GDPR with Deceptive Technology Perspective

What is GDPR and Why Should Businesses be Concerned?

GDPR is The General Data Protection Regulation which will radically change the data usage and protection landscape when the document comes into force on May 25th, 2018. This European legal framework will hold any business collecting, controlling, or processing EU personal data (including the UK for the time being) accountable to safeguard it. Businesses that do not comply will risk potentially crippling penalties of up to €20m or 4% of its annual turnover. The Payment Card Industry Security Standards Council has reported that had the GDPR been in effect during 2015, UK organizations would have been fined a cumulative total of about £122 billion in 12 months. Data security and data privacy will require a new set of practices. Businesses should not be surprised if other countries soon follow suit given the amount of personal data processed throughout the world daily.

We live in a world where personal information is shared at an astonishing pace through social media, online shopping, and marketing. The goal of GDPR is to protect this information and require a demonstration of compliance with protective measures. However, traditional information security systems have repeatedly proven to be inadequate, with most companies in the US and EU at risk of a breach and exposed to substantial violations and penalties; just reference the latest high-profile businesses to fall victim to a breach (Equifax, Yahoo, Forever 21, Kmart, Uber, Anthem). Breaches are on the rise and show no signs of subsiding unless there is a material change in how organizations approach security defenses. A prevention-only approach to information security is simply not adequate or reliable, and attention and investment must shift to an active defense that includes detection and response. ESG Master Survey Results have reported that only 11% of organizations in North American and Europe believe they would be fully compliant if GDPR went into effect tomorrow. Businesses that heed this GDPR call to action and shift from a posture of compliance to a spirit of embedded security design will not only avoid heavy fines, but create an organization that has improved processes, systems, and efficiencies that are compliant, measurable, and built for actionable security breach response. Businesses can no longer rely on traditional reaction-based defenses such as data loss prevention, spam filters, and firewalls. The need will shift to a proactive defense that is built for early detection and efficient response. Deception-based cybersecurity will be a crucial tool in an active defense toolkit to secure Personal Identifiable Information (PII) while meeting GDPR regulations.
Where are Businesses Most Vulnerable With GDPR?

Article 33 – Notification of a personal data breach to the supervisory authority

The regulation states: “In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55.” “A ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

Previous directives from the EU 95/46 made no specific mention of data breaches. GDPR sets a clear directive as to what constitutes a data breach, how the incident is to be reported and the substantial penalties for not complying. Businesses will need to evaluate their technology and processes to assess their ability to detect, audit, and report breaches to comply with GDPR. Closing the gaps will, in many cases, require the adoption of new technology to ensure that the attack is not only detected but also understood in a way that can explain the magnitude of the breach and the corrective actions to contain it.

The notification of the breach must include:

- Nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and number of personal data records concerned;
- Communicate the name and contact details of the data protection officer from whom more information can be obtained;
- The likely consequences of the personal data breach;
- The measures taken or proposed by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Based on the clear expectations outlined in the GDPR, it is expected that most organizations will need to take additional measures to implement the safeguards and systems required to comply and report breaches. The implications of a data breach and potential penalties as outlined will be material and are designed to far outweigh the investment that an organization would have needed to invest to support compliance with these requirements.

Deception Technology can help organizations prepare for GDPR Article 33 by providing a powerful security control for an active defense through early and accurate threat detection. Deception technology can be valuable in obfuscating the attack surface with deception traps and lures, making it difficult for an attacker to decipher what assets are real and which ones are fake. Credential deceptions can also play a crucial role in directing attackers to deception servers where an attacker will reveal their presence as they look to interact with an engagement server. Once engaged, the deception server will safely study the attack and provide detailed information on tools, techniques, and procedures used by the attacker. Additionally, the full indicators of compromise are collected, providing additional adversary intelligence that can be used to strengthen defenses. Data deceptions can also be extremely valuable in gaining counterintelligence on what the attacker was seeking to steal and information from beaconing technology, which will tell the location of stolen files.

Integrations with 3rd party prevention tools like firewalls, SIEMs, NAC, and EDR solutions can be set up for information sharing and the ability to automatically block, quarantine, and threat hunt. This can be used to support demonstration of preventing adverse effects.
Article 25 – Data protection by design and by default

One of the key initiatives brought forth by GDPR relates to “Privacy by Design” along with “Privacy by Default”. Businesses will now be required to integrate data privacy during all stages of design along with the entire lifecycle of the relevant data. This will be a new mindset for most businesses with a start-to-end process, minimizing the amount of data needed, using data for only the intended purpose, and destroying the data at the end of the cycle. There will be much-needed transparency with customers, partners, and regulators.

Privacy by Design (a concept developed by Ontario’s former Information and Privacy Commissioner, Dr. Ann Cavoukian, in the 1990’s,) has seven key principles:

• Proactive not reactive – privacy from the start
• Privacy as the default setting – data must be private
• Privacy embedded into the design – data must be secured using encryption and pseudonymizing (replaces identifying fields with artificial identifiers)
• Full functionality – positive sum, not zero sum where there are no unnecessary trade-offs such as privacy versus security.
• Full lifecycle of protection from end to end security – retention limits, “right to be forgotten”
• Transparency – data use must be disclosed and accessible – “right to access data”
• Respect for user privacy – data must be used only as agreed

Businesses must anticipate, prevent, and detect perpetrators before they can complete their mission. With an ever-changing onslaught of attacks and an evolving attack surface, it is critical for organizations to prevent what they can by backing this with tools that provide early and accurate detection, helping organizations understand and anticipate where the weakest links in their security infrastructure are. Deception technology plays a key role in building a proactive vs. reactive security posture and can play an instrumental role in turning the game against the modern-day perpetrator.

