Wrocław University of Science and Technology

Faculty of Information and Communication Technology

Incident Response Plan for a large scale e-lottery system

Adrian Cinal	247312
Alisa Pogodaeva	269689
Oliwer Sobolewski	247291
Gabriel Wechta	250111

Supervisor:
Wojciech Wodo, PhD

April 21, 2022

Report
Compliance and Operational Security

Contents

0 | Introduction

The following document constitutes an Incident Response Plan (IRP) for a large scale e-lottery system - Wide Open Drawing Olympics (WODO). Below a brief overview of the system's infrastructure is provided while a more in-depth analysis of the organization's assets and how they can be compromised is presented in the later chapters, i.e. in the IRP proper.

WODO is a nationwide lottery system with number drawings occurring precisely every 15 minutes, where each draw is comprised of 5 numbers between 1 and 25 (without repetitions). The strict timing requirements preclude the possibility of user participation in the drawing process itself and/or winner identification process. For this reason, people's trust in the lottery's fairness is of utmost importance. In order to ensure continuous upholding of the lottery's reputation, fault tolerance via extensive redundancy has been incorporated into the system's infrastructure at many levels. These measure have been taken to ensure high availability and reliability of the system.

Great financial risks are associated with running a lottery (or: "with great money, comes great responsibility"). Any vulnerability that is not properly patched and ends up being exploited by a malicious party can result in millions in damages. A lottery system is thus a particularly delicate system in terms of security, not necessarily because of the complexity of the system and difficulty in assuring soundness and robustness, but because of the astronomical cost of any failure to prevent an attack.

On top of the common CIA triad (Confidentiality, Integrity and Availability) the lottery system must provide exceptional levels of accountability to ensure users' trust. Trust is especially important in information systems that include exchanging money. If a person were to choose between two systems with a similar probability of winning, no matter how sophisticated or expensive the system is, they will choose one that they trust more. In this context trust may not stem from personal experience with the system but the reputation of the system. It is also important to note that the system that has once lost people's trust will be very unlikely to regain it. Because of this it is crucial to minimize the probability of the system's failure.

The core functionality of the lottery system is achieved with the help of a set of three computers: two generators (one redundant) and a verifier (see Figure 1). A generator generates pseudorandom lottery numbers and sends them to the verifier responsible for the numbers' validation, that later sends the numbers to the central computer responsible for publishing the winning numbers and searching for a match among the submitted coupons.

