SikkerhedsBranchen
Information Viden Kvalitet

IT-sikkerhed i dit sikkerhedssystem

7 punkter du skal forholde dig til for at øge IT-sikkerheden i dit:

- **Indbrudsalarmsystem**
- **Adgangskontrolsystem**
- **TV-overvågningsanlæg**

Hvorfor skal du IT-sikre dit sikkerhedssystem?

Mange af de komponenter der i dag installeres i et sikkerhedssystem, er i virkeligheden selvstændige små computere, og er derfor sårbare overfor mange af de samme ting som de computere, du allerede bruger i din virksomhed. (Disse komponenter betegnes ofte som IoT-komponenter, hvor IoT står for Internet of Things).

Vi tænker ikke altid på dem som computere, og de sidder tit steder, hvor vi ikke lægger mærke til dem.
Da komponenterne ofte placeres på dit netværk, kan de udnyttes af hackere til at lave angreb på dit firmas IT-systemer, men også til at kompromittere dit sikkerhedssystem.

Hackerne udnytter bl.a. huller i IT-sikkerheden, og derfor er det vigtigt for dig, at du også forholder dig til IT-sikkerhed i dit indbrudsalarmsystem (AIA), dit adgangskontrolsystem (ADK) eller i dit TV-overvågningsanlæg (TVO).

Dette gælder ved nye installationer, men også løbende i eksisterende installationer, da hackerne hele tiden opdager nye svagheder, som de kan udnytte.

Sikkerhedssystemer vil som udgangspunkt lagre personfølsomme data og dette skal du være særligt opmærksom på, da du jf. artikel 24 i persondataforordningen, er forpligtet til at beskytte disse data. I vejledningen kan du under punkt. 2 og 5 læse mere om, hvordan du sikrer dig, at dette overholdes.

Kom godt fra start

Sikring af dit sikkerhedssystem, vil altid udspringe af en risikovurdering. Hvad vil konsekvenserne være, hvis der sker et brud? Hvordan kan sandsynligheden og/eller konsekvensen af denne hændelse imødegås? Disse spørgsmål bør du starte med at stille dig selv og din virksomhed.

Denne vejledning giver dig en kort introduktion til syv punkter, som du skal have fokus på, hvis du tænker på at få, eller allerede har, et sikkerhedssystem. Vejledningen skal ses som et supplement til de myndighedskrav og branchebestemte regelsæt, som allerede findes på sikringsområdet.

På bagsiden finder du en tjekliste, som kan hjælpe dig med at holde styr på, om du har husket det hele på alle syv punkter, ligesom den vil hjælpe dig til at stille de rigtige spørgsmål og krav til installatøren.

SikkerhedsBranchen
Information Viden Kvalitet

1. Komponenter

Først og fremmest bør du sørge for at have et samlet overblik over, hvad der findes i virksomheden af IoT-komponenter. Se evt. vejledningen fra sikkerdigital.dk.
Dernæst er det vigtigt kun at bruge komponenter, som du har tillid til, da konsekvensen kan være, at dit sikkerhedssystem eller dit administrative system bliver sat ud af drift, hvis du bliver hacket.

For at du kan have tillid til en komponent, er der en række krav, du som minimum skal sikre dig, er opfyldt:

- **i.** det skal være muligt at lægge et unikt password ind i hver komponent
- **ii.** alle komponenter skal kunne firmware- og software-opdateres manuelt eller automatisk
- **iii.** du skal kende alle komponenters forventede levetid i relation til firmware- og software-opdateringer (gammelt produkt – manglende komponenter)
- **iv.** produktet skal nulstilles/data skal slettes, når produktet skiftes ud

2. Passwords og rettigheder

For at man kan få adgang til den enkelte komponent, kræver det, at man har det rigtige password. Det gælder også for hackeren, og derfor er passwords et meget vigtigt led i din IT-sikkerhed.
Du sikrer desuden personfølsomme data i dit sikkerhedssystem ved at bruge passwords, men også ved at afgrænse adgangen til systemet med forudbestemte brugerrettigheder.

Du skal derfor kræve af installatøren:

- **v.** at du har adgang til alle de passwords, der benyttes i dit sikkerhedssystem
- **vi.** at der benyttes stærke og **unikke** passwords, gerne med to-faktor-validering, hvis det er muligt – se evt. SikkerhedsBranchens *Opbygning af passwords*, som findes i samme mappe som denne vejledning
- **vii.** at installatøren ændrer passwords i alle komponenter, så der ikke benyttes default passwords (forudindstillede kodeord)
- **viii.** at brugerrettighederne fastlægges for de enkelte personer, der omgås komponenterne – i hvilket omfang og med hvilket formål kan de få adgang til systemet

3. Opdatering af firmware og software

Hackere udnytter bl.a. huller i IT-sikkerheden, og de opdager hele tiden nye svagheder. Derfor er det vigtigt med løbende opdatering af firmware og software, fuldstændigt som på dine øvrige computere og din telefon.

