Vad säger NIS2 om strategier för riskanalys och informationssystemens säkerhet?

Vad säger regleringen?

NIS2-direktivet betonar att organisationer ska implementera utvecklade strategier för riskanalys och säkerhet för informationssystem för att identifiera, hantera och minska risken för cyberintrång (se artikel 21.2 a). Regleringen syftar till att säkerställa att potentiella hot mot nätverks- och informationssystem upptäcks i tid och att relevanta säkerhetsåtgärder vidtas.

Vad menas med strategier för riskanalys?

Direktivet ställer krav på att organisationer genomför riskanalyser, för att proaktivt kunna identifiera, och bedöma risker som kan påverka verksamheten. Detta syftar särskilt till områden som cybersäkerhet, och menar att berörda entiteter bör vidta åtgärder för att hantera eller minska dessa risker. Organisationer ska alltså kunna bedöma sannolikheten och konsekvenserna av olika hot, utveckla planer för att hantera dessa risker, samt att kontinuerligt övervaka och uppdatera riskhanteringsåtgärder för att säkerställa en dynamisk säkerhetsstrategi. Riskbedömningen handlar i grund och botten om att besvara de fyra frågorna: 'Vad kan hända?', 'Varför kan det hända?', 'Vad blir konsekvenserna?' och 'Hur sannolikt är det att det inträffar?'.

Vad menas med strategier för informationssystemens säkerhet?

Vidare bör även organisationen forma strategier för informationssystemens säkerhet, vilket syftar till skyddet av system som hanterar, lagrar och bearbetar information. Det handlar om att försäkra att dessa system är skyddade mot hot som kan påverka konfidentialitet, integritet och tillgänglighet av information. Detta inkluderar även åtgärder för att förhindra obehörig åtkomst, dataförlust, manipulation, cyberattacker och andra säkerhetsrisker som kan skada eller störa systemens funktion.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Vad säger NIS2 om incidenthantering?

Vad säger regleringen?

Enligt artikel 21.2 b kräver NIS2-direktivet att organisationer införskaffar starka åtgärder för incidenthantering, inklusive att snabbt identifiera, rapportera och åtgärda cybersäkerhetsincidenter för att minimera deras påverkan på samhällsviktig verksamhet.

Vad menas med incidenthantering?

Organisationer ska ha tydliga och effektiva processer för att hantera och rapportera cybersäkerhetsincidenter. Detta betyder att en entitet bör snabbt kunna upptäcka, bedöma, och åtgärda incidenter som kan påverka nätverks- och informationssystem, samt att rapportera allvarliga incidenter till relevanta myndigheter inom en specifik tidsram. Syftet är att minimera skador på verksamheter och säkerställa en snabb återhämtning för att upprätthålla samhällsviktig funktionalitet och tjänster.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Vad säger NIS2 om driftskontinuitet, säkerhetskopiering och katastrofhantering, samt krishantering?

Vad säger regleringen?

Artikel 21.2 c syftar till att säkerställa att berörda entiteter har en tydlig strategi och genomtänkta åtgärder för driftskontinuitet, säkerhetskopiering, katastrofhantering och krishantering. Detta för att kunna säkerställa att kritiska tjänster snabbt kan återställas vid störningar eller incidenter.

Vad menas med driftkontinuitet?

Enligt NIS2-direktivet avser driftskontinuitet de åtgärder och processer som organisationer måste vidta för att säkerställa att deras kritiska tjänster och system förblir operationella även vid tekniska problem, störningar eller säkerhetsincidenter. I en kontinuitetsplan ska det finnas en tydlig agenda om vilken ordning man ska återställa systemen för att försäkra en snabb och effektiv återställning.

Vad menas med säkerhetskopiering?

