Kronik.

Et svagt led kan lamme os alle - derfor kræver forsyningskæder stærk cybersikkerhed

Jan Stentoft, professor, Ole Stegmann Mikkelsen, lektor, og Kent Adsbøll Wickstrøm, lektor, Institut for Erhverv og Bæredygtighed, SDU

Jan Stentoft, professor, Institut for Erhverv og Bæredygtighed, SDU. Pressefoto

Ole Stegmann Mikkelsen, SDU. Pressefoto: Jonas Ahlstrøm

Kent Wickstrøm, SDU. Pressefoto

Forestil dig, at en enkelt leverandør i en kompleks global forsyningskæde bliver ramt af et cyberangreb. Produktionen går i stå, logistikken bryder sammen, og samfundskritiske funktioner rammes – ikke fordi virksomheden i sig selv er uerstattelig, men fordi den udgør et vitalt led i en kæde, vi alle er afhængige af.

Fra energi og fødevarer til sundhedsvæsen og transport er vores moderne samfund bygget på digitale forbindelser, der gør os mere effektive - men også mere sårbare. I maj 2023 blev for eksempel 22 danske virksomheder i den danske energisektor ramt af et cyberangreb, der potentielt kunne lamme 100.000 borgere.

Når hackere kan lamme hele sektorer gennem blot ét svagt punkt, bliver cybersikkerhed i forsyningskæderne ikke længere et nicheanliggende for IT-specialister, men et samfundsanliggende af højeste prioritet. Systemer, der er målet for cyberangreb, er såvel IT-systemer som kommunikationssystemer, ERP-systemer og netværk samt servere som OT-systemer (Operational Technology), hvor fysiske processer styres af systemer som SCADA, PLC'er og MES-systemer.

DET ER IKKE kun store virksomheder, der skal have fokus på cybersikkerhed, men også små og mellemstore virksomheder (SMV'er).

Grundpillerne i informations-sikkerhed bygger ofte på det såkaldte CIA-princip, som står for *Confidentiality*, *Integrity* og *Availability*. *Confidentiality* (fortrolighed) handler om at beskytte data mod uautoriseret adgang, for eksempel via kryptering eller adgangskontrol.

Integrity (integritet) sikrer, at information ikke ændres utilsigtet eller ondsindet - data skal være korrekte og pålidelige. *Availability* (tilgængelighed) betyder, at information og systemer er tilgængelige, når de skal bruges, eksempelvis gennem backup og robuste systemer.

For at styrke fortroligheden kan virksomheder gøre brug af awareness-træning, hvor medarbejdere uddannes i for eksempel phising og insidertrusler.

Integriteten kan blandt andet sikres gennem backup og versionsstyring, logning og overvågning samt brug af digitale signaturer. Tilgængeligheden kan styrkes ved at udarbejde nød- og beredskabsplaner og ved at sikre, at systemer og maskiner holdes opdateret for at reducere risici for ransomware og andre angreb.

FORSYNINGSKÆDER ER I sagens natur komplekse, fordi de er flerleddede med aktører som kunder, transportører, lagersteder, producenter, leverandører og underleverandører. Hver af disse parter anvender egne systemer og processer, tit med vidt forskellige sikkerheds- og modenhedsniveauer.

Interaktionen foregår gennem digitale grænseflader, hvor data deles og behandles på tværs af organisationer og landegrænser - ofte uden fuldt overblik eller kontrol. Kompleksiteten øges yderligere af den teknologiske sammensmeltning af IT, OT og IoT, hvor driftskritiske systemer kobles tæt sammen med administrative platforme og internetforbundne enheder.

Et enkelt angreb kan derfor forplante sig på tværs af både digitale og fysiske led. Hertil kommer udfordringer som manglende gennemsigtighed i 3.- og 4.-partsleverandører, forskellige nationale lovkrav og reguleringer samt kulturelle forskelle i risikoforståelse.

Resultatet er et netværk af indbyrdes afhængigheder, hvor ét svagt led kan skabe en dominoeffekt, der rammer mange aktører på én gang.

CYBERSIKKERHED BØR SES som en *license to operate*. Det er ikke længere kun en teknisk disciplin, men et strategisk vilkår for at drive forretning.

Krav fra myndigheder og reguleringer som NIS2 omkring sikring af kritisk infrastruktur og DORA-forordningen til den finansielle sektor er direkte lovkrav for at kunne drive virksomhed. Store virksomheder stiller stigende sikkerhedskrav til deres leverandører.

