VANJA KORAĆ
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,
e-mail: vanja@mi.sanu.ac.rs

MILAN TODOROVIĆ
Mathematical Institute SASA,
Kneza Mihaila 36/III, 11 000
Belgrade, Serbia,
e-mail: mtodorovic@mi.sanu.ac.rsMilan Todorović

ZORAN DAVIDOVAC
Mathematical Institute SASA,
Kneza Mihaila 36/III,
Belgrade, Serbia,
e-mail: zorandavidovac@mi.sanu.ac.rs

343.533::004
COBISS.SR-ID 264127500
Original research article

Received: March 25th 2018
Accepted: April 30th 2018

RESPONDING TO CYBER INCIDENTS WITHIN ORGANISATIONS BY APPLYING ADEQUATE POLICIES

ABSTRACT

The first cyber threats occurred in the 1970s [CW Jobs, 2016], in the form of rootkit, a hidden software which enabled continuous privileged access to computers, and also in the form of spam. The number and diversity of cyber threats has increased immeasurably up to today, and every such attack can cause serious damage. Since computers and the internet represent omnipresent and pervading technologies, the targets of these attacks are ever more often different organisations – those of the state, international companies, or parts of the local business sector. In order to respond to these threats in a quick and efficient manner, it is necessary to introduce certain policies at the entire organisation level, which would respond to cyber incidents. The purpose of the cyber incident response policies is to provide general instructions for the staff within an organisation, so they can perform, efficiently and precisely, those actions intended for establishing whether a cyber incident has occurred. If such an incident did occur, the staff would determine, on the basis of the given procedures, which actions should be taken so that the incident could be limited and the threat removed.

KEYWORDS: CYBER THREAT, CYBER INCIDENTS, TRAINING AND SECURITY AUDIT, INCIDENT RESPONSE TEAM.

CYBER THREATS

To recognise a cyber security incident, especially those behind which there are serious cyber attacks (which have become ever more common) and which are turning into a very persistent threat, has become a necessity for all organisations.[1] Cyber attacks cause serious damage to all organisations, those of the state, but also international institutions and local business sector companies. The correct manner to fight a cyber attack is to have a swift and efficient response to it. In order to achieve that, it

1 The article is the result of the project: *Viminacium, Roman city and military camp – research of material and non- material culture of inhabitants by using the modern technologies of remote detection, geophysics, GIS, digitalization and 3D visualization (no 47018)*, funded by The Ministry of Education, Science and Technological Development of the Republic of Serbia.

is necessary to have active preventive mechanisms and ready responses to cyber attacks that have been prepared at the highest possible level within organisations themselves and the institutions of the state. Cyber attacks are usually not a local occurrence and, hence, sometimes it is even necessary to establish international cooperation.

With common distributed-denial-of-service attacks (DDOS), sites being brought down or cracked, their contents deleted or changed, and also network infiltrations, ransomware threats and other types of attacks, all of which are claiming ever more space on public information media, it is obvious that cyber attacks are a reality of today. As such, they cannot be subdued without the exceptional cooperation of the international community at the highest levels.

CYBER SECURITY INCIDENTS – CSI

There is no universal point of view which would determine what can be called a cyber security incident, because there is such a wide range of variations and interpretations. Without having an agreed upon definition, and considering the fact that most organisations apply different views and practices for CSI, it is difficult for organisations to define types of CSI, and even more so to plan and secure resources or support level for preventive actions or responses to CSI.

The media has contributed to having CSI traditionally listed as Security IT incidents up until the point when the national infrastructure or security network becomes threatened, and in that case a CSI would be declared, because it would have the properties of cyber terrorism.

Even though good practice in CSI responses certainly exists and is constantly being improved, organisations still avoid information exchange, precisely because of the already mentioned fact – the lack of a general understanding and limited capacities and resources regarding CSI, which puts them into the context of limited, i.e. a low level of response to CSI.

Types of CSI

In practice, types of CSI are differentiated according to whether they are viewed according to the source of the indecent – minor crimes/organised crimes, or according to the manner in which the incident was executed (e.g. cracking, malware or social engineering). Thus, we have the basic CSI on one hand – minor offences, local interruption and theft, while on the other, on the extreme side of CSI, we have organised crime, national or worldwide interruptions and critical damage to national or international infrastructure. The nature of the attack can be public (e.g. compromising the reputation of a company) or concealed (e.g. profit).

