En bättre digital säkerhet

Stärkt cybersäkerhet för nutid och framtid

Centerpartiet

Innehållsförteckning

Inledning

Internets roll som en arena för aktörer som utmanar svensk säkerhet bortom fredstid har blivit allt viktigare. Flera av de omedelbara hoten mot svenska intressen är digitala. Det påverkar såväl svenska företags konkurrenskraft som samhällets funktionalitet och sammanhållning. Samtidigt blir den kriminella ekonomin allt mer digital. Phishing och identitetsstölder drabbar allt fler. Försäljning av droger sker inte i mörka gathörn utan på darknet. På nätet blir det också allt svårare att veta vem som ligger bakom de säkerhetshotande aktiviteterna när oheliga allianser med gemensamma intressen växer fram mellan främmande makts underrättelsetjänster, kriminella nätverk och extremister.

Utvecklingen har pågått i flera år, men den politiska nivån i Sverige har inte svarat upp mot utvecklingen. Sverige ska enligt regeringens strategi vara det land i världen som är bäst på att nyttja digitaliseringens möjligheter. Det är bra. Men det innebär som utgångspunkt också att vi blir det land som blir mest utsatt för digitaliseringens risker. Det ger politiken ett stort ansvar att skapa förutsättningar för en säker digitalisering av myndigheter, företag och medborgare.

Medvetenhet kring frågans aktualitet, komplexitet och potentiella konsekvenser saknas på högsta politiska nivå i kommuner, regioner men också inom regeringskansliet. Det kan ifrågasättas om en statsminister som säger att han aldrig handlat på nätet kan utgöra det ledarskap som behövs för att frågan ska komma högre upp inom Regeringskansliet. Cybersäkerhet är en fråga som hanteras på ett stort antal departement där bristande helhetsbild leder till konkurrens om resurser och mandat mellan myndigheter snarare än fokus på hur samhällsproblem ska lösas.

Sveriges geopolitiska läge och starka innovationskraft gör oss till ett utsatt land. Till de stora underrättelsehoten brukar Ryssland, Kina och Iran pekas ut av Säkerhetspolisen. Men oavsett om det är en stat eller en kriminell gruppering som ligger bakom attacken är det lätt för individer, företag och myndigheter att bli drabbade direkt eller indirekt.

I en händelse av en större cyberkonflikt, antingen som en del av en större konventionell konflikt eller begränsad till den digitala domänen, kommer alla att bli drabbade med potentiellt mycket stora konsekvenser för vårt samhälles funktionalitet, vårt lands handlingsfrihet och enskilda individers integritet.

I ett digitalt samhälle är vi beroende av digitala tjänster för välfärd och vardag. När de facto monopol som BankID inte fungerar kan du inte längre göra digitala betalningar, boka vård eller legitimera dig digitalt. Ju mer digitala vi blir desto mer sårbara blir vi samtidigt. Därför måste kraven på de samhällskritiska funktionerna öka liksom att säkerhetshotande monopol måste undvikas. Kan du legitimera dig med flera tjänster är konsekvensen av en attack mot en enskild tjänst mindre.

Det svåra med IT-säkerhet är inte säkerheten, utan hur den kombineras med att ha fungerande, enkla, öppna tjänster som kontinuerligt är uppkopplade till ett överkomligt pris. Sverige måste digitaliseras för att inte förlora konkurrenskraft och innovation. Men det måste ske säkert. Här har Sverige halkat efter.

> “If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders”
>
> Dan Farmer, IT-säkerhetsforskare, Purdue University

Det är i gränslandet mellan säkerhet och samhällsutveckling som politiska förslag kring cybersäkerhet måste balansera. Det är med den inställning som denna rapport har tagits fram.

Sverige måste fortsätta vara en spjutspets för öppen handel, individuella friheter och digitala tjänster. Skyddet för vårt samhällets säkerhet, att värna befolkningens liv och hälsa, samhällets funktionalitet och grundläggande värden såsom demokrati, rättssäkerhet och mänskliga fri- och rättigheter tar sin början på den digitala arenan. Och för att klara det behövs en sköld som skyddar mot de som vill skada eller utnyttja våra friheter och vår öppenhet.

En god cybersäkerhet är också en konkurrensfördel i en global digital ekonomi. Den som har en robust verksamhet som klarar att leverera även under cyberattacker vinner över den som står still. Den som kan skydda sina hemligheter behåller sina konkurrensfördelar.

Centerpartiet vill att Sverige ska ligga i framkant i den digitaliserade utvecklingen och upptrappningen vi ser på den internationella arenan påverkar alla delar av det svenska samhället. För att Sverige ska kunna möta de komplexa hoten har Centerpartiets internationella kommitté tillsammans med ansvariga riksdagsledamöter gjort ett stort insamlingsarbete och samtalat med en lång rad av Sverige mest kunniga personer inom cyber- och informationssäkerhet från myndigheter, fristående experter och näringsliv men också internationella organisationer inom cybersäkerhet.

Denna rapport bygger på ett stort antal samtal med experter på området, liksom genomgång av litteratur kring cybersäkerhet. Det är genom dessa samtal och kunskapsinhämtning som förslagen i denna rapport har arbetats fram. Därtill har vi läst och tagit till oss olika rapporter på området och satt oss in i olika fallbeskrivningar.

Vår förhoppning är att denna rapport kan bidra till att göra Sverige säkrare och inleda en politisk debatt som sätter cybersäkerhet så högt på agendan som den behöver vara.

Sveriges tillväxt och säkerhet förutsätter att Sveriges förmågor att hantera digitala hot ökar.

Vi är redan under attack. Vi behöver ett starkare digitalt försvar.

Sårbarheter och hot från främmande makt

Systematisk kartläggning, underrättelser, överbelastningsattacker, cyberintrång för att få skyddsvärd information om företag, samhällsviktig verksamhet eller individer, både FRA, Säpo och försvarsberedningen konstaterar att det är de cyberattacker som utförs av statsunderstödda aktörer eller statliga aktörer som utgör de största cyberhoten mot vårt land.

Syftet är att stänga ner samhällsviktig verksamhet, göra oss rädda och minska vår handlingsfrihet. Och alla drabbas; enskilda individer, små företag, stora företag, kommuner och regioner, samhällsviktig verksamhet och statlig verksamhet. Sveriges cybersäkerhet måste förbättras med ett öppet och hållbart samhälle som grund. Ett cybersäkerhetscenter bestående av ett antal statliga myndigheter och cybersoldater hos Försvarsmakten räcker inte. Fler måste göra mer och tänka längre som Säkerhetspolisens chef Klas Friberg uttryckte det när Säpo presenterar sin årsrapport för 2020.

Gapet mellan digitaliseringshastigheten och utvecklingen av cybersäkerhet i Sverige behöver minska. En person med god kunskap sa under ett av våra samtal *”Den stora oron idag är att vi inte gör tillräckligt kvalificerat jobb på bredden i samhället.”* Här finns stor anledning till oro men också möjlighet till bättring, om samhället kraftsamlar.