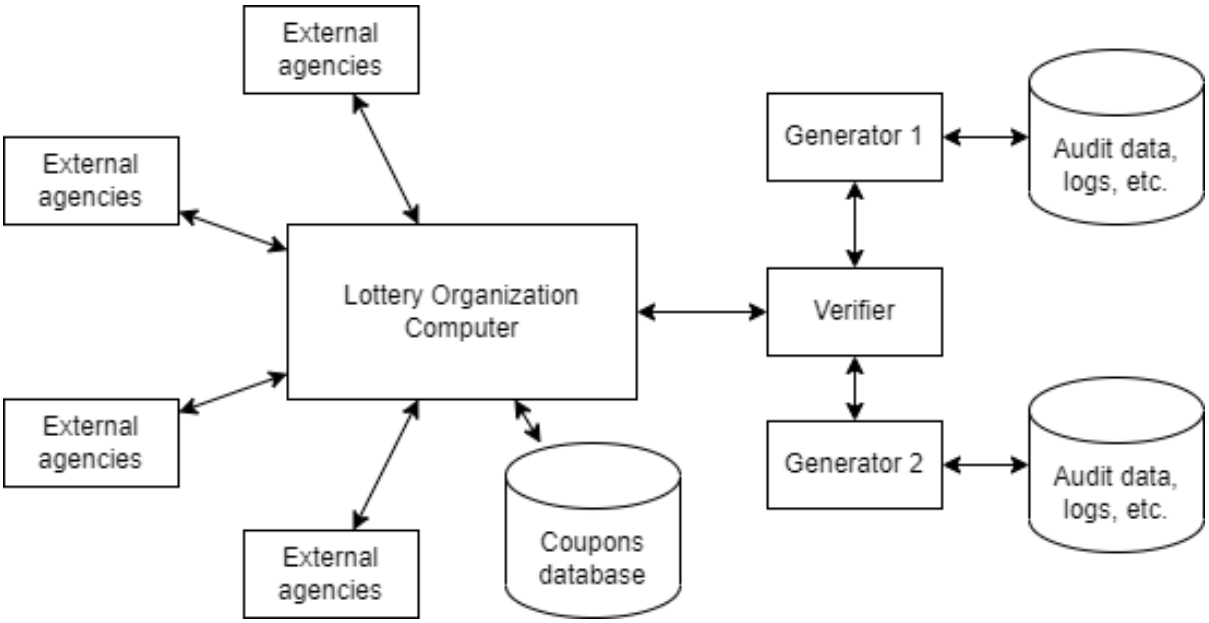

Figure 1: Infrastructure of the system

Arbitrary environmental events such as earthquakes or power grid failures should be also taken into account, although human capability to prepare for those is limited. Redundancies are still implemented, however, as far as power and network failures are concerned.

1 | Purpose and scope

> No matter how sophisticated or expensive an information system is, if people do not trust it, the system is bound to fail to deliver the services for which it was designed and built
>
> *E. Konstantinou, et.al,*
> *"Trust Engineering: From Requirements to System Design and Maintenance..."*

1.1 General information

The following Incident Response Plan (IRP) was developed for the Wide Open Drawing Olympics e-lottery system, herein referred to as WODO, and is classified as the confidential property of that entity.

Due to the sensitive nature of the information presented herein, the document is available only on a need-to-know basis, i.e. only to persons who play a direct role in the incident response and recovery process. These include management teams overseeing incident handling and incident response team members themselves.

Unless otherwise instructed, each plan recipient shall be provided with two copies of the plan, with one stored at the recipient's office and the other one at the recipient's home. If additional copies are needed, please contact Adrian Cinal at 018247312.

1.2 Scope

WODO recognizes and affirms the importance of people, processes, and technology to the corporation's operations and incident handling and recovery. It is thus the responsibility of all managers and other company employees to personally attend to safeguarding and keeping confidential all the corporate assets.

This plan establishes recommended procedures and processes needed to quickly recognize and respond to a computer security incident (defined in the next chapter). These processes shall be comprised of several steps that include, e.g. efficient and effective assessment of the situation, notification of the appropriate parties, as well as organization and necessary escalation of the company's activities and efforts based on the severity of the incident. The plan defines the requirements, strategies and proposed actions needed to respond to a computer security event from identification and classification as an incident to containment and subsequent eradication.

Finally, the plan also delineates business recovery efforts that should be made in the

aftermath of an incident to ensure continuation of operations and minimization of impact on the company as a whole.

1.3 Purpose

The document is designed to minimize operational and financial impacts of a computer security incident, and comes into force the moment when a local Computer Security Incident Manager (or a relevant deputy) determines that an incident has occurred.

The plan is in keeping with the trust engineering requirements specific to the WODO system and takes into account the trust life cycle at all stages of the incident response, from carefully delineating information disclosure procedures to formulating requirements pertaining to documenting the incident response and recovery process. It is expected that every recipient and user of the plan understands and values the importance of customer trust and company's reputation.

1.4 Planning scenarios

This plan was developed to respond to an event with the capability of rendering the WODO system unable to provide customer service, inaccessible to its personnel or otherwise compromised. The documents takes into account, but is not limited to, the following scenarios:

1. Power outage.
2. No access to buildings or floors.
3. Physical breach and trespassing.
4. Unauthorized access to the computer infrastructure.
5. Denial-of-service attack or other loss of data communication.
6. Data integrity compromise.

For any unprecedented incidents that are not explicitly mentioned in this document, one or more of the above scenarios can be adapted at the discretion of the local Computer Security Incident Manager.

The document makes the assumption that sufficient staff with adequate knowledge and expertise will be available to handle an incident and facilitate speedy recovery.

