INTERNET OF THINGS

Datasikkerhed:
Er du klar, når din virksomhed bliver angrebet?

Spørgsmålet i dag er ikke, om din virksomheds data bliver angrebet. Spørgsmålet, som alle virksomheder i dag bør stille sig selv, er; hvad skal vi gøre, NÅR vores data bliver angrebet? Vi har taget en snak med eksperter på området.

Flere og flere virksomheder tager skridtet ind i industriens 4. tidsalder, Industri 4.0, hvor maskinerne er koblet på internettet og udveksler data både med hinanden og med mennesker.

For større virksomheder sker udviklingen ofte som en del af en større strategi. Og for mindre virksomheder kommer Internet of Things gerne snigende ind i takt med, at udstyret bliver udskiftet.

Fordelene er åbenlyse. Med den store dataudveksling kan produktionen toptunes. Men uanset om man er en stor eller lille virksomhed, er der også en kæmpestor udfordring, som skal tages meget alvorligt, når man begynder at arbejde med store mængder data: Datasikkerhed.

Der er spørgsmål, man skal forholde sig til i forhold til datasikkerhed fx, hvad sker der, og hvordan kan jeg sikre mig, at mine data ikke bliver delt af andre? Skal vi benytte en cloud-løsning eller fysisk datalagring på egen lokation? Skal vi have en data-backup-løsning (redundans)? Og i så fald hvilken? Eller noget helt fjerde? Det kan være en svær beslutning især for mindre virksomheder.

Vi har bedt eksperter give deres bud på, hvordan datasikkerheden er ude i de danske industrivirksomheder, og på hvor virksomhederne bør optimere, hvis det ikke allerede er sket.

Datasikkerhedspolitik er første skridt

Så hvor skal man starte for at få skabt en sund datasikkerhed? Med en veldefineret sikkerhedspolitik, mener eksperterne.

Steen Broberg Jensen, Teknisk Supporter i Solars Cisco team:
Det handler om at have en politik for datasikkerhed, hvor man har taget højde for, hvad man gør før, under og efter et angreb eller nedbrud.

Sikkerhedspolitik (før, under og efter et brud på datasikkerheden).

Jan Minche, Security lead hos Cisco, opfordrer virksomheder, der starter helt fra bunden med datasikkerhed til at kigge på institut for informationssikkerhed SANS Institute. Her kan man finde hjælp til at få lagt rammerne for sin datasikkerhed. Det er et fornuftigt sted at starte, og det foregår i et sprog, som man kan forstå, også selv om man ikke er sikkerhedskonsulent.

Jan Minche påpeger også, at man skal finde ud af, hvilket sikkerhedsniveau man ønsker at efterleve. Der kan være nogle branchespecifikke offentlige reguleringer fx i forhold til vand- og spildevandsbranchen. I maj 2018 træder også den nye persondataforordning i kraft. Det betyder, at alle virksomheder, der forvalter persondata, kan risikere enorme bøder i en størrelsesorden, vi slet ikke er vant til her i Danmark.

Største datasikkerhedstrusler for virksomheder i dag

Morten Kromann, der er Product Chef Communications hos Siemens, er ikke i tvivl – det største datasikkerhedsproblem for de fleste danske virksomheder i dag er noget så simpelt, som at de ikke holder sikkerheden opdateret.

- Du kan købe det dyreste og bedste system, men hvis du ikke opdaterer dine systemer kan der efter ganske få dage opstå kritiske sikkerhedshuller. Når der opdages en fejl, rundsendes security releases til virksomhederne, hvor de kan finde firmware der retter fejlene. Det er meget vigtigt, at man holder sig opdateret her. Og det er der ikke mange slutbrugere, der gør, er min erfaring, siger Morten Kromann.

Security lead hos Cisco, Jan Minche, er enig og har desuden bemærket en anden årsag til, at datasikkerheden ikke altid er i top.

