Adopt Robust Breach Detection and Meet One of the Key GDPR Requirements

CounterCraft

Executive Summary

With the enforcement of the GDPR just around the corner, organisations are devoting a lot of time on what they need to do to comply. This white paper does not cover that. Instead, we'll focus on some of the components of this new law that the majority have so far overlooked. The regulation, in its article 83 and in the data breach context, refers to the need for organisations to ensure that they have robust breach detection and investigation mechanisms in place. It is a deception solution that enables organisations to enhance their ability to detect the presence of threat actors within their global network environment, delivers a detailed targeted threat intelligence stream to aid incident response, and provides insights into what tools, tactics and procedures have been used against them.

Deception is an effective mechanism for early threat detection and luring attackers away from the production environment into a highly engaging synthetic environment, thereby reducing their chances of accessing business-critical data assets. This proactive approach to protection enables organisations to strengthen existing risk management strategies and reduce the probability of a breach, not to mention the associated reputational impact. Many consider data breaches solely in terms of regulatory costs and short-term damage to share prices. This approach overlooks the cost of business disruption and the subsequent loss of revenue.

The CounterCraft Cyber Deception Platform provides a sophisticated layered approach to threat intelligence which has been designed to keep pace with the ever-evolving threat landscape.

The solution significantly enhances an organisation's breach detection and investigation capabilities, without the need to deploy an army of analysts or becoming buried under an avalanche of alerts dependent on human analysts to decipher what is important and what is not. Significant cost savings and advanced functionality aside, the CounterCraft Cyber Deception Platform delivers client specific threat intelligence, revealing in clear, unambiguous terms what operations are being executed against your organisation. It's real-time intelligence and it's immediately actionable, eliminating the need for manual intervention. As a result, the SOC team and threat analysts are able to operate with much greater efficiency and focus their efforts on the complexities that contribute towards improving overall security posture.

If you want to

- ☑ Enhance your breach detection and investigation ability in line with the GDPR requirement
- ☑ Reduce significantly the risk of a data breach
- ☑ Obtain actionable intelligence specific to your organisation
- ☑ Be able to share that intelligence with your existing security tools
- ☑ Identify what data assets threat actors are really interested in
- ☑ Identify insider threats
- ☑ Reduce costs while significantly enhancing your security posture

Then, you need to know more about CounterCraft Cyber Deception Platform.

Introduction

Many papers and conferences have already dealt with the topic of The General Data Protection Regulation (GDPR) which came into effect on the 25th of May 2018. The intent of this paper is to shed light on a very specific component of the new regulation: article 83 (A83) explains the guidelines that regulatory authorities will follow when dealing with data breaches.

One inescapable truth is that it's not a question whether you will be breached or not. The simple dominant trend is a year-on-year growth in the number of data breaches occurring. The 2017 Verizon Data Breach Investigations Report tracked 2,216 data breaches across 65 different countries. Very close attention needs to be given to A83 and what organisations need to do under this article. So, let us begin by taking a look at the high level requirements of GDPR, before digging deeper into A83.

What is GDPR?

The General Data Protection Regulation (GDPR) will supplant existing data regulations by introducing a more stringent framework for handling and processing data that is of a personal nature. This directive protects EU citizens' personal data and therefore represents a significant challenge for global organisations that store, handle and process data associated with EU citizens, regardless of whether they're in fact based there.

What is Personal Data?

This is any information relating to an identifiable person. It's worth noting that the GDPR now includes IP addresses and cookie identifiers in the definition of 'online identifiers'; the key point being is that this information could be used to trace an individual and create a profile of them when combined with another unique identifier and data received by the server. Whether or not data is deemed to be personal will depend on the context in which the data is collected. For example, if you have a website and you ask users to state their occupation, this does not fall within the definition of personal data. Why? Because there will be many others who also have that particular occupation. However, if in addition you collected the user's name, these two datasets would now mean that the GDPR applies. Below is a short and illustrative list of datasets that either individually, or combined with other datasets, can be construed as personal data:

- Looks, appearance and behaviour
- Salary, tax, and student information geo-tracking data
- Medical history including sick leave

A simple and pragmatic approach would be to err on the side of caution–if you are unsure, assume by default that data is personal and handle it according to the requirements set out in this new law.

Who Does GDPR Apply to?

The GDPR applies to **'controllers'** and **'processors'**. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved–the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR. The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

CounterCraft Cyber Deception Platform

The major benefit that the CounterCraft Cyber Deception Platform brings to an organisation is the ability to significantly reduce the risk of attackers going undetected having infiltrated the corporate network. The longer the threat actors lurk, the greater the probability that they will identify key company data and asset information they want to extract. In terms of managing your risk exposure to data breaches and regulations, the CounterCraft Cyber Deception Platform has the capacity to significantly bring your risk exposure down to a manageable level. But how is this achieved?

CounterCraft provides a pioneering solution to distributed deception that protects businesses all over the world by fooling their adversaries with decoy computers, false data, and fake identities.

Key Provisions of GDPR

1.Global Organisations

GDPR will apply to organisations that are based outside of the EU, but are processing personal data that relates to EU citizens. A very important aspect of this is that it's irrelevant whether payment is required for the goods or services that are being offered. Many organisations have assumed that the law only applies if they are selling goods or services, but quite simply, if you are offering a free application that requires users to register before they can download it, then you fall within the ambit of the legislation.

