Maj 2025

Sammen om cybersikkerheden

Et cybersikkerhedspolitisk udspil fra forsikrings- og pensionsbranchen

F&P FORSIKRING OG PENSION

Indhold

Forord

Danmark står over for en meget høj og kompleks cybertrussel. Det er en kendsgerning, og det er et grundvilkår, vi skal vænne os til. Vi befinder os i en usikker og uforudsigelig tid, og Danmark er et attraktivt mål for aktører, som vil os det ondt i cyberspace.

Vi står som samfund allerede på et godt cyber- og informationssikkerhedsfundament. I Danmark er vi på mange områder modne i arbejdet med at højne cybersikkerheden på tværs af staten og den private sektor. Men truslen udvikler sig, og vi skal kunne imødegå den, det er et ansvar både for staten, virksomhederne og borgere. Derfor er der behov for en styrket indsats, hvor vi forener ressourcer, viden og handlekraft for at sikre, at Danmark også i fremtiden kan modstå og håndtere de stadigt mere komplekse cybertrusler.

I forsikrings- og pensionsbranchen løfter vi vores del af indsatsen og tager arbejdet med cybersikkerhed seriøst. Vi er sat i verden for at skabe tryghed og velstand for danskerne, og de skal kunne have tillid til, at vi forvalter de værdier og data, der rækker ind i deres hverdag på fortrolig og sikker vis. Det særlige ansvar, sektoren har over for den enkelte dansker og det danske samfund, er vi meget bevidste om.

Men ingen kan løfte ansvaret alene - vi skal stå sammen om cybersikkerheden i Danmark.

Cyberangreb udgør en stor trussel mod samfundet som helhed. Derfor skal vi styrke den fælles indsats mellem den private sektor og staten, og vores borgere skal kunne bidrage til robustheden ved at være digitalt dannede og trænede.

Den dybe tallerken skal ikke genopfindes, for vi har allerede mange gode løsninger og erfaringer, som virker. Men vi skal være villige til at forny vores tilgang. Og så skal vi sætte ind der, hvor den geopolitiske og teknologiske udvikling har skabt nye udfordringer. Gør vi det, kan vi blive ved med at udnytte digitaliseringen og den teknologiske udvikling, samtidig med at danskerne kan være trygge i en digital hverdag.

I dette udspil kommer vi med otte forslag, som vi i forsikrings- og pensionsbranchen mener kræver særlig opmærksomhed i fremtidens cybersikkerhedsarbejde. Forslagene er vores input til regeringens kommende nationale strategi for cyber- og informationssikkerhed. Forslagene vil understøtte Danmarks rejse mod at være bedst muligt forberedt til fremtidens cybertrusler.

Kent Damsgaard
Administrerende direktør, F&P

Overblik over forslag

F&P foreslår følgende initiativer for at styrke cybersikkerheden i Danmark:

Samfundsrobusthed

Forslag 1: Opret et nordisk-baltisk cybercenter i Danmark
- Der skal oprettes et grænseoverskridende cybersikkerhedsoperationscenter, beliggende i Danmark, med støtte fra EU, i samarbejde med vores nordiske og baltiske kolleger.

Forslag 2: Styrk den kritiske infrastruktur og forsyningssikkerheden
- Der skal igangsættes en målrettet analyse af, hvor der findes sårbarheder og svagheder i den kritiske infrastruktur – både fysisk og digitalt.

Forslag 3: Styrk rådgivning og støtte til virksomheder i kampen mod cybertruslen
- Styrelsen for Samfundssikkerheds rolle som rådgiver og støttefunktion for erhvervslivet skal styrkes, når det gælder forebyggelse og håndtering af cyberangreb.

Forslag 4: SMV-anbefalinger til enkel og effektiv cybersikkerhed
- Myndighederne skal udarbejde en række klare og brugbare anbefalinger, der kan hjælpe de små og mellemstore virksomheder med at opnå et grundlæggende og forsvarligt niveau af cybersikkerhed.

Rammevilkår

Forslag 5: Styrk regulering af cloud-leverandører og sikkerhed i it-produkter
- Den danske regering skal arbejde for, at der på EU-niveau indføres en cloudforordning, der skal sikre høje krav til cyber- og informationssikkerhed i cloud-løsninger.