Det är många länder som har en förmåga att utföra cyberangrepp, ofta med hög uthållighet och samordningsförmåga. Både Ryssland och Kina genomför koordinerade antagonistiska handlingar mot Sverige och kan använda sig av stora resurser för att nå sina målsättningar. Den som har tid, kompetens och resurser kan ta sig in i alla delar av internet. Och dom som gör det är andra länders säkerhetstjänster, underrättelsetjänster och försvarsmakter. Ingen skillnad görs mellan civilt och militärt, offentligt och privat. Ingen är fredad. Det betyder att alla är en potentiell måltavla. Storskaligheten i attackerna kan vara svåra att stå emot också för den bästa. För andra är attacken helt omöjliga att ens upptäcka förrän det är för sent. De aktörer som utför dessa aktiviteter har utrikes- säkerhets- och försvarspolitiska samt ekonomiska syften med sin verksamhet och vill gynna sitt lands intressen.

Försvarsberedningen skriver att konsekvenserna av ett cyberangrepp kan bli lika stora för samhällsviktig verksamhet och kritisk infrastruktur som ett konventionellt militärt angrepp. En skillnad är dock att det kan göras från distans. Genom cyberangrepp kan länderna uppnå sina syftet på ett sätt som ofta är både anonymt och förnekbart. Det är en utmaning för Sverige och andra länder att hantera eftersom det riskerar att leda till att länderna kommer undan med sina attacker.

Det ökande antalet cyberattacker kan sägas vara symptom på de globala geopolitiska utmaningarna. Det är en del i den hybridkrigföring som pågår. Andra medel är påverkansoperationer, desinformation och sabotage. Det är medel som i sig får både större spridning och effekt i en digitaliserad värld.

Angripande länder försöker öka det egna landets handlingsfrihet genom att angripa andra länders sårbarheter, försöka påverka förtroendet mellan ett lands ledning och dess befolkning, tillförskaffa sig information man annars inte hade haft och slå split mellan allierade länder. Komplexa beroenden gör att konsekvenserna av cyberangrepp är mycket svåröverblickbara, och därmed svårhanterliga för den som blir utsatt.

Den starkes rätt, maktpolitik, har blivit viktigare på bekostnad av den nu utmanade multilaterala, regelbaserade världsordning. Sverige, ett litet export- och importberoende demokratiskt land baserat på en kunskapsekonomi, riskerar att bli en av de stora förlorarna om den regelbaserade ordningen går förlorad.

Vårt lands sårbarheter och beroenden kan mycket väl redan vara kartlagt av främmande makt redan idag. Kanske har de till och med en bättre samlad uppfattning om dessa än vad våra egna myndigheter har eftersom någon samlad översyn inte gjorts av svenska myndigheter. Vi utgår som samhälle ifrån att främmande makt inte redan har ett informationsövertag över våra samlade it- och cybersårbarheter. Men det kan man på inget sätt räkna med.

Men det är inte bara utländsk makt som ägnar sig åt aggressiv och subversiv verksamhet, kriminella ligor agerar allt oftare i cyberdomänen och kostar stort lidande hos enskilda utsatta.

De förslag som läggs i den här rapporten kommer många gånger också att minska sårbarheterna och öka skyddet mot den typ av verksamhet också. Ytterst handlar en bättre cybersäkerhet om vår demokrati och hur vi säkrar den från hot i en digital tid samtidigt som vi tar utgångspunkt i människors fri- och rättigheter.

För att förbättra samhällets motståndskraft mot cyberhot på bredden i samhället vill Centerpartiet:

- Se en solidarisk cybersäkerhet i en orolig värld.
- Stärka Sveriges försvar mot cyberattacker.
- Se en cybersäkerhet för hela samhället där näringsliv och det offentliga arbetar tillsammans.
- Skydda den digitala infrastrukturen
- Bygga kompetens på bredden i samhället genom kraftsamling och specialiserade utbildningar både inom studieförbund och universitet och högskolor.

En solidarisk cybersäkerhet i en orolig omvärld

Som vi beskrivit ovan utsätts Sverige och andra länder för statsunderstödda cyberattacker med geopolitiska, ekonomiska och försvarsmässiga syften. De är ofta både anonyma och förnekbara. Det finns en uppenbar risk att länder riskerar komma undan om de vare sig avslöjas eller straffas för sina antagonistiska handlingar. Ett sätt för länder att ändå få kunskap om och kunna veta vem som ligger bakom sådana statsunderstödda cyberattacker är genom underrättelsearbete och samarbete mellan underrättelsetjänster. Men information som fås genom underrättelsearbete kan inte alltid avslöjas vilket bidrar till att det är svårt att peka ut ansvariga, även om underrättelsetjänsten vet vem som står bakom. Det finns också ett politiskt pris för den som pekar ut andra länder som skyldiga.

Det finns dock exempel på länder som har gått ut och avslöjat vilket land som ligger bakom en cyberattack, nämnas kan Norge när Stortinget utsattes för en stor cyberattack där både anställdas och stortingsledamöters e-postadresser utsattes för dataintrång och stora mängder information stals. Syftet var att tillförskaffa sig information om och från norska politiker. En cyberattack som alltså riktades mot demokratins kärna vilket i sig inte är något ovanligt, också Demokraterna i USA har drabbats såväl som Macron i Frankrike. Ryssland nekade inte bara till anklagelserna utan kom också med motanklagelser, skyllde på Norge för att försämra de bilaterala relationerna och dagen därpå genomfördes också en rysk en flygning med strategiskt bombflyg med nukleär kapacitet i norska havet. Inga EU-länder, inte heller de nordiska länderna, ställde upp bakom Norge då de pekade ut Ryssland som ansvariga, vilket lämnade dem ensamma att stå upp mot rysk aggressivitet.[1] Stortinget utsattes för ytterligare ett dataintrång i mars 2021.

Samtidigt saknas ett internationellt regelverk, en digital Genevekonvention, som tydliggör både vad som är acceptabla handlingar i cyberdomänen, men också vad som är en adekvat respons. Tallinmanualen ger en indikation av nuläget men ett större grepp behöver tas. När det saknas tydlighet riskerar en outtalad och icke överenskommen praxis utvecklas som inte gynnar små länders säkerhet. När internationella regler och standarder saknas blir också samarbete mellan länder svårare, både förebyggande, kapacitetsbyggande och responsivt. Mer behöver göras och allt fler länder har en uttalad syn på hur man vill att det internationella samarbetet utvecklas, vilka normer och standarder som vi vill se i ett internationellt regelverk kring cybersäkerhet. Dock inte Sverige. Här måste vidare steg tas, också för att Sverige ska kunna påverka och driva utvecklingen på den internationella arenan.

Det saknas också förtroendeskapande mekanismer vad gäller internationellt cybersäkerhetssamarbete. Länge och tidigare har det funnits många sådana exempelvis inom nedrustningsområdet. På samma sätt som Sverige varit aktiv i det arbetet skulle vi kunna bidra aktivt till att det skapas sådana mekanismer vad gäller cybersäkerhet.

Kostnaden för aggressiva statsunderstödda cyberaktiviteter mot Sverige måste höjas, och det rejält. Det är en del av vårt lands motståndskraft att kunna agera när vi och våra demokratiska grannländer utsätts, i fred, krig och allt däremellan.

