Liten självgranskning inför Cybersäkerhetslagen (NIS2)

Målgrupp: Ledningsgruppen (VD, GD, COO, CTO, CIO)

Syfte: Att ge en högnivåbedömning av organisationens efterlevnad av cybersäkerhetslagen.

---

1. Inledning

Den nya cybersäkerhetslagen representerar ett skifte för styrning av cybersäkerhet. En stor förändring är införandet av ett personligt ansvar för organisationens ledning. Bristande efterlevnad kan leda till sanktionsavgifter och personliga påföljder.

Detta dokument grankar vår nuvarande position relativt cybersäkerhetslagen inom sex områden. Syftet är att skapa en gemensam förståelse för vår beredskap och att initiera de beslut som krävs för att säkerställa efterlevnad och stärka vår motståndskraft mot cyberhot.

---

2. Analys av Strategiska Beredskapsområden

2.1 Strategi & Förankring

Krav: Organisationen måste ha en formellt godkänd och kommunicerad cybersäkerhetsstrategi. Ledningsgruppen ska aktivt granska och godkänna denna strategi minst en gång per år, samt efter betydande incidenter.[1]

Analys: En formell, ledningsförankrad strategi är grunden för ett systematiskt säkerhetsarbete. Den säkerställer att säkerhetsåtgärder är i linje med verksamhetens övergripande mål och att det finns ett tydligt mandat för säkerhetsfunktionen. Utan en sådan strategi blir säkerhetsarbetet reaktivt och fragmenterat.

Bedömning:

- *Har vi en formellt dokumenterad och godkänd cybersäkerhetsstrategi?*
- *När granskades och godkändes den senast av ledningsgruppen?*
- *Är strategin kommunicerad inom organisationen?*

Rekommenderade Åtgärder:

- Om en strategi saknas: Initiera omedelbart ett projekt för att utveckla en, med tydlig involvering från ledningen.
- Om befintlig strategi är äldre än 12 månader: Schemalägg en formell granskning och ett nytt godkännande på nästa ledningsmöte.

2.2 Resurser

Krav: Ledningsgruppen måste säkerställa att cybersäkerhetsstrategin stöds av tillräckliga resurser, inklusive personal, budget och tekniska verktyg.[1]

Analys: En strategi utan resurser är verkningslös. Lagen kräver ett explicit åtagande från ledningen att finansiera och bemanna säkerhetsarbetet på en nivå som står i proportion till organisationens risker. Detta kräver att cybersäkerhet är en integrerad del av den ordinarie budget- och planeringsprocessen.

Bedömning:

- *Finns det en dedikerad och godkänd budget för cybersäkerhet som är tillräcklig för att möta strategins mål?*
- *Har vi den personal och kompetens som krävs för att hantera våra cyberrisker?*

Rekommenderade Åtgärder:

- Använd resultaten från riskanalyser för att bygga ett tydligt business case för nödvändiga investeringar.
- Säkerställ att resursbehov för cybersäkerhet är en stående punkt i den årliga budgetprocessen.

2.3 Riskacceptans

Krav: Ledningen måste ha en process för att förstå organisationens cyberrisker och formellt godkänna de kvarstående risker som man väljer att inte åtgärda.[1]

Analys: Detta är en central styrningsfunktion. Det säkerställer att ledningen är medveten om och tar ett aktivt ansvar för organisationens riskprofil. Att formellt acceptera en risk innebär ett medvetet beslut att verksamheten kan bära den potentiella konsekvensen om risken skulle materialiseras.

Bedömning:

- *Finns det en etablerad process för att regelbundet rapportera de största cyberriskerna till ledningsgruppen?*
- *Dokumenteras ledningens beslut att acceptera specifika risker?*

Rekommenderade Åtgärder:

- Implementera ett formellt ramverk för riskhantering.
- Inför en stående agendapunkt på ledningsmöten (t.ex. kvartalsvis) för genomgång av riskläget och formellt godkännande av riskacceptans.

