Was ist Shadow AI, und wer in meiner Organisation erzeugt dieses Risiko?

Kurze Antwort: Shadow AI bezeichnet Mitarbeitende, die KI-Tools nutzen, die von der IT nicht genehmigt wurden oder ihr nicht bekannt sind. Das Risiko beschränkt sich nicht nur auf einfache Mitarbeitende – privilegierte Administratoren und kompromittierte Konten stellen oft die größere Gefährdung dar.

Drei Quellen der Gefährdung

- **Mitarbeitende**, die nicht genehmigte KI-Tools für alltägliche Produktivitätsaufgaben nutzen.
- **Privilegierte Administratoren**, deren weitreichender Zugriff bedeutet, dass alles, was sie einem KI-Tool zuführen, hochsensible Unternehmensdaten enthalten kann.
- **Kompromittierte Konten**, bei denen ein Angreifer mit gültigen Zugangsdaten KI-Tools als Exfiltrationskanal nutzt – Datenverkehr, der wie gewöhnliche Produktivität aussieht.

Dies geschieht bereits

Cyber Crucible hat direkt beobachtet, wie Mitarbeitende mithilfe von KI-Tools massenhaft auf große Datenmengen gleichzeitig zugreifen, um Informationen zu suchen und hochzuladen. Dies ist kein theoretisches, zukünftiges Risiko, das lediglich modelliert wird; es handelt sich um Verhaltensweisen, die bereits heute in realen Umgebungen sichtbar sind.

Die dritte Kategorie verdient besondere Aufmerksamkeit. Ein Angreifer, der KI-Tools nutzt, um Daten abzuziehen, ist kaum von einem engagierten Mitarbeitenden zu unterscheiden – es sei denn, die Durchsetzung erfolgt auf der Ebene des Datenzugriffs, wo Absicht und Richtlinie unabhängig davon bewertet werden können, wer angemeldet ist.

Revision #1
Created 2026-07-24 04:36:12 UTC by Dennis Underwood
Updated 2026-07-24 04:36:12 UTC by Dennis Underwood