Vad man behöver tänka på och vad som är viktigt vid upphandling av moderna IT- och molntjänster,

- speciellt inom offentlig verksamhet.

Anders Jonsson, Member Enisa AHWG EUCS

Kort om mig:

Anders Jonsson

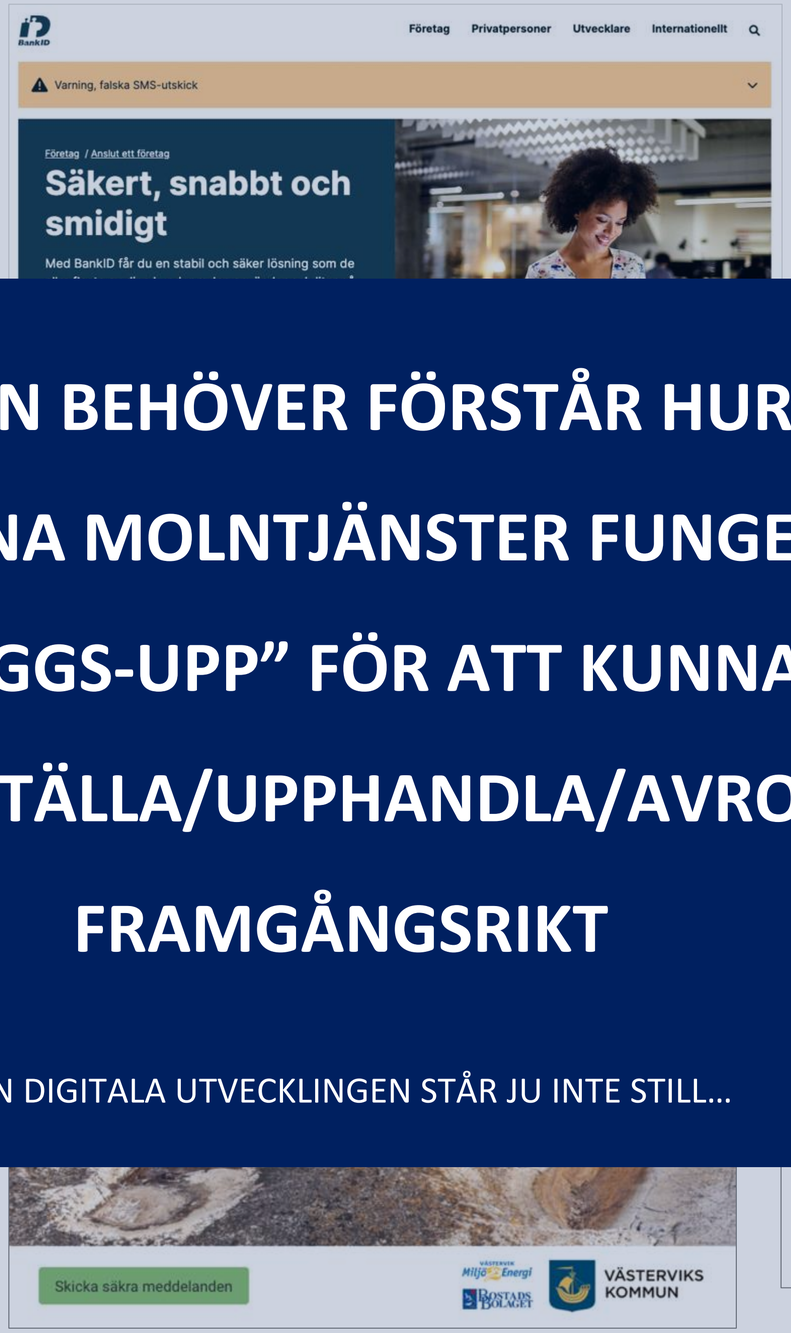
Mob: +46708655301
anders@securemailbox.com

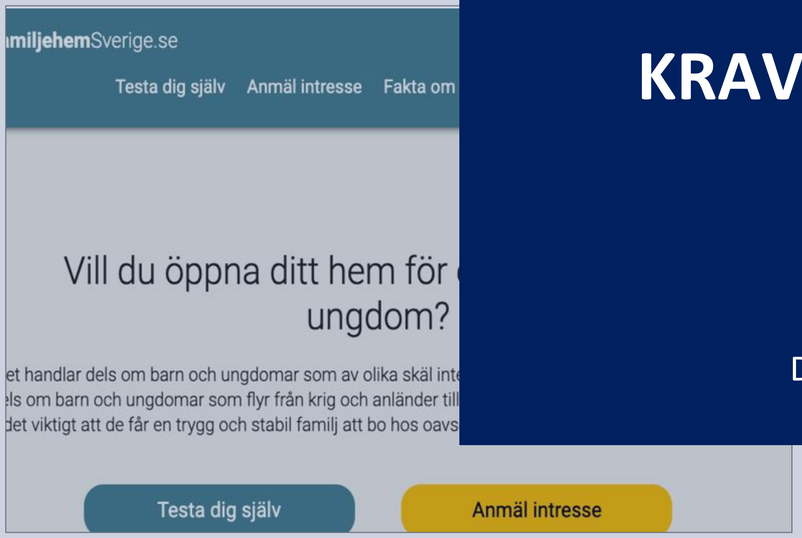
- Senior Advisor Cyber Security & GDPR Expert
- Member ENISA AHWG EUCS & Rapportour ENISA for EUCS Guidelines
- Member in EU Alliance for Data Edge and Cloud
- Member in EDPB support group of Experts
- Har de senaste 10 åren anpassat system/tjänster till de nya kraven som vi inom EU tagit fram för att skydda invånare och viktiga tjänster i vår uppkopplade värld
- Har tidigare en lång karriär inom IT, Tech och mjukvaruutveckling internationellt.

EUROPEAN ALLIANCE FOR INDUSTRIAL DATA, EDGE AND CLOUD

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

edpb European Data Protection Board





MAN BEHÖVER FÖRSTÅR HUR MODERNA MOLNTJÄNSTER FUNGERAR, ”BYGGS-UPP” FÖR ATT KUNNA KRAVSTÄLLA/UPPHANDLA/AVROPA FRAMGÅNGSRIKT

DEN DIGITALA UTVECKLINGEN STÅR JU INTE STILL…

EU – ”CLOUD FIRST”

"Cloud-first" innebär att all ny utveckling helst bör vara molnbaserad, och befintliga informationssystem bör omvärderas för omvandling, omskrivning eller ersättning inom ramen för de moderniseringsplaner som förutses.