Du skal derfor sikre dig:

- **ix.** at alle enheder er opdateret med den seneste firmware eller software, når installationen afsluttes
- **x.** at alle komponenter som har mulighed for en sikker automatisk opdatering, er sat til automatisk at opdatere
- **xi.** at du har en aftale med en certificeret installatør om minimum et årligt servicebesøg, hvor alle komponenter opdateres med den nyeste version af firmware og software

4. Firewall

Internettet og de øvrige komponenter på dit netværk udgør en risiko. Det er derfor vigtigt for sikkerheden på dit netværk og i dine computere, at der er helt styr på, hvem der må kommunikere til og fra internettet samt hvilke komponenter, der må transmittere til hinanden.

Du skal derfor sikre dig:

- **xii.** at din firewall er opsat således, at ingen komponenter inden for netværket utilsigtet kan åbnes mod internettet - al kommunikation skal være veldefineret og aftalt
- **xiii.** at der er gennemført en segmentering (opdeling) af komponenterne i dit sikkerhedssystem og komponenterne på dit øvrige netværk
- **xiv.** at ekstern adgang til dit netværk (f.eks. som installatør) sker via en sikker forbindelse, f.eks. en VPN – se evt. SikkerhedsBranchens *Opbygning af passwords*
- **xv.** at kommunikation på og fra dit netværk sker krypteret, så vidt det er muligt

5. Fysisk sikkerhed (adgangssikring)

Det er vigtigt at indtænke dit sikkerhedssystems fysiske placering, da du også skal beskytte dit system ved at sørge for, at der ikke er fysisk adgang til det for uvedkommende. Ved at adgangssikre dit sikkerhedssystem sikrer du samtidig de lagrede personfølsomme data.

Du skal derfor sikre dig:

- **xvi.** at dit system og dets komponenter er placeret et fysisk sted i virksomheden, hvortil der er sikret mod uvedkommende adgang, med fysisk og elektronisk sikring – se evt. F&P's *AIA-katalog* eller *Suppleringskataloget*
- **xvii.** at de fysiske adgangsrettigheder fastlægges for de enkelte personer der skal omgås komponenterne – i hvilket omfang og med hvilket formål kan de få adgang til området, hvor systemet er placeret

6. Service

Da nye svagheder og huller i IT-sikkerheden hele tiden opstår, er det vigtigt, at dit sikkerhedssystem altid er optimeret i forhold til de IT-mæssige sikkerhedskrav, og det bør derfor tilses jævnligt.

Du skal derfor sørge for:

- **xviii.** at lave en serviceaftale, hvor installatøren forpligtiger sig til at gennemføre mindst et årligt servicebesøg, der indbefatter opdatering af alle komponenter med den seneste firmware- og software-version, samt kontrol af firewallopsætningen

7. Valg af installatør

At overlade sikkerheden i sit firma til andre kan for nogle være lidt grænseoverskridende, og det er derfor vigtigt, at du finder den rigtige installatør til at håndtere dit sikkerhedssystem.

Ved at vælge en certificeret installatør indenfor TVO, AIA eller ADK, som er medlem af SikkerhedsBranchen, sikrer du dig følgende:

- At arbejdet udføres på baggrund af en risikovurdering
- At arbejdet udføres af uddannede og kvalificerede medarbejdere, og at du har mulighed for at få en installationserklæring efter endt installation
- At dine kundedata håndteres i overensstemmelse med persondataforordningen, og jf. pkt. 60 i kravspecifikationerne – læs evt. mere om datahåndtering her
- At installatøren tager højde for den fysiske sikkerhed
- At installatøren lever op til SikkerhedsBranchens etiske regler

Derudover skal du sikre dig, at installatøren er certificeret til det eller de sikringsområder, han/hun skal arbejde med.

Installationserklæringen er din dokumentation for omfanget af installationen over for bl.a. forsikringsselskaberne, hvilket kan have afgørende betydning på et kravanlæg, hvis det ikke er i orden. Du skal derfor **altid** forlange at få en installationserklæring, og den skal udfyldes af en certificeret installatør, hvis den skal være gældende.

Du kan finde din certificerede installatør hos SikkerhedsBranchen her.

Tjeklisten

Hvis du skal have et nyt sikkerhedssystem og dermed skal stille krav, eller hvis du ønsker at gennemgå dit eksisterende sikkerhedssystem, så er der på bagsiden en tjekliste som kan hjælpe dig med, hvad du skal huske.

