TENZING™

more than managed hosting

RESPONDING TO

Technology firms were rocked by the discovery of an Open SSL Bug in early April. Many struggled to respond to the threat, mitigate the vulnerability and communicate clearly with clients. Tenzing's best in class security team and adherence to ITIL best practices allowed it to secure all vulnerable devices without any service disruptions - **up to two days before other service providers.**

Day One

12:17 ET

Discovery Phase Initiated

Upon hearing of the possible vulnerability Tenzing Security teams meet to discuss and begin the discovery phase.

13:24 ET

Urgent Incident Meeting

ITIL best practices guide Tenzing processes to ensure organized and thorough responses to security incidents. Preliminary discovery results and an incident response plan is developed.

13:33 ET

Initiate Major Incident Process

Security and Service Desk teams are well versed in company operations and are quick to organize remediation and action plans.

17:12 ET

Communicate with Clients

Details regarding the Heartbleed threat and action plan are posted on the Tenzing customer portal.

17:28 ET

Identify Vulnerable Devices

Tenzing Security team confirms list of vulnerable devices and patching commences.

21:23 ET

Email Notification

Notification is sent to all affected customers with details on vulnerability and action plan.

21:27 ET

Individual Communications Start

Service desk starts notifying potentially impacted customers by phone, ticket and email.

Day Two

00:23 ET

Notification Complete

Within 12 hours, all affected Tenzing clients have been individually notified of the threat and Tenzing's action plan.

02:53 ET

Patching Complete

Tenzing Service Desk complete patches on all vulnerable servers.

08:15 ET

Scan Complete

Tenzing Teams complete a thorough scan of all affected servers to ensure security.

13:00 ET

Less than **24 hours** after initiating its major incident process Tenzing Security & Operations teams declare **all known vulnerable systems patched** with **no service disruptions.**