Forslag 6: Lovgivning skal målrettes risici – med ordentlige frister
- Cyberregulering skal være fit for purpose og skabe sikkerhed frem for blot compliance.

Kompetencer

Forslag 7: Styrk cyberværnepligten – en investering i Danmarks sikkerhed
- Cyberværnepligten ligestilles med den almindelige værnepligt, så de værnepligtige får elleve måneder i stedet for seks til at opbygge de nødvendige færdigheder til at forebygge og håndtere cyberangreb.

Forslag 8: Cybersikkerhed begynder med mennesker
- Uddannelsesinstitutioner og myndigheder skal samarbejde om at udvide uddannelsesmulighederne inden for cybersikkerhed, samtidig med at kommunikationsindsatsen styrkes for at øge bevidstheden om området.

Cybersikkerhed er en opgave for alle

Cybertruslen er allestedsnærværende, og cyberangreb rammer bredt - fra kritisk infrastruktur og centrale myndigheder til små virksomheder og borgere. Konsekvenserne kan være vidtrækkende og påvirker ikke kun den enkelte, men hele samfundets funktionsevne og tillid. I en dugfrisk publikation fremhæver Styrelsen for Samfundssikkerhed, at udfordringen med cyberhændelser bevæger sig op imod det ekstreme[1].

Fælles udfordring – fælles ansvar
I alle dele af samfundet, på tværs af det offentlige og den private sektor, er der samtidig udfordringer med at sikre et tilfredsstillende cybersikkerhedsniveau.

Derfor skal det fremadrettede arbejde for et cyberrobust Danmark også tage udgangspunkt i hele samfundet. Udviklingen i cybertruslen stiller ikke kun nye krav til staten og virksomhederne, den kræver også, at vi danskere styrker vores digitale kompetencer og sikkerhedsbevidsthed. Samtidig skal indsatsen gå på tværs af det civile og militære.

I F&P hilser vi regeringens udmelding om en ny, ambitiøs cyber- og informationssikkerhedsstrategi meget velkommen. Strategien bør afspejle det ansvar, der ligger på skuldrene af både det offentlige og erhvervslivet og ikke mindst sikre, at vi får de nødvendige rammevilkår til at beskytte Danmark i en stadig mere digital virkelighed. Det er der behov for.

Der er stadig udfordringer med sikkerheden hos en række myndigheder[2] trods mange års fokuseret indsats. Det samme gælder for regionerne[3], hvor Rigsrevisionen for nyligt har konkluderet, at regionerne ikke har gjort nok for at begrænse skaderne af succesfulde cyberangreb.

Hos de danske små og mellemstore virksomheder er der også fortsat et markant udviklingspotentiale. En aktuel analyse viser, at 40% af SMV'erne ikke har et tilstrækkeligt digitalt sikkerhedsniveau[4]. Samtidig er det en kendsgerning, at cyberkriminalitet og digital svindel er noget, der rammer stadigt flere danskere. Eksempelvis steg andelen af digital investeringssvindel med 47,3 mio. kroner i 2024[5], hvilket er en stigning på 99,2% sammenlignet med 2023.

[1] Nationalt Risikobillede 2025, Styrelsen for Samfundssikkerhed, april 2025

[2] Notat om beretning om beskyttelse mod ransomware-angreb, Rigsrevisionen, juni 2024
[3] Statsrevisorerne beretning SB9/2024 - Bilag 1: Beretning nr. 9/2024 om regionernes beskyttelse af sundhedsdata mod cyberangreb, Rigsrevisionen
[4] Digital sikkerhed i danske SMV'er 2024, Styrelsen for Samfundssikkerhed
[5] Investeringssvindel, Finans Danmark

Foruden forsikrings- og pensionsselskabernes selvstændige indsatser for et højt internt niveau af cybersikkerhed, er samarbejdet med myndighederne afgørende for, at branchen er rustet til at imødegå cybertruslen. Derfor deltager branchen aktivt i Finansielt Sektorforum for Operationel Robusthed (FSOR)[6] under Nationalbanken, hvor der samarbejdes om at øge den operationelle robusthed over for cyberangreb i den finansielle sektor.

