De flesta intrång börjar inte med teknik – utan med identitet

Secured By Telia Cygate

Fem fallgropar i identitets- och behörighetshanteringen

Identiteter och behörigheter är nyckeln till hela IT-miljön, och en central del i cybersäkerhetslagen. De avgör vem som får tillgång till vilka system och vilken information som kan nås. När hanteringen inte är systematisk uppstår risker som ofta går under radarn i vardagen, men som snabbt får konsekvenser när något väl händer. Här är fem vanliga fallgropar i identitets- och behörighetshanteringen, och vad som krävs för att ta sig över dem.

1. För många behörigheter – till för många

Utmaning:
Behörigheter delas ofta ut generöst, för att människor ska kunna "jobba effektivt". Med tiden samlas åtkomst på hög. Användare får rättigheter till system de sällan använder, eller inte längre arbetar i. Resultatet blir en miljö där det är svårt att veta vem som egentligen har tillgång till vad – och varför.

Lösning:
Utgå från principen om minsta möjliga behörighet. Tilldela åtkomst utifrån faktisk roll och behov, och följ upp regelbundet. Behörigheter ska inte vara permanenta som standard, utan något som kan justeras när roller förändras.

2. Otydligt ägarskap för identiteter och konton

Utmaning:
När ansvaret är oklart händer ofta ingenting. IT hanterar tekniken, HR hanterar anställningen, chefer ansvarar för verksamheten – men ingen känner fullt ansvar för identiteten som helhet. Det gör att beslut om åtkomst, förändringar och avveckling drar ut på tiden eller uteblir helt.

Lösning:
Gör ägarskapet tydligt. Vem ansvarar för att en identitet är korrekt över tid? Vem godkänner behörigheter? Vem tar bort åtkomst när något förändras? När ansvar och mandat är tydliga minskar både risk och friktion.

3. Konton som lever längre än relationen

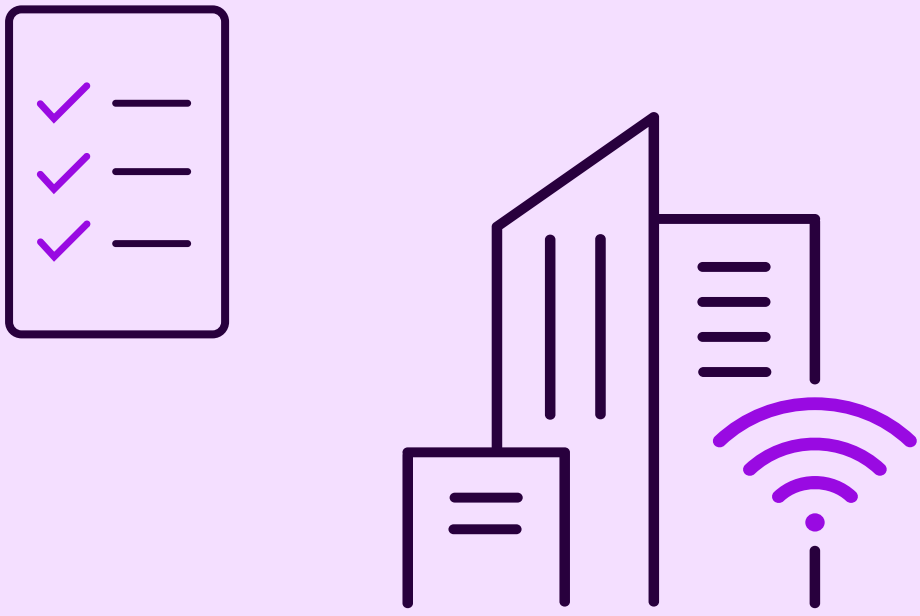
Utmaning:
När anställda byter roll, konsulter avslutar uppdrag eller samarbeten upphör, följer behörigheterna inte alltid med i förändringen. Konton och åtkomst blir kvar – ibland av gammal vana, ibland av rädsla för att något ska sluta fungera.

Lösning:
Knyt identiteter och behörigheter till livscykler. När relationen till verksamheten förändras, ska också åtkomsten göra det. Avveckling behöver vara lika självklar som tilldelning.

4. Skydd finns – men används inte konsekvent

Utmaning:
Multifaktorautentisering och andra skydd finns ofta tillgängliga, men används inte överallt. Undantag görs för vissa system, användargrupper eller äldre lösningar. Det skapar en falsk känsla av säkerhet, samtidigt som angripare ofta hittar just de svagaste länkarna.

Lösning:
Sträva efter konsekvens. Skydd ska gälla brett och följas upp över tid. Undantag behöver vara medvetna, motiverade och dokumenterade – inte något som bara blivit kvar.



5. SIdentitet ses som teknik – inte som styrning

Utmaning:
Identitets- och behörighetshantering behandlas ofta som en teknisk fråga. Men i grunden handlar det om beslut, ansvar och risk. När identitet lämnas till IT utan tydligt verksamhetsansvar saknas ofta både prioritering och förankring.

Lösning:
Lyft identitet till en styrningsfråga. När ledning och verksamhet är involverade blir det tydligare vad som är viktigt, vad som är acceptabel risk och hur arbetet ska följas upp. Det är först då identitet kan bli ett verkligt skydd, och inte bara en teknisk lösning.

Identitets- och behörighetshantering handlar inte om perfektion, utan om kontroll. När ansvar, livscykler och arbetssätt hänger ihop minskar risken för intrång, och organisationen står bättre rustad när något händer.

Läs mer