Hvis en mindre underleverandør ikke kan dokumentere robust cybersikkerhed, risikerer den at miste kontrakter. Cybersikkerhed er dermed en adgangsbillet til at være en del af globale forsyningskæder.

> **Trusselsbilledet vokser hastigt, og angrebene bliver stadig mere sofistikerede, ikke mindst gennem de komplekse forsyningskæder.**

Investorer vurderer cybersikkerhed som en del af ESG og risikostyring. En virksomhed uden cybersikkerhed betragtes som højrisiko.

Kunder forventer, at deres data og drift beskyttes. Et brud på fortrolighed eller tilgængelighed kan ødelægge omdømmet.

Angreb, der stopper produktionen eller lammer IT-systemer, kan føre til økonomiske tab og forsinkelser. Cybersikkerhed er en konkurrencefordel og en del af kerneydelsen.

AT STYRKE CYBERSIKKERHEDEN starter med at øge bevidstheden gennem træning, klare retningslinjer og en kultur, hvor sikkerhed er en naturlig del af hverdagen.

Undersøgelser har vist, at den største trussel mod angreb er virksomhedens medarbejdere. Når medarbejderne er bevidste om risici og deres eget ansvar, bliver de det stærkeste første forsvar mod cyberangreb.

Når perspektivet på cybersikkerhed løftes fra et virksomheds- til et forsyningskædefokus, kommer der nye opgaver til. Industriens Fond har støttet en portefølje af cyberprojekter med fokus på forsyningskæderne, hvor projektet Cybersikkerhed og Forretningskontinuitet (www.cyber-smv.dk) fra SDU og Forsvarsakademiet har operationaliseret konkrete værktøjer til, hvordan cybersikkerhed kan styrkes ud i forsyningskæderne på baggrund af rammeværket Cybersecurity Framework (CSF) fra National Institute of Standards and Technology (NIST).

NIST er et institut under det amerikanske handelsministerium, der har udviklet standarder, retningslinjer og best practices inden for teknologi, målinger og sikkerhed. Værktøjerne omfatter blandt andet prioritering af kunder, cybersikkerhed i kontrakter, due diligence mod kunder og leverandører samt beskyttelse af data, systemer og forretningskritiske oplysninger ved ophør af samarbejdsrelationer.

I EN TRAVL hverdag med drift kan det være svært at finde tid til at prioritere cybersikkerheden. Imidlertid er det vigtigt at agendasætte arbejdet.

Start med at prioritere de vigtigste ting først. Hvad er de mest kritiske systemer og data? Er der lavet risikovurderinger af kunder og leverandører? Dernæst kan der udpeges ansvarlige for arbejdet og eventuelt indgå samarbejde med en IT-leverandør om opgaverne.

Endelig bør man undgå at lægge alt for ambitiøst ud, da det øger risikoen for at kuldsejle med tiltagene. Begynd i stedet med at fokusere på få konkrete forbedringer som backup, multifaktorgodkendelser og awareness-træning.

Sådanne mindre, men kontinuerlige tiltag, kan reducere risikoen markant og fastholde cybersikkerhed på dagsordenen.

SELVOM FORSYNINGSKÆDER ER komplekse, og svage led kan ramme os alle, er der mange muligheder for viden, værktøjer og fremgangsmåder til at styrke cybersikkerheden i et forsyningskædeperspektiv.

Værdifuldt materiale kan blandt andet findes på initiativet "Hele Danmark øver", DI, Dansk Erhverv, Center for Cybersikkerhed, D-mærket og de danske Erhvervshuse.

Cybertrusler er ikke et forbigående fænomen - de er en varig realitet. Trusselsbilledet vokser hastigt, og angrebene bliver stadig mere sofistikerede, ikke mindst gennem de komplekse forsyningskæder.

Derfor er det afgørende at give cybersikkerhed høj prioritet, selv i en travl hverdag præget af drift. Relevansen gælder ikke kun store virksomheder, men i høj grad også SMV'er.

Hver dag starter med Erhverv+

Det siger vores læsere:

"Det første, jeg tjekker om morgenen."
"Mere relevant for mig end de landsdækkende medier."
"Jeg deler artiklerne med min ledelse."
"Kærlighed til virksomheder tæt på mig."

Scan QR-koden eller gå ind på erhvervplus.dk

Tilmeld dig nyhedsbrevet gratis

Erhverv+