2 | Definitions

- **INFORMATION SECURITY (IS)** — The field of science and technology, covering a set of problems, related to ensuring the security of information objects spheres in the presence of threats. Protection of *Confidentiality*, *Integrity* and *Availability* of information is at the heart of information security. Those key concepts are usually referred to as the *CIA triad*.
- **EVENT** — Any identified occurrence in a system or network.
- **INCIDENT** — An *event* that actually or potentially violates the company's information security and the CIA triad.
- **THREAT** — Any circumstance or *event* with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via violation of the *CIA triad*. Threat can be also defined as the potential for a threat-source to successfully exploit a particular information system vulnerability.
- **WEAKNESS** — A type of mistake that, in proper conditions, could contribute to the introduction of *vulnerabilities* within system. This term applies to mistakes regardless of whether they occur in implementation, design, or other phases of a system lifecycle.
- **VULNERABILITY** — An occurrence of a *weakness* (or multiple weaknesses) within a system, in which the weakness can be used (*exploited*) by a malicious party to attack the system and violate the *IS*.
- **EXPLOIT** — A computer program, a piece of program code, or sequence of commands used by a malicious party to exploit system *vulnerabilities*, resulting in violation of the *IS*.
- **INCIDENT RESPONSE** — The mitigation of violations of security policies and recommended practices. Usually takes a form of structured set of actions aimed at establishing the details of the *incident*, minimizing the damage from the *incident* and preventing a recurrence of an information security *incident*.
- **ATTACK** — Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- **ATTACK SURFACE** — The set of points on the boundary of a system where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.
- **ATTACK VECTOR** — A specific path, method, or scenario that can be exploited to break into a system, thus compromising its *IS*.

- **TARGETED ATTACK** — An *attack* that targets a single person, company, or group. Those are especially dangerous as threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have sufficient resources to conduct their schemes over a long-term period.
- **DENIAL OF SERVICE (DOS) ATTACK** — An *attack* that results in prevention of authorized access to a system resource or delaying of time-critical system operations and functions. Time-critical may be milliseconds or it may be hours, depending upon the service provided.
- **APT (ADVANCED PERSISTENT THREAT)** — An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different *attack vectors* (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
- **KILL CHAIN** — A security concept which identifies the structure of an *attack* on a system. It consists of 7 phases:

  1. **Reconnaissance**: Intruder selects target, researches it, and attempts to identify *vulnerabilities* in the target network.
  2. **Weaponization**: Intruder creates remote access malware *exploit*, such as a virus or worm, tailored to one or more *vulnerabilities*.
  3. **Delivery**: Intruder transmits *exploit* to target (e.g., via e-mail attachments, websites or USB drives)
  4. **Exploitation**: *Exploit's* program code triggers, which takes action on target network to exploit *vulnerability*.
  5. **Installation**: Exploit installs access point (e.g., *"backdoor"*) usable by intruder.
  6. **Command and Control**: Exploit enables intruder to have "hands on the keyboard" persistent access to target network.
  7. **Actions on Objective**: Intruder takes action to achieve their goals, compromising the *IS*.

- **CIA TRIAD** — A security model designed to guide policies for *information security* within an organization. It consists of three core components:

  - **Confidentiality** measures protect information from unauthorized access and misuse.
  - **Integrity** measures protect information from unauthorized alteration. These measures provide assurance in the accuracy and completeness of data.
  - **Availability** measures protect timely and uninterrupted access to the system.

Violation of any of those components means violation of the entire CIA triad. Violation of the CIA triad in turn means that the *IS* has been compromised.

- **SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)** — A system that provides analysis of IS events originating from network devices and applications, in real time. One of capabilities of SIEM systems is the comparison of events with threat data streams.
- **IDS (INTRUSION DETECTION SYSTEM)** — A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
- **FIREWALL** — An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall).

3 | Roles and responsibilities

This section defines the roles and different functional areas of the organization's technology services, as well as their responsibilities within the CIRT.

At the time of the incident, the employees responsible for information security are required to take quick and accurate steps to minimize the damage from the incident and collect evidence for the criminal prosecution of attackers. To follow these steps correctly it is necessary to have instructions for responding to information security incidents created by information security experts.

If the employees of the departments responsible for information security do not know how to respond to an incident that has arisen and how to ensure the prompt collection of data necessary for conducting an investigation, the attacked organization will suffer significant losses. Errors in responding to information security incidents lead to the attacker achieving the goals of the attack and give them the opportunity to remove traces of their presence in the IS.

