
CyberSecure

REGELVERK OCH EFTERLEVNAD - 12 NOVEMBER

CYBER WAKE-UP CALL

Var med och skapa ett CyberSäkert lokalt näringsliv.

Nätverket CyberSecure - Mission och Vision

Mission -

Att skapa trygghet i den digitala världen genom att skapa ett forum och mötesplats som erbjuder expertkunskap, lösningar och metoder som skyddar företag mot cyberhot.

Vision - Att göra regionen till en CyberSäker bastion där företag drivs med hög motståndskraft och beredskap och där cybersäkerhet är en naturlig och integrerad del av verksamhetskulturen.

CyberSecure

Nätverket CyberSecure - Uppgift och roll

Utbilda

Vi stärker företag med kunskap, medvetenhet och metodik gällande cybersäkerhet.

Samverka

Vi bygger en kollektiv säkerhetskultur genom aktiva samarbeten.

Rådgöra

Vi erbjuder expertstöd, kompetens och råd i cybersäkerhetsfrågor och regelverk.

Motverka

Vi arbetar proaktivt för att förhindra och bekämpa cyberhot.

CyberSecure

Cyber WakeUp - Regelverk och efterlevnad

Strategisk prioritet

Cybersäkerhet påverkar företagets rykte, ekonomi och kundförtroende.

Ledningsansvar

Cybersäkerheten - en strategisk ledningsfråga och inte en taktisk IT fråga.

Helhetsgrepp

Effektiv cybersäkerhet kräver bredare riskbedömning och policyhantering och inte enbart taktiska teknikåtgärder.

Konkurrensfördel

Ett starkt fokus ger företaget en konkurrensfördel och ökar förtroendet.

Begränsad synvinkel

Cybersäkerhet, som en taktisk IT-fråga, begränsar ett bredare strategisk perspektiv på risk.

Ledarskap gör skillnad

Ett tydligt ledningsfokus stärker organisationens beredskap och motståndskraft.

CyberSecure

Talare - Regelverk och Efterlevnad 12 November 2024

Tova Elmhav

Jurist - IT-rätt och InfoSäk

Cybersäkerhet och lagstiftning.

Elmhav Sweden

Oliver Zellweger

Head of Privacy Advisors

Cybersäkerhetens affärsvärde.

Secify

Anders Thornborg

Landshövding - Halland

Framtidens säkerhetsutmaningar.

Länsstyrelsen Hallands Län

CyberSecure

Framtidens säkerhetsutmaningar

Anders Thornberg | **Landshövding**
anders.thornberg@lansstyrelsen.se
www.lansstyrelsen.se

CyberSecure

Lagar och regler inom Cyber

Varför lagstiftar vi inom cybersäkerhet.

Tova Elmhav | **Jurist - IT-rätt och InfoSäk**
tova@elmhav.se
www.elmhav.se

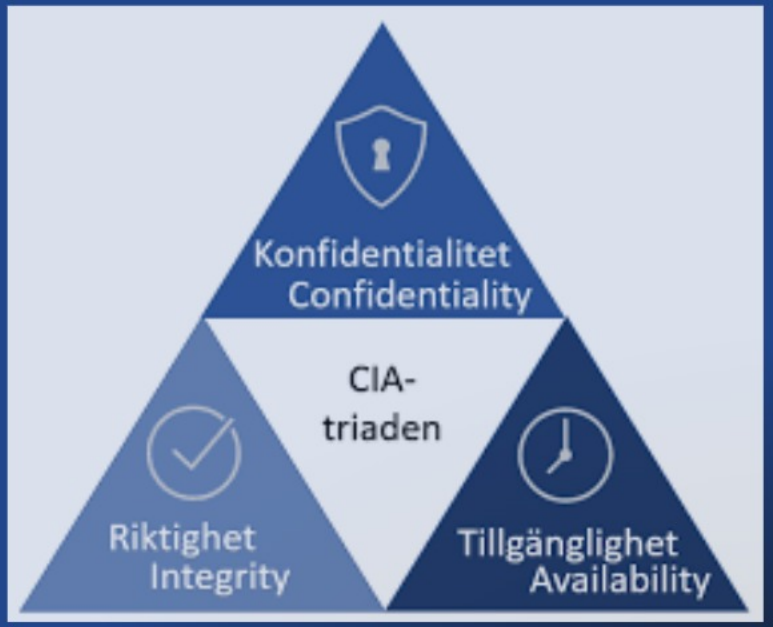
CyberSecure

Vad är Cybersäkerhet?

