> **Hver femte SMV har været udsat for cyberangreb indenfor de seneste år.**

Kronik.

Cybersikkerhed i forsyningskæderne: Har det relevans for SMV'er?



Jan Stentoft, professor, Institut for Erhvervsøkonomi og Bæredygtighed, Marco Peressotti, lektor, Institut for Matematik og Datalogi, og Peter Mayer, adjunkt, Institut for Matematik og Datalogi, SDU

Små og mellemstore virksomheder (SMV'er) spiller en vigtig samfundsrolle ved at bidrage med økonomisk vækst, jobskabelse, innovation og eksport. Cirka to tredjedele af jobbene i den private sektor findes i SMV'er. De cirka 300.000 danske SMV'er beskæftiger i omegnen af en million medarbejdere.

Sammenlignet med store virksomheder har SMV'er ofte et stort driftsfokus på bekostning af udviklingstiltag af forretningsgange, de har færre finansielle og menneskelige ressourcer og har mindre viden om IT. Netop IT-siden giver SMV'er en række nye udfordringer med cybersikkerhed i takt med den stigende udbredelse af cyberangreb.

Cybersikkerhed handler om at beskytte systemer, kommunikation og data mod uautoriseret eller skjult adgang, ændring, ødelæggelse og afbrydelse og om at verificere ægtheden af brugere, systemer og enheder.

Cyberangreb som for eksempel ransomware kan lamme virksomheders drift, og opstår der datalæk, kan det resultere i store bøder og kompensationskrav. Effektiv cybersikkerhed sikrer, at virksomheders drift ikke forstyrres af cybertrusler, hvilket er essentielt for at opretholde tilliden hos kunder og leverandører.

DANMARK ER ET af de mest digitaliserede lande i verden. På den ene side er det godt for konkurrenceevnen, men på den anden side gør det også de enkelte virksomheder mere sårbare overfor cyberangreb.

SMV'er er digitalt forbundet til mange forskellige aktører såsom kunder, leverandører, myndigheder, finansielle partnere, serviceudbydere og IT-leverandører. Enhver forbindelse udgør en trussel for et angreb.

Flere er af den fejlagtige opfattelse, at SMV'er ikke er oplagte mål for cyberangreb, da de ikke er attraktive nok. Men *alle* virksomheder er attraktive for hackere, der via angreb kan lamme virksomheders drift for derefter at afkræve penge for at frigøre data igen.

Faktisk ser man, at SMV'er i stigende grad er mål for cyberkriminelle, som ofte opfatter dem som lettere mål sammenlignet med større virksomheder med mere robuste sikkerhedsforanstaltninger. Samtidig kan SMV'er være attraktive for hackere, da de via SMV'ernes systemer eller produkter kan opnå adgang til de større virksomheders systemer.

Derudover håndterer SMV'er ofte følsomme kundedata og forretningsoplysninger, som, hvis de bliver kompromitteret, kan skade deres omdømme og udhule tilliden til dem. Manglende cybersikkerhed kan derfor føre til betydelige økonomiske tab for SMV'er.

FOKUS PÅ CYBERSIKKERHED er også vigtigt, idet lovkrav om overholdelse af databeskyttelseslove som for eksempel GDPR bliver stadig mere strenge. Manglende overholdelse kan resultere i store bøder og juridiske konsekvenser, hvilket yderligere understreger behovet for robuste cybersikkerhedspraksisser.

Investering i cybersikkerhed øger samtidig en SMV's samlede modstandsdygtighed, hvilket gør det muligt for at opretholde forretningskontinuitet i lyset af cybertrusler og reducere risikoen for driftsforstyrrelser.

Den stigende afhængighed af digitale værktøjer og online platforme har også udvidet SMV'ers angrebsflade, hvilket gør cybersikkerhed til en væsentlig del af deres driftsmæssige strategi.

