Nya regleringar kräver omfattande förstärkning av cybersäkerheten!

Vi är många som har anpassningen till GDPR (2018) i färskt minne, och under de senaste åren har kraven på cybersäkerhet inom allt fler områden trappats upp.

- Framförallt **EU** är väldigt aktivt inom hela området Informationssäkerhet, cybersäkerhet, IT-säkerhet. (Inte minst inom *GRC = Governance, Regulations, Compliance*.)
- De flesta organisationer måste på ett eller annat sätt förhålla sig till den nya lagstiftning som nu träder (eller redan har trätt) i kraft.
- Det försämrade säkerhetsläget i Europa, med kraftigt ökade cyberangrepp och intrångsförsök, visar tydligt att cybersäkerhetsarbetet måste intensifieras.
- Organisationer kommer framöver att behöva arbeta med att:
    - Avgöra om man omfattas av de nya kraven.
    - Tolka och implementera de nya kraven.
    - Dokumentera och presentera att detta gjorts.
    - Göra Gap-analyser och planera verksamhet därefter.
    - Följa upp och säkerställa att skyddsnivåerna efterlevs över tid.
    - Ta fram verktyg, utbildningar, stöd, metodik, processer och allt runtikring, för att säkerställa att kraven uppfylls och att man kan bibehålla detta över tid.
- Om en organisation inte klarar av att uppfylla de skärpta kraven, kan den bli tvungen att betala dryga böter. Beloppen har skärpts upp och kan utgöra flera procent av omsättningen eller tiotals miljoner Euro.

- De nya/utökade regelverken pekar mycket tydligare ut verksamhetens LEDNING som ansvarig för cybersäkerheten. Detta gör att det blir mycket svårare att komma undan, både ansvarsmässigt/operativt och budgetmässigt. Det är nog det EU-lagstiftarna vill åstadkomma – att ingen organisation härefter skall våga ignorera sin IT-säkerhet.
- För samtliga regelverk gäller proportionalitetsprincipen, det vill säga att ”*en åtgärd för att uppnå sitt syfte inte får vara mer betungande eller långtgående för den enskilde än vad som kan anses nödvändigt för att uppnå det eftersträvande syftet med åtgärden*.” En hel del juridisk bedömningssport alltså.
- Flera av regelverken överlappar varandra eller säger ungefär liknande saker. Det krävs att man sätter sig in i detta så att säkerhetsarbetet blir koordinerat och att inte flera ”springer på samma boll”. Att utgå från befintliga ramverk, till exempel ISC/ISO 27000, CIS, NIST eller liknande rekommenderas, annars tenderar sådant här att bli väldigt mycket reaktivt och brandsläckning.

Summerat ställer flera av de nya regleringarna krav på att organisationer som har IT-system skall ha ordnande processer för:

- Riskhantering
- Incidenthantering
- Kris/katastrofhantering inklusive *Recovery*
- Rapportering vid incident (till användarna och till utpekad myndighet)
- Förmåga till kontinuitet (resiliens, motståndskraft) vid incidenter

Man skall dessutom ha ordning på

- Säkerheten hos tredjepartsleverantörer, *supply-chain*
- Sina egna produkters svagheter och risker. SBOM (*Software Bill of Materials*) blir legio, likaså säkerhetstestning av egenutvecklade produkter
- Cyberhygien i egna nät och system
- Medarbetarnas säkerhetsmedvetande

Vilka är då dessa nya lagar och regelverk? Här är några av de viktigaste som har kommit eller kommer i närtid:

- NIS2 (Network and Information Systems directive version 2)
  - *“Direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen”*
- CER (Critical entities resilience directive)
  - *“Direktivet om kritiska entiteters motståndskraft”*
- CRA (Cyber Resilience Act)
  - *”Cyberresilliensakten”*
- DORA (Digital Operational Resillience Act)
  - *“rättsakten om digital operativ motståndskraft”*

- AIA (AI Act)
    - *”AI-förordningen”*
- LEK(v2) – Lagen om Elektronisk Kommunikation
- Övriga:
    - CDPF (EU policy on Cyber Defence)
    - CSoA (Cyber Solidarity Act)
    - CDT (Cyber Diplomacy Toolbox)
    - Data Act
    - DGA (Data Governance Act)
    - DMA (Digital markets Act)
- För övrigt lades det omstridda förslaget till ”Chat Control 2.0” fram 2022 men behandlas inte vidare här då det handlar om helt andra IT-funktioner, men skulle få omfattande konsekvenser om det infördes.

CER (Critical Entities Resillience Act)

Fokuserar på att minska sårbarheter, stärka samhällsviktiga verksamheter. Betoning på resilliens (=motståndskraft) där andra regelverk (tex NIS2) fokuserar på cybersäkerhet. Samma scope i övrigt som de ”nya” regelverken, det vill säga utökat till fler sektorer; bland annat hälso/sjukvård, banker, dricksvattenförsörjning med flera.

