5 Gründe, warum Schäden durch Insider-Bedrohungen oft unbemerkt bleiben

Der schnelle Übergang zu cloudbasierten Systemen und Remote-Arbeitsumgebungen hat die Risiken von Insider-Bedrohungen erheblich vergrößert. Das Problem liegt darin, dass Insider-Bedrohungen oft weniger schädlich wirken als externe Bedrohungen, was ihre Identifikation und effektive Bekämpfung erschwert.

WAS SIE MÖGLICHERWEISE SEHEN	WAS DARUNTER VERBORGEN IST
Akteur	
Vertraute Kollegen Insider-Bedrohungen gehen von Mitarbeitern und Auftragnehmern aus, die gemeinsame Interessen verfolgen, nicht von kriminellen oder staatlichen Akteuren.	Berechtigter Zugriff bleibt unbemerkt Insider müssen nicht hacken – sie haben bereits die Schlüssel, um sich unbemerkt zu bewegen.
Absicht	
Selten böswillig Die meisten Mitarbeiter sind wirklich vertrauenswürdig und versuchen einfach, schneller und effizienter zu arbeiten.	Schädlich, unabhängig von der Absicht Das Offenlegen von IP oder sensiblen Daten verursacht ernsthaften Schaden für das Unternehmen – unabhängig von der Absicht.
Geschwindigkeit & Umfang	
Isolierte Vorfälle Insider-Bedrohungen sind in der Regel isolierte Vorfälle, die einen bestimmten Satz von Dateien betreffen.	Unentdeckt und beständig Insider-Bedrohungen bleiben typischerweise monatelang – oder jahrelang – unentdeckt, wodurch Ihr IP oder sensible Daten mehr Zeit haben, in die falschen Hände zu geraten.
Incident Response	
Gemeinsame Verantwortungen Sicherheitsteams sind nicht allein – HR und die Rechtsabteilung spielen eine entscheidende Rolle bei der Reaktion.	Die gemeinsame Reaktion hängt von vollständiger Transparenz ab Sicherheit muss das Problem schnell erkennen und HR sowie der Rechtsabteilung den Kontext für eine effektive Reaktion liefern.
Geschäftsauswirkungen	
Wird das Geschäft nicht zum Stillstand bringen Es gibt selten einen dringenden Wettlauf, Insider-Bedrohungen zu blockieren, da diese einen nuancierten Ansatz erfordern, um den Kontext zu verstehen.	IP-Verlust = Verlust des Wettbewerbsvorteils Insider-Bedrohungen zielen auf die wertvollsten Informationen in Ihrem Unternehmen: Ihre IP. Das tägliche Geschäft läuft weiter, aber ein geleaktes IP kann langfristig exponentiell teurer werden.

Die Art, wie wir arbeiten, hat sich verändert. Es ist Zeit, dass sich auch der Datenschutz verändert.

60%

der Mitarbeiter in mittelständischen Unternehmen geben zu, Arbeitsdateien in ihre persönlichen Konten zu verschieben.

$15M

Die durchschnittlichen Kosten eines einzelnen Insider-Bedrohungs-Vorfalls.

99%

der Unternehmen verwenden herkömmliche DLP-Lösungen, aber trotzdem nehmen die von Insidern verursachten Datenvorfälle zu.

Sehen Sie den Incydr-Ansatz

Sicherheitsteams benötigen einen neuen Ansatz, der ihnen die nötige Sichtbarkeit, den Kontext und die Kontrollen bietet, um wertvolle Daten vor unbefugtem Zugriff zu schützen, ohne das Geschäft zu behindern. **Erfahren Sie mehr über Incydr.**