[6] FSOR: Samarbejde om operationel robusthed, Nationalbanken

Forsikrings- og pensionsbranchen prioriterer cybersikkerheden

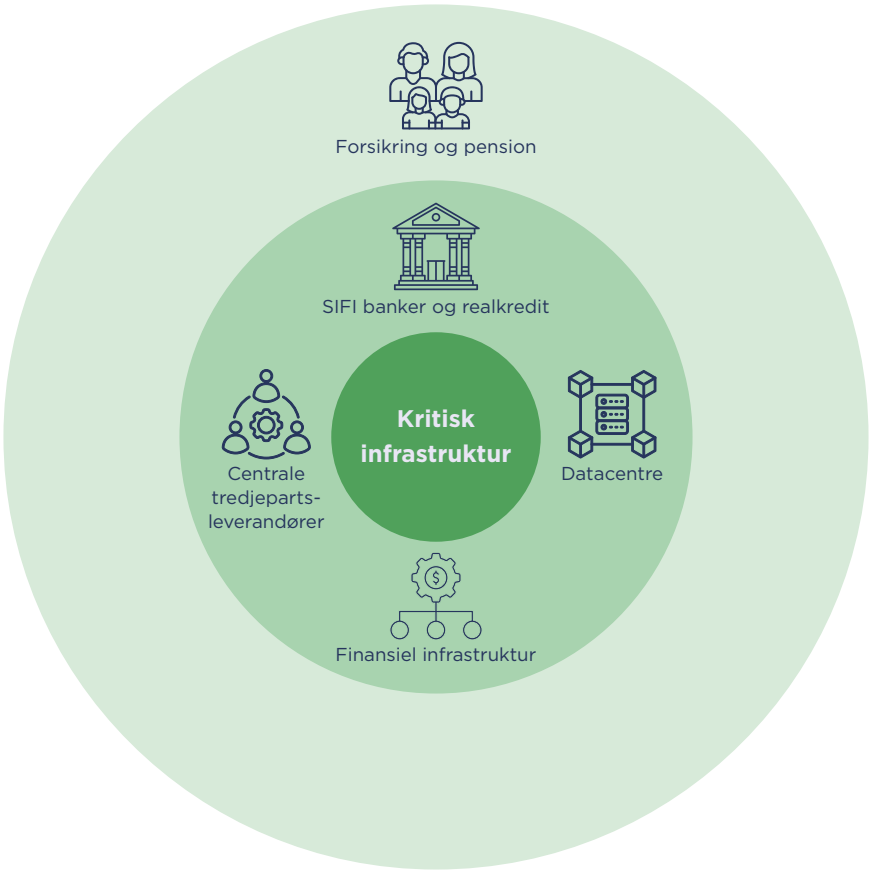
De danske forsikrings- og pensionsselskaber er ligesom resten af det danske samfund gennemdigitaliserede. Der sker stor udveksling af data i samspil med kunder, leverandører, andre finansielle virksomheder og det offentlige. Digitaliseringen og ny teknologi er den største driver til forandring i branchen og er et strategisk konkurrenceparameter.

Den finansielle sektor, som branchen er en del af, er samfundskritisk for Danmark, og angreb eller hændelser i sektoren kan potentielt have alvorlige konsekvenser. Men aktørerne i sektoren er meget forskellige, har forskellige risikoprofiler, og har derfor ikke på samme måde indvirkning på samfundets finansielle stabilitet i tilfælde af en hændelse. De danske forsikrings- og pensionsselskaber udgør ikke kritisk infrastruktur i den finansielle sektor.

Det betyder dog ikke, at branchen ikke er bevidst om dens ansvar. Cybersikkerhed er *license to operate* - også hos forsikrings- og pensionsselskaberne. Der ind- og udbetales store summer og investeres for milliardbeløb. Branchen er derfor et attraktivt mål for cyberangreb og -kriminalitet. Det er således afgørende, at de danske borgere kan have tillid til, at selskaberne kan beskytte deres data og penge, tilstrækkeligt, og at de digitale løsninger, vi bruger, er sikre.

