Auditní seznam SaaS aplikací

Pokud chcete udělat konkrétní kroky bez velké teorie, odpovězte si na otázky z tohoto základního auditního seznamu. Rychle tak zjistíte, kde hrozí rizika a co řešit jako první.

Přehled a vlastnictví

- Máte aktuální katalog používaných SaaS aplikací a bezpečnostní standard pro jejich používání?
- Je jasné, které aplikace jsou schválené, které ne a které na schválení čekají?
- Má každá klíčová aplikace jasného vlastníka, který za ni ručí?

Data a sdílení

- Máte definováno co jsou citlivá data a kde se v SaaS typicky objevují?
- Je pod kontrolou externí sdílení (kdo smí sdílet mimo firmu a za jakých podmínek)?
- Jsou ošetřeny veřejné odkazy (povolené/nepovolené, případně časové omezení)?
- Určili jste, kdo může exportovat citlivá data a jak s nimi může dál nakládat?

Přístupy a oprávnění

- Je zapnuté vícefaktorové ověření u klíčových aplikací?
- Kdo má administrátorská práva a proč?
- Existují sdílené účty nebo účty bez vlastníka?

Integrace a tokeny

- Má každá integrace vlastníka a popsaný účel?
- Víte, jak integraci vypnout a jak zneplatnit její přístupy (tokeny/klíče)?
- Probíhá pravidelná revize, co integrace skutečně umí a k čemu má oprávnění?

Offboarding

- Máte daný postup, co dělat napříč SaaS aplikacemi po odchodu zaměstnance?
- Kontroluje se zrušení „bočních“ přístupů (integrace, tokeny, sdílení dokumentů)?
- Je vyřešen převod vlastnictví (dokumenty, složky, automatizace)?

Průběžná kontrola

- Máte nastaveny pravidelné revize (oprávnění/role, sdílení, integrace) u klíčových aplikací?
- Máte u SaaS aplikací zapnuté logování a upozornění na podezřelé události?
- Pokud je aplikací hodně, využíváte podpůrné nástroje pro průběžný dohled (např. SSPM/CASB)?
- Víte, kdo zasahuje, když přijde upozornění na neobvyklý přístup nebo sdílení?

Tato kontrola vám dá rychlou mapu rizik.
Ve firmách, kde SaaS aplikace přibývají organicky, bývá největším přínosem už to, že máte přehled, vlastníky a pár jasných pravidel, která se dají dlouhodobě udržet.