axians

Förberedelser för NIS2

En vägledning för berörda verksamheter

VINCI ENERGIES

INNEHÅLLSFÖRTECKNING

Inledning	3
Om Axians	4
1. Förstå NIS2 – vad innebär det för er verksamhet?	5
2. Kom igång – första stegen i förberedelserna	5
3. Kärnrollerna som driver NIS2-arbetet framåt	6
4. Förbättring av teknisk infrastruktur – vad ni behöver tänka på	7
5. Axians roll i att stötta verksamheter	8
6. Praktiska tips och checklista för att komma igång	9
7. Sammanfattningsvis	10

Inledning

EU's nya NIS2-direktiv, som syftar till att förbättra cyber-säkerheten i medlemsländerna, kommer att påverka en stor mängd verksamheter inom kritiska sektorer. Direktivet ställer högre krav på säkerhetsåtgärder och rapportering av incidenter. Det här dokumentet är tänkt att hjälpa företag som berörs av NIS2 att förstå vad som krävs och att påbörja förberedelserna.

Om Axians

Som partner till våra kunder är vårt uppdrag att leverera hållbara och tillgängliga IT-lösningar 24/7. Vårt uppdrag är att säkra våra kunders informationstillgångar och leverera förstklassig vägledning och expertis i nära dialog och med transparens. Vi ligger alltid steget före genom förebyggande vägledning och är en IT-partner som du kan lita på. Dygnet runt, året om. Våra expertisområden är: Cloud & Datacenter, Cybersecurity, Business Application & Data Analytics, Enterprise Networks, ITIL, ServiceNow, Telecom Infrastructure och Digital Workplace.

Vi är en global partner med lokal närvaro. Axians i Sverige har ca 400 anställda och Axians globalt har 16.000 anställda i 37 länder. Det svenska huvudkontoret ligger i Stockholm.

1. Förstå NIS2 – vad innebär det för er verksamhet?

NIS2 är en uppdatering av det tidigare NIS-direktivet, och det utökar omfattningen till fler sektorer och strängare krav på säkerhetsåtgärder. NIS2 gäller nu för en bredare grupp av företag, inklusive energisektorn, sjukvård, finans, transport och leverantörer av digitala tjänster. Det innebär också att företag måste uppfylla krav för både cybersäkerhet och rapportering av incidenter till relevanta myndigheter inom strikta tidsramar. Misslyckande med att uppfylla kraven kan resultera i sanktioner och böter.

2. Kom igång – första stegen i förberedelserna

2.1 Kartläggning av befintliga system och tjänster:

- Börja med att identifiera vilka system, nätverk och tjänster som är kritiska för er verksamhet. Det handlar om allt som kan påverka kontinuiteten och säkerheten i era tjänster.

- Utför en riskanalys för att förstå potentiella sårbarheter. Frågor att ställa är: "Vilka system kan vara måltavlor för cyberattacker?" och "Vilka konsekvenser skulle ett intrång i dessa system få?"

2.2 Granska befintliga säkerhetsåtgärder och policys:

- Genomför en genomlysning av era nuvarande säkerhetsrutiner. Uppfyller de kraven enligt NIS2, såsom säker kommunikation, åtkomstkontroller, incidenthantering och regelbunden säkerhetsgranskning?

- Se över och uppdatera incidenthanteringsplaner. NIS2 kräver att organisationer snabbt rapporterar incidenter, vilket innebär att det behövs tydliga rutiner för att upptäcka hot och eskalera åtgärder.

3. Kärnrollerna som driver NIS2-arbetet framåt

IT- och säkerhetsteamet:

IT-specialister behöver säkerställa att alla tekniska säkerhetsåtgärder är tillräckliga. Deras insatser innefattar kontinuerlig övervakning av nätverk, hotdetektering och regelbunden uppdatering av säkerhetsverktyg.

Ledningsgruppen:

Ledningsgruppen spelar en viktig roll i att fatta beslut om budget och prioriteringar för säkerhetsinvesteringar. De behöver också vara medvetna om de potentiella konsekvenserna av att inte uppfylla NIS2-kraven.

