© IT-Läraren (itlararen.se)

Instuderingsuppgift: Lagar och bestämmelser inom nätverk och säkerhet (EU & Sverige)

Kurs: Nätverksteknologier (gymnasiet) **Område:** Nätverk och säkerhet **Fokus:** EU och Sverige

Syfte

Du ska undersöka hur lagar och andra regler styr arbetet med nätverkssäkerhet i praktiken. Du tränar på att koppla juridiska krav (t.ex. riskhantering, incidentrapportering, åtkomstkontroller, dokumentation) till tekniska och organisatoriska säkerhetsåtgärder i en verksamhet.

Mål

- Beskriva huvudsyftet med centrala EU- och svenska regelverk som påverkar nätverk och cybersäkerhet.
- Förklara skillnaden mellan personuppgiftsincident (GDPR) och cybersäkerhetsincident (t.ex. NIS2/cybersäkerhetslagen) och vad som ska rapporteras.
- Identifiera typiska krav på riskhantering, styrning, kontinuitet och säkerhetsåtgärder och översätta dem till konkreta tekniska kontroller.
- Resonera om ansvar (ledning, IT-drift, leverantörer) och möjliga konsekvenser vid bristande efterlevnad.
- Tillämpa reglerna i ett kort scenario och föreslå en rimlig åtgärdsplan.

Regelverk som ingår (urval)

- **EU:** NIS2-direktivet (Direktiv (EU) 2022/2555) – minimikrav för cybersäkerhet och incidentrapportering i fler sektorer.
- **EU:** GDPR (Dataskyddsförordningen, Förordning (EU) 2016/679) – regler för behandling av personuppgifter och krav vid personuppgiftsincidenter (bl.a. 72-timmarsregeln).
- **EU:** Cybersecurity Act (Förordning (EU) 2019/881) – ENISA:s mandat och ramverk för cybersäkerhetscertifiering av ICT-produkter/tjänster.
- **Sverige:** Cybersäkerhetslagen (svenskt genomförande av NIS2) – krav på riskhantering, säkerhetsåtgärder och incidentrapportering för berörda verksamhetsutövare (i kraft 15 januari 2026).
- **Sverige:** Lag (2022:482) om elektronisk kommunikation (LEK) – bl.a. krav kopplade till säkerhet i elektroniska kommunikationsnät och -tjänster.
- **Sverige:** Säkerhetsskyddslagen (2018:585) – skydd av säkerhetskänslig verksamhet (t.ex. säkerhetsskyddsanalys, behörighetsstyrning, vissa krav vid outsourcing).
- **Sverige:** Offentlighets- och sekretesslagen (2009:400) – sekretessregler för myndigheter och hantering av skyddsvärd information.
- **Sverige:** Brottsbalken – dataintrång (4 kap. 9 c §) som exempel på när IT-händelser också är brott.

Centrala begrepp

- Cybersäkerhet / informationssäkerhet
- Riskhantering (riskanalys, riskägare, riskacceptans)
- Incident / betydande incident
- Personuppgiftsincident
- Konfidentialitet, riktighet (integritet) och tillgänglighet (CIA)
- Leveranskedjesäkerhet / tredjepartsrisk
- Loggning och spårbarhet
- Behörighetsstyrning (least privilege, MFA)
- Kryptering (i transit / i vila)
- Säkerhetsrevision / säkerhetsskanning

Uppgifter

A. Snabb orientering: vad regleras av vad?

1. Förklara i 3–5 meningar vad NIS2/cybersäkerhetslagen handlar om och varför den finns.
2. Förklara i 3–5 meningar vad GDPR handlar om och ge två exempel på personuppgifter som kan förekomma i nätverksloggar.
3. Vad är en *förordning* jämfört med ett *direktiv* i EU? Ge ett exempel från listan ovan på varje.
4. Välj två av de svenska lagarna i listan och beskriv vad de innebär för en IT-/nätverksfunktion i praktiken (t.ex. vilka krav de kan skapa på rutiner, teknik eller dokumentation).

B. Incidenter och rapportering: GDPR vs cybersäkerhetslagen

1. Förklara skillnaden mellan en IT-incident, en cybersäkerhetsincident och en personuppgiftsincident.
2. Vad innebär 72-timmarsregeln vid personuppgiftsincidenter? När börjar tiden räknas och vad ska typiskt dokumenteras?
3. Ge exempel på en incident som: (a) är en personuppgiftsincident men inte en större driftsincident, (b) är en större driftsincident men inte en personuppgiftsincident, (c) är båda.
4. Varför kan samma händelse behöva rapporteras till olika mottagare/myndigheter (t.ex. dataskydd och cybersäkerhet)? Resonera.

C. Krav → kontroll: översätt lagkrav till tekniska åtgärder

Välj **fyra** krav/teman nedan och skriv för varje: (1) vad kravet betyder, (2) en teknisk åtgärd, (3) en organisatorisk åtgärd, (4) hur ni kan kontrollera att åtgärden fungerar (”bevis”).