- Organisationer skall förstå sina kritiska processer, tjänster och tillgångar.
- Verksamheten skall kartläggas, enligt gap-analys (*NIS2 (Network and Information Systems directive version 2*) och **DORA** (*Digital Operational Resillience Act)* brister skall dokumenteras.
- Kartläggningen skall utgå från aktuellt hotlandskap när dessa analyser görs (kräver aktiv och regelbunden riskanalys) och hotanalys.
- Fokus på områden där insatser ger störst förbättring; ett försummat område är *Supply chain*-risker.

NIS2 (Network and Information Systems directive version 2)

- På svenska heter direktivet ”*åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen*”.
- Uppdaterad lag jämfört med NIS1 från 2016.
- Krav på nationell CSIRT (Computer Security Incident Response Team) (i Sverige = **`cert.se`**, som sköts av MSB).
- Krav på nationell strategi för cybersäkerhet.
- NIS2 och CSA (Cyber Security Act) samordnar regelverken.

- En organisations ledning är personligt ansvarig för cybersäkerheten – dryga böter kan utfärdas om detta negligeras. (För Väsentlig entitet: 10 M€ eller 2% av omsättning.)
    - Ledningen har också krav på sig att godkänna säkerhetsåtgärder och att vara utbildad inom dessa frågor.
    - Ledningen skall se till att verksamheten uppfyller NIS2 och regelbundet kontrollera att så sker. Personalen skall ha lämplig utbildning så att NIS2-reglerna kan uppfyllas.
- Skall vara fullt implementerat i oktober 2024
    - den svenska lagstiftningen, baserad på EU-direktivet, kan finnas framme i början av 2024. Det kan bli bråttom med andra ord.
- Många fler verksamheter omfattas av NIS2 än gamla NIS1. Man talar om SAMHÄLLSVIKTIGA, VÄSENTLIGA och VIKTIGA tjänster för samhället. Både privata och offentliga aktörer berörs.
    - Samhällsviktiga omfattar bland annat
        - Energisektorn
        - Transportsektorn – luft, järnväg, sjöfart, väg
        - Bank/finanssektorn
        - Hälso/sjukvårdssektorn
        - All leverans och distribution av dricksvatten
        - Digital infrastruktur inklusive digitala tjänster, internetbaserade marknadsplatser, sökmotorer, och inte minst molntjänster!
    - Väsentliga tjänster (nytt begrepp i NIS2) omfattar alla de samhällsviktiga (ovan) plus
        - Avloppsvatten
        - Offentlig förvaltning
        - Rymdfart
    - Viktiga (också nytt begrepp i NIS2) tjänster omfattar
        - Post/budtjänster
        - Avfallshantering
        - Kemikalier – tillverkning, distribution
        - Livsmedelssektorn – produktion, bearbetning, distribution
        - Digitala tjänster – tillverkning och leverans
- Enda undantagen till NIS2 är småföretag (under 50 anställda), som inte klassas som kritisk verksamhet med betydelse för samhället, människors liv och hälsa eller den allmänna säkerheten enligt ovan. Vissa undantag finns dock.

- Enda sättet att vara säker på om man omfattas av NIS2 eller ej är att göra en grundlig analys av den egna verksamheten enligt lagtexten.
- Om man omfattas av NIS2, krävs det att man som verksamhet har ordning på:
    - Hantering av
        - Risker inklusive hantering och processer
        - Effektiva processer för hantering av Incidenter (rapporteras inom 24 timmar!), rapportering enligt mall till nationell CSIRT (I Sverige: **`cert.se`**)
        - Cyberhygien
        - Kontinuitetsplanering
        - Kriser
        - Generell förbättring av all Cybersäkerhet
            - Saker som explicit pekas ut är kryptering ,nätverkssegmentering, VPN-krypton m m
    - Utbildning av personalens Säkerhetsmedvetenhet
    - Policy och hantering av Kryptering
    - Autentisering, säkra möten, till exempel MFA
    - Säker hantering av personal/*human resources*-delar
    - Säkerhet i leverantörskedjor, bland annat SBOM (*Software Bill Of Materials*). Skall till och med samordnas på EU-nivå.
    - Kartläggning av leveranskedjor (*SCRM-Supply Chain Risk Management*)
- Kortfattat ställer NIS-direktivet nya högre krav på säkerhet i nätverk och informationssystem. ”Lämplig säkerhetsnivå skall åstadkommas” enligt lagtexten.