Cybersäkerhet handlar om att skydda datasystem, nätverk och programvara från digitala attacker, obehörig åtkomst och skador. Målet är att säkerställa att känslig information, som personuppgifter, företagshemligheter och finansiella data, förblir säker och inte hamnar i fel händer.

Det innefattar flera områden:

- Nätverkssäkerhet
- Informationssäkerhet
- Operativ säkerhet
- Katastrofåterställning och kontinuitetsplanering
- Slutanvändarsäkerhet



Säker från vad?

ELMHAV SWEDEN

Coopbutiker landet över hålls stängda till följd av en omfattande it-attack som slagit mot deras kassasystem – och det är oklart när de kan öppna igen.
Tusentals företag kan ha drabbat[illegible]d som tycks vara ett ovanligt stort fall av[illegible]

Tillverkningsindustrin är inte beredd på cyberhot

En ny rapport visar att de flesta företagen inom tillverkningsindustrin sällan eller aldrig övar på att återställa IT-systemen efter ett cyberintrång. Inte heller är de väl förberedda på att information kan stjälas och raderas.

Ökat cyberhot första kvartalet: ”Allt viktigare med robusta säkerhetssystem”

I Check Point Researchs senaste rapport framkommer det att antalet cyberattacker fortsätter öka jorden runt.

Under 2024 har antalet cyber[illegible] föregående år. [illegible]rocent globalt. Detta jämfört med

2023: Cyberangreppen ökade kraftigt

MSB:s senaste årsredovisning visar att under 2023 ökade antalet försök till cyb[illegible] mot statliga myndigheter och leverantörer av samhällsviktiga tjä[illegible]

[illegible]ört med sam[illegible] säger Mats E[illegible]

Nya uppgifter: Pojke köpte it-attack på nätet för 340 kronor

UPPDATERAD 21 DECEMBER 2023 PUBLICERAD 4 NOVEMBER 2021

Tidigare i år utsattes Region Gotland för kraftiga it-attacker. Bakom attackerna låg en 12-årig pojke som för 40 dollar (340 kr) ska ha köpt en överbelastningstjänst på nätet.

It-attacken mot Tietoevry

Hackergruppen Akira har genomfört en omfattande cyberattack mot den finska IT-leverantören Tietoevry [illegible]januari 2024.

[illegible] 120 myndigheter ha[illegible] kommuner ha[illegible] även [illegible]

2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet

Cyberattackerna allt fler – svenska vården extra utsatt

Crowdstrike-uppdatering har lett till avbrott världen över

ELMHAV SWEDEN

- **60 %** av småföretagen som drabbas av cyberattacker tvingas stänga ner inom sex månader på grund av de höga kostnaderna och förlorat förtroende
- En studie från CISCO visar att 40% av de små och medelstora företag som utsattes för en cyberattack drabbades av minst åtta timmars driftstopp. Nedtid står för en stor del av de totala ekonomiska skadorna av en säkerhetsöverträdelse.
- **Genomsnittlig kostnad för cyberintrång i Sverige:** 14,6 miljoner kronor per incident under 2023, vilket inkluderar både direkta kostnader för lösensummor och återställning samt indirekta kostnader såsom förlorat förtroende
- **Globala kostnader:** Den globala genomsnittskostnaden för ett dataintrång är cirka 4,88 miljoner USD (cirka 55 miljoner SEK), beroende på bransch och företagets storlek
- Medan 43% av cyberattacker riktas mot småföretag anses endast 14% vara förberedda, medvetna och kapabla att försvara sina nätverk och data.
- 83% av små och medelstora företag är inte beredda att återhämta sig från de ekonomiska skadorna av en cyberattack.
- 91% av småföretagen har inte köpt någon cyberansvarsförsäkring, trots att de är medvetna om risken och sannolikheten för att de inte skulle kunna återhämta sig från en attack.

ELMHAV SWEDEN

Varför lagstiftar EU inom digitalisering?