> *Cyberforsikringer går hånd i hånd med den forebyggende indsats hos virksomhederne*

Den finansielle sektor



Derfor arbejder forsikrings- og pensionsselskaberne også ambitiøst og kontinuerligt med at bidrage til et højt niveau af cybersikkerhed, både i branchen, men også ude hos de danske virksomheder og samfundet som helhed.

Branchen bidrager også positivt til at løfte cyberrobustheden hos de danske virksomheder gennem cyberforsikringer. Virksomheder, der tegner cyberforsikringer, er dækket for eventuelle tab, hvilket underbygger økonomisk resiliens i virksomheden og samfundet som helhed.

Derudover understøtter branchen forebyggelsen af cyberangreb som en del af cyberforsikringerne ved at løfte vidensniveauet og bevidstheden om cyberrisici og -hændelser for særligt de små og mellemstore virksomheder. Branchen bidrager bl.a. med løbende kommunikation om viden og indsigt i tendenser for cyberhændelser og cyberforsikringer. På den måde bliver virksomhederne klædt på til, på et oplyst grundlag, at kunne tegne en cyberforsikring eller vælge at bære risikoen selv.

Cyberforsikringer kan være med til at reducere risikoen for virksomheder ved en given cyberhændelse og går derfor hånd i hånd med den forebyggende indsats hos virksomhederne. En afledt effekt ved at forsikre sig mod cyberhændelser er, at robustheden i virksomhederne øges. På den måde kan cyberforsikringer medvirke til at skabe et mere cybersikkert samfund, der i højere grad kan modstå cyberangreb.

Forsikrings- og pensionsbranchen både kan og skal bidrage til det vigtige arbejde, der ligger i at ruste vores samfund til at kunne imødegå cybertruslen. Vi står klar til at understøtte indsatsen for et mere cybersikkert Danmark.

Samfundsrobusthed

Forslag 1: Opret et nordisk-baltisk cybercenter i Danmark

Vi foreslår, at Styrelsen for Samfundssikkerhed går forrest i et nordisk-baltisk myndighedssamarbejde om et styrket cybersikkerhedsberedskab, som skal imødegå truslen fra mulige omfattende cyberhændelser, der kan resultere i store skader på vores kritiske infrastruktur.

Der skal oprettes et grænseoverskridende cybersikkerhedsoperationscenter, beliggende i Danmark, med støtte fra EU, i samarbejde med vores nordiske og baltiske kolleger. Centeret skal anvende avanceret teknologi til at opdage, analysere og derefter dele advarsler om cybertrusler og -angreb på tværs af grænser til relevante offentlige og samarbejdende private aktører. Samtidig skal der etableres et stærkt grænseoverskridende videndelingssamarbejde på tværs af offentlige myndigheder, private aktører og civilsamfundet, så der etableres best practices og viden, som kan komme til gavn i Danmark og på tværs af Europa.

Finansiering af tiltaget vil dels ske gennem EU's program for et digital Europa, hvor der allerede er afsat budget til initiativet gennem Cybersolidaritetsforordningen, dels gennem finansiering i Forsvarsforliget 2024-2033 ved delforligsaftaler på cyber- og efterretningsområdet.

Ved at styrke den fælles situationsbevidsthed om cybertruslen, vil også kapaciteten til at håndtere cybertruslen både i den offentlige og den private sektor blive styrket. Forslaget vil lede til:

- Styrket regional videndeling på cybersikkerhedsområdet
- Styrket fælles regionalt cyberberedskab
- Bedre mulighed for at finde fælles løsninger på fælles udfordringer, fx truslen mod den kritiske infrastruktur, som vi deler med vores naboer
- Understøttelse af et af hovedformålene i Europa-Kommissionens nye hvidbog for EU's forsvar, der går på at skabe cybersikkerhed gennem grænseoverskridende samarbejder.

Den fælles situationsbevidsthed om cybertruslen i den offentlige og den private sektor skal styrkes. Der er et stadig større behov for, at vores nationale myndigheder understøtter den private sektors arbejde med at sikre et højt niveau af cyber- og informationssikkerhed ved at forbedre muligheden for at opdage og håndtere cybertrusler. Behovet er kun blevet større som følge af øget geopolitisk ustabilitet og et trusselsbillede i udvikling.