[1] Frivärld, 2020. https://frivarld.se/rapporter/den-ryska-cyberattacken-mot-stortinget/

Den solidariska säkerhetspolitiken bör, som vi ser det, omfatta också cyberdomänen och hot och attacker som länder utsätts för på den arenan.

Inte heller Sverige har en historia av att avslöja vilka länder som ligger bakom cyberattacker mot vårt land. Ett undantag är värt att notera våren 2021 är när Säkerhetspolisen pekade ut Ryssland och GRU (ryska militära underrättelsetjänsten) för att ligga bakom cyberdataintrånget mot Svenska Riksidrottsförbundet 2017-2018 där syftet var att svartmåla svenska idrottare som fuskare, och på så sätt sätta sig själv och sina egna dopade idrottare i bättre dager. Eftersom det psykologiska försvaret av Sverige börjar i avslöjandet så är det viktigt att också från politiskt håll vara tydlig med att Sverige utsätts för andra staters cyberangrepp, och att vi har en hotbild mot oss så att medborgarna kan agera utifrån känd fakta. Därtill bör övervägas om ytterligare åtgärder såsom sanktioner och diplomatiska utvisningar behövs i varje enskilt fall. Hade det funnits ett internationellt regelverk och internationella normer hade sådana beslut underlättats. Sverige bör med likasinnade inom Norden, EU och i det transatlantiska samarbetet arbeta för en gemensam ordning så länge ett globalt regelsystem saknas.

Därtill kan man tänka sig att EU på samma sätt som för exempelvis skogsbränder får till uppgift att koordinera enskilda medlemsländers expertresurser inom cyberområdet i det fall ett land utsätts för en omfattande cyberattack som de inte kan klara av själva, och landets myndigheter ber om stöd. Sverige kan också bidra till en solidarisk cyberpolitik genom att både självständigt och inom ramen för EU:s civila krishanteringsmekanism bygga upp ett världsledande digitalt katastrofteam som kan tillhanda kommunikativ infrastruktur i kriser, naturliga kriser såväl sådana som skapats av cyberangrepp, eller krig.

För en solidarisk internationell cybersäkerhet vill Centerpartiet.

- Att statsunderstödda cyberaktiviteter omfattas av den solidariska säkerhetspolitiken.
- Att Sverige oftare och tydligare än idag när vi blir utsatta för omfattande cyberangrepp uttalar vilket land som står bakom när attribuering har varit möjlig.
- Att Sverige ska driva på för att länderna i Norden och inom EU uttalar stöd för och sluter upp bakom varandra vid cyberattacker och när det utsatta landet pekar ut en statsaktör.
- Att Sverige utvecklar en tydlig politik för hur man vill se den internationella rättsordningen utvecklas inom cyberområdet.
- Att Sverige driver på för att en digital Genevekonvention skapas med tydliga normer för lagliga och olagliga aktiviteter och adekvat respons.
- Att Sverige inom ramen för internationella organisationer driver på för att ta fram förtroendeskapande åtgärder inom cyberområdet.
- Att EU får en större roll i frågor som rör standarder kring cybersäkerhet och att EU får till uppgift att koordinera medlemsländernas expertresurser vid större cyberattacker för att hjälpa varandra vid behov vid storskaliga cyberattacker som ett enskilt land inte ensamt kan hantera.
- Att Regeringen uppdrar till PTS att tillsammans med relevanta myndigheter och företag upprätta ett digitalt katastrofteam som på kort varsel kan rycka ut i världen och bygga upp ett kommunikationsnät i kris- och katastrofområden.

Stärkt försvar mot cyberattacker

När statsminister Thorbjörn Fälldin beordrade ÖB att Försvarsmakten skulle hålla gränsen under ubåtskrisen med grundstötningen av U137 i Karlskrona skärgård så hade Sverige förmågan att göra så. Någon riktig gräns går inte att hålla i cyberrymden, men en svensk statsminister måste ha medlen att på ett aktivt sätt kunna skydda kritiska svenska intressen också i den digitala arenan. Kopplingarna mellan infrastruktur, psykologiskt försvar och samhällets totala försvarsförmåga är digitala och avgörs i en digital arena där frågorna hänger ihop. Sverige attackeras varje dag digitalt, det är på tiden vi får förmågor som motsvarar hotet.

Sverige behöver ha en aktiv försvarsförmåga att snabbt kunna skydda viktiga tillgångar, spåra angripare, störa angripare och slå tillbaka mot angripare. Försvarsmakten har idag ansvaret för detta när en statsaktör attackerar och kan genomföra både defensiva och offensiva operationer. De defensiva operationerna syftar till ett försvar av informationssystem för att förneka motståndaren tillgång till att påverka svenska nätverk. Offensiva operationer handlar om att förhindra motståndaren från att genomföra angreppen, bland annat genom att attackera motståndarens system eller genomföra andra aktiviteter som får motståndaren att avbryta attacken.

Sedan 2020 utbildar Försvarsmakten värnpliktiga cybersoldater i samarbete med KTH där värnplikten beskrivs så här: *"Kärnan i arbetet med att förstärka cyberförsvarsförmågan är utökad kapacitet till defensiva och offensiva cyberoperationer mot kvalificerade motståndare i cyberdomänen. Cyberoperationer är en lika självklar del i modern krigföring som mark-, sjö- och luftoperationer och är därmed en naturlig del av det nationella försvaret av Sverige och svenska intressen."* Det är angeläget att cybersoldaterna på sikt blir fler. Den kompetens som de individer då utvecklar kan sedan, förutom att stärka Försvarsmaktens egen kompetens och cyberförmåga, också stärka cyberkompetensen i samhället i stort, exempelvis inom andra totalförsvarsmyndigheter men också inom näringsliv eller kommuner och regioner. Som vi ska se nedan är bristen på kompetens inom detta område skriande.

Det är också vanligt att strategisk kompetens kring cybersäkerhet saknas i olika organisationers ledningar. Det hanteras som en it-fråga vilket inte är tillräckligt. För att belysa ett eventuellt behov av att stärka cyberfrågornas vikt i Försvarsmakten vill Centerpartiet utreda om det finns ett behov av att införa ytterligare en cyber-försvarsgren jämte armén, flygvapnet och marinen.

Under höjd beredskap och krig har staten stora befogenheter att beslagta och förfoga över Sveriges privatägda industri, privatpersoners fordon och andra resurser som fysiskt kan behövas i en krigssituation. Syftet med förfogandelagstiftningen är att stärka Sveriges förmåga att hantera och motstå krig utan att staten självt måste äga all materiell självt. Var och en är en del av totalförsvaret i Sverige. Förfogandelagstiftningen är baserad på fysiska enheter i en materiell värld. Men i och med att krigsarenan har utvecklats till att också omfatta en digital värld är inte bara fysiska utan även digitala resurser avgörande för statens förmågor idag. Lagen om elektronisk kommunikation ger vissa möjligheter kopplat till själva näten, men det är oklart om dessa skrivningar räcker i dagens läge. Vi vill därför se över om förfogandelagstiftningen behöver uppdateras för att också inkludera digitala resurser för krigsföring i cyberdomänen.

