Kom i dialog med din IT-leverandør

Som virksomhedsleder, der køber IT-løsninger, har du det overordnede ansvar for at sikre, at den løsning, du køber, er tilstrækkelig sikker, og at løsningen bliver anvendt forsvarligt. Det er dog ikke nødvendigvis dig, der skal eksekvere de nødvendige sikkerhedsforanstaltninger, men derimod typisk din IT-leverandør og den IT-ansvarlige i din virksomhed.

Med dette dialogværktøj kan du afdække, om leverandøren har tilstrækkelig fokus på IT-sikkerhed. I bør tale med jeres IT-leverandør om alle punkterne, men kravene til sikkerhed kan naturligvis variere alt efter, hvor kritiske og følsomme din virksomheds data er.

Dialogværktøjet er primært tiltænkt dialog med mindre IT-leverandører, hvor det er vigtigt at kontrollere, at de har styr på sikkerheden.

Du kan sende spørgeskemaet til din IT-leverandør og bede dem besvare spørgsmålene, så du kan få et overblik over deres sikkerhedstiltag og bruge skemaet som udgangspunkt for en dialog. Med afsæt i svarene kan I afdække ansvarsfordelingen. Der er nemlig nogle opgaver, du som virksomhedsleder har ansvaret for, når du køber IT-løsninger.

Spørgeskemaet er holdt kort og overskueligt, og omhandler derfor kun de væsentligste forhold som du skal være opmærksom på. For yderligere og mere detaljeret information henvises til f.eks. Center for Cybersikkerheds vejledning om informationssikkerhed i leverandørforhold.[1]

Det er altid en god idé at få ekstern bistand fra en rådgiver, hvis der er noget, du er usikker på.

Overblik over leverandører

Når et nyt behov opstår, er det en god idé at få skabt et overblik over jeres eksisterende leverandører og se om en af disse kan løse behovet. På den måde kan antallet af leverandører begrænses og det sikres samtidig, at der ikke forekommer et funktionsoverlap.

Risikovurdering og din virksomheds behov for sikkerhed

Når du skal vælge en ny IT-løsning, skal du overveje, hvor stor en risiko der er forbundet med at anvende den pågældende løsning. Det betyder, at du skal have overblik over, hvilke data løsningen skal håndtere for din virksomhed og hvor vigtige de er for forretningen. Der skal også tages stilling til, hvilke tekniske og organisatoriske konsekvenser, der er forbundet med at anvende løsningen. Dét omfatter ikke kun IT-leverandørens sikkerhed, men også hvilken betydning det vil have for din virksomhed, hvis noget går galt. Hvis konsekvenserne ved brug af løsningen er store for forretningen, skal der stilles tilsvarende høje krav til IT-leverandøren. Dialogen om leverandørens sikkerhedstiltag er en vigtig del af risikovurderingsprocessen. For yderligere information om hvordan I vurderer risici henvises til vejledning og skabelon til risikovurdering på sikkerdigital.dk.

Spørgeskemaet er ikke en tjekliste eller et juridisk dokument som f.eks. en data-behandleraftale. Skemaet kan hjælpe dig med at fastlægge de ting, som skal indgå i den kontrakt, der typisk udarbejdes mellem virksomhed og leverandør af IT-løsninger.

1) fe-ddis.dk/cfcs/nyheder/arkiv/2019/Pages/Leverandoerstyring-cyberforsvar.aspx

fe-ddis.dk/cfcs/publikationer/Documents/Vejledning-Informationssikkerhed-i-leverandoerforhold.pdf

Erhvervsstyrelsen

Brugen af IT-leverandørens løsning kan også stille krav til jer og jeres sikkerhedspolitik. Det er derfor vigtigt at få klarlagt, hvilket ansvar I har i relation til løsningen.

Dialogværktøjet kan både anvendes ved indgåelse af aftaler med nye IT-leverandører og ved den løbende vurdering af eksisterende IT-leverandørers sikkerhedsniveau.

On-premise løsninger og cloud-services

Traditionelt har IT-løsninger været noget virksomheden køber og afvikler på egne servere placeret hos virksomheden selv (også betegnet som en on-premise løsning). I dag leveres mange IT-løsninger som hostede løsninger eller cloud-services, dvs. tjenester der afvikles på centrale servere, der står hos enten IT-leverandøren selv eller i store centrale datacentre. Ofte tilgås cloud-servicen via en almindelig web-browser.

De krav, der skal stilles til IT-leverandøren, er forskellige alt efter om det er en cloud-service eller on-premise løsning. Ved en cloud-service lægger du mere af ansvaret for sikkerhed over på IT-leverandøren, bl.a. ansvaret for den fysiske sikkerhed, opdatering af løsningen og opbevaring af data. Men der vil stadig være en række ting, du selv er ansvarlig for.

