leverandøren. På den måde indgår kravene på lige fod med krav til funktionalitet. Og de kan håndhæves på samme måde som andre kontraktlige krav – fx med bod, hvis leverandøren ikke overholder kravene.

Før sikkerhedskrav kan skrives ind i kontrakten, skal kunden fastlægge dem: Hvad ønsker kunden beskyttet på hvilket niveau?

Når kravene er på plads, skal kunde og leverandør aftale, hvem der har ansvaret for hvad. Det kan med fordel gøres via såkaldte RACI-skemaer (Responsible, Accountable, Consulted, Informed).

Fordelen ved RACI-skemaer eller lignende opstillinger er, at de giver et entydigt overblik over roller og ansvar. Dermed ved både kunde og leverandør, hvad der forventes af dem.

Rådet anbefaler, at man lader sig inspirere af Understanding Responsibility Assignment Matrix (RACI Matrix) af Cara Doglione[2].

[1] https://www.bitsighttech.com/blog/vendor-risk-management-definition
[2] https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/

Hvis data omfatter personoplysninger, skal det i forhold til GDPR bestemmes, hvem der er dataansvarlig og databehandler for hvilke behandlinger. Der skal eventuelt indgås en databehandleraftale eller en aftale om fordelingen af ansvaret mellem to dataansvarlige. Hvis der er tale om en databehandleraftale, skal kravene i artikel 28 i persondataforordningen opfyldes. Datatilsynet har lavet udmærkede skabeloner til begge situationer, som kan findes på tilsynets hjemmeside[3].

3. Opbyg et rammeværk med roller og rapportering

Til at holde styr på samarbejdet bør kunden udarbejde et rammeværk, som aftales med leverandøren, før de underskriver kontrakten. Større organisationer kan med fordel udvikle eller erhverve sig et standard-rammeværk, som er dækkende for alle leverandørerne og har defineret politikker, guidelines og vejledninger for arbejdet. Rammeværket bør også beskrive governance.

Rammeværket er en samling af sikkerhedskontroller, der skal efterleves. Ofte er de først udviklet til intern brug, fx i form af en sikkerhedspolitik. Med udgangspunkt i de interne sikkerhedskrav kan virksomheden udarbejde et tilsvarende rammeværk målrettet leverandører.

Afhold regelmæssige møder

Efter at kontrakten er underskrevet, begynder det daglige samarbejde mellem leverandør og kunde. Når it-driften ligger internt, skal den sikkerhedsansvarlige nok høre om det, når der opstår sikkerhedshændelser. Det er mindre sikkert, når driften er lagt ud til en ekstern partner. Derfor er kommunikation afgørende.

En større virksomhed kan fx afholde møder med disse intervaller:

- Ugentlige telefonmøder med leverandøren om den aktuelle status.
- Månedlige møder med leverandøren, hvor også mere principielle emner tages op.
- Kvartalsmøder på en til to dage i form af workshops, hvor man fx aftaler ændringer af processer og metoder.

Aftal regelmæssige rapporter fra leverandøren

Leverandøren skal løbende rapportere om sikkerhedshændelser og status på de kontroller, som er aftalt i forbindelse med rammeværket. Derved opnår kunden indsigt i, hvorvidt de aftalte kontroller er blevet gennemført, og om der har været sikkerhedshændelser. Tilsammen bør det give et retvisende billede af sikkerhedsniveauet. Kunde og leverandør kan aftale, at der sendes rapporter op til hvert møde. Dermed kommer der fx en månedsrapport og en kvartalsrapport.

Måneds- og kvartalsrapporterne kan fx analysere tendenser, der fremgår af statistikker over de sikkerhedshændelser, leverandøren har behandlet.

[3] https://www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/

Hvis der er tale om behandling af personoplysninger, og der er indgået en databehandleraftale, bør aftalen reviewes årligt. Der skal også mindst årligt foreligge en rapport, som redegør for sikkerhedsforholdene, f.eks. baseret på ISAE 3402 type II[4] eller ISAE3000[5].

Integrer sikkerhed i den øvrige leverandørstyring

Andre afdelinger end sikkerhedsafdelingen hos kunden har også et forhold til leverandøren. Det gælder fx kontraktafdelingen og alle de afdelinger, der anvender de it-ydelser, leverandøren leverer.

Derfor er der behov for en intern metode til leverandørstyring på tværs af afdelinger. Den skal sikre en fælles forståelse for, hvilket modenhedsniveau leverandøren befinder sig på, og hvor den er på vej hen.

Den interne leverandørstrategi skal være forankret på både det operationelle, det taktiske og det strategiske plan.

Det operationelle plan har fokus på mål og rapportering. Arbejdet foregår blandt andet via de ugentlige møder.

