18.4. Intrusion Detection and Prevention

Objective

18.4.1. An intrusion detection and prevention strategy is implemented for systems in order to respond promptly to incidents and preserve availability, confidentiality and integrity of systems.

Context

Scope

18.4.2. This section covers information relating to detection and prevention of malicious code propagating through networks as well as the detection and prevention of unusual or malicious activities.

Methods of infections or delivery

18.4.3. Malicious code can spread through a system from a number of sources including:

- files containing macro viruses or worms;
- email attachments and Web downloads with malicious active content;
- executable code in the form of applications;
- security weaknesses in a system or network;
- security weaknesses in an application;
- contact with an infected system or media; or
- deliberate introduction of malicious code.

18.4.4. The speed at which malicious code can spread through a system presents significant challenges and an important part of any defensive strategy is to contain the attack and limit damage.

References

18.4.5.

Reference	Title	Publisher	Source
ISO/IEC 27001:2013	**Information technology — Security techniques — Information security management systems — Requirements, A.15.3, Information Systems Audit Considerations**	ISO	https://www.iso.org/standard/54534.html
HB 171:2003	**Guidelines for the Management of Information Technology Evidence**	Standards NZ	https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB171.PDF [PDF, 350 KB]

References - Endpoint Security

18.4.6.

Reference	Title	Publisher	Source
	Transport Layer Protection Cheat Sheet	OWASP	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
RFC 5246	**The Transport Layer Security (TLS) Protocol Version 1.2**	IETF	https://datatracker.ietf.org/doc/html/rfc5246
RFC 8446	**The Transport Layer Security (TLS) Protocol Version 1.3**	IETF	https://datatracker.ietf.org/doc/html/rfc8446
RFC 7525	**Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)**	IETF	https://datatracker.ietf.org/doc/html/rfc7525
RFC 6749	**The OAuth 2.0 Authorization Framework**	IETF	https://datatracker.ietf.org/doc/html/rfc6749
	OpenID Connect	OpenID Foundation	https://openid.net/connect/
	New Zealand Security Assertion Messaging Standard	NZ Government Department of internal affairs	New Zealand Security Assertion Messaging Standard | NZ Digital government

Rationale & Controls

Intrusion Detection and Prevention strategy (IDS/IPS)

18.4.7.R.01. **Rationale**

An IDS/IPS when configured correctly, kept up to date and supported by appropriate processes, can be an effective way of identifying, responding to and containing known attack types, specific attack profiles or anomalous or suspicious network activities.

18.4.7.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:3802]

Agencies MUST develop, implement and maintain an intrusion detection strategy that includes:

- appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary;
- the audit analysis of event logs, including IDS/IPS logs;
- a periodic audit of intrusion detection procedures;
- information security awareness and training programs;
- a documented Incident Response Plans (IRP); and
- provide the capability to detect information security incidents and attempted network intrusions on gateways and provide real-time alerts.

18.4.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3803]

Agencies SHOULD develop, implement and maintain an intrusion detection strategy that includes:

- appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary;
- the audit analysis of event logs, including IDS/IPS logs;
- a periodic audit of intrusion detection procedures;
- information security awareness and training programs; and
- a documented IRP.

18.4.7.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3804]

Agencies SHOULD ensure sufficient resources are provided for the maintenance and monitoring of IDS/IPS.

IDS/IPSs on gateways

18.4.8.R.01. **Rationale**

If the firewall is configured to block all traffic on a particular range of port numbers, then the IDS should inspect traffic for these port numbers and alert if they are detected.

18.4.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3807]

Agencies SHOULD deploy IDS/IPSs in all gateways between the agency's networks and unsecure public networks or BYOD wireless networks.

18.4.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3808]

Agencies SHOULD deploy IDS/IPSs at all gateways between the agency's networks and any network not managed by the agency.

18.4.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3809]

Agencies SHOULD locate IDS/IPSs within the gateway environment, immediately inside the outermost firewall.

IDS/IPS Maintenance

18.4.9.R.01. **Rationale**

When signature-based intrusion detection is used, the effectiveness of the IDS/IPS will degrade over time as new intrusion methods are developed. It is for this reason that IDS/IPS systems and signatures need to be up to date to identify the latest intrusion detection methods.

18.4.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3815]

Agencies MUST select IDS / IPS that monitor uncharacteristic and suspicious activities.

18.4.9.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3843]

When signature-based intrusion detection is used, agencies MUST keep the signatures and system patching up to date.

Malicious code counter-measures

18.4.10.R.01. **Rationale**

Implementing policies and procedures for preventing and dealing with malicious code outbreaks that enables agencies to provide consistent incident response, as well as giving clear directions to system users on how to respond to an information security incident.

18.4.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3851]

Agencies MUST:

- develop and maintain a set of policies and procedures covering how to:
  - minimise the likelihood of malicious code being introduced into a system;
  - prevent all unauthorised code from executing on an agency network;
  - detect any malicious code installed on a system;
- make their system users aware of the agency's policies and procedures; and
- ensure that all instances of detected malicious code outbreaks are handled according to established procedures.

Configuring the IDS/IPS

18.4.11.R.01. **Rationale**

Generating alerts for any information flows that contravene any rule within the firewall rule set will assist security personnel in identifying and reporting to any possible breaches of agency systems.

18.4.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3857]

In addition to agency defined configuration requirements, agencies SHOULD ensure that IDS/IPSs located inside a firewall are configured to generate a log entry, and an alert, for any information flows that contravene any rule within the firewall rule set.

18.4.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3859]

Agencies SHOULD test IDS/IPSs rule sets prior to implementation to ensure that they perform as expected.

18.4.11.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3864]

If a firewall is configured to block all traffic on a particular range of port numbers, the IDP/IPSs SHOULD inspect traffic for these port numbers and generate an alert if they are detected.

Event management and correlation

18.4.12.R.01.

Rationale

Deploying tools to manage correlation of suspicious events or events of interest across all agency networks will assist in identifying suspicious patterns in information flows throughout the agency.

18.4.12.R.02. **Rationale**

The history of events is important in this analysis and should be accommodated in any archiving decisions.

18.4.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3875]

Agencies SHOULD deploy tools for:

- the management and archive of security event information; and
- the correlation of suspicious events or events of interest across all agency networks.

Host-based IDS/IPSs

18.4.13.R.01. **Rationale**

Host-based IDS/IPS use behaviour-based detection schemes and can therefore assist in the detection of previously unidentified anomalous and suspicious activities such as:

- process injection;
- keystroke logging;
- driver loading;
- library additions or supercessions;
- call hooking.

They may also identify new malicious code. It should be noted that some anti-virus and similar security products are evolving into converged endpoint security products that incorporate HIDS/HIPS.

18.4.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3886]

Agencies SHOULD install host-based IDS/IPSs on authentication, DNS, email, Web and other high value servers.

Active content blocking

18.4.14.R.01. **Rationale**

Filtering unnecessary content and disabling unwanted functionality reduces the number of possible entry points that an attacker can exploit.

18.4.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3892]

Agencies SHOULD use:

- filters to block unwanted content and exploits against applications that cannot be patched;
- settings within the applications to disable unwanted functionality; and
- digital signatures to restrict active content to trusted sources only.