- Skydda individens rättigheter och integritet
- Främja innovation och konkurrenskraft
- Skapa rättvisa spelregler
- Skydda konsumenter och öka tilliten
- Främja cybersäkerhet
- Stödja digital inkludering

ELMHAV SWEDEN

Table 1: Overview of EU Legislations in the Digital Sector

Applicable law	Published in the Official Journal of the European Union.
In negotation	Proposal by the European Commission entered the legislative process.
Planed initiative	Mentioned by the European Commission as potential legislative initiative.

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	ePrivacy Directive, (EC)2002/58, 2017/0003(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881, 2023/0108(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	EC Merger regulation, (EC) 2004/139	Satellite and Cable Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	European Statistics, (EC) 2009/223, 2023/0237(COD)	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	Price Indication Directive, (EC) 1998/6	Technology Transfer Block Exemption, (EU) 2014/316	Information Society Directive, (EC) 2001/29	Administrative cooperation in the field of taxation, (EU) 2011/16
Regulation on a pilot regime for distributed ledger technology, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Open Internet Access Regulation, (EU) 2015/2120	General Data Protection Regulation (GDPR), (EU) 2016/679	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa, (EU) 2019/817	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173, 2024/0016(CNS)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Directive on the protection of trade secrets, (EU) 2016/943	Cybersecurity Regulation, (EU) 2023/2841	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Portability Regulation, (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	.eu top-level domain Regulation, (EU) 2019/517	Regulation on the free flow of non-personal data, (EU) 2018/1807	Design Directive, 2022/0392(COD)	Information Security Regulation, 2022/0084(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	eIDAS Regulation (European Digital Identity Framework), (EU) 2014/910	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Satellite and Cable II Directive, (EU) 2019/789	Crypto-assets Regulation (MiCA), (EU) 2023/1114
	Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	Open Data Directive (PSI), (EU) 2019/1024	Compulsory licensing of patents, 2023/0129(COD)	Cyber Resilience Act, 2022/0272(COD)	E-evidence Regulation, (EU) 2023/1543	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), (EU) 2023/1781	Union Secure Connectivity Programme, (EU) 2023/588	Data Governance Act (DGA Regulation), (EU) 2022/868	Standard essential patents, 2023/0133(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)	Digitalisation of cross-border judicial cooperation, (EU) 2023/2844	General Product Safety Regulation, (EU) 2023/988	Regulation on cooperation for the enforcement of consumer protection laws, (EU) 2017/2394	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	European Media Freedom Act, (EU) 2024/1083,	Payment Services Regulation, 2023/0210(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP), (EU) 2024/795	Gigabit Infrastructure Act, (EU) 2024/1309	European Data Act (Regulation), (EU) 2023/2854			Directive on combating violence against women, 2022/0066(COD)	Machinery Regulation, (EU) 2023/1230	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Remuneration of musicians from third countries for recoredd music played in the EU	Digital euro, 2023/0212 (COD)
	European critical raw materials act (Regulation), (EU) 2024/1252	New radio spectrum policy programme (RSPP 2.0)	Interoperable Europe Act, (EU) 2024/903			Directive for combating sexual abuse and child sexual abuse material, 2024/0035(COD)	AI Act (Regulation), 2021/0106(COD)	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560		Regulation on combating late payment, 2023/0323(COD)
	Net Zero Industry Act, 2023/0081(COD)	Digital Networks Act	Regulation on data collection for short-term rental, (EU) 2024/1028			Digitalization of travel documents	Eco-design Regulation, 2022/0095(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067		
	EU Space Law		European Health Data Space (Regulation), 2022/0140(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
			Harmonisation of GDPR enforcement procedures, 2023/0202(COD)					Political Advertising Regulation, (EU) 2024/900	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Access to vehicle data, functions and resources					Right to repair Directive, 2023/0083(COD)			
			GreenData4all					Consumer protection: strengthened enforcement cooperation			

NIS2 eller Cybersäkerhetslagen?

NIS 2

Ett direktiv från EU med syfte att uppnå en hög gemensam nivå av cybersäkerhet inom unionen.

Direktivet gäller leverantörer av samhällsviktiga tjänster inom områden som energi, transport, hälsovård, och digital infrastruktur, samt vissa digitala tjänsteleverantörer.

