Sikkert hjemmekontor

TIPS OG TRIKS

FOR VIRKSOMHETER

Lag interne regler og prosedyrer (test på forhånd hvis mulig)

Lag klare regler for hjemmekontor, inkludert retningslinjer for tilgang til virksomhetens systemer og hvem som skal kontaktes hvis det oppstår problemer. Lag klare rutiner for sikkerhetshendelser. Innfør ekstra sikringstiltak for dokumentasjon som mellomledere og ledere skal lese, signere, godkjenne eller gi tilbakemeldinger på.

Sikre hjemmekontorutstyret

Innfør sikringstiltak som harddiskkryptering, utlogging etter en viss tid uten aktivitet, innsynsbeskyttelse på skjermen, sterk autentisering og sikring og kryptering av flyttbare medier (f.eks. minnepinner). Få på plass mekanismer for å låse stjålne eller tapte enheter.

Sikker fjerntilgang

Tillat kun tilkobling til virksomhetens nettverk gjennom virksomhetens VPN og flerfaktorautentisering. Sørg for at hjemmekontorinnlogginger automatisk kobles fra slik at man må logge inn igjen etter en viss tid uten aktivitet.

Sørg for at enhetenes operativsystemer og apper er oppdaterte

Dette vil gjøre det vanskeligere for kriminelle å utnytte gamle sikkerhetshull.

Sikre virksomhetens kommunikasjon

Krev flerfaktorautentisering for tilgang til virksomhetens e-postkontoer. Sørg for at de ansatte har tilgang til sikre kommunikasjonskanaler seg imellom, og til eksterne.

Styrk sikkerhetsovervåkingen din

Sjekk aktivt om det foregår uvanlig fjernbrukeraktivitet og skjerp årvåkenheten for VPN-relaterte angrep.

Styrk de ansattes forståelse av risikoen ved hjemmekontor

Gi de ansatte opplæring i virksomhetens regler for hjemmekontor. Brukt tid på å gjøre folk bevisste på digitale trusler, spesielt phishing og sosial manipulasjon.

Hold jevnlig kontakt med de ansatte

Avtal realistiske mål, arbeidstider og oppfølgingsmekanismer, vær fleksibel om mulig og ta hensyn til personlige omstendigheter.

EUROPOL | EC3 European Cybercrime Centre | POLITIET