Forslag 2: Styrk den kritiske infrastruktur og forsyningssikkerheden

Vi foreslår, at der igangsættes en målrettet analyse af, hvor der findes sårbarheder og svagheder i den kritiske infrastruktur – både fysisk og digitalt. Analysen skal give os et klart overblik over, hvor vi er mest udsatte og danne grundlag for et såkaldt "forsyningssikkerhedscheck" med fokus på cybertruslen. Samtidig skal den pege på, hvor vi mest effektivt kan styrke sikkerheden med konkrete tiltag, der er tilpasset de enkelte sektorer.

Styrelsen for Samfundssikkerhed skal stå i spidsen for arbejdet, som skal give myndigheder og virksomheder et fælles og mere nuanceret billede af, hvor der er behov for handling. Et bedre overblik giver bedre mulighed for at prioritere i arbejdet hos myndigheder såvel som erhvervslivet.

Den digitale infrastruktur er afgørende for opretholdelsen af vores samfundskritiske og -vigtige funktioner. Samtidig er den i stadig stigende grad omdrejningspunktet for alt vi foretager os i vores dagligdag. Men den digitale infrastruktur er sårbar. Vores forsyningssikkerhed kan i dag sættes under pres som følge af cyberangreb. For at opretholde forsyningssikkerheden i fx elforsyningen eller den finansielle sektor skal den kritiske digitale infrastruktur være tilgængelig, troværdig og stabil.

Forslaget skal ses i sammenhæng med F&P's forslag til en national udrykkerenhed på kritisk infrastruktur i beredskabsudspillet *Tryghed i Fællesskab*[7]. Her foreslog F&P, at der etableres en national udrykkerenhed for kritisk infrastruktur, der hurtigt kan reagere på angreb mod vores kritiske infrastruktur, fx el-, vand- og kommunikationsnetværk. For at vi effektivt kan beskytte vores samfund, er det afgørende, at vi tænker fysisk og digital sikkerhed sammen. Den foreslåede analyse er derfor et vigtigt første skridt på vejen mod en mere robust og modstandsdygtig infrastruktur.

[7] tryghed-i-faellesskab-2024-et-beredskabsudspil-fra-forsikrings-og-pensionsbranchen.pdf, F&P

Forslag 3: Styrk rådgivning og støtte til virksomheder i kampen mod cybertruslen
Vi foreslår at styrke Styrelsen for Samfundssikkerheds rolle som rådgiver og støttefunktion for erhvervslivet, når det gælder forebyggelse og håndtering af cyberangreb. Der skal udgives flere aktuelle publikationer og vejledninger, fx gennem SikkerDigital, og så skal den operative rådgivning styrkes, så virksomhederne i højere grad kan blive understøttet til at håndtere en hændelse, mens den sker, eller når en ny trussel bliver aktuel.

Virksomhederne står i første række over for cybertruslen mod Danmark. Ved at styrke den løbende og realtidsbaserede kommunikation fra myndighederne, får virksomhederne bedre mulighed for at handle hurtigt og effektivt, samtidig med at de får adgang til brugbar og målrettet rådgivning. Det betyder også, at den viden og ekspertise, som findes hos den nationale it-sikkerhedsmyndighed, i højere grad bliver bragt i spil og omsat til konkret værdi for den private sektor.

I forsikrings- og pensionsbranchen er der et ønske om en mere aktiv indsats fra Styrelsen for Samfundssikkerhed, når det kommer til rådgivning og kommunikation om cybertruslen. I den private sektor har der historisk været en opfattelse af uklarhed om roller og ansvar i relation til den virksomhedsrettede rådgivning fra myndighederne. Med oprettelsen af Styrelsen for Samfundssikkerhed er der nu en oplagt mulighed for at samle og styrke rådgivningen ét sted – på tværs af sektorer – og skabe større klarhed om, hvem virksomhederne kan henvende sig til, og hvad de kan forvente.