Cybersäkerhetslagen

Syftar till att införliva och genomföra kraven från NIS2 i svensk rätt.

Ett bredare fokus än bara NIS2 eftersom den även tar hänsyn till nationella säkerhetsbehov och andra specifika krav på verksamhetsutövare, inklusive incidentrapportering och sanktioner.

NIS2 fungerar som en övergripande europeisk ram, medan cybersäkerhetslagen ger det rättsliga stödet på nationell nivå.

ELMHAV SWEDEN

Cybersäkerhetslagen – omfattande verksamheter

Arbetar din verksamhet inom någon av följande sektorer?

- Transport
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Energi
- Hälso- och sjukvård
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer
- Forskning

Uppfyller verksamheten något av följande storlekskrav?

- ✓ **Minst 50 anställda eller**
- ✓ **En årsomsättning som överstiger 10 miljoner euro.**

Eller är ni leverantörer till någon i följande sektorer?

ELMHAV SWEDEN

Cybersäkerhetslagen

Skyldigheter enligt cybersäkerhetslagen:

- **Registreringsskyldighet**
- **Riskhantering**
- **Systematiskt informationssäkerhetsarbete**
- **Utbildning och kompetensutveckling för ledning och anställda**
- **Incidentrapportering**
- **Krav på leverantörskedjan**

Konsekvenser vid brister i efterlevnad

- ✓ **Sanktionsavgifter**
- ✓ **Åtgärder mot VD och ledning**
- ✓ **Uteslutning från upphandlingar**

ELMHAV SWEDEN

Möjligheter med regler och efterlevnad.

Att arbeta aktivt med kraven i cybersäkerhetslagen/NIS2-direktivet kan ge företag flera betydande möjligheter, trots de initiala utmaningarna, såsom:

- Förbättrad cybersäkerhet och riskhantering
- Ökad kundförtroende och marknadsposition
- Reglering och efterlevnad som konkurrensfördel
- Förberedelse för framtida regleringar
- Effektivare incidenthantering och resiliens
- Förbättrad samverkan och samordning
- Möjlighet till innovation och förbättrade processer
- Tillgång till nya marknader och kundsegment
- Förbättrad organisatorisk kultur kring säkerhet

Att arbeta med NIS2 är alltså inte bara en fråga om att undvika sanktioner och efterleva lagkrav, utan också en strategisk möjlighet att stärka företagets säkerhet, effektivitet och marknadsposition.

ELMHAV SWEDEN

Coopbutiker landet över hålls stängda till följd av en omfattande it-attack som slagit mot deras kassasystem – och det är oklart när de kan öppna igen.
Tusentals företag kan ha drabbats i vad som tycks vara ett ovanligt stort fall av utpressni

It-attacken mot Tietoevry

Hackergruppen Akira har genomfört en omfattande cyberattack mot den finska IT-l
januari 2024.
en Tietoevry

Tillverkningsindust
cyberhot

En ny rapport visar att de flesta före
aldrig övar på att återställa IT-syste
förberedda på att information kan

Det är inte p.g.a. lagstiftningen som vi jobbar med cybersäkerhet.

2023: Cyber

MSB:s senaste årsredo
mot sta

Nya uppgifter: Pojke köpte it-attack på nätet för 340 kronor

UPPDATERAD 21 DECEMBER 2023 PUBLICERAD 4 NOVEMBER 2021

Tidigare i år utsattes Region Gotland för kraftiga it-attacker. Bakom attackerna låg en 12-årig pojke som för 40 dollar (340 kr) ska ha köpt en överbelastningstjänst på nätet.

Cyberattacker
svenska vården extra

Crowdstrike-uppdatering har lett till avbrott världen över

ELMHAV SWEDEN

NIS2 som affärsstrategi

Affärsvärde och vägen till systematiskt informationssäkerhetsarbete.