CRA (Cyber Resillience Act)- *Förordningen om maskinprodukter*

Är främst ett certifieringsprogram för säkra produkter (hårdvara + mjukvara), beslutat från april 2023, i full kraft 2026. En sorts CE-märkning för cybersäkerhet, kan man kanske säga.

- Digitala produkter skall innefatta cybersäkerhet för att kunna lanseras på marknaden.
- Tillverkaren måste göra en cybersäkerhetsbedömning av produkten, vilken skall gälla under produktens hela livstid. Även underhåll skall beaktas här.
- Tillverkaren ska omedelbart rapportera till ENISA om sårbarheter upptäcks och utnyttjas.
- Det skall finnas regelverk som gör att marknaden kan övervakas och att cybersäkerhetskraven efterlevs.
- Importörer och distributörer måste säkra att alla icke EU-godkända produkter inte får släppas ut på marknaden.

Sveriges Certifieringsorgan för IT-säkerhet (CSEC) är en oberoende enhet inom FMV och verkar som Sveriges nationella certifieringsorgan för it-säkerhet i produkter och system.

Det finns en utbredd oro för att CRA kan slå hårt mot Open Source-sektorn då kravet på självcertifiering av produkter kan innebära omfattande kostnader och arbete för en *open source-community*. Flera organisationer har svarat detta i remisser till lagen.

DORA (Digital Operational Resillience Act)

- Digital resilliens (motståndskraft) inom IKT (informations- och kommunikationstjänster)
- Samfogning och *streamlining* av flera befintliga finansiella regelverk inom EU
- I laga kraft senast 17 januari 2025
- Fokus på finansmarknader och betalsystem
- Tre huvudmål:
    - Reducera risk för finansiell instabilitet och disruption
    - Reducera administrativ börda och effektivisera övervakningsmöjligheter
    - Öka kunders och investerares skydd
- Vem omfattas?
    - Banker
    - Investmentbolag
    - Kreditinstitut
    - Försäkringsbolag och Återförsäkrare
    - Finansmäklare
    - Kreditbedömningsinstitut
    - Crowdfunding
    - Tradingbolag
    - Kryptovalutor
    - Betalningsinstitut
    - Värdepappershandel
    - Förmögenhetsförvaltning
    - Revisorer
    - Leverantörer av rapporteringstjänster inom sektorn
    - Tredjepartsleverantörer av IT- och kommunikationstjänster rörande sektorn
    - Samt alla IT-bolag som levererar mjukvara till dessa organisationer
- DORA har fem ”pelare”:
- ***Pelare 1 - ICT Risk Management requirements (Artikel 5 till 14)***
    - Riskhantering, analys, uppföljning, response, recovery
- ***Pelare 2 - ICT incident reporting (Artickel 15 till 20)***
    - Incidenthanteringsprocess, klassificering, rapportering

- ***Pelare 3 - ICT third-party risk (Artikel 21 till 24)***
    - Hantering av risker i tredjepartsprodukter
- ***Pelare 4 - Digital operational resilience testing (Artikel 25 till 39)***
    - Regelbundna säkerhetstester på olika nivåer
- ***Pelare 5 - Information sharing (Artikel 40)***
    - Threat Intelligence (TI), CSIRT knowledge sharing etc

LEK (Lagen om Elektronisk kommunikation)

- Lag (2022:482) om elektronisk kommunikation, baserar sig på EU-direktivet om inrättande av en europeisk kodex för elektronisk kommunikation
- Trädde i kraft 2022 (version 2, utökad). En tidigare version av LEK har funnits sedan 2003.
- Alla som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster eller använder *radiosändare* som kräver tillstånd. De aktörer som berördes av den tidigare lagen omfattas också av den nya lagens regler. **Leverantörer av e-post, chatt- och meddelandetjänster omfattas också numera.**
- I den nya versionen av lagen kan PTS besluta om sanktionsavgifter om inte operatören et al följer reglerna.
- Förutom många regler kring nät, nummerportabilitet mm finns en rad säkerhetskrav:
    - Utvidgat säkerhetsbegrepp som nu också omfattar
        - tillgänglighet, autenticitet, riktighet och konfidentialitet
    - Utvidgad rapporteringsskyldighet av incidenter mm
    - Informationsskyldighet och granskning
- Omfattar teleoperatörer, nätverksoperatörer, tjänsteleverantörer samt stipulerar rättigheter för abonnenter och användare
- 15 kapitel varav flera handlar om frekvensspektrum, tillgänglighet, PPDR, mm
- ***Kapitel 8****: Säkerhet i nät och tjänster. Regler om åtgärder för säkerhet i nät och tjänster och skydd av uppgifter samt om skyldighet att rapportera säkerhetsincidenter.*
    - Ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt **hantera risker** som hotar säkerheten i nät och tjänster.
    - Operatören kan tvingas till **granskning** om särskilda skäl finns
    - Rapporteringsskyldighet för **incidenter**. Skyldighet att bistå utredande myndighet vid incidenter