Når du skal vurdere sikkerheden i cloud-services, er det vigtigt at prioritere indsatsen. Store og udbredte cloud-services har som regel godt styr på den basale sikkerhed. Her giver det bedst mening at rette opmærksomheden på dit eget ansvar. Ved mindre IT-leverandører af cloud-services (f.eks. udbydere af branchespecifikke løsninger eller hosting af egne løsninger) er der derimod ofte behov for en mere uddybende dialog om deres sikkerhed.

Hvis din virksomhed selv driver løsningen på egne eller hostede servere, bør den IT-ansvarlige kunne besvare en stor del af spørgsmålene.

Forstå svarene fra IT-leverandøren

Hjælp til at forstå svarene fra din IT-leverandør
Selve spørgeskemaet er opdelt i følgende fem hovedområder:

1. Hvad gør IT-leverandøren for at beskytte mod uønsket adgang?
2. Hvad gør IT-leverandøren for at sikre tilgængelighed og høj oppetid?
3. Hvad gør IT-leverandøren for at dokumentere deres sikkerhed?
4. Hvad gør IT-leverandøren for at passe på persondata (GDPR)?
5. Hvad er ansvarsfordeling mellem jer som kunde og IT-leverandøren?

I det følgende finder du en række uddybende bemærkninger til de enkelte spørgsmål i spørgeskemaet. Bemærkningerne er tænkt som en hjælp til at forstå svarene fra IT-leverandøren og angiver de svar, som kan forventes ved et passende sikkerhedsniveau. Husk at oversigten ikke er en facitliste, men derimod er tænkt som input til en dialog med IT-leverandøren.

1. Hvad gør IT-leverandøren for at beskytte mod uønsket adgang?

1. A. For at I ved, hvor jeres data opbevares, skal IT-leverandøren af cloud-services kunne oplyse, hvor serverne til deres løsning er placeret og hvorvidt de benytter underleverandører, afvikles leverandørens løsning f.eks. via en hosting eller en anden cloud udbyder? IT-leverandøren skal desuden kunne oplyse, hvordan de sikrer den fysiske adgang til deres datacenter og servere.

Hvis IT-leverandøren opbevarer eller overfører data udenfor EU, skal du være særligt opmærksom på evt. overførsel af persondata (GDPR).

Den fysiske sikkerhed bør bl.a. omfatte passende fysiske sikringstiltag mod indbrud (fx indhegning, aflåste områder, videoovervågning og logget adgangskontrol).

1. B. IT-leverandøren af cloud-services skal kunne redegøre for, hvordan jeres data er beskyttet og hvilke tekniske sikkerhedsforanstaltninger de har etableret. Dette kan indebære mange forskellige ting, herunder anvendelse af malwarebeskyttelse (antivirus), firewall, netværkssegmentering og kryptering (både ved opbevaring og i transit).

IT-leverandøren af cloud-services bør som minimum have etableret en firewall-løsning samt passende beskyttelse mod malware, mens de øvrige foranstaltninger skal ses i forhold til hvordan løsningen fungerer.

1. C. IT-leverandøren af cloud-services forventes løbende at overvåge sikkerheden i deres løsning og systemer, dvs. holde øje med anormal aktivitet og at løsningen ikke bliver kompromitteret af hackere, der stjæler data eller kompromitterer tilgængeligheden.

IT-leverandøren bør som minimum opsamle logfiler fra firewall, antimalware, servere og applikationer, samt have en fast procedure for løbende gennemgang af logfiler for mulige sikkerhedshændelser.

Leverandøren bør desuden kunne redegøre for overvågningen herunder brug af værktøj til opsamling af sikkerhedshændelser, f.eks. brug af Security Information and Event Management (SIEM), processer og bemandingen.

1. D. Sårbarheder kan lede til kompromittering af løsningen og dermed ramme sikkerheden af jeres data. Derfor er det vigtigt, at IT-leverandøren løbende opdaterer løsningen med sikkerhedsrettelser. En opdatering skal gennemføres kort tid efter opdateringen er blevet gjort tilgængelig. IT-leverandøren skal desuden kunne redegøre for, hvordan de håndterer henvendelser om sikkerhedsproblemer.

IT-leverandøren bør som minimum kunne redegøre for, hvornår de opdaterer deres systemer. Almindelige sikkerhedsopdateringer bør installeres senest en måned efter de er frigivet og leverandøren bør desuden have en proces for hurtig installation af kritiske sikkerheds-opdateringer.

