ZUORA

Security Incident Response Policy

Overview

This guide outlines the process for detecting, analyzing, and responding to cybersecurity incidents that may impact Zuora's systems and data. It details specific steps to take when encountering various security threats.

Types of Security Incidents:

- Malicious software designed to harm systems (viruses, worms, trojan horses)
- Misuse of computer accounts or unauthorized access attempts
- Data Security Incidents:
    - Disclosure of sensitive information like cardholder data or internal systems
    - Breaches within Zuora-developed or utilized services (applications, APIs, websites)
- Unauthorized access points connected to the Zuora network
- Violations of Zuora's Acceptable Use Policy
- Missing key security safeguards

Objective

The objective of Zuora’s Security Incident Response Policy is to serve as a formal document outlining the organization's established procedures for efficiently detecting, containing, eradicating, and recovering from security incidents. Its primary objective is to safeguard the organization's critical assets, data, and overall operational integrity.

Definitions

- **Information Resources**: Any and all computer printouts, online display devices, storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, servers, personal computers, notebook computers, handheld computers, personal digital assistants (PDA), telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- **Cyber Security Incident Response Team (CSIRT):** Personnel responsible for coordinating the response to cyber security incidents in Zuora.
- **Virus:** A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.
- **Worm:** A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.
- **Trojan Horse:** Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent looking piece of software, such as a game or graphics

program. Victims may receive a Trojan horse program by email or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

- **Security Breach Incident:** In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.
- **Key Security Control Missing:** Key Security Controls refer to but not limited to: HIDS, NIDS, WAF, Firewall or central log server would trigger this incident.

Audience

Zuora Incident Response Policy applies equally to all individuals that use any Zuora Information Resources.

Roles

Chief Security Information Officer (CISO): The designation of an incident response manager is intended to establish clear accountability for setting policy for incident response activities, provide for greater coordination of Zuora's incident response activities, and ensure greater visibility of such activities within and between Zuora, its customers and law enforcement agencies. The CISO has been given the authority and the accountability by Zuora management to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the Zuora. This individual is responsible to executive management for administering the information security functions within Zuora and shall be the internal and external point of contact for all information security matters. The CISO is required to be active in industry organizations and standards groups focused on information security. It is the

responsibility of the CISO to incorporate industry developments into Zuora's security and incident response programs.

Cyber Security Incident Response Team (CSIRT): In addition to the CISO, Zuora has established an CSIRT team of senior executives of the organization including Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Product Officer (CPO), General Counsel, Senior VP R&D Operations, SVP of Customer Success, SVP of Engineering, and VP Technical Operations. Each CSIRT member is required to name a surrogate. All CSIRT members will be informed of confirmed security incidents.

CSIRT Responsibilities

The CSIRT provides accelerated problem notification, damage control, and problem resolution. CSIRT members are granted the authority to fulfill their responsibilities.

CSIRT members:

- Investigate, verify, and remedy critical incidents
- Manage communication with key clients during incident troubleshooting or service disruption
- Ensure that incident evidence is safeguarded for forensic investigation
- Conduct and document forensic investigations and post incident evaluations
- Coordinate with Media, Security, Legal, and external law enforcement as needed
- Maintain and update policy and procedures as required

Management Responsibilities

Zuora Management:

- Organize and maintain an in-house CSIRT
- Prepare, update, revise and regularly test the incident response plan

- Establish, maintain, and periodically test an incident notification system that enables personnel to report suspected incidents promptly to the appropriate staff
- Provide training (and periodic retraining) for personnel who are expected to follow any phase of the procedure, including those employees who are not on the CSIRT
- Grant appropriate authority to CSIRT members to fulfill their responsibilities

Incident Response Process

Due to the high risk associated with security incidents, all suspected security incidents will be classified as P0 or P1 and follow an escalated response process.

Incident Identification/Alert

The incident response process is started when Zuora Support or Zuora Security notes a potential incident. Incident discovery can occur in many ways including:

- Email alerts from system monitoring
- Customer notifications of suspected activity
- Routine inspection of Zuora systems

Investigate

Zuora will perform a thorough investigation; the Zuora's Security team will log all potential security incidents for investigation. If the security team determines the activity as suspicious, the team will contact the process owner that is responsible for the activity reported.

If the incident is determined to be malicious the Security team will notify the appropriate CSIRT members immediately regarding the incident and the assessment of its impact.

Respond

Immediately contain and limit the exposure: Zuora will prevent further loss of data by conducting a thorough investigation of the confirmed compromise of information.

To minimize evidence tampering and aid investigation, the Cyber Security Incident Response Team (CSIRT) will prioritize isolating compromised systems from the network (e.g., unplugging cables) without powering them down. They will avoid accessing or altering these systems, and meticulously document all their actions.

If using Wi-Fi, the CSIRT will secure the network by changing the SSID on access points and other connected devices, except for potentially compromised ones. Finally, they will alert TechOps to heighten monitoring of systems containing sensitive data.

Alert all necessary parties immediately**:** If an incident is suspected or confirmed compromise of cardholder data the CSIRT must immediately notify the payment brands affected.

Zuora's incident response procedure has been designed to meet the payment brands incident response procedures. In the event that cardholder data is suspected to be accessed, the CSIRT will contact the brands affected.

If the incident is related to financial fraud, Zuora is required to contact the local office of the United States Secret Service or FBI, Zuora legal will determine the correct notification.

Zuora is legally obligated to notify customers even if they can confirm cardholder data wasn't accessed, but personally identifiable information (PII) was compromised. The VP of Support will lead the customer notification process.

Retrospective

The CSIRT will produce an after-action evaluation, assessing the following areas of concern:

- IRT Performance
- Policies and Procedures
- System Functioning
- Lessons learned from the incident

The results of the postmortem will be used to evaluate this Incident Response Procedure and update it as necessary to improve the overall process.

Testing

Testing of the IRP shall be conducted at least annually. The IRP test may include a mock security event conducted by a member of the Security team and additional departments as appropriate, not on call to respond to a security event. The security test will include formal documentation of how the security event will be executed.

Note, this test does not have to be a blind test and all members responding to the event can be aware that the event is only a test. In any case the entire IRP will be executed as if it were a real security breach.

Note: As the IRP mandates a post-incident “lessons learned” session meant to improve the IRP, any incident response conducted during a year is considered a process test and satisfies the annual test requirement.