NIS2-direktivet kräver att organisationer säkerställer att de har tillräckliga åtgärder för säkerhetskopiering av data och system, för att skydda mot förlust eller förvanskning av kritisk information. Detta innebär att organisationer måste ha en bra process för att regelbundet säkerhetskopiera sina system och sin data, så att de snabbt kan återställa driften i händelse av en incident, såsom en cyberattack eller tekniskt fel. Säkerhetskopiorna ska vara lättåtkomliga och lagras på ett sätt som skyddar dem från att bli manipulerade. Information som anses avgörande för en organisations verksamhet bör säkerhetskopieras en gång per dygn. Det är rekommenderat att följa en 3-2-1 princip gällande säkerhetskopiering (tre kopior av data, fördelade på två olika lagringsmedier, samt en kopia förlagd off-site som kan behövas vid en katastrofåterställning).

Vad menas med katastrofhantering samt krishantering?

Katastrofhantering handlar om att utveckla planer för att återställa och säkerställa drift efter större störningar, såsom tekniska fel eller externa attacker, så att organisationen snabbt kan återgå till normal verksamhet. Krishantering innebär att ha strategier och resurser på plats för att hantera akuta situationer, som cyberattacker eller systemfel, för att minimera skador och försäkra en snabb återhämtning, samtidigt som det sker en kontinuerlig kommunikation och koordinering under hela krisens förlopp. Att utse ansvariga är ett viktigt steg i en krishanteringsplan för att säkerställa en effektiv hantering.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Vad ställer NIS2 för krav om säkerhet i leveranskedjan?

Vad säger regleringen?

NIS2-direktivet betonar att organisationer måste ha koll på säkerheten i sina leveranskedjor. Enligt artikel 21.2 d syftar detta till de säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess leverantörer för att minska risker och sårbarheter som kan påverka deras cybersäkerhet. Organisationen behöver även ställa krav som minskar risken för inlåsningseffekter, det vill säga svårigheter att avsluta en leverantörsrelation utan att riskera oförutsedda kostnader.

Vad menas med säkerhet i leveranskedjan?

NIS2-direktivet betonar vikten av att säkerställa att den egna organisationens cybersäkerhet är skyddad samt även de leverantörer som är en del av leveranskedjan, och att de upprätthåller en tillräcklig nivå av cybersäkerhet. Detta innebär att organisationer måste bedöma och hantera risker från sina leverantörer och samarbetspartner och se till att dessa följer relevanta säkerhetskrav för att minska potentiella sårbarheter som kan utnyttjas av angripare. En leverantör kan därför behöva följa de säkerhetskrav som ställs i artikel 21.2 d i NIS2, mer information om exakta kriterier finnes i cybersäkerhetslagen.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Vad säger NIS2 om säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem?

Vad säger regleringen?

NIS2-direktivet kräver att organisationer vid förvärv, utveckling och underhåll av nätverks- och informationssystem ser till att säkerhetsåtgärder integreras i hela livscykeln för att skydda systemen mot potentiella risker och hot, inbegripet hantering av sårbarheter och sårbarhetsinformation (se artikel 21.2 e).

Vad menas med säkerhet vid förvärv av nätverks- och informationssystem?

Säkerhetskrav och åtgärder beaktas redan vid anskaffning eller förvärv av nya nätverks- och informationssystem eller tjänster. Det innebär att när organisationer köper eller ingår avtal om nya system eller tjänster, ska de se till att dessa uppfyller nödvändiga säkerhetsstandarder och inte medför nya sårbarheter eller risker för cybersäkerheten.

Vad menas med säkerhet vid utveckling av nätverks- och informationssystem?

Säkerheten vid utveckling av nätverks- och informationssystem ska integreras från början och genom hela utvecklingsprocessen. Det innebär att organisationer måste vidta lämpliga säkerhetsåtgärder redan i designfasen och under hela utvecklingen för att säkerställa att systemen är skyddade mot säkerhetshot och sårbarheter. Detta inkluderar säker kodning, att testa systemen för sårbarheter och använda säkerhetsprotokoll och verktyg som skyddar information och systemens integritet, konfidentialitet och tillgänglighet.

Vad menas med säkerhet vid underhåll av nätverks- och informationssystem?

