DATA SECURITY UNDER GDPR: HOW TO PREPARE FOR THE INEVITABLE
The European Union’s (EU’s) General Data Protection Regulation (GDPR), which takes effect on May 25, 2018, dramatically increases the penalties for failing to properly protect users’ personal data. The maximum fines that can be leveraged against an organization eclipse penalties that have been imposed in the past; they could be as high as 4 percent of the offending company’s global revenue or 20 million euros, whichever is larger.

In spite of the high stakes, GDPR provides companies with little guidance on how to comply. But that’s no reason to panic. The upside is that companies that have been found to be non-compliant with the regulations have the ability to reduce the fines they face, or avoid fines altogether, by demonstrating they have made good decisions around handling personal data. This is particularly true in the case of potential data breaches.

Proactive and well-thought-out data protection policies and practices can help fortify an organization not only against GDPR penalties, but also against the legal and reputational consequences that data breaches may entail. Thus, shoring up processes around data loss prevention and threat detection are more important now than ever.

In developing data protection policies, organizations need to keep the following three key points in mind:

- Intrusions are inevitable.
- Security architecture may require pseudonymization and segmentation.
- State-of-the-art security is key.
There are no guarantees in the data protection business. As IT security firms continue to improve corporate defenses, criminals work tirelessly to stay one step ahead. Cyber criminals are increasingly creative, and the incentive to innovate is huge.

The velocity and complexity of attacks today mean that no matter how much a company spends on IT security, it can only reduce the likelihood that a criminal will get into corporate systems, not fully eliminate the possibility of an intrusion. Therefore, in addition to dedicating resources to threat prevention, organizations should consider ways to shrink the criminal’s window of opportunity in the event of an intrusion.

On average, a cyber criminal who breaches a corporate network has 65 days to wreak havoc before the intrusion is detected. The longer this window of opportunity is open, the more time the criminal will have to search for, find, and steal important data. Conversely, the more quickly a company identifies a threat, the more likely it is to mitigate, or even prevent, data breaches.

Part of a company’s IT security program needs to focus on minimizing the length of time between a data breach and its detection and remediation. IT security directors need to:

---

UNDERSTAND THE DATA YOUR COMPANY COLLECTS AND STORES

Every organization should closely examine what personally identifiable information (PII) it collects or otherwise handles. Does any of this data belong to an EU resident? If so, the company should determine whether it is using that data for the purposes it originally intended, and whether it must continue collecting or storing that information.

If the answers to these questions are yes, then the organization needs to understand where it stores individuals’ personal data, how it protects that data, and how that information moves among corporate systems, as well as how the information is transferred to third parties, if it is.

PREPARE FOR THE INEVITABLE

If a company discovers a personal data breach subject to GDPR, it has 72 hours to report the event to the appropriate supervisory authority, unless the personal data breach “is unlikely to result in a risk to the rights and freedoms of natural persons.” This means that within three days, the company must determine whose PII was affected, what aspects of their PII were exposed, and the degree to which the breach is likely to impact those individuals.

Reporting requirements are amplified when a personal data breach “is likely to result in a high risk to the rights and freedoms of natural persons.” In that case, the company must also communicate about the breach with the EU residents whose data was affected.

To meet these obligations, an organization that discovers a data breach must very quickly determine which systems the hacker touched. This usually involves examining network traffic and checking individual devices and applications.

---

2 General Data Protection Regulation, Article 33: “Notification of a personal data breach to the supervisory authority.”

3 General Data Protection Regulation, Article 34: “Communication of a personal data breach to the data subject.”
In addition to compiling the information needed for the data breach notification, the IT team needs to root out how the criminal got into the network. Doing so helps prevent future breaches, and helps the IT security team ensure the attacker does not still have an access point into the network. It’s also crucial for the company to fully understand both the purpose and impact of the breach in order to instill confidence in the information the company is reporting to its relevant data protection authority (DPA) and/or the individuals whose data was affected. Alternatively, if the company is not reporting the data breach externally, it needs complete confidence that the incident meets the GDPR criteria for not reporting.

Regardless, speed of response is critical. In fact, companies that respond very quickly to a cyber criminal’s exploit on their network may be able to contain the threat so well that they minimize the incident’s possible GDPR impact.

Businesses need to have thoroughly documented incident response plans that cover procedures for both detecting and understanding network intrusions. They need to determine who will be involved in these processes in the event of a data breach. In most cases, breach responses involve the IT security director, corporate counsel, and an executive or board member. The latter is tasked with making the final decision about the company’s public reaction.

Then, like all cybersecurity processes, threat detection and response plans need to be tested on a regular basis.
ENSURE BACKUP AND RECOVERY SYSTEMS AND PROCESSES ARE IN PLACE

Solid backup and recovery for all key corporate systems is another necessary element in preparations for a potential network intrusion. Recovered files may be helpful in tracing an attack back to its point of origin. And they may be invaluable in the event of a ransomware attack, in which the criminals threaten to permanently destroy encrypted and exfiltrated company data unless they receive a ransom payment.

ENSURE SYSTEMS AND PROCESSES ARE COORDINATED ACROSS THE ENTIRE ATTACK SURFACE

Strong threat prevention and detection capabilities demand that information, plans, and processes be coordinated across the corporate network. Complexity and disjointed systems undermine the organization’s ability to find and respond to security breaches—particularly in a network’s security infrastructure. The situation is exacerbated if threat intelligence updates come from multiple vendors. One system’s patch might stop a particular exploit today, while another system’s security alert takes a few weeks to catch up.

