Cybersäkerhet Mognadsrapport 2025

OneMore Secure

Utgiven av OneMore Secure AB

Utgåva 1 - Oktober 2025

©OneMore Secure 2025. All rights reserved.

www.onemoresecure.com

Innehållsförteckning

Förord

Föreställ dig en karta över Sveriges digitala landskap. På den kartan ser vi inte bara våra styrkor, utan också de sprickor som kan bli avgörande vid en kris. Den här rapporten är just en sådan karta, en unik inblick i hur vi tillsammans lyckas, misslyckas och framför allt lär oss i arbetet med cybersäkerhet.

När vi sammanställde resultatet slogs vi av något hoppfullt: Sverige har kommit längre än vad många tror. Men vi ser också en sanning som inte går att blunda för: Sveriges motståndskraft, kontinuitet och grundläggande cyberhygien är inte självklar. Det kräver uppmärksamhet och allas gemensamma ansvar.

”Cybersäkerhet Mognadsrapport 2025” baseras på data från över 750 verksamheter och ger en av de mest omfattande lägesbilderna hittills i Sverige. Mognadsrapporten visar med tydlighet att cybersäkerhet inte bara handlar om teknik, det är i lika hög grad en ledningsfråga, en kulturfråga och en fråga om förtroende mellan affärspartners. Cybersäkerhet är en fråga för hela verksamheten.

Styrkor och utmaningar

Det finns mycket att bygga vidare på utifrån den kunskap rapporten ger. Vi ser förhållandevis hög mognadsgrad i incidentrapportering och policyarbete. Samtidigt visar resultaten att viktiga grundåtgärder såsom logghantering, multifaktorautentisering och säker konfiguration fortfarande saknas i många verksamheter. Åtgärder som enligt NIS2, GDPR och ENISA:s rekommendationer borde vara självklara.

Ännu mer talande är kunskapsbristen vi ser på ledningsnivå vad gäller cybersäkerhet. När det inte finns på styrelsens eller ledningsgruppens agenda blir arbetet lätt splittrat och otillräckligt.

Självskattning och mognadsgrad

Vi är medvetna om att rapporten har begränsningar. Självskattningar kan snedvrida bilden, och vissa sektorer är underrepresenterade. Resultaten i rapporten visar dock att många inte skönmålar sina utmaningar. Detta är ett tecken på att medvetenheten ökar.

Ett nytt regelverkslandskap

Med EU:s NIS2, DORA och Cyber Resilience Act förändras spelplanen. Säkerhet är en skyldighet juridiskt, organisatoriskt och etiskt. Genom att sätta resultaten i relation till dessa krav kan rapporten hjälpa verksamheter att se gemensamma brister och utmaningar samt ge en bild av hur vi framöver bygger ett motståndskraftigt samhälle.

Med denna rapport vill vi på OneMore Secure erbjuda en bild över mognadsgraden gällande cybersäkerhet i Sverige och möjligheten att förändra den. Inte bara för att uppfylla direktiv, utan för att bygga motståndskraft mot cyberhot i enskilda verksamheter, leveranskedjor och samhället i stort.

Robert Willborg
Cybersäkerhetsexpert, rådgivare och sakkunnig

Om OneMore Secure och dess data

I OneMore Secures (OMS) saas-tjänst för säkerhet i leveranskedjan visualiseras risker och sårbarheter i leveranskedjan. Både kunder och leverantörer svarar på en digital deklaration för att åskådliggöra verksamhetens mognadsgrad när det gäller cybersäkerhet. Verksamheten får ett säkerhetsindex (mellan 0–5), ett Key Performance Indicator (KPI), som är jämförbart mellan verksamheter. Uppföljningen är automatiserad under hela avtalsperioden. Har en leverantör tidigare svarat på säkerhetsdeklarationen för en kund, så behöver de inte svara igen för en annan kund, de accepterar bara relationsförfrågan och den nya kunden får då tillgång till leverantörens resultat.

Grunddeklarationen innehåller kontroller som täcker säkerhetskultur, informationssäkerhet, IT-säkerhet och Integritetsskydd (GDPR). Det finns även tilläggskontroller för efterlevnad av NIS2, DORA, Säker utveckling, AI-Förordningen. I denna rapport redovisar vi endast data för NIS2, då övriga tilläggskontroller för närvarande innehåller för få data för att vi ska kunna dra några tillförlitliga slutsatser. Kontrollerna i tjänstens säkerhetsdeklaration bygger på, och är mappade mot, bland annat de stora ramverken ISO27000, NIST, CIS18. Kontrollerna är formulerade på ett mer användarvänligt, pedagogiskt och begripligt språk.

All data bygger på självskattningar från leverantörer och kunder. Tredjepartsvalidering är dock något som kommer att bli krav med NIS2 och DORA, och kommer troligtvis att öka i omfattning framöver.

Översikt över cyberlandskapet

Hotbilden mot vårt digitala samhälle fortsätter att utvecklas snabbt, drivet av alltmer sofistikerade cyberhot, geopolitiska spänningar och utbredda svagheter inom de globala leveranskedjorna.

Verksamheter i samtliga sektorer står i dag inför ett flertal samtidiga och överlappande hot:

- **Utpressningstrojaner (ransomware)** fortsätter vara det mest kostsamma hotet globalt, med en genomsnittlig driftstörning för drabbade verksamheter på över 21 dagar och genomsnittliga kostnader som stiger år för år (ENISA, 2023 Covewave 2020).
- **Nätfiske (phishing)** utgör porten till många incidenter och riktar sig främst mot mänskliga sårbarheter – särskilt i tider av organisatorisk stress eller förändring (ENISA, 2022).
- **Distributed denail of service, s.k. DDoS-attacker** används både som störning och som distraktion vid mer komplexa angrepp.
- **Supply chain-attacker** (SolarWinds, Kaseya, MOVEit) visar att sårbarheter hos tredje part ofta fungerar som språngbräda in i skyddade miljöer (ENISA, 2021).
- **Avancerade ihållande hot, s.k. APT-aktörer och statligt stödd cyberkrigföring** har ökat kraftigt i omfattning efter invasionen av Ukraina, där kritisk infrastruktur, media och finanssektorer utgör prioriterade mål (MSB & NCSC, 2024).

Samtidigt har geopolitiska spänningar ökat de statligt sponsrade cyberattackerna som riktar sig mot kritisk infrastruktur och känsliga sektorer, vilket förstärker behovet av robusta cybersäkerhetsramar och proaktiva försvarsmekanismer.

Sammantaget kan vi konstatera att cybersäkerhet inte längre är en teknisk stödfunktion eller en kostnadspost, utan en strategisk förutsättning och investering för stabil verksamhetskontinuitet. Den ökade kopplingen mellan hotaktörer och nationella intressen innebär dessutom att hoten är samhällspolitiska och inte bara ekonomiska.

