Contingency plan for hacking attempts

1. Introduction

The hacking attempts are divided according to the areas they affect.

First area is applies to attacks directed directly at the system (internet shop).

Second area applies to attacks directed at workers (programmers, testers). Due to epidemiological threat, many of them is forced to work remotely, what   
opens up new opportunities for attacks.

Last, third area applies to attacks directed at user, e.g. stealing their login credentials.

2. Preparation

Security information and event management provides reports for unusual traffic and behaviors detected in network. They are grouped into 3 categories, based on threat level, in order to make them maintainable. Any incident or breach detected, classified at level 2 is saved separately. If incident or breach is well known and described, automated steps can be taken. If so, they are also reported.

Any incident or breach detected, classified at level 3 causes immediate alert to the first contact administrator. In this case, the first contact administrator checks, what resources have been compromised, and then takes further steps.

Other incidents are aggregated into one document, evaluated weekly. They are sorted into categories and increased grow in one of them may be the reason to initiate the investigation.

Any person involved in contingency plan, must be must be trained, in order to determine the method of communication. After serious incident, all people involved in the process are informed via company’s communicator, and text message. After that, an online meeting is taking place at company’s video communication platform, in specially prepared room. In case, when company’s network is unavailable, the meeting takes place directly at company’s building, in specified conference room. When one of people involved is unable to arrive within one hour, he informs about this fact the first contact administrator, and have to be on a standby on phone until the meeting is finished, in order to get information what steps needs to be taken.

3. Detection and analysis

Detection of incident is based log aggregation solution and intrusion prevention system (IPS).

Areas that are monitored are:

* suspicious, unusual activity on users and employees accounts
* recognition of brute force attack (e.g. multiple connections from same address)
* filtering and blocking emails

After detection of incident, the suspected address is added to the watch-list for 24 hours. If new suspicious actions are detected in this period of time, the incident level of risk is increased and the incident is reported.

Any e-mail, that contains links is considered as suspicious, alike e-mails from unknown senders. After confirming an malicious e-mail incident or breach, all messages from sender are blocked.

Login attempts are monitored and logged. If there appears a significant number of login attempts to single account, the owner of the account is informed about it via e-mail.

Also, geolocalization is used, in order to detect anomalous connections.

Any unusual traffic from single user is logged. This includes also monitoring the external/removable data sources (like monitoring usb ports of workers). If many of incidents are detected, then specific user is reported as suspicious of being compromised (e.g. affected with malware).

Unavailability of any of the services offered by the system, when detected, is marked as maximum threat level. The first contact administrators are immediately informed about that fact, and manually take further steps. If it is possible ( implemented procedures includes such event), automated actions are taken ( like disconnecting device from company’s networks) in order to stop the spread of threat.

4.Containment and alarming

Appearance of incident or breath of third level of significance requires immediate action. First contact administrator is informed and starts the investigation. Having access to data connected with incident, he has to evaluate the seriousness and impact of problem.

After determining the sources of danger, and affected parties further actions are taken.

If alert turns out to be false (no action needed), then these information should be included in learning phase. Otherwise, the step against spreading of the issue are taken. Also, depending on initial threat analysis, the right people are put on standby.

1. If problem concerns employees, specific employee is blocked in system until case is resolved. That means, he is unable to access any of company’s data, nor communicate with other devices inside network. The worker gets notification about the issue, and should wait for further information.

2. If problem concerns unavailability of services, the administrator has to check, if are they critical to the correct work of shop. If it is possible, and there is and existing procedure for such case,

admin can restart such service in order to make it work again. If it is not the case, such affected service should be isolated from the rest of the system during the investigation. Also, IT Manager is notified about that fact immediately. The website should be changed to previously prepared one, containing information about technical break and apology.

3. If problem concerns other system related threat, admin has to investigate the seriousness of it and affected assets. If unknown (not noted before) problem occurred, and possible damages are impossible to predict, IT Manager is notified immediately, and the meeting is taking place.

4. If problem concerns users, that means a lot of similar incidents, related to users appeared.

For example, significant number of login attempts may be result of some databases leakage. Someone is trying to use leaked data for other websites (many users use same password).

In this case, first step is to change tuning of monitoring tools, in order to focus on incidents connected with attack vector. Users should be notified on possible threat via email. The email can contain (depending on situation) recommendation to change password. Customer Service Manager should be notified about this fact to prepare eventual statement to users.

Generally, any incident reported, that can not be classified as false positive and cannot be handled automatically, leads to investigation. If basic services or data stored might be in danger, IT Manager is notified immediately. If there is a suspicion, than incident is intentional action of one of the employees, the Human Resources Manager is notified.

If possible sources of problem are found, the monitoring devices are tuned to recognize similar ones and report them for at least 7 days.

Next step is to identify damage caused. If data leakage or loss is confirmed, then Media Relations Manager is notified. If there is an evidence of fake transactions, that might took place due to attack (like shopping without payment), the Vendor/Contraction Manager is notified about that fact.

If a violation of these goods is discovered at a later stage, the same persons should be informed.

5. Eradication and Recovery

In cases, when IT Manager is involved his duty is to establish actions that will allow system recovery. Provided information from first contact administrators, he has to found out the source of problem, identify the consequences and contact the Crisis Manager in order to get authorization for

actions needed. With help of his team, he performs:

* neutralize the danger: depending on situation in may be blocking specific requests, that led to unauthorized actions
* in case of service loss: restarts affected services, recovers system back to work
* after data loss: checking backups in order to restore data, estimates the size of data that cannot be restored
* after data leakage: estimates the size and data sensitivity

All estimations are forwarded to the Crisis Manager, who is responsible to take eventual business, legal or other actions, supported by Critical Operations Support Staff.

In case, when the attack cannot be stopped immediately (like in case of well prepared DDoS attack),

the IT Manager is in charge of stopping the system, or it’s affected part and convening a team meeting (the team is predetermined and consists of the most experienced programmers and architects in the company) in order to create fixes that will allow recovery.

After all, IT Manager creates report that will allow to avoid such incidents in the future. This may include changes in procedures, including new ones, that will allow to automate similar incidents in the future, or new security features that should be implemented in the system in order to prevent.

In cases where the IT Manager is not called, the administrator is responsible for fixing the problem.

When one of your employees' computer is at risk, removing the threat involves checking the infected machine in person. If it is not possible to get rid of the problem non-invasively (for example, the disk was encrypted by the attacker) possible data losses are determined. On this basis, a decision is taken on further action. The employee's computer may be restored to factory state, or further attempts are being made to solve the problem non-invasively.

If incident, that is being monitored starts to appear more frequently, First Contact Administration is obliged to inform the IT Manager about this fact.

6. Learning

Learning phase includes usage of information acquired during the alert. In general, nearly half of alerts are so called false positives, that do not require action, but only wastes the time of First Contact Administrators who have to check them.

After alert, that found out false, there should be applied tuning to the detection system. It may include the higher rate of similar incidents needed to trigger the alert – connected for example with growing number of users. Finding correlated assets and binding them together is one of the ways.

If alert seemed to be serious, but not in the specific environment (like SQL Injection attack on part of the system that does not have access to the database), is should be addressed more accurately, including not only the attack itself, but also the context that in which it appears.

The tuning should be done continuously.

The recommendations in reports that are created by IT Manager after recovery should be included in the system as soon as possible. The Recovery Management Team is subject responsible for applying changes, after they are confirmed by Crisis Manager.