Inlämningsuppgift: Cybersäkerhetsanalys för Tech-Högskolan

Företagsbeskrivning – Tech-Högskolan

Tech-Högskolan är en utbildningsinstitution med campus på två orter och över 900 inskrivna elever. Skolan använder Microsoft Azure för sina användarkonton och viss datalagring, men saknar intern IT-kompetens och personal dedikerad till cybersäkerhet. All administration hanteras av utbildningsledare, affärsutvecklare och andra administrativa roller utan erfarenhet inom IT-säkerhet, vilket innebär att medvetenheten kring cybersäkerhetsrisker är låg.

Infrastruktur och datahantering

Skolan har en molnbaserad lösning via Microsoft Azure, där de hanterar användarkonton och vissa applikationer, inklusive en lärplattform som innehåller känsliga uppgifter som elevers persondata, betyg och akademiska prestationer. Flera elever och personal har tillgång till molnsystemet, men åtkomsten är inte särskilt begränsad eller differentierad.

Fysisk och digital säkerhet

För fysisk åtkomst till skolans lokaler används en fyrsiffrig kod. När man har kommit in i byggnaden finns inga ytterligare skydd eller begränsningar, och koden är gemensam för både studenter och personal. Det finns heller ingen övervakning av lokalerna, vilket gör att obehörig fysisk åtkomst är svår att upptäcka.

Incidenter och cybersäkerhetshistorik

Tech-Högskolan har nyligen drabbats av ett allvarligt cybersäkerhetsincident: en obehörig aktör lyckades få tillgång till deras Azure-miljö och använde skolans virtuella maskiner för att utvinna kryptovaluta. Incidenten resulterade i stora ekonomiska förluster för skolan, vilket tydliggjorde behovet av förbättrad IT-säkerhet och ett mer systematiskt förhållningssätt till cybersäkerhet. I nuläget saknar skolan både rutiner för incidenthantering och en formell återställningsplan.

Uppgiftsinstruktioner

Du arbetar nu som cybersäkerhetsanalytiker för Tech-Högskolan. Din uppgift är att leverera en rapport som beskriver hotbilden, identifierar säkerhetsbrister och föreslår konkreta säkerhetsåtgärder. Din rapport ska vara tydlig och baserad på relevanta teorier, verktyg och standarder inom cybersäkerhet.

Del 1: Identifiera hot och risker (cirka 1 sida)

- **Beskriv hotbilden** för Tech-Högskolan. Identifiera minst tre olika typer av hot (t.ex. obehörig åtkomst, social manipulation, phishing).
- **Analysera konsekvenser**: Vad kan hända om dessa hot blir verklighet? Diskutera hur dessa cyberrisker påverkar elevernas personuppgifter och skolans verksamhet.
- **Beskriv potentiella hotaktörer**: Vem kan tänkas attackera skolan och varför?

Del 2: Förklara grundläggande verktyg och tekniker (cirka 1 sida)

- **Identitets- och åtkomsthantering**: Beskriv vilka tekniker som kan användas för att stärka åtkomstkontrollerna på skolan. Ge exempel på verktyg, som tvåfaktorsautentisering och åtkomstloggning.
- **Infrastrukturell cybersäkerhet**: Ge exempel på enkla säkerhetsrutiner och verktyg (t.ex. brandväggar, antivirusprogram) som skolan kan använda för att öka säkerheten.

Del 3: Förberedelse inför och försvar mot cybersäkerhetsincidenter (cirka 1-2 sidor)

- **Föreslå tekniker för att förebygga och upptäcka hot**: Beskriv hur tekniker som EndPoint Detection and Response (EDR) och Network Detection and Response (NDR) kan skydda skolans system. Förklara kortfattat hur dessa verktyg fungerar.
- **Incidenthantering och återställningsplan**: Beskriv hur en incidenthanteringsplan kan se ut och varför den är viktig. Skapa ett exempel för en incidentplan anpassad till Tech-Högskolan, t.ex. hur man skulle hantera en situation liknande den tidigare incidenten med kryptomining.
- **Återställning efter intrång**: Förklara vad en återställningsplan innebär och varför det är viktigt för skolan att kunna återgå till normal drift efter ett intrång.

Del 4: Riskhantering och sårbarhetsanalys (cirka 1 sida)

- **Riskbedömning och hotanalys**: Gör en enkel riskbedömning för Tech-Högskolan, där du identifierar och prioriterar minst tre risker.
- **Förslag på riskhantering**: För varje risk, föreslå en metod för att minska eller eliminera den. Beskriv hur resultatet av en sårbarhetsskanning kan hjälpa till att identifiera risker.

Betygskriterier

För att få godkänt ska den studerande:

- Visa en förståelse för olika typer av hot och deras konsekvenser.
- Kunna förklara grundläggande cybersäkerhetsverktyg och tekniker.
- Beskriva tillvägagångssätt för incidenthantering, riskbedömning och återställning.
- Ha en grundläggande förståelse för juridiska och etiska aspekter inom cybersäkerhet.

För att få väl godkänt ska den studerande:

- Visa fördjupad förståelse av hot och intrång samt hur dessa påverkar Tech-Högskolans verksamhet.
- Ge konkreta och välmotiverade förslag på säkerhetslösningar anpassade till skolans situation.
- Visa förmåga att analysera och prioritera risker samt föreslå lämpliga metoder för att hantera dessa.