Attacker mot leveranskedjan

Attacker mot leveranskedjan är en realitet där angriparen utnyttjar asymmetrin mellan små leverantörers svaga skydd och större kunders beroende av dem. Angripare riktar sig strategiskt mot tredjepartsaktörer med bristfälliga cybersäkerhetsrutiner, för att komma åt deras kunders data.

Incidenter som SolarWinds (2020), Kaseya (2021) och MOVEit (2023) visar hur en enskild sårbar leverantör kan bli **systemhotande**. I SolarWinds-fallet påverkades 18 000 kunder, inklusive amerikanska federala myndigheter och Fortune 500-företag. Kaseya incidenten är i Sverige mer känd som Coop-attacken. MOVEit-incidenten under 2023 drabbade över 2600 verksamheter globalt, inklusive flera svenska kommuner och statliga aktörer och över 93 miljoner individer (NCSC Sverige, 2024, Emisoft 2024).

I en alltmer sammankopplad värld räcker det att en aktör i ekosystemet är oskyddad för att hela kedjan ska bli sårbar. Enligt ENISA (2021) kan 66 % av cyberattacker som drabbar större verksamheter härledas till tredje part. Det sker genom bristande segmentering, svaga autentiserings- och uppdateringsrutiner eller dataöverföring med bristande och/eller utan korrekt kryptering mellan partner. Denna siffra stöds nationellt av MSBs rapport från 2021.

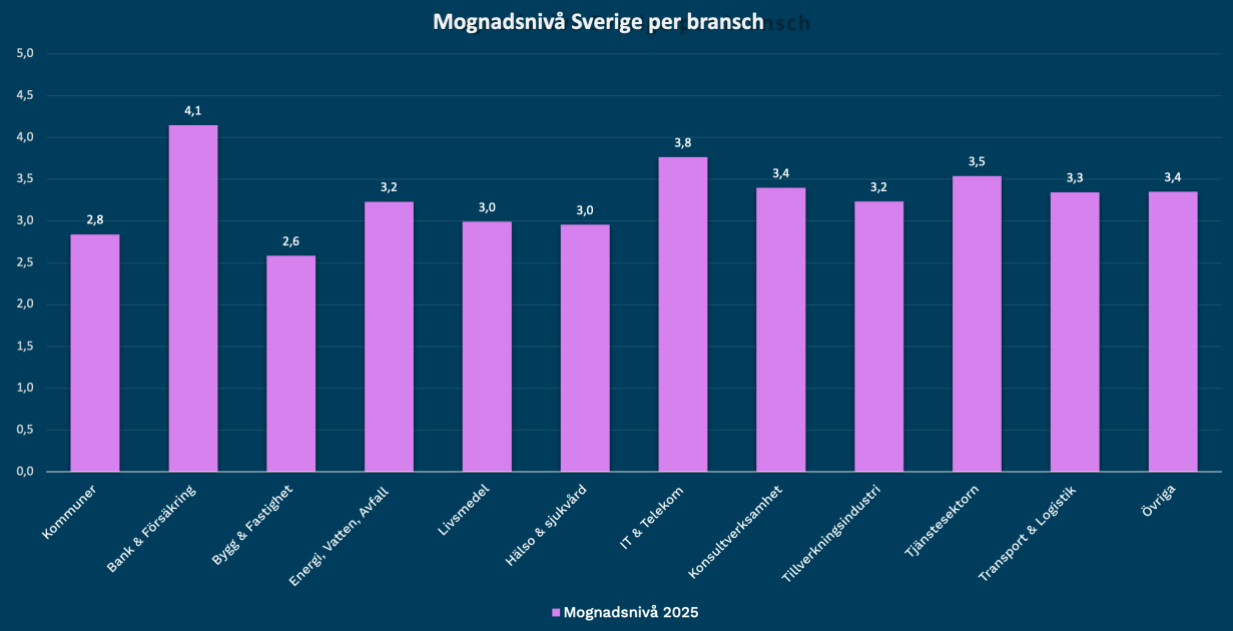
EU:s **NIS2-direktiv** (artiklarna 21–23) och **Cyber Resilience Act** ställer explicita krav på att verksamheter tar ansvar för säkerheten i sin leveranskedja, både juridiskt och operativt. Det innebär att proaktiva åtgärder som riskklassificering av leverantörer, tydliga säkerhetskrav i avtal (t.ex. MFA, incidentrapportering, säker logghantering) och löpande uppföljning inte längre är frivilliga.

Det betyder också att varje verksamhet måste betrakta sina leverantörer som en förlängning av sin egen digitala infrastruktur och därmed sin egen attackyta.

Övergripande Insikter

Cybersäkerhetsmognad efter bransch

När vi tittar på mognadsgraden hos olika branscher så ser vi ganska stora skillnader. Mognadsgraden spänner mellan 2,6 och 4,1 på en femgradig skala. Genomsnittlig mognadsgrad är 3,5. En viktig aspekt är att många av verksamheterna i rapporten är IT & Telekomföretag. Dessa har en mognadsgrad på 3,8 i genomsnitt. Det drar upp snittet för alla. Skulle vi exkludera IT & Telekom hamnar den genomsnittliga mognadsgraden på 3,3.