1. E. IT-leverandøren skal kunne redegøre for hvilke initiativer de har taget for at sikre løsningen mod uønsket adgang. Uønsket adgang kan forekomme af forskellige årsager, f.eks. ved at en hacker der har fået adgang til en brugerkonto.

Løsningen bør bl.a. gøre brug af en krypteret forbindelse (f.eks. https) og være sikret mod hacking af passwords f.eks. ved låsning af kontoen efter 10 forkerte loginforsøg, brug af multifaktor login eller Single Sign-On (SSO).

2. Hvad gør IT-leverandøren for at sikre tilgængelighed og høj oppetid?

2. A. IT-leverandøren bør kunne redegøre for om de har sørget for en redundant løsning. Dette er særligt vigtigt ved løsninger, der indeholder data, der er kritisk for forretningen. En redundant løsning sikrer oppetid ved nedbrud af hardware, netværksforbindelser eller lignende.

IT-leverandøren kan have mange forskellige niveauer af redundans, f.eks. flere forbindelser til internettet, ekstra servere og mulighed for at afvikle løsningen fra forskellige fysiske lokationer. Typen af redundans skal give mening i forhold til hvor vigtig løsningen er.

2. B. IT-leverandøren skal oplyse hvordan, hvornår og hvor hurtigt I kan få hjælp ved kritiske problemer. For cloud-services skal den garanterede tilgængelighed oplyses. Dette angives normalt i form af en Service Level Agreement (SLA), der bl.a. angiver hvornår en service er tilgængelig og reaktionstider ved fejl og problemer.

IT-leverandøren bør kunne redegøre for hvilke SLA-niveauer der tilbydes og hvad disse indebærer. Ofte vil der kunne tilkøbes et højere SLA-niveau. Du skal vurdere, hvilket niveau din virksomhed har brug i forhold til vigtigheden af oppetid for løsningen.

2. C. IT-leverandøren af cloud-services bør have en plan for, hvordan løsningen kan genskabes, hvis noget går galt. Det kan være en hacker der er kommet ind i systemet, en server der er brudt sammen eller noget helt tredje. Det er for sent at udtænke løsninger, når skaden er sket.

Leverandøren bør have daglige backup-rutiner. Det er vigtigt at IT-Leverandøren kan redegøre for, hvor ofte der tages backup, hvordan backuppen opbevares og de processer de har på plads for at sikre hurtig retablering. IT-leverandøren skal ligeledes have testet backuppen for at sikre at denne er funktionel. Leverandøren skal kunne redegøre for hvor ofte deres backup testes og kunne angive hvornår denne sidst er blevet testet. Disse tests kan f.eks. være månedlige, dog skal der altid foretages en test når der er blevet udført en større ændring af løsningen.

Ved on-premise løsninger skal din virksomhed have egne rutiner og procedurer for dette. Det er vigtigt at vide, hvor hurtigt løsningen kan genskabes efter et nedbrud.

2. D. I tilfælde af en hændelse, f.eks. ransomware, er det vigtigt at have en plan for hvordan hændelser skal håndteres. Planen skal være prædefineret, så der ikke er nogen tvivl om, hvordan situationen skal håndteres og hvem der skal kontaktes, hvis noget går galt.

IT-leverandøren bør som minimum have udarbejdet en beredskabsplan, der som minimum indeholder en eskalationsprocedure, kontaktpunkt og responstid.

Din virksomhed bør overveje om der er behov for tilsvarende interne procedurer i jeres virksomhed.

3. Hvordan arbejder IT-leverandøren med sikkerhed og hvordan dokumenteres det?

3. A. Leverandøren kan evt. henvise til, eller være certificeret efter, en eller flere standarder eller rammeværker, der findes i forhold til IT-sikkerhed. Dette kan f.eks. være

- ISO 27001, der er en international ISO-standard som man kan blive certificeret efter når man har processer på plads til styring af ens IT-sikkerhed.

www.ds.dk/da/standardisering/ledelsesstandarder/informationssikkerhed
www.iso.org/isoiec-27001-information-security.html

- ISAE 3402, som er en international revisionserklæringsstandard, som primært anvendes til revision af de tekniske kontroller hos IT-service-leverandører.

  en.wikipedia.org/wiki/ISAE_3402

  www.stil.dk/administration-og-infrastruktur/systemrevision-af-studieadministrative-systemer/isae-3402-standarden

- OWASP, der er et projekt med en række anbefalinger og best practice i forhold til beskyttelse af især webapplikationer.

  www.owasp.org/

- STRIDE, der er en model for modellering af trusler mod software løsninger for at sikre alle potentielle sårbarheder og trusler er overvejet.

