simplisys
SERVICE DESK

Managing a data breach in a GDPR World

Introduction

Maintaining security of your data, particularly personal data, is an issue that has been with us for many years. The Data Protection act formalised the requirements for businesses to take care when processing personal data imposing penalties for breaches of the act.

GDPR has increased both the expectations around protecting personal data and its processing and businesses have to up their game to ensure that they comply with the new, enhanced, requirements.

Are you ready for the inevitable data breach? How will you respond? Do you have the process in place to manage the breach and comply with the GDPR?

Responding to a potential data breach

The GDPR has imposed a number of requirements regarding the response to data breaches, including time bound notification requirements.

When the dreaded day occurs, and it will, and your organisation suffers a data breach how should you react, and how should you prepare yourself? The key is quite naturally being well prepared with your plans and process well designed and tested and suitable tools used to manage the situation.

There are 5 key stages in a Data Breach response. These are

- Detection Response
- Containment
- Impact Assessment
- Notification / Communications
- Remediation
- There is also an overarching process that takes place alongside these 5 stages. This is Audit Trail

We take a slightly more in-depth look at these stages below:

- Detection Response

You need to activate the plan fast, but only if needed. Your monitoring needs to alert you to potential issues but your filtering and triage process needs to accurately and quickly pick out those security events that need further response.

- Containment

  Once a potential breach has been identified you need to take immediate action to contain the damage. The escalation from a security event to a security incident needs to trigger a pre-prepared series of containment actions. Password changes, taking impacted servers off line, securing backups for example.

- Impact Assessment

  By now you should know which one of your system assets or services has been compromised. This is not the time to try and identify what the impact of that is. You need to have a system already in place that can identify what the likely scope and nature of the impact is for any given service or asset.

Using the information, you will need to identify:

  - Who has been affected
  - The nature of the data involved
  - The risk the breach poses to those people

- Notification / Communications

  There is a requirement to notify the ICO (Information Commissioners Office) within 72 hours of a breach if the breach has the potential to impact the data protection rights of individuals. The individuals impacted will need identifying and notifying as well.

  Both of these requirements need to be part of the breach management process and as they have time limits attached your breach process needs to be time driven. You need clear indication of where you are in the time line with escalations and notifications to the Security management team where these time limits are getting close.

- Remediation

  Now you need to turn to remediating the issue that led to the breach. This could be a change in process, software or infrastructure. The key element is that the remediation process also needs to be managed and ideally managed in a way that directly links it back to the breach and its impact.

- Audit Trail

  Throughout this process you need to keep a clear and reportable audit of your actions, decisions and communications. One of the key elements in the subsequent investigation that the ICO and possibly the police will take, is to identify if you have fulfilled your obligations. You need to be able to provide detailed records detailing the actions/decisions including the reasons for those decisions.

Conclusion

The key takeaway is that perpetration is key. During a Security event there simply isn't time to invent processes, identify impacts or implement management procedures. You need to have all that set up in advance in a way that allows you to easily activate the required processes and provides the management information you need.
In an ideal world such a security incident management system should manage everything from capturing the initial security events, allowing escalation to full blown security incidents, provide ready canned process flows and notifications and most importantly be available even if your infrastructure is compromised.

For more information on how Simplisys' Service Desk software enables you to manage this process and comply to the regulations do not hesitate to contact Simplisys.

References

The full text of the GDPR