2019/2020

EU – ”CLOUD FIRST”

EUs strategi är inriktad på att erhålla de ”bästa” möjliga molntjänsterna utifrån:

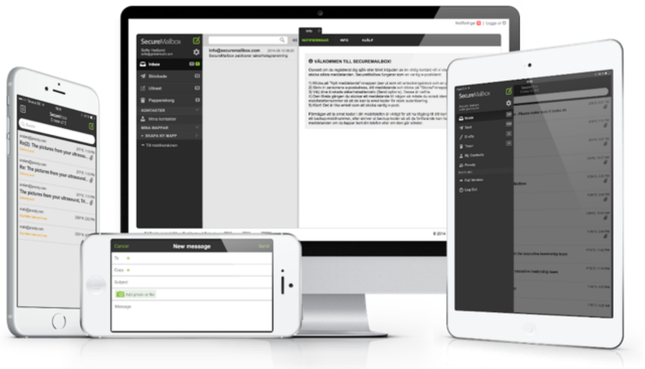
- **SÄKRA -** genom att identifiera och hantera IT-säkerhetsrisker (NIS) och data i enlighet med dess klassificering, samt överensstämma med gällande dataskyddskrav (GDPR).
- **HYBRIDA -** genom att använda tjänster både från offentliga molnleverantörer såväl som lokalt hanterade privat moln
- **MULTIMOLN –** Kunna använda den molnleverantör som är bäst lämpad att tillhandahålla den begärda tjänsten
- **ENERGIEFFEKTIVA-** i linje med EU:s prioritet att minska koldioxidavtryck och med grön offentlig upphandlingspolitik.

VARFÖR MAN BYGGER APPAR/TJÄNSTER PÅ ”WEBBEN”!

Alla kan nå och använda webben, från valfri enhet, oavsett tid och plats..

ANVÄNDARE/KLIENT

Moderna applikationer behöver snabbt kunna användas, nyttjas, distribueras, uppdateras till sina användares olika typer av enheter, oavsett tid eller plats



UTVECKLINGEN GÅR FORT..

Google Chrome	79.9%
Safari	3.0%
Mozilla Firefox	4.8%
Microsoft Edge	10.0%
	July 2023

GOOGLE CLOUD

Google SÖK!

MICROSOFT “COPILOT”!

Office 365 (CoPilot) släppt 26/9 (ChatGDP)

VARFÖR MAN BYGGER APPAR/TJÄNSTER PÅ ”WEBBEN”!

Alla kan nå och använda webben, från valfri enhet, oavsett tid och plats..

ANVÄNDARE/KLIENT

Moderna applikationer behöver snabbt kunna användas, nyttjas, distribueras, uppdateras till sina användares olika typer av enheter, oavsett tid eller plats

ADRESSERING / BEHÖRIGHET

För att nå sina Webtjänster genom de redan installerade webbläsarna skriver man in en DNS adress. Många tjänster kräver behörighet.

HTTPS://Familjehemsverige.se

HTTPS://connect.secureappbox.com

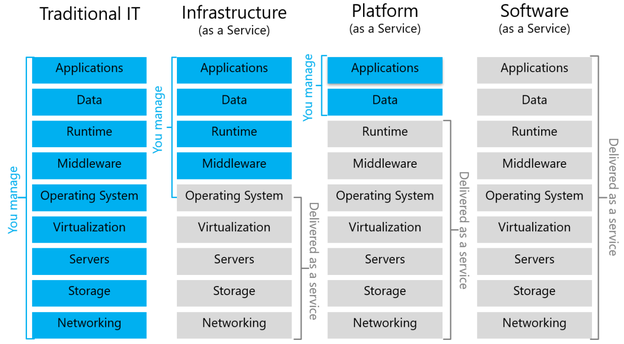
LOA1

LOA2

LOA3

WEBBTJÄNST/SERVER

Webtjänster byggs i ”containers” genom användning av färdiga ramverk, komponenter & API tjänster. Dessa implementeras sedan i olika molninfrastrukturer där IaaS, PaaS, SaaS kombineras…

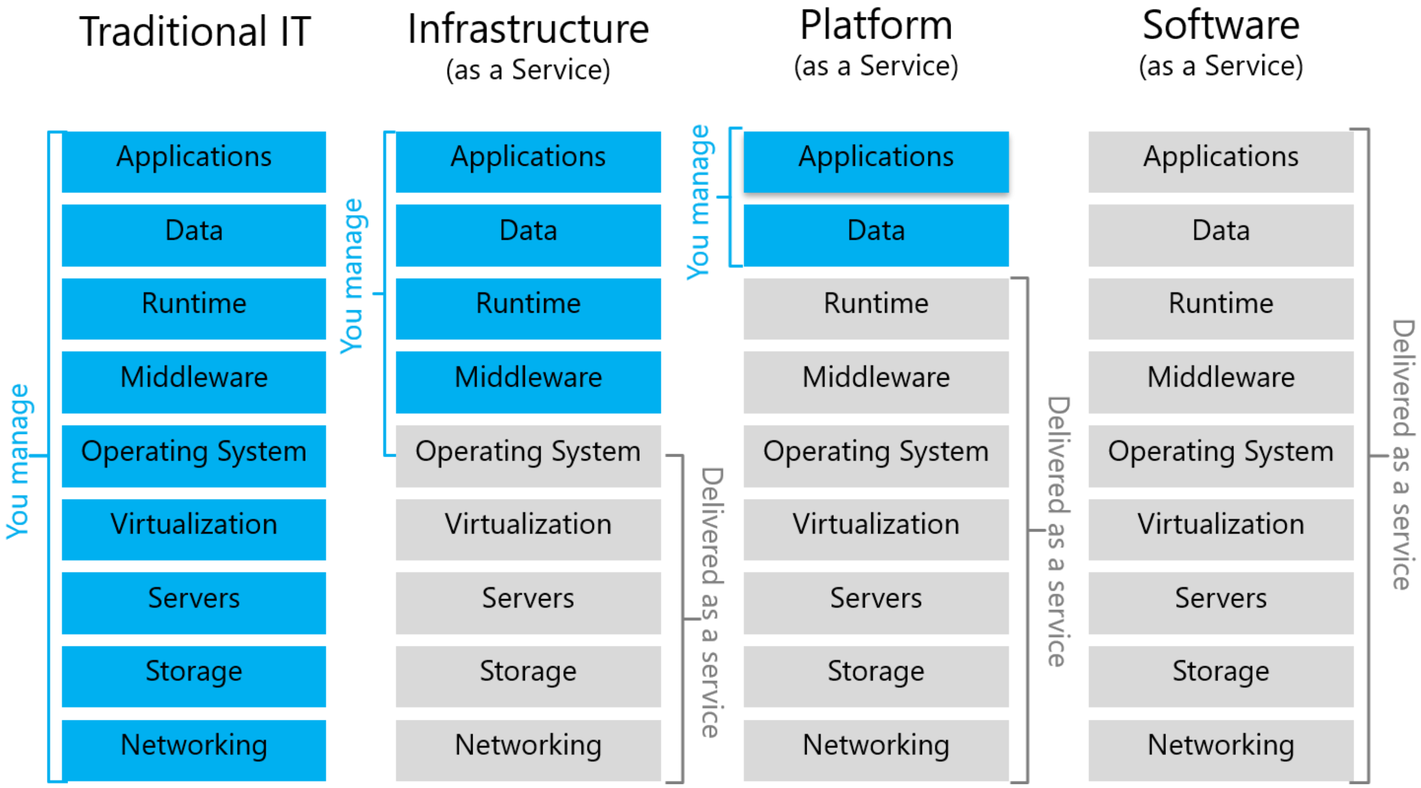


MÅNGA VÄLJER EXTERN INFRASTRUKTUR

Fokus på det man är bra på!

