Contingency plan for users data leakage

1. Introduction

There are many different types of data leakage and it is important to understand that the problem can be initiated via an external or internal source. The term “data leakage” can be used to describe leakage of data that are transferred not just electronically but also physically. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices such as optical media, USB keys, laptops or simply on paper.

This Contingency Plan establishes comprehensive procedures to recover quickly and effectively users data leakage disruption. Steps described in the following refer to actions to be taken when a data leak is detected.

2. Detection

This phase describes potential causes of users data leakage. At the completion of the Detection Phase, worker that suppose occurrence of users data leakage should have an intuition of what is the cause of this disruption.

Possible causes of the users data leakage:

* Malicious attack (e.g. phishing attack, keylogging malware, exploiting vulnerabilities attack, remote spying, eavesdropping )
* Human error (e.g. weak passwords, an employee sends an email with sensitive information to the wrong person, loss of paperwork, malicious worker)
* System failure (e.g. application failures, accidental data dumps, errors in data transfer)
* Theft (e.g. laptops, cell phones, paperwork, tablets)

4. Notification

The Notification Phase defines initial actions taken once the users data leakage has been detected or appears to be imminent to leak. This phase includes activities to notify proper workers in the company and activate the Contingency Plan. At the completion of the Notification Phase, Recovery Team of the company will be prepared to perform recovery measures.

The contingency plan of users data leakage may be activated if one or more of the following criteria are met:

1.Users data leakage has been detected and it is provable;

2. It is suspected to have occurred users data leakage.

The following persons or roles may activate the CP if one or more of these criteria are met:

1. Data Administrator
2. System Engineering Manager
3. Director of the company

The first step upon activation of the Users Data Leakage Contingency Plan is notification of appropriate mission/business and system support personnel. Contact information for appropriate operations point of contact is included in Contact List.

Obraz zawierający tekst

Opis wygenerowany automatycznieFor Users Data Leakage the following method and procedure for notifications are used:

In the event of a threat of users data leakage, quick action is extremely important.

The methods of notification should be the fastest as possible. Above methods are just a suggestion and are adjustable in order to speed up the notification procedure.

5. Recovery

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by Recovery Team of the company. Assessment results are provided to the CP Coordinator to assist in the coordination of the recovery of users data.

Potential for disruptions or damage:

* System damage
* Financial cost of specific skills to repair the damage
* Work/time loss
* Safety loss
* Customers loss
* Confidentiality loss
* Image reputation and goodwill loss

Assessment of affected physical infrastructure:

* Malicious attack could affect:
  + proper operation of devices
  + structural integrity of computer room
  + telecommunications
* Human error could affect:
  + proper operation of devices
  + structural integrity of computer room
  + telecommunications
  + condition of electric power
* System failure could affect:
  + proper operation of devices
  + structural integrity of computer room
  + telecommunications
  + condition of electric power
* Theft
  + proper operation of devices
  + structural integrity of computer room
  + telecommunications

Items to be replaced:

* In case of malicious attack:
  + software
  + firmware
* In case of human error:
  + worker
* In case of system failure:
  + hardware
  + software
  + firmware
  + equipment
  + supporting materials
* In case of theft:
  + software
  + passwords

Inventory and functional status of system equipment:

|  |  |
| --- | --- |
| System Equipment | Functional Status |
| Laptop 1 | fully functional |
| Laptop n | fully functional |
| Tablet 1 | fully functional |
| Tablet n | fully functional |
| Mobile phone 1 | fully functional |
| Mobile phone n | fully functional |
| Printer 1 | fully functional |
| Printer n | fully functional |
| Payment terminal 1 | fully functional |
| Payment terminal n | fully functional |
| Air conditioning in the server room | fully functional |
| Server 1 | fully functional |
| Server n | fully functional |

Estimated time to restore services to normal operations:

* In case of malicious attack: from 24h to 96h
* In case of human error: from 1h to 96h
* In case of system failure: from 24h to 96h
* In case of theft: from 1h to 96h

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. The tuning should be done continuously.

Personnel with outage assessment responsibilities should understand and be able to perform these procedures in the event the plan is inaccessible during the situation. Once impact to the system has been determined, the appropriate teams should be notified of updated information and the planned response to the situation.

Bibliografia:

<https://www.newhorizons.com/article/7-it-roles-every-modern-company-needs-to-stay-competitive>

<https://poradnikprzedsiebiorcy.pl/-wyciek-danych-osobowych-pracownikow-warto-wiedziec>

<https://creately.com/blog/business/business-contingency-plan-templates/>

<https://www.sciencedirect.com/topics/computer-science/notification-procedure>