THALES
Building a future we can all trust

Thales er ekspert i datasikkerhed. Du kan finde meget mere information om vores sikkerhedsløsninger til virksomheder og organisationer her: **www.thalesgroup.com**

Kryptering er det bedste sikkerhedsredskab i virksomhedens værktøjskasse

Erhvervsledere frygter organiseret cyberkriminalitet

D-mærket skal øge fokus på IT-sikkerhed

Er din data sikker?

Er din virksomheds data sikre, ved du, hvor de befinder sig, overholder du lovgivningen? Læs mere her og få gode råd om datasikkerhed.

Kryptering er det bedste sikkerhedsredskab i virksomhedens værktøjskasse

Af Henrik Malmgreen

Ifølge 2022 Thales Data Threat Report mener 66 pct. af virksomheder og organisationer, at deres digitale transformationsinitiativer er meget eller ekstremt sikre - f.eks. hvis data er flyttet fra on-premise til skyen. Ikke desto mindre har mindre end 30 pct. af selv samme virksomheder og organisationer på egen hånd taget ansvar for at kryptere data i de nye miljøer.

Det er tankevækkende ud fra især tre perspektiver. For det første vokser mængden af data eksplosivt, for det andet benytter mere end 90 pct. af alle virksomheder i en eller anden udstrækning cloudbaserede løsninger, og for det tredje udviser antallet af datalæk samme eksponentielle vækstkurve som mængden af data. Det betyder, at risikoen for, at virksomhedens data kompromitteres, dag for dag øges.

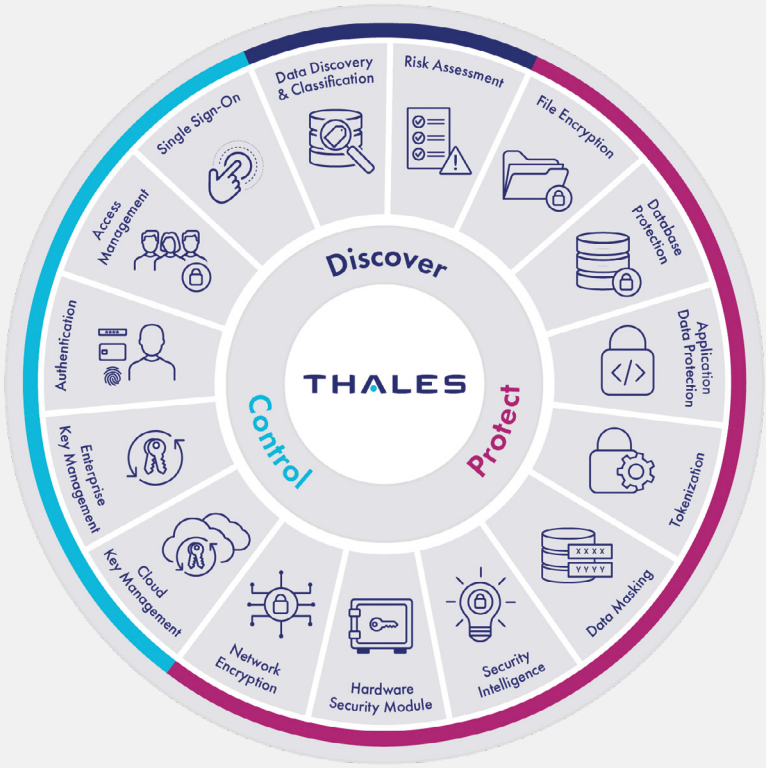
Sætter datasikkerheden på spil

Undersøgelsen viser samtidig, at mange virksomheder og organisationer godt ved, at kryptering er det mest effektive værktøj til at beskytte data i skyen, men springet til rent faktisk at få det gjort er åbenbart stort. Desværre vælger mange virksomheder at acceptere risikoen i forhold til datasikkerheden, især måske fordi mange virksomheder ikke har det fulde overblik over, hvor data rent faktisk befinder sig, om de er beskyttet godt nok, og hvem der har adgang til dem.