- Även användarna måste **informeras** vid incident
- **Lagring** av trafikdata skall ske enligt regelverk och måste skyddas från intrång mm

- ***Kapitel 9****: Behandling av trafikuppgifter samt integritetsskydd. "*GDPR-light för abonnentdata"
- **utplåna** eller **avidentifiera trafikuppgifter** som har lagrats eller behandlats på något annat sätt när de inte längre behövs för överföring av ett elektroniskt meddelande
- Trafikuppgifter **sparas** till dess att betalning/fakturering skett
- **Anmälningsplikt** till PTS vilka uppgifter som sparas, nummerpresentation, portabilitet, lokationsdata mm
- **Förbud mot avlyssning**, undantag signalspaning. **Tystnadsplikt** hos operatörer

Övriga nya regleringar

- **CSA** (Cyber Security Act)
  - Förordning om cybersäkerhetscertifiering
  - I kraft 17/4 2019, fullt ut från 28/6 2021
  - Mandatet för ENISA (The European Union Agency for Cybersecurity)
    - EUCC – common criteria
    - U5G – 5G
    - EUCS – molntjänster
  - Definierar de gemensamma begrepp som övrig lagstiftning baserar sig på (NIS, DORA, GDPR…)
  - I Sverige är ICC tillsynsmyndighet för dessa entiteter (Cybersäkerhetscertifiering).
- **CDP** (EU policy on cyber defence)
  - NATO-EU samarbete mm
- **CSoA** (Cyber solidarity Act)
  - Militärt-civilt inklusive insatsarbete, "European Cyber Shield"
- **CDT** - Cyber Diplomacy toolbox
  - Antogs 2017, ses över 2023, Avser förebyggande av konflikter

- EU **Data Act**

- Föreslaget 2022, (oklart när det kan träda i kraft). Reglerar dataöverföringar mellan B2B, B2C, and B2G och molntjänstleverantörer
- Skall harmonisera GDPR, datalagringsdirektiv, dataförvaltning

- EU **AI Act**
  - Skall antas under 2023, i kraft två år senare
  - Säkra AI-system, utvecklade i enlighet med grundläggande rättigheter, unionsvärden, rättssäkerhet, förutsebarhet, lagligt, säkert, pålitligt
  - Stränga regler kring AI-system som anses "hög-risk" samt förbjuder vissa applikationer av AI
- Data Governance Act (**DGA**) dataförvaltningsakten
  - Föreslaget 2021, trädde i kraft i juni 2022
  - *"främja tillgången till uppgifter från den offentliga sektorn och skapa en tillförlitlig miljö för att underlätta användningen av sådana uppgifter för forskningsändamål och för skapandet av nya innovativa tjänster och produkter."*
- Digital markets Act (**DMA**)
  - Föreslaget 2020, i kraft senast 2024
  - Göra de digitala marknaderna mer rättvisa och konkurrensutsatta
  - Etablerar tydliga regler och mål för "Grindvakter" (gatekeepers).
    - Grindvakter är de stora digitala plattformarna som erbjuder kärntjänster, dvs sökmotorer, app-stores, meddelandetjänster och liknande.
  - Komplement till EU:s existerande konkurrenslagstiftning

Förhållandet till andra lagar och mellan lagarna

Hur förhåller sig framför allt NIS2 till SSKL (Säkerhetsskyddslagen), DORA och GDPR?

- GDPR och NIS2 gäller inte nationens säkerhet utan omfattar personuppgiftshantering respektive cybersäkerhet.
- När SSKL gäller, övertrumfar den GDPR och NIS2. T ex omfattas inte Försvarsmaktens verksamhet av GDPR.
- NIS2 ställer högre krav på cybersäkerhetsfunktioner än vad "gamla" GDPR gjorde.
- CIA-triaden; GDPR fokuserade på **C** (konfidentialitet), medan NIS2 snarare adresserar **I** (Integritet) och **A** (tillgänglighet).

En verksamhet kan påverkas av flera av dessa lagar. T ex kan ett elhandelsföretag lyda under GDPR för all sin hantering av kunduppgifter men under NIS2 som samhällskritisk verksamhet vad gäller själva eldistributionen.

DORA ”övertrumfar” NIS2 i de fall en organisation berörs av bägge regelverken. DORA går längre i sin kravställning på stabilitet och motståndskraft än NIS2. DORA kräver t ex explicit att organisationen har hotunderrättelser (Threat Intelligence, TI) och regelbunden säkerhetstestning på flera nivåer.

Fredrick Beste, CISSP

IP-Solutions AB 2023-09-12