SMV'er har typisk den laveste cybersikkerhed givet deres begrænsede finansielle og menneskelige ressourcer og viden om IT. Hackere udnytter svage led i forsyningskæderne og angriber via usikre systemer hos leverandører.

Cybersikkerhed i forsyningskæden.

Hvor piv-åben er din virksomhed?




KRONIK

Jan Stentoft, professor, Institut for Entreprenørskab og Relationsledelse, SDU. Olivier Schmitt, professor, Center for War Studies, SDU. Marco Peressotti, lektor, Institut for Matematik og Datalogi, SDU. Amelie Theussen, lektor, Forsvarsakademiet

Danske små og mellemstore virksomheder (SMV'er) er i dag stærkt afhængige af IT både til håndtering af interne processer og kommunikation, men også i forbindelse med outsourcing og samhandel med eksterne partnere, leverandører og kunder. IT-teknologi og internettet – og den brede anvendelse heraf – har gjort interaktionen, koordineringen og integrationen med omgivelserne både nemmere, hurtigere og billigere.

Digital omstilling har på den ene side bidraget til effektivisering af forretningsgangene i de små og mellemstore produktionsvirksomheder, men den har på den anden side også skabt sårbarheder overfor cyberangreb. Derfor er det vigtigt at have fokus på cybersikkerhed, som omfatter gruppen af teknologier, processer og praksisser, der er designet til at beskytte netværk, computere, programmer og data mod angreb, skade eller uautoriseret adgang.

OMGIVELSERNE FOR DANSKE produktions SMV'er er ligeledes under kraftig forandring. Vi er gået fra en lang periode med et lavt niveau af internationale konflikter til et mere konfliktfyldt niveau, hvor den tiltagende stormagtskonkurrence påvirker vestlige allierede, og hvor fokus på kritisk infrastruktur har fået en ny strategisk vigtighed.

Den geopolitiske udvikling øger samtidig risikoen for cyberangreb fra såvel stater som cyberkriminelle. SMV'er er ofte afhængige af eksport for at vækste deres forretning. Det betyder, at forstyrrelser i forsyningskæderne grundet geopolitiske spændinger og restriktioner i forhold til markedsadgang, f.eks. i tilfælde af internationale sanktioner, vil få større konsekvenser for dem.

Ny forskning fra SDU afslører mangel på viden om og parathed til cybersikkerhed blandt danske produktions SMV'er. Det nye EU NIS2 direktiv (Network and Information Security), der har til formål at forbedre medlemslandenes samlede IT-sikkerhed, indeholder strengere krav til virksomheders cybersikkerhed, som også omfatter danske produktions SMV'er. Direktivet vil sikre, at alle organisationer, der tjener en væsentlig funktion i samfundet, har et højt IT-sikkerhedsniveau.

Informationssikkerhed består af grundelementerne fortrolighed, integritet og tilgængelighed.

Fortrolighed refererer til beskyttelsen af data mod uautoriseret offentliggørelse. Uautoriseret, utilsigtet eller uforudset offentliggørelse kan resultere i retslige skridt, økonomisk tab og tab af offentlig tillid.

Integritet handler om, at informationen beskyttes mod uautoriseret eller utilsigtet ændring. Hackere kan for eksempel stjæle og modificere data via malware.

Tilgængelighed vedrører adgangen til kritiske forretningsdata, når det er nødvendigt. Hvis en hjemmeside hackes, kan dens tilgængelighed forsvinde.

Forskellige forretningsenheder både indenfor virksomheden og mellem virksomheder er forbundet via IT-enheder. Der kan opstå, hvad der kaldes for et man-in-the-middle-angreb, når en hacker får adgang til netværket, hvor data kan stjæles og manipuleres. Der kan også finde distribuerede netværksangreb sted, hvor en server overbelastes.

Angreb i form af ransomware er også en praksis, hvor ejeren af en inficeret enhed afpresses til at betale for dataadgang igen. Endelig sker der angreb gennem phishing, hvor der opnås adgang til et system ved at narre medarbejdere til at klikke på falske e-mails. Ikke mindst kan virksomheders egne medarbejdere påføre risici grundet mangel på opmærksomhed på cybersikkerhed.

