CHECKLISTA

Skapa en effektiv process för att motarbeta insiderbrott

1. Ta reda på vilka insiderhot som är unika för er organisation:

- ✔ Vilken data är kritisk eller viktig? (Tänk i banor som: Ostrukturerad data, intellektuell egendom, kunder, lagstiftade krav, GDPR)
- ✔ Var finns denna kritiska och viktiga data?
- ✔ Vilka individer utgör störst risk? (Tänk i banor som: Anställda på väg att lämna företaget, anställda med tillgång till känslig data, anställda som ofta visar bristande förståelse för datasäkerhet, underentreprenörer, externa konsulter etc.)
- ✔ Om ni inte redan har en klar bild över ovanstående punkter är det klokt att börja med att skapa en rapport som omfattar organisationens risker och hur dessa risker påverkar verksamheten.

2. Erhåll stöd från ledning och andra viktiga intressenter:

- ✔ Presentera en korrekt bild över risker och konsekvenser som är unika för er organisation, samt var okända risker kan finnas.
- ✔ Samla in data om insiderhot och trender — Verizon DB, CERT, Ponemon, etc.
- ✔ Samla in, och informera om, insiderbrott som synts i nyheter och media.
- ✔ Diskutera organisationens beredskap, var ni befinner er idag och vart ni vill nå och hur.

3. Bedöm vilka verktyg som behövs för att hantera insiderhot:

- ✔ Utvärdera de verktyg ni har idag och identifiera vad som saknas för att kunna hantera insiderhot och insiderbrott.
- ✔ Sök reda på verktyg som kan integreras med, eller komplettera, era befintliga verktyg.
- ✔ Fokusera på verktyg som har förmågan att upptäcka, undersöka och agera på risker snabbt och effektivt.
- ✔ Genomför ett ”Proof-of-Concept” för att se om projektet är hållbart och kan genomföras framgångsrikt.

4. Skapa en process och dokumentera

- ✔ Bestäm vilka kriteria som skall användas för kontroll och förebyggande samt vilken typ av händelser som skall hanteras som risker, samt vilka som skall exkluderas från att hanteras som insiderrisker.
- ✔ Dokumentera hur processen vid en insiderincident skall se ut, så att processen kan återupprepas och leda till samma resultat hela tiden.
- ✔ Dokumentera hur en insiderincident eskaleras till att bli ett möjligt insiderbrott, och hur det skall behandlas.
- ✔ Genomför regelbunden test av er process och uppdatera systemet utifrån nya arbetssätt och rutiner.

5. Kommunicera

- ✔ Ta fram och använd en policy för hur data inom organisationen får användas (UAP - Acceptable Use Policy) och se till att alla inom organisationen tar del denna policy — inkludera även underentreprenörer och konsulter.
- ✔ Inkludera er Insiderhotpolicy i interna säkerhetsutbildningar.
- ✔ Gör anställda medvetna om att det finns ett system för förebyggande av insiderbrott, men avslöja inte vilka verktyg som används.
- ✔ Rapportera till ledning och viktiga intressenter om hur systemet används och erfarenheter av systemet.

6. Förenkla och utveckla programmet så att det hela tiden är upp-to-date med risker i omvärld och internt.