Austrian Foreign Ministry website breached via external provider; diplomats' contact details accessed



Hackers breached a Foreign Ministry website run by an external provider on 12–13 November and accessed names and official contact details of staff. The ministry says the incident is contained and no public data was affected.

- The breach took place between 12 and 13 November on a website operated by an external service provider.
- Names and official contact details of staff at the Vienna headquarters and at missions abroad were accessed.
- The ministry says the incident is contained and no personal data of members of the public was compromised.
- The attackers are unidentified, and it is unclear how they got in or whether data was actually

stolen.

- The ministry notified Austria's cybersecurity and data protection authorities and has not attributed the incident to any actor.

Austria's Foreign Ministry said it was the target of a breach affecting one of its websites. According to a ministry statement reported by public broadcaster ORF, the intrusion took place on 12 and 13 November and involved a site run by an external service provider.

What is known

The attackers accessed the names and official contact information of employees at the ministry's Vienna headquarters and at Austrian diplomatic missions abroad. The ministry states that the breach has been contained and that no personal information of members of the public was compromised.

Much remains unclear. The hackers have not been identified, the method of access has not been disclosed, and it is not known whether any information was actually exfiltrated. The ministry declined to share technical details, citing security reasons, and said the incident has not been attributed to any actor. It has informed the national cybersecurity and data protection authorities.

The timing coincided with a global Microsoft service outage, which Microsoft attributed to a software bug and infrastructure failures. Austrian authorities have not established any link between the two events.

Why it matters for Saudi institutions

The case illustrates how a website managed by a third party can expose staff directory information of a government body. Even basic names and contact details can be useful for targeted phishing or social engineering. Regulated institutions in the Kingdom that rely on external providers for web or portal hosting may wish to confirm what staff data those environments hold and how incidents are escalated.

What to do now

1. Inventory websites and portals run by external providers and record which staff or customer data each one holds.
2. Confirm that third-party contracts require prompt incident notification, log access and containment support.
3. Reduce staff directory details published on public sites to what is operationally necessary.
4. Warn staff, especially those named in public directories, about targeted phishing and impersonation attempts.
5. Check that incident response plans cover third-party breaches and the notification duties to NCA and, where relevant, SDAIA or SAMA.