Cybersikkerhed er ikke kun en teknisk udfordring, men også en organisatorisk og ledelsesmæssig opgave.

Kronik.

Hvordan sikrer vi, at cybersikkerhed bliver taget alvorligt?

Jan Stentoft, professor, Institut for Erhverv og Bæredygtighed, Vincent Keating, lektor, Center for War Studies, Marco Peressotti, lektor, Institut for Matematik og Datalogi, samt Peter Mayer, adjunkt, Institut for Matematik og Datalogi, SDU

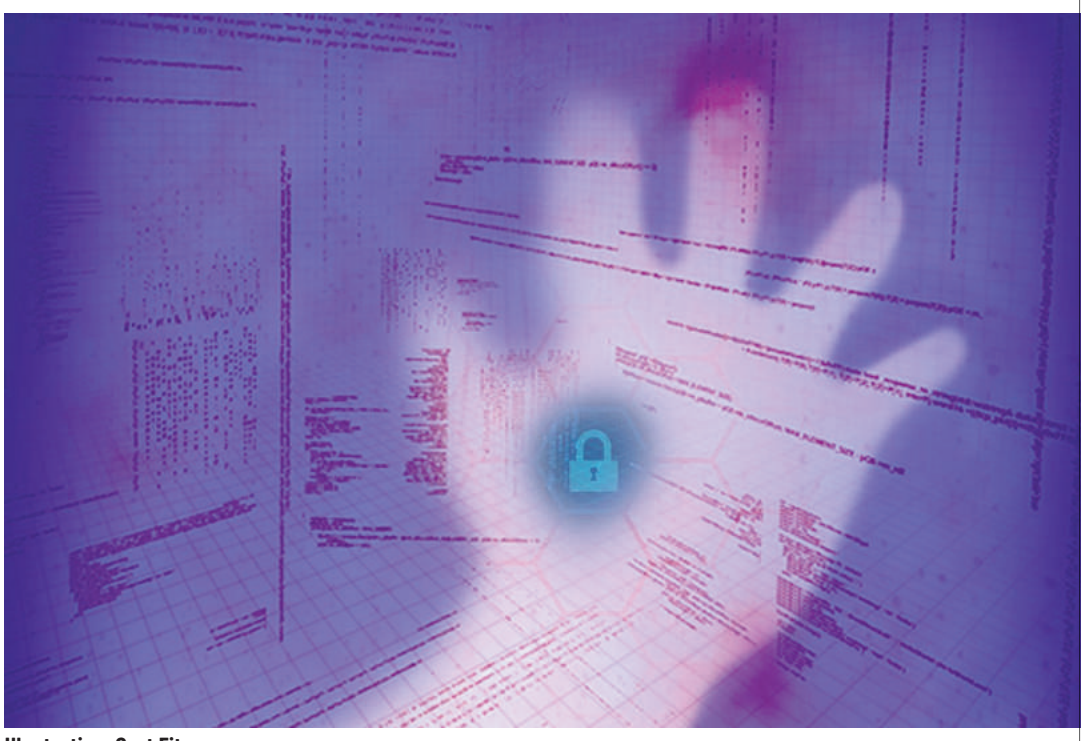

Illustration: Gert Ejton

Manglende vedligeholdelse af cybersikkerhed i både private og offentlige virksomheder i Danmark er en stadigt voksende udfordring. Ikke mindst på grund af den fremadskridende digitalisering af samfundet.

Center for Cybersikkerhed vurderer i øjeblikket trusselsniveauet for Danmark som meget højt. Det gør de i lyset af øgede geopolitiske spændinger og potentialet for, at ondsindede statslige aktører kan udnytte cybersvagheder til at chikanere danske enheder eller hindre danske økonomiske og politiske mål.

Angrebene er blevet mere præcise og fokuserer ofte på ransomware, der låser computere, samt dataudvinding - og de er målrettet kritisk infrastruktur som energiforsyning, sundhedssektoren og transport. Også danske virksomheder og institutioner er sårbare over for såkaldte supply chain-angreb, hvor cyberangrebene sker indirekte gennem tredjepartsleverandører, hvoraf mange er uden for de danske myndigheders direkte kontrol.

HVORDAN SIKRER VI så, at både offentlige og private virksomheder forholder sig til trusselsbilledet og tager cybersikkerhed seriøst?

For nogle virksomheder er tankegangen om cybersikkerhed styret af direktivet om netværks- og informationssikkerhed, NIS-2, der forventes at træde i kraft den 1. juli 2025. Direktivet, som bygger på det tidligere NIS-direktiv, søger at adressere de stigende trusler mod net- og informationssystemer for at sikre en mere ensartet og effektiv tilgang til cybersikkerhed i hele EU. Formålet er at styrke cybersikkerheden og robustheden i kritiske sektorer på tværs af EU's medlemslande.

NIS-2 udvider cybersikkerhedskravene, hvad angår de sektorer og virksomheder, der er omfattet, og indfører strengere regler for risikostyring, hændelsesrapportering og samarbejde mellem EU-landene. Direktivet kræver blandt andet, at flere virksomheder implementerer robuste sikkerhedsforanstaltninger og rapporterer cyberhændelser til de relevante myndigheder inden for en kort tidsramme.

I Danmark forventes NIS-2 at få betydelig indvirkning på både offentlige og private aktører inden for sektorer som energi, sundhed, transport og finans.

