ISO/IEC 27035-3:2020 (E)

Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Overview

5.1 General
5.2 Structure of this document

6 Common types of attacks

7 Incident detection operations

7.1 Point of contact
7.2 Monitoring and detection
7.3 Common ways detection is performed
7.3.1 Monitoring public sources to look for potential reports (and threats)
7.3.2 Validation of external source data
7.3.3 Proactive detection
7.3.4 Reactive methods

8 Incident notification operations

8.1 Overview
8.2 Immediate incident notification
8.2.1 Incident reporting forms
8.2.2 Critical information that incident reports should (ideally) contain
8.2.3 Methods to receive reports
8.2.4 Considerations for escalation
8.3 PoC structure
8.3.1 Incident response operation notification if a single PoC exists
8.3.2 Incident response operation notification if multiple PoCs exist

9 Incident triage operations

9.1 Overview
9.2 How triage is conducted

10 Incident analysis operations

10.1 Overview
10.2 Purpose of analysis
10.3 Intra-incident analysis
10.4 Inter-incident analysis
10.5 Analysis tools
10.6 Storing evidence and analysis results

11 Incident containment, eradication and recovery operations

11.1 Overview
11.2 Conducting the response for containment, eradication and recovery

11.2.1 Containment description
11.2.2 Containment goals
11.2.3 Common containment strategies
11.2.4 Issues associated with containment
11.3 Eradication
11.3.1 Eradication description
11.3.2 Eradication strategies
11.3.3 Issues associated with eradication
11.4 Recovery
11.4.1 Recovery description
11.4.2 Recovery strategies
11.4.3 Issues associated with recovery

12 Incident reporting operations

12.1 Overview
12.2 How to establish reporting
12.3 How to establish external reporting, if required
12.4 Information sharing
12.5 Other reporting considerations
12.6 Types of reports
12.7 Methods for storing reports and analysts' knowledge

Annex A (informative) Example of the incident criteria based on information security events and incidents

A.1 Information security events and incidents
A.1.1 Fundamental incident criteria
A.1.2 Impacts according to each incident type
A.1.3 Damage scale of incidents
A.1.4 Importance of the information/system
A.2 Incident alarm level

Page count: 31