- Den organisatoriske siloopdeling. Ofte er der en produktchef, en IT-chef og en sikkerhedschef. De får ikke helt snakket sammen og suboptimerer i stedet hver deres område. Men sikkerhed går jo på tværs af hele organisationen. Hvis der er to sikkerhedsløsninger, der ikke kan tale sammen, så kan den ene ikke advare den anden, hvis der opdages en trussel i systemet.

- Det er ikke bare nødvendigt at kigge på trusler udefra. Det er lige så vigtigt at have en klar sikkerhedspolitik for medarbejdere og eventuelle eksterne. Der skal opstilles sikkerhedspolitik, hvor man fx får styr på sine sikkerhedsniveauer. En god måde at beskrive niveauerne på, er ved at bruge en fysisk dør som eksempel. Hvis du vil have sikkerhedsniveau 1, skal du have lås på døren. Vil du have sikkerhedsniveau 2, skal du have adgangskort. Niveau 3 kræver både adgangskort og en sluse, så du ikke lukker en person ind, som ikke har adgangskort. Og vil du have sikkerhedsniveau 4, skal du yderligere tilføje scanner eller videoovervågning, forklarer Morten Kromann fra Siemens.

En af de løsninger, der ligger lige for, er fx password for interne medarbejdere og politikker for, hvordan eksterne konsulenter tilgår virksomhedens netværk eller anvender virksomhedens computere, siger Steen Broberg Jensen.

Morten Kromann er enig: Passwords er en af de virkelig lavt hængende frugter. Brug altid passwords. Alle PLC og Switch understøtter password. Men ofte har man ikke den funktion slået til. Det er supernemt at gøre og giver virkelig meget ekstra sikkerhed, siger han.

Er det nok at dele netværket op?

Det er forskelligt, hvilke sikkerhedsforanstaltninger virksomhederne foretrækker. Det er erfaringen hos Jesper Amsinck, som er salgschef hos Solar Industri.

- Når vi snakker datasikkerhed i industrien, er best practise at dele netværket op i et industrinetværk og et administrativt netværk, men dette er ikke helt nok i en moderne produktionsvirksomhed; sikringer som DeMilitarisedZone (DMZ), firewall, sikkerhedsovervågningssystemer, sikker fjernadgang til maskiner/områder for at forbedre service, supportmuligheder, og også beskyttelse mod ubudne gæster er emner, der skal prioriteres, siger Jesper Amsinck, salgschef hos Solar Industri.