Det er essentielle problemstillinger for enhver virksomhed, og problematikken gælder ikke kun virksomhedens forretningskritiske data, men også kundedata samt andre former for data med personrelaterede oplysninger. ▶

"Databeskyttelse er essentiel, og i den sammenhæng er kryptering afgørende. Men virksomheden skal sørge for selv at have kontrol med krypteringsnøglerne"

Kenneth Fenger Jeppesen
Ansvarlig for Thales, Data protection, CPL i Danmark



▲ At etablere og vedligeholde et optimalt sikkerhedsberedskab i en virksomhed eller organisation kan i dag være en ganske kompleks affære. Thales kan hjælpe med alle aspekter heraf i en professionel og skræddersyet løsning.

▶ Verden over findes der i omegnen af 1.800 forskellige regulatoriske dataforordninger, og ifølge analysefirmaet Gartner vil halvdelen af jordens befolkning i løbet af 2022 være omfattet af General Protection Regulation (GDPR).

Kritisk hvis overblikket ryger

"I dag er enhver virksomheds eksistensgrundlag datadrevet, og data har en ekstrem høj værdi. Derfor skal du som virksomhedsleder selv tage ansvaret for, at dine data er sikre og at virksomheden overholder lovgivningen. Det vil sige, at de er krypteret således, at de er ulæselige, for 3. part, hvis uheldet skulle være ude". Det siger Kenneth Fenger Jeppesen, der ansvarlig for Thales Data Protection, CPL i Danmark.

I en tid, hvor flere og flere data flytter op i skyen i cloudbaserede løsninger, og hvor virksomhederne arbejder på flere platforme - de såkaldte multicloud løsninger - er han godt klar over, at en virksomhed kan miste overblikket. Det er en vanskelig opgave at håndtere, men den er bestemt ikke uløselig, og Thales tilbyder skalérbare løsninger til såvel store som mellemstore og små virksomheder.

Hånd i hanke med krypteringen

Cloud er med til at demokratisere adgangen til innovative teknologiløsninger, fordi der er tale om skalerbare løsninger, som kan tilpasses såvel det store som det lille behov. Men cloud er ikke en standard, hvilket betyder, at sikkerhedsniveauet kan variere fra udbyder til udbyder. Desuden er der risiko for, at virksomheden - hvis ikke den tænker sig om - kan risikere at komme til at stå i en meget ubehagelig situation.

"Hvis man f.eks. vælger en udbyder, som både varetager kryptering af data og håndterer krypteringsnøglerne, har virksomheden i virkeligheden mistet kontrol over sine data. Derfor skal virksomheden altid sørge for selv at have kontrol over sine krypteringsnøgler og ikke stole på en cloududbyder. Tillid er godt, men kontrol er bedre. Det er blandt andet noget, vi kan hjælpe med," siger Kenneth Fenger Jeppesen videre. ■

2022 Thales Data Threat Report

- Kun 56 pct. af respondenterne er helt sikre på at have det fulde overblik over, hvor virksomhedens data befinder sig.
- Kun 25 pct. af respondenterne mener at kunne klassificere alle data, og kun 53 pct. mener at kunne klassificere mindst halvdelen af alle data.
- 52 pct. af respondenterne fortæller, at virksomheden tidligere har oplevet en sikkerhedsbrist, og 18 pct. har oplevet det inden for de seneste 12 måneder.
- 56 pct. af respondenterne identificerer malware som den største sikkerhedsrisiko. Dernæst følger phishing med 40 pct. og Denial of Service med 37 pct.
- 21 pct. af respondenterne oplyser, at de har oplevet et ransomware angreb. Ud af disse oplyser 43 pct., at det har haft alvorlige konsekvenser for virksomheden.
- 59 pct. af respondenterne er overbevist om, at kryptering er det mest effektive værktøj til at beskytte data i skyen - men kun halvdelen af disse oplyser, at 40 pct. eller mere af deres data rent faktisk ér krypteret.