2. Data Breaches

The GDPR imposes a strict obligation on all organisations that fall within its scope to report certain types of personal data breaches within 72 hours of becoming aware of the breach, where feasible. In the UK, the Information Commissioner's Office (ICO) will launch a special hotline that can be called to engage with and get advice from the ICO in the event of a suspected breach. The following example is provided by the ICO to help organisations understand when they would and would not need to inform the ICO of a data breach:

"The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list."

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

Article 83 and data breaches

The following is a paragraph taken directly from the ICO in the context of data breaches.

Source:http://www.privacy-regulation.eu/en/article-83-general-conditions-for-imposing-administrative-fines-GDPR.htm

"You should ensure you have ***robust breach detection, investigation*** *and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals."*

This is an interesting statement when combined with A83, which provides guidelines for imposing fines for those who are found to be in breach of the GDPR. These guidelines refer to the fact that actions taken to mitigate damage to data subjects shall be taken into consideration before the imposition of any fine. There are two levels to this fine, described as a lower and upper level:

*"**Lower Level:** Up to €10 million, or 2% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements of:*

***Upper Level:** Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements of: "*

From the outset, it is important to acknowledge that no particular technology sets are being mandated in the regulation, but what organisations are being asked for, (and I am paraphrasing here,) is that they can demonstrate that they have **breach detection and investigation in place**. So, how can deception technology, and in particular the CounterCraft Cyber Deception Platform, help you as an organisation demonstrate to data protection agencies that you have complied with this requirement?

It is important to note that CounterCraft is not only relevant in the context of the GDPR, but to any data breaches of any kind will result in heavy financial costs on an organisation.

The total running costs of headline breaches from 2017 and 2018 are astronomical. This tells us that aside from any liability that may have existed under the GDPR had it been in force, there is a compelling reason for organisations to examine alternative and more advanced technology to help minimise the risk of incurring the huge financial loss and reputational damage that comes with a data breach. One must not also overlook the fact that there is a whole raft of indirect losses that aren't factored in or reported on, including brand damage, loss of revenue and disruption to doing business.

GDPR & Deception

Deception campaigns appear to process and collect personal data, and many have asked whether the GDPR hinders the deployment of such technology. The relevant provisions are contained in what is referred to as 'recitals'; these are not enforceable in the same way as regulations but have been included to help with the interpretation of the relevant regulation. Recitals are intended to be read in conjunction with the relevant regulation that they apply to, and in this instance, it is Recital 49 that states that processing:

1) Is performed "to the extent necessary and proportionate for purposes of ensuring network and information security", such as ensuring that the confidentiality, integrity and availability of the personal data stored or transmitted and the security of the related systems is preserved, and

2) Constitutes a legitimate interest of the data controller, such as preventing unauthorised access to electronic communication networks and malicious code distribution or "denial of service" attacks.

Therefore this regulation can be interpreted to confirm that processing personal data is allowed in the context of deploying a security asset that protects personal data and prevents unauthorised access to networks.

It is worth considering what drove the need for such regulations in the first instance. The working groups that have drawn up the legislation did not design the regulation to reduce organisations' capability to identify and stop threat actors from hacking networks and stealing data. It is important to remember that the GDPR has come into force with a focus on protecting lawful users going about their everyday business online as a result of technological advancements and incompatible jurisdictions across the EU.

Conclusion

Due to the complexity and diversity of the threat actors targeting corporate infrastructure, organisations need to vastly improve their ability to not only detect breaches, but to anticipate unknown attack surfaces. Dependency on human analysts and manually processing high volumes of alerts is not only resource intensive but costly. There is a clear business need for automated deception platforms that identify how potential attackers will leverage your infrastructure against you, and what tools and techniques they will deploy in order to get to your critical business assets. GDPR is placing the onus very much on businesses to ensure that they have **robust breach detection and investigation** measures in place.

A failure to do so not only exposes organisations to potential liability under GDPR, but equally as importantly, it runs the risk of incurring significant direct and indirect costs associated with data breaches. CounterCraft Cyber Deception Platform allows businesses to:

- ☑ Identify potentially vulnerable infrastructure
- ☑ Deflect threats into synthetic environments
- ☑ Acquire targeted and actionable intelligence
- ☑ Strengthen their infrastructure against targeted attacks
- ☑ Obtain relevant and detailed reporting on attack trends
- ☑ Deploy security resources and budgets more efficiently

All of this can be achieved with fewer resources by using the CounterCraft automated deception technology. The threat landscape is constantly evolving and shifting on a daily basis. CounterCraft operates around an advanced modular infrastructure that launches dynamic deception campaigns in response to the latest threats and delivers highly accurate management information without disrupting business' activity. As a result, businesses are in a stronger position to stay aligned with targeted threats, eliminate wasted resource, and focus their security spend where it's most needed. Longer term, the CounterCraft solution has been proven to reduce overall security spend, drive greater efficiency, and improve security posture.

For more information contact our security crafters at **craft@countercraft.eu**

About CounterCraft

CounterCraft is a pioneering cyber security company that provides active defense to large enterprises by the use of cyber deception and counterintelligence. The Cyber Deception Platform detects targeted attacks and brings trustworthy alerts and real-time active response. Award-winning, the company was founded in 2015 by an experienced executive team. Headquartered in San Sebastian and with offices in London, Madrid and Los Angeles, its solution is used by Government, Law Enforcement Agencies, and Fortune500 companies. CounterCraft is backed by leading VC firms and operates globally.