A Computer Security Incident Response Team highlights the following roles within the group:

3.1 Management

- **General manager** — sets the incident response policy, budget and staff formation. General manager is responsible for coordinating incident response among various stakeholders, mitigating damage, and notifying the CEO of an incident declaration.
- **Human Resources (HR) Representative** – manages any personnel-related issues that occur, especially if they involve insider theft.

3.2 Auxiliary staff

- **Legal advisor** — reviews incident response plans, policies, and procedures to ensure they comply with laws and federal guidelines, including the right to privacy.
- **Communications consultant** — presents complex technical issues in more understandable way for clients or media partners. The communications expert also provides feedback from clients to the technical experts.
- **Accountant** — establishes a budget and plans information security costs

3.3 Technical staff

- **Technical Director** — staffing, monitors team's functionality, analyzes architectural schemes of IT systems and subsystems, identifies possible risks of cyber attacks, formulates optimal requirements for their prevention and minimization, ensures prompt response to incidents; creates typical incident response scenarios.
- **Incident Manager** — information security incident process specialist (classification and assessment of an incident, formation of an IS incident response plan, control of its implementation, analysis and closure of an investigation, analysis and closure of an IS incident), has access to the register of information security events and the register of incidents for which this user is assigned responsibility.
- **Investigator** — collects and analyzes all evidence, determines root cause, directs the other security analysts, and implements rapid system and service recovery.
- **Public Relation Officer** — maintains communication channels with third parties involved in the incident handling, customers and stakeholders, media reporters etc.
- **Internal Point of Contact** — provides on-call support for internal employees; facilitates incident reporting for employees, provides information on the current status of the case etc.
- **External consultants** — hired when needed.

3.4 Incident Response Team Responsibilities

The main task of the incident response team is to perform incident response. The team's responsibilities also include:

- Intrusion detection.
- Distribution of alerts.
- Education and development. Education and absorption are resource multipliers - the more users and technicians know about detecting, reporting, and responding to incidents, the less effort an incident response team needs to have.
- Dissemination of information. Incident response teams often manage distribution efforts information about incidents in the organization, such as aggregating information related to incidents and effectively sharing this information with other organizations, as well as ensuring that relevant information is distributed throughout the enterprise.

4 | Incidents and escalation

A computer security incident is any event that violates the CIA triad of the WODO e-lottery system. Any attack on system's communication protocol is also considered as a security incident. Any violation of WODO's security policies, acceptable use policies, or standard computer security practices is an incident as well.

Due to the big risk of direct money loss in almost any adverse incident, detection mechanism is very sensitive. When incident is not fully detected yet, but there exists a suspicion that some incident took or is taking place IM is notified immediately. This kind of approach yields many false-positives but in the case of WODO e-lottery system spending resources on investigating false-positives is much better than omitting true-positives.

4.1 Incident levels

Following part of the document defines and clarifies incident levels with respect to severity and impact. Although, as mentioned before, Incident Response Team is informed about any potential incident. The main reason for defining severity level is to create hierarchy in case of many incidents taking place concurrently. Label, definition and some examples are provided below.

Critical level: Incident so serious that any prepared measure may not be sufficient to properly address threats raised by that incident. Also incidents that were not analyzed or to some measure foreseen are automatically given the highest priority. Or incidents that are direct threat for correctness of a lottery.

- Premature disclosure of lottery numbers
- Denial-of-service attacks preventing timely draws
- Physical breach by breaking and entering into, e.g. the generators' room
- Malicious insider with high privileges
- Introducing a winning ticket "after the fact" - so-called *postbetting*
- Compromise of randomness sources or PRNG's seeds

High level: Incident that requires instantaneous reaction, but does not constitute direct threat to correctness of WODO system, at least for foreseeable future. If the impact for predictable future is not known the incident should not be classified as high but as critical.

- Leak of knowledge about insights of the e-lottery system

- Unauthorized access to users' information
- Malicious insider with low privileges

Low level: Incident which does not represent any danger to WODO system, provides no impact on operations but is considered some potentially dangerous derivation from normal way of things.