Erhvervsledere frygter **organiseret cyberkriminalitet**

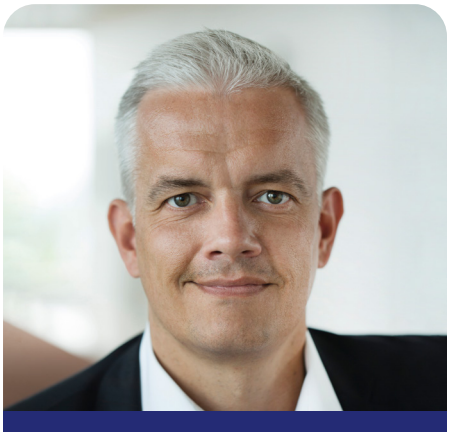
"I virkeligheden er det en klassisk problemstilling. Mange virksomheder har ikke overblik over, hvad de har af data, hvor de har dem og, hvad de indeholder. Når man ikke har den viden, er det svært at beskytte data". Sådan siger Mads Nørgaard Madsen, der er partner og Head of Technology & Security i PwC, idet han føjer til, at nogle virksomheder givet er overbevist om, at de har styr på tingene.

Hvis ikke det er tilfældet, er risikoen for en eller anden form for utilsigtet hændelse imidlertid stor. F.eks. i form af en datalæk, et dataindbrud eller ganske enkelt, at de forkerte brugere i virksomheden får adgang til de forkerte data på det forkerte tidspunkt. Frygten for organiseret cyberkriminalitet udgør langt den største trussel, hvis man spørger de danske erhvervsledere.

Truslen er høj i Danmark

Det viser PwC's Cybercrime Survey fra 2021, hvor knapt 8 ud af 10 virksomhedsledere giver udtryk for dette - og frygten er velbegrundet, for angrebene bliver til stadighed mere avancerede. Undersøgelsen bakkes op af Center for Cybersikkerhed, der vurderer, at truslen fra cyberkriminalitet er meget høj i Danmark. Blandt andet er der en stigning i en speciel type af angreb, nemlig det såkaldte Supply Chain Attack.

"Her angribes ikke blot den enkelte virksomhed, men hele den datamæssige værdikæde, der f.eks. binder producent, leverandør, distributør, forhandler og kunde sammen. Det kan f.eks. ske ved ▶



"Mange virksomheder har ikke overblik over, hvad de har af data, hvor de har dem og, hvad de indeholder. Så er det svært at beskytte dem"

Mads Nørgaard Madsen

at implementere en ondartet kode blot et enkelt sted i kæden, hvorefter de kriminelle får en hel række af angrebspunkter", siger Mads Nørgaard Madsen videre.

Faste sikkerhedsprocedurer

Den slags angreb sætter ikke blot erhvervslivet, men hele samfundet under pres, og derfor er det vigtigt, at topledelsen adresserer sikkerhedsproblemet. Heldigvis vurderer 80 pct. af de adspurgte erhvervsledere i undersøgelsen da også, at direktion og ledelse vil fokusere på at opnå den rette balance mellem cybertrusler og investeringer i cybersikkerhed. Det er dog også vigtigt at få implementeret faste sikkerhedsprocedurer.

"I den sammenhæng er kryptering af data et kerneparameter. Desuden er det vigtigt med en procedure for Identity Management, således at der er styr på, hvem, der skal have adgang til hvad, lige som der skal være styr på præcis på, hvilken server og hos hvilken udbyder data befinder sig", siger Mads Nørgaard Madsen. ■

Fakta om rapporten

- 78 pct. af de adspurgte erhvervsledere anser nu organiserede kriminelle for at være blandt virksomhedens største cybertrusler, hvilket er den hidtil største andel i Cybercrime Surveys historie.
- 81 pct. af CXO'erne (Chief Experience Officer) er bekymrede for, at virksomhedens kritiske systemer bliver utilgængelige i længere tid som følge af et cyberangreb. Desuden er man bekymret for økonomisk tab og kompromitterede eller stjålne data.
- 62 pct. af de adspurgte erhvervsledere forventer en stigning i cybersikkerhedsbudgettet inden for de næste 12 måneder. 6 ud af 10 forventer en budgetstigning på op til 25 pct., mens 3 ud af 10 forventer en stigning på mere end 25 pct.