Detta innebär att kontinuerligt vidta åtgärder för att identifiera och åtgärda säkerhetsbrister, hantera uppdateringar och patchar, samt säkerställa att systemen förblir skyddade mot nya och föränderliga hot. Det handlar om att bibehålla och förbättra säkerheten genom hela systemens livscykel, inklusive regelbundet underhåll för att minimera riskerna för attacker och driftstopp.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Hur bedömer vi effektiviteten i riskhanteringsåtgärderna för cybersäkerhet?

Vad säger regleringen?

Tillväxten i antalet cyberattacker och hot ökar, och i takt med det ser vi förödande konsekvenser. En del i detta arbete är därför att applicera starkare krav på åtgärder för cybersäkerhet. Aktörer som omfattas av NIS2 direktivet ska därmed, enligt förhållningskraven implementera en grundläggande praxis för cyberhygien och utbildning i cybersäkerhet (se artikel 21.2 f). Syftet för denna praxis är att skydda nätverk och informationssystem och systemens fysiska miljö från incidenter, det vill säga minimera de risker som kan härledas till en bristande kunskap och bristande rutiner inom organisationen.

Vad menas med bedömning av effektivitet i riskhanteringsåtgärder?

För att bedöma och förbättra riskhanteringsåtgärder enligt NIS2-direktivet är en kombination av penetrationstester, sårbarhetsskanningar, phishingsimuleringar och regelbundna säkerhetsinventeringar avgörande. Penetrationstester identifierar sårbarheter genom att simulera verkliga cyberattacker, medan sårbarhetsskanningar automatiskt kartlägger kända svagheter och möjliggör prioritering och åtgärder av dessa. Phishingsimuleringar används för att testa de anställdas förmåga att hantera phishingattacker, stärka medvetenheten om potentiella hot och mäta kunskapsnivåer genom kontinuerlig utbildning. Regelbundna säkerhetsinventeringar försäkrar att tekniska och organisatoriska åtgärder bibehålls och uppdateras i enlighet med NIS2-kraven, vilket går i enlighet med artikel 32. 2 (e) om efterlevnadskontroller. Denna artikel menar att myndigheter kan begära ut dokumenterade cybersäkerhetsstrategier för att bedöma de riskhanteringsåtgärder som antagits för den berörda entiteten.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivining?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Vad ställer NIS2 för krav på cyberhygien och utbildning i cybersäkerhet?

Vad säger regleringen?

Antalet cyberattacker och hot ökar stadigt, och med detta ser vi förödande konsekvenser. Som en del av arbetet för ökad cybersäkerhet har starkare krav på åtgärder införts. Aktörer som omfattas av NIS2-direktivet ska, enligt direktivets krav, implementera grundläggande praxis för cyberhygien och utbildning i cybersäkerhet (se artikel 21.2 g). Syftet med denna praxis är att skydda nätverk och informationssystem, inklusive deras fysiska miljö, från incidenter och målet är att minimera risker som uppstår på grund av bristande kunskap eller otillräckliga rutiner bland medarbetare.

Föreskriften innebär att respektive organisation som omfattas av direktivet ansvarar för att säkerställa att såväl anställda (det vill säga personer berörda inom organisationens ledningsorgan), direkta leverantörer och tjänsteleverantörer är medvetna och vidtar åtgärder för att försäkra en säker miljö.

Vad menas med cyberhygien?

Begreppet cyberhygien kan ibland uppfattas som svårtolkat, men det kan förenklas genom mer konkreta förslag. Ni kan upprätta praxis för cyberhygien genom att införa policies inom områden som identitets- och åtkomsthantering, enhetskonfiguration, programuppdateringar samt säkerhetskoncept såsom zero trust. Precis som ordet "hygien" antyder handlar det om att hålla system och rutiner "rena". Detta inkluderar på så vis även policies för clean desk, riktlinjer för säkert distansarbete, att datorer stängs av när de inte används, samt att konsekvent använda multifaktorautentisering. Det omfattar också skydd mot nätfiske, säker hantering av e-post och andra grundläggande säkerhetsrutiner.

