March 12, 2019 | Issue # 19

Information Security

TOPIC: Defence in-depth for endpoints and networks

Endpoint devices include mobile devices, workstations, servers and IoT devices. These devices should be connected to a network via a secure channel (e.g. Virtual Private Network "VPN") to ensure that data is not intercepted when it is retrieved by end-users.

Endpoint devices must also have adequate security controls, such as encryption, virus protection, and firewalls, to protect both data in transit and data at rest, which will be beneficial in situations where devices are stolen or lost.

The Defensible Security objectives outlines a number of controls that should be in place to secure endpoints. It mandates that endpoint devices should be hardened, meaning that out-of-the-box/default configurations should not be used when a device is connected to a network. Endpoint devices should be configured based on industry standards and unnecessary services and insecure protocols should be disabled.

UPCOMING SECURITY EVENTS:

- **The last Conference Call in this series will be on: March 27, 2019**
  At the last conference call, 2 control areas of Defensible Security will be discussed; Defense in Depth on Endpoints & Networks and Vulnerability Management & Patching.

- **BC Security Day: June 13, 2019**
  The Province organizes two "Security Day" events annually, admission is free of charge and you can either attend in-person or via webcast. At the event, experts in the field of security present and discuss topics pertaining to advancement in technology and security implications. Join us for the 2019 spring Security Day and learn about "Smart Cities"; check our website for more information: http://www.gov.bc.ca/securityday.