D-mærket skal øge fokus på **IT-sikkerhed**

Danmark er et af de mest digitaliserede lande i verden. Derfor skal virksomhederne også være helt fremme i skoene, når det gælder it-sikkerhed og ansvarlig dataanvendelse. Med det såkaldte D-mærke har danske virksomheder, i øvrigt som de første i verden, nu fået en unik mulighed for at sende et klart signal til omverden om, at de prioriterer datasikkerhed, databeskyttelse og ikke mindst dataetik.

"D-mærket blev lanceret i september 2021, og det er ikke blot et tilfældigt klistermærke. Det skal være med til at skabe tillid og vise omverden, at virksomheden rent faktisk har gjort en indsats. Tillid på datafronten bliver nemlig i stadig højere grad en konkurrenceparameter". Det siger Morten Rosted Vang, der er fagleder for Digital Ansvarlighed og Cybersikkerhed i Dansk Industri.

Et mærke, der stiller krav

Forbrugerrådet, Tænk, Dansk Erhverv, SMV Danmark og Dansk Industri er sammen med Industriens Fond, der har støttet projektet med 18 mio. kr., initiativtager til mærket, som vil blive administreret af et dedikeret sekretariat, der har til huse i Industriens Hus. Morten Rosted Vang understreger, at det ikke er et mærke, man blot får tildelt, fordi man beder om det.

"Virksomhederne skal leve op til en række forskellige kriterier, og vores håb er, at dette mærke for alvor kan få datasikkerheden på dagsordenen", siger han. Han understreger dog samtidig, at hvis sikkerheden svigter, er det langt fra altid, fordi virksomhederne sjusker, men fordi datasikkerhed er blevet en særdeles kompleks affære, hvor det kan være nemt at miste overblikket.

Søg gerne hjælp udefra

"Vi gør en brav indsats for at informere virksomhederne, og på vores medlemmers vegne har vi faktisk en god dialog med myndighederne på området. Men i en travl hverdag er det ikke altid, at emnet står øverst på dagsordenen", siger Morten Rosted Vang. Datasikkerhed kræver jo et komplet overblik over såvel it-infrastruktur som servere, data og processer, understreger han.

I de store virksomheder har man måske de tekniske ressourcer til at gøre noget ved det, men savner overblikket. I de små virksomheder har man måske overblikket, men savner de tekniske ressourcer. Derfor er hans råd, at man får fod på data og dataflow, eventuel ved hjælp af ekstern assistance. Det er grundlæggende, både i forhold til at overholde lovgivningen og i forhold til at beskytte virksomheden it-sikkerhedsmæssigt. ■

"I Dansk Industri gør vi, hvad vi kan for at informere om datasikkerhed, men det er ikke altid nok. Forhåbentlig kan D-mærket være med til at øge fokus"

Morten Rosted Vang

digital tryghed

Fakta om D-mærket

D-mærket tildeles virksomheder og ikke specifikke produkter eller tjenester. Det består af 8 overordnede kriterier som dækker it-sikkerhed, persondatabeskyttelse, kunstig intelligens og dataetik. D-mærkets tilpasses den enkelte virksomhed, så en mindre virksomhed ikke skal leve op til de samme antal kriterier, som en stor virksomhed.

For at sikre, at D-mærket bygger på "best practice" i virksomhederne samt den nyeste forskning og ekspertviden, er der nedsat et "advisory board". Medlemmerne har kompetencer indenfor it-sikkerhed, jura, privatlivsbeskyttelse, virksomhedshensyn, forretningsmodeller, gennemsigtighed og kunstig intelligens.