Der er mulighed for at krydse af i takt med, at du som kunde stiller kravene, samt når installatøren har leveret det ønskede resultat.

SikkerhedsBranchen
Information Viden Kvalitet

Tjekliste	Som kunde skal du	Installatøren sikrer ved endt installation
Komponenter	☐ sikre dig, at installatøren kun benytter komponenter, som du kan have tillid til ☐ sikre dig, at det er muligt at indlægge et unikt password i alle komponenter ☐ sikre dig, at firmware og software som minimum manuelt kan opdateres i alle komponenter, og gerne automatisk ☐ sikre dig, at du kender alle komponenters forventede levetid, for firmware og softwareopdateringer ☐ sikre dig, at produktet nulstilles/data slettes, når produktet skiftes ud	☐ at der kun er brugt komponenter fra en producent, som installatøren har tillid til ☐ at alle komponenter kan beskyttes med unikke passwords ☐ at firmware og software i alle komponenter kan opdateres ☐ at der er udleveret dokumentation for forventet levetid, for firmware og software
Password	☐ have adgang til alle relevante passwords ☐ godkende styrken af benyttede passwords ☐ sikre dig at alle komponenter er opdateret med kundespecifikke passwords ved endt installation ☐ fastlægge brugerrettighederne til systemet	☐ at alle komponenter er opdateret med kundespecifikke passwords ☐ at alle relevante passwords er udleveret til kunden ☐ at alle passwords er unikke for kunden
Firmware og software	☐ sikre, at alle komponenter er opdateret med seneste relevante firmware og software, når installationen afsluttes	☐ at alle enheder er opdateret med den seneste relevante firmware og software ☐ at alle komponenter som kan opdatere automatisk, er sat til at opdatere automatisk ☐ at der er udleveret liste med seneste gældende firmware og software til kunden
Firewall	☐ sikre, at din firewall er opsat således, at ingen komponenter inden for netværket utilsigtet kan åbnes op mod internettet ☐ sikre at komponenterne i sikkerhedssystemet er adskilt fra øvrige komponenter på netværket ☐ sikre dokumentation for opsætning af firewall ☐ sikre at ekstern adgang til dit netværk sker via en VPN-forbindelse	☐ at kunden er rådgivet om, at alle komponenter og firewall er opsat, så der ikke foregår uautoriseret og utilsigtet kommunikation til og fra internettet ☐ at fuld dokumentation for netværksopsætningen af komponenter er udleveret til kunden ☐ at kunden er rådgivet om, at komponenterne i sikkerhedssystemet er adskilt fra øvrige komponenter på netværket ved segmentering ☐ at kunden er rådgivet om, at al ekstern adgang til dit netværk kun sker via en VPN-forbindelse
Fysisk sikkerhed	☐ sikre, at der er taget højde for den fysiske sikkerhed ved, at systemet er placeret et adgangssikret sted ☐ fastlægge de fysiske adgangsrettigheder til systemet	☐ at kunden er orienteret om de fysiske sikringstiltag som bør installeres for at sikre, en passende beskyttelse af hardware og data
Service-aftale	☐ sikre dig, at der tilbydes en serviceaftale, som bl.a. omfatter firmware- og software-opdatering af alle enheder til seneste version, min. en gang om året	☐ at serviceaftalen som omfatter firmware- og software-opdatering af alle enheder til seneste version og kontrol af firewall opsætning min. en gang om året, er tilbudt til kunden ☐ at al service udføres af kvalificeret personale
Installatør	☐ sikre dig, at installatøren er medlem af SikkerhedsBranchen og certificeret indenfor installation af: ☐ Automatisk indbrudsalarm (AIA) ☐ TV-overvågning (TVO) ☐ Elektronisk adgangskontrol (ADK)	☐ at være medlem af SikkerhedsBranchen og certificeret indenfor installation af: ☐ Automatisk indbrudsalarm (AIA) ☐ TV-overvågning (TVO) ☐ Elektronisk adgangskontrol (ADK) ☐ Certifikat-nr._____ ☐ at al installation og idriftsætning udføres af kvalificeret personale
Installations-erklæring	☐ kræve, at der afleveres en installationserklæring fra en godkendt installatør på: ☐ Automatisk indbrudsalarm (AIA) ☐ TV-overvågning (TVO) ☐ Elektronisk adgangskontrol (ADK)	☐ at der er udfyldt og afleveret en installationserklæring på: ☐ Automatisk indbrudsalarm (AIA) ☐ TV-overvågning (TVO) ☐ Elektronisk adgangskontrol (ADK)