August 14, 2018 | Issue 5

OCIO | Office of the Chief Information Officer

TOPICS:
Backup & Retention
Logging & Monitoring

The importance of retaining backups cannot be over emphasised. Think about the loss of productivity if backups are not conducted and retention period is not defined to fall within the organization's risk tolerance and cost justification.
A policy should be in place which outlines the frequency of backups, the retention period, and a schedule for testing backups. Management to ensure that backups are conducted and tested regularly.

Logging of system activity is necessary as it provides an audit trail to know who did what and when. Logging should be turned on by default on all critical systems and retention of logs should be based on a retention policy. Proactive monitoring is necessary for timely flagging and responding to an incident. Monitoring can be done manually by generating system reports, which should be reviewed regularly. For systems that have large number of users, a Security Information and Events Management (SIEM) solution should be implemented. (Note SIEM should be configured according to industry best practices).

A security breach is not a question of "if" it happens but "when" it happens. Therefore, conducting regular backups and ensuring offline backups are in place will be beneficial to an organization most especially in a situation when infected by a ransomware attack. Activities relating to backup (i.e. frequency of backups and testing) should be defined in a policy and executed. A Backup and Retention policy should be reviewed annually.

Considering the threat landscape today, centralized logging, correlation and alerting is extremely necessary for a networked organization. A software solution such as a SIEM would be beneficial. However, before implementing a SIEM, ensure logging capability is robust, so that logs collected can be ingested by a SIEM. Activities relating to Logging and Monitoring should also be defined in a policy.

KEY EVENTS

- **Monthly Defensible Security Conference Call: September 5, 2018**
  At the next conference call, we will discuss Backup & Retention, Logging & Monitoring, and Logical Access control areas of the DefSec framework.

- **BC Security Day: Nov 7, 2018**
  The Province organizes and hosts two "Security Day" events each year (Spring and Fall), free of charge. Representatives from the broader public sector, school districts, post secondary institutions, municipalities, and crown corporations are encouraged to attend. Visit the Security Day website for more information.

- **20th Privacy and Security Conference: Feb 2019**
  Held in Victoria, British Columbia, Canada this conference is a must attend. This three-day conference, is recognized as one of the top tier events in North America. Anyone working in the information privacy and security fields will benefit from the speakers, discussions, and networking at the conference. The conference draws an international audience of some 1,000 delegates with an interest in cutting edge policy, programs, law, research, and technologies aimed at the protection of privacy and security.

For more information visit: www.gov.bc.ca/defensible-security