FACTORS THAT AFFECT CSI AND HOW TO PREPARE A RESPONSE

CSI are usually linked to information, technology, processes and employees. Hence, the goal of the attack is always linked to the availability/unavailability, i.e. the theft of information. In order to enable a CSI attack, from within or outside, certain technology is required, from network devices up to computers or devices containing information. The exception, of course, are papers containing information; however, theft from within is still possible here by taking photos (CSI), and stealing papers containing information, while not CSI, is still a Security Incident. When it comes to processes (services), process interruption also leads to unavailability of information. Additionally, employees can cause CSI, and it is estimated that ca 70% of security breaches are performed wth the help of insiders [M. Reardon, 2005].

Preparation of an incident response

Regarding the already mentioned, one must know what to save and protect, and, therefore, how to respond as well.

Information – It is necessary to have a Central Registry for Information (CRI) and a list of people with access privileges and the Information Owner. It is necessary to comprehend the use of the Information, as well as to comprehend the exchange of information between employees, users, support and the ISP in order to ensure a correct response.

Consequently, it is necessary to make a record, for every incident, of details relative to the time of the incident: how and when it was noticed, what happened and what was affected by the incident.

Technology – It is necessary to have a Central Registry for Technology, which usually exists in the list of Basic Assets, but is often lacking certain information, which should be added to it. It is of paramount importance to know the data and network topology, especially where access points and the firewall are, where the incoming internet network is (or several of them) and where (back-up) logs are stored. Also, it is very important to know who configures network devices and has access to or works on a computer (which is also a network device).

Processes (Services) – Knowing what, and in what manner, the processes do, recognising if a process is active or missing is solved by defining a Central Registry for Processes. It comprehends the description, verification and installation (should the entire process be re-established from the start) of every process. To make it clearer, let us give the example of software (a basic asset) or, more specifically, a database or a webpage used by all employees. Knowledge on the process is necessary in order to limit and remove CSI, to restore critical systems, data, networks and work processes.

Employees and other human resources – Every organisation has a Central Registry for Employees, with their work description (contract), behaviour code, policy of acceptable usage or standard security policy and, if it has specified registries, it is known precisely who does what, and what their function, job description, contact (work phone number) and access to network devices are.

According to what has already been said, it is clear that there should be a Central Registry for Resources / Information Assets, which needs to contain all the necessary data and specified details on the Information, list of network devices and software (also a basic asset).

An additional registry which should exist is a centralised list of suppliers, which would significantly shorten the response time.

It is clear that someone should always respond in cases of SI and CSI, hence, it is also necessary to create a list of members of the Incident Response Team, with a list of replacement members, and to make it known to the employees.

Backup – the regular creation of a backup and periodical verifications have to be established.

Training – An annual or biennial lecture, which can be performed internally by a security officer, for all employees, with a test of some 10 to 20 questions, is necessary in order to maintain a perception of the importance of security. This small investment of money offers significant returns. An annual CSI simulation is desirable and represents the best possible training, especially when a complete restoration of processes is included.

Security Audit – An Annual Internal Security Audit represents the verification of documents, IT policies and procedures, knowledge of the IT personnel, including IT Security, and provides management with a clear image of the situation in IT/Sec within organisations and, most importantly, it highlights deficiencies and bad practices.

It is very important to note that Security audits provide an indication of the places where management must invest resources: hardware/software/human resources, training, external partners or support in order to bring the situation to an acceptable level.

RECOGNISING A COMPUTER OR CYBER INCIDENT

After an occurrence happens which raises concerns of a possible incident, it is essential to determine whether the events, data and facts gathered can be qualified as a cyber incident. Those pieces of information can be obtained through different sources, including events examined by computer administrators, through IT security, legal and corporative risks, privacy risks, process owners or business owners and higher management levels, and even employees and end users.

Finally, it is necessary to examine the gathered information in order to determine if they fulfil the conditions needed to pronounce that it was in fact a computer or cyber incident. A breach or the imminent danger of a breach of computer security policies, acceptable usage policies or standard security policies has a significant chance of leading to:

- negative influence on the reputation of an organisation;
- loss of intellectual properties or assets;
- unauthorised access to confidential (classified) data and personal (user) data.

If the data gathered does not fulfil the correct definition of a cyber incident, it is not accepted categorically as a computer or a cyber incident, but merely represents, instead, a sequence of computer events (any notable occurrence in a system or a network) which should be dealt with in an operational manner.

