NIS 2
krav och lösningar

Gridheart vägleder er gällande NIS2 direktivet

GRIDHEART

Förord

Denna rapport riktar sig till er MSPer i syfte att ge vägledning och insikter om en säker digitalisering och implementering för era kunder som påverkas av NIS2 direktivet. Rapporten redogör för den ökade hotbilden och risken mot vår fortsatta digitala utveckling och konkurrenskraft, vilket såväl ni som era kunder påverkas av.

För att hjälpa er vara förberedda på villkor och lösningar inför detta direktiv bidrar denna rapport med en summerad nulägesrapport, introduktion till NIS2, samt de utmaningar och lösningar som ni som MSPer står inför.

I rapporten presenteras en lättöverskådlig vägledning för att komma i gång med en implementering av NIS2 direktivet, genom konkreta exempel på tjänster som kan hjälpa er att uppnå de uppsatta kraven för NIS2. Dessa bör däremot inte användas som ett ramverk för att uppfylla NIS2 krav, men snarare en guide med rekommendationer på relevanta verktyg.

Bakgrund

NIS2 (Network and Information Systems Directive 2) är en uppdatering av EU:s tidigare NIS-direktiv från 2016, med syftet att stärka cybersäkerheten och skydda kritisk infrastruktur. Direktivet riktar sig till organisationer inom kritiska sektorer samt tjänsteleverantörer och infördes för att möta de växande cyberhoten. Det omfattar fler sektorer och ställer hårdare krav på organisationer. NIS2 anger regler för medlemsländer, företag och myndigheter kring hantering av säkerhetsincidenter, riskhantering och rapporteringsskyldigheter.

I EU:s nya cybersäkerhetsstrategi beslutades det om en revidering av det ursprungliga NIS-direktivet för att åtgärda de brister som identifierats sedan dess införande, samtidigt som direktivet uppdaterades för att bättre hantera dagens och framtidens digitala utmaningar och risker. NIS2 anses vara mer konkret och praktiskt inriktat, samt närmare kopplat till verksamheternas faktiska behov än det ursprungliga NIS-direktivet.

GRIDHEART

Viktiga datum

17 oktober 2024
Den ursprungliga NIS-direktivet (EU) 2016/1148 kommer att upphävas och det slutgiltiga datumet för implementeringen av NIS2 i lag av varje EU-medlemsstat är satt (Europeiska parlamentet, 2022).

18 oktober 2024
Åtgärder som krävs enligt lag enligt NIS2 direktivet träder i kraft.

Efter den 18 oktober 2024
Trots NIS2:s strävan att undvika en ojämn implementering som med NIS, ansvarar varje EU-land för att införa direktivet i sin egen lagstiftning. Detta leder till ökade cybersäkerhetskrav, men utan en enhetlig modell för alla EU-länder. Det som är ett krav i ett land kan vara en riktlinje i ett annat, vilket skapar komplexitet för företag och tjänsteleverantörer som verkar över nationsgränserna.

17 januari 2025
ENISA kommer att skapa och upprätthålla ett register över ett brett urval av leverantörer av IT-tjänster. Vid detta datum ska varje land kräva att berörda enheter registrerar sig hos behöriga myndigheter. Tjänsteleverantörer (MSP’s) och leverantörer av säkerhetstjänster (MSSP’s) nämns specifikt i detta krav.

