Enter Security | Innovasjoner for en tryggere hverdag

NABONETTVERK SMART HOME

Retningslinjer for overvåkningskamera på Internett

Denne veiledningen bygger på informasjon fra NorSIS i samarbeid med Datatilsynet. Den gir råd til privatpersoner og virksomheter som ønsker å sikre overvåkningskameraene sine, samt å overholde generelle myndighetskrav. Årsaken til at mange kameraer havner ubeskyttet på Internett skyldes ofte manglende teknisk kompetanse hos de som konfigurerer kameraene samt manglende kunnskap om regelverket.

For privatpersoner:

1. **Plassering av kamera**
   Privatperson kan lovlig overvåke eget hus og hage, men vær klar over at kameraet ikke skal kunne fange opp deler av et offentlig område eller en annen persons eiendom. Du kan heller ikke overvåke andres private affære, slik som leieboere og deres besøkende. Dette gjelder også lydopptak.
2. **Gjør en risikovurdering**
   Er det nødvendig at kameraet skal være tilgjengelig på Internett?
3. **Bytt standardpassordet**
   Mange enheter kommer utstyrt med standard brukernavn og passord. Bytt disse.
4. **Sikkerhetsoppdatering**
   Hackere finner stadig sårbarheter i kameraene, det er derfor viktig at du regelmessig sjekker om det finnes sikkerhetsoppdateringer til kameraet ditt.
5. **Hjemmeruteren**
   Forstå konsekvensene av de endringer du gjør i hjemmeruteren for å få tilgang til kameraet fra Internett, feilkonfigurasjon kan føre til at også andre tjenester blir tilgjengelige for uvedkommende.

6. **Bruk sikker kommunikasjon**
   Når du logger deg på kameraet ditt, så husk å kun benytte sikre forbindelser/kryptering.
   Dette hindrer at brukernavn og passord kommer på avveie.
   Eksempel på sikker forbindelse er nettsider som starter med https:// og ikke http://

For virksomheter:

Kravene til informasjonssikkerhet i personopplysningsloven gjelder også for kameraovervåkingsanlegg.

Dagens overvåkningsanlegg er moderne informasjonssystem. Når disse knyttes til et nettverk må man være bevisst på sikringen av anlegget. Det må gjøres risikovurderinger og innføres sikkerhetstiltak. Sikkerhetstiltakene skal sikre at opptakene ikke kommer på avveier (konfidensialitet), at de ikke går tapt (tilgjengelighet), og at de er til å stole på – for eksempel hvor og når opptaket er gjort (integritet). Det er et krav at virksomheten følger de samme prinsippene for sikring av et kameraovervåkingsanlegg som for et hvilket som helst annet informasjonssystem hvor personopplysninger blir behandlet.

Hvordan sikre overvåkningsanlegget?

1. Overvåkningsanlegget skal sikres. Dette krever kunnskap, og dersom ikke virksomheten har det må den skaffe profesjonell hjelp.
2. Gjør en risikovurdering: Hva kan gå galt og hva er konsekvensen hvis det går galt?
3. Dersom løsningen skal gjøres tilgjengelig fra utsiden av virksomheten må man sørge for sterk autentisering. Dette kan gjørs som en del av andre fjerntilganger til virksomhetens systemer(hjemmekontorløsning), eller som en egen løsning for overvåkningsanlegget. Det kan for eksempel være tilgang fra kun én dedikert pc, bruk av kodebrikke, sikkerhetskode tilsendt på SMS eller lignende.
4. Sørg for at systemet logger bruken av anlegget. Brukerne bør få individuelle brukernavn og passord slik at det i ettertid er mulig å kontrollere hvem som har sett hva og når.
5. Sørg for at datatrafikken er kryptert.
6. Sørg for gode rutiner for bruk og kontroll av anlegget.
   Ikke stol på at en ekstern leverandør kjenner alle kravene i regelverket, men sjekk at disse punktene er fulgt opp. Det er virksomheten som har ansvaret for at regelverket følges.

Noen råd for de ansatte og (virksomheten):

- På en velfungerende arbeidsplass skal det være en dialog rundt eventuell bruk av kameraovervåking. Tar ikke arbeidsgiver initiativ bør de ansatte gjøre det.

- Gjensidig trygghet om hvordan overvåkningsanlegget brukes er viktig på en arbeidsplass. Når det åpnes for tilgang fra utsiden av virksomheten kan denne tryggheten undergraves. Diskuter derfor hvordan anlegget skal brukes – også hvor det brukes fra. Skal det åpnes for tilgang fra utsiden av virksomheten, eller skal tilgang kun skje i kontrollerte omgivelser og ved konkrete hendelser?
- Diskuter hvordan sikkerheten skal ivaretas. Etter personopplysningsloven har du som arbeidstager rett på innsyn i overordnet informasjon om hvordan løsningen er sikret. Spør om hva som skal til for å få tilgang fra utsiden – og forvent et svar som sier noe mer enn bare passord.
- Spør om bruken av overvåkningsanlegget logges.
- Tillit er viktig på arbeidsplassen. En avtale om at tillitsvalgte regelmessig får se loggen kan være en god løsning her.

Hvis du er i tvil om du har gjort dette riktig, be profesjonelle om hjelp!

Les mer om kameraovervåking hos Datatilsynet.

«Merk: Informasjon fra Enter Security er hentet fra flere kilder. Enter Security vurderer informasjon før publisering, men Enter Security kan ikke holdes ansvarlig for skade eller tap som kan oppstå som følge av ukorrekt, manglende eller utilstrekkelig informasjon»

2017