Kealan Crilly

setstats  Dundalk Institute of Technology

sECURITY STEPS TO TAKE IN EVENT OF a BREACH

Security Report

Contents

***Introduction***

[**Preparation** 2](#_Toc131525078)

[**Response** 3](#_Toc131525079)

[**Conclusion** 5](#_Toc131525080)

Introduction

This paper will summarise and identify the best steps to take if the website suffers an attack. Whether this is through a denial-of-service attack, a hack, a breach of data or any other incident. The main areas to consider is the best measures to implement as quickly as possible after such an event occurs. The purpose of this document will go further in that it can be used as a template to be looked at and reviewed should such an event happen in your workplace or business. It may also serve to save the business in terms of time, finance, and the reputation of the business itself among its customers and in potential markets worldwide.

While not ideal the best time to act is as soon as a data breach happens. This means immediately notifying all your employees in the workplace then your customers and then the rest of your audience that there has been a breach. The notification is best suited to be communicated through social media or even in a personal email to all the customers that frequent your website. Under GDPR the main time to notify users is up to 72 hours after an attack has occurred and no later and the Information Commissioner’s Office (ICO) must be notified. If, however it is a serious breach then all data recipients must be notified straight away without delay. Further to this a record needs to be kept of all and any data breach which occurred. Failure to do this can result in a 20 million fine or 4% of the revenue that the business makes.

Graphical user interface, application

Description automatically generated

# **Preparation**

The first thing to do is plan. Planning allows the organisation to recognise and quickly react to a data breach with less damage done in the long run if the response is quick enough. To effectively plan the organisation must have a system or structure in place that deals in preventing any data breaches and reacting to them. A person or a co-ordinated team in the organisation will see to this. This person or team will be responsible for the security of the website including data travelling to and from the site as well as data stored in the database and being sent to the database. Other members of the organisation can report a suspected incident or issue to the response team. As part of their role, they shall conduct analysis on the website and look for any areas of concern. Areas for concern can include but are not limited to buffer overflow attempts against the database system, multiple failed logins attempt from a remote system, emails that failed to send and contain suspicious content. Of course, the key to stop this beforehand is to minimise the risk. This can be done through encryption and hashing of user’s passwords. Ensuring smooth transit of data over networks by making sure they are being sent over HTTPS/SSL for maximum protection. Storage of the data has to be kept secure in the database through authentication and a person part of the team overseeing the transit of that data and checking it is consistent, up to date and above all else protected. Checking of documents before they are sent across the network to look for missing or incorrect information.

Another area of security that is often overlooked and many organisations fail to even recognise this never mind try to prevent it is a social engineering attack. The famous author and convicted felon Frank Abagnale argues that the human element is often the most important factor for privacy and security. A social engineering attack relies on a desperate need and a sense of urgency. The psychology of persuasion goes into these attacks. The goal of the attacker is to establish rapport with their victim and gain their trust. Often, they impersonate or claim to be a member of a legitimate organisation to gain trust of the victim. Once their trust is gained then their guard is down which in turn means they are more prone to divulge sensitive or personal information about a person or the organisation, or open web links or emails that contain malicious content.

## **Response**

As soon as a breach happens within 24 hours the team must document the time and date the breach was found, notify all members of the organisation what happened, notify the police, begin to document the investigation into the breach, conduct a throughout analysis of what caused the breach and look to identify the source of the problem, collect all and any data related to the breach. Any documents offline must be kept secure and backup copies must be created if necessary. The organisations devices and electronics all need to be analysed and checked for any suspicious activities. Contacting third party companies such as insurance, legal and cybersecurity experts will go further in your organisation’s response to react quicker. The response to your customers, employees, media and worldwide markets has to be clear, straight to the point and with as little emphasis as possible on any negative consequences of the breach. If the organisation has the resources, then a PR company can contact and deal with the media and social media companies about the breach to stop any rumours or negative media feedback from building. The last thing to do is to inform all customers to change their passwords, emailing clients that the situation will be resolved as quickly as possible, activating data loss and recovery procedures, and performing an evaluation breach response to modify and improve the response plan for future use.

Graphical user interface, application

Description automatically generated

**7 Steps after the breach**

***Graphical user interface, application

Description automatically generated***

### **Conclusion**

To conclude it is best to have a well thought out and established contingency plan in place to prepare for a data breach or risk to the security of your website or system. A clear and comprehensive guide with steps to follow must be the main priority for all involved in the organisation and has to be established throughout the culture of the workplace so that in the event an incident happens then all will respond and react quickly to the situation. The social element needs to be looked at to and any suspicious activity like login attempts, phone calls with dubious questioning etc should all be double checked and thoroughly reviewed before proceeding with authorisation.

Graphical user interface

Description automatically generated

***References***

<https://datagraphic.co.uk/news/what-is-document-security-and-why-is-it-important/>

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

<https://www.ekransystem.com/en/blog/data-breach-investigation-best-practices>

<https://whatarmy.com/blog/the-gdpr-and-how-it-applies-to-small-business-websites/>

<https://www.trusona.com/news/frank-abagnale-no-technology-can-beat-a-social-engineering-attack>

<https://www.abagnale.com/About-Frank-Abagnale-Jr.html>

<https://www.cisco.com/c/en_uk/products/security/what-is-social-engineering.html>

<https://www.techtarget.com/searchsecurity/feature/How-to-develop-a-data-breach-response-plan-5-steps>

<https://www.businesstechweekly.com/cybersecurity/data-security/5-essential-data-security-best-practices-for-keeping-your-data-safe/>