Oliver Zellweger | **Head of Privacy Advisors**
oliver.zellweger@secify.com
www.secify.com

CyberSecure

Bakgrund NIS2

Ett direktiv för att framtidssäkra samhällsviktiga och digitala tjänster

- NIS2-direktivet (The directive on security of Network and Information Systems)
- Direktivets syfte är att stärka och harmonisera medlemsländernas krav vad gäller cybersäkerheten inom EU.
    - Identifiering
    - Rapportering
    - Säkerhetsåtgärder
    - Tillsyn
- För införande i Sverige krävs en kompletterande nationell lagstiftning, den s.k. Cybersäkerhetslagen.
- Regeringens ambition är att en proposition ska lämnas över till Riksdagen under våren 2025, därav en förväntad försening av ikraftträdande (kanske 1 oktober 2025 men möjligtvis senare)

Secify

Bakgrund NIS2

Direktivets upplägg – en kort genomgång

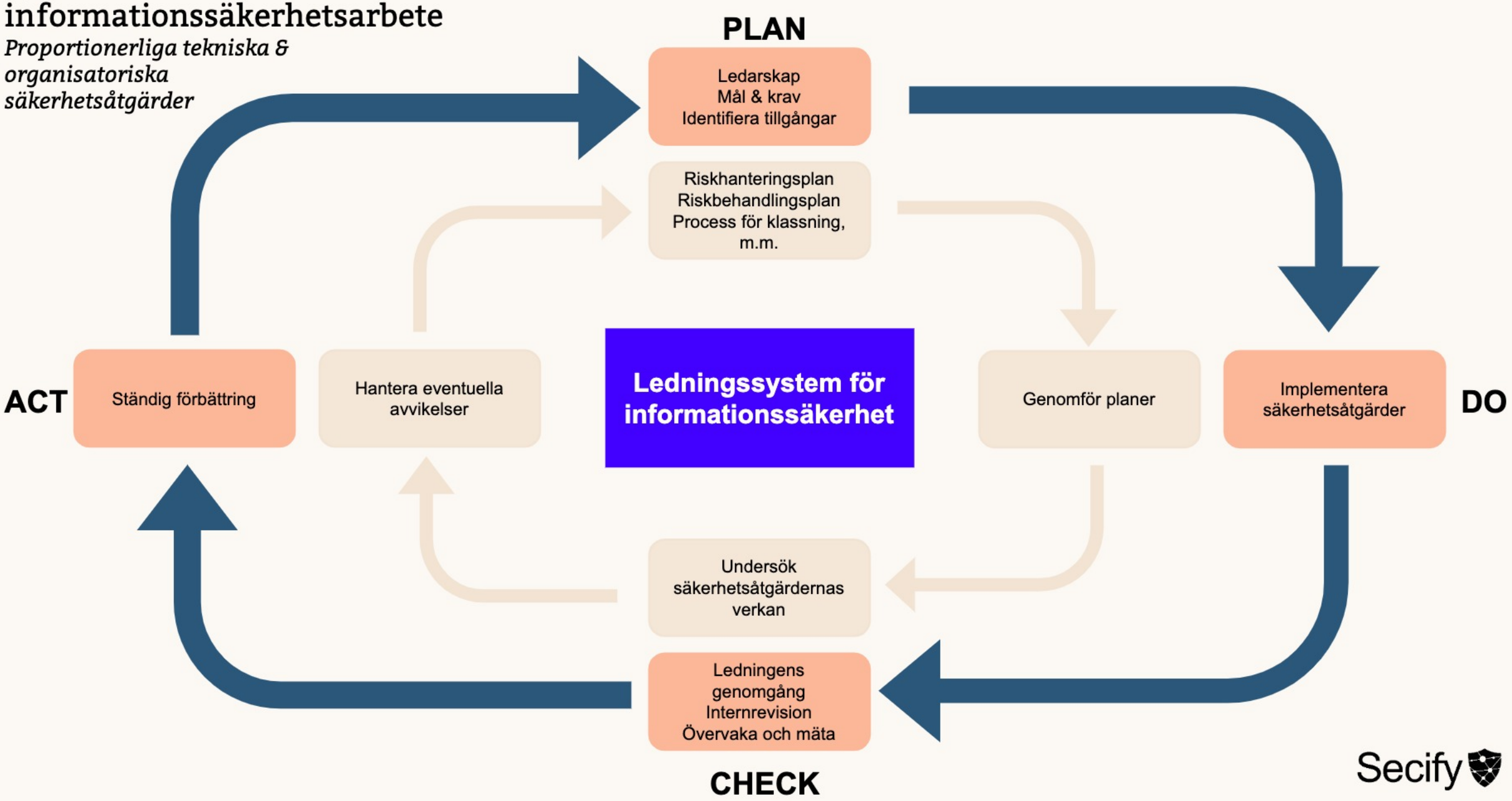
- **Kap 1. Allmänna bestämmelser:** syfte, tillämpningsområde, lex specialis, minimiharmonisering och definitioner.
- **Kap 2. Samordnande ramverk för cybersäkerhet:** hur direktivet ska samordnas på nationell nivå.
- **Kap 3. Samarbete på unionsnivå och på internationell nivå:** hur direktivet ska samordnas på internationell nivå.
- **Kap 4. Åtgärder för riskhantering och rapporteringskrav för cybersäkerhet:** styrning, riskhanteringsåtgärder, leveranskedjor, rapportering, cybersäkerhetscertifiering.
- **Kap 5. Juristiktion och registrering:** register över de som omfattas, juristiktion om aktörer har verksamheter i flera länder.
- **Kap 6. Informationsutbyte:** fokus på samverkan, informationsutbyte för entiteter om cybersäkerhet, frivillig underrättelse till CSIRT.
- **Kap 7. Tillsyn och efterlevnadskontroll:** tillsyn och kontroll för väsentliga respektive viktiga entiteter, sanktionsavgifter, personuppgiftsincidenter etc.
- **Kap 8. Delegerade akter och genomförandeakter:** ev. ytterligare reglering från kommissionen dvs ytterligare konkretisera ex. vilka säkerhetsåtgärder som ska göras.
- **Kap 9. Slutbestämmelser:** översyn, införlivande och ikraftträdande.

