N-able confirms cyberattack behind Mail Assure and SpamExperts disruption



N-able says a single compromised web server caused the multi-day disruption of Mail Assure and SpamExperts Hosted Cloud. Mail filtering kept running, but the portal and API remain disabled while the investigation continues.

- The disruption began on November 16 and affected all regions; N-able first cited platform configuration and service dependencies.
- On November 18 the company confirmed a cyberattack, isolated to one web server where credentials stored on the platform may have been accessed.
- N-able reports no evidence that customer data was compromised; its investigation is ongoing.
- Mail flow and filtering were unaffected, but logging, mailbox synchronization, the portal and quarantine went offline.

> - Customer API tokens were revoked, OAuth tokens invalidated and local user passwords reset; portal and API access remain disabled.

N-able has confirmed that a cyberattack was behind a disruption of its Mail Assure and SpamExperts Hosted Cloud services that began on November 16 and lasted several days across all regions. The company initially attributed the problem to platform configuration and service dependencies, then confirmed the attack on November 18.

What happened

According to N-able, the incident was isolated to a single web server, where an unauthorized party may have been able to access certain credentials stored on the platform. Mail flow and filtering were not affected, but logging, mailbox synchronization, the management portal and quarantine were taken offline. The company says it has found no evidence that customer data was compromised.

Containment and current status

N-able took the affected server offline, rotated internal platform credentials, revoked existing customer API tokens, invalidated OAuth tokens and proactively reset passwords for local users. Inbound and outbound filtering are operating, but portal and API access remains disabled while the company works to restore them securely. The investigation continues. N-able states the incident is unrelated to its recent N-central incident.

Why it matters

Organizations in the Kingdom that use these services through a managed service provider or directly may find that integrations depending on API tokens or OAuth no longer work. Because credentials were potentially exposed, this is also a third-party risk event to be recorded and followed up, even though no customer data compromise has been identified so far. N-able says it has issued specific guidance depending on how customers access and configure the services, and will continue to provide updates.

What to do now

1. Confirm whether your organization or its managed service providers use Mail Assure or SpamExperts Hosted Cloud, and identify who administers them.
2. Follow the guidance N-able has issued to customers and check for its updates.
3. Identify integrations that rely on API tokens or OAuth with these services and plan to re-issue them once access is restored.
4. Review any credentials or passwords tied to the service, and rotate those reused elsewhere.
5. Log the event in the third-party risk register and ask the provider for investigation findings when available.
6. Watch the mail security gateway for delivery or filtering anomalies while the portal and quarantine are

unavailable.