Vejledning til sikring af kundedata i forbindelse med installation af sikringsanlæg

SikkerhedsBranchen

Information Viden Kvalitet

Formål
Denne vejledning beskriver overordnet, hvordan man kan sikre sine kundedata i forbindelse med installation af alarmanlæg. Vejledningen uddyber kravene i kravspecifikationen til indbrudsalarmanlæg, afsnit 60.20, om grundlæggende krav til it-sikkerhed. Vejledningen er især rettet mod mindre installatører, som ikke har et egentligt ledelsessystem for it-sikkerhed.

Baggrund
I kravspecifikationen for indbrudsalarmanlæg og TVO-anlæg opstilles der krav til den grundlæggende it-sikkerhed beskrevet i kravspecifikationens pkt. 60.20.

God it-sikkerhed handler grundlæggende om at tilvejebringe tilgængelighed, fortrolighed og integritet samtidigt. Tilgængelighed vil sige, at data er tilgængelige (f.eks. at it-systemet ikke er gået ned) for dem, de er tiltænkt, på det tidspunkt, som det er hensigten, at de skal kunne tilgå data. Fortrolighed handler om, at uvedkommende (f.eks. hackere) ikke kan få adgang til data (og f.eks. bruge dem til kriminelle formål). Integritet handler om, at data er, som de giver sig ud for at være (og f.eks. ikke er blevet ændret som følge af fejl eller af hackere).

60.20 a) Klassifikation
Al information, som vedrører AIA-anlæg, skal klassificeres. Installatørerne skal vurdere, hvilken skade der kan ske, ved at informationerne kommer til uvedkommendes kendskab. Man kan basere sin klassifikation på nedenstående simple model:

a) Informationer, hvor offentliggørelse er naturlig og ikke forvolder skade (f.eks. tekniske opdateringer, manualer og installationsvejledninger, som alligevel er tilgængelige på producentens hjemmeside).
b) Informationer, som er interne hos installatørerne, og hvor offentliggørelsen kan forårsage mindre væsentlige problemer eller gener for driften (f.eks. beskrivelse af visse interne forretningsgange eller lister over kunder).
c) Informationer, som er fortrolige / hemmelige, og hvor offentliggørelse kan forårsage væsentlige problemer med konsekvenser for driften eller taktiske målsætninger (f.eks. informationer om sammenhæng mellem AIA-systemer og kunder samt generelle oplysninger om kundernes infrastruktur).
d) Informationer, som er følsomme / yderst hemmelige, og hvor offentliggørelse kan forårsage alvorlige problemer for driften eller strategiske målsætninger eller decideret sætter organisationens overlevelse på spil (f.eks. passwords og nøgler til installatørernes egne og kundernes systemer og AIA-anlæg).

Som anført ovenfor skal al information relateret til AIA-systemer, herunder også installatørernes egne forretningsgange samt oplysninger relateret til kunder til AIA-systemer, klassificeres.

60.20 b) Risikovurdering
Risiko kan måles ved at bedømme, hvor stor sandsynlighed der er for, at en trussel kan udnytte en sårbarhed og hvor stor konsekvens det kan have for installatørerne. For hver trussel skal installatørerne altså identificere sandsynligheden for, at der succesfuldt kan udnyttes en sårbarhed, og hvilke konsekvenser det vil have.

Menneskelige trusler kan komme fra interne medarbejdere eller fra personer udenfor virksomheden. Menneskelige trusler kan også være tilsigtede eller uheld. I denne hovedkategori finder vi f.eks. korrupte medarbejdere, medarbejdere som glemmer en bærbar PC, hackere, og oursourcingpartnere der laver en fejl. Systemmæssige trusler findes f.eks., når der er en indbygget logisk fejl i et program og truslerne udenfor virksomhedens kontrol er f.eks. optøjer eller skybrud, der oversvømmer serverrummet. Derudover findes der trusler udenfor virksomhedens kontrol.

Risikostyringsprocessen forløber som følger:

a) Installatørerne vurderer, hvilke forretningsprocesser og it-systemer risikovurderingen skal udføres på. Man kan passende bruge sin dataklassifikation, som jo gerne skulle have opregnet alle installatørernes aktiver relateret til AIA-systemer.
b) Derefter fastlægges konsekvenserne ved brud på tilgængelighed, fortrolighed og integritet. Konsekvenserne kan fastlægges i niveauer som stor, medium eller lille.
c) Dernæst vurderes sandsynligheden for, at en trussel erfaringsmæssigt optræder som en faktisk sikkerhedshændelse. Sandsynlighederne kan fastlægges i niveauer som ofte, indimellem og sjældent. Når man vurderer sandsynlighederne, skal man tage højde for de administrative og

tekniske sikkerhedstiltag, der allerede er implementeret, og som har medvirket til at reducere de erfaringsbaserede sandsynligheder.

d) En figur kan på denne bagrund opstilles:

Sandsynlighed/ Konsekvens	Sjældent	Indimellem	Ofte
Stor			
Medium			
Lav			

Det resultat man har opnået, skal gemmes som dokumentation. Den risiko, man står tilbage med, kaldes restrisikoen. Grøn farve er lav risiko, gul farve er mellem risiko og rød farve er høj risiko.

e) Sidste skridt er at udarbejde en risikohåndteringsplan, hvor man med udgangspunkt i ovenstående risikovurdering vurderer, om sikkerheden er på et acceptabelt niveau, eller om man skal iværksætte flere sikkerhedstiltag, for at reducere sandsynligheden for den enkelte trussel mod det enkelte aktiv. Dette vil bero på om det er økonomisk rentabelt. Man kan også overveje at ophøre med de risikobetonede aktiviteter, hvis det er muligt. Endelig kan man overveje, om man kan dele den resterede risiko med leverandører eller forsikre sig ud af det.