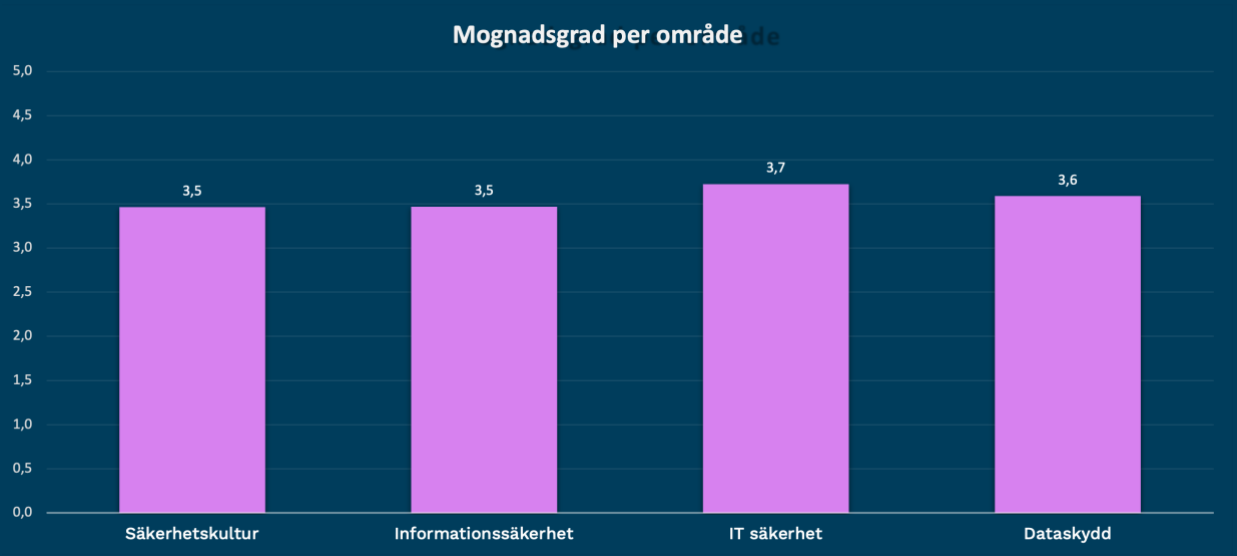
1. **IT & Telekom** prioriterar regelbundna säkerhetsbedömningar, omfattande incidenthanteringsplaner och proaktiv hotinformation. Trots starka övergripande resultat med ett genomsnitt på 3,8 måste IT och telekom fortsätta att vara vaksamma mot snabbt föränderliga hot på grund av deras centrala roll i infrastrukturer.
2. **Bygg & Fastighetsbranschen** presenterar över lag låga mognadsnivåer för cybersäkerhet med ett genomsnitt på 2,6. Trots att fastighetsbranschen hanterar omfattande finansiella och personliga data uppvisar den anmärkningsvärda luckor när det gäller robusta cybersäkerhetsåtgärder, inklusive begränsad användning av avancerade säkerhetsrutiner som kontinuerlig övervakning och detaljerade leverantörsutvärderingar. Bygg-

och fastighet är två ganska skilda branscher men är i rapporten hopslagna då de visar i stort sett samma mognadsgrad.

3. **Bank och försäkring** uppvisar högst cybersäkerhetsmognad på 4,1 tack vare stränga regulatoriska krav och det höga värdet hos de data som hanteras. Branschen lyder också i större utsträckning under DORA som varit i kraft sedan januari 2025.
4. **Hälso- och sjukvård** uppvisar måttlig cybersäkerhetsmognad på 3,0, vilket kan ha att göra med betydande sårbarheter på grund av komplexiteten och känsligheten hos hälso- och sjukvårdsdata. Sektorn bör prioritera att säkra elektroniska patientjournaler (EHR), säkerställa efterlevnad av bestämmelser om skydd av hälsodata och stärka försvaret mot utpressningstrojaner.
5. **Tillverkningsindustrin** visar måttlig cybersäkerhetsmognad med ett genomsnitt på 3,2 med utrymme för förbättringar, särskilt när det gäller att säkra ICS- (Industrial Control Systems) och IoT-enheter (Internet of Things). Det är viktigt att förbättra ramverken för cybersäkerhet och incidenthanteringsplaner som är skräddarsydda specifikt för tillverkningsmiljöer.
6. **Energi och allmännyttiga företag** har en måttlig mognadsgrad på 3,2 vilket gör det lite problematiskt utifrån att de levererar kritisk infrastruktur i samhället. Just deras roll gör dem till attraktiva måltavlor och de står inför kritiska cybersäkerhetsutmaningar. Att stärka cybersäkerhetspraxis, anta avancerade övervakningsverktyg och regelbundna säkerhetsövningar är avgörande för att skydda driftskontinuitet och infrastrukturstabilitet.
7. **Transport och logistik** har en måttlig mognadsnivå på 3,3 med betydande sårbarheter relaterade till störningar i leveranskedjan, IoT-säkerhet och navigationssystem. Förbättrade cybersäkerhetsprotokoll, grundliga leverantörsbedömningar och fokuserade utbildningsinitiativ bör prägla initiativ för att minska dessa risker.

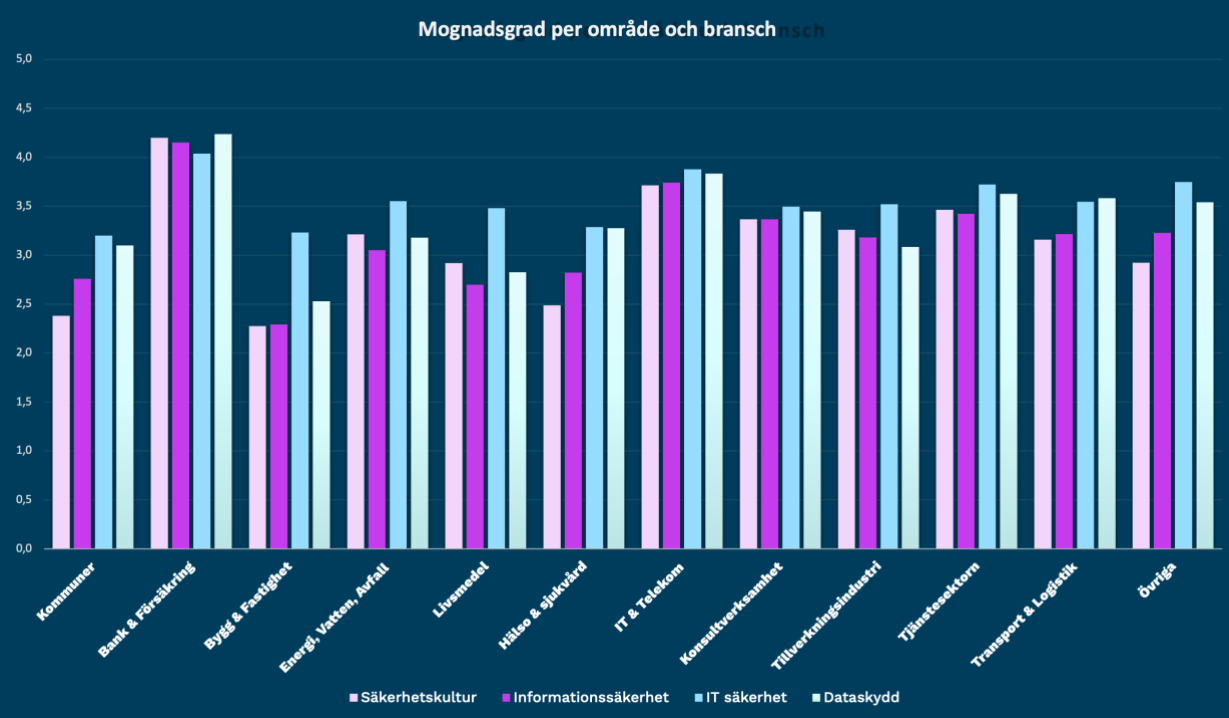
Cybersäkerhetsmognad efter område

Tittar vi på enskilda områden i deklarationen så ser vi att medelvärdet är något varierande där svenska verksamheter visar högst mognad inom IT-säkerhet 3,7 och Dataskydd (GDPR) 3,6. Strax under kommer säkerhetskultur och informationssäkerhet på 3,5.