Forslaget skal ses i sammenhæng med forslag 1 om oprettelsen af et grænseoverskridende cybercenter i Danmark for nordisk-baltisk samarbejde om situationsbevidsthed.

Forslag 4: SMV-anbefalinger til enkel og effektiv cybersikkerhed
Vi foreslår, at myndighederne udarbejder en række klare og brugbare anbefalinger, der kan hjælpe de små og mellemstore virksomheder med at opnå et grundlæggende og forsvarligt niveau af cybersikkerhed, uden at det kræver store investeringer eller ressourcer. Det skal ikke kun være de store virksomheder, der er godt beskyttet mod cybertrusler – det skal hele erhvervslivet være.

Anbefalingerne skal etableres med inspiration fra Net- og Informationssikkerhedsdirektivet (NIS2), som stiller krav til cybersikkerhed, risikostyring og hændelseshåndtering, men tilpasses virkeligheden i mindre virksomheder. De skal være frivillige og praktisk anvendelige, så virksomhederne kan styrke sikkerheden på en måde, der giver mening i deres hverdag, med fokus på balancen mellem indsats og effekt.

Samtidig bør myndighederne udnytte det arbejde og de midler, der allerede er afsat til vejledning i forbindelse med implementeringen af NIS2 i den offentlige sektor. Med en pulje på 800 millioner kroner frem mod 2033, er der oplagt mulighed for at udvikle materiale og rådgivning, som også kan komme de mindre virksomheder til gode, så de kan høste frugterne af myndighedernes bundne opgave med vejledning.

Næsten 300.000 danske virksomheder står i dag uden for de gældende cybersikkerhedskrav, men de møder de samme trusler som alle andre. Mange af dem har fokus på drift og kundeservice, ikke på it-sikkerhed. Derfor er der fortsat mange virksomheder, som mangler helt basale sikkerhedstiltag.

Ved at gøre det nemmere og mere overskueligt at komme i gang kan vi løfte cybersikkerheden bredt og sikre, at alle virksomheder, store som små, er bedre rustet mod truslerne i den digitale verden.

Rammevilkår

Forslag 5: Styrk regulering af cloud-leverandører og sikkerhed it-produkter

Virksomheder i Danmark og EU er i stigende grad afhængige af cloudløsninger, men leverandørerne er i høj grad uregulerede og markedet domineres af især amerikanske techgiganter. Små virksomheder har ofte ikke reel mulighed for aktivt at sikre tilstrækkelig leverandørsikkerhed (compliance) og de juridiske og geopolitiske udfordringer kan ende som en bremse for brugen af cloud, som ellers er en væsentlig forudsætning for den digitale innovation.

Derfor er vi i dag meget afhængige af de amerikanske leverandører. Denne sårbarhed kan blive en udfordring på sigt. Vi foreslår, at den danske regering skal arbejde for, at der på EU-niveau indføres en cloudforordning, der skal:

- Sikre høje krav til cyber- og informationssikkerhed i cloudløsninger
- Standardisere og regulere cloudtjenester for interoperabilitet
- Flytte dokumentations- og sikkerhedskrav fra kunder til cloud-leverandører
- Etablere tilsyn med leverandørerne ift. produktsikkerhed
- Sikre at ydelser leveres fra datacentre i EU for at sikre forsyningssikkerheden
- Styrke alternative europæiske cloudløsninger.

Initiativet skal skabe en mere robust europæisk cloud-infrastruktur, reducere afhængigheden af amerikanske udbydere og understøtte europæisk teknologisk suverænitet. Den nuværende amerikanske politiske udvikling og usikkerhed om databeskyttelsesaftaler (fx Schrems III) øger behovet for digital autonomi.

Derfor foreslås der en direkte regulering hvor leverandører af software og cloudløsninger får et større ansvar for sikkerheden – ligesom produktansvar i andre brancher – hvilket vil lette byrden for virksomhederne. Dette er i tråd med principperne i GDPR, NIS2 og DORA, men hvor ansvaret i dag i praksis ligger hos kunderne.