Redundant nät anslutning, skalbar- genomtänkt- och testad infrastruktur, hög säkerhet, klarar regulatoriska krav, hög tillgänglighet (24/7) och man betalar bara för nyttjandet

Traditionella molnmodeller



Idag: Multi/hybrid modeller

Idag handlade molnprojekt mer om att komponera funktioner, oavsett vilken "molnmodell" som användes av en viss implementering (t.ex. API, komponent, funktion, tjänst, etc.).

I moderna molnprojekt komponera man tjänster och funktioner byggda på både IaaS, PaaS och SaaS alternativ. Dessutom har mognaden kring hybrid modeller ökat så även linjerna med interna IT-miljöer suddades ut.

Trust in a Digital Society

European Commission | powered by **European Commission**, CONNECT Digital Society, Trust and Cybersecurity Directorate

REGULATORISK STYRNING - EU

EU – CYBERSECURITY STRATEGY

Styrning genom förordningar och tydliga direktiv

STYRNING

STRATEGY

2013-2019

2020-2025

2010 2013 2016 2019 2022 2024..

CER Directive
- **Energy**
- **Transport**

GDPR
NIS1

CSA
Cyber Security Act

NIS2 (CER)

NIS2 implemented
CSA (EUCC/EUCS/5G)
DORA (RTS/ITS)
Cyber Resilience Act
AI Act
Chips Act
Etc..

IMY – GDPR
MSB - NIS
- IVO
- PTS
- DIGG
- etc

ENISA
- EU Cybersecurity Agency
- Develop NIS
- Cybersecurity certification framework (EUCC/EUCS/5G…)

REGULATORISK STYRNING - NIS

NIS2

Öka motståndskraften hos våra samhällsviktiga tjänster

Nätverks- och informationssystemen har utvecklats till ett centralt inslag i vardagslivet i och med den snabba digitala omställningen och samman-kopplingen av samhället. Denna utveckling har lett till en utvidgad **cyberhotbild***, som medfört nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater.

Nya uppdaterade NIS2-direktivet innehåller många nyheter:

- ny klassificering, väsentliga entiteter och viktiga entiteter samt tillämpning på flera sektorer;
- **nya krav på säkerhetsåtgärder;**
- **krav på säkerhet i leverantörskedjor;**
- utökade krav på incidentrapportering;
- införande av sanktioner;
- mm

Cybersecurity: Parliament adopts new law to strengthen EU-wide resilience | News | European Parliament

*** Cyberattacker, växer snabbt i omfattning, kostnader och i hur sofistikerade de är.**
- en av de snabbast växande formerna av brottslighet i världen

NIS2 - oktober 2024

CYBERHOT & INTERNA BRISTER

EXTERNA CYBERHOT

STYRNING

1
- **Cyber attacker**
- Av andra länder/ eller anlitade av dessa
- Strategisk infrastruktur – målet data / skapa kaos

2
- **Cyber attacker**
- Kriminella attacker på er/leverantörskedjan
- ”Hitta svagaste punkten” - målet är pengar

ÖKA VERKSAMHETENS MOTSTÅNDSKRAFT

3
- **Brister i lösningar och leverans “no redundancy”**
- Dålig kontroll på andras faror/leverantörskedjan
- Brister i upphandling/underlag/implementation

4
- **Omedvetna eller medvetna misstag**
- Dåligt utvecklade tjänster/design – Brist QA
- Bristande instruktioner, kompetens eller bara otur

INTERNA HOT OCH BRISTER

Ny klassificering och tillämpning på flera sektorer;

Väsentliga entiteter (och kan även vara kritiska)

1. Energi	a) Elektricitet, b) Fjärrvärme/fjärrkyla, c) Olja, d) Gas, samt e) Vätgas
2. Transport	a) Lufttransport, b) Järnvägstransport, c) Sjöfart, samt d) Vägtransport
3. Bankverksamhet	Kreditinstitut enligt EUF 575/2013
4. Finansmarknadsinfrastruktur	Handelsplatser (värdepapperscentraler), direktiv 2014/65/EU, centrala motparter, EUF 648/2012
5. Hälso- & sjukvårdssektorn	Vårdgivare (direktiv 2011/24/EU), EU-laboratorier inom smittforskning, läkemedelsforskning (direktiv 2001/83/EG), tillverkare av farmaceutiska basprodukter och läkemedel, tillverkare av kritiska medicintekniska produkter
6. Dricksvatten	Leverantörer enligt direktiv 98/83/EG
7. Avloppsvatten	Företag som hanterar avloppsvatten mm enligt direktiv 91/271/EEG
8. Digital infrastruktur	Internetknutpunkter, DNS-tjänster, toppdomänregistrerare, molntjänst datacentraler, nättjänst innehållsleverans, betrodda tjänster (EUF 910/2014), leverantör av elektroniska kommunikationsnät/tjänster
9. Offentlig förvaltning	Offentliga förvaltningsentiteter under regeringen, regioner (och kommuner)
10. Rymden	Operatörer som tillhandahåller infrastruktur till stöd för rymdbaserade tjänster (direktiv 2018/1972)

Viktiga entiteter

1. Post- och budtjänster	Tillhandahållare av post- och budtjänster (direktiv 97/67/EG)
2. Avfallshantering	Företag som sköter sophämtning mm (direktiv 2008/98/EG)
3. Tillverkning, produktion och distribution av kemikalier	Företag som tillverkar, producerar och distribuerar kemtekniska ämnen och varor (EGF 1907/2006)
4. Produktion, bearbetning och distribution av livsmedel	Livsmedelsföretag (EGF 178/2002)
5. Tillverkning	a) Medicintekniska varor (EUF 2017/745 och 2017/746) b) Datorer, elektronikvaror, optik c) Elapparater d) Övriga maskiner e) Motorfordon, släpvagnar och påhängsvagnar f) Andra transportmedel
6. Digitala leverantörer	- Internetbaserade marknadsplatser - Internetbaserade sökmotorer - Plattformar för sociala nätverkstjänster

Stor del av kommunal verksamhet omfattas

Underleverantörer omfattas

IT-infrastruktur omfattas inkl. fastighetsbolag.