Beskyttelse af digitale aktiver og sikring af integriteten og tilgængeligheden af online tjenester bør derfor en være del af den normale risikostyring. Der er således vigtige argumenter for, at SMV'er øger deres indsigt i og praksis med cybersikkerhed i et forsyningskædeperspektiv.

EN NY FORSKNINGS-RAPPORT om cybersikkerhed i danske produktions-SMV'er, der er gennemført i projektet Cybersikkerhed og Forretningskontinuitet (www.cyber-smv.dk) med midler fra Industriens Fond, afslører flere interessante forhold.

For det første har hver femte SMV været udsat for cyberangreb indenfor de seneste år. For det andet er der generelt en høj opmærksomhed på cybersikkerhed, og virksomhederne synes at være godt internt integreret mellem de forskellige funktioner fra salg over produktion og indkøb til IT og økonomi.

Det er gode betingelser for at styrke arbejdet med cybersikkerhed, for det er ikke nok blot er være bevidst om det. Der skal også handling til.

Det gælder ikke kun i forhold til intern sikkerhed, men også sikkerhed ud i forsyningskæderne. Undersøgelsen afslører nemlig også, at SMV'er har en lav grad af praksis med at sikre cybersikkerhed i et forsyningskædeperspektiv.

Det angår for eksempel risikostyring af cybersikkerhed, risici ved leverandører og deres produkter og serviceydelser, krav til sikkerhed i kontrakter samt aftaler både under og efter afslutning af samhandlen. Der er således behov for, at der udvikles metoder og værktøjer, der kan hjælpe produktions-SMV'erne med at få konkrete indsatser igangsat om cybersikkerhed.

HVIS VI TAGER et blik i krystalkuglen, er der intet, der peger på, at cybertruslerne aftager. Tværtimod.

Den stigende brug af kunstig intelligens er et yderligere forhold, der kan give cyberkriminelle nye værktøjer og metoder og dermed øge risikoen for cyberangreb. Stigende (geo)politiske og sociale spændinger har også ført til en stigning i antallet af hacktivister, der udnytter sårbarheder og sikkerhedshuller til at udtrykke uenighed eller støtte til sager som væbnede konflikter eller sociale uenigheder.

Yderligere er dis-information en praksis i vækst, hvor man bevidst videreformidler fejlagtige oplysninger. Denne udvikling peger på et stort behov for at øge træningen indenfor cybersikkerhed.

Det er et område, der bør have den fulde opmærksomhed blandt SMV'ers bestyrelser, ledelser og medarbejdere. Et cyberangreb er nemlig ikke længere væk end et enkelt forkert klik.

Illustration: Gert Ejton

SMV'ER ER SOM nævnt tidligere udfordret på ressourcesiden, hvilket kan være en barriere for at arbejde med sikkerheden. Imidlertid er der assistance at hente gennem SMV: Digital.

Det paradoksale er dog, at der er et lavt kendskab til offentlige støttemuligheder blandt danske SMV'er.

En anden mulighed for SMV'erne er at styrke sikkerheden gennem D-mærket, der er en mærkningsordning med afsæt i internationale standarder, som kombinerer både IT-sikkerhed og ansvarlig dataanvendelse. Det er gratis at bruge D-mærkets selvevalueringsværktøj, men man skal betale, hvis tilsyns- og kontrolprocessen igangsættes.

Man kan også søge viden gennem brancheforeninger, det kommunale erhvervsfremmesystem eller de seks danske erhvervshuse. Hvis der ikke udbydes aktiviteter omkring cybersikkerhed, så foreslå at få det sat på agendaen. Deltag i online møder om emnet, der udbydes af banker, konsulenter, interesseorganisationer med videre.

Cybertruslerne forsvinder ikke. De er kommet for at blive. Det er et område i kraftig vækst, og angrebene bliver mere og mere sofistikerede gennem de komplekse forsyningskæder.

Det er et vigtigt område at få prioriteret – også i en travl hverdag med drift. Derfor har cybersikkerhed stor relevans. Også for SMV'er.