De frivilliga försvarsorganisationerna ligger sedan länge Centerpartiet varmt om hjärtat. Alla i Sverige ska kunna bidra till totalförsvaret, också om ens intresse och kompetens i huvudsak inte finns inom det traditionellt militära området, dvs. armén, flygvapnet och marinen. Samhällets förmåga att stå emot och återhämta sig från cyberattacker måste bli bättre. Vi vill därför att ett cybervärn som står på två ben skapas. Ett ben för att bidra till att stärka samhällets förmåga att hantera stora cyberattacker, och ett ben för att stå emot otillbörlig informationspåverkan under höjd beredskap och ytterst krig, dvs. cybervärnet ska också ha uppgifter inom det psykologiska försvaret. På så sätt kan vi också tydliggöra sambandet mellan cyber och psykologiskt försvar. Cybervärnet ska utgöra en aktiv del av totalförsvaret med kompetens som kan nyttjas av olika aktörer som själva saknar tillräcklig kompetens. Det blir en förstärkningsresurs på samma sätt som vissa andra kritiska resurser som frivilliga redan gör inom ramen för de frivilliga försvarsorganisationernas arbete.

En nyckelaktör i Sveriges cyberförsvar är FRA som idag skyddar de mest skyddsvärda verksamheterna. FRA identifierar och följer angripare från utlandet i syfte att skydda Sveriges digitala integritet. Även om FRA fått utökade anslag de senaste åren är utmaningarna som ska mötas fortsatt så stora att ytterligare förstärkningar på sikt kommer behövas.

För att stärka försvaret mot cyberattacker och dess effekter vill Centerpartiet:

- Utöka resurserna på cybersäkerhetsområdet de kommande åren i takt med att försvarsanslagen höjs till 2 procent av BNP.
- Inrätta ett cybervärn med frivilliga med stor IT-kompetens som kan kallas in vid större cyberattacker samt vid höjd beredskap och ytterst krig också för att stödja inom det psykologiska försvaret.
- Öka antalet cybervärnpliktiga de kommande åren i takt med att försvarsanslagen höjs till 2 procent.
- Fortsätta utveckla Försvarsmaktens förmåga till både defensiva och offensiva operationer.
- Utveckla kopplingen mellan cyberförsvar och psykologiskt försvar.
- Tillsätta en utredning om behovet av förfogandelagstiftning inom cyberområdet som träder i kraft vid höjd beredskap eller krig.
- Tillsätt en utredning för att se över ett eventuellt behov av att göra cyberförsvar till en egen försvarsgren.

Cybersäkerhet för hela samhället

Det offentliga är bara en liten del av det svenska samhället. Ska Sverige ha ett bättre skydd är det alltså inte bara det offentliga Sverige som behöver ett bättre skydd. Det är också näringslivet, civilsamhället och inte minst den enskilda medborgaren. Civilsamhällets aktörer måste med in i utvecklingen av de policys som ska säkra medborgarnas rättigheter i den digitala vardagen.

För den enskilda medborgaren är den avgörande insatsen en ökad säkerhetsmedvetenhet. Det krävs kompetenssatsningar brett i samhället. Vi skriver mer om detta i kommande kapitel. Samtidigt måste så klart produkter, såsom exempelvis en mobil etc., som köps in hålla en viss säkerhetsnivå. Idag går det att i handeln köpa smartphones som inte kommer säkerhetsuppdateras efter att den lämnar butiken. Det innebär i praktiken att den säljs med öppna säkerhetshål från dag ett vilket försvårar, om inte omöjliggör, för en enskild individ att kunna skydda sig och sin information. Det samma gäller andra typer av hårdvara, också sådan som köps in av offentliga aktörer. Samhället ställer krav på konsumentsäkerhet på en lång rad områden men inte på säkerhetsområdet. Det är dags att ändra på det och i konsumentlagstiftningen och vid offentlig

upphandling kräva uppdateringsgarantier på tre år eller produktens levnadstid om denna är kortare.

Näringslivet och civilsamhället är avgörande delar av samhällets funktion och även av samhällets beredskap. Utan fabriker som producerar varor och tjänster och utan organisationer som hjälper till i vardagen och stödjer det offentliga blir utmaningar till kriser. Som vi sett det under den pågående pandemin. Därför är näringslivets och civilsamhällets cybersäkerhet också ett nationellt intresse - men ansvar för varje organisation som inte riktigt vet vad som är tillräckligt bra nivå. Statens viktigaste roll är att skapa bättre förutsättningar för dessa organisationer och företag att vara motståndskraftiga samtidigt som förmågan att skapa, utveckla och uppfinna behålls.

Ett exempel på dagens utmaningar är EU-domstolens beslut i Schrems II domen. Alla svenska organisationer som använder molntjänster famlar inför hur de ska agera. Kan man fortsätta använda molntjänster som ägs av företag med bas utanför EU? Ska vi avsluta alla digitala utvecklingsprojekt där molntjänster ingår? Hela vårt CRM-system ligger i molnet, måste vi avsluta det? Det är frågor som ställs över hela Sverige. Men från staten kommer inga riktlinjer. Ska vi ha en fungerande digitalisering där företag och civilsamhälle får möjlighet att agera baserat på krav och hot måste staten, i detta tillfälle genom Integritetsmyndigheten, vara mer konsekvent och snabb i att ge rekommendationer kring aktuella informationssäkerhetsutmaningar.

Vi måste också konstatera att en del av problemet i dagens digitalisering av samhället ligger i samarbetet mellan företag och offentliga organisationer. Antalet havererade IT- och digitaliseringsprojekt är för omfattande för att nämna. Och det kostar miljarder av skattekronor och det kostar på säkerhetssidan. Stockholms Skolplattform är ett i skrivande stund aktuellt exempel där återkommande allvarliga säkerhetshål har negligerats eller hanterats allt annat än skyndsamt. Personer som uppmärksammat säkerhetshålen har uppfattats som motståndare och inte medspelare. Det är en kultur som motverkar säkerheten i systemen.

En orsak till problemen kring skolplattformen och liknande stora system kan vara att samma aktörer som bygger systemen ansvarar för att avgöra om de är säkra. Vid stora och samhällsviktiga IT- och digitaliseringsupphandlingar måste såväl köpare och leverantör ha kompetens att kravställa respektive leverera säkra system. Och dessa krav bör kontrolleras och dokumenteras av en oberoende granskare. På så sätt kan samhället undvika en lång rad allvarliga digitala säkerhetsbrister och stärka it-konsulternas fokus på säkerhet. Ett uppdrag ska även ges till relevanta myndigheter, tex Statens Haverikommission och CERT-SE, att utreda stora IT-relaterade incidenter. Myndigheter som redan idag tar emot incidentrapporter, tex baserat på NIS-direktivet, ska ges i uppdrag att offentliggöra rapporter om det som inträffat för att möjliggöra lärande även utanför den drabbade organisationen.

Näringsliv och civilsamhället besitter både kompetenser och förmågor som det offentliga Sverige inte besitter. Men enligt våra samtal är det tydligt att samarbete och förtroende saknas för varandras kompetens mellan det offentliga och det privata näringslivet.