Hänvinningar:

NIS2 delas i KRITISKA, VÄSENTLIGA OCH VIKTIGA

KRITISKA: Särskilt utpekade som *samhällsviktiga*, med *kritisk infrastruktur* och där en incident skulle kunna medföra *betydande störning* (se art. 2.3 och direktiv EU 2022/2557 CER)

VÄSENTLIGA: Entiteter som räknas upp som ”väsentliga” (se art. 3.1 och Bilaga I)

VIKTIGA: Entiteter som anges i Bilaga I eller II och som inte anses vara väsentliga enligt art. 3.1 (se art. 3.2 och Bilaga I och II)

SÄKERHETSANSVAR NIS2 - ART 20

ANSVAR ATT INFÖRA ÅTGÄRDER FÖR RISKHANTERING OCH RAPPORTERINGSKRAV FÖR CYBERSÄKERHET

NIS2

ART 20: Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.

Det är ett tydligt krav i NIS 2-direktivet att styrelsen och VD ska ha de kunskaper och färdigheter som krävs för att bedöma cybersäkerhetsrisker, utmana säkerhetsplaner, diskutera aktiviteter, formulera åsikter och implementera lösningar som skyddar digitala processer och tillgångarna i deras organisation.

SÄKERHETSKRAVEN
NIS2 - ART 21.2 a-j

VAD BEHÖVER NI SÄKRA (ART 21.2)?
VILKA ÄR MINIMI KRAVEN?

Hur överensstämmer dessa krav med vad ni har idag?

ARTIKEL 21(2): NIS2 SÄKERHETSKRAV:

a) Aktuell riskanalys/säkerhetspolicyer för IT-systemen.

(b) incidenthantering.

c) Kontinuitet i verksamheten.

d) Säkerhet i försörjningskedjan.

e) Säkerhet i nätverk och informationssystem.

f) Bedömning av effektiviteten av cybersäkerhets åtgärder;

g) Grundläggande datorhygienpraxis och utbildning.

(h) Policyer/förfaranden för användning av kryptografi.

(i) Säkerhet för personal, policyer för åtkomstkontroll och tillgångar/förvaltning.

(j) multifaktorautentisering, säker röst, video och text kommunikationer och fungerande nöd-system inom enheten.

Om ni upphandlar nya tjänster/IT-system, så är dessa krav minimum?

HUR SÄKRAS ”EXTERN” INTERNET INFRASTRUKTUR?
VILKA ÄR DERAS MINIMI KRAV?

Art 21.5. Senast den 17 oktober 2024 ska kommissionen anta en genomförande akt som fastställer de tekniska och metodologiska kraven för de åtgärder som avses i punkt 2 med avseende på:

- **Toppdomännamnsregister och DNS tjänsteleverantörer,**
- **Molntjänsteleverantörer och leverantörer av datacentertjänster,**
- **Leverantörer av säkerhetstjänster, hanterade tjänster och förtroendetjänster,**
- **Online marknadsplatser, plattformar för sök, sociala nätverkstjänster.**

Kommissionen får anta en genomförande akt som fastställer de tekniska och metodologiska kraven. När kommissionen utarbetar akter skall de i möjligaste mån **följa europeiska och internationella standarder samt relevanta tekniska specifikationer.**

Art 21.5 Implementing Act – leds av ENISA i samarbete med ECASEC (the Article 40, former Article 13A Expert Group)

https://resilience.enisa.europa.eu/article-13

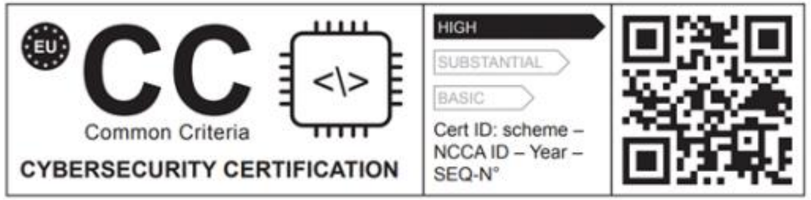
HUR KAN LEVERANTÖRER (UNDERLEV.) VISA FÖLJSAMHET TILL MINIMIKRAVEN I ART 21.2?

Har era befintliga leverantörer planer på att certifiera sina tjänster?

Art 24. Användning av cybersäkerhetscertifiering för IT-produkter, molntjänster och IT-processer

För att visa att vissa krav enligt artikel 21 är uppfyllda får medlemsstaterna ålägga väsentliga och viktiga entiteter att använda särskilda IT-produkter, moln-tjänster och IT-processer, som har utvecklats av den väsentliga eller viktiga entiteten eller **upphandlats från tredje part, som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering.**

- **EUCC - Certifiering av produkter**
- **EUCS - Certifiering av molntjänster/Appar**



Framöver så kommer ni kunna kravställa på att leverantörers produkter och tjänster är certifierade.

CSA

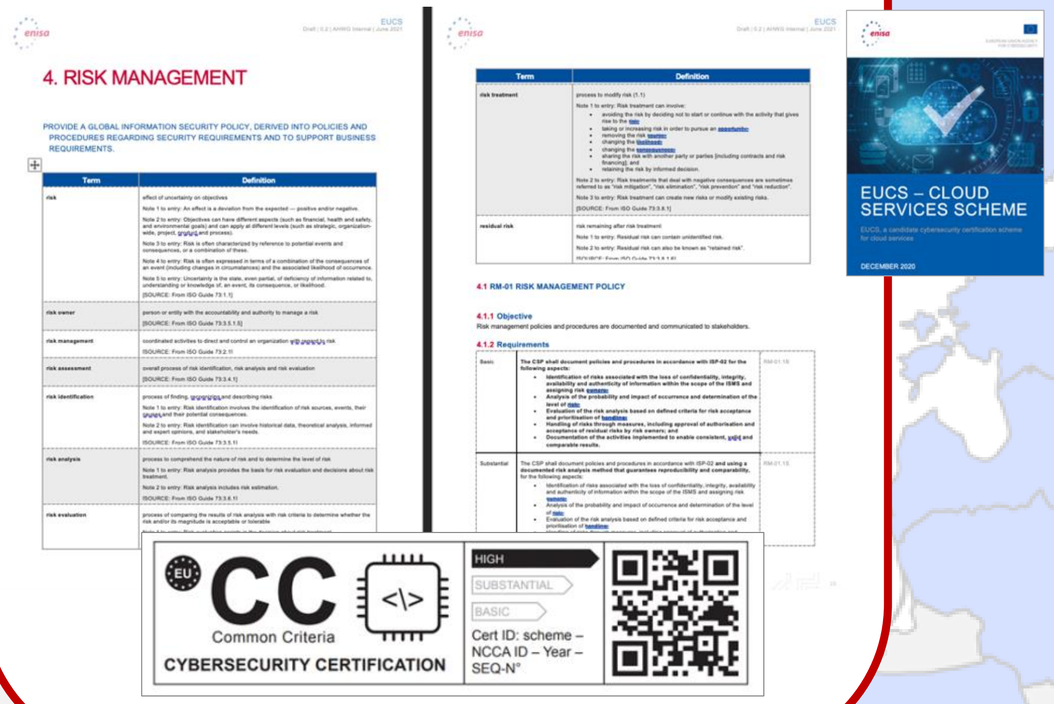
EUCS - certifiering av moln och applikationstjänster