Vad behöver ni som verksamhet göra?

Secify

Systematiskt ock riskbaserat informationssäkerhetsarbete

Proportionerliga tekniska & organisatoriska säkerhetsåtgärder



Secify

Vad behöver er verksamhet göra?

Gäller för samtliga organisationer

Hantering av risker i leverantörskedjan

- Leverantörsbedömning, avtal, uppföljning av befintliga leverantörer och säkerställande av effektiv incidenthantering.

Utbildning och medvetenhet

- Utbildningsprogram för ledning och anställda som är anpassade efter deras roll och ansvarsområden.
- Utbildningar inom phishing, cybersäkerhet, social engineering, dataskydd (GDPR) och hur man rapporterar incidenter.
- För ledning och IT-personal bör mer avancerade utbildningar tillhandahållas ex. riskhantering, incidenthantering och analys av hotbildsinformation.
- Simulera attacker och övningar där ledning och anställdas beredskap testas, med åtgärder som följd.

Ledningens ansvar och fokus

- Engagemang och styrning, med ledningen tydligt ägandeskap för säkerhetsstrategin. Ex. målsättning, roller och ansvar, fördelning av resurser. Regelbunden rapportering för att säkerställa insyn och ansvarstagande.
- Tydlig resurstilldelning och budget: investering i teknik, utbildning och personal, ta in extern personal vid behov.
- Framtagande av tydliga policyer och ramverk och att dessa är kommunicerade till de anställda.
- Kontinuerlig förbättring och anpassning av befintliga processer i säkerhetsarbetet ex. riskhantering, incidenthantering etc. Det inkluderar även omvärldsbevakning.

Vad behöver er verksamhet göra?

Små bolag

Grundläggande säkerhetsrutiner
- Patchning av mjukvara och drivrutiner.
- VPN och kryptering.
- Behörighetsstyrning i form av rutiner.

Utbildning och medvetenhet
- Ledning och anställda
- Säkerhetskultur, phising, incidenthantering, personuppgifter etc.

Incidentrapportering
- Policys, rutiner och checklistor för incidentrapportering.

Medelstora bolag

Riskbaserat säkerhetsarbete
- Arbeta i enlighet med en säkerhetsstandard, ex. ISO27001, utan att för den delen certifieras.
- Genomföra riskanalyser för att identifiera risker och prioritera säkerhetsåtgärder baserat på aktuella hotbilder.