For at sikre et højt cybersikkerhedsniveau og fair konkurrencevilkår bør reguleringen foregå på EU-niveau, så cloudleverandører forpligtes til samme standarder på tværs af medlemslandene. Med dette initiativ vil virksomheder få et mere sikkert marked at operere i, hvor det primære ansvar ligger hos leverandørerne – ligesom produktansvar gør i andre sektorer. Samtidig vil det bidrage til, at leverandører arbejder efter de samme klare vilkår for at operere i markedet.

Regulering skal være fit for purpose, og skabe sikkerhed frem for blot compliance

Branchen oversvømmes af regler og krav

- Branchen er blevet ramt af 10.700 siders regler - eller seks sider om dagen - i perioden 2019-2024.
- Pr. juni 2024 var der 154 retsakter eller politikker relateret til cyber- og it-sikkerhed i EU (interface kompendium)[8] - en betydelig del af disse skal forsikrings- og pensionsselskaberne forholde sig til.
- DORA-forordningen, som skal sikre et højt niveau af cybersikkerhed i den finansielle sektor, er alene flere hundrede sider fordelt på niveau 1 og niveau 2 regulering.

[8] navigating-the-eu-cybersecurity-policy-ecosystem (1).pdf, Interface, 2024

Forslag 6: Lovgivning skal målrettes risici – med ordentlige frister

I F&P bakker vi op om at hæve kravene til de finansielle virksomheder, når det kommer til at øge cybersikkerheden i samfundet gennem regulering. Det er dog afgørende, at reguleringen ikke kvæler innovation og konkurrenceevne – værdien af regulering skal stå mål med byrderne.

Den finansielle sektor er samfundskritisk for Danmark, og hændelser i sektoren kan derfor potentielt have alvorlige konsekvenser for Danmark. Men aktørerne i sektoren har ikke på samme måde indvirkning på samfundets finansielle stabilitet i tilfælde af en hændelse. Det gælder for de danske forsikrings- og pensionsselskaber, som ikke udgør kritisk infrastruktur i den finansielle sektor.

Cybersikkerhed er essentiel for samfundet, men der bør ikke blot reguleres for at regulere. Det er afgørende for EU's konkurrenceevne og en rimelig balance mellem sikkerhed og innovation, at ny regulering indføres proportionel. Regulering skal være *fit for purpose* og skabe sikkerhed frem for blot compliance.

Vi foreslår derfor, at proportionalitetskravet i nuværende og fremtidig lovgivning respekteres og bruges aktivt i implementering af lovgivning. Reguleringen på cybersikkerhedsområdet skal være proportionel med de risici, som de forskellige selskaber står overfor, og de traktatfæstede principper respekteres. Reguleringen bliver kun proportionel, hvis der fra myndighedernes side kommer handling bag ordene, når det gælder de politiske mål om reduktion af administrative byrder.

Derudover foreslår vi, at der for fremtidig cyberregulering er længere implementeringsfrister. Det er meget vanskeligt for vores selskaber at efterkomme basisregulering, når niveau 2- og 3-regulering i nogle tilfælde offentliggøres kort før – eller sågar efter - implementeringsfristen. Dette er fx tilfældet med DORA-forordningen, som trådte i kraft 17. januar 2025, men hvor niveau 2-reguleringen endnu ikke er helt på plads. Det kan vores selskaber ikke være tjent med.

I F&P arbejder vi ambitiøst for at få nedbragt de administrative byrder for forsikrings- og pensionsselskaberne. Til gavn for samfundet, vores konkurrenceevne og forbrugerne.

Kompetencer

Forslag 7: Styrk cyberværnepligten – en investering i Danmarks sikkerhed

Vi foreslår, at cyberværnepligten ligestilles med den almindelige værnepligt, så de værnepligtige får elleve måneder i stedet for seks til at opbygge de nødvendige færdigheder til at forebygge og håndtere cyberangreb.

Men det handler ikke kun om teknik. Cyberværnepligtige skal også lære at bruge deres viden i praksis – i organisationer, hvor der arbejdes med risikostyring, procedurer og anerkendte sikkerhedsstandarder som ISO27001 og NIST. På den måde sikrer vi, at de får en helhedsforståelse og bliver til eftertragtede cybersikkerhedsprofiler, både i og uden for Forsvaret.

