ISO/IEC 27039:2015 — Information technology — Security techniques — **Selection, deployment and operation of intrusion detection and prevention systems (IDPS)** *(first edition)*

Abstract

"ISO/IEC 27039:2015 provides guidelines to assist organisations in preparing to deploy intrusion detection and prevention systems (IDPS). In particular, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which these guidelines are derived."

[Source: ISO/IEC 27039:2015]

Introduction

Intrusion **D**etection **S**ystems are largely automated systems for identifying attacks on and intrusions into a network or system by hackers and raising the alarm. **I**ntrusion **P**revention **S**ystems take the automation a step further by automatically responding to certain types of identified attack, for example by closing off specific network ports through a firewall to block identified hacker traffic. IDPS refers to either type.

Scope and purpose

The scope states "This International Standard provides guidelines to assist organisations in preparing to deploy Intrusion Detection Prevention System (IDPS). In particular, it addresses the selection, deployment and operations of IDPS. It also provides background information from which these guidelines are derived."

Well designed, deployed, configured, managed and operated IDPS are valuable in several respects, for example:

- Automation leverages scarce security engineers who would otherwise have to monitor, analyse and

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

respond to network security incidents as best they could;

- Automation tends to speed-up identification and response to attacks, particularly common types of attack that can be identified unambiguously through unique attack signatures;
- They give additional assurance to management that security issues on the networks and networked systems are being identified and mitigated.

The standard is, in effect, an ISPS implementation guide and advisory.

Structure

Three main sections comprise the bulk of the standard's ~50 pages:

- Selection of IDPS - various IDPS types, complementary tools *etc*. to consider (in some detail, expanded still further in the annex);
- Deployment of IDPS;
- IDPS operations.

Status of the standard

The *first* edition was published in **2015**, "revising and canceling" (*i.e.* replacing) ISO/IEC 18043:2006.

A technical corrigendum in 2016 corrected the title of the published standard, introducing *"and prevention"* that somehow got lost.

The standard was confirmed unchanged in 2020.

Personal comments

I had hoped the standard would mention, in addition to the network security risks that they are meant to address, various information risks and issues associated with or introduced by the IDPS themselves, such as:

- They are technologically advanced and complex, making them difficult to configure, deploy and use effectively, hence there is a risk that they may be incorrectly configured, deployed or used in practice, with various consequences on the organisation and other systems. Furthermore, they probably introduce additional technical security vulnerabilities into the very networks and/or systems they are supposed to protect;
- They may adversely affect network traffic, restricting legitimate traffic and hence normal use of the network and systems, as well as hacking traffic;
- They are not 100% capable, meaning that certain types or modes of attack (particularly novel ones) may not be reliably identified and hence blocked, potentially creating a false sense of security (inappropriate assurance);
- They can only detect and react to available information, making them blind and deaf to attacks that bypass the networks and systems being monitored (including, for examples, social engineering and physical intrusion attacks);
- They usually require network bandwidth, processing and storage capacity for their own operations and record-keeping, and require hooks into the networks and systems being monitored and/or controlled, impinging upon normal use;
- They are complicated to configure and manage for best effect, requiring the involvement of competent security engineers who, potentially at least, may themselves be hackers;
- They require privileged access to network traffic, network devices and/or systems, and could potentially be misused as a vector or mechanism to compromise them.

However, it does not ...

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799