GRC-plattform, identifiering av hot och sårbarheter
- Tillämpning av GRC-plattform som omsätter strategi i praktisk handling, som säkerställer löpande efterlevnad av lagar och regler. Sårbarhetsskanningsverktyg som identifierar och klassificerar sårbarheter i datorer, nätverk och applikationer.

Incidenthantering och kontinuitesberedskap
- Intern process för incidenthantering och kontinuitetsövningar som hjälper personal att veta hur de ska agera vid en störning i verksamheten.

Secify

Vad behöver er verksamhet göra?

Stora bolag

Heltäckande säkerhetsorganisation
- Fokus på såväl tekniska, organisatoriska och legala säkerhetsåtgärder.
- Tekniska åtgärder: nätverkssegmentering, sårbarhetsskanning, SOC-lösning och regelbunden penetrationstestning.

Internationella standarder och certifieringar
- Införande och arbete enligt internationella standarder som ISO27001 och NIST Cybersecurity Framework.
- Regelbundna intern och externrevisioner för att säkerställa måluppfyllelse med säkerhetsarbetet.

Ständiga förbättringar
- En centraliserad säkerhetsfunktion som kontinuerligt arbetar för att förbättra och anpassa säkerhetsarbetet.

Leverantör till NIS2-aktör

Hur påverkas du?

Secify

Du som leverantör

NIS2 lägger stor vikt vid säkerheten i hela leveranskedjan. Leverantörer som är en del av kritiska system och tjänster kommer indirekt att omfattas av högre säkerhetskrav för att garantera att man inte utgör en svag länk.

Som underleverantör till en NIS2-aktör kan du räkna med:

- Högre säkerhetskrav
- Krav på riskhantering
- Rapportering av incidenter
- Ökad transparens och dokumentation
- Avtal och kontraktskrav – mer omfattande dokumentation
- Sanktioner och ansvarsskyldighet
- Utbildning och säkerhetsmedvetenhet
- Certifieringar och standarder

Exempel - leverantörsgranskning

Policy för inköp

Styrande dokument som ska ange vilka regler och förhållningssätt som ska gälla vid anskaffning av nya system eller tjänster.

Checklista för anskaffning av nya system & tjänster

- Klassificering av information och det system eller tjänst som är tänkt att användas
- Inhämtande av information från leverantör kring dennes säkerhet t.ex. white-paper, säkerhetsbilagor etc.
- Utvärdering hantering av personuppgifter
- Säkerställande av avtal som behövs t.ex. PuB-avtal, SLA-avtal, NDA-avtal etc.

Uppföljning

- Extern granskning av leverantör
- Uppföljning av säkerhetsrutiner
- Uppföljning av eventuella incidenter

Secify

Exempel - Incidenthantering

1. Notifiera MSB
(inom 6h)

Notifiera via verktyget IR-ON (msb.se) alternativt underrätta CERT-SE vid MSB om incidenten via telefon på tel.
010-240 40 40

2. Rapportera
(inom 24h)

Rapportering vara verktyget IR-ON (msb.se) tillhanda inom 24 timmar.

3. Skicka slutrapport till MSB (inom 4 veckor)

Inom fyra veckor ska en slutrapport om händelsen skickas in till MSB, verktyget IR-ON (msb.se).

Secify


Frågor & diskussion
Secify

Frågor och svar (FAQ)

Vad är NIS2?
NIS2-direktivet syftar till att uppnå en hög gemensam cybersäkerhetsnivå i hela unionen och ställer tydligare krav på bl.a. riskanalyser, olika säkerhetsåtgärder, ledningens deltagande i säkerhetsarbetet. Det är ett minimidirektiv dvs att det är det man minst ska leva upp till i omfattning och krav.

Vad är CER-direktivet?
CER-direktivet (Directive on the resilience of critical entities) ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet.

När ska NIS2 vara implementerat på nationell nivå?
Börjar tillämpas den 18 oktober 2024 och träder i kraft i svensk lag under 2025.

Kommer vi att omfattas av NIS2?
Huvudregeln är att om har verksamhet inom de 18 nämnda sektorerna i direktivet, har 50 anställda och en omsättning på 10 miljoner så omfattas man.

Det kan vara utmaning att definiera sig själv, ex. offentlig förvaltning. I direktivet nämner man offentliga förvaltningsmyndigheter på nationell och regional nivå men även kommuner inkluderas.

