IT-Governance und Risk Management

written by Christian Hafner | 22 September, 2022

Riskmanagement & IKS News

Wirtschaft und Recht

IT-Governance und Risk Management

Wenn CIO (Chief Information Officer) Fehler machen, können die Folgen verheerend sein.

«Die IT-Governance sollte gut definiert, sowie klar verständlich sein und sich an Prinzipien orientieren, die die Mission, Vision und Strategie des Unternehmens widerspiegeln.»

Diesem Grundsatz würde wohl jeder IT-Chef zustimmen. Trotzdem wird immer wieder vergessen, die IT-Governance an neuen Geschäftspraktiken oder die veränderte Unternehmens-Governance anzupassen.

Risk Management tut not.

Kommt dazu, dass CIOs (Chief Information Officer) häufig strategische Initiativen starten, ohne alle damit verbundenen Risiken vollständig zu berücksichtigen.

Allzu oft werden kritische Initiativen von CIOs vorangetrieben, ohne dass sie genau wissen, ob das System seine strategischen Ziele erreichen kann.

Für den Erfolg einer strategischen Initiative ist es unerlässlich, diese Risiken frühzeitig zu erkennen und sie mit einem organisierten Risikominderungsprozess als Teil eines umfassenden Governance-Programms anzugehen.

Kommt dazu, dass die dezentrale, hybride IT-Arbeitsumgebung – in Kombination mit hoher

Mitarbeiterfluktuation – das Risiko von Schäden durch Innentätern erhöht.

Während alle Arten von Insider-Bedrohungen potenziell schädlich sind, können böswillige Mitarbeiter, die mit externen Angreifern zusammenarbeiten, besonders schädlich sein.

FAZIT: Die IT-Governance sollte drei Dinge priorisieren:

- Datensicherheit,
- Implementierung von Best Practices für die Netzwerksicherheit und
- optimale Cyber-Schulungen für Anwender.

Um ein effektives Content-Governance-Programm aufzubauen, ist es zudem wichtig, einen umfassenden Einblick in strukturierte und unstrukturierte Daten zu haben.

Wenn man die Daten nicht sehen kann, kann man sie auch nicht richtig verwalten.

Zudem ist es empfehlenswert, Datenansichten zentral zu verwalten, um zu verstehen, auf welche Inhalte von wem zugegriffen wird.

Auf diese Weise kann das Unternehmen bösartige Aktivitäten erkennen, indem es alltägliches Benutzerverhalten und Muster erkennt.

Quellen: *John Edward «Die beliebtesten IT-Governance-Fehler» 6.9.2022 cio.de*