ISOLATING WEB-FACING APPLICATIONS

FEBRUARY 2022

ITSAP.10.099

Web facing-applications come in various forms, and you probably use them on work and personal devices. If proper security measures are not built into these services, they are vulnerable to data leaks and other security issues.

A web-facing application is any program that can be accessed over the Internet and that uses web technology and browsers to perform tasks. Examples include email services, word processors, online file converters, and calendars. The data you enter on these applications is stored in the cloud, making it easily accessible when you need it but also putting it at risk to cyber attacks.

COMMON THREATS

Threat actors may attack web-facing applications to expose information, steal credentials and identities, carry out denial of service attacks, or damage the application. Threat actors may use these applications as an entry point to damage other systems that are important to you and your organization. Some common cyber threats include:

- **Cross-site scripting (XSS):** A threat actor injects malicious scripting into a trusted web application. A user's device becomes infected with malicious code that gives the actor access to sensitive information saved by the application.
- **Structured query language (SQL) injection:** A threat actor runs a malicious SQL statement where a user's input is requested (e.g. username or password text field). This gives the actor the ability to manipulate sensitive data in your database.
- **Command injection flaws:** A threat actor takes control of the application by relaying malicious code through the application to another system.
- **Buffer overflows:** A threat actor crashes or takes over an application by sending exceedingly large amounts of data to the application.
- **Brute force attacks:** A threat actor uses a trial-and-error method to obtain authentication information (e.g. a password). If successful, they then have access to a user's account and any sensitive information associated with the account (e.g. stored credit card information).
- **Path traversal:** A threat actor accesses files and directories stored outside the file system's root folder. They can access source code, user credentials, databases, or configuration and critical system files.

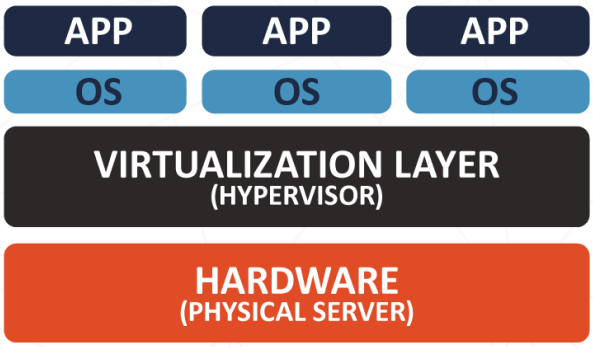
AWARENESS SERIES

Cat. No. D97-1/10-099-2022E-PDF
ISBN 978-0-660-42178-0

PROTECTING YOUR ORGANIZATION'S WEB-FACING APPLICATIONS

We strongly recommend isolating web-facing applications to reduce the risk of backend networks and information systems becoming compromised. Upon doing so, if an isolated web-facing application is infected or compromised, the exploit is contained and cannot spread (i.e. the application is sandboxed).

A common way to isolate web-facing applications is through virtualization. Desktop virtualization creates a simulated, equivalent virtual resource or virtual resources (e.g. server, desktop, operating system, storage, network) of a computer system.



VIRTUAL ARCHITECTURE

This simulation operates in an isolated environment and separates a user's applications from other programs or the operating system on which they run. Although the applications still open and run as expected, they are not installed on a user's computer.

For more details on isolating your web-facing applications, refer to *ITSAP.70.011 Virtualizing Your Infrastructure* on the Cyber Centre website.

In addition to virtualization, your organization should consider taking the following actions:

- **Scanning and testing applications for vulnerabilities**
  - Vulnerabilities are flaws or weaknesses in an information system or its environment that threat actors can exploit to harm your organization's assets or operations.
- **Updating and patching applications**
  - Updates and patches improve the security and enhance the functionality of the application.
- **Implementing an application allow list**
  - An application allow list identifies the applications that are allowed to run on a computer system.
- **Implementing web application firewalls**
  - There are two different types of application firewalls: network-based application firewalls and host-based application firewalls. Both provide a barrier which protects local system resources from being accessed from the outside.
- **Applying the principle of least privilege**
  - Adhering to the principle of least privilege, you grant individuals only the set of privileges that they need to do their jobs. This principle limits the damage caused by the accidental, incorrect, or unauthorized use of an information system.

REMEMBER

Isolating web-facing applications limits the damage that threat actors can cause to your organization's networks, information systems, and devices. Virtualization is a common and effective way to isolate web-facing applications.

Isolating web-facing applications is just one way of improving cyber security. To better protect your organization against cyber threats, you should review and implement all the actions recommended in *Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* (ITSM.10.089).

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**