DigiCert reports data breach after migration error exposed an internal system



DigiCert says a server migration mistake left an internal business system reachable from the internet, allowing unauthorized access to customer information and identity documents.

- DigiCert disclosed a data breach affecting customer information and identity documents.
- The cause was a server migration that mistakenly exposed an internal business system to the internet.
- Unauthorized parties were able to access the exposed system.
- The source excerpt gives no figures on how many customers were affected.

DigiCert has warned that it suffered a data breach. According to the report, a server migration was carried out incorrectly and left an internal business system exposed to the internet. That exposure allowed unauthorized

access to customer information and identity documents.

What is known

The available source text is brief. It confirms the cause (a migration mistake), the nature of the exposed data (customer information and identity documents) and that access was unauthorized. It does not provide details here on the number of customers affected, the time window, or the specific data fields involved.

Why it matters for regulated institutions

Organizations in the Kingdom that buy certificates or validation services from DigiCert may have supplied identity documents during onboarding or validation. Such documents can contain personal data, so a supplier-side exposure can raise obligations under the **PDPL** and third-party risk requirements, even though the fault lies with the vendor.

The incident also illustrates a wider point: infrastructure changes such as migrations can open unintended exposure when they are not reviewed against security baselines.

Recommended approach

Avoid assumptions until DigiCert provides direct notification. Confirm whether your organization is affected, establish what data was shared with the vendor, and document your assessment so it can support any later regulatory discussion.

What to do now

1. Check whether your organization holds DigiCert products or services and identify the business owner.
2. Review which identity documents and personal data were submitted to DigiCert for validation.
3. Watch for and request direct notification and incident details from DigiCert.
4. Assess PDPL notification obligations with your data protection officer once impact is confirmed.
5. Add change-review checks for exposure to your own migration procedures.