Om kommuner anses som samhällsviktig verksamhet, ska det i så fall omfatta hela kommunen?
Ja, med NIS2-direktivet så tar man ett helhetsgrepp.

Omfattas tillverkare av medicintekniska produkter?
Ja, i tillhörande bilaga till NIS2-direkivet, under sektorn ”5. Hälso- och sjukvård” och vårdgivare, artikel 3 (g) står det att ”varje fysisk eller juridisk

Frågor och svar (FAQ)

Vi är ett bageri, omfattas vi av NIS2?
Det är möjligt. Även här behöver man tolka definitionerna i direktivet t.ex. ”4. Produktion, bearbetning och distribution av livsmedel”, därefter titta närmare på definitionen för ”2. Livsmedelsföretag”. Ex. storleken kan avgöra.

Vem är NIS2-leverantör mellan ett moder- och dotterbolag?
Utgångspunkten är att ansvaret utgår från moderbolaget men sen kan det vara dotterbolagen som ansvarar för att identifierade säkerhetsåtgärder implementeras. Enligt direktivet som omfattas hela organisationen och det är ledningen som ansvarar för att tillsätta

Vi är en IT-leverantör som levererar IT till en NIS2-aktör, vad behöver vi i så fall tänka på?
Just för IT framgår det i tillhörande bilagor i NIS2-direktivet, att dessa har en särskild roll och ansvar.

I direktivet har man delat upp IT inom områdena molntjänstleverantör, datacenterleverantörer etc.
Dessa har en särskild roll utifrån att man har många kunder som påverkar många.
Inom ramen för genomförandeakter från kommissionen kommer det att komma ytterligare krav för vad som gäller för dessa IT-leverantörer.

Frågor och svar (FAQ)

Vad menar man med ledningen i NIS2-direktivet?
I regel är det bolagets styrelse som utgörs av ledningen. För kommuner är det kommunstyrelsen.

Vad har ledningen för ansvar enligt NIS2-direktivet?
Ledningen har flertalet ansvarsområden i den dagliga verksamheten. Utöver det är det viktigt att veta att det i NIS2 finns ett personligt ansvar inskrivet.

Hur kan man förbereda sig som organisation?
Analysera hur ni arbetar med cybersäkerhet genom en GAP-analys eller (små bolag) MSB:s verktyg ”Cybersäkerhetskollen”.

Om man inte omfattas av NIS2-direktivet, finns det värde av att ändå arbeta i enlighet med det?
Kraven från NIS2-direktivet är inte några orimliga krav att efterleva utan, en grundläggande nivå för en organisationens cybersäkerhetsarbete.

Att arbeta i enlighet med NIS2 bidrar med förtroende, såväl internt som mot externa intressenter (ex. kunder).
Dessutom får organisationen bättre förmåga att bedriva verksamhet i samband med verksamhetsstörningar, ledning och anställda får bättre koll på den information som hanteras och hur incidenthantering ska göras.

Nästa steg - Kostnadsfri Workshop

Innehåll

1. **Affärsvärdet av cybersäkerhet**
    - Kostnader och risker med cyberattacker för företag.
    - Diskussion: Vad innebär cybersäkerhet för vår affär?
- **Ledarskapets roll i cybersäkerhet**
    - Ledningens ansvar enligt NIS2 och Cybersäkerhetslagen.
    - Diskussion: Hur bidrar vi som ledning till säkerhetskultur?
- **Regelverk och efterlevnad**
    - Översikt av NIS2 och Cybersäkerhetslagen.
    - Steg för att säkerställa efterlevnad och skapa en compliance-strategi.
- **Riskhantering och incidentberedskap**
    - Grunder i riskbaserat säkerhetsarbete.
    - Övning: Incidenthantering vid cyberattack.
- **Handlingsplan för cybersäkerhet**
    - Skapa en handlingsplan och prioritera resurser för ökad motståndskraft.

Syfte

Ge ledningsgruppen insikter i cybersäkerhetens affärsvärde, relevanta regelverk, och praktiska verktyg för att stärka motståndskraften mot cyberhot.

När du behöver hjälp

www.cybersecure.nu

CyberSecure Halmstad

host@cybersecure.nu