Det taktiske niveau lægger planer for, hvad det operationelle plan skal lave. Her arbejder lederne med den videre udvikling af samarbejdet og samler op på elementer fra det operationelle plan. Hvis rapporter viser, at målene ikke bliver nået, eskaleres sagen fra det operationelle til det taktiske niveau. Her diskuterer lederne, hvilke konsekvenser problemerne skal have for leverandøren.

Det strategiske niveau, det vil sige topledelsen, ser på de store linjer i aftalerne med leverandører, herunder økonomien. Her foregår det visionære, strategiske arbejde. Hvis kunde og leverandør ikke kan blive enige på det taktiske niveau, eskaleres sagen til det strategiske niveau.

4. Mål og overvåg, at leverandøren overholder sikkerhedskravene

For at sikre, at sikkerhedskravene i kontrakten bliver overholdt i praksis, bør kunden måle og overvåge leverandørens præstation. Det kan dels ske via den løbende rapportering, dels via en egentlig audit (revision).

Faste KPI'er (Key Performance Indicator) gør det lettere at vurdere indsatsen. Det er målbare indikatorer, som kunde og leverandør er enige om.

[4] http://isae3402.com/ISAE3402_reports.html

[5] https://www.fsr.dk/Faglige_informationer/Om_revisor/Persondataforordningen/Erklaering%20om%20persondata_210917

Der kan fx være et mål om, at leverandørens softwareudvikling skal følge anbefalingerne for sikker softwareudvikling. Her kan en KPI være, hvor mange udviklere der er uddannet inden for secure software development lifecycle (SSDLC)[6]. Nogle eksempler på KPI'er:

- Hvor lang tid går der, fra en sårbarhed bliver opdaget, til sikkerhedshullet er lukket?
- Er der foretaget det aftalte antal sårbarhedsscanninger?
- Hvor hurtigt er der taget hånd om hver sikkerhedshændelse?

Rapporter til kundens topledelse

Der skal være en løbende rapportering til topledelsen om status for samarbejdet med leverandøren om sikkerhed. Det er både en status over, hvor sikker leverandøren er, og over styringen og samarbejdet (governance).

Rapporteringen kan fx finde sted hvert kvartal og dække fire punkter:

- Årlig vurdering af sikkerhedsniveau – bliver den udført?
- Regelmæssige møder – bliver de afholdt med værdi?
- Regelmæssig rapportering – kommer rapporterne som aftalt?
- Modenhed inden for governance af sikkerhed – hvor langt er leverandøren nået?

5. Kommuniker løbende om trusler, sårbarheder og risici

Den løbende kommunikation er afgørende for, at samarbejdet om sikkerhed fungerer. Derfor må rapporteringen ikke ende som envejskommunikation, hvor rapporterne i værste fald end ikke bliver læst hos kunden.

Hvis der fx opstår sikkerhedsbrister i forbindelse med behandling af personoplysninger, skal leverandøren/databehandleren uden unødig forsinkelse rapportere det til den dataansvarlige. Den dataansvarlige skal rapportere det til Datatilsynet inden for 72 timer.

Både leverandør og kunder skal afsætte personer til opgaven

Samarbejde kræver en indsats fra alle involverede.

Kundens medarbejdere skal læse leverandørens rapporter om sikkerhed. Og de skal reagere på oplysninger, der kræver handling.

Nyttige værktøjer

Database over leverandører og kontrakter

Det kan være en fordel at opbygge en samlet database over virksomhedens leverandører og kontrakterne med dem (kontraktstyring). Den kan udbygges med en tjeneste, der løbende oplyser

[6] https://www.microsoft.com/en-us/sdl/default.aspx

om sikkerhedsforhold angående de enkelte leverandører. Den type tjeneste kan fx oplyse om aktuelle sikkerhedshændelser eller softwareopdateringer relateret til hver leverandør.

Især virksomheder med mange leverandører kan overveje at indføre sådan et værktøj. Her kan de opdele leverandørerne i kategorier efter deres vigtighed og oprette alarmer på de mest kritiske leverandører, når de fx er udsat for en sikkerhedshændelse.

Virksomheden kan oprette en samarbejdsdatabase med status på udeståender både fra den løbende sikkerhedsrapportering og fra de årlige revisionserklæringer. Derved bliver der løbende fulgt op på status, og alle parter er enige om, hvilke udeståender der er. Disse udeståender bør løbende rapporteres til det taktiske niveau og i særligt kritiske tilfælde også til det strategiske niveau.

Konklusion

Leverandørens niveau af informationssikkerhed har direkte indflydelse på kundens sikkerhedsniveau. Derfor er der behov for stram styring af sikkerheden og afklaring af behov og forventninger på begge sider. Det kan med fordel ske ved at indskrive sikkerhedskrav, roller og ansvarsfordeling i kontrakten. Derefter bør det daglige arbejde foregå på en struktureret måde, fx med den opdeling i fem faser, dette holdningspapir foreslår.