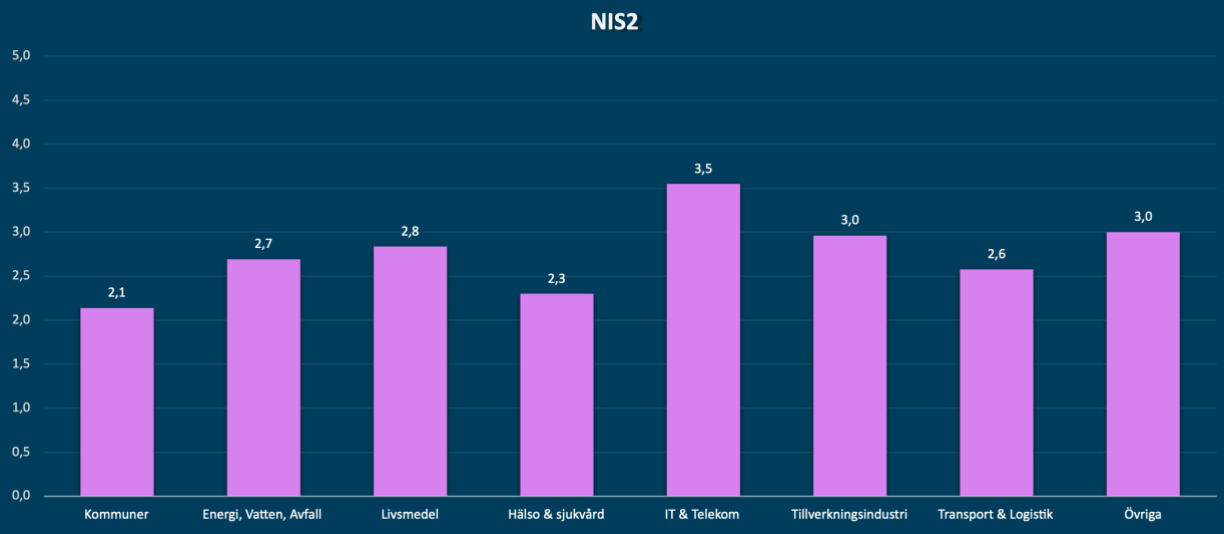
Cybersäkerhetsmognad efter bransch och område

I nästa steg går vi än längre och bryter vi ner data på bransch och område. Tittar vi närmare på sektionen kring säkerhetskultur ser vi att kommuner, bygg- och fastighetsbranschen samt Hälso- och sjukvård sticker ut negativt. Vissa branscher har även en låg mognadsgrad kring dataskydd. Detta kan anses anmärkningsvärt eftersom GDPR varit i laga kraft sedan 2015.



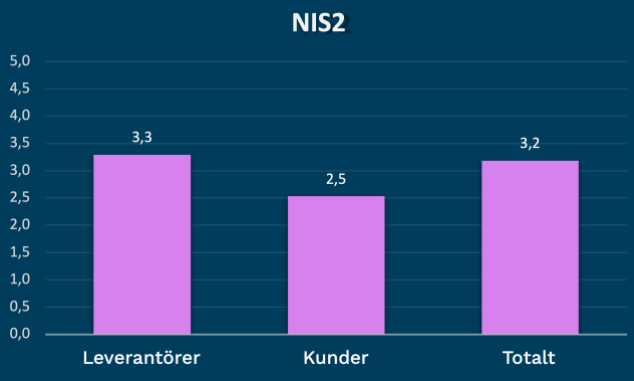
NIS2

NIS2 (Direktivet för säkerhet i Nätverk och informationssystem) genomförs i Sverige via en ny Cybersäkerhetslag som enligt lagrådsremissen föreslås gälla från **15 januari 2026**. Rapporten visar tydligt att svenska verksamheter har mycket att göra för att efterleva lagen när den kommer. Av de som berörs direkt (berörda branscher) och indirekt (leverantörer), uppfyller inte 78% av verksamheterna kraven i NIS2.



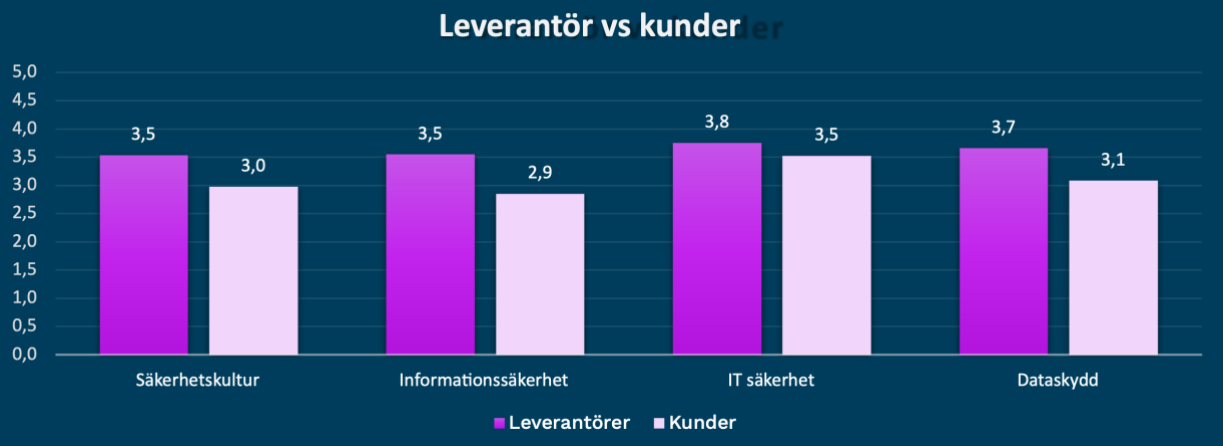
Mognadsnivån för alla gällande NIS2 är 3,2 vilket får anses vara medel och följer mognadsgraden kring övriga områden (3,5). De branscher som sticker ut negativt är kommuner (2,1) och hälso- och sjukvård (2,3). Återigen visar IT & Telekom en hög mognad (3,5).

Samtidigt ser vi på svaren under NIS2 att det är en skillnad mellan de som är registrerade som leverantörer och de som är direkta kunder till dem. Det kan återigen förklaras med att många leverantörer är IT-företag som uppvisar en högre mognadsgrad.