Vad menas med utbildning i cybersäkerhet?

Den andra delen syftar till att organisationer ska säkerställa att de anställda tar del av utbildning i cybersäkerhet. Denna åtgärd ska arbetas med över tid, vilket menas med att ett program eller utbildning ska påbörjas där de berörda successivt ökar sin medvetenhet om relevanta cyberhot och riskhanteringsåtgärder. Utbildningen ska innefatta information om hur de anställda ska behandla cyberrisker, vad det finns för potentiella cyberhot och hur de ska agera vid en händelse. Denna utbildning ska ske löpande, och innefatta såväl nyanställda samt annan personal.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Hur kan vi utveckla strategier och förfaranden för användning av kryptografi och kryptering?

Vad säger regleringen?

Att utveckla strategier för förfaranden innebär att organisationer behöver skapa en genomtänkt och långsiktig plan för hur specifika aktiviteter eller processer ska genomföras på ett konsekvent och säkert sätt. Strategierna kommer fungera som en övergripande ram, och förfarandena utgör de mer detaljerade stegen och instruktionerna som ska följas för att uppnå de önskade resultaten. Artikel 21.2 (h) kräver att kryptografiska lösningar används som en del av övergripande säkerhetsåtgärder för att skydda såväl nätverk som informationssystem.

Vad menas med kryptografi och kryptering?

Vi kan börja med att reda ut skillnaderna mellan kryptografering och kryptering, för att sedan förstå helheten och hur det appliceras i regleringen. Kryptografi är tekniken för att skydda information genom olika metoder som kryptering, digitala signaturer och hashning. Kryptering är en del av kryptografi och innebär att data görs oläslig för obehöriga genom att den omvandlas med en nyckel, och endast den som har rätt nyckel kan läsa den krypterade informationen. Kort sagt, kryptografi är det stora området, och kryptering är en specifik metod inom det.

Direktivet efterfrågar strategier och förfaranden för användning av kryptografi och kryptering, vilket sätter krav på organisationer att implementera relevanta verktyg. Organisationer kan använda TLS för kryptering av webbtrafik, men även VPN för att kryptera webbtrafik och diskkryptering, vilket skyddar data på enheter med verktyg som BitLocker.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Vad ställer NIS2 för krav på personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning?

Vad säger regleringen?

I en tid där cyberhoten ökar i både omfattning och komplexitet, ställer EU:s NIS2-direktiv höga krav på organisationers förmåga att skydda sina system och tillgångar. Artikel 21.2 (i) i direktivet lyfter fram tre viktiga punkter: personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning. Dessa är viktiga för att hålla en stark cybersäkerhetsnivå och motverka obehörig åtkomst eller förlust av kritisk information.

Vad menas med personalsäkerhet?

Personalsäkerhet handlar inte bara om att skydda organisationen från externa hot, utan också om att skapa en trygg och säker arbetsmiljö där både anställda och externa parter är medvetna om sitt säkerhetsansvar. Organisationer bör därför kunna säkerställa att alla som har åtkomst till kritiska tillgångar eller information är behöriga och är utbildade inom säkra processer.

Vad menas med åtkomstkontroll?

NIS2 direktivet ställer även krav på åtkomstkontroll, vilket handlar om att kontrollera och begränsa vem som har tillgång till organisationens system, nätverk och information. Genom att skapa riktlinjer för åtkomstkontroll säkerställer man att endast behöriga personer, och/eller system kan komma åt känslig information, samtidigt som obehörig åtkomst förhindras.

Vad menas med tillgångsförvaltning?

Tillgångsförvaltning enligt NIS2 artikel 21.2 (i) innebär att organisationer måste ha en strukturerad process för att identifiera, övervaka och skydda sin information. Organisationer bör därför skapa en detaljerad lista för alla ITC tillgångar, inklusive mjukvaror, servrar, datalagring och brandväggar. Utöver detta bör även en behörig utnämnas som ansvarstagande för respektive tillgång där varje enhet behandlas utifrån sin individuella risknivå.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Vad säger NIS2 om multifaktorautentisering och säkrare kommunikationer?