First, deception technology provides a proactive threat defense of traps and lures designed to deceive attackers into revealing themselves early in an attack cycle, reducing dwell time. Deception plays a unique role in that it can proactively entice an attacker into revealing themselves vs. waiting for set behaviors to attempt to discern wrongful behavior. Second, since deception is engagement-based, each alert is substantiated with attack analysis and forensic reporting that includes the full tactics, techniques, and procedures (TTP) of an attack and the indicators of compromise (IOC). Through 3rd party integrations, information is shared to strengthen defenses and accelerate incident response with automated blocking, isolation, and threat hunting.
Privacy by Default requires further protection by only using data required for the task at hand. Protective controls must be built into all processes and systems, so data remains private and secure from being compromised and breached. The controller shall:

- Implement appropriate technical and organizational measures such as pseudonymizing and data minimization in an effective manner to protect the rights of data subjects.
- Implement appropriate technical and organizational measures for ensuring that, by default, only personal data necessary for each specific purpose are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Organization’s using deception credentials should verify with their provider their ability to anonymize deception names. Being transparent at the end-point is core to authenticity, however, established providers design for GDPR compliance and will provide pseudonymized data for reporting and in compliance with Data Across Borders requirements.

**Article 32 – Security of processing**

Article 32 addresses implementation of technical and organizational measures to ensure the ongoing resilience of the processing systems and services. Businesses must have the ability to restore the personal data in a timely manner in the event of a physical or technical incident. There must also be a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Deception Technology provides an ongoing active defense for the early detection of in-network threats and their lateral movement. Additionally, deception platforms that provide network visibility and attack path assessment tools can lend to the comprehensiveness of a program for continuous risk assessment and vulnerability monitoring.

Deception technology has also become a de facto tool for demonstrating security resiliency during penetration testing. Snaring a red team during a pen tester and being able to document their actions is a widely proven approach for demonstrating the efficacy of an organization’s security controls.

"We did a red team test and my team came back and said, WOW! This thing (Attivo Networks Deception) is good. It kept our red team busy for a long time!"

*Snr Director Info Sec at Fortune 50 Retailer*

Organizations have also benefitted from deploying deception platforms to detect and slow ransomware attacks. By planting mapped shares, malware is directed to an engagement server where it is fed reams of fake data to encrypt. This engagement reveals the presence of an attack and efficiently isolates the infected system from the network while slowing the attack. Testing has recorded a 25X slowing factor of the ransomware attack using this approach.

Additional information on how deception was used to derail ransomware: [WannaCry attack analysis research by Attivo Labs](#).
Attivo Networks Deception Technology for GDPR Compliance

GDPR is an extensive regulatory framework and all businesses with PII from EU citizens must take proactive measures to protect their customers, employees, third-party relationships, and to mitigate the risk of being fined. Company security policies must address the following factors and be able to quickly and accurately alert on security policy violations:

- How is data collected?
- Where is data stored?
- How secure is our data?
- How is data transferred/processed?
- What is the scope of our data (how many records)?
- Is our data encrypted?
- With whom is the data shared?
- Who can access the data?
- How are we monitoring the data?
- Would we be able to detect a breach of our data?
- How is the data destroyed?

The Attivo Networks ThreatDefend™ Platform can play an active role in a GDPR compliance plan when embedded into an organization’s security policies and used for early detection of, and response to, threats. Cybercriminals are constantly advancing their strategies and tactics, but by design, the Attivo deception technology is built for an evolving threat landscape and attack surface. Deception has been a part of a successful warfare strategy throughout history (think of the Trojan Horse), so it makes sense to carry this tactic to the cybersecurity battlefield. This technology uses realistic decoys, lures, deception files hidden as goldmines, and a deception grid designed to baffle and derail perpetrators. By using “smoke and mirrors” the attackers waste time and money chasing deceptions and tripping virtual landmines that alert to their presence. The Attivo ThreatDefend platform provides an active defense that not only uses deception to set traps but also proactively entices an attacker to reveal their presence. Once the attacker is engaged, the system’s attack analysis engine records attacker movement and gathers the threat and adversary intelligence required to substantiate the attack and record the information for compliance and forensic reporting. Extensive 3rd party automations make it fast and efficient to automate the incident response to an attack. Based on security policies, attacks can be automatically blocked, quarantined or threat hunting activated to stop the attack and to demonstrate that corrective action has been actively taken.

Summary

As the time comes upon us for GDPR compliance, businesses must ask themselves, “Can I demonstrate that my organization has the necessary controls in place?” Am I able to monitor user behaviors and investigate abnormalities quickly? Under GDPR not only will businesses be held to these regulations, but individuals will have the ability to sue organizations that cause material or non-material damage due to a breach of personal information. In preparation for the initial launch and for ongoing compliance, it is time for organizations to objectively assess their readiness and to invest in solutions that protect PII data across all channels, devices, location, networks and cloud storage. The Attivo Networks ThreatDefend Platform is globally proven for delivering early detection and accelerated incident response. The solution’s approach to an active defense will play a key role in GDPR readiness by detecting breaches early, understanding attacks with threat-, adversary-, and counterintelligence, along with the reporting and automation to demonstrate that the attack has been properly addressed. Network and attack path visibility tools and the inclusion of deception during penetration testing will also be instrumental in building a proactive defense and demonstrating security controls resiliency. All, ultimately lowering your risk of attack, further protecting your business from costly fines and disruption to business and preserving your organization’s reputation.