- Alla säkerhetskrav skall vara uppfyllda utifrån en framtagen kravkatalog av ”säkerhetskontroller”
- Kravkatalogen hanterar bla frågeställningarna i Art 21.2, i tre nivåer av motståndskraft: Grundläggande, Betydande (NIS2) och Hög.
- Kontroll av följsamhet är: Grundläggande - ”self assessment”, CAB* på betydande och myndighet (ICC-FMV) på högsta nivåerna.
- EUCS lägger grund för fler certifieringar 5G, IOT mm

*CAB – Conformity Accreditation Body

Basic, Substantial, High

Cloud Service Scheme



TILLSYN GÖRS AV ICC (SWE)

CSA

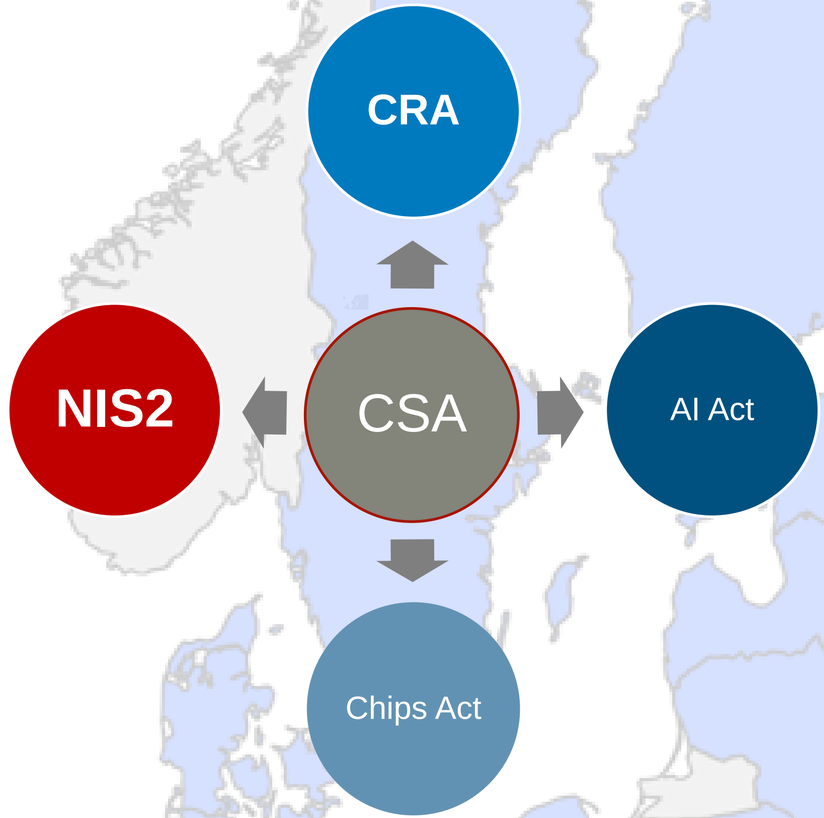
Ansvarar för CSA i Sverige:

Tillsynsmyndigheten ICC

- **Etablerades genom beslut av FMV GD juni 2021.** Ansvar för uppgifter som följer av EU:s cybersäkerhetsakt samt lag och förordning med kompletterande bestämmelser till EU:s cybersäkerhetsakt.
- I uppgiften ingår
  - **Omvärldsbevakning** av frågor som rör cybersäkerhet och cybersäkerhetscertifiering av IKT-produkter, -tjänster och -processer,
  - **Samverkan** med nationella och internationella aktörer på området och
  - **Tillsynsansvar** över efterlevnaden av det europeiska ramverket för cybersäkerhetscertifiering (EUCC, EUCS…)

FMV

Cybersecurity Certification
referenced in the different EU Laws



Den snabba digitaliseringen ger stora möjligheter, men utsätter också samhällen för nya typer av hot.

Cyberattacken mot Kaseya i juli 2021 är ett olyckligt och välkänt exempel på attacker i leveranskedjan.


SÄKERHET 2022-12-02 10:32

Softronics kunder utslagna efter attack

På grund av vad som beskrivs som en säkerhetsrelaterad incident så har många av konsultbolaget Softronics kunder drabbats hårt under morgonen. Just nu finns ingen prognos för när problemen väntas vara lösta.

NIS2 - Krav på säkerhet i leveranskedjan

Enligt NIS2-direktivet ska berörda verksamheter ”entiteter” hantera säkerhetsaspekter i relationen mellan entiteten och dess direkta leverantörer och tjänsteleverantörer (samt deras ev underlev).

Detta gäller såväl i förhållande till eventuella sårbarheter hos varje direkt leverantör och tjänsteleverantör som den generella kvalitén av produkter och hur leverantören och tjänsteleverantören tillämpar cybersäkerhetskrav.

”offentliga förvaltningsentiteter” – har således inte bara ansvar för säkerheten i sin egen verksamhet, utan även de leverantörer de väljer att använda sig av.

Det nya kravet får betydelse för bedömningen av leverantörer i samband med IT-upphandlingar inom offentlig sektor. Kravet tillämpas vid sidan av de krav på säkerhet som uppställs i GDPR om tjänsteleverantören behandlar personuppgifter för myndighetens räkning.