One of the most important steps an IT security director can take in preparation for a potential security breach is to evaluate the level of integration among the security systems the company has in place. Many companies run a hodgepodge of security technologies, each of which performs a specific function within the security infrastructure. The problem is that these systems are not designed to work together. When technologies don’t communicate, the IT team has a silo-based view of threats and lacks transparency across the entirety of the attack surface. Having to aggregate data across systems takes time, and gaps can occur in the analysis.

In such an environment, hackers may be able to exploit the gaps in visibility between systems. And if a data breach is detected, scattered data and systems amplify the difficulty of determining whether the breach meets GDPR reporting criteria. For all of these reasons, companies need an IT security infrastructure in which systems share threat information and deliver transparent visibility in real time.
In addition to evaluating the degree of integration among security systems throughout the network infrastructure, IT security directors preparing for GDPR need to consider whether, and how, data is encrypted and stored on the corporate network.

Some organizations choose to protect personal data by anonymizing it, a process that permanently deletes personally identifiable information. For example, a healthcare organization could strip patient names off records so that the medical data could not be tied to an individual. This is an effective way of removing PII for IT security purposes, but it’s obviously problematic if the company needs to access the information in the future. Data that has been anonymized can never be restored to its original state.

An alternative is pseudonymization. As the name suggests, this process replaces personal identifiers, such as names, with a string of reversible, consistent characters that serves as a pseudonym. A separate file serves as a key, correlating each personal identifier with the pseudonym it has been assigned. If a cyber criminal were to access a pseudonymized medical record, nothing in that medical file would tie the patient data to a specific individual. The hacker would need to also access the key file to gain the personal identifiers.
PSEUDONYMS ARE CRUCIAL TO MORE CONVENIENT SECURITY

In fact, GDPR specifically calls out pseudonymization as one of the “appropriate technical and organizational measures [companies can take] to ensure a level of security appropriate to the risk.” Pseudonymization also demonstrates to the relevant DPA, in the event of a data breach, that the company has made a significant effort to minimize the impact on the owners of the data. Reporting requirements under GDPR are less onerous for companies that use pseudonymization than for companies whose PII is stored in plain text, because pseudonymization minimizes the likelihood of loss of personal data.

NETWORK SEGMENTATION KEEPS KEYS OUT OF REACH

After a company has created a file that can serve as the key for a set of pseudonymized records, the next logical step is to separate the key from the records by putting them on separate segments of the network. To further increase the protection of these files, the organization should add security to the network segments, deploying firewalls internally to prevent a prospective hacker from moving laterally between segments.

As an example, a company might store employee records in the HR department but use pseudonymization so that none of those records can be tied directly to an individual. It might then store the key that connects pseudonyms with employee names in the finance department, and place a firewall on the internal network between the two functions. Even if a criminal gains access to the segment of the network that contains HR records, that person will not be able to connect the dots without also accessing the finance segment of the network. And the internal firewall will significantly inhibit the ability to move between these two network segments.

4 General Data Protection Regulation, Article 32: “Security of processing.”
The language of GDPR also encourages companies to incorporate state-of-the-art security technologies. Article 25 begins: “Taking into account the state of the art ... the controller shall implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles...”

The rule does not define “state of the art,” other than specifically calling out pseudonymization. Clearly, which technologies qualify as state-of-the-art will evolve as the IT security market evolves. For now, it’s fair to assume that organizations need to ensure their security environment uses modern technologies to protect data that’s at rest, in use, and in motion.

Just as it undermines threat detection efforts, complexity is also the enemy of state-of-the-art technology. Individual security products cannot reside in silos. Integration is crucial to effectiveness in an IT security infrastructure, and it is crucial to meeting GDPR’s state-of-the-art requirement. Likewise, automation of threat mitigation activities is crucial both to keeping the company secure and to meeting GDPR’s requirement for state-of-the-art technologies.

Continuous risk assessment is also necessary. Solutions that automatically incorporate information about emerging threats reduce the risk of data theft while also reducing the risk of fines should a breach occur. Thus, security solutions and services need to incorporate continuously updated threat intelligence in an attempt to stay a step ahead of cyber criminals.
Until GDPR takes effect, no one really knows how the individual countries will enforce these guidelines. The UK Information Commissioner’s Office (ICO) offers some excellent resources, including a recent blog post by Information Commissioner Elizabeth Denham that says, “it’s scaremongering to suggest that we’ll be making early examples of organizations for minor infringements or that maximum fines will become the norm.” While GDPR will be the “law of the land,” focused on the objective of data protection rather than detailed technology analysis, it will place the spotlight on all aspects of an organization’s security posture and philosophy.

Now is not the time to panic. Now is the time for every company around the world that touches personal data of EU residents to re-evaluate its IT security infrastructure. Are the technologies state of the art? Does the network include sophisticated data-protection measures such as threat prevention and detection, pseudonymization and internal segmentation? Has the data-breach response plan been documented and tested? And are all the IT security solutions communicating in a way that optimally protects data and provides network-wide visibility?

IT security directors who can answer “yes” to all these questions are well on their way to being prepared for the inevitable.

---

6 Information Commissioner’s Office (ICO)
7 Elizabeth Denham, “GDPR—sorting the fact from the fiction,” August 9, 2017.