- Stopped attempt to break into premises
- Momentary lack of internet connection
- Not serious OS warnings

4.2 Escalation

The roles and responsibilities of each of the WODO Incident Response Team members involved in incident response vary with the particular escalation and severity level. It's important to always, in the first place inform Incident Response Team Chief about accident and allow him to change response plan accordingly to the seriousness of the incident.

With respect to previously established hierarchy of incidents general specification of these roles and responsibilities is described below.

4.2.1 Critical level

- **General Manager**
  - Continue monitoring the incident
  - Decide whether the system should be shut down or can continue operations
- **Legal Advisor**
  - Continue monitoring the incident
  - Prepare a response to legal threats
- **Public Relation Officer**
  - If necessary alert users/external service providers (as appropriate)
- **Incident Response Team**
  - Set up command center
  - Take required actions
- **Incident Manager**
  - Identify countermeasures for containment of the incident
  - Continue reporting status to the General Manager
  - Stay calm
  - Coordinate Investigators work
  - Monitor effectiveness of the countermeasures in reducing the threats

- **Investigator**
  - Analyze the incident
  - Investigate the source of the incident
  - Continuously inform Incident Manager
  - If incident can be continuously constitute danger inform Incident Manager

4.2.2 High level

- **General Manager**
  - Continue monitoring the incident
- **Incident Response Team**
  - Set up command center
  - Take required actions
  - Receive technical information from relevant system administrators
  - Determine if countermeasures have reduced the risks to an acceptable level
- **Incident Manager**
  - Identify countermeasures for containment of the incident
  - Coordinate Investigators work
  - Monitor effectiveness of the countermeasures in reducing the threats
- **Investigator**
  - Analyze the incident
  - Investigate the source of the incident

4.2.3 Low level

- **Incident Manager**
  - Monitor all known sources for alerts or notification of a threat
- **Investigator**
  - Analyze the incident
  - Investigate the source of the incident
  - If possible prepare immediate response

5 | IR life cycle

The following chapter delineates how the incident response life cycle as specified by NIST's *Computer Security Incident Handling Guide* applies and maps to the system and organization in question.

5.1 Preparation

To prevent post-betting, i.e. submitting a coupon (e.g. via modification of the relevant file storing the coupons) after the current drawing is closed, a cryptographic hash of the coupon file is calculated when the betting is over and is then followed by the drawing itself (to prevent exploitation of race conditions). Bit-commitment protocols are used to ensure there occurs no tampering with the seeds used for random numbers generation.

Other than the connection to the verifier, the generator(s) are isolated from any external network. For auditing purposes the numbers generated by the generator are also stored on a hard disk for later verification, along with the relevant logs. Because the only viable mean of accessing the generator(s) is physical entry, the generators' room is electromagnetically shielded and employs biometric access control system. The entire floor is under a 24-hour-a-day CCTV surveillance.

Personnel with direct access to the IT infrastructure shall be subject to extensive monitoring and logging. Every access made must be documented and the document signed.

Numerous redundancies are put in place in terms of software components, i.e. cryptosystems, randomness generators and communication channels. The system must gracefully recover from any isolated error and there should be no single point of failure.

To ensure continual compliance with newly published security regulations as well as easy integration of newly approved, state-of-the-art cryptosystems and quick phasing out of redundant technologies, the WODO system has been designed with strict scalability and extensibility requirements in mind. Maintaining said extensibility is crucial in everyday work of the software development teams. To this end a thorough and exhaustive code review practices and detailed continuous integration and delivery (CI/CD) pipelines must be set up by and for said teams. As part of the acceptance criteria of software changes Security-oriented static code analysis is hereby defined as a necessary part of the software changes acceptance criteria in order to ensure implementation soundness and robustness.

Incident Response Team Technical Group, as defined in Chapter 3, shall have a direct involvement in risk assessment and preliminary controls implementation as well as provide technical requirements pertaining to both hardware and software tools to be used by the Incident Response Team.