MEN HVORFOR BØR alle virksomheder ikke være underlagt lovkrav om cybersikkerhed? Kravene laves jo netop for at ruste virksomhederne mod cyberangreb.

Et angreb kan lægge en virksomhed ned i dage, uger, måneder eller år afhængig af styrken og den løsesum, der evt. kræves fra hackerne. Til sammenligning arbejder Fødevarestyrelsen for at sikre fødevaresikkerhed, dyrevelfærd og folkesundhed samt at styrke forbrugernes tillid til fødevarer.

Styrelsen kontrollerer produktionen, importen og salget af fødevarer hos alle virksomheder i branchen for at sikre, at de lever op til gældende standarder og lovgivning. Derudover informerer Fødevarestyrelsen borgere og virksomheder om regler og anbefalinger inden for fødevaresikkerhed, ernæring og dyrevelfærd, hvilket bidrager til at skabe et trygt og sundt miljø for både virksomheder, mennesker og dyr i Danmark.

Dårlige fødevarer kan koste menneskeliv og virksomheders eksistens. Tilsvarende kan dårlig cybersikkerhed også true virksomheders eksistens og medføre tab af arbejdspladser.

MED EN STYRELSE for Cybersikkerhed ville vi kunne styrke forebyggelse, modsvar og regulering. Typen af cyberangreb udvikler sig hurtigt, og de kan have fatale konsekvenser for både virksomheder og samfundet i form af økonomiske tab, læk af kritiske data, dårligt omdømme og en generel mindsket tillid til digitale tjenester blandt befolkningen.

Styrelsen ville kunne fokusere på at udvikle forebyggende tiltag, herunder uddannelse, træning og udvikling af sikkerhedsstandarder, samtidig med at den sikrer hurtige reaktioner på akutte trusler. Ved at samle disse kompetencer under én enhed vil det blive muligt at skabe en mere proaktiv og dynamisk tilgang til dansk cybersikkerhed.

En Styrelse for Cybersikkerhed ville kunne fungere som et videnscenter og en ressource for både offentlige og private aktører. Mange virksomheder, især små og mellemstore virksomheder, mangler de nødvendige ressourcer og ekspertise til at beskytte sig mod cyberangreb.

RÅDGIVNING, TRÆNING OG værktøjer kan gøre det lettere for virksomheder at styrke cybersikkerheden. Dette er særlig vigtigt i en tid, hvor supply chain-angreb og angreb på underleverandører bliver stadig mere almindelige.

Det betyder, at selv tilsyneladende ikke-kritiske virksomheder har brug for robuste cybersikkerhedstiltag og beredskabsplaner, og at alle virksomheder skal være opmærksomme på, hvilke cybersikkerhedskrav de bør stille, når de samarbejder med danske såvel som udenlandske leverandører og underleverandører.

En Styrelse for Cybersikkerhed ville også kunne bidrage til at opbygge større tillid i samfundet. I dag er de fleste tjenester digitaliserede, og borgerne er i høj grad afhængige af teknologi i dagligdagen.

Derfor er det vigtigt, at der er tillid til, at data og systemer er sikre. Tillid til systemer er en grundlæggende forudsætning, hvis vi ønsker, at digitaliseringen fortsat skal skabe værdi for samfundet.

Ved klart at kommunikere og håndtere cybersikkerhed, ville en Styrelse for Cybersikkerhed dermed hjælpe borgerne til at føle sig trygge i brugen af digitale løsninger.

DET ER KLART, at en ny styrelse medfører øgede administrative omkostninger og bureaukrati. Men omkostningerne ved ikke at investere i cybersikkerhed kan være langt højere gennem økonomiske tab, tab af tillid, skader på kritisk infrastruktur og tab af fortrolige offentlige og private data.

En samlet og strategisk tilgang til cybersikkerhed vil på sigt være en investering i Danmarks sikkerhed og stabilitet.

En Styrelse for Cybersikkerhed kan udføre kontrolopgaver, såsom stikprøvebaserede undersøgelser, for at evaluere sikkerhedsniveauer. Andre opgaver kan omfatte certificeringsordninger, træning og rådgivning, rapportering samt udstedelse af påbud, bøder eller sanktioner.

Implementeringen af sådanne kontrolfunktioner, samtidig med at der stilles ressourcer til rådighed for at opfylde målene, vil hjælpe med at sikre, at danske virksomheder tager cybersikkerhed mere alvorligt og lever op til deres ansvar for at beskytte både sig selv, deres samarbejdspartnere og samfundet mod cyberangreb.

ETABLERINGEN AF EN Styrelse for Cybersikkerhed vil være en naturlig og nødvendig udvikling i den danske stats digitaliseringsproces. Styrelsen vil ikke kun styrke Danmarks kapacitet til at håndtere nutidens komplekse cybertrusler, men også til at tackle fremtidige udfordringer.

Ved at etablere en central enhed, der samler og koordinerer indsatsen, fremmer samarbejde med internationale partnere og øger offentlighedens opmærksomhed på cybersikkerhed, kan danske virksomheder stå stærkere i kampen mod cyberkriminalitet.

Cybersikkerhed er ikke kun en teknisk udfordring, men også en organisatorisk og ledelsesmæssig opgave. Vi skal behandle det som en samfundsmæssig nødvendighed, der kræver en holistisk og målrettet tilgang.