2.4 Incidentrapportering

Krav: Organisationen måste ha förmåga att rapportera allvarliga cyberincidenter till berörd myndighet. En första varning ska lämnas inom 24 timmar efter upptäckt.

Analys: De strikta tidsramarna för rapportering ställer höga krav på en välövad och effektiv incidenthanteringsprocess. Detta kräver att roller, ansvar och tekniska system är förberedda innan en incident inträffar.

Bedömning:

- *Har vi en testad incidenthanteringsplan som inkluderar den nya 24-timmarsregeln?*
- *Är det tydligt vem som har mandat att fatta beslut och skicka in en rapport under en pågående kris?*

Rekommenderade Åtgärder:

- Genomför regelbundna övningar (t.ex. "table-top exercises") med ledningens deltagande för att testa incidenthanteringsplanen.
- Säkerställ att det finns tydliga, dokumenterade rutiner och kontaktvägar för rapportering till myndigheter.

2.5 Säkerhet i Leverantörskedjan

Krav: Organisationen måste hantera de cyberrisker som uppstår via leverantörer. Detta inkluderar att ställa säkerhetskrav och följa upp dem, vilket ofta behöver formaliseras i avtal.

Analys: Leveranskedjan är ofta en organisations svagaste länk. Lagen gör det tydligt att ansvaret för säkerheten inte upphör vid den egna organisationens gränser. Vi måste aktivt säkerställa att våra kritiska leverantörer upprätthåller en godtagbar säkerhetsnivå.

Bedömning:

- *Har vi en process för att bedöma cybersäkerheten hos våra kritiska leverantörer?*
- *Innehåller våra standardavtal med leverantörer specifika och juridiskt bindande klausuler om cybersäkerhet (t.ex. krav på incidentrapportering till oss)?*

Rekommenderade Åtgärder:

- Kartlägg och riskbedöm kritiska leverantörer.
- Ta fram en standardiserad säkerhetsbilaga för leverantörsavtal i samarbete med juridisk expertis.

2.6 Ledningens Kompetens

Krav: Medlemmar i ledningsorganet måste genomgå utbildning för att förstå sina skyldigheter och de risker de förväntas hantera enligt lagen.

Analys: För att kunna ta ett aktivt och informerat ansvar krävs en grundläggande förståelse för cyberrisker och de legala kraven. Lagen specificerar att ledningen inte kan delegera bort detta ansvar och därför måste ha tillräcklig kunskap för att kunna styra och ställa krav på verksamheten.

Bedömning:

- *Har ledningsgruppen som helhet genomgått en specifik utbildning om NIS2 och dess konsekvenser för ledningens ansvar?*

Rekommenderade Åtgärder:

- Schemalägg en obligatorisk utbildning för hela ledningsgruppen, skräddarsydd för vårt företag och vår bransch.

---

3. Slutsats och Nästa Steg

Analysen visar att även om vi har ett pågående säkerhetsarbete, ställer den nya cybersäkerhetslagen skärpta och formaliserade krav på ledningens direkta engagemang och ansvar. Att se cybersäkerhet som enbart en IT-fråga är inte längre ett alternativ; det är en strategisk verksamhetsrisk som måste ägas och styras från högsta nivå.

För att säkerställa efterlevnad och stärka vår organisation rekommenderas följande omedelbara åtgärder:

1. **Formellt Godkännande:** Säkerställ att en uppdaterad cybersäkerhetsstrategi formellt godkänns av ledningsgruppen.
2. **Etablera Riskprocess:** Inför en formell process för riskrapportering och riskacceptans på ledningsnivå.
3. **Prioritera Leverantörsrisker:** Initiera ett projekt för att kartlägga och hantera risker i vår leverantörskedja.
4. **Obligatorisk Utbildning:** Boka och genomför en skräddarsydd NIS2-utbildning för hela ledningsgruppen.