  en.wikipedia.org/wiki/STRIDE_(security)

- NIST Cybersecurity Framework, som er en ramme for de processer og kompetencer som skal være på plads for at opretholde et ordentligt sikkerhedsniveau.

  www.nist.gov/cyberframework

- Center for Internet Security (CIS) Top 20 Controls, der er en prioriteret liste over de 20 kontroller, der mest effektivt imødegår cyberangreb.

  www.cisecurity.org/controls/cis-controls-list/

Der er stor forskel på, hvad de enkelte standarder eller rammeværker omfatter og hvorvidt det blot er en best practice anbefaling der efterleves eller om IT-leverandøren har været igennem en egentlig certificerings- eller revisionsproces. Det er din virksomheds aktuelle sikkerhedsbehov, der afgør om en certificering er relevant. Hvis virksomheden har store sikkerhedskrav, der indbefatter mange kritiske data, giver det mening at IT-leverandøren har passende certificering. Behandler løsningen mindre kritiske data, bør løsningen stadig efterleve best practise fra en af de ovenstående standarder eller rammeværk.

3. B. IT-leverandøren bør få sikkerhedstestet deres produkt eller service, og resultaterne bør kunne fremvises. Alt efter løsningen kan der gennemføres sikkerhedstest på forskellige niveauer, f.eks. penetrationstests, 3. parts audit, codereview eller sikkerhedsreview.

- Penetrationstest er en form for lovlig hacking, hvor der identificeres sårbarheder i løsningen via de samme metoder som en kriminel ville bruge.

- 3. parts audit betyder, at en ekstern certificeret auditør gennemgår løsningens IT-kontroller for sikkerhedshuller.

- Codereview omfatter at sikkerhedskontrollerne i løsningen (kildekoden) gennemgås og det vurderes om løsningen er sikker.

- Sikkerhedsreview kan indeholde forskellige elementer, bl.a. en vurdering af sammensætningen af anvendte sikkerhedsprodukter og hvilken beskyttelsesevne disse udgør.

IT-leverandøren bør som minimum få udført sikkerhedstests, når der sker større ændringer af løsningen. For cloud-services bør der foretages regelmæssige sikkerhedstests i forhold til leverandørens risikovurdering.

3. C. IT-leverandøren bør have tænkt sikkerheden ind i design og udvikling af løsningen. I forlængelse af dette bør leverandøren kunne præsentere en samlet (skriftlig) overvejelse om sikkerheden i løsningen (risikovurdering). Der findes forskellige best practice-værktøjer, man kan læne sig op ad, og detaljegraden bør afhænge af, hvor forretningskritisk løsningen er og hvor følsomme oplysninger der behandles. Det kan f.eks. være "Security by design" og "Privacy by design", der begge bygger på at sikkerhed er tænkt ind i løsningen fra starten.

IT-leverandøren bør kunne forklare deres proces samt sikkerhedsmæssige overvejelser.

3. D. Det er vigtigt, at IT-leverandøren arbejder systematisk med afhjælpning af de sikkerhedsproblemer, der findes ved revisionsgennemgange, f.eks. ISAE3402 der vedrører generelle IT-kontroller i relation til IT-drift og hosting-aktiviteter. Ligeledes er det vigtigt, at IT-leverandøren jævnligt overvejer, hvordan sikkerheden i løsningen kan forbedres.

IT-leverandøren bør som minimum én gang årligt kunne fremsende opdateret dokumentation for sikkerheden. Det kan være i form af en årlige revisorerklæring eller gyldig certificering efter en af de nævnte standarder.

4. Hvad gør IT-leverandøren for at passe på persondata?

Det er vigtigt, at du ved, hvilke persondata leverandøren kan komme i kontakt med, da din virksomhed som regel altid vil være den dataansvarlige. Typen eller omfanget af persondata kan have betydning for, hvilke sikkerhedskrav din virksomhed skal stille.

Persondataforordningen opstiller en lang række krav til både virksomhedens egen og IT-leverandørens behandling af persondata, bl.a. krav til risikovurdering i forhold til data, passende sikkerhedsforanstaltninger samt indgåelse af databehandleraftale. En databehandleraftale er et juridisk dokument, der sørger for at IT-leverandøren ikke behandler persondata uden jeres instruks.

4. A. Hvis IT-leverandøren skal behandle persondata for virksomheden, er det vigtigt, at de lever op til de krav, der stilles i forhold til persondataforordningen (GDPR) og databeskyttelsesloven, når de skal fungere som databehandler for virksomheden. Vær opmærksom på at en behandling ikke alene er opbevaring, men også blot "se"-adgang.