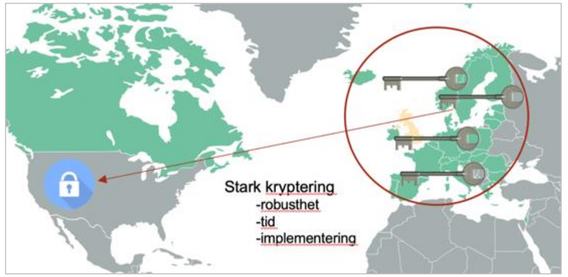
SCHREMS 2

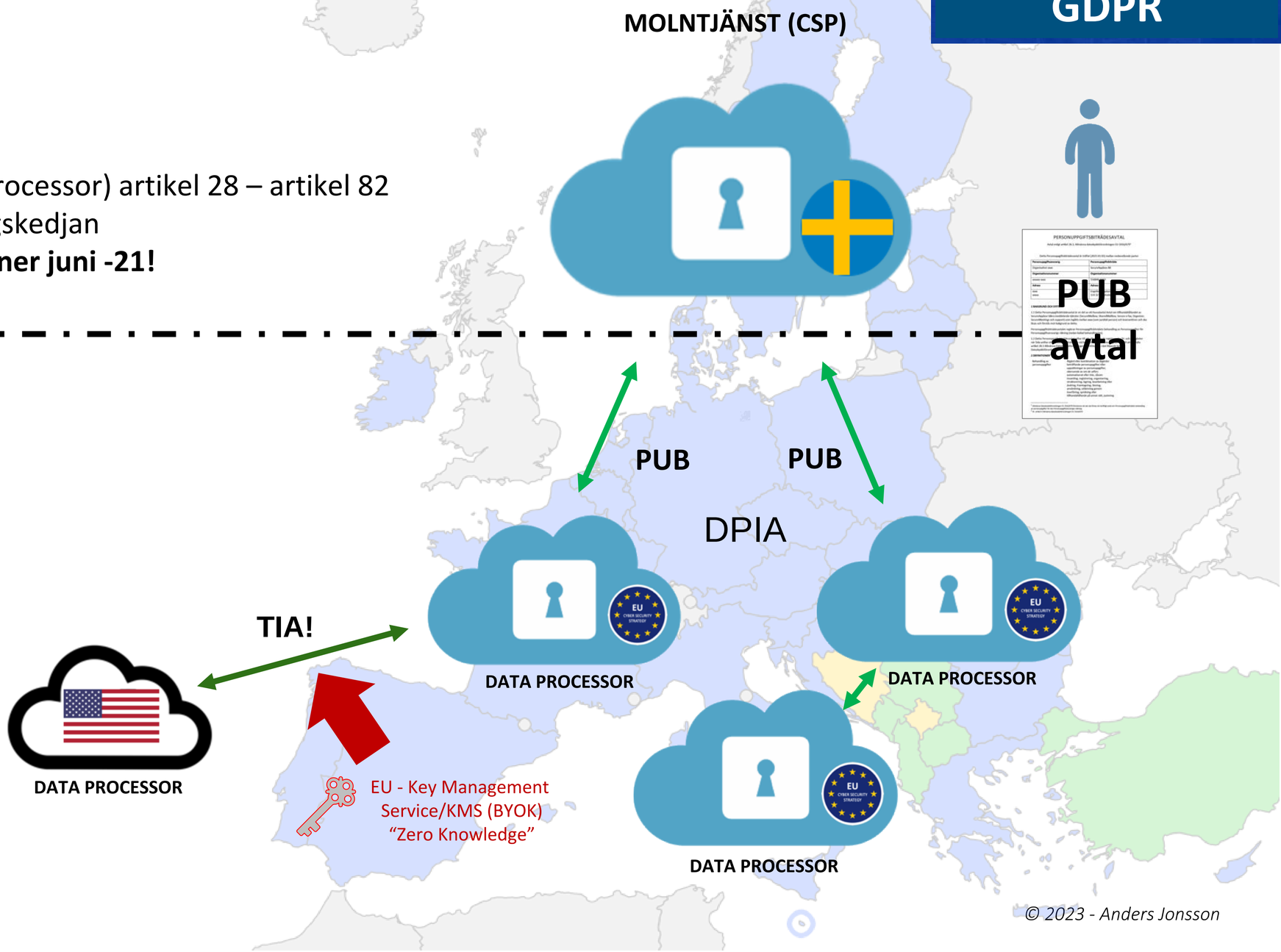
GDPR

2021 - SCHREMS 2

- Registeransvarig, (processor/sub-processor) artikel 28 – artikel 82
- PUB-avtalet säkerställer försörjningskedjan
- **Schrems 2 - EDPB-rekommendationer juni -21!**

GDPR:
PERSONUPPGIFTSBITRÄDE
”DATA PROCESSOR”

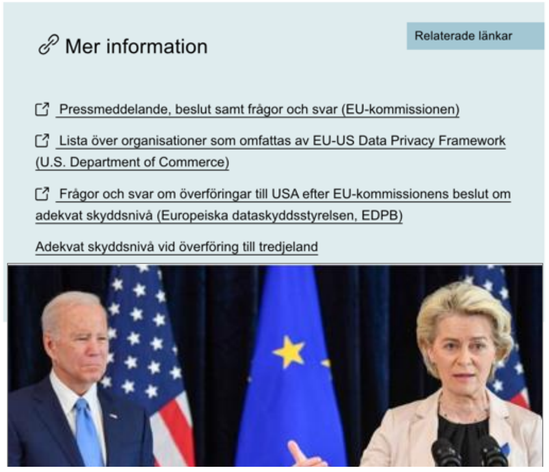




GDPR - DELA ANSVAR MED DINA TJÄNSTELEVERANTÖRER

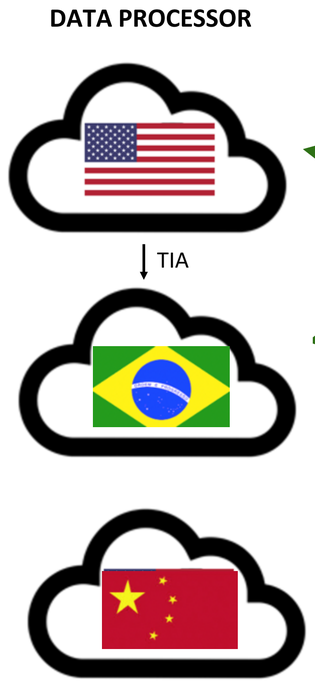
- Registeransvarig, (processor/sub-processor) artikel 28 – artikel 82
- PUB-avtalet säkerställer försörjningskedjan
- Privacy Shield (2) gäller igen, sedan 10 Juli 2023

IMY: Privacy Shield (2)

