AMCHAM

AMERICAN CHAMBER OF COMMERCE IN SWEDEN

The Home of American Business

Introduktion

Amerikanska handelskammaren i Sverige (AmCham) är den enda handelsorganisationen som arbetar för att främja Svensk-Amerikansk handel och investeringar. AmCham's medlemmar består av fler än 160 svenska och amerikanska bolag. AmCham representerar därför många av de största amerikanska bolagen i Sverige. Totalt skapar amerikanska bolag i Sverige ca 63,550 jobb årligen, bidrar med 634 miljarder SEK i utländska direktinvesteringar samt 262 miljarder SEK i export och import av varor och tjänster. Med anledning av regeringens arbete med att ta fram en ny nationell cybersäkerhetsstrategi har AmCham sammanställt synpunkter från våra medlemmar kring detta och med följande förslag:

Teknikutveckling, forskning och innovation

Sverige har en rik tradition av forskning, utveckling och innovation inom den teknologiska sektorn samt en stark försvars- och techsektor. AmCham's medlemsbolag har också investerat miljarder i säker digital infrastruktur i Sverige. Detta ger Sverige starka grundförutsättningar för att ta en större roll inom cybersäkerhetsområdet, inte minst i sin kommande roll som fullvärdig NATO-medlem.

NATO

Natomedlemskapet, liksom kommande EU-direktiv som *Network and Information Security Directive* (NIS2), kommer att ställa högre krav på Sveriges beredskap och därför bör fokus läggas på bland annat stabila resilienta civila kommunikationssystem för att säkerställa landets beredskap för de utmaningar som kommer med medlemskapet.

Partnerskap

Inför växande cyberhot har beslutsfattare lagt fram en ambitiös policyram för att bygga cyberresiliensen hos kritisk infrastruktur i Sverige och Europa. För effektiv implementering bör partnerskap med pålitliga offentliga och privata partners prioriteras. För att Sverige ska kunna ta en ledande roll inom cybersäkerhet bör man se till att integrera sig med vänner, där exempelvis dataflöden mellan allierade länder ses som en styrka snarare än en svaghet, där regler och standarder utvecklas tillsammans med allierade och en modern förståelse av resiliens. Detta bygger på erfarenhet från exempelvis kriget i Ukraina där amerikanska företag har jobbat nära landets regering för att rädda några av deras viktigaste samhällstjänster.

AI

I framtidens cybersäkerhet är AI en integrerad del för vår förmåga att förebygga, upptäcka och hantera cyberhoten. Tillämpad AI inom cybersäkerhetsområdet för ökad reseliens är ett högst relevant område att belysa när man pratar om cybersäkerhet. AI bör därför hanteras i strategin både som en möjlighet men även ur aspekten att AI kan utnyttjas för cyberhot.

Box 190, SE-101 23 Stockholm, Sweden | Klarabergsviadukten 63, Stockholm, Sweden
Tel: +46 8 506 126 10 | Org. No. SE 8020171883
info@amcham.se | amcham.se

Utbildning och kompetensförsörjning

För att kunna hantera den föränderliga cybersäkerhetsmiljön och ett omfattande regelverk måste regeringen bygga en kvalificerad arbetsstyrka. Detta innebär partnerskap med den privata sektorn, civilsamhället och den akademiska världen för att dela kunskap om cybersäkerhetsbehov på arbetsmarknaden, utbildning och attrahera talanger.

Utbildning

Det är positivt att regeringen satsar stort med exempelvis inrättandet av ett cybersäkerhetscampus. Därutöver tror vi att man också kan göra mer för att utbilda i cybersäkerhet tidigare, till exempel redan i grundskolan. En effektiv cybersäkerhet är integrerad i arkitekturen och därför förordar vi att cybersäkerhet blir obligatorisk kurs inom alla tekniska vidareutbildningar. Vi rekommenderar även att myndigheten för samhällsskydd och beredskap (MSB), samt andra myndigheter som ansvarar för viktiga säkerhetsfrågor bör bidra till effektiva sätt att höja medvetenheten om informations- och cybersäkerhetshoten genom att bedriva ett långsiktigt och effektivt informationsarbete.

Kompetensförsörjning

Viktigt för kompetensförsörjning är även tillgången till ledande teknik. Den spetskompetens som Sverige vill attrahera och behålla drivs ofta av möjligheten att arbeta med ledande teknologiska verktyg och Sverige måste därför försäkra sig om att marknaden är öppen för dessa. Det gäller även offentlig sektor, där lönerna ofta är mindre konkurrenskraftiga, ett sätt att locka talang kan därför vara intressanta arbetsuppgifter som drivs av stora datamängder, tillgång till ledande teknologi och den samhällsnytta talangen kan bidra med.

Exempel från Europa:

Mindre offentliga organisationer i Sverige kan ibland ha svårt att genomföra de utvärderingar som behövs för att upphandla ledande teknologiska säkerhetslösningar. De kan därför stödjas genom att man från nationellt håll tillhandahåller ett upphandlingsstöd där digitala tjänster certifieras via en nationell myndighet. Här rekommenderar vi speciellt att kolla på Finlands erfarenheter med det såkallade *PiTuKri*.