A "jump-kit" must be available at all times for use by the Incident Response Team. It shall contain an extra forensic workstation to be used for sandboxing and analysing malware, blank removable media for evidence collection, removable media containing clean OS and application images for restoration purposes, as well as storage bags, tags, evidence tape, audio recorders and other equipment deemed necessary by the Incident Response Team Technical Director. The workstation shall have installed on it commercial-grade packet sniffers, memory dump analyzers and disk image analyzers chosen by the Incident Response Team Technical Director in cooperation with the Technical Group.

A dedicated conference room shall be designated, such that in the case of an incident all meetings in the room shall be postponed and/or rescheduled and the room itself shall server the purpose of a "war room."

IT infrastructure documentation shall be reviewed by the Incident Response Team on a quarterly basis to ensure continual familiarity of the team with the environment. Said documentation includes, but is not limited to:

- System architecture specification
- OS configuration
- Network configuration (used ports, routing configuration, etc.)
- Intruder Detection System configuration
- Firewall configuration

Critical assets' list shall be maintained and reviewed on an annual basis. Incident Response Team Technical Group shall have direct involvement in the process.

Baselines of expected system behaviour and state shall be maintained. This includes, but is not limited to:

- Cryptographic hashes of critical files
- Typical network throughput before and after the number drawing (this baseline shall be established separately for weekdays, weekends and bank holidays)
- Typical user behaviour, e.g. login times, geographic locations of logins etc.

5.2 Detection and analysis

First person to observe an incident notifies the Incident Response Team, which assembles and assesses the impact of the event. The initial assessment is followed by launching a notification process by the Internal Point of Contact. This process is department- or company-wise depending on the severity of the incident. Decision about the scope of

notification is left for the General Manager to make. Further handling of the incident is dispatched internally in the Incident Response Team.

Any deviation from the baseline shall be raised to the IRT as a potential incident. Detection of such deviations shall be conducted using the UEBA (User and Entity Behaviour Analytics) capabilities of the SIEM (Security Information and Event Management) software in use on premises. These deviations may include:

- Large number of bounced emails
- Multiple failed login attempts
- Login attempts from an unfamiliar remote system
- Login times significantly varying from the norm for a given user
- Network throughput over (incoming coupons) or below (outgoing media feed) the designated thresholds
- Unscheduled and undocumented configuration change (OS, applications, network stack)

IDS, antivirus and/or firewall alerts shall be immediately investigated by the IRT.

Logs shall be collected by the SIEM, preliminary analysis performed, and an automated response shall be run as part of the SOAR (Security Orchestration, Automation and Response) capability of the system. Further checking and incident handling is dispatched to the Incident Response Team Technical Group. Preliminary findings documentation and the collected logs shall be retained to facilitate event correlation and speed up subsequent analyses.

5.3 Containment, eradication & recovery

Physical incident e.g. breaking into premises by jumping over the fence or somehow getting into a restricted area, when detected, is immediately reported to the building guards. It is their responsibility to find and neutralize the intruder. They have non-stop access to inside and outside CCTV and are obliged to monitor entrances to the building. One must assume that the intruder may be armed, so every guard is equipped with incapacitating weapons and is legally authorized to use them. During an intrusion, every employee is informed via text message. Every employee is supposed to stay in their office and lock the doors.

In order to not allow incidents as such to be used as a way to deny or otherwise interfere with the drawings, the WODO system shall not cease operations while the situation is handled by the guards. Inflicting actual harm on the system would require the intruder to know the access keys to the server room, which is highly unlikely.

After the situation is handled and the intruder is captured, before employees leave their rooms, guards are supposed to thoroughly search places that were visited by the intruder. This action's purpose is to find whether any of the rooms were contaminated with some remote devices. Employees are obliged to check if all paperwork and equipment are accounted for. A captured intruder shall be handed over to the police.

Another addressed incident is compromised PRNG. Not keeping generated bits unpredictable might be one of the most devastating attacks when orchestrated by the attacker correctly. It may be very hard to detect when the attack is this kind of attack. On the other hand, a compromised PRNG doesn't have to be induced by the attacker but simply by a programming mistake or some other factor like a corrupted randomness source. This is also very dangerous because one may deeply analyze drawings of the WODO system, which may lead to predicting future drawings. As stated before it is especially dangerous because it is almost impossible to categorize whether a player is truly placing random bets or placing predicted bets.

