Evaluation and Process of Resolving a Security Incident by the CSIRT Team MASTER.CZ-CSIRT

Within the response of the team, it is necessary to process, evaluate and register specific types of incidents.

Risk Levels

The following table describes the risk levels that we identify.

Level of risk	Risk definition	Typical incident	Typical consequence of the incident	Response time
3	High	DoS	Unavailability, threats to asset integrity	60 minutes
2	Medium	Scanning	Threat to an asset	24 hours
1	Low	Spam	Complaint, notification	Next working day

Identification

This step is necessary to verify that a sender of a message is trustworthy. In the event of a reported incident by a sender denoting as our customer or acting on their behalf, it is essential to authorize them. The authorization is described in the internal directive of the security team.

Security Incident Classification

It is necessary to correctly classify each security incident according to knowledge and then perform an escalation for a specific event based on a known procedure.

All incidents managed by the CSIRT team MASTER.CZ-CSIRT should be classified into one of the categories in the following table.

Incident category	Level of risk	Description
Spam report	1	A request for exclusion from the newsletter is part of this classification as well.
Mailing list report	2	Reports concerning the inclusion of an IP address of our range in blacklists.
Bounce spam	1,2	Reports regarding the use of our range of IP addresses for bounce spam.
Incoming DoS a DDoS	3	Network device attack technique used to disable a device's service. The incoming attack will escalate to the administrators who will solve the problem. An attack captured by area antiDDoS protection is not taken into account.
Outgoing DoS a DDoS	3	Network device attack technique used to disable a device's service. Outgoing attacks of this type usually indicate an attacked device from our scope and it is necessary to deal with it immediately.
Copyright infringement	1,2	Sharing material, content, or tampering with the copyright of the copyrighted work.
Phishing, pharming	2,3	Tools for unauthorized acquisition of sensitive information (passwords, cryptographic keys etc.)

Application scanning, cracking	2,3	Techniques used to obtain network information resources and possible misuse of network services, or their resources.
Malware	3	A program for intrusion, usage, or damage computer system (rootkit, infected server).
Compromised assets	2,3	Includes compromised host, network device, application or user account. This category includes an infected host that is actively controlled by an attacker.
Open DNS, NTP server	1,2	By using open DNS, NTP servers is possible to perform amplification attacks. It is therefore necessary to address customers and most importantly not use name servers with open recursions.
Compromised information	3	Successful attempt to destroy, disrupt or change sensitive data.
Violation of the laws of the Czech Republic	3	Blackmailing, fraud and other activities that are in conflict with the laws of the Czech Republic.
Other	1,2,3	Another security incident, which was consulted with CSIRT team members.

The risk level depends on the circumstances.

Measures

The individual steps are taken on the basis of two main criteria – if it is a security incident directed from or to assets under our management or if it is assets under the management of our customers.

a) **Assets under our management**: escalation of the problem to the owners/administrators who are responsible for running this asset. This is usually a server/service under our management. We pass security incidents directly to the administrators who manage the server/service (contact e-mail: managed@master.cz).
b) **Assets under management of a customer**: contacting and escalating a security incident to the owner of the asset (service / server / range of IP addresses etc.) According to the classification of a security incident, we will perform an action corresponding to the level of risk of the incident.

Procedure and Escalation According to the Category of the Incident

Each incident must be classified according to the entity (owner) to which it relates and proceed accordingly. When implementing measures for “Assets under our management”, always hand over the ticket created for the incident to managed@master.cz, and depending on the level of risk contact the administrator, who will solve the problem.

The number of reports/complaints or findings is always considered within 24 hours. In case there are significantly more of these complaints, it is necessary to go directly to the next step of the procedure.

Type of incident	**Number of reports / complaints / findings**	**Procedure**
Spam report	1	Forwarding the complaint to the owner with own comment of the report.
	2	Forwarding the complaint to the owner with notification of recurring report of the incident.
	3	Calling the owner of a security incident alerting them to a possible blockage of services by us until the problem is resolved. Requesting for their statement into the created ticket.
	4 and more	Blocking the SMTP port of the service for which the security incident occurs.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	**Number of reports / complaints / findings**	**Procedure**
Mailing list report	1	Forwarding the complaint to the owner with own comment on the report.
	2	Calling the owner with an alert and requesting them for their statement into the created ticket.
	3	Calling the owner and alerting them to a possible blocking of services by us until the problem is resolved. Requesting for their statement into the created ticket, where the security incident is being solved.
	4 and more	Blocking the SMTP port of the service for which the security incident occurs.