- Riskanalys och riskbaserade säkerhetsåtgärder
- Åtkomstkontroll (MFA, minst privilegium, behörighetsrecension)
- Loggning, övervakning och incidentdetektering
- Sårbarhetshantering (patchning, scanning, prioritering)
- Backup/återställning och kontinuitetsplanering
- Segmentering av nät och skydd av kritiska system
- Kryptering och nyckelhantering

- Leveranskedjesäkerhet (krav på leverantörer, avtal, uppföljning)
- Utbildning och medvetenhet (phishing, rutiner)

D. Case: "Ransomware i skolans nät" (tillämpningsuppgift)

Scenario: En organisation får en misstänkt ransomware-incident. Flera filservrar blir krypterade och användare kan inte logga in. IT upptäcker samtidigt ovanlig utgående trafik från en server. I loggarna finns användar-ID:n och IP-adresser. Det finns indikationer på att ett konto med admin-rättigheter missbrukats. Leverantören som sköter drift av en del system nås via fjärråtkomst.

1. Lista **tre** saker ni gör första timmen (tekniskt) och motivera varför (t.ex. isolering, bevis, stoppa spridning).
2. Vilka delar av händelsen kan bli en **personuppgiftsincident** enligt GDPR? Motivera.
3. Vilka roller behöver kopplas in (t.ex. IT-säkerhet, ledning, dataskydd, kommunikation, leverantör) och varför?
4. Vilka krav/skyldigheter kan bli aktuella att uppfylla eller visa upp (t.ex. dokumentation, incidentrapportering, loggar)? Koppla till minst **två** regelverk i listan.
5. Föreslå en kort **åtgärdsplan** för 7 dagar framåt: återställning, hårdning, uppföljning och lärande.

E. Certifiering och krav vid inköp

1. Vad är poängen med ett EU-gemensamt ramverk för cybersäkerhetscertifiering (Cybersecurity Act)? Resonera utifrån perspektiven "tillit" och "gemensam marknad".
2. Ge exempel på hur en organisation kan använda certifiering, krav i avtal och uppföljning för att minska leverantörsrisk.
3. Välj ett IT-inköp (t.ex. brandvägg, identitetsplattform, molnlagring). Skriv **fem** säkerhetskrav du skulle ta med i upphandlingen/avtalet och koppla varje krav till en risk.

F. Reflektion (kort)

1. Vilket regelverk upplever du påverkar nätverksarbete mest i praktiken – och varför?
2. Ge ett exempel på en säkerhetsåtgärd som både förbättrar teknisk säkerhet och hjälper regelefterlevnad. Ge också ett exempel där säkerhet och integritet kan hamna i konflikt.

Inlämning

- Lämna in som dokument (PDF eller Word).
- Använd rubrikerna A–F i din text så att det är lätt att följa.
- Skriv tydligt och använd fackspråk där det passar, men förklara med egna ord.
- Ange källor (länkar) i slutet under rubriken **Källor**. Prioritera myndigheter och EU-källor.

Bedömning (översikt)

Aspekt	Grundläggande nivå	God nivå	Mycket god nivå
Regelverksförståelse	Beskriver några regelverk översiktligt.	Förklarar flera regelverk och skiljer på deras syften.	Jämför regelverk, visar god begreppskoll och ger träffsäkra exempel.

Tillämpning (krav → åtgärd)	Ger exempel på åtgärder men kopplingen är ibland otydlig.	Kopplar krav till relevanta tekniska/organisatoriska åtgärder och "bevis".	Resonerar riskbaserat, prioriterar och visar förståelse för trade-offs.
Incidentresonemang	Identifierar incidenttyper på en grundnivå.	Skiljer tydligt på personuppgiftsincident och cybersäkerhetsincident och motiverar.	Gör nyanserade bedömningar, roller/ansvar och tydlig tidslinje.
Källor och fackmässighet	Enstaka källor, blandad kvalitet.	Flera relevanta källor, mestadels myndigheter/EU, korrekt användning.	Väl valda primärkällor, god källkritik och tydliga referenser.

Förslag på källor att utgå från (skriv länkarna i din källista)

- EU-kommissionens faktasidor om NIS2-direktivet.
- Myndigheten för civilt försvar (MCF): information om cybersäkerhetslagen (NIS2 i Sverige) och vägledningar.
- Integritetsskyddsmyndigheten (IMY): vägledning om personuppgiftsincidenter.
- Riksdagen/SFS: originaltexter för LEK (2022:482), säkerhetsskyddslagen (2018:585) och OSL (2009:400).
- EUR-Lex: Cybersecurity Act (Förordning (EU) 2019/881).

Avgränsning: Uppgiften handlar om att förstå och tillämpa krav på en nivå som passar gymnasiekursen. Du ska inte göra juridiska bedömningar "som en jurist", utan visa att du kan koppla reglerna till säkerhetsarbete i nätverk.