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

Sociala medier

TÄNK PÅ VAD DU LÄMNAR UT FÖR INFORMATION OM DIG SJÄLV OCH DIN FAMILJ. SE TILL ATT ÄGA DIN IDENTITET I SOCIALA MEDIER ÄVEN OM DU VÄLJER ATT INTE VARA AKTIV. DET MINSKAR RISKEN FÖR ATT NÅGON SKA UTGE SIG FÖR ATT VARA DU.

Tänk på:

- Ta del av användarvillkoren, vilken information lagras om dig och dina vänner. Hur hanterar plattformen platsdata, vänlistor, historik eller access till kamera och mikrofon? Välj bort så mycket som möjligt.

- Hur publik är du? Ofta är det du själv som måste ändra inställningar för vem som ska kunna se din profil och vad du publicerar. Undvik att låta främlingar ta del av foton och inlägg.

- Dina digitala fotspår. Det är lätt att kartlägga en person via sociala medier. Intressen och vanor finns i överflöd och kan utnyttjas av kriminella eller andra aktörer med oärliga avsikter för att skapa en profil av dig för till exempel bedrägerier.

- Bilder och video kan avslöja för mycket! Bakgrund, andra personer och föremål kan avslöja saker om dig som du inte vill att andra ska veta.

- Omvärldsbevaka din identitet. Se till att regelbundet söka efter din identitet på olika plattformar så ingen använder den utan din vetskap.

- Säkra lösenord och säkra enheter. Aktivera tvåfaktorsautentisering för dina sociala medier. Då minskar du risken att någon kapar ditt konto.