AT SIKRE INFORMATIONSSIKKERHED i forsyningskæden er langt mere komplekst end blot at downloade det seneste antivirus software. Information er blevet demokratiseret.

I en digital tidsalder er sårbarheder til virksomhedens systemer kompromitteret af anden eller tredje leds underleverandør, som er en del af en forbundet forsyningskæde. Information om lagerniveauer, produktionsplaner, kundeordrer, leverandører og forsendelser er tilgængelige og kan let flyde mellem virksomheder ved brug af bærbare computere og en stregkodescanner. Fremmarchen af Internet of Things skaber også sårbarheder, når IT-enheder, der eksempelvis styrer intelligente robotter eller temperaturer og overvåger servicering af udstyr, kobles på nettet.

Med disse cyberudfordringer bliver det centrale spørgsmål, hvad man som SMV bør gøre. Først skal der skabes bevidsthed om geopolitiske spændinger og cybertrusler. Cybersikkerhed er ikke et IT-spørgsmål, men et anliggende for alle medarbejdere i en virksomhed.

Det handler om at investere tid i medarbejderne på tværs af organisatoriske funktioner og skabe forståelse for, hvad der skal beskyttes, hvilke angreb der skal beskyttes mod og derefter klargøre, hvilke investeringer der bør foretages for at forbedre cybersikkerheden.

Det er vigtigt at træne medarbejdere i cybersikkerhed, og det gælder alle lag i virksomheden, idet for eksempel medarbejderes internetadfærd kan udgøre en trussel. SMV'er er oplagte mål for cyberangreb, fordi de ofte har forholdsmæssig stor adgang til vigtig information givet deres størrelse indenfor forsyningskæden.

SMV'ER HAR TYPISK den laveste cybersikkerhed givet deres begrænsede finansielle og menneskelige ressourcer og viden om IT. Hackere udnytter svage led i forsyningskæderne og angriber via usikre systemer hos leverandører. Der kan skabes en bagdør til software og derigennem adgang til at ændre kildekoderne. Bliver en leverandør ramt, kan det føre til, at kunden ikke kan levere, fordi der ikke kan fås råvarer/komponenter fra leverandøren.

Illustration: Gert Ejton, ved hjælp af Midjourney, kunstig intelligens.

Man kan således have godt styr på egen butik, men kan blive ramt af en leverandør. Hvis en leverandør hackes, kan der opnås adgang til kundedata. Hvis en tredjeparts logistikleverandør rammes, kan virksomhedens drift påvirkes, hvis ERP-systemet er cloudbaseret, hvis data er lagret eksternt, og hvis man bruger andre eksterne IT-serviceydelser. Performancetabet er ikke isoleret til den enkelte virksomhed.

Det påvirker også kundernes performance negativt. Lige så kritisk er det med tab af troværdighed overfor nuværende og potentielle kunder – en konsekvens, der kan være direkte ødelæggende for virksomhederne.

ET NYT PROJEKT, der har fokus på at styrke cybersikkerheden i danske produktions SMV'er (se www.cyber-smv.dk), er netop igangsat med midler fra Industriens Fond. Projektet har fokus på at identificere sårbarheder i forsyningskæderne afledt af geopolitiske spændinger og cybertrusler, samt hvilke kapabiliteter virksomhederne bør styrke for at kunne opnå større cybersikkerhed.

Det handler om at sikre konkurrencekraft.

Der er behov for at styrke kompetencerne, så virksomheden ikke er piv-åben for cyberangreb. Et styrket niveau indenfor cybersikkerhed og en øget opmærksomhed på sårbarhedsrisici bør altså ikke anses som en omkostning for SMV'erne, men som en investering i at (ved)blive at være en attraktiv og sikker samarbejdspartner i forsyningskæderne på linje med god kvalitet, fokus på miljø og social ansvarlighed.

Der er brug for at ændre mindset til at se cybersikkerhed som en kilde til konkurrencefordele.