If an individual or a team determines that there is sufficient evidence to declare an incident, they have to forward that information to the person authorised to declare a cyber incident. That person can be the Chief Operating Officer, Chief Financial Officer, Chief Human Resources Officer, General Counsel or an officer in charge of privacy, IT or security. If there is a security officer, then they, according to the procedure, notify the General Counsel, and in case there is no such officer, the General Counsel takes over this role and declares the incident. In practice, the first person to be informed is always the manager /officer (CISO/ISO[2]) in charge of security, and then he or she notifies the CEO of the organisation.

Establishing an Incident Response Team

The Incident Response Team is a team in charge of examining and resolving discovered computer security problems, as well as finding suitable solutions through data gathering, information examining, risk measuring and implementing solutions in a suitable manner.

When the existence of an incident is declared, the Incident Response Team must be notified and activated. Generally, the following professionals are considered part of the Team in order to provide coverage for every individual segment of the incident:

- General Counsel – should be legally informed as soon as possible;
- Head of information security and/or Head of IT;
- Technical leaders – such as heads of security, network or infrastructure;
- Risk management / insurance;
- specialised experts (external forensic attorney);
- Human resources – except in cases when it is necessary to prevent physical access to an employee because of a breach of work discipline;
- Public relations / marketing;
- Security organs / HTC services.

Additionally, it is necessary to name the Incident Manager, who will be in charge of the incident. He can be the information or process owner, depending on the nature of the incident. The Incident Manager serves as the main organiser in cyber incident resolution.

The Project Manager can also be of use in organising notes and goals. It is very important to

2 Chief Information Security Officer / Information Security Officer

carefully select the members of the Incident Response Team, because the perpetrator of the incident could be one of the employees.

Once the incident is declared, it is important to establish the communication route to and from the Incident Response Team. The Team must establish whether it is safe to use the electronic mail of the institution. The Team must seek advice (from the General Counsel) on what would be appropriate for oral communication, and what should be communicated via electronic mail. If necessary, a communication room can be established.

Limiting the incident (if convenient)

The Incident Manager will determine (with the help of the Incident Response Team) whether the adverse computer events demand quarantine. Adverse events comprise computer events with negative consequences, such as system failures, package overload, unauthorised use of system privileges, unauthorised access to sensitive data and setting up of malware that destroys data.

If deemed convenient, actions could be taken which would isolate systems, block access or prevent suspicious activities. It is necessary to carefully evaluate quarantine risks versus the ability to thoroughly investigate the problem, while taking into account business management risks. It is also important to note that any actions taken can show the attacker that he has been exposed.

Extent of the incident

The Incident Response Team has to instruct the system administrator to make a preliminary list of endangered information assets, including servers, systems and/or data affected by the event. This should include timeframes, people known to be involved in imminent actions, during and after the event, as well as all information such as network data or warnings, alarms or other information obtained during the investigation. It is important that the administrators report all relevant facts which can be directly or indirectly brought into connection with the incident which occurred. It is essential that managers of work organisations also provide reports if the processes came to a complete or partial halt because of the CSI.

Information analysis by the Incident Response Team

The Incident Response Team has to take into consideration all the information gathered and to document the following:

- suspicious activities, such as unwanted visitors or suspicious network traffic;
- access to information by the attacker, e.g. capability of physical transfer of devices or data confiscation through network;
- data that was accessed, along with witness statements and computer logs;
- duration of danger, with time marked when the data could have been, or was, endangered;
- method of attack, such as malevolent visitors or network intruders who used the hacked assets;
- data accessed without authorisation, or which is under suspicion of being accessed from external systems;
- loss estimation comes down to data loss estimation, time estimation in relation to the actual loss of data. Aside from material, loss can also be non-material, e.g. the compromising of the organisation's reputation.

Recovery or recuperation of the environment and verification of the environment

The Incident Recovery Team should work together with the system administrator in order to restore information assets into the regular working state. This may include:

- Implementation of information security controls which resolve vacancies in policies,

processes or procedures.

- Implementation of technical controls, such as stronger passwords, limited access or obligatory multi-factor authentication.
- Implementation of administrative controls, such as logging, processes for obtaining or removing accessibility or strict access time.
- Implementation of physical controls, such as locks, barriers and protection of information assets.
- After restoring work status, it is necessary to verify that all the processes have been re-established, which is the task of the managers of the organisational units and employees who have the testing scenarios (Central Process Registry). Alongside them, the Information Owners also perform the verification.
- If it is necessary to restore some of the information which was entered just before the CSI and which does not exist in the BACKUP, but which are available in another form, a team is established for entering and verifying that data

Work on communications

The organisation can have the duty of revealing certain information concerning a possible or actual incident. The Incident Response Team has to establish whether and which communication can be shared internally, within the management, within the entire business or with external parties, such as newspaper agencies, social networks and/or government institutions.