Civilsamhällets förtroende för staten som garant för frihet och öppenhet är också utmanat. Och särskilt när det kommer till cybersäkerhet är det avgörande att säkra att staten arbetar för att försvara medborgarnas rättigheter - inte utarmar dem. Därför måste civilsamhällets aktörer vara aktiva parter i framtagandet av policy på cybersäkerhetsområdet.

Det är en utmaning för näringslivet att det inte finns EN ansvarig aktör, man vet inte vart man ska vända sig, eller så måste man vända sig till många olika aktörer som i värsta fall säger olika saker. Oklar ansvarsfördelning gör att frågor riskerar som vi skriver ovan hamna mellan departement, budgetposter, ansvarsutkrävande. Vi har under våra samtal fått höra exempel från stora näringslivsaktörer, relevanta branschorganisationer, att de ser ett stort mervärde med att samarbeta med det nya cybersäkerhetscentret, att de har skrivit och föreslagit det men mötts av tystnad. Det är synd för kopplingen mellan centret och privata näringslivet är essentiell, inte minst för att företag äger samhällsviktig infrastruktur.

Det kan möjligtvis ha att göra med att flera av de myndigheter som utgör cybersäkerhetscentret är underrättelsemyndigheter och att det eventuellt präglar deras kultur. Men cybersäkerhetsfrågorna i samhället blir inte bättre av isolering och brist på samverkan. Kopplingen mellan offentlig och privat sektor är oerhört viktig men det offentliga tycks vara så oerhört rädda för att sitta ner och samverka, eller ens samtala. Detta trots att det finns bra exempel på bra samverkan som lett till stor nytta, exempelvis Lindholmen science park. Det riskerar ytterst få konsekvenser både för hur lagförslag utformas och svensk konkurrenskraft, om svenska krav blir högre än inom resten av EU. Staten och det offentliga kan inte lösa allt självt. Näringslivet är avgörande för en hög cybersäkerhet och näringslivets säkerhet en del av samhällets säkerhet.

Att det saknas säkerhetskrav på digitala produkter som enskilda använder, kanske till och med mer eller mindre tvingas att använda såsom Bank-ID så blir det ännu viktigare att de håller en hög säkerhetsnivå. Att en stor mängd produkter utvecklas utan krav på säkerhet möjliggör en ny typ av brottslighet. Och som samhälle har vi accepterat det.

Här skulle fler kunna göra mer. Det gäller inte minst bankernas interna flaggningssystem. Kanske behöver bankerna ha en intern kontrollmekanism eller fördröjningsprocesser när Agda 90 som aldrig förr gjort en utlandsbetalning helt plötsligt vill föra över en miljon kronor till Nigeria. Wishingbrott riktade mot främst äldre för ca 40 miljoner kronor av privatpersoners besparingar ut från landet varje månad. Lägg därtill kontokortsbedrägerier där 99.7% av brotten inte lagförs, och kanske aldrig ens anmäls. I de fall någon döms är straffen låga. I princip innebär det att samhället har avkriminaliserat denna typ av kriminellt beteende. Och det är inte bara enskilda individer som utsätts, också småföretagare som utsätts för cyberangrepp såsom ransomware och intrång är oerhört utsatta.

Brott kopplat till digitalisering är en stor del av dagens brottslighet. Runt 90 procent av alla polisärenden innehåller digitala bevis, med utökningen av IoT kommer den andelen att öka. Men de som utsätts för cyberbrott är hänvisade till den lokala polismyndigheten som inte sällan lägger ner ärendet och som sällan har kompetens att värdera innebörden i cyberbrottslighet. Det gör det också svårt att få en nationell lägesbild över omfattning och konsekvenser. Anmälningsprocessen för cyberbrott måste digitaliseras och anmälningarna gå direkt till IT-brottscentrum under NOA. Idag skrivs det mesta av direkt och många anmäler inte då det är för krångligt.

Sverige är det kanske mest digitaliserade landet i världen. Det gör också att svenska bolag är särskilt utsatta för cyberkriminalitet. Sverige ligger till exempel klart i topp när det kommer till kostnaden för ransomwareincidenter. Men bland

de sämsta när det kommer till att stoppa attackerna innan data krypteras.[2] Det kan också förklara varför svenska företag i mycket större omfattning än företag i andra länder betalar lösensummor för att få tillbaka sin data. Vilket i sin tur ökar incitamenten att attackera Sverige.

Svenska försäkringsbolag betalar generellt inte ut ersättning för lösensummor och cyberförsäkringar är ännu i sin linda. Det kan alltså ha oerhört stora konsekvenser för de företag som drabbas. Ett intrång kostar typiskt tiotals miljoner kronor och kan pågå länge innan det upptäcks. Därför är det också en utmaning att bara 1 av 7 svenska informationssäkerhetschefer rapporterar direkt till VD eller styrelse.[3] Att ge Sveriges företag bättre förutsättningar att skydda sig mot cyberattacker är en avgörande fråga för svensk konkurrenskraft. Samtidigt kan kraven på företagen inte hindra svensk konkurrenskraft så konsekvensen av regleringar blir ett fattigare Sverige istället för ett säkrare Sverige.

Det finns idag ett regeringsuppdrag till polisen att höja förmågan inom organisationen kring cyberbrottligshet. Men IT-brottscentrum måste också få finansiering och bättre it-system för att kunna täcka uppdraget. Det saknas idag. Det innebär att kunskapshöjande insatser uteblir, att utredningar läggs ner och att brottslingar går fria. För Sveriges medborgare och företag är det IT-brottscentrum, och inte cybersäkerhetscentret, som är den viktigaste aktören för att få hjälp mot cyberkriminalitet. Därför kan inte cybersäkerhetscentret ses som den enda spjutspetsen i kampen mot cyberhot.

För att stärka näringslivets och civilsamhällets motståndskraft vill Centerpartiet:

- Förenkla anmälningar av cyberbrottslighet till e-anmälningar som möjliggör nationell lägesbild och hantering.
- Utöka resurserna till IT-brottscentrum.
- Få bankerna att införa kontrollsystem för utlandsbetalningar som avviker från det normala för att försvåra whishingbrott.
- Införa en IT-haverikommission.
- Införa garantier för säkerhetsuppdateringar i digitala konsumentprodukter.
- Ha tydligare kravställning gällande funktionalitet och säkerhet vid upphandlingar.
- Att oberoende säkerhetsgenomgångar blir ett krav vid större upphandlingar.
- Att civilsamhället inkluderas i utveckling av policys som påverkar medborgarnas digitala rättigheter och möjligheter.
- Ny lagstiftning måste ta hänsyn till svensk konkurrenskraft och begränsningar bör helst tas fram inom EU-samarbetet.

