Sikkerhetsovervåking på SNOW boksen med ThreatDown

Nasjonal sikkerhetsmyndighet (NSM) anbefaler å benytte sikkerhetsovervåkning. Snow teamet har tidligere benyttet internt utviklede verktøy for å ivareta sikkerhetsovervåkning på Snow boksen. For å styrke vår evne til å oppdage og avverge forsøk på data-innbrudd på Snow boksen, har vi anskaffet og installert et profesjonelt verktøy på Snow boksene. Produktet heter ThreatDown og benytter programvare fra Malwarebytes til å overvåke prosesseringen på Snow boksen. Løsningen motvirker at Snow boksen brukes som springbrett til å nå fastlegenes arbeidsstasjoner og legekontorets EPJ server.

ThreatDown produktet overvåker all prosessering som foregår på Snow boksen og sender noe overvåkningsdata til en portal installert på en server i skyen som Snow teamet kontrollerer. Produktet sender kun metadata til portalen, ingen informasjon om innholdet i dataene som er lagret på Snow boksen. ThreatDown har ikke mulighet til å logge seg på Snow boksen eller datamaskinen og gjennomgå innholdet på disse maskinene. Andre produkter vi har vurdert har denne muligheten. Det er derfor ikke fare for at pasientinformasjon eller informasjon om de ansatte på legekontoret overføres fra Snow boksen til portalen eller andre steder.
Mer informasjon om hvordan ThreatDown (Malwarebytes) bruker informasjonen de laster ned fra Snow boksen finnes her: https://www.malwarebytes.com/legal/privacy-policy

Legekontorene kan nå være enda sikrere på at det ikke innebærer stor risiko å være med i PraksisNett. Det er heller motsatt, om andre maskiner på et legekontor blir hacket og hackerne forsøker å spre seg videre til Snow boksen, så har vi en mulighet til å oppdage dette og kan varsle legekontoret.

Dersom du har spørsmål i forbindelse med dette produktet, er det bare å ta kontakt med oss på email adressen: snow.support@ehealthresearch.no.