Artikel

Er hospitaler et mål for cyber-kriminelle?

> Det er et fælles ansvar at sørge for sikkerhed, men der er ikke fokus nok på sikkerhed, og der bliver ikke stillet høje nok krav til det.
>
> Sune Mark Henriksen, Adm. direktør, Sectra Danmark

For to år siden lammede WannaCry IT-systemer på en række engelske hospitaler i flere dage. Det samme kan ske i dag, hvis der ikke stilles krav til sikkerheden.

”Mit ønske er, at der er mange flere der spørger om IT-sikkerheden i deres systemer. Alle er ofte fokuserede på pris og effektivitet, som også er fornuftige områder. Men man bør spørge sig selv, hvad koster det, når et hospital ikke kan anvende deres IT-system?,” siger Sune Mark Henriksen.

Sune er administrerende direktør i Sectra Danmark. Sectra er den største udbyder af Enterprise Imaging Software i Skandinavien. Sune husker tydeligt den 12. maj 2017, da WannaCry ramte England.

Sådan ser et angreb ud

”Hello, Sune speaking”. Sune Mark Henriksen forventede ingen opkald. Han var på landevejen med sin familie, og havde fri fra arbejdet. Pludselig ringede ledelsen til hans mobiltelefon. Han blev hurtigt briefet om situationen: Flere hospitaler i England var inficeret af ransomware, og man var usikker på, om deres egne systemer var impliceret.

Sune fik hurtigt kontaktet sit team i Danmark. De fleste havde fri, men nu skulle beredskabet aktiveres. Sune ringede og forklarede situationen. ”Vi ved det godt, vi er i gang,” var svaret i den anden ende. Over den hektiske weekend hjalp Sectras team med at opdatere og sikre over 4.000 servere på hospitalerne. Ingen af deres egne systemer var inficerede, men de hjalp hvor de kunne.

SECTRA

Knowledge and passion

Ekspertisen gør forskellen

Selv om Sectra primært er kendt for deres billedhåndteringssystemer til sundhedssektoren, så er de også NATO -og EU kryptocertificerede inden for IT-sikkerhed. Sectra udvikler sikker kommunikationssoftware til militæret og sikrer også infrastruktur for energiforsyninger.

”Hos Sectra har vi arbejdet med IT-sikkerhed i 25 år. Vores erfaring med sikkerhed er med i tankerne når vi udvikler software til hospitaler og sundhedsmarkedet. Så det var kun naturligt, at vi kunne og ville hjælpe, når behovet opstod.”

Sikkerheden skal passe med behovet

I takt med, at hospitalerne får mere billedmateriale og databehandling udover deres eget IT-netværk, opstår en ny form for sikkerhedstrussel, hvor et ransomwareangreb kan være altødelæggende. Et ransomwareangreb er et indbrud i systemet, hvor cyberkriminelle låser data eller manipulerer med data, så det ikke kan anvendes, før man betaler en løsesum.
”Det kan være meget ødelæggende og det handler jo om patientsikkerhed. I yderste konsekvens kan det være livsfarligt,” siger Sune og fortsætter: ”Ingen systemer er 100% sikre, men niveauet af sikkerhed skal stemme overens med ens behov, og vigtigheden af de opgaver, som man løser.”

Efterspørg mere sikkerhed

Indkøberne af nye systemer har ikke nødvendigvis kompetencerne til at skille de sikre systemer fra de usikre systemer, når der skal købes nyt. Det kræver nogle kompetencer, som der er meget få af i sundhedsvæsenet.

Men ifølge Sune er der heller ikke nok interesse for det: ”Det er jo et fælles ansvar at sørge for sikkerhed, men der er ikke fokus nok på sikkerhed, og der bliver ikke stillet høje nok krav til det. Mange efterspørger blot effektive patologi- eller radiologisystemer til en god pris.”

Lige så vigtigt som økonomi

I IT-branchen forudser man, at vi indenfor de næste tre til fem år vil se det første store IT-sikkerhedsbrud i sundhedssektoren. Og i den sammenhæng var WannaCry kun et mindre brud.

Truslen kræver, at regionerne arbejder med sikkerhed, på samme måde, som man arbejder med økonomi og effektivitet. ”De skal ønske mere information og stille højere krav til samarbejdet. Leverandøren af software har ansvaret for produktet, men regionerne skal lære at spørge ind til det,” siger Sune. Man kan for eksempel spørge, hvordan sikkerheden er i forhold til andre udbydere på markedet og hvordan organisationen arbejder med sikkerhed.

Hvad er oppetid værd?

Sikkerhed koster ikke nødvendigvis mere, men for Sune er det oplagt at prioritere i fremtiden: ”Hvis et hospital ikke kan anvende deres kritiske IT-systemer, så må de sende patienter hjem, aflyse operationer og ventelisten stiger voldsomt. Hospitalerne er jo højproduktionsvirksomheder i dag, og mængden af data og opgaver vokser.”
Regionerne konsoliderer og indkøber regionale systemer. Dette udgør en ekstra risiko fra et sikkerhedsmæssigt perspektiv, da det i fremtiden gælder en hel regions hospitaler, hvis et IT-system bliver ramt.

Alle ved, at virus og hackere eksisterer. Men det er de færreste, der har været ramt af det. England blev ramt i 2017. Og nu her i 2019 blev skaderne ved WannaCry opgjort til knap 100 millioner pund.

Hvad var konsekvenserne af WannaCry i England?

- Over 70.000 computere og andet hardware blev påvirket.
- Cirka 19.000 patientaftaler skulle efterfølgende annulleres.

Omkostningerne er i dag opgjort til £ 92 millioner.

Kilde: Forbes

SECTRA

Knowledge and passion