

Roadmap zur Meldung von Datenvorfällen

Auf einen Vorfall aufmerksam gemacht

Ergreifen Sie sofortige Maßnahmen zur Risikominderung und **benachrichtigen Sie die lokale IT**. Beschränken Sie die schriftliche Kommunikation, arbeiten Sie nach dem Need-to-Know-Prinzip und vermeiden Sie die Verwendung definierter Rechtsbegriffe wie „Verletzung“. **Die lokale IT benachrichtigt den RPM-Direktor über Info-Sek.**

Wo ist der Zugangspunkt?

Identifizieren Sie die Grundursache oder den anfänglichen Zugangspunkt. **Group IT wird zusammen mit dem RPM Director von Info Sec den Vorfall isolieren und mindern.**

Sind kritische Systeme betroffen?

Die IT bestimmt den Schweregrad der Auswirkungen. **RPM Director von Info Sec benachrichtigt RPM General Counsel und RPM CFO**. GC und CFO bestimmen, ob/wann der RPM BoD benachrichtigt werden soll.

Betroffen sind Operationen, Beziehungen oder Finanzen?

Wenn ja, bestimmen Sie, welche davon betroffen waren, und den **Director of Info Sec, um RPM VP of Ops und VP Corp. zu benachrichtigen. Nutzen- und Risikomanagement, VP Corp.**

Die Leistungen bestimmen, ob/wann der Versicherungsanbieter benachrichtigt werden muss.

Rechtliche Meldepflichten?

Dies wird von RPM Legal and Compliance in Zusammenarbeit mit externen Datenschutz- und Sicherheitsberatern festgelegt. **Melden Sie einen Vorfall nicht extern ohne Rücksprache mit der RPM-Rechtsabteilung.**

Meldepflichtiges Ereignis (RE) ablegen

REs müssen **unverzüglich nach Kenntnisnahme von Datenvorfällen** eingereicht werden. **RPM-Direktor von Info Sec und Datenschutzteam über das meldepflichtige Ereignis benachrichtigt.**

Welche Daten sind beteiligt?

Der RPM-Direktor von Info Sec benachrichtigt den zuständigen Gruppenanwalt. Beziehen Sie interne EU/UK-Rechtsanwälte ein, wenn Daten aus Europa involviert sind. Sensible Daten werden die potenziellen Auswirkungen erhöhen.

Betroffene Finanzsysteme?

Wenn ja, muss die IT den Umfang der Auswirkungen identifizieren. **Direktor von Info Sec benachrichtigt die internen Prüfer von RPM.** Die interne Revision bestimmt, ob/wann externe Auditoren benachrichtigt werden sollen.

Potenzielle Reputationsschäden?

Wenn ja, bestimmt die IT in Zusammenarbeit mit dem Unternehmen das Ausmaß des Schadens und **benachrichtigt das RPM Communications Team.**

War das Vorfalldmaterial?

RPM Legal bestimmt die Wesentlichkeit, die angemessene Berichterstattung, Pressemitteilungen und andere erforderliche Kommunikationen.

Kommentieren Sie keinen Vorfall extern ohne vorherige Genehmigung.