Appendiks 9. Sikkert arbejde på distancen

Den øgede brug af ”fjernarbejde” eller ”distancearbejde” efter COVID-19 er for mange virksomheder kommet for at blive. Det har påvirket trusselsbilledet ift. hvilke angrebsmetoder, hackerne vælger. Følgende handlinger kan bl.a. mitigere disse trusler:

- **MFA**. Implementering af multifaktor-autentifikation (MFA) på samtlige VPN forbindelser til at øge den generelle sikkerhed. Hvis MFA ikke kan anvendes, kan der bruges længere og mere komplekse adgangskoder.
- **Opdatering**. Opdatering af VPN, netværksinfrastrukturenheder og enheder for at opnå fjernadgang til organisationens miljø med de seneste softwareopdateringer og sikkerhedskonfigurationer.
- **Adgange**. Monitering af privilegerede adgange ved optimering af adfærdsanalytiske værktøjer for at identificere mistænksomme aktiviteter.
- **Filtrering**. Web og e-mailbeskyttelse ved implementering af web-filtrering. Således blokeres ondsindede hjemmesider. E-mailfiltreringen kan implementeres og anvendes til at blokere spam og phishing e-mails.
- **Overvågning**. Øge monitoreringskapaciteten og identificeringen af potentielle malware eller kampagner, f.eks. via blacklisting eller markering af udefrakommende e-mails. Øge organisationens end point-monitorering.
- **Offentlig WiFi**. Instruere medarbejderne i at bruge (hvis muligt) internetdeling via mobiltelefon fremfor åbne offentlige netværk, der som udgangspunkt anses for usikre. Se f.eks. vejledningen ”God kultur ved distancearbejde udgivet af Center for Cybersikkerhed i samarbejde med Digitaliseringsstyrelsen.
- **Virtuelle platforme**. Virtuelle platforme, såsom Microsoft Teams, Skype eller Cisco Webex, har sikkerhedsmæssige problemstillinger, som særligt risiko-ledelsen og it-ledelsen bør forholde sig til. Se f.eks. vejledningen ”Råd om sikkerhed på virtuelle mødeplatforme” udgivet af Center for Cybersikkerhed i samarbejde med Digitaliseringsstyrelsen.
- **Sikkerhedspolitikker**. Genbesøge sikkerhedspolitikker og retningslinjer. Dels for at sikre, at de faktisk understøtter denne måde at arbejde på og dels for at sikre, at organisationen får adresseret de særlige risici, der kan være forbundet med distancearbejde. Se også vejledningen: "Beskyt organisationen: Opdater sikkerhedspolitikkerne til en »ny normal«" udgivet af Center for Cybersikkerhed i samarbejde med Digitaliseringsstyrelsen.