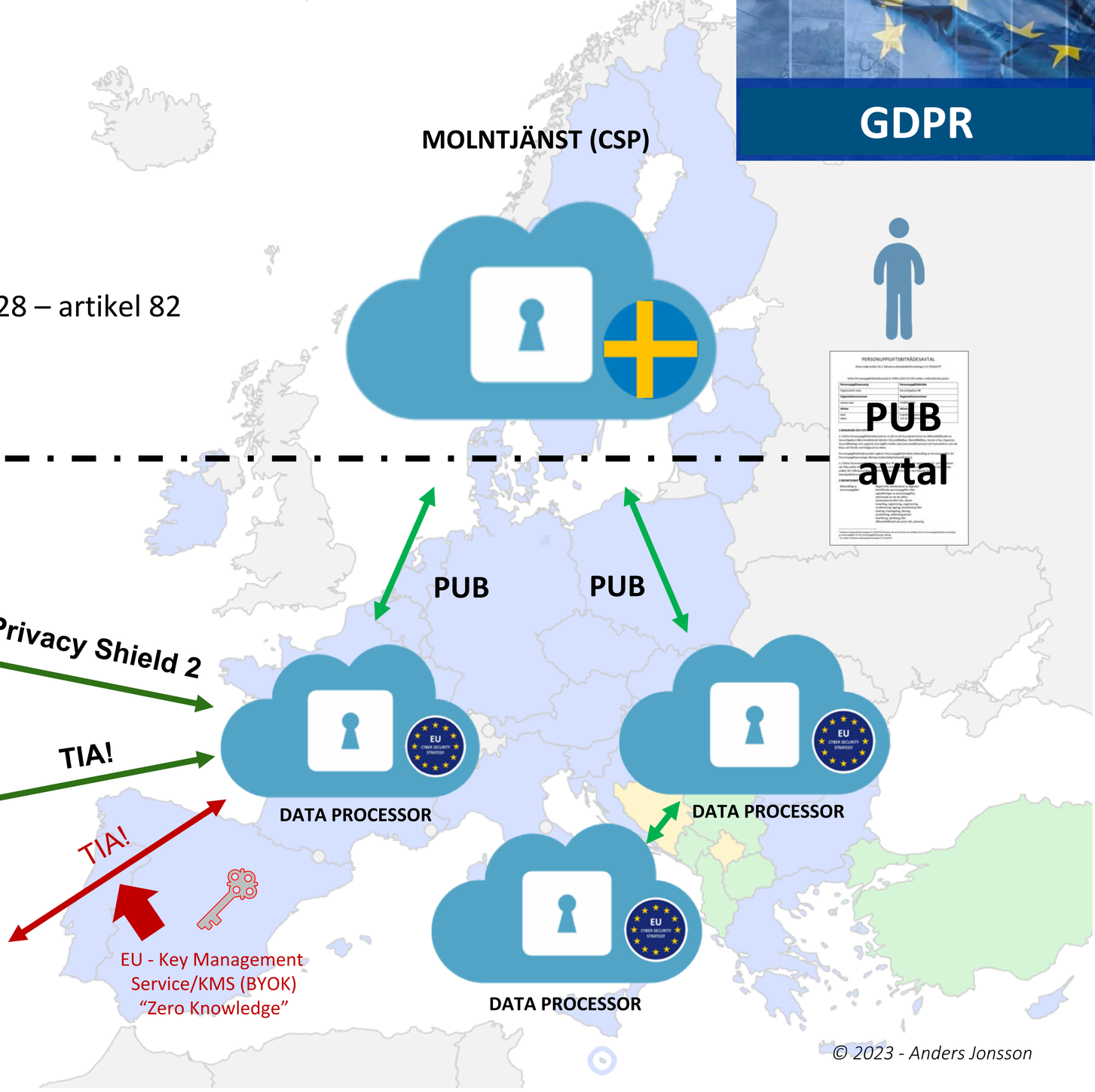


12 oktober 2023

"The European Union General Court ruled against interim measures to pause the implementation of the EU-U.S. Data Privacy Framework. The court said to EU-member Philippe Latombe - **cannot prove the individual or collective harm the agreement raises**."



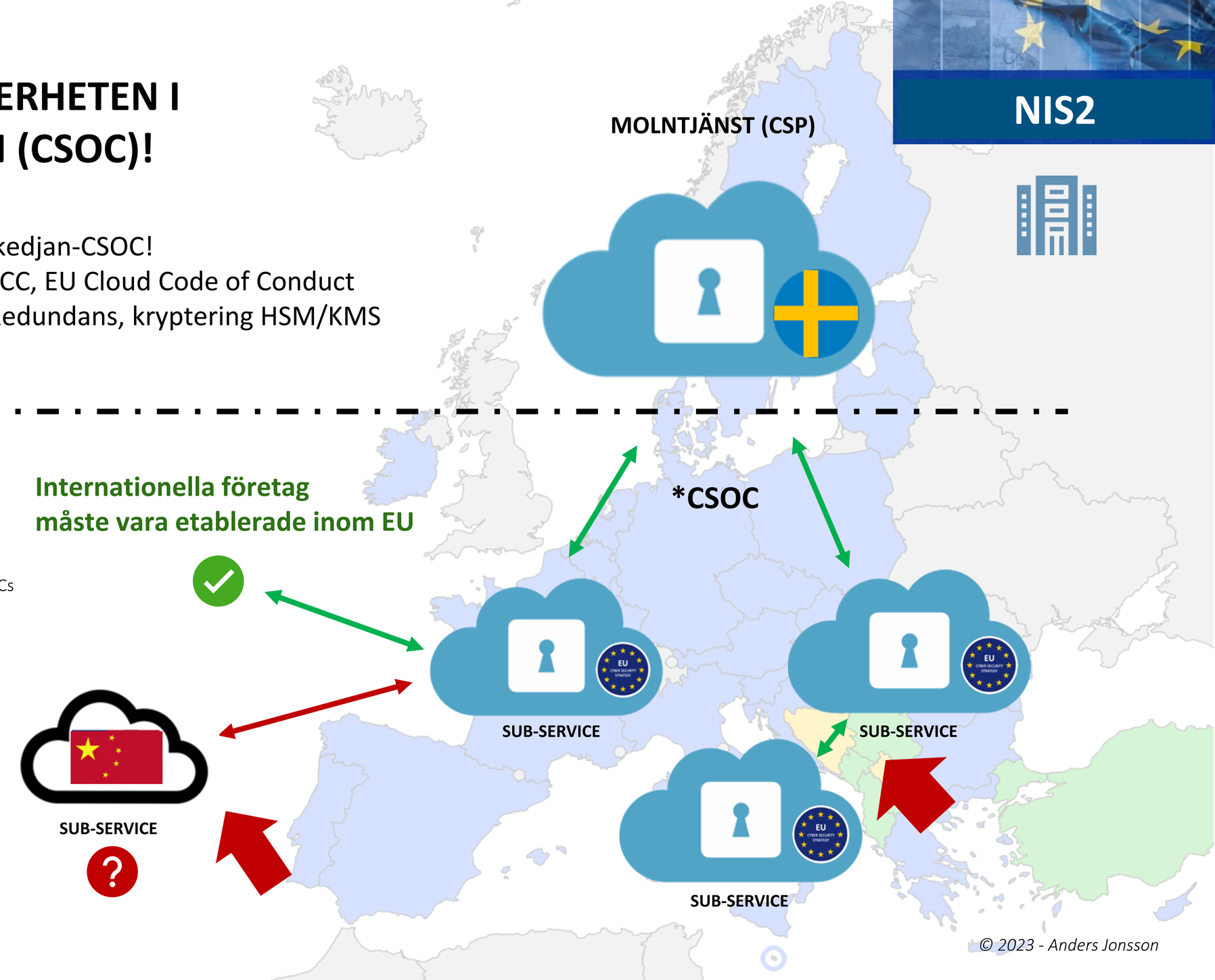
Kina behöver ha tillgång till Nycklarna



NIS2- SÄKERSTÄLL SÄKERHETEN I FÖRSÖRJNINGSKEDJAN (CSOC)!

NIS2

- Kravställer säkerheten i leveranskedjan-CSOC!
- Certifiering: ISO 270XX, EUCS, EUCC, EU Cloud Code of Conduct
- SLA/QoS, Säker utv. Pen-tester, Redundans, kryptering HSM/KMS
- **Laglig etablering inom EU krävs.**



*EUCS - CSOC

Complementary Subservice Organization Controls

CABs will evaluate whether the controls related to the CSOCs are suitably designed, implemented and, for levels CS-Substantial/CS-High, operating effectively. Controls like access controls, authentication protocols, data encryption..