Juridiska avdelningen:

Juridiska experter måste förstå de rättsliga aspekterna av NIS2, inklusive rapporteringskraven och påföljderna vid överträdelser. De kan bidra till att utforma ett regelverk för hantering av incidentrapporter.

Risk- och compliance-ansvariga:

Dessa roller behövs för att övervaka riskhanteringen och se till att verksamheten följer alla nödvändiga regelverk. De bör också ansvara för att säkerställa att riskbedömningar genomförs regelbundet samt implementerar åtgärder för att minska risker.

4. Förbättring av teknisk infrastruktur – vad ni behöver tänka på

System och verktyg för övervakning och upptäckt av hot:

För att uppfylla NIS2 krav behövs lösningar för kontinuerlig övervakning av nätverket och detektering av avvikande beteenden. Verktyg för Security Information and Event Management (SIEM) kan vara användbara här.

Automatisering av säkerhetsåtgärder:

Automatiserade lösningar, såsom Intrusion Detection Systems (IDS) och Intrusion Prevention Systems (IPS), kan hjälpa till att snabbt identifiera och åtgärda hot.

Incidenthantering och kontinuitetsplanering:

Verksamheter måste ha robusta incidenthanteringsplaner som inkluderar hur man snabbt identifierar och svarar på incidenter. Detta innebär också att ha planer för affärskontinuitet för att minimera påverkan på verksamheten.

Cybersäkerhetsutbildning för anställda:

Många säkerhetsincidenter sker på grund av mänskliga misstag. Regelbunden utbildning i cybersäkerhet för alla anställda är därför avgörande för att minimera riskerna.

5. Axians roll i att stötta verksamheter

Axians expertis inom IT- och cybersäkerhet:

Vi erbjuder omfattande tjänster som hjälper verksamheter att uppfylla NIS2-kraven. Med lösningar som täcker allt från riskanalys till övervakning av nätverk. Samt implementering av säkerhetsåtgärder och incidenthantering.

Vår personal inom övervakning jobbar dygnet runt och året om för att stötta er vid eventuella incidenter. En leverans från Axians garanterar en kontrollerad process vad gäller åtkomster, behörigheter och att era lösningar är säkra över tid. Axians behöver också leva upp till de krav som NIS2 medför. Som kund till oss kan ni känna en trygghet i att vi delar med oss av den kunskap och kompetens som vi nyttjat i vårt egna NIS2-arbete.

Våra tjänster och lösningar:

- Axians erbjuder georedundanta infrastrukturlösningar som kan garantera både hög tillgänglighet och en effektiv återställningsförmåga
- Konsultation: Genom en initial analys av ert cybersäkerhetsläge kan vi skapa en handlingsplan för att möta NIS2-kraven.
- Övervakning och incidenthantering: Axians experter hjälper er gärna med implementering och hantering av system för hotdetektering och incidentrespons.
- Utbildning och support: Vi kan tillsammans med våra juridiska partners erbjuda skräddarsydda utbildningar för att förbättra säkerhetsmedvetandet hos era anställda.

6. Praktiska tips och checklista för att komma igång

Prioritera de mest kritiska systemen och tjänsterna:

Börja med de system och processer som har störst påverkan på verksamheten.

Utveckla en handlingsplan och tidplan för att uppfylla kraven:

Säkerställ att alla steg är tydligt definierade och att det finns resurser för att implementera dem.

Se över och uppdatera säkerhetspolicys regelbundet:

Policys bör granskas och anpassas minst årligen, eller vid stora förändringar i verksamheten.

7. Sammanfattningsvis

NIS2 kommer att ställa högre krav på verksamheter, men med rätt förberedelser och stöd kan ni möta dessa krav och samtidigt stärka er cybersäkerhet. Axians står redo att hjälpa er på resan mot fullständig NIS2-efterlevnad. Vi erbjuder expertis inom IT- och cybersäkerhet samt skräddarsydda lösningar som möter just era behov.

Läs mer på Europeiska Kommissionen; **"Direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) – Vanliga frågor"**.

Vill ni veta mer? Kontakta oss för ett förutsättningslöst möte: info.axiansse@axians.com