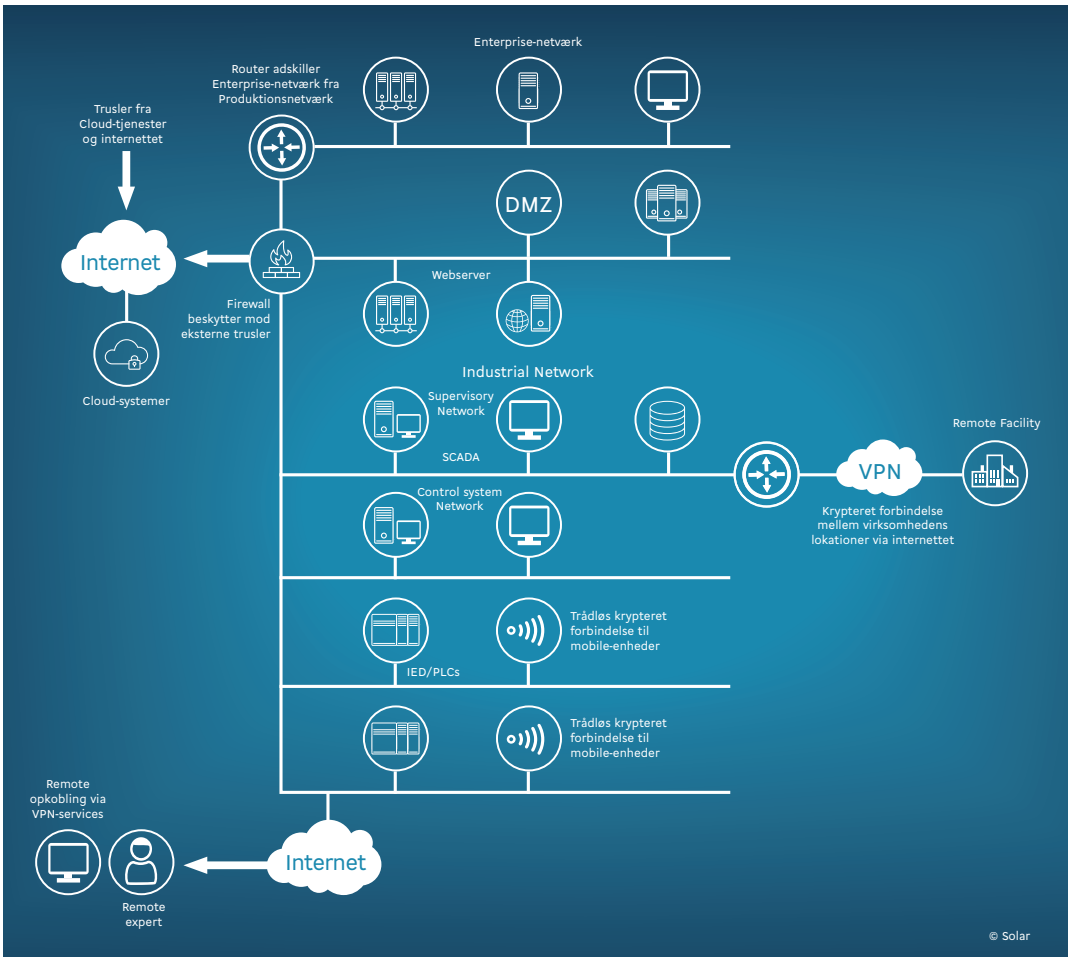
Samtidig med al sikkerheden, er der også krav om bedre performance, logning af data og adgang til hele produktionen fra et sted.

- Nogle virksomheder vil gerne have data gemt i en cloud, andre ønsker en On-Premises-løsning, hvor hardware er låst inde, så ingen kan stjæle ens data. Og hvor man så selv har styr på datasikkerheden. Ulempen ved en cloud-løsning er risikoen for at miste forbindelsen ud af huset. Nogle laver så en spejling af deres datalager ud i en cloud om natten.

Steen Broberg Jensen, Teknisk Supporter i Solars Cisco team

Jesper Amsinck, salgschef hos Solar Industri

Hos Solar har vi fx to identiske datacentre, hvor alle data er spejlet. Servere, storage og andre hardwaresystemer er redundante, og de to datacentre er placeret på to forskellige, fysiske lokationer, siger Jesper Amsinck.



Her skal du have styr på datasikkerheden.

- Oppetiden i netværksinfrastrukturen er i dag essentiel for alle virksomheders effektivitet. Sikkerhedsbrister kan derfor få store økonomiske konsekvenser, hvis man ikke er effektivt beskyttet med en klar og veldefineret datasikkerhedspolitik, slutter Steen Broberg Jensen fra Solar.

Hvad er Industri 4.0?

Begrebet Industri 4.0 bruges om den 4. industrielle bevægelse, som vi befinder os i netop nu. Før Industri 4.0 havde vi først mekaniseringen, så masseproduktionen og derefter computerautomatiseringen. Under Industri 4.0 bliver maskiner koblet på internettet og kan både udveksle data med hinanden og med mennesker. Derfor bruges også begrebet Internet of Things – tingenes internet. Med Internet of Things har maskiner mulighed for at give besked, når de har brug for service eller skal repareres, og de kan sende status på deres løbende produktion. På den måde kan produktionen hele tiden optimeres.

Kom i gang: Få rådgivning om datasikkerhed ved Internet of Things

Kontakt din Solar kontaktperson, og få styr på datasikkerhed ved implementering af Internet of Things.