a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #19
Internet-Facing Systems and Services

Introduction

1. UBC Systems and services that are Internet-facing (i.e. visible or accessible from the Internet) are prime targets for exploitation. Without adequate security, these systems and services provide an avenue for malicious activity such as theft of UBC Electronic Information or the denial of service to UBC resources.
2. This document defines minimum standards to be followed by University IT Support Staff for the security architecture, protected network protocols, hardening/patching and monitoring/logging of UBC's Internet-facing systems and services to ensure they are adequately protected. This standard focusses on Web Servers because these are primary targets for exploitation and therefore pose the highest risk to the University. Servers that are not internet-facing, such as intranet servers, should also follow this standard, wherever feasible.
3. The Chief Information Officer has issued this document under the authority of Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

Security Architecture Requirements

4. Ideally, web, application and database functions should be hosted on separate servers; however, it is acceptable to host all of these functions on the same server in the following circumstances:
    a. Confidential Information is not being processed through these servers; and/or
    b. hosting the functions on separate servers would not be technically feasible or would cause unreasonable business disruption (e.g. render the application unusable or unsupportable).
5. If functions are hosted on the same server, compensating controls must be implemented to commensurate with the risk, such as:
    a. web application (layer 7) firewall;
    b. file integrity monitoring;
    c. Intrusion Detection Systems/Intrusion Prevention Systems; and
    d. log monitoring (e.g. SIEM).
6. When web, application and database functions are hosted on separate servers, Web Servers are permitted to communicate with Application Servers but not with Database Servers.
7. All Internet-facing servers must be placed in a Demilitarized Zone (DMZ) configured as follows:
    a. the DMZ must contain all Web Servers;
    b. the DMZ may only contain Application Servers if they are combined with Web Servers;
    c. the DMZ must not contain Database Servers that store or process Confidential Information;
    d. a firewall must be in place between the DMZ and the Internet as well as between the DMZ and the UBC internal network;
    e. wherever possible the DMZ should be protected from the Internet by web application firewalls, as they are better equipped to protect web applications from threats;
    f. firewalls must use ingress filtering at a minimum, and must also use egress filtering if the firewall is used to protect Confidential Information; and
    g. firewalls must use access rules that restrict traffic to only the minimum necessary to conduct University Business; access rules must not be wide-open allowing any source to connect to any destination, as this defeats the security of the firewall.
8. Access to all Confidential and Sensitive Information on servers must be authorized and limited based on the User's role, following the principle of least privilege.

Network Protocol Requirements for Confidential or Sensitive Information

9. Secure transmission of Confidential or Sensitive Information must comply with the following requirements:

a. any form, application or service that requires some type of authentication, or that is used to collect or transmit information from User to server or between servers, must be encrypted using HTTPS with TLS version 1.0 at a minimum, TLS version 1.1 is preferred (or the equivalent, for non-web-based applications; and
b. information transmitted via SSH must be encrypted using a minimum of AES-256 bit encryption with mutual authentication between the server and User.

10. Users frequently access desktops, laptops and servers remotely. Remote access covers a broad range of technologies, protocols and solutions (e.g. RDP, SSH, VNC, VDI, terminal services, etc.). Remote access transmissions must comply with the following requirements:
    a. remote access servers (e.g. terminal server, VDI, Remote Access Gateways, etc.) must be located in the DMZ and use strong encryption for server-to-User transmissions, e.g. RDP with Network Level Authentication, SSH with AES-256 bit encryption, etc.;
    b. host desktops, laptops or servers not located in the DMZ should only be remotely accessed via a Remote Access Gateway, VPN or SSH; and
    c. VPN connections must be encrypted and restricted at both ends to the minimum number of systems necessary; split tunneling must not be enabled.
11. Servers running other internet-facing protocols (e.g. Telnet, FTP, etc.) must be located in the DMZ and must encrypt transmissions of Confidential or Sensitive Information.

Additional Requirements for Merchant Systems

12. University IT Support staff must configure remote access technologies, used in Merchant Systems, to automatically disconnect User sessions after a specific period of inactivity. 30 minutes is recommended.

Hardening and Patching Requirements

13. Servers must be hardened, patched and scanned in accordance with the Vulnerability Management standard.

Logging and Monitoring Requirements

14. Servers must be logged and monitored in accordance with the Logging and Monitoring of UBC Systems standard.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Logging and Monitoring of UBC Systems standard

Vulnerability Management standard