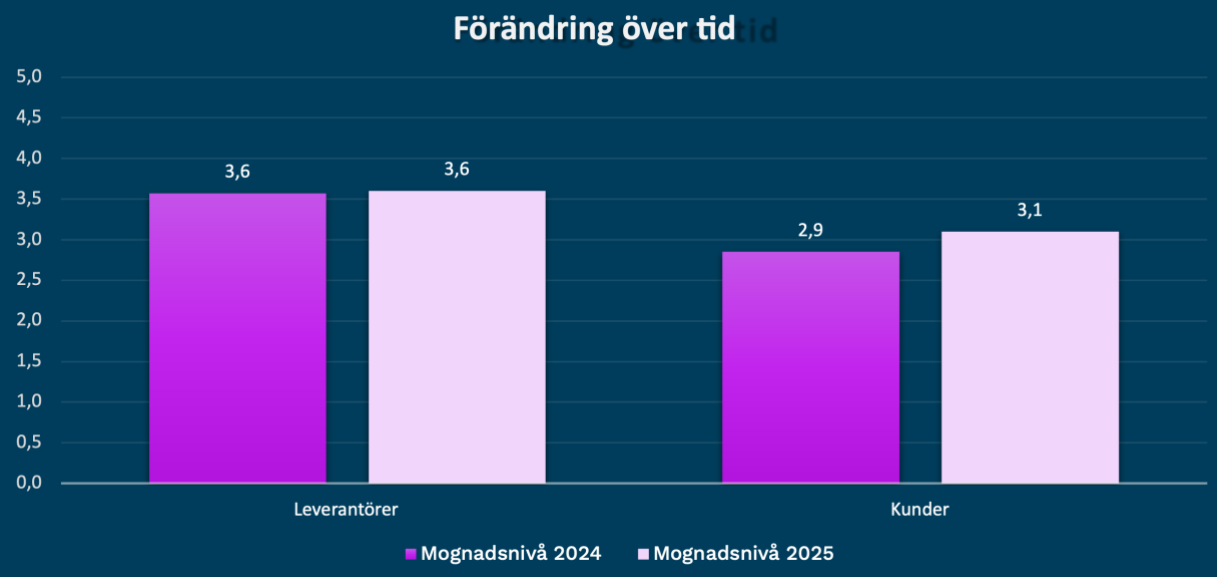
Leverantörer vs kunder

Om vi fördjupar oss lite i skillnaderna mellan leverantörer och kunder så ser vi ett par intressanta saker. Kunder har en genomsnittlig mognadsgrad om 3,1 medans leverantörer har en mognadsgrad på 3,6. Att leverantörerna har en högre mognadsgrad kan åter igen förklaras med att många leverantörer är IT-företag vilka allmänt har en högre mognadsgrad. Kunderna återfinns i alla branscher. Skillnaden mellan kunder och leverantörer är minst under IT-säkerhet.



Förändringar över tid

Hos leverantörer så ser vi ingen större ökning av mognadsgrad mellan 2024 och 2025. Kundernas mognadsgrad ökar dock något från 2,9 till 3,1 i genomsnitt.

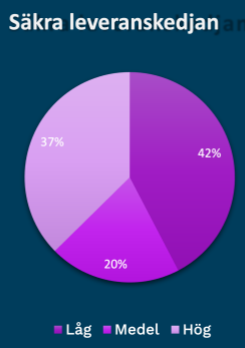


Insikter om specifika kontroller

Vi ger i denna rapport ett urval av kontroller för att visa på mognadsgraden för några specifika frågor.

Säkra leveranskedjan

Kontrollen för säkra leveranskedjor sticker ut. Hela 42 % av verksamheterna uppvisar en låg mognadsgrad kring säkra leveranskedjor. Det placerar denna kontroll bland de absolut svagaste i hela rapporten. Att skillnaden mellan branscher är liten tyder på att detta är en genomgående nationell svaghet, inte ett nischproblem.



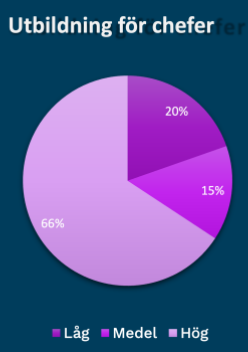
Detta är särskilt allvarligt i ett läge där cybersäkerheten blivit ett geopolitiskt verktyg. Statliga och statsstödda aktörer riktar sig i allt högre grad mot leverantörer i väst för att nå in i samhällskritisk infrastruktur, en trend bekräftad i både ENISA:s och MSB:s hotbildsanalyser. Angrepp via tredjepart har, efter Rysslands invasion av Ukraina 2022, ökat med över 100 % enligt flera internationella underrättelserapporter.

I en sådan omvärld kan Sveriges låga mognad vad gäller säkerhet i leveranskedjan inte försvaras. Det handlar inte längre bara om regelefterlevnad enligt NIS2 och DORA, utan om nationell motståndskraft. Att vi i ett digitalt integrerat samhälle inte har bättre koll på vilka vi är beroende av, och hur sårbara de är, utgör en risk för hela samhället.

Den strategiska frågan är alltså inte längre *om* vi behöver stärka kontrollen i leveranskedjan, utan *hur snabbt* vi kan etablera grundläggande kontroller, kravställning och uppföljning.

Utbildning för chefer

Att chefer förstår cybersäkerhetsrisker kopplade till sina roller är avgörande. Detta för att beslutsfattande under tidspress eller osäkerhet ofta är den svagaste länken vid incidenter. Ett strukturerat utbildningsprogram för ledare skapar inte bara ökad medvetenhet, utan också förmåga att leda med säkerhet i fokus.



Att 66 % av verksamheterna har hög mognadsgrad inom chefsutbildningar, och 71 % när det gäller utbildning för anställda, är positiva siffror i sammanhanget. Men det finns en risk för feltolkning: höga nivåer av generell utbildning betyder inte att verksamheterna är tillräckligt förberedda för den psykologiska belastning och desinformation som ofta förekommer i moderna cyberincidenter, särskilt från statliga aktörer. Närmare en tredjedel av alla har en låg mognadsgrad när det gäller desinformation och informationspåverkan.

Sverige befinner sig just nu i ett skärpt säkerhetsläge, där påverkan och kognitiv manipulation blivit ett allt vanligare inslag vid cyberoperationer. I detta läge måste ledarskapets säkerhetsmedvetande omvandlas från medvetenhet till **operativ förmåga**. Det räcker inte med att "ha utbildat", det krävs att ledare kontinuerligt tränas i att fatta beslut under tryck, tolka tekniska risker och agera samlat vid kriser.

I NIS2 betonas behovet av ledningsansvar och personlig ansvarsskyldighet vid säkerhetsbrister. Det betyder att chefsutbildningar är ett konkret ansvar enligt EU-rätt.

Årliga säkerhetsgranskningar

Att mer än var fjärde verksamhet inte genomför någon säkerhetsgranskning under ett år är ett allvarligt tecken på bristande processmognad. Säkerhetsgranskningar är inte en formalitet. De är navet i det kontinuerliga förbättringsarbetet. Utan dem saknas både lägesbild och kontroll över om identifierade brister faktiskt åtgärdats.