NIS2, Art 26

3. Om en enhet som avses inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den utse en representant i unionen. Ombudet ska vara etablerat i en av de medlemsstater där tjänsterna erbjuds. En sådan enhet ska anses falla under jurisdiktionen i den medlemsstat där företrädaren är etablerad.

I avsaknad av en företrädare i får varje medlemsstat där enheten tillhandahåller tjänster vidta rättsliga åtgärder mot enheten för överträdelse av detta direktiv.

SUMMERING

Vad man behöver tänka på och vad som är viktigt vid upphandling av moderna IT- och molntjänster,

- speciellt inom offentlig verksamhet.

Vad gäller de som INTE omfattas av NIS2?

- Bra säkerhetsrutiner och motståndskraft är bra för alla verksamheter.

Alla behöver förstå riskerna och ledningen har ett tydligt ansvar

- **NIS2 sätter Cybersäkerhet på agendan**. Högsta ledningen i varje organisation behöver förstå vilken motståndskraft man har och vilken cyberrisk man tar.
- Alla behöver få till ett ”nuläge” - en **riskanalys utifrån NIS2** utökade omfattning och kartlägga verksamhetens risker i olika leverantörs och försörjningskedjor.
- **Analys och plan avseende kontinuitet** i verksamheten. Vad händer om kritiska system/tjänster går ner, internt/externt!
- EU kom med förtydligande 13 oktober kring NIS2 – ”en allrisk ansats”…

Kräver resurser…

Alla bör vara medvetna om att implementering av denna typ av praxis och kontroller kan kräva ytterligare ekonomiska och mänskliga resurser.

Det krävs högre nivå av testning, dokumentation av säkerhetsfunktioner från leverantörer, system integratörer och externa tjänsteleverantörer/ molntjänster. Vilket ökar deras/era kostnader och ev priset på produkter eller tjänster.

När man beslutar om detta, bör man beakta både kostnaderna för att implementera dessa kontroller och riskerna med att inte implementera dem.

Förtydligande kring “allrisk ansats” 13 Sep..

Verksamhetssäkra

Fokus på fysiska risker som kan störa möjligheten att utföra sitt samhällsuppdrag

- Motståndskraft mot fysiska attacker
- Naturkatastrofer, brand, översvämning..
- Inbrott, Terrorist attacker
- Pandemier
- Energiförsörjning/Transport

+

Informationssäkra

Fokus på IT-risker som kan störa möjligheten att utföra sitt samhällsuppdrag

- IT-säkra, kvalitetssäkra och skydda
- Informations klassning
- Hantering av personuppgifter-DPIA/TIA*
- Tillgänglighet/molntjänster
- Driftsäkerhet

+

Cybersäkra

Fokus på de cyber risker som kan störa möjligheten att utföra sitt samhällsuppdrag

- Motståndskraft mot Cyber attacker
- Integrera/Separera/Kryptera
- Leveranskedjesäkerhet
- Externa beroenden
- IOT/Molntjänster

Pandemi!

** Nytt avtal EU och USA 10/7-23 – Privacy Shield 2*

2010 2016 2022

***Bryssel den 13.9.2023**: Därför bör de riskhanteringsåtgärder för cybersäkerhet som entiteten vidtar skydda inte bara entitetens nätverks- och informationssystem utan också dessa systems fysiska miljö mot sådana händelser som sabotage, stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst som kan undergräva tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.*

PRAKTISK GENOMFÖRANDE

Skapa en översiktlig handlingsplan för NIS2

Genomförs i olika steg och med delmål

PLAN

Var står vi idag?

Starta arbetet för att ta reda på om och hur er verksamheten träffas av det nya uppdaterade NIS2 regelverket. Man behöver en grov handlingsplan, göra en GAP-analys och besluta vilka som ansvarar för vad.

Utbildning

Genomför en kort cyber-utbildning av personer i ledningen kring Cyberrisker och NIS2.

Info Ledningen (delmål)

Presentera delrapport för ledningen med underlag på vilka risker verksamheten bedömer finnas och vilka konsekvenserna kan bli. Behöver vara överskådligt.

Infomöte

Genomför en informationsträff kring vad NIS2 är och förklara skillnaderna med tidigare direktiv. Bjud in de som ni tror omfattas.

Kvalificera

Kvalificera mer i detalj vilka nyckelområden som omfattas och vilka som behöver involveras

Identifiera och Analysera

Statusrapport / verksamhetsområde innehållande minst följande:

- Identifiering av viktiga leverantörskedjor och beroenden
- **Gå igenom era befintliga leverantörs avtal***
- Uppdatera er riskanalys – gör ett ”allrisk” antagande

lev möten

Genomför möten med viktiga/kritiska under-leverantörer för att veta hur de tänker kring NIS2

Sammanställ

Sammanställ en rapport med följande:

- En gemensam/sammanslagen analys
- Identifierat kritiska beroenden/lev.
- Förslag på prioriterad åtgärder

Mars/April - 2024…

Gör en ny konsekvensanalys utifrån publicerade villkor och den riskanalys man gjort. Presentera dessa för ledningen som kan besluta om vad som behöver justeras/ändras.

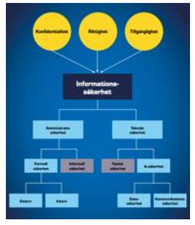
Maj - 2024…

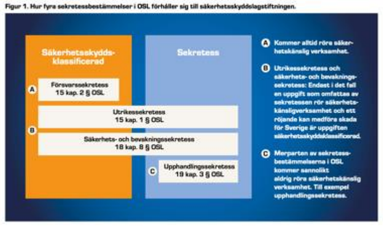
Åtgärda de saker som beslutas och förankra de risker man har kvar med ledningen och **lägga upp rutiner för Incidenthanteringen i enlighet kraven**

Intern

*Glöm inte era SCADA/OT processer

Nationella sekretess/säkerhetskrav: OSL 10.2 underlättar ut kontraktering
NIS2 och Säkerhetsskyddslagen bygger på samma grundprinciper





Februari/Mars 2024

PTS/MSB presenterar detaljer hur NIS2 implementeras i svensk lag, vilka som berörs och när.

Oktober 2024

NIS2 träder i kraft över hela EU med krav på hög motståndskraft mot cyberattacker och rapporteringskrav

Extern

TRYGG DIGITALISERING I MOLNET

- Regulatorisk följsamhet, inte bara krav, utan stöd! – PUA, CSOC mm
- Gör en övergripande handlingsplan för era risker (NIS2)
- Er säkerhet bygger på bra samarbete med era underleverantörer

”Säkerhet handlar om nära samarbete och långsiktighet, inte lägsta pris!”

FRÅGOR…

Tack och lycka till…

Anders Jonsson