Skydda den digitala infrastrukturen

Även om samhället snabbdigitaliserats under pandemin så hamnar Sverige långt ner på OECD digitaliseringsrankningslista och långt efter OECD snittet när det kommer till digitalisering av den offentliga sektorn[4] och vi ligger på plats 52 i National Cyber Security Index. Både Sverige och EU är dessutom extremt

[2] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
[3] https://www.pwc.se/sv/cyber-security/cyberbrottslighet.html.
[4] https://www.pwc.se/sv/cyber-security/cyberbrottslighet.html.

beroende av andra länder för att få tag på hårdvara och eftersom leveranserna sker "just-in-time" principen finns heller inga lager att använda vid stoppade leveranser. I princip ingen produktion finns inom EU. Vi noterar att amerikanska It-jätten Intel nu ska investera 20 miljarder dollar i utökad produktion av halvledare- dvs. microchip, i USA. Det är den globala bristen som gör att produktionen nu plockas hem till USA. Bristen påverkar inte minst bilindustrin.[5]

En mycket stor andel av all hårdvara som används i EU kommer från Taiwan. Taiwan som Kina länge har hotat med militärt våld. Det är inte omöjligt att föreställa sig att Kina skulle lägga exportrestriktioner på Taiwan i händelse av ett väpnat angrepp. Det återstår att se hur Sverige och EU skulle hantera en sådan situation, inte minst om cyberattacker samtidigt slår ut viktig infrastruktur eller applikationer i våra egna länder. Vår förmåga att hantera en sådan situation ter sig i dagsläget som mycket liten. Vi saknar beredskap för det.

På nationell nivå finns i Sverige idag ingen samlad kunskap om hur säkra våra digitala nät och vår digitala infrastruktur är. De stora operatörerna har koll på sina respektive nät men ingen aktör har koll på knutpunkterna eller vad som sker om dessa släcks ned, vilka kaskadeffekter som då kan uppstå eller hur vi ska komma till rätta med dem. Det kan uppenbart vara så redan idag att främmande makt har koll på dessa men att Sverige som land saknar det helt enkelt för att ingen aktör, ingen myndighet eller organisation har ett utpekat ansvar för att ha en sådan lägesbild. Alla de små enskilda problem som kan finnas blir ett främmande-makt-problem för oss om de idag sitter och kartlägger var dessa brister finns.

Vi vet att utländsk makt bedriver kartläggningsverksamhet mot Sverige och att de på olika sätt testar våra system inkl. sårbarheter i vår infrastruktur. Vi måste därför utgå från att informationen redan finns hos främmande makt. Att någon annan kan sitta på en samlad information om sårbarheter och svagheter i vår digitala infrastruktur men inte vi som land är en stor försvars- och säkerhetspolitisk utmaning för oss. Uppenbart riskerar det kraftigt begränsa vårt lands handlingsfrihet vid en stor cyberattack som påverkar samhällsviktig verksamhet. Vi ser behov av att PTS får i uppdrag att genomföra en nationell kartläggning om risker och sårbarheter i fibernäten och noder samt att i en sådan ta ett helhetsgrepp om beroenden och vad som behöver göras för att fibernäten tillsammans ska ge ökad förmåga för alla de aktörer som utnyttjar dem. En sådan kartläggning behöver göras tillsammans med näringslivet som äger mycket av infrastrukturen.

Vattenrening, elförsörjning och andra helt grundläggande delar av samhällets infrastruktur är idag digitaliserade och därmed sårbara mot attacker. Men sårbarheterna testas inte på ett strukturerat sätt och överblick över sårbarheterna saknas. Den kritiska infrastrukturen måste sårbarhetstestas så vi själva känner till bristerna. Våra motståndare testar den redan.

Idag finns tydliga säkerhetskrav på att sjukhus måste ha reservkraft eller att offentliga aktörer ska ha ett brandskydd mm, men det finns inga krav på robusthet i digital infrastruktur. Digital infrastruktur är ett vitalt samhällsintresse och måste beaktas som det. Digitalisering utan krav på säkerhet och robusthet kan få stora konsekvenser för människors integritet, ökar risken för att utländska statsaktörer såväl som kriminella ligor kan få tillgång till information de inte ska

[5] https://www.industrinyheter.se/20210324/31459/intel-bygger-tva-nya-halvledarfabriker-20-miljarder-dollar

ha, ger dem möjlighet att utnyttja säkerhetsluckor för att stänga ner samhällsviktig verksamhet och tjänster vi gjort oss beroende av i vardagen. Människors möjligheter att arbeta effektivt hemifrån påverkas vid störningar. Experter vi pratat med har bedömt att det främst är de underliggande näten, som utgör en svag punkt, en sårbarhet. Det påverkar inte minst människors möjligheter att jobba hemma på ett effektivt och hanterbart sätt när kommunikationen avbryts titt som tätt. Dessutom kostar avbrott både företag och medborgare tid och pengar.

Att det saknas krav på digital säkerhet gör det svårt för bl.a. kommuner och regioner att ställa krav på säkerhet i sin egen digitaliseringsresa, man har inte kunskapen själv inom sina organisationer och olika kommuner ställer olika krav vilket i sin tur gör det svårt för företag att utveckla produkter och delta med ”standard-säkerhetsprodukter” i upphandlingar. Branschorganisationer vi pratat med efterfrågar standarder eftersom det då också blir lättare att utveckla produkter som är användbara för fler vilket de kan tjäna pengar på, och spara tid i en upphandlingsprocess. Centerpartiet har länge, inom ramen för försvarsberedningen, drivit att funktionskrav för samhällsviktig verksamhet ska tas fram. Att det skulle omfatta också den digitala infrastrukturen känns viktigt och nödvändigt.

Samhället digitaliseras också i mångt och mycket utan att hänsyn tas till vare sig hotbild eller förståelse för säkerhetsbehov, inte minst inom offentlig sektor. Snarare är det vanligt att nya system utvecklas och när det är färdigt så tänker man säkerhet, men då är det ofta för dyrt eller komplext för att göra någonting åt det. Istället vill man få ut sin nya produkt, exempelvis en app. En expert vi pratat med beskrev det som att många incidenter är onödiga, både systemmässigt och kompetensmässigt. Vi bygger helt enkelt för dåliga IT-system där inställningen ofta är följande: *“Snälla vi har precis fått systemet att fungera - ställ nu inga säkerhetskrav på oss”.* Teknologiutvecklingen går framåt, och sen lägger vi i bästa fall på säkerhetsperspektivet efteråt. Inte undra på att gapet mellan digitalisering och cybersäkerhet ökar. Fler aktörer måste på bredden se den vardagliga nyttan för medborgaren med ett integrerat cybersäkerhetsperspektiv i det fortsatta digitaliseringsarbetet. Det är de minsta, men viktiga aktörerna, som inte har kraft att komma ikapp och minska det gap som ständigt vidgas. Här borde staten kunna stödja i större utsträckning än idag. Inte minst i arbetet med att formulera grundläggande funktions- och säkerhetskrav. Det hade underlättat också för kommuner och regioner när de utvecklar nya IT-system och produkter i takt med att samhället digitaliseras. Hade sådana funnits hade det också varit lättare för näringslivet att utveckla produkter att använda sig i utvecklingen av nya tjänster och produkter.

