Cybersikkerhed handler om sund fornuft. Og det er noget, vi kun for alvor lykkes med, hvis vi løfter i flok, og der konkret handles på det.

Kronik.

Det bugner med tilbud om cybersikkerhed - hvordan griber vi dem og sikrer fremdrift?

Jan Stentoft, professor, Institut for Erhverv og Bæredygtighed og Tina Højrup Kjær, projektleder, Odense Robotics

Cybersikkerhed er ikke blot en teknisk disciplin for de få. Det er et forretningskritisk område, der kræver opmærksomhed, investering og samarbejde.

De seneste års stigende antal cyberangreb har lammet alt fra store globale koncerner til mindre lokale virksomheder inden for alle brancher. Når produktionslinjer står stille, ordrer ikke kan leveres, og kunder mister tilliden, er der ikke blot tale om et it-problem.

Det er en reel trussel mod virksomhedens overlevelse. Industriens Fond har derfor investeret massivt i at styrke cybersikkerheden i dansk erhvervsliv – ikke mindst i små og mellemstore virksomheder (SMV'er).

Gennem projekter som "Cybersikkerhed og Forretningskontinuitet" (www.cyber-smv.dk) ved SDU og "Cyber Safe Robotics" i regi af Odense Roboticsklyngen bliver cybersikkerhed gjort konkret, tilgængelig og værdiskabende. Det sker i tæt samarbejde med virksomhederne selv. Løsningerne skal nemlig udvikles i praksis og i fællesskab og ikke bag skriveborde af enkeltpersoner.

VI STÅR OVERFOR en usynlig trussel med synlige konsekvenser. For mange virksomheder er cybersikkerhed stadig noget, man 'bør' tage sig af, når der er tid. Men realiteten er, at det ikke kan vente.

Angrebene bliver stadig mere sofistikerede, og det er sjældent tilfældigt, hvem der rammes. Særligt SMV'er er sårbare, både fordi de er mindre digitalt rustede, og fordi de ofte er leverandører til større aktører og dermed indgangsveje til mere komplekse værdikæder.

Når en ny CNC-maskine eller robot skal købes, stilles der sjældent spørgsmål. Den er nødvendig for, at produktionen kan køre effektivt. Men når der skal investeres i cybersikkerhed, melder tvivlen sig: Hvad får vi egentlig for pengene?

Det er et relevant spørgsmål. Men det samme spørgsmål kan stilles til en brandforsikring.

Vi håber aldrig, vi får brug for den, men vi sover roligere om natten, fordi vi ved, at virksomheden er bedre rustet, hvis uheldet er ude. Man bør derfor ikke anskue cybersikkerhed som en omkostning, men som et middel til at sikre robusthed og konkurrencefordele.

I EN TID med stigende geopolitisk uro og usikre markeder, som vi eksempelvis ser det med Trump-administrationens handelsstrategier, bliver det endnu vigtigere at sikre digital robusthed. En virksomhed, der kan levere pålideligt, sikkert og uden driftsforstyrrelser, står stærkere over for både kunder og samarbejdspartnere.

Cybersikkerhed handler ikke blot om at beskytte sig. Det handler i lige så høj grad om at vise, at man er en troværdig og professionel aktør i forsyningskæderne.

I Danmark gøres der mange tiltag for at styrke SMV'ers konkurrenceevne. Imidlertid er det svært for virksomhederne at orientere sig i alle de muligheder og værktøjer, der findes.

Ny forskning om digitalisering i SMV'er har undersøgt digitalisering som en dynamisk kapabilitet, det vil sige en virksomheds evne til at tilpasse, forny og omforme sine ressourcer og kompetencer for at reagere på ændringer i omgivelserne.

Dynamiske kapabiliteter består af tre primære aktiviteter:

1) *Sensing* (identifikation af muligheder), 2) *Seizing* (evnen til effektivt at mobilisere ressourcer for at udnytte mulighederne) og 3) *Transforming* (evnen til at justere og tilpasse ressourcer og kompetencer for at implementere løsninger).

På en skala fra 1 til 5, hvor 1 er 'i lav grad' og 5 er 'i høj grad', opnås der i en landsdækkende spørgeskemaundersøgelse for danske produktions SMV'er et gennemsnit på 2,48 for *Sensing* og 2,21 for henholdsvis *Seizing* og *Transforming*.

Et gennemsnit på 2,48 er ikke prangende, men et gennemsnit på 2,21 indikerer, at det er svært for SMV'er at mobilisere ressourcer og implementere løsninger. Vi ser derfor et behov for at styrke SMV'ernes *Seizing* og *Transformation* kapabiliteter.

SMV'ER HAR INTERESSE for cybersikkerhed, men kan ikke afsætte den nødvendige tid, fordi de har travlt med drift.

Man kan derfor overveje at skrue lidt ned for aktiviteter med *Sensing* for derved at styrke *Seizing* og *Transformation*. Og man kan overveje, hvordan vi kan hjælpe SMV'erne med at mobilisere ressourcer – og hvordan vi kan understøtte dem med at implementere løsninger, der styrker deres robusthed og konkurrenceevne.