Additionally, the Incident Response Team might be obliged to inform other stakeholders as well (e.g. sponsors) according to legal contracts which define the time period in which the endangering of the data has, or may have occurred. Communications must be performed according to guidelines given by the General Counsel.

Discussions after taking actions

The General Counsel will determine if there is need to conduct a series of discussions on the incident after taking actions. If they are deemed necessary, these discussions will ensure that the incident process was well responded to – including all public relations, internal communication with the staff and/or technical changes concerning the incident, as well as vacancies relative to the incident. On the basis of these discussions, if necessary, it may be deemed opportune to revise procedures and polices after the CSI, and, again, if necessary, change the topology of the network or processes in order to avoid a further CSI. The creation of a policy is approved by the General Counsel, and is recorded in a table, where revisions can be monitored with descriptions, dates and signatures of all the people who wrote the policy and signatures of persons responsible for accepting the policy.

FINAL CONSIDERATIONS

To recognise a cyber security incident, especially one behind which there are serious cyber attacks, has become a necessity in all organisations. A response to these incidents comes from the existence of active mechanisms and ready responses which are defined through a policy for cyber incidents responses. It is necessary to know all the factors which can be influenced by a cyber security incident, and what is to be preserved as well, but it is also necessary to be aware of a suitable way to react. An organisation must have a Central Registry for Information, Central Registry for Technologies, Central Registry for Processes, Central Registry for Employees and Central Registry for resources/information assets, which, together, enable a more efficient way to recognise an incident, its influence and possible source. The determination of the manner and intervals of making backup copies of data represents a basic step in limiting the damage that a cyber incident can cause.

When an incident occurs, it is essential to gather as much data as possible, on the basis of which it can be determined what type of incident it was, and to notify the person in charge in cases of such an incident. Additionally, it is necessary to have an Incident Response Team, whose responsibility it is to investigate and resolve discovered incidents, which must be notified and activated when an incident occurs. It is essential to establish the scope of the incident, i.e. which part of the information system was affected by the incident, which occurrences happened immediately before and after the incident, as well as other important information for the Incident Response Team to investigate. After that, the team, along with system administrators, has to work on activities concerning the restoration of the system to its regular state. After a response to a cyber incident, discussions can be held, which would determine if the reaction was suitable. On the basis of those discussions, it is possible to revise procedures, policies or various systems for the future avoidance of incidents, if deemed necessary.

* * *

BIBLIOGRAPHY

CW Jobs [Internet]. London, UK: 2016. Cyber crime timeline; URL: https://www.cwjobs.co.uk/careers-advice/it-glossary/cyber-crime-timeline. Accessed: 26.3.2018.

Marguerite Reardon, *Securing data from the threat within*, Computer Crime Research Center, 2005, URL : http://www.crime-research.org/news/12.01.2005/893/. Accessed: 26.4.2017.

REZIME
ODGOVOR NA SAJBER INCIDENTE U OKVIRU ORGANIZACIJE KROZ PRIMENU ADEKVATNE POLISE

KLJUČNE REČI: SAJBER PRETNJA, SAJBER INCIDENTI, TRENING I SECURITY AUDIT, TIM ZA ODGOVOR NA INCIDENTE.

Broj i raznovrsnost sajber pretnji se do danas neuporedivo povećao, a svaki od napada može naneti ogromnu štetu. Kako su računari i internet danas sveprisutne i sveprožimajuće tehnologije, mete napada su sve češće različite organizacije koje mogu biti državne, međunarodne ili deo biznis sektora. Kako bi se na ove pretnje brzo i efikasno reagovalo, neophodno je uvođenje određene polise na nivou cele organizacije za odgovor na sajber incidente. Odgovor na ove incidente podrazumeva postojanje aktivnih mehanizama i spremnih odgovora koji se definišu polisom za odgovor na sajber incidente. Neophodno je znati na šta sve može uticati sajber bezbednosni incident, kao i to šta je potrebno čuvati, ali je potrebno primeniti i odgovarajuću reakciju. Svrha polise za odgovor na sajber incidente je da pruži opšta uputstva osoblju u okviru organizacije, kako bi se efikasno i uredno sprovele akcije koje služe za utvrđivanje postojanja sajber incidenta. Ako incident postoji, osoblje na osnovu procedure određuje koji je postupak neophodno sprovesti kako bi se incident ograničio i otklonio. Na osnovu razmatranja je moguće revidirati procedure, polise ili različite sisteme radi budućeg izbegavanja incidenta, ukoliko je to neophodno.