Vi foreslår samtidig, at Føringsstøtteregimentet aktivt bidrager til at skabe faste og effektive rammer for, at de værnepligtige kan absorberes i det civile erhvervsliv, skulle de vælge ikke at fortsætte i Forsvaret. Der er stor efterspørgsel på cybersikkerhedsspecialister, og de cyberværnepligtige kan spille en nøglerolle i at løfte cybersikkerheden bredt i samfundet.

Selvfølgelig skal Forsvaret have alle muligheder for at fastholde specialisterne. Vores forsvar skal kunne beskytte Danmark og danskerne, når nogen vil os det ondt. Det er dog lige så vigtigt, at de, der vælger en civil karrierevej, får optimale muligheder for at bruge deres viden til gavn for hele Danmark. Et stærkt cyberforsvar kræver samarbejde på tværs af militære og civile grænser.

Med den permanente etablering af cyberværnepligten har vi allerede en stærk platform til at uddanne flere unge med digitale kompetencer, der er afgørende for Danmarks fremtidige sikkerhed og robusthed. Det er nu, vi skal tage næste skridt og sikre, at denne indsats bliver endnu mere ambitiøs, målrettet og værdiskabende – for den enkelte og for samfundet.

Forslag 8: Cybersikkerhed begynder med mennesker
F&P foreslår, at uddannelsesinstitutioner i tæt samarbejde med myndighederne øger udbuddet af uddannelser inden for cybersikkerhed. Det gælder både ved at optage flere studerende på eksisterende tilbud og ved at etablere nye relevante uddannelser. Samtidig skal forskningsmiljøet styrkes, så vi sikrer et stærkt fagligt fundament, der kan udvikle og fremtidssikre området.

Vi anbefaler også, at kommunikationsindsatsen styrkes markant – både nationalt og lokalt - så flere unge og voksne får øjnene op for de mange muligheder inden for cybersikkerhed. Det kan fx ske gennem kampagner, temauger og samarbejde med uddannelsessteder, herunder i regi af den nationale cybersikkerhedsmåned.

Hvis vi skal stå stærkere mod digitale trusler, kræver det et bredt løft af cybersikkerhedskompetencer og digital dannelse i hele samfundet. Vi har brug for flere mennesker med viden og færdigheder inden for cybersikkerhed, og vi skal samtidig nedbringe antallet af angreb, som starter med menneskelige fejl.

Det er positivt, at vi allerede ser nye initiativer på erhvervsakademier og i Forsvaret. Men vi har brug for mere synlighed og kendskab, så flere vælger at uddanne eller efteruddanne sig – eller gå forskningsvejen – i en sektor, der kun bliver vigtigere med tiden.

Vi foreslår også, at virksomhederne i højere grad skal prioritere konkrete tiltag, der kan styrke sikkerhedskulturen. Det kunne fx være obligatorisk cybersikkerhedstræning, foranstaltninger der præmierer god sikkerhedsadfærd, løbende evaluering og vurdering af sikkerhedskulturen samt løbende test.

Samtidig spiller erhvervslivet en central rolle. Vi foreslår derfor, at virksomheder i højere grad arbejder aktivt og målrettet med sikkerhedskulturen fx gennem obligatorisk cybersikkerhedstræning, incitamenter til sikker adfærd og løbende test og evaluering.

I rigtig mange tilfælde starter sikkerhedsbristerne hos os mennesker. Derfor skal cybersikkerhed gøres til en naturlig del af hverdagen, på arbejdspladsen og i uddannelsessystemet. Kun ved at løfte den menneskelige faktor kan vi skabe et mere robust, trygt og digitalt Danmark.

Philip Heymans Allé 1
2900 Hellerup
Tlf. 41 91 91 91
fp@fogp.dk
www.fogp.dk

F&P er brancheorganisation for forsikrings- og pensionsselskaber. Vi varetager branchens interesser og arbejder for, at branchen bliver kendt for sit bidrag til at løse nogle af de største udfordringer, det danske og internationale samfund står over for. Det drejer sig om velfærd og tryghed for den enkelte dansker, og det drejer sig om bæredygtighed og den nødvendige grønne omstilling.