Gode sikkerhedsråd fra Thales:
Sådan optimerer du din datasikkerhed

Thales er en ledende spiller inden for databeskyttelse og kryptering samt ikke mindst håndtering af krypteringsnøgler. Vi er ikke knyttet til en enkelt cloudprovider, og vi håndterer såvel cloud som multicloud og on-premise samt neutrale teknologileverandører.

Kryptering er processen med at kode data, så kun autoriserede parter har adgang til at læse dem - men kryptering har kun værdi, hvis virksomheden selv har adgang til krypteringsnøglen, og krypteringsnøglen har kun værdi, hvis virksomheden kan sikre kontrollen med den og har adgang til den.

Thales leverer sikkerhedsløsninger til såvel store som mellemstore og små virksomheder. Når din virksomhed er kunde hos os, garanterer vi end-to-end datasikkerhed ud fra tre kerneområder, nemlig Discover, Protect og Control. Det vil sige vi har styr på, hvor data er, om de er beskyttet - altså krypteret - og ikke mindst, om du er compliance i forhold til regulativer.

Et mantra for os er separation. Det vil sige, at selv om en virksomhed vælger en cloududbyder, der tilbyder kryptering, er det essentielt, at virksomheden selv har ansvaret for håndtering af krypteringsnøglerne. I modsat fald giver virksomheden tredjemand fri adgang til de forretningskritiske data.

Datasikkerhed handler imidlertid ikke kun om at beskytte data. Det handler også om at leve op til gældende lovgivning. Stort set alle virksomheders samhandel krydser i dag landegrænser, og på verdensplan eksisterer omkring 1.800 forskellige regulatoriske forordninger, som skal overholdes.

Fra starten af 2024 træder en ny udgave af EU's Net- og Informationssikkerhedsdirektiv, NIS2, i kraft. Det regulerer virksomheder og myndigheder på cyber- samt informationssikkerhedsområdet og kommer til at omfatte en række sektorer, der ikke tidligere har været omfattet af regulering. Blandt andre sektorer inden for fødevarer, spildevand og affald samt udvalgte sektorer i fremstillingsindustrien. Det udvider kravene til og sanktioneringen af cybersikkerhed og betyder, at flere danske virksomheder skal forholde sig til blandt andet øgede krav til risikostyring, kontrol og tilsyn.

Det er ikke afgørende, om det er virksomheden eller cloudleverandøren, der træffer de supplerende foranstaltninger, forudsat foranstaltningerne er effektive. Der vil dog være typer af supplerende foranstaltninger, herunder navnlig implementering af effektiv kryptering, som kan være vanskelige for cloudleverandøren at træffe. Det er navnlig tilfældet, hvis leverandøren selv ønsker at være i besiddelse af krypteringsnøglen, hvorved krypteringen ikke anses som værende effektiv.

I tilfælde, hvor cloudleverandøren kan træffe effektive foranstaltninger, er det fortsat virksomhedens ansvar at sikre, at de supplerende foranstaltninger, som cloudleverandøren træffer, reelt er effektive og i kombination med det relevante overførselsgrundlag sikrer et beskyttelsesniveau, som i det væsentlige svarer til niveauet i EU/EØS.

Ligeledes er det den modsatte vej rundt et krav, at eventuelle samarbejdspartnere uden for EU lever op til GDPR-forordningen. Hvis en virksomhed har samhandel med og udveksler data med udlandet, kan det derfor godt svare sig at søge professionel rådgivning om, hvorledes de regulatoriske krav efterleves.

Derfor - husk at datasikkerhed er essentiel. Både i forhold til beskyttelse af virksomhedens egne data, beskyttelse af eksterne data samt ikke mindst i relation til overholdelse af gældende lovgivning i de lande, virksomheden opererer i. Thales kan hjælpe med at få styr på alle disse forhold. ■

EXCLUSIVE NETWORKS

Exclusive Networks Denmark A/S, er distributør af Thales løsninger og kan henvise til en forhandler.
Tlf. 70 234 235 eller email: sales_dk@exclusive-networks.com