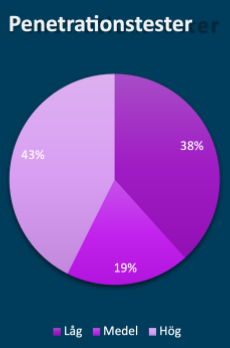
Från ett riskperspektiv är detta särskilt oroande eftersom hotbilden förändras snabbt, både tekniskt och geopolitiskt. På senare tid har hotaktörer skiftat taktik mer frekvent, bland annat genom att kombinera cyberangrepp med påverkans-kampanjer. En verksamhet som inte har återkommande kontroller riskerar att fokusera på en gammal hotbild eller i värsta fall, ingen hotbild alls.

Både NIS2 och kända ramverk ställer krav på löpande intern kontroll, dokumentation och uppföljning. Men från rapportens data framgår att detta fortfarande inte är en självklar del av den operativa kulturen i många svenska verksamheter. Det tyder på att säkerhetsarbetet fortfarande i många avseenden är reaktivt snarare än förebyggande.

Att etablera en årlig, halvårsvis eller helst kvartalsvis, granskning är inte bara ett efterlevnadskrav. Det är en förutsättning för robusthet. Utan det står verksamheter sämre rustade både att stå emot nästa incident.

Penetrationstester

Att 38 procent av verksamheterna har låg mognadsgrad avseende penetrationstester är oroande, särskilt med tanke på vilken central roll dessa säkerhetstester spelar för att upptäcka sårbarheter innan en angripare gör det. Även om majoriteten har någon form av testning på plats, visar siffran att det fortfarande finns en blind fläck i svensk cybersäkerhetskultur i offensiv säkerhetsvalidering.



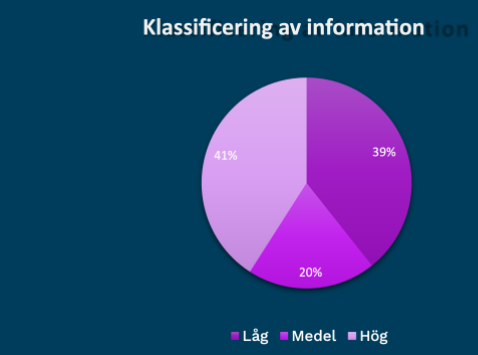
Penetrationstester är en etablerad metod för att simulera verkliga attacker och validera försvars-förmågan i praktiken. Det räcker inte att ha säkerhetssystem på plats, viktigt är också att testa om de faktiskt håller.

De senaste åren har flera incidenter visat att brister ofta upptäcks först efter att skadan är skedd. Många av dessa hade kunnat förhindras med regelbundna tester och åtgärder mot sårbarheter.

NIS2 och även Cyber Resilience Act understryker vikten av att sårbarheter hanteras proaktivt. Att vara förberedd är i dag inte bara en teknisk fråga. Det är en ledningsfråga, ett ansvar, och en direkt indikator på verksamhetens motståndskraft.

Klassificering av information

Dataklassificering är grunden för att kunna skydda information på rätt sätt. Utan den vet man inte vilka tillgångar som är mest skyddsvärda, vilket gör det omöjligt att prioritera insatser. Trots detta saknar 39 procent av verksamheterna helt policy, process och/eller utbildning kopplat till dataklassificering.



Det innebär att nästan hälften av verksamheterna riskerar att behandla känslig information som vilken data som helst. Detta ökar risken för läckor, felaktig åtkomst och bristande efterlevnad av regelverk som GDPR och NIS2 men även ramverk, standarder och normer.

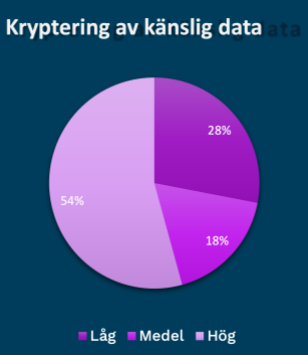
I en miljö där informationsläckor utnyttjas inte bara för ekonomisk vinning utan också som påverkansmedel i hybridkonflikter är det särskilt allvarligt. Det senaste året har flera incidenter visat hur interna dokument, felaktigt hanterade, har läckt ut och använts i informationsoperationer riktade mot både myndigheter och företag.

Regelverk som GDPR ställer krav på att känsliga personuppgifter hanteras med särskild försiktighet, men utan dataklassificering blir sådan kontroll svår att genomföra i praktiken. Även DORA och Cyber Resilience Act förutsätter att verksamheter vet vilka data som kräver särskilt skydd.

Här krävs en snabb uppväxling då våra data indikerar att grundläggande säkerhetsförmåga fortsatt saknas hos en stor andel av verksamheterna.

Kryptering av känsliga data

Kryptering är en av de mest grundläggande teknikerna för att skydda känslig information, både i vila och under överföring. Trots det visar resultaten att över var fjärde verksamhet inte krypterar sina känsliga data. Det är en oroande siffra, särskilt med tanke på att det inte bara är en rekommendation, utan ett krav enligt både GDPR och NIS2.



Att lämna data okrypterad innebär att ett intrång snabbt kan leda till full exponering av personuppgifter, affärshemligheter eller system-information. I ett förhöjt geopolitiskt läge, där cyberoperationer ofta syftar till just stöld av data och informationspåverkan, blir konsekvenserna ännu mer allvarliga.

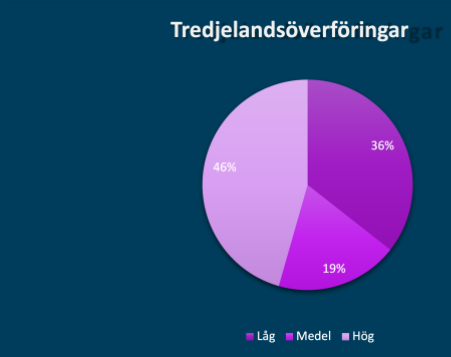
Under senare år har flera incidenter, bland annat inom offentlig sektor i Norden, visat hur bristande kryptering lett till att stora mängder data snabbt kunnat läsas, spridas och utnyttjas i utpressningssyfte. I vissa fall har angriparna inte ens behövt dekryptera, data var redan i klartext.

Krav enligt artikel 32 i GDPR och artikel 21 i NIS2 är tydliga: känsliga uppgifter ska skyddas med starka tekniska och organisatoriska åtgärder.

Att så många verksamheter fortfarande inte krypterar känsliga data visar på ett glapp mellan lagstiftning och praktisk implementering som behöver stängas, snabbt.