En annan strategi som Finland och andra länder använt är en såkallad Cloud First-policy, där all data lagras i molnet om det inte finns någon legitim anledning att låta bli. Detta har hjälpt länder då man i molnet kan uppnå en säkerhet som är svår att uppnå i såkallade ’on-prem’-lösningar. Cloud First rekommenderas till exempel av Storbritanniens NCSC och landets försvarsdepartement som en väg till ökad cybersäkerhet i offentlig sektor.

Den offentliga sektorns cybersäkerhet skulle också kunna tjäna på en tydlig dataklassificering som är enkel att implementera. Här rekommenderar vi att studera Storbritanniens erfarenheter med ett system i tre nivåer, där offentliga organisationer enkelt kan kategorisera sin data och sedan vet hur de kan lagra och bearbeta datan inom respektive nivå.

För samhället i allmänhet, inklusive privat sektor, är det viktigt att påpeka att många cyberattacker inte är så sofistikerade och därför kan förhindras genom ett antal enkla steg. Här

vill vi tipsa om Storbritanniens 'Cyber Essentials' som är ett enkelt program med fem komponenter som företag kan certifiera sig via och som stöds av den brittiska regeringen.

Former för samverkan inom området

Vi välkomnar Sveriges ökade ambitioner inom cyber, där man inte minst satsar mer på det nationella cybersäkerhetscentret (NCSC). För att utveckla formerna för hur myndigheterna och privata företag och organisationer samverkar och delar information om säkerhetshot rekommenderar vi att man ser över befintliga nätverk och utvecklar fler nätverk för samverkan mellan företag och offentlig sektor.

Samordning

Vi uppmanar staten att samordna inom informations- och cybersäkerhet för att undvika att företag behöver rapportera incidenter eller vidtagna åtgärder till flera myndigheter. Vi förordar även inrättandet av en "one-stop-shop" för cybersäkerhetsrapportering som omfattar olika bestämmelser, för att förenkla efterlevnad och administrativ rapportering samt säkerställa att cybersäkerhetsvarningar delas över hela EU på ett begripligt och kostnadseffektivt sätt.

När Sverige nu gått med i NATO blir den redan goda relationerna med USA:s Cybersecurity and Infrastructure Security Agency (CISA) och deltagandet i Joint Cyber Defense Collaborative (JCDC) en styrka. I det fortsatta samarbetet med allierade, kan Sverige fortsätta samverka genom införandet av såkallade 'secure-by-design-and-default'-strategier, som rekommenderats av USA:s CISA och implementerats av t.ex alla Five Eyes-länder, Tyskland och Nederländerna.

Samarbete inom EU

EU bör arbeta för harmonisering av befintlig politik – på nationell nivå och EU-nivå. Detta inkluderar ömsesidigt erkännande av standarder med likasinnade partners och effektivisering av internationella initiativ för produkt- och leveranskedjors säkerhet – som exempelvis *Software Bill of Materials* (SBOM). Sverige kan fortsätta spela en viktig roll inom EU genom att verka för harmonisering med allierade, till exempel i *Cyber Resilience Act* (CRA), *Cyber Security Act* (CSA) och *European Union Cybersecurity Certification Scheme on Cloud Services* (EUCS). Här skulle EU:s cybersäkerhet tjäna på att inkludera även aktörer från länder utanför EU.

AI

Även inom området AI, som kommer kunna vara en stor tillgång för att implementera och rapportera cyberkrav enligt direktiven, är det viktigt att jobba med allierade och till exempel se till att datalokaliseringslagar inte står i vägen för tillgången till ledande teknologi. Framgent kan Sverige också driva en större regulatorisk konvergens inom EU, där regelverk som CRA, CSA, Digital Operational Resilience Act (DORA) och NIS2 täcker liknande områden och därför kan centraliseras/konsolideras. Vi vill även understryka vikten av transparens och tillförlitlighet när det kommer till användningen av AI inom cybersäkerhet. Det kräver öppna standarder och integrationer för att teknik och lösningar från olika leverantörer ska fungera tillsammans.

Informationsdelning i vardagen samt vid större cyberhot och it-incidenter

Vi förespråkar ett utvecklat samarbete mellan staten och näringslivet, genom bland annat mer dubbelriktad information, för att stötta företag och organisationer avseende informations- och cybersäkerhet. Det nuvarande säkerhetsrapporteringsarbetet kan berikas av att näringslivet får ta del av information och resultat av myndigheternas arbete med informations- och cybersäkerhet. I många fall besitter näringslivet information och kunskap som skulle öka säkerheten för fler aktörer om rätt förutsättningar kom på plats för att dela denna information under trygga former.

Vi förespråkar även stärkt förmåga hos statliga, kommunala och regionala myndigheter inom informations- och cybersäkerhet, bland annat i offentliga upphandlingar och i övrigt samarbete med den privata sektorn med offentlig IT-drift.

När cybersäkerhetslagstiftningen går in i implementeringsfasen är det viktigt att göra den flexibel för nya och framväxande hot. I takt med att teknik som AI och kvantdatorer blir allt vanligare är det väsentligt att samarbeta med teknikleverantörer för att förstå hur cybersäkerheten påverkas samt anpassa politiken för att göra den framtidssäker. I synnerhet bör integrering av post-kvantumkryptografi vara en del av de aktuella revideringarna av cybersäkerhetsstrategin.