CYBERSÄKERHET

EARHART BUSINESS PROTECTION AGENCY

Earhart Business Protection Agency

+46-8 400 215 70

contact@earhart.se

www.earhart.se

Besöksadress: Malmskillnadsgatan 44 A
Stockholm

Vi hjälper er skapa en robust och motståndskraftig organisation

Dagens föränderliga värld kräver en stark, flexibel och motståndskraftig organisation.
Vi hjälper er att stärka skyddet mot cyberkriminalitet, samhällsstörningar och morgondagens hotbilder. Kunskap är bästa försvar.

Ledningsstöd:
Managementkonsult stöd där vi ger värdefull insikt om hotbilderna i er bransch, vilka regulatoriska krav som kommer ställas ifrån EU och hur de påverkar er, eller hur verksamheten bör hantera digitalisering och AI.

GAP-analys:
Ni kanske omfattas av NIS2, DORA eller vill ni se till att ni håller en hög informationssäkerhetsnivå för en mer motståndskraftig organisation. GAP-analysen skräddarsys efter era behov och mål.

Krisövning:
Vi rekommenderar att ni genomför minst 2 övningar med krisledningen per år. Vår övningsmodell bygger på skräddarsydda inspel med syfte att öka krisledningens kunskap och förmåga men även att identifiera vilka förbättringsområden som finns och ta fram en åtgärdsplan för dessa.

CHECKLISTA

Informationssäkerhet för företag

Nyckeln till god informationssäkerhet är att veta vilken typ av informationstillgångar som finns och vem som behöver komma åt dem.

Informationssäkerhet är till stor del en fråga om hur system och arbetsrutiner organiseras och kontrolleras. Alla berörda i ett projekt eller en organisation behöver inte ha tillgång till all information i alla system.

Ett viktigt steg är att avgöra vilka roller som behöver tillgång till vilken typ av information och skapa behörighetstrappor och sedan ge dem åtkomst till rätt nivå.

Ett annat viktigt steg är att se till att projektet eller organisationen inte läcker information via tredjepartsleverantörer, dvs underleverantörer, partners och inhyrda konsulter.

Genomför bakgrundskontroller av leverantörer, samarbetsparter och resurser på nyckelfunktioner.

• Säkerställ att systemägarna känner till sitt ansvar och sina system, inklusive behörighetsrutinerna.

• Säkerställ att alla viktiga och kritiska system har tydliga kontinuitetsplaner.

• Säkerställ att behörigheter och åtkomster avslutas när avtal, inkl arbetskontrakt, upphör.

• Fastställ rutiner för informationssäker upphandling/inköp av nya system, tjänster, enheter, mm.

• Följ upp tredjepartsrelationerna regelbundet.

• Följ regelbundet upp klassning av information och tredjepartsleverantörer. Justera vid behov.