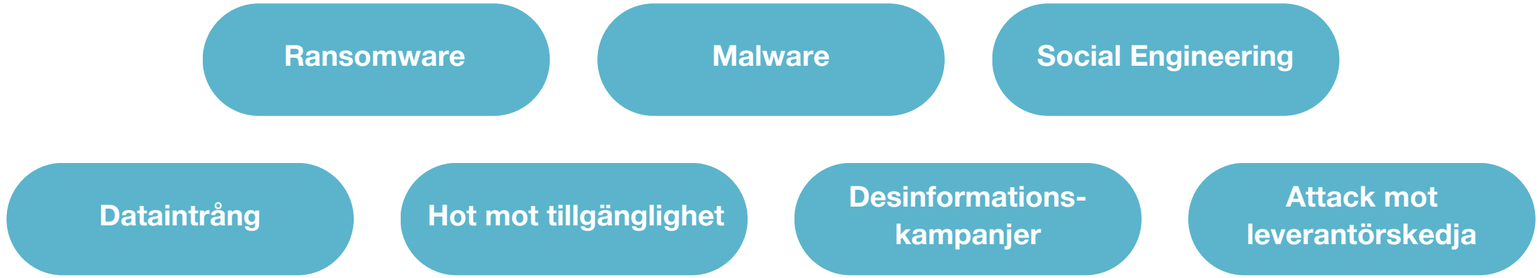
GRIDHEART

Det nya hotlandskapet

Cyberattacker är bland de snabbast växande formerna av brottslighet

Som en av de mest digitaliserade ekonomierna i världen står Sverige inför en tydligt förhöjd hotbild. Den ökade sammanlänkningen av vår digitala infrastruktur, i kombination med det starka fokuset på digitalisering, gör oss mer sårbara och skapar fler möjliga ingångspunkter för cyberattacker. Cyberattacker är en av de snabbast växande formerna av brottslighet och blir allt mer komplexa och kostsamma att försvara sig mot och vi står inför ett omfattande säkerhetshot drivet av aktörer med politiska, militära eller ekonomiska intressen.

Kriminella aktörer drivs i första hand av ekonomiska motiv och de är snabba att anpassa sig till ny teknologi och metoder för att maximera sina vinster. Till skillnad från statliga aktörer bryr de sig mindre om vem de attackerar, så länge målet ger största möjliga avkastning till minsta möjliga risk. Deras verksamhet börjar alltmer likna startups, med en ökad grad av specialisering och en utvecklad infrastruktur för att bedriva cyberbrott, där brottslighet ofta "tjänstefieras" genom försäljning och uthyrning av verktyg och metoder. Gridheart tar cybersäkerhet på största allvar och har därför utformat en bred portfölj med leverantörer för att stärka motståndskraften mot cyberattacker och intrång. Nedan presenteras de vanligaste attackerna genomförda av cyberkriminella.



GRIDHEART

NIS blir NIS2

Det uppskattas att omkring 150 000 organisationer och verksamheter i Europa kommer att omfattas av NIS2 direktivet. För Sveriges del beräknas antalet stiga till så många som 20 000 verksamheter.

Den kraftiga ökningen, upp till 40 gånger fler än under det nuvarande NIS-direktivet, beror på att fler sektorer inkluderas samt att fler verksamheter inom de redan befintliga sektorerna omfattas. Dessutom påverkas leverantörsledet hos dessa verksamheter, vilket ytterligare bidrar till det ökade antalet berörda organisationer.

500

Berörda verksamheter av NIS-lagen i Sverige

x40

=20 000

Uppskattad andel fler verksamheter i Sverige som berörs av NIS2

Nya Säkerhetsåtgärder

Inom ramen för implementeringen av NIS2 direktivet måste organisationer etablera policyer och processer som täcker allt från riskbedömningar och kontinuitetsplanering till incidenthantering, utbildning och åtkomstkontroller. En ny komponent i direktivet är bland annat att organisationer även ansvarar för att säkerställa att deras leverantörer uppfyller de säkerhetskrav som ställs.

Nedan presenteras de sex stödpelare som vi tagit fram ur NIS-2 direktivet. Dessa bör däremot inte användas som ett ramverk för att uppfylla NIS2 krav, snarare en guide för MSPer och IT-leverantörer.

1. **Organisatoriska** säkerhetsåtgärder
2. **Mänskliga** säkerhetsåtgärder
3. **Fysiska** säkerhetsåtgärder
4. Säkerhetsåtgärder för **IT**
5. Säkerhetsåtgärder för **OT**
6. Säkerhetsåtgärder för **Egenutvecklad IT**

Organisatoriska säkerhetsåtgärder

Etablera regler för säker användning av information och relaterade ICT-resurser, som nätverksutrustning och molntjänster. Klassificera information enligt en fastställd modell, till exempel att en passkopia tillhör kategorin personuppgifter, för att ge medarbetare en tydlig översikt för korrekt hantering och skydd.

Dokumentera personalens identitetsuppgifter och implementera en process för hur dessa ska registreras, ändras och raderas (livscykelhantering). Utveckla en cybersäkerhetsstrategi med tydliga riktlinjer för grundläggande cyberhygien, och säkerställ styrningsgodkännande med tydligt definierat ansvar för säkerhetsåtgärder.

