servicenow

5 Best Practices

for protecting your company from outages caused by TLS certificates

Certificate management mistakes have costly impacts on the business. Sometimes, expired certificates bring down services, and other times, they open critical applications to security vulnerabilities. In today's digital environment, there's no safe business without working certificates. Here are five best practices to ensure your company stays out of trouble caused by certificate issues.

1 Define policy with stakeholders before requesting certificates

Revisit current and upcoming policies with security, governance, IT support, and PKI teams. Set certification requirements with Certificate Authority providers according to those policies. With this approach, your company can avoid unwanted security vulnerabilities.

2 Automate inventory of certificates at all times

Although this is a pretty common best practice, it's often missed. Make sure all deployed certificates are discovered. But also make sure all users, networks, servers, and sites have up-to-date certificates. You can automate the discovery of certificates via port scans, entry point URL scans, and Certificate Authority. Having inventory in one place helps with the documentation process for compliance and auditing reasons as well.

3 Digitize request fulfillment process

Requesting new certificates and renewing can become a daunting approval process, typically supported by a service management team. It's critical to know the owners, applications, devices, and other information useful to track the use of these certificates. Even more critical is to decommission certificates when any related entities, such as the above list, are removed. This process is not scalable for thousands of employees and hundreds and thousands of certificates. Hence, create a digital workflow to do it properly that understands IT and employee workflows.

4 Create certificate renewal tasks 60 days before the expiration

As a digital business, you can't wait to renew certificates when they expire; it's already too late. Instead, a platform approach ensures that there's an automated task generated well-in-advance of expiration. Renewal tasks should have a list of actions if not addressed in time such as create an incident for an outage if certificates are not renewed 48 hours before expiration. These renewal tasks should be deployable for certificates in any hybrid and cloud-native environments such as Google, AWS, and Azure; these can be done with various spokes.

5 Use intelligent alerting to validate certs, keeping your sites away from outages

Browsers are continually revisiting certificate validity timelines to increase security. Understand the potential impact to services and users due to the browser's changing trust policy. You should consider an AIOps-based workflow to create automated alerts before expiration and continuously scan the certificates, infrastructure, applications, and services to create tasks to avoid outages proactively.

Key takeaway

- Reduce the risk of exposure while also increasing the productivity of your PKI teams.
- Eliminate outages due to expired certificates.
- Get visibility across all the certificates that are issued and installed across the infrastructure, applications, and services.

For more information, get the Guide: **TLS Certificate Management - ITOM Visibility & ITOM Product Management**