Set i lyset af SMV'ernes udfordringer er der hjælp at hente. I hele landet tilbyder lokale erhvervsfremme-organisationer, regionale erhvervshuse, klynger som Odense Robotics, brancheorganisationer som Dansk Industri og SMVdanmark og GTS-institutter som FORCE Technology og Teknologisk Institut konkrete træningsforløb, workshops og sparring.

Projekter finansieret af Industriens Fond har netop fokus på at bringe viden ud dér, hvor den skal bruges – i produktionshallen, på kontoret og i bestyrelseslokalet. Men det kræver, at virksomhederne griber bolden. For arbejdet med cybersikkerhed kræver ledelsesmæssig opbakning og en erkendelse af, at digital sikkerhed er en del af moderne forretningsudvikling.

DET NÆSTE STORE sikkerhedsbrud kan ske i morgen. Eller aldrig. Men det er ikke spørgsmålet.

Spørgsmålet er, hvordan erhvervslivet rustes bedst muligt – og hvordan vi sikrer, at investeringer i cybersikkerhed bliver set som det, de er – *a license to operate* i en digital tidsalder.

SMV'er kan støttes i at sikre ressourcer til cybersikkerhed gennem en kombination af økonomisk støtte, teknisk rådgivning og praktisk træning. Økonomisk støtte kan omfatte tilskud eller skattefradrag målrettet investeringer i cybersikkerhedsteknologi

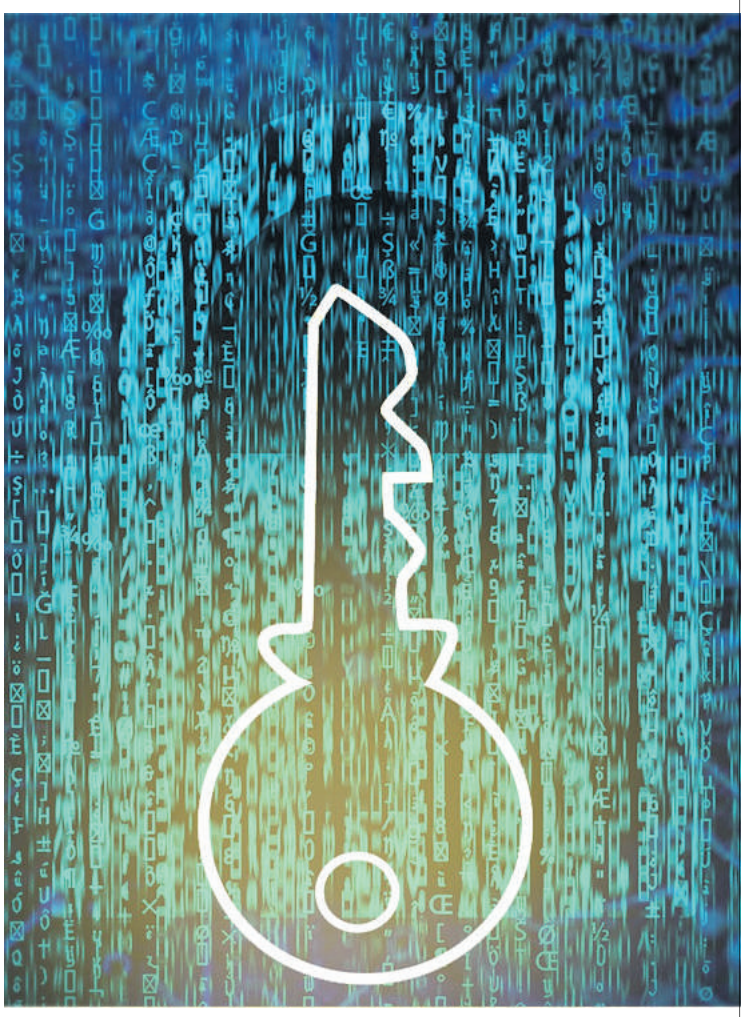

Illustration: Gert Ejton

og forsikringer, hvilket gør det lettere for virksomhederne at prioritere sikkerhed uden at belaste deres budgetter unødigt.

Teknisk rådgivning kan tilbydes i form af gratis eller subsidieret adgang til cybersikkerhedseksperter, som kan hjælpe med risikovurdering, udvikling af sikkerhedspolitikker og løbende sikkerhedstjek.

TRÆNING SPILLER EN afgørende rolle, og derfor kan man tilbyde SMV'er adgang til e-læringskurser og workshops, der øger medarbejdernes bevidsthed om trusler som phishing og sikrer, at ledelsen forstår vigtigheden af at afsætte ressourcer til sikkerhed.

Netværk og erfaringsudveksling kan styrke SMV'ernes forståelse af cybersikkerhed ved at lade dem dele erfaringer og løsninger med andre virksomheder, hvilket skaber et fællesskab af viden og støtte. Derudover kan adgang til standardiserede værktøjer som antivirus, backup-løsninger og systemer til sårbarhedsscanning tilbydes gratis eller til reduceret pris.

Praktiske beredskabsøvelser, hvor virksomheder kan teste deres reaktionsplaner mod forskellige typer cyberangreb, kan sikre, at de ikke kun har teoretisk viden, men også praktisk erfaring med at håndtere trusler.

Cybersikkerhed handler om sund fornuft. Og det er noget, vi kun for alvor lykkes med, hvis vi løfter i flok, og der konkret handles på det.