En del i ett robust samhällssystem är att ha redundanta system. Idag har Sverige en monopolberoende på flera områden. Ett tydligt sådant exempel är Swish som har de facto monopol på digitala mobila betalningar idag. I vissa länder finns det ett flertal tjänster att välja bland vilket minskar risken för att inte kunna betala. BankID har också nästan monopol och Försäkringskassan godkänner till exempel enbart identifiering via BankId. Möjligheten att hantera välfärden ligger i händerna på en monopoltjänst från bankerna som dessutom inte accepterar alla som behöver interagera med offentlig sektor som kunder. Digitala betalningar och offentliga tjänster måste vara tillgängliga för alla och via mer än en enskild digital identitetslösning. Staten bör även ha en egen identifiering utöver att det ska vara öppet för andra aktörer.

De senaste åren har cyberattacker mot sjukvården runt om i världen stängt ner kliniker, ambulanssystem och hela sjukhus. Det har kostat liv och miljarder och gett kriminella aktörer möjlighet att tjäna stora pengar genom att utpressa både sjukhusledningar och enskilda patienter genom att antingen ta kontroll över

systemen eller genom att hota läcka personlig och integritetskänslig information som de stulit. En vanlig metod är att skicka mejl som verkar vara helt legitima som när de öppnas försätter vitala sjukvårdssystem i känsligt läge, stänger ner journalsystem eller stjäl information om patienter eller för politiska syften. Man har också sett att cyberattackerna allt mer riktar in sig på vitala styrsystem i sjukvården, exempelvis olika livsuppehållande apparater. En angripare som kommer åt en hjärt- och lungmaskin har direkt påverkan på en människas liv och död. Samtidigt ser vi att säkerheten inom vårdsektorn inte följt med digitaliseringen. Samtidigt som ansvaret för cybersäkerheten ofta legat hos drifttekniker, som dessutom haft det som en tillikauppgift och heller inte fått rätt utbildning eller förutsättningar att veta hur de ska agera om en attack faktiskt sker, hur incidentrapporteringen ska gå till osv.[6]

Det har också visat sig svårt att ställa rätt krav, att veta vad som är rätt krav vid upphandlingar. Idag finns i Sveriges regioner flera kritiska system, livsviktiga system som drivs av operativsystemet Windows XP. Problemet är att Windows XP inte längre uppdateras och dessutom innehåller flera kända sårbarheter. Samtidigt sätter juridiken stopp för att sjukhusen/regionerna uppdaterar programmen själva. Det betyder att svensk sjukvård sitter på extremt sårbara och osäkra system som de inte har råd att byta ut samtidigt som de inte får uppdatera dem själva. Livslängden på sjukvårdssystemet är längre än på operativsystemet. Idag saknas i Sverige också best practices på hur man i framtiden undviker att liknande situationer uppstår. Här menar vi att det nyinrättade cybersäkerhetscentret bör kunna göra mer för att sprida information om detta och stödja regioner och andra aktörer.

Att det i stort saknas krav på säkerhet och robusthet gör det också svårt för enskilda företag att veta vilken säkerhetsnivå de själva ska lägga sig på. Och andra sidan, om staten skulle ställa allt för specifika, hårda krav på säkerhet som inte återfinns på EU-nivå, så kommer svenska företag drabbas av konkurrensnackdelar. Det är viktigt att utforma statliga krav på säkerhet i ett helhetsperspektiv och att liknande regler gäller i andra länder och också beakta andra perspektiv såsom integritet och tillgänglighet, som vi skriver ovan.

För att höja säkerheten i digital infrastruktur och digitaliserad samhällsviktig verksamhet vill Centerpartiet:

- Uppdra åt PTS att genomföra en utredning om sårbarheterna i fibernät och noder
- Ta fram minimistandarder och funktionskrav för samhällsviktig verksamhet.
- MSB/SÄPOs rekommendationer för best practices utvecklas, förtydligas och anpassas så flera olika typer av organisationer har förutsättningar att följa rekommendationerna.
- Kritisk infrastruktur måste sårbarhetstestas löpande. Ansvar för detta ges till respektive expertmyndighet.
- Monopol och “single point of failure” i den digitala infrastrukturen ska undvikas.

[6] David Lindahl, FOI på Folk och Försvars rikskonferens 2021.

Stärkt kompetens kring cybersäkerhet

Det saknas idag kompetens och förståelse för den digitala hotbilden mot Sverige, både i det politiska systemet, i näringslivet och på bredden i samhället. Kompetensbrist och långsiktig kompetensförsörjning är utmaningar som lyfts tidigt av i princip alla som vi pratat med i framtagandet av den här rapporten. Problemen beskrivs som skriande och akuta. USAs Department of Defence har kallat avsaknaden av kompetens ett nationellt säkerhetsproblem.[7] Problemet är inte mindre i Sverige.

Det saknas kompetens både på bredden och spetsen i samhället för att kunna minska det ständigt vidgade glapp som finns mellan en accelererande digitalisering och en god cybersäkerhet. Både det politiska systemet, offentlig sektor och allmänheten i övrigt ligger i mångt och mycket efter i förståelse för den faktiska hotbilden, och åtgärderna och skyddet är inte heller dimensionerade för den hotbild vi ser. Sverige ligger idag långt ner på internationella rankningar när det gäller cybersäkerhet.

Att samhället lider av kompetensbrist inom området är också någonting som uppmärksammats av ett stort antal myndigheter under många år. Faktiskt också av regeringen i den nationella informations-och cybersäkerhetsstrategin, men ytterst lite konkret har hänt därefter. Upphandlingar av digitala tjänster sker till exempel fortfarande ofta utan adekvata säkerhetskrav. Framträdande exempel inkluderar Transportstyrelsen, Stockholms Skolplattform och 1177 där säkerhetsbrister i alla tillfällen har lett till att integritetskänslig data har eller har kunnat bli tillgänglig för parter som inte har rätt att se den.

Många offentliga och privata organisationer inser först värdet av en hög nivå på sin digitala säkerhet när de redan har fått stora problem. Efter att världens största shippingföretag, Maersk, förlorade över 300 miljarder kronor på NotPetya attacken deklarerade VDn att de först då insåg hur viktigt det är med en solid säkerhet i de digitala systemen. Det är en händelsekedja som går igen i många verksamheter, offentliga som privata.

***CASE* NotPetya: Rysk attack mot Ukraina får stora effekter på världshandeln**.*
I 2017 genomförde Ryssland en cyberattack mot Ukrainas samhällsfunktioner. Den statliga hackergruppen Sandworm använde ukrainska redovisningstjänsten MeDoc till att störa ut allt från banktjänster och sjukhus till energisektor och polisen. MeDoc användes av 9 av 10 ukrainska företag till att redovisa skatt och genom att skicka en snabbtspridande kryptomask som krypterade de drabbade datorerna kunde Ryssland förstöra stora delar av den civila infrastrukturen i Ukraina i ett slag. Men ett virus känner inte till gränser. Ett av företagen som använde MeDoc var danska shippinggiganten Maersk som förutom att äga olja- och gasproduktion och hamnar hanterar cirka en femtedel av all global varutransport till havs. Viruset kom via Maersks interna nätverk ut i alla kontoren i hela världen och stängde ner alla servrar och datorer. Över 40 000 datorer och 4 000 servrar fick raderas och förstöras. All data om behörigheter låg på infekterade servrar. Enbart en domänkontrollserver i hela Maersks globala

[7] https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND-DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

verksamhet överlevde attacken. Den stod i Ghana och hade inte blivit infekterat på grund av att det hade varit elavbrott. Kostnaden för enbart Maersk var på över 300 miljoner dollar. Totalt drabbades ett okänd antall personer och företag i över 60-talet länder. I Sverige drabbades APM Terminals i Göteborgs hamn av störningar i system för leveranser och hanterande av gods. Verksamheten fick avslutas då systemen var utslagna samtidigt som det pågick en strejk.

