Modtag kun data gennem lægesystemet

> Stik aldrig USB-nøgler eller andet fremmed udstyr i arbejdscomputeren

Der er mange måder, hvorpå IT-kriminelle kan få adgang til systemer med personfølsomme data. En måde er ved at placere skadelige programmer på USB-nøgler eller andet eksternt udstyr og placere det steder, hvor relevante personer vil finde udstyret og efterfølgende anvende det. IT-kriminelle placerer eksempelvis USB-nøgler på strategiske steder som eksempelvis klinikkens parkeringsplads, indgangsparti eller på en stol i receptionen, så medarbejdere nemt finder dem og potentielt tager dem i brug på en arbejdscomputer. Den IT-kriminelle kan også være en patient, der selv stikker en USB-nøgle ind i en forladt arbejdscomputer. Uanset hvem der benytter et ukendt, eksternt udstyr, kan skadelige programmer blive installeret, så snart udstyret anvendes, og klinikkens interne netværk kan angribes.

Hvis du står i den uheldige situation, at en IT-kriminel lykkes med at installere skadelige programmer, kan vedkommende få adgang til følgende data:

- Helbredsoplysninger for alle klinikkens patienter
- CPR-numre
- Personaleinformation
- Adresse- og telefonlister over medarbejdere og redaktionelle kilder
- Brugernavne og passwords til arbejdscomputere, mailsystemer og interne programmer
- Betalingskortoplysninger
- Regnskabs- og økonomidata

Som klinikansvarlig læge og dataansvarlig er du pålagt at have passende organisatoriske og tekniske sikkerhedsforanstaltninger på plads, så du varetager ovenstående oplysninger i overensstemmelse med persondataforordningen. Det kan have store konsekvenser for både patienter og lægepraksis, hvis der sker læk af personfølsomme data.

Tre gode råd

- Sørg for aldrig at koble patienters, gæsters eller dit private udstyr på klinikkens kablede netværk, da det potentielt kan give IT-kriminelle adgang til klinikkens interne netværk. Det gælder også, selvom en ukendt person påstår at være fra IT-support.

- Vær opmærksom på, hvem der besøger klinikken og bruger ukendt elektronik i klinikken – og ring altid til en IT-rådgiver, hvis du er i tvivl.

- Sæt password på din arbejdscomputer og alle dine mobile enheder, og slå det til, hver gang du forlader rummet. På den måde kan uvedkommende personer ikke foretage uønskede handlinger på din computer, når du eller dine kollegaer ikke er i nærheden.