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

Cyberhygien

DIN DIGITALA SÄKERHET HANDLAR OCKSÅ OM DITT BETEENDE OCH DIN MEDVETENHET OM RISKER

- Se till att din dator, surfplatta och smartphone kräver inloggning (skärmlås)
- som automatiskt aktiveras.
- Använd långa lösenord med små och stora bokstäver, siffror och specialtecken. Återanvänd inga lösenord, vare sig till olika tjänster eller gamla lösenord.
- Sprid inte ut ditt lösenord genom att skriva upp det i närheten av din dator eller annan lättillgänglig plats.
- Använd flerfaktorsinloggning där det är möjligt. Det ökar säkerheten ordentligt.
- Hantera dina inloggningsuppgifter varsamt! Spara aldrig inloggningsuppgifter i din webbläsare eller i din dator.
- Lämna aldrig ut dina inloggningsuppgifter till andra.
- Låna inte ut ditt konto eller din utrustning som dator/ mobiltelefon.
- Klicka inte på länkar och bilder som du inte vet var de kommer ifrån.
- Scanna inte QR-koder du inte är säker på att de är legitima. De kan leda till falska sidor med skadlig kod.
- Klicka aldrig OK utan att läsa vad du ger OK till. Du kan råka installera virus eller annan skadlig programvara på din enhet.
- Håll dina enheter uppdaterade med senaste versionen av programvara, operativsystem, antivirusprogram, mm.
- Hantera externa USB-minnen, minneskort och hårddiskar med försiktighet. De kan innehålla skadlig kod.
- Undvik att använda publika wifi.