Att stärka kompetensen inom cybersäkerhet handlar inte enbart om att få fram fler specialister i IT-säkerhet. Cybersäkerhet är mycket mer än en IT-fråga, det är en kulturfråga. Det handlar om att var och en i vårt land behöver känna till hur de kan skydda sig mot cyberhot inkl. cyberbedrägerier som idag drabbar många människor. Ett phishingmejl där någon utger sig för att vara din VD eller ditt barnbarn kan fortfarande få många att avslöja hemligheter, ladda ner komprometterande filar eller värre. Det finns exempel där phishingmejl har lett till överföringar av hundratals miljoner kronor från företag till bedragare. Phishing, social engineering och liknande tekniker fungerar för att vi som människor vill lita på folk och vara effektiva. Det är enkelt att utnyttja om vi inte alla är medvetna om riskerna för att bli utnyttjade.

Precis som alla nu under Covid-19 vet att det är viktigt att tvätta händerna ofta för att förebygga smitta ska alla i vårt land veta vad de ska göra för att kunna skydda sig exempelvis mot phishing eller hur de kan formulera ett säkert lösenord. Det ska också veta varför det är viktigt. Det behövs kompetensstrategier för bredden och spetsen i samhället, som höjer kunskapen hos enskilda medborgare, bredden i offentlig sektor och näringsliv såväl som hos beslutsfattare inkl. den politiska nivån.

“Brist på relevant kompetens inom cybersäkerhet är ett samhällsproblem”[8]

FRA, Försvarsmakten, MSB, Polisen, SÄPO

Inom näringsliv och offentlig sektor är en utmaning inte sällan att det saknas förståelse och insikt om att cybersäkerhet inte endast är en säkerhets- eller IT-fråga utan en strategisk ledningsfråga och behöver hanteras som det också. För ett framgångsrikt cybersäkerhetsarbete krävs förståelse för frågan i en organisations alla funktioner, inte minst ledningsnivå men också bland jurister, analytiker, ekonomer, upphandlingsexpertis, registratur m.fl. behöver alla ha kunskap om och kunna förhålla sig till vad som är skyddsvärd information. Idag saknas som sagt ofta cyberkompetens på ledningsnivå, men därtill i de fall förståelse finns, förmår eller har mellancheferna inte rätt förutsättningar att omsätta övergripande inriktningar i resten av organisationen. Ett generellt kunskapslyft om informationssäkerhet och cybersäkerhet behövs inom de flesta organisationer. Finns ingen förståelse för vikten av systematiskt informations- och cybersäkerhetsarbete hos allt från en organisations registratur och vaktmästeri till högsta ledning så ökar risken för brister och att vi utsätter verksamheten för risker och samtidigt ökar våra egna sårbarheter.

Inom området nationell säkerhet finns idag förvisso kompetens om både hot och sårbarheter och det är också här som satsningar har gjorts senaste åren i form av inrättandet av ett antal cybersoldater inom Försvarsmakten och etablerandet

[8] https://www.sakerhetspolisen.se/download/18.f2735ce171767402ba202/1591164566288/Rapport-Cybersakerhet-Hot-Metoder-Brister.pdf

av ett nationellt cybersäkerhetscentrum. Men på sikt är kompetensförsörjningen en stor utmaning också här.

Det samma gäller inom polisen där polisutbildningarna idag inte inkluderar cyberbrott. Det gäller både de de grundläggande polisutbildningarna och i stort även vidareutbildning inom polisen. Trots att det redan är en stor del av polisens arbete och dessutom starkt växande. Det måste ändras.

Centerpartiet anser sedan länge att det finns en kraft med stor spridning i folkrörelserna, inte minst studieförbunden och vi tror att de kan ha en viktig roll i att höja kompetensen på bredden. Därtill lägger Centerpartiet också värde i YH-utbildningar och vi ser en potential i att de också utvecklar och breddar sitt erbjudande. Vi tror också på och uppmuntrar initiativ för att fånga upp och sprida intresse för cybersäkerhetsfrågorna hos ungdomar. Här skulle exempelvis Försvarshögskolan kunna få uppdraget att genomföra nationella tävlingar för både universitetsstudenter och gymnasiestudenter där prestige byggs genom priserna, exempelvis stipendier eller att representera Sverige i internationella tävlingar.

För spetskompetens kring frågorna kan mycket mer också göras i vårt land, inte minst inom högre utbildning så att jurister, ekonomer, civilingenjörer, statsvetare etc får en tydlig inriktning och möjlighet till fördjupning och expertkompetens på området. Obligatoriska utbildningar för beslutsfattare kan vara en väg framåt. Vi måste bort från synen att cybersäkerhet är en IT-fråga. Här kan vi jämföra vårt land med flera andra länder som kommit längre. Frankrike har exempelvis annonserat en miljard euro på cybersäkerhet, varav hälften på forskning, efter att flera sjukhus har varit utsatta för attacker. Vi behöver även i Sverige göra mer som nation i gränslandet forskning, innovation och utbildning. Vi föreslår därför etableringen av ett cybercampus där frågorna får möjlighet att utvecklas i en helhet. Cybercampus existerar redan idag i Norge, Tyskland, Schweiz och alla dessa länder satsar kraftigt på forskning och utveckling kring cybersäkerhet. Sverige borde inte vara sämre.

För att öka förståelsen, kunskapen och kompetensen på bredden och spetsen på kort och lång sikt i samhället vill Centerpartiet:

- Bredda kompetensen i samhället via civilsamhället, exempelvis ge studieförbunden i uppdrag att folkbilda om grundläggande cybersäkerhet, hot och risker.
- Se fler yrkesutbildningar inom cybersäkerhet, exempelvis YH-utbildningar som berättigar till CSN-lån.
- Etablera ett cybercampus för att stärka forskning, utbildning och innovation kring cybersäkerhet.
- Att det tas fram kompetensstrategier för att säkerställa en miniminivå av kunskap om cybersäkerhet i offentlig sektor samt fördjupade och obligatoriska utbildningar för beslutsfattare.
- Få etablerat masterutbildningar inom cybersäkerhet.
- Se ett traineesystem inom statliga myndigheter inom totalförsvaret samt relaterade företag som bemannas av personer som gått masterutbildningar enligt ovan.
- Upphandlingsmyndigheten ges i uppdrag att skapa ett digitalt stödverktyg till användning vid upphandlingar för att förenkla upphandling av säkra digitala tjänster.
- Utreda om arbete med vissa uppgifter ska förutsätta certifiering av kompetens inom cybersäkerhet.

- Stödja olika initiativ till att sprida information och medvetenhet om cybersäkerhet.
- För kunskap om cyberbrottslighet in i polisutbildningarna på alla nivåer.