Tilldela säkerhetsansvar och inventera alla data och ICT-tillgångar, som programvara och brandväggar, samt utse en ansvarig för varje tillgång. Slutligen, skapa en rutin och checklista för återlämning av företagets tillgångar, som datorer och smartphones, vid avslut av anställning för att skydda konfidentiell information.

Vi på Gridheart distribuerar tjänster som kan hjälpa er med policyhantering, och för detta rekommenderar vi Upolicy i Usecure. För inventering av ICT-tillgångar föreslås N-able samt Acronis som kan inventera en del ICT tillgångar så som nätverksenheter och servrar.

ICT inventering	Acronis N-ABLE
Policyhantering	usecure

GRIDHEART

Mänskliga säkerhetsåtgärder

Direktivet ställer inte bara krav på att organisationer har de tekniska lösningarna på plats, utan även att de arbetar kontinuerligt med cybersäkerhetsträning för de anställda. Idag erbjuder allt fler arbetsplatser sina anställda möjligheten att arbeta både remote och hybrid, vilket ökar vikten av att organisationer implementerar säkra rutiner för att skydda känsliga data och åtkomst till system, oavsett vart de anställda befinner sig. DNS filtrering genom Acronis eller N-able kan hjälpa er stärka säkerheten, genom att blockera åtkomst till skadliga eller oönskade webbplatser med filtrering av domännamn på DNS-nivå. Den hindrar användare från att ansluta till vissa webbplatser genom att förhindra upplösning av deras domännamn till IP-adresser.

Utöver detta ställer NIS2 krav på incidentrapportering, vilket innebär att ni som MSP behöver kunna identifiera, hantera och rapportera säkerhetsincidenter som inträffar hos era kunder. Detta betyder att företag regelbundet måste utvärdera hur väl deras säkerhetsåtgärder fungerar, för att minska risker och hot mot deras informationssystem. För er innebär detta utmaningar i att kontinuerligt mäta och analysera säkerhetsåtgärder för flera olika kunder med varierande behov och det krävs noggrann övervakning och regelbunden rapportering för att även kunna säkerställa att alla åtgärder är effektiva och uppdaterade. Gridheart tar mänskliga säkerhetsåtgärder på största allvar, och vi erbjuder därför tjänster som hjälper er stärka dessa. För utbildning inom cybersäkerhet rekommenderar vi er Usecure och Acronis, och för DNS filtrering tillhandahåller både N-able och Acronis sådana lösningar.

Utbildning inom cybersäkerhet

Acronis usecure

DNS filtrering

Acronis N-ABLE

GRIDHEART

Fysiska säkerhetsåtgärder

För att förhindra att konfidentiell information hamnar i orätta händer är det avgörande att organisationer implementerar tydliga och väl genomtänkta policies som reglerar hur anställda hanterar känslig information. En viktig policy är exempelvis "clean desk"-principen, som innebär att inga dokument, datorer eller annan känslig information får lämnas obevakad eller oskyddad på arbetsbordet. Vid utbyte eller återanvändning av utrustning måste även känslig information och programvara säkert raderas eller skrivas över, för att säkerställa att allt har tagits bort korrekt. Detta kan säkerställas genom policies, vilket minskar risken för att obehöriga personer, både inom och utanför organisationen, får tillgång till känsliga uppgifter.

Direktivet ställer också krav på att organisationer hanterar och efterlever policies för hantering av konfidentiell information. Detta innebär att det måste finnas riktlinjer för hur data klassificeras, överförs och lagras, samt hur anställda får dela eller vidarebefordra känslig information. Tjänster som kan hjälpa er upprätta dessa policies är Upolicy i Usecure, för policyhantering både internt hos er som MSP, men även som ett vertyg till era kunder.

3.

Policyhantering usecure

GRIDHEART

Säkerhetsåtgärder för IT

NIS-2-direktivet kräver dessutom åtgärder inom organisationers cybersäkerhetsplan. Ni som MSP bör därför skydda era alla era kunders servrar, datorer och telefoner från cyberincidenter genom att implementera verktyg för kryptering och begränsning av administrativa rättigheter. Detta görs smidigt genom att aktivera kryptering samt MFA för åtkomst och kommunikation, både hos er internt och för era kunder.

För att upprätthålla en stark cybersäkerhet ska ni även kunna förhindra dataförlust genom en säkerhetskopieringsplan enligt 3-2-1-systemet samt genomföra regelbundna säkerhetskopieringar och tester. Ni bör även kunna se till att programvaror uppdateras genom att vara snabb på att installera uppdateringar. Se därför till att även skapa och analysera loggar för att upptäcka avvikelser som uppstår i bland annat nätverk och applikationer, redan i ett tidigt skede.