60.20 c) Nødvendige sikringsforanstaltninger

Det er vigtigt, at virksomheden kommer hele vejen rundt om sikkerheden og ikke risikerer at eksponere egne, kunders og leverandørers data for uvedkommende. Virksomheden bør derfor som minimum indføre følgende tiltag:

a) Awareness træning
- Medarbejdere skal have instruktion og oplæring i, hvad de må gøre med informationerne, og hvordan de skal beskyttes.

b) Adgangsstyring
- Der bør være en proces for at håndtere brugeroprettelse, -ændring og nedlægninger.
- Der bør være regler for styring af hvad man har adgang til og med hvilke rettigheder.
- Der bør være regler for sikkerheden og beskyttelsen af de anvendte adgangskoder.

c) Krypteringspolitik
- Bærbare enheder (PC'er, tablets, mobiltelefoner) og datamedier bør være krypterede, ligesom personoplysninger, der sendes eller indtastes over nettet.

d) Udstyr
- PC'er og andet dataudstyr bør som minimum være beskyttet med firewall og antivirus.
- Ved reparation, service eller bortskaffelse af udstyr med personoplysninger, skal de fornødne sikringsforanstaltninger være truffet.

e) Backup
- Der bør være en proces for backup af systemer og informationer, samt for kontrol og tests af disse backup.
- Backup af personoplysninger skal beskyttes på samme måde som de oprindelige data og krav til opbevaringsperioden skal være afklaret.

f) Logning og overvågning
- Adgang og forsøg på adgang til personoplysninger skal logges, og deres behandling skal dokumenteres.

g) Patchmanagement
- Det bør være en proces for at holde dataudstyr opdateret med sikkerheds- og andre patches.

h) Sikring af netværkstjenester
- Dataudstyr på ens netværk skal være beskyttet med/bag firewall og viruskontrol.

i) Netværkssegmentering
- Det interne netværk bør være opdelt i passende segmenter, med kontrol af trafikken imellem de enkelte segmenter.

j) Aftaler om informationsoverførsel
- Alle informationsoverførsler bør være baseret på aftaler, hvor sikkerhedskravene er afstemt med risici.

k) Håndtering af informationssikkerhedsbrud
- Det bør være beskrevet og kendt hvad man gør, hvis man oplever et brud på informationssikkerheden. Herunder hvad dette kunne være have af konsekvens.

l) Beskyttelse af personoplysninger
- Der bør være regler for håndtering af de mere procesmæssige krav til beskyttelse af personoplysninger.

SikkerhedsBranchen
Jernholmen 12
2650 Hvidovre

Telefon 36 49 40 80
info@sikkerhedsbranchen.dk

www.sikkerhedsbranchen.dk

Dubex:

Denne pjece er udarbejdet af Dubex.

Dubex er Danmarks førende, forretningsorienterede it-sikkerhedsspecialist. Vi leverer og supporterer sikkerhedsløsninger til over 500 lokationer globalt og har siden 1997 hjulpet private og offentlige virksomheder med at håndtere risici, imødekomme forandringer og understøtte en fleksibel vækst.

Vi er ISO 27001:2013-certificeret inden for informationssikkerhed og har fokus på end-to-end rådgivning omkring strategi, proces og teknologi, herunder også implementering og drift samt uddannelse af medarbejderne. Vi tilbyder bl.a. rådgivning om og løsninger inden for de nævnte områder i pjecen:

- Dataklassificering
- Risikovurderinger

Samt de andre sikkerhedsforanstaltninger der nævnes. Desuden yder vi konsulenthjælp inden for:

- Informationssikkerhed og databeskyttelse generelt
- EU-persondataforordningen
- Sikkerhedsanalyser
- Cloud-sårbarhedsanalyse
- Sikkerhedspolitikker med tilhørende retningslinjer
- Generel håndtering af brugere, deres roller og styring af adgange til systemer og programmer
- Dataflowanalyser
- Styring af sikkerhedshændelser og brud på sikkerheden
- Nødberedskabs- og reetableringsstyring
- Endpoint- og netværkssikkerhed
- Overvågning og analyse
- Awareness-uddannelse

I kan kontakte os på info@dubex.dk eller Tlf.: (+45) 3283 0430

Læs mere på dubex.dk og tilmeld dig vores nyhedsbrev.

SikkerhedsBranchen
Den danske brancheforening for sikkerhed og sikring