BETRIEBSRÄTE/BETRIEBSRATSVEREINBARUNGEN UND VARONIS

Überblick

Betriebsräte fungieren in Deutschland als Arbeitnehmervertretung eines Unternehmens und ergänzen an dieser Stelle die nationalen Arbeitsorganisationen.

Eines der Ziele des Betriebsrates ist es, sicherzustellen, dass Mitarbeiterdaten und Informationen geschützt und komplett vertraulich behandelt werden.

Varonis-Lösungen sind entwickelt worden, damit Unternehmen produktiver arbeiten, um IT-Risiken zu minimieren und gleichzeitig Kosten zu reduzieren. Varonis unterstützt Firmen dabei, ihre Sicherheitsrichtlinien zu verstärken und die Vertraulichkeit von Mitarbeiterdaten umfassend zu verbessern. Varonis erlaubt es IT-Abteilungen, das Berechtigungsmanagement zu optimieren und entsprechend zu kontrollieren.

Dadurch wird verhindert, dass unautorisiert auf sensible Daten zugegriffen wird oder Datenschutzverletzungen die Folge sind. Varonis unterstützt Unternehmen zusätzlich dabei, vertrauliche Mitarbeiterdaten zu schützen.

Varonis bietet einen komplett transparenten Audit-Trail aller Zugriffsaktivitäten in Bezug auf unstrukturierte oder semi-strukturierte Daten. Das führt in manchen Fällen zu Bedenken beim Betriebsrat inwieweit diese Informationen zu Leistungskontrollen bei Mitarbeitern benutzt werden könnten oder die Vertraulichkeit der Daten in anderer Weise gefährdet sein könnte.

Dies ist nicht der Fall. Der Varonis Audit-Trail dokumentiert weder die Zeitdauer innerhalb derer an einer Datei gearbeitet wird, noch die Art der Nutzungsaktivität.

Varonis-Lösungen verbessern die IT-Sicherheit, da sie Informationen bereitstellen, die bei forensischen Nachforschungen hilfreich sind, veraltete Datenbestände identifizieren, Empfehlungen aussprechen wie Zugriffsberechtigungen am besten vergeben werden, die eigentlichen Dateneigentümer finden sowie die Modellierung von Berechtigungsänderungen erlauben.

Varonis-Software stärkt die Sicherheitsrichtlinien innerhalb eines Unternehmens, denn sie garantiert, dass die richtigen Personen auf die richtigen Daten zugreifen, dass dieses Berechtigungsmodell kontinuierlich umgesetzt wird und dass unbefugte Zugriffe auf Daten aufgedeckt und kontrolliert werden. Dies trägt unmittelbar dazu bei, die Privatsphäre der Mitarbeiter zu schützen.