4. B. Det er vigtigt at forhold relateret til persondataforordningen er på plads, før I begynder at bruge en ny IT-leverandør. IT-leverandøren skal kunne oplyse hvor og hvordan persondata lagres og hvorvidt de

benytter underleverandører til behandlingen. IT-leverandøren skal desuden kunne redegøre for proceduren for sletning af persondata.

IT-leverandøren skal som minimum sørge for at eventuelle underdatabehandlere er placeret indenfor EØS, et af EØS' liste over sikrelande eller er beskyttet af anden hjemmel. Udover dette skal de kunne redegøre for de præcise sletterutiner. Data skal slettes når behandlingen ikke længere har relevans.

4. C. IT-leverandøren bør kunne redegøre for, hvilke af deres medarbejdere der vil have adgang til løsningen, f.eks. i forbindelse med support, og om disse underskriver en fortrolighedserklæring. De bør ligeledes kunne redegøre for, hvordan de styrer og monitorerer adgang til løsningen, så kun relevante medarbejdere opnår adgang. IT-leverandøren bør som minimum sørge for, at alle der har adgang til persondata, er underlagt fortrolighed og der bør være restriktioner på, hvilke medarbejdere der har adgang til disse data.

4. D. Skulle der forekomme et brud på sikkerheden, der involverer persondata, skal dette anmeldes til Datatilsynet indenfor 72 timer efter opdagelse af bruddet. IT-leverandøren skal kunne redegøre for hvordan og hvor hurtigt din virksomhed bliver underrettet, hvis der sker et brud på sikkerheden, der omhandler persondata.

IT-leverandøren bør som minimum sørge for, at din virksomhed kan anmelde brud på sikkerheden indenfor 72 timer efter opdagelse af bruddet. De skal derfor give dig besked indenfor 48 timer og kunne bistå i anmeldelse af bruddet.

Persondataforordningen (GDPR) har en lang række specifikke krav og fortolkninger, for yderligere information, herunder eksempler på databehandleraftaler, henvises til Datatilsynet der i Danmark er ansvarlig for tilsyn og efterlevelse af persondataforordningen. For yderligere information om dette henvises til www.datatilsynet.dk.

5. Hvad er ansvarsfordeling mellem jer selv som kunde og IT-leverandøren

5. A. Ved on-premise løsninger er det i udgangspunktet din virksomhed, der er ansvarlig for alle forhold, dvs. både de fysiske og tekniske sikkerhedsforanstaltninger. Det betyder, at det blandt andet er jeres ansvar at sikre fysisk sikkerhed, vedligeholdelse og opdatering, ligesom I skal sørge for, at der bliver foretaget og testet backup. I vil evt. kunne lave en serviceaftale med jeres IT-leverandør.

IT-leverandøren skal kunne redegøre for ansvarsfordelingen, dvs. hvilke sikkerhedsforanstaltninger din virksomhed står for og hvilke de står for. De bør ligeledes kunne redegøre for, hvilke ydelser de kan tilbyde i forbindelse med dette.

5. B. Styring af brugerkonti kræver særlig opmærksomhed, da det ofte er nemt at glemme at nedlægge fratrådte brugere, brugere der bibeholder gamle rettigheder når de skifter job eller lignende.

IT-leverandør skal kunne redegøre for, hvilke dele af konfigurationen I selv er ansvarlige for i forbindelse med såvel implementeringen som driften af løsningen. Typisk vil din virksomhed have ansvaret for de data, der indlæses i løsningen, ligesom det er jeres ansvar at styre, hvilke af jeres brugere, der har adgang til løsningen.

5. C. Mange cloud-services indeholder ganske avancerede og veludviklede sikkerhedsfunktioner, men ofte er disse ikke slået til som standard. Derfor er det i dialogen med leverandøren vigtigt at undersøge, hvilke sikkerhedsfunktioner leverandøren tilbyder og sørge for at alle relevante funktioner bliver slået til.

Mange cloud-services giver mulighed for såkaldt to-faktor eller multi-faktor loginbeskyttelse, hvor brugerne i stedet for et simpelt password modtager eksempelvis en besked eller popup på deres mobiltelefon for at kunne logge ind i løsningen. Findes denne funktion i løsningen, er det vigtigt at den slås til og anvendes for alle brugere, da langt de fleste sikkerhedsbrud i cloud-services skyldes brud på login-sikkerheden.

Ved løsninger, der indeholder kritiske data, bør IT-leverandøren som minimum tilbyde muligheden for to-faktor eller multifaktor login-beskyttelse.