Säkerhetsriskbedömning – Nätverkshärdning

1. **Anställda delar lösenord.**
2. **Administratörslösenordet för databasen är fortfarande standardinställt.**
3. **Brandväggar saknar regler för att filtrera nätverkstrafik.**
4. **Multifaktorautentisering (MFA) är inte aktiverad.**

Om dessa problem inte åtgärdas **riskerar företaget ytterligare attacker**

Verktyg och metoder för nätverkshärdning

Inför starka lösenordspolicyer

Problem: Anställda delar lösenord, och databasen använder ett standardlösenord för administratörskontot.
Lösning:
- Användning av **unika, komplexa lösenord** (minst 12 tecken med siffror och specialtecken).
- Använd **lösenordshanterare** för att undvika att anställda delar lösenord.
- Inför **regelbundna lösenordsbyten** för att minska risken för intrång.

Konfigurera brandväggsregler

Problem: Det finns inga brandväggsregler för att filtrera inkommande och utgående nätverkstrafik.
Lösning:
- Ställ in **brandväggsregler** för att **blockera skadlig trafik** och endast tillåta nödvändiga tjänster.
- Aktivera **portfiltrering** för att stänga oanvända portar och minska angreppsytan.
- Genomför **regelbundna granskningar av brandväggsloggar** för att identifiera ovanlig aktivitet.

Inför multifaktorautentisering (MFA)

Problem: Ingen MFA används.
Lösning:
- Kräva **MFA vid alla inloggningar**, särskilt för **administratörskonton** och **fjärråtkomst**.
- Använd **tidsbaserade engångslösenord (TOTP)** eller **hårdvarunycklar** för extra säkerhet.

Slutsats

Dataintrånget kunde ha förhindrats genom **grundläggande nätverkshärdningsmetoder**. Genom att implementera **starka lösenord, brandväggsregler och MFA** kan företaget **minska risken för intrång och förhindra framtida attacker**.

Förberett av: Zayn AK **Roll:** Säkerhetsanalytiker