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

Säker användning av AI på arbetsplatsen

AI GER STORA MÖJLIGHETER TILL EFFEKTIVISERING PÅ ARBETSPLATSEN. SAMTIDIGT BYGGER ANVÄNDANDET IN SÅRBARHETER OCH NYA HOTBILDER.

- Säkerställ att de AI-verktyg som används är säkra och har genomgått grundliga säkerhetskontroller. Medarbetare bör endast använda godkända verktyg och plattformar.
- Det är viktigt att alla medarbetare har kunskap om de potentiella riskerna med AI och har fått utbildning i att hantera AI-system på ett säkert sätt.
- AI-verktyg kan hallucinera, dvs hitta på saker som inte är korrekta eller till och med absurda. Medarbetarna måste vara medvetna om detta för att undvika allvarliga misstag.
- De flesta AI-tjänster tränar sina modeller på den information användarna matar in. Känslig och personlig information ska inte få användas i AI-system eftersom den återanvänds och kan komma upp hos någon annan. Medarbetarna behöver förstå vikten av att hantera data säkert och följa företagets riktlinjer för dataskydd.
- AI kan användas för att skapa trovärdiga phishing-attacker och sociala manipulationer, inklusive kloning av röst och video. Regelbunden träning i att känna igen och rapportera misstänkta meddelanden är avgörande.
- Se till att AI-system och säkerhetsprotokoll hålls aktuella för att hantera nya hot. Informera medarbetarna om uppdateringar och ändrade rutiner.