Tredjelandsöverföringar

Mer än var tredje verksamhet genomför inte en Transfer Impact Assessment (TIA) vid överföring av personuppgifter till tredjeland. Det innebär att en betydande andel saknar strukturerad bedömning av om överföringen uppfyller kraven enligt GDPR, särskilt artiklarna 45, 46 och 49.



En TIA är avgörande för att identifiera om den mottagande staten har lagar eller praxis som undergräver skyddet av personuppgifter. Att säkerställa att så inte är fallet är centralt efter EU-domstolens vägledande dom i Schrems II. Brister verksamheter här kan det snabbt leda till olaglig behandling, överträdelser av individers rättigheter och få kännbara sanktioner.

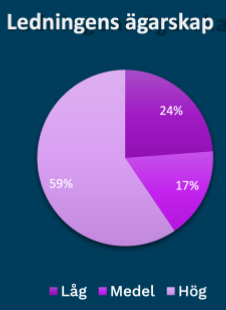
I ett omvärldsläge där persondata allt oftare används som råvara i geopolitiska intressen, inklusive massövervakning, profilering och påverkan, blir bedömningen av tredjelandsrisk inte bara en juridisk fråga, utan även en strategisk.

EDPB:s rekommendationer 01/2020 ställer tydliga krav på dokumentation, tekniska skyddsåtgärder och övervakning av tredjelands lagstiftning. Verksamheter som inte genomför TIA riskerar att stå sig slätt om tillsynsmyndigheter ställer dem till svars eller om incidenter inträffar.

Våra data kan läsas som en tydlig signal: efterlevnaden inom tredjelandsöverföring måste förbättras. Det räcker inte att lita på standardavtal eller tredjepartsförsäkringar. Riskerna måste analyseras och hanteras konkret.

Ledningens ägarskap

NIS2 tydliggör att det inte längre räcker att delegera säkerhetsansvar nedåt i verksamheten. Ledningen måste enligt direktivet aktivt uppfylla kraven och kan hållas personligen ansvarig enligt nationell rätt. Det handlar inte bara om formellt ansvar, utan om faktisk delaktighet i konsekvensbedömningar, riskanalyser och GAP-analyser kopplade till säkerhet och efterlevnad.



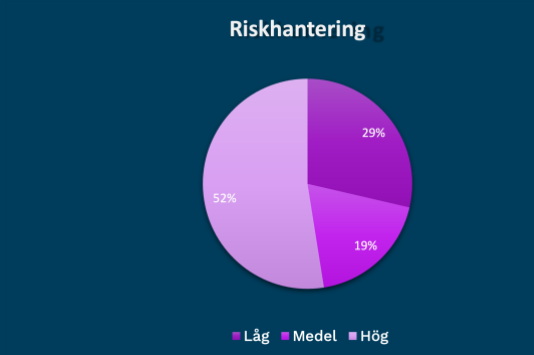
Rapportens data visar att många verksamheter har börjat utbilda ledningsnivån i NIS2 och involverar dem i strategiska processer. Det är positivt. Men i praktiken är det fortfarande vanligt att cybersäkerhet betraktas som ett tekniskt specialistområde, inte som en integrerad del av affärsstyrningen.

I ett osäkert geopolitiskt läge, där kritisk infrastruktur är ett strategiskt mål för statsstödda cyberangrepp, är detta en farlig inställning. Felbedömningar i ledningsrummet kan få lika allvarliga konsekvenser som tekniska sårbarheter. NIS2 tydliggör detta genom att lägga ansvaret direkt på styrelse- och ledningsnivå.

Ledningens förmåga att förstå, väga och agera på cybersäkerhetsrisker är nu en förutsättning för regelefterlevnad, men också för affärskritisk motståndskraft.

Riskhantering

Enligt NIS2 ska verksamheter ha formella policyer och rutiner för att identifiera, hantera och följa upp risker. Inte bara inom IT, utan ur ett helhetsperspektiv för hela verksamheten. Det innebär ett allriskangreppssätt där cyberhot bedöms i relation till affärsverksamhet, drift, leverantörs-beroenden och samhällspåverkan.



Trots det saknar närmare en tredjedel av verksamheterna en process för riskhantering. Det är särskilt oroande då det rör sig om en kärnkomponent i efterlevnaden av NIS2 och en direkt förutsättning för att kunna hantera risker mot verksamheten.

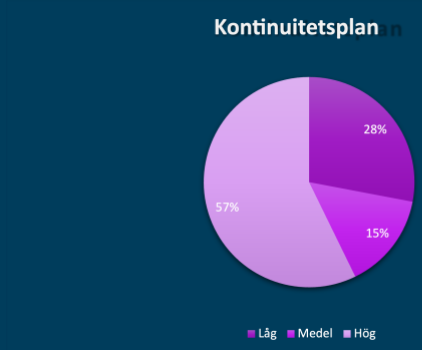
I dagens läge, där hybridpåverkan, desinformation och cyberangrepp alltmer smälter samman krävs en samlad bild för att förstå hur olika hot samverkar och påverkar verksamheten strategiskt.

Frånvaron av helhetsrutiner gör det svårt att fånga just dessa kopplingar, och ökar risken att allvarliga sårbarheter förblir osynliga. I värsta fall innebär det att risker inte upptäcks förrän de materialiseras som incidenter.

Tydligt är att allriskperspektivet inte är en administrativ detalj i NIS2. Det är ramen för hela säkerhetsstyrningen.

Kontinuitetsplan

Cyberhygien och förmåga till motståndskraft och kontinuitet ställer krav på att verksamheter har en dokumenterad plan för att upprätthålla och säkerställa kontinuitet vid störningar, inklusive backup, krishantering och återställning efter incidenter. Planen ska hållas uppdaterad och innehålla aktuell information om tillgångar, ansvarsfördelning och kontaktpersoner.



Trots detta saknar över en fjärdedel av verksamheterna en sådan kontinuitetsplan. Det innebär att många verksamheter står utan ett förankrat regelverk för hur de ska hantera allvarliga driftstörningar, oavsett om de orsakas av cyber-attacker, leverantörsproblem eller samhällskriser.

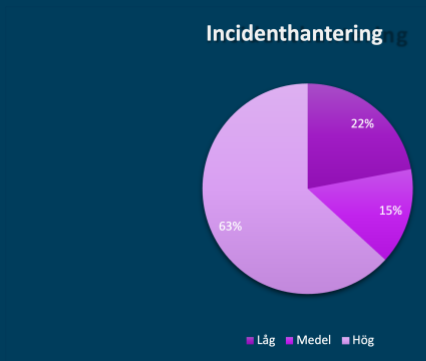
Det geopolitiska läget kräver förmåga att hantera konsekvenserna av angrepp och återgå till drift på ett kontrollerat sätt. Att sakna en plan för detta är inte bara ett brott mot NIS2, det är en strategisk sårbarhet.