Type of incident	Number of reports / complaints / findings	Procedure
Bounce spam	1	Forwarding the complaint to the owner with own comment on the complaint of bounce spam from our scope.
	2	Forwarding the complaint to the owner with notification of recurring bounce spam report.
	3	Calling the owner and alerting them to a possible blocking of services by us until the problem is resolved. Requesting for their statement into the created ticket, where the security incident is being solved.
	4 and more	Blocking the SMTP port of the service for which the security incident occurs.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Incoming DoS and DDoS	1	Restricting inbound traffic to the targeted IP addresses of the attack. Sending a notification about traffic restriction to the customer.
	2	Blocking incoming traffic to the targeted IP addresses of the attack. Sending a notification about blockage to the customer.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Outgoing DoS and DDoS	1	Restricting outbound traffic to the source IP addresses of the attack. Sending a notification about traffic restriction to the customer.
	2	Blocking outbound traffic from the source IP addresses of the attack. Sending a notification about blockage to the customer.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Copyright infringement	1	Forwarding the complaint to the owner with own comment of the report.
	2	Forwarding the complaint to the owner with notification about recurring copyright infringement.
	3	Calling the owner and alerting them to a possible blockage of services by us until the problem is resolved. Requesting for their statement into the created ticket.
	4 and more	Blocking the HTTP port of the service for which the copyright infringement occurs.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Phishing, pharming	1	Forwarding the complaint to the owner with own comment of the report.
	2	Calling the owner and alerting them to a possible blockage of services by us until the problem is resolved. Requesting for their statement into the created ticket.
	3 and more	Blocking the HTTP port of the service on which are located the fraudulent sites.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Application scanning, cracking	1	Forwarding the complaint to the owner with own comment of the report.
	2	Calling the owner and alerting them to a possible blockage of services by us until the problem is resolved. Requesting for their statement into the created ticket.
	3 and more	Blocking outbound traffic from the source IP address of the attack. Sending a blockage notification to the customer.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Malware	1	Forwarding the complaints to the owner with own comment of the report.
	2	Calling the owner and alerting them to a possible blockage of service by us until the problem is resolved. Requesting for their statement into the created ticket.
	3 and more	Blocking the HTTP port of the service on which the malware is located.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Compromised assets	1	Forwarding the complaints to the owner with own comment of the report.
	2	Calling the owner and alerting them to a possible blockage of service by us until the problem is resolved. Requesting for their statement into the created ticket.
	3 and more	Blocking the compromised service.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Open DNS, NTP server	1	Forwarding the complaints to the owner with own comment of the report.
	2	Forwarding the complaint to the owner with notification about recurrent report of the problem.
	3	Calling the owner and alerting them to a possible blockage of service by us until the problem is resolved. Requesting for their statement into the created ticket.
	4 and more	Blocking DNS, NTP port of the service on which the open DNS, NTP server is located.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedures
Compromised information	1	Forwarding the complaints to the owner with own comment of the report.
	2	Calling the owner and alerting them to a possible blockage of service by us until the problem is resolved. Requesting for their statement into the created ticket.
	3 and more	Blocking the compromised service.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Type of incident	Number of reports / complaints / findings	Procedure
Violation of the laws of the Czech Republic	1	Forwarding the complaints to the owner with own comment of the report and alerting them to a possible blockage of service by us until the problem is resolved.
	2	Calling the owner and alerting them to a possible blockage of service by us until the problem is resolved. Requesting for their statement into the created ticket.
	3 and more	Blocking of the service that violates the laws of the Czech Republic.

If the customer reacts to the created ticket with the solution of the problem, it is possible to consider the case as solved. If there is another complaint about the same scope of the same customer, we always proceed with one level up of the above procedure.

Archiving

Individual security incidents are archived in the RT ticketing system. Records and archiving are kept according to the subject to which the incident relates and the ticket number of the specific incident.

Useful Tools

Various tools can be used to validate an incident report and confirm it. The tools can be used as a prevention as well.

Website Scanner

- Free site security scanning
- www.skenerwebu.cz

Mail Server Test

- Complete test of mail servers IP and its listing within many blacklists (RBL/DNSBL)
- http://multirbl.valli.org/lookup/
- For each listing it is necessary to read a note – some blacklists are obsolete or no longer used.

Searching for Contact Information

- Finding the right contact is one of the most important parts of reporting security incidents.
- https://apps.db.ripe.net/search/query.html
- https://whois.domaintools.com/