In order to make sure that bits are generated randomly, the bitstream output of the PRNG is being evaluated by the Diehard and TestU01 tests. This evaluation process happens with enough time threshold to ensure that no drawing with corrupted bits takes place. If more than 3 subtests turn out negative, then the input to PRNG is changed to a second, alternative source of randomness, which is a meteorology station located at the top of the building. Having a second source of randomness allows the WODO system to operate even if the first one is down. If the second source fails as well the WODO system is stopped.

It is crucial to make sure that random bits are legitimate. When the first source of randomness is detected to be corrupted, eradication actions are supposed to be taken right away. An employee with suitable IT-knowledge is obliged to check in which part of the generating process this breach happened. When detected, the employee decides the severity of this incident. If it is simple to fix, then they fix it immediately and operations are resumed. When it is not then they alarms the Incident Manager. It is not unlikely for Diehard and TestU01 to raise false alarms and this is the reason why IM is not contacted immediately.

After the issue is resolved and the source of the incident is detected then lessons must be learned and an appropriate response implemented minimizing the possibility of the issue occurring again.

Yet another possible issue worth mentioning is a denial of service attack (e.g. coupon flood). Due to the obligatory payment before sending a coupon to the server any potential attack would be very costly therefore we consider the possibility of this kind of attack negligible. Nevertheless, we took into account the predicted popularity of WODO e-lottery and tripled the most optimistic capabilities of the servers to ensure the availability of the e-lottery for others.

Postbetting and other tampering with the betting procedure are detected by comparing cryptographic hashes of the coupon databases: the main file and a committed copy. The copy is committed one minute before the the drawing and past this point no betting is allowed anymore. In the case of a mismatch, the validity of a committed copy is checked, and the copy is used to retrieve the legally submitted coupons. An alert is also raised to the General Manager's office.

In the case of an incident, the place where everyone involved in containment and eradication should be stationed, the so-called "war room", is conference room 42 on floor 1. This conference room is big enough for 20-30 people, has both Wi-Fi and Ethernet access and is close to the bathroom and a vending machine.

5.4 Post-incident activity

Collected logs and documentation of the incident response handling process shall be retained in long-term storage. An expiration date of two years shall be put on the logs. The documentation of the incident shall be retained no less than five years. The materials gathered shall be used by the Incident Manager to conduct debriefing meetings and subsequent trainings for both the security staff and other employees.

Review cryptanalytic advances and revisit the use of cryptographic primitives in the system, e.g. hash functions that are not considered secure anymore, obsolete ciphers, broken (predictable) pseudorandom number generators. No less than two security engineers should be delegated to produce a report of analysis of the system in the light of the new advances. Based on this report, issues shall be raised in the internal ticketing system to introduce needed changes to the security infrastructure.

Independence of evaluators should be reviewed and new external parties involved if needed. If the functional impact of the incident was deemed high, contingency plans should be revisited.

Increase users' awareness and regain their trust by educating them about security and data-protection issues in non-technical terms. To this end a seminar detailing the incident and the steps taken to contain and recover from it should be held on premises as well as streamed online and recorded for further reference.

At minimum one "lessons-learned" meeting should be held internally by the Incident Response Team. There is no upper limit on the number of such meetings pertaining to a given incident as long as their number does not interfere with current operations of the team.

6 | Final remarks

This document shall be reviewed at least once a year and each time a high severity incident is handled and recovered from. This document shall serve as a basis for incident response drills and mock incident handling organized for the purpose of ensuring all interested parties are aware of the standard procedures and able to make speedy assessment, containment and recovery.

Bibliography

[1] J. Zhou, *Information security : 8th international conference, ISC 2005, Singapore, September 20-23, 2005 : proceedings*. 2005, p. 516, ISBN: 354029001X.

[2] G. Goos and J. Hartmanis, *Lecture notes in computer science*. 1980, vol. 106, p. i, ISBN: 3540224203. DOI: 10.1007/978-3-662-19161-3.

[3] *NIST Computer Security Resource Center Glossary*, https://csrc.nist.gov/glossary/, Accessed: 21-04, 2022.