Vad säger regleringen?

Aktörer som omfattas av NIS2-direktivet ska, enligt direktivets krav, se till så att behöriga inom organisationen applicerar multifaktorautentisering eller kontinuerlig autentisering, säkra kommunikationsvägar (dvs. röst, video och text) - och nödkommunikationsvägar (se artikel 21.2 j). Detta i syfte för att skydda nätverk och informationssystem, inklusive deras fysiska miljö, från incidenter.

Föreskriften innebär att respektive organisation som omfattas av direktivet ansvarar för att försäkra att såväl anställda (det vill säga personer berörda inom organisationens ledningsorgan), direkta leverantörer och tjänsteleverantörer är medvetna och vidtar åtgärder för att säkerställa en säker miljö.

Vad menas med autentiseringsverktyg?

Autentiseringsverktyg används för att verifiera att en användare, en enhet eller en tjänst verkligen är den de utger sig för att vara. Dessa verktyg spelar en avgörande roll i att säkra åtkomst till system och nätverk, vilket förhindrar obehörig åtkomst och skyddar känslig information. Inom ramen för NIS2-direktivet har multifaktorautentisering (MFA) en särskilt viktig roll. Genom att tillföra ett extra säkerhetslager blir det betydligt svårare att utnyttja ett kompromitterat lösenord.

Vad menas med säkrare kommunikationsvägar?

Direktivet ställer även krav på säkra kommunikationsvägar (dvs. röst, video och text) - och nödkommunikationsvägar. Det betyder att organisationer behöver ta till både tekniska lösningar och praktiska rutiner för att skydda informationen som skickas mellan system, användare och tjänster, så att den inte kan avlyssnas, ändras eller hamna i fel händer. Detta kan hanteras genom krypteringsverktyg, skydd mot phishing och spoofing, men även incidentshantering med logging, för att på ett säkert sätt kunna analysera misstänkta incidenter.

Det finns flera verktyg som han hjälpa er komma igång och implementera dessa åtgärder på bästa sätt, och vi på Gridheart erbjuder tjänster för detta. Är ni intresserade av att veta mer och få rådgivning?

Kontakta oss på **info@gridheart.com** så fortsätter vi dialogen!

Är du en kritisk leverantör till en verksamhetsutövare enligt NIS2?

Inför att NIS2 direktivet träder i kraft, är det högst väsentligt för organisationer att ta reda på om de kan vara en kritisk leverantör till en verksamhetsutövare som omfattas. Vi har därför punktat upp de sektorer som anses vara högkritiska, respektive andra kritiska sektorer enligt direktivet. En viktig aspekt att komma ihåg är att NIS2-direktivet inkluderar verksamheter inom de sektorer som även täcktes av det ursprungliga NIS-direktivet, samt de som nu har lagts till. Det ursprungliga NIS-direktivet omfattar verksamheter inom sektorer som energi, digital infrastruktur, transporter, sjukvård, bankverksamhet, finansmarknadsinfrastruktur samt leverans och distribution av dricksvatten, vilket framgår i NIS-direktivets andra bilaga.

Med NIS2-direktivet delas de sektorer som omfattas in i två huvudkategorier: Högkritiska sektorer och andra kritiska sektorer. Nedan ser du en fördelning av samtliga berörda sektorer utifrån dessa kategorier. Mer detaljerad information om kategorierna och deras underkategorier finns i direktivets bilagor 1 och 2.

Högkritiska sektorer

- Energi
- Hälso- och sjukvårdssektorn
- Transport
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- IKT-tjänsteförvaltning
- Rymden
- Offentlig förvaltning

Andra kritiska sektorer

- Digitala leverantörer
- Post- och budtjänster
- Avfallshantering
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Tillverkning, produktion och distribution av kemikalier
- Forskning