Gridheart är specialister inom cybersäkerhet, och vi har därför ett brett utbud på tjänster som gör er motståndskraftiga mot hot och intrång. Till vänster ser ni de tjänster vi rekommenderar till er för respektive område.

MFA tillämpning	KEEPER AUGMENTT
Patchhantering	N-ABLE ATERA
Lösernordshygien	KEEPER LastPass
Säkerhetskopiering och återställning	N-ABLE Acronis
Malware protection	Bitdefender N-ABLE Acronis

GRIDHEART

Säkerhetsåtgärder för OT

Direktivet initierar på att ni som organisation ska kunna identifiera och dokumentera alla affärskritiska hårdvaru- och mjukvarukomponenter, dvs. operativ teknologi-tillgångar som används. Det ska även innehålla information om versioner och patchningar för respektive komponent. Ni måste möjliggöra mappning av tillgångarna och även kunna fastställa hur kritiska de är för organisationen samt riskerna vid avbrott.

Vi vet att det är viktigt med backup, men först nu ställer även direktivet krav på konfigruering och operationell backup. Dessa säkerhetskopior är avgörande för att snabbt återställa system efter tekniska problem eller cyberattacker, vilket förhindrar längre driftstopp och säkerställer affärens kontinuitet.

Organisationer bör även utforma en recovery plan för att kunna planera huruvida de kan återhämta sig från tekniska problem eller cyberattacker. För att testa detta, kan ni simulera återställningsprocessen genom att följa er recovery plan och på så vis se till att de nödvändiga resurserna (såsom konfigurationer, dokumentation etc.) fungerar som de ska. För att utforma en sådan Disaster recovery plan rekommenderar Gridheart er att lägga till Acronis eller N-able i er portfölj.

5.

Disaster recovery

Acronis

N-ABLE

GRIDHEART

Säkerhetsåtgärder för egenutvecklad IT

NIS2 direktivet ställer krav på säkerhet vid anskaffning, utveckling och underhåll av nätverk och informationssystem. Det innebär att organisationer måste säkerställa att alla system och nätverk, från inköp till underhåll, är utformade och hanteras med säkerhet i åtanke. Se till att skydda programvarans källkod med strikt versionskontroll och starka åtkomstkontroller, så att ni kan säkerställa både integritet och säkerhet för applikationen.

Som MSP behöver ni på ett strukturerat och planerat sätt kunna kartlägga all levererad program. Ni behöver alltså få en tydlig överblick över vilken programvara och vilka versionsnummer som används av kunderna, för att kunna planera underhåll och uppdateringar.

6.

Backuptjänster

Acronis

N-ABLE

GRIDHEART

Övergripande sammanfattning

Säkerhets-åtgärder	Acronis	N-ABLE	AUGMENTT	usecure	KEEPER	Bitdefender	ATERA	LastPass
Organisatoriska säkerhetsåtgärder	✓	✓		✓				
Mänskliga säkerhetsåtgärder	✓	✓		✓				
Fysiska säkerhetsåtgärder				✓				
Skerhetsåtgärder för IT	✓	✓	✓		✓	✓	✓	✓
Säkerhetsåtgärder för OT	✓	✓						
Säkerhetsåtgärder för Egenutvecklad IT	✓	✓						

Slutord

Det står nu klart att NIS2 direktivet medför betydande krav och utmaningar för många organisationer. För att uppfylla dessa krav krävs tydliga strategier och rätt lösningar på plats. Vi förstår att det kan vara en komplex och resurskrävande process, och att varje verksamhet har unika behov när det gäller säkerhet och efterlevnad, men vi vill gärna hjälpa er att ta nästa steg. Även om ni, eller era kunder inte direkt påverkas av dessa regleringar är det viktigt att vara proaktivt förberedd, och ni kan även använda detta som en stark standard och en viktig sales enabler.

Genom att arbeta tillsammans kan vi hjälpa er utveckla ett skräddarsytt utbud och implementera de tjänster ni behöver för att möta NIS2 direktivets krav. Vi ser fram emot att ta en diskussion gällande era specifika behov och hjälpa er i att säkra er verksamhet för framtiden.

Vill ni komma i kontakt med oss?

sales@gridheart.com