Ett exempel är ransomware-attacker där frånvaron av fungerande kontinuitetsplaner förlänger tiden hela eller delar av verksamheten ligger nere med veckor. Samma mönster har setts i flertalet attacker, där osäkerhet kring återställning förvärrat effekterna av incidenter.

Kontinuitetsplanen är en kärnkomponent i verksamhetens motståndskraft och bör behandlas därefter.

Incidenthantering

Enligt NIS2 ska alla verksamheter ha en dokumenterad incidenthanteringsplan som omfattar både tekniska och organisatoriska åtgärder. Planen ska testas och granskas regelbundet, och personalen ska veta exakt vad som förväntas av dem vid en incident.



Trots detta saknar nästan var fjärde verksamhet en sådan plan. Det innebär att många står utan ett strukturerat förhållningssätt vid säkerhetsincidenter just när förmågan att agera snabbt och samordnat är som mest avgörande.

I takt med att attackerna blivit mer koordinerade och komplexa har också kraven på incidentrespons ökat. Angripare använder sig av taktiker som överbelastning, desinformation och samtidig påverkan av flera system. Utan en fungerande plan ökar risken för felbeslut, på grund av informationsbrist vilket leder till längre återställningstider.

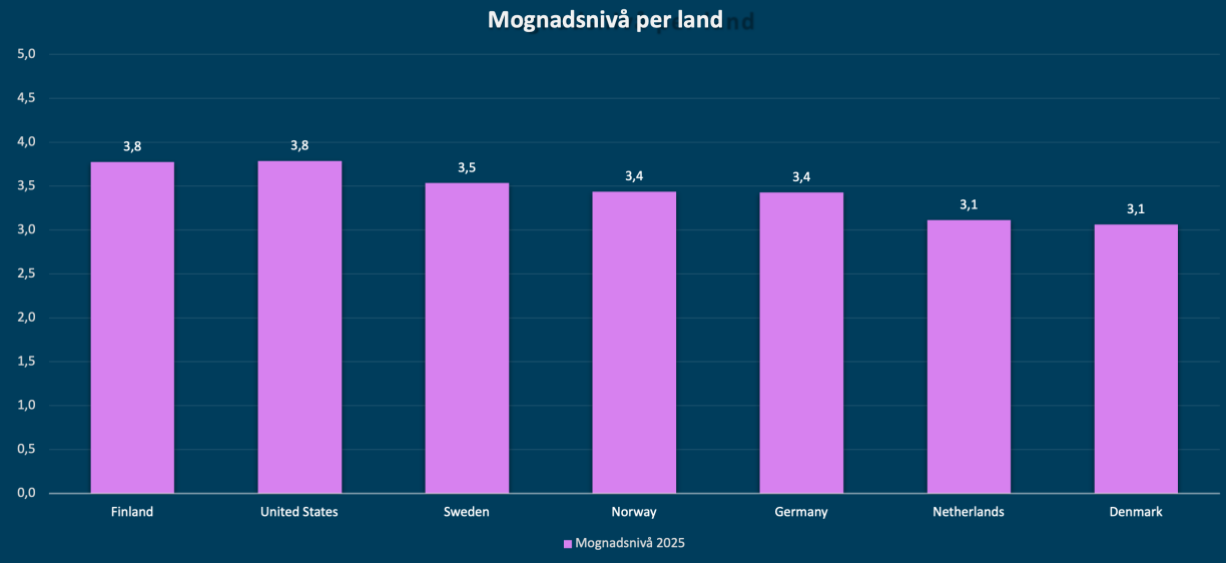
Flera incidenter, både inom offentlig sektor och privat näringsliv, har visat att frånvaron av incidenthanteringsförmåga ofta leder till förvärrade konsekvenser, även när det tekniska skyddet varit relativt starkt.

En incidentplan är ett verktyg för att skydda verksamheten när något går fel. I dagens läge är det inte längre en fråga *om*, utan *när*.

Cybersäkerhetsmognad i Norden

Genom en geografisk analys kan vi identifiera signifikanta mognadsskillnader mellan de nordiska länderna. Datamaterialet för övriga länder är begränsat, vilket gör att resultaten bör tolkas med försiktighet och inte kan generaliseras.

1. **Finland**: Finland är ledande när det gäller cybersäkerhetsmognad och uppvisar avancerade säkerhetsrutiner, robusta regelverk och en hög nivå av medvetenhet om cybersäkerhet. Verksamheter utnyttjar aktivt sofistikerade säkerhetslösningar, har kontinuerlig övervakning och gör omfattande riskbedömningar, vilket sätter en exemplarisk standard för cybersäkerhetsberedskap.
2. **Sverige**: Återspeglar genomsnittlig mognadsnivå, vilket indikerar solida men varierade cybersäkerhetsmetoder. Svenska verksamheter följer i allmänhet grundläggande cybersäkerhetsregler, men bör öka takten när det gäller införandet av omfattande säkerhetsbedömningar och proaktiva funktioner för upptäckt av hot.
3. **Danmark**: Uppvisar för närvarande den lägsta cybersäkerhetsmognaden i denna jämförande analys. Danska verksamheter bör prioritera att stärka cybersäkerhetsåtgärderna, förbättra regelefterlevnaden och avsevärt öka medvetenheten för att minska sårbarheter och förbättra den övergripande cybersäkerhetsmognaden.



Referenser

American Association for Public Opinion Research (AAPOR). (2013). *Report of the AAPOR Task Force on Non-Probability Sampling.*

CrowdStrike. (2024). *Global Threat Report 2024*. https://www.crowdstrike.com

ENISA. (2021). *Threat Landscape for Supply Chain Attacks*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ENISA. (2024). Awareness and Cyber Hygiene
https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box

ENISA. (2025) *Awareness and Cyber Hygiene*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene

ENISA. (2023). *Threat Landscape 2023 – The Year in Review*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA. (2023b). *Cybersecurity Requirements in Public Procurement*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-requirements-in-public-procurement

ENISA. (2020). *Procurement Guidelines for Cybersecurity in Hospitals*
https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

Europeiska kommissionen. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 december 2022 on measures for a high common level of cybersecurity across the Union (NIS2). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

Europeiska kommissionen. (2024). *State of NIS2 Implementation Report – Q1*. Publications Office of the European Union. https://digital-strategy.ec.europa.eu

Hadlington, L. (2021). Cybercognition and the Human Factor: Understanding the psychology of cybercrime, security and risk online. Routledge.

MSB & NCSC Sverige. (2024). Lägesbild cybersäkerhet – Kritisk infrastruktur och nationella hotaktörer. https://www.ncsc.se

NCSC Sverige. (2023). *Lägesbild: Cyberhot mot försörjningskedjan*. Nationellt cybersäkerhetscenter. https://www.ncsc.se

OneMore Secure