RAPID7

EU GENERAL DATA PROTECTION REGULATION (GDPR):

10 THINGS TO HELP SECURITY TEAMS PREPARE

The EU GDPR is one of the biggest changes in data privacy regulations. Here is what Security Teams need to know before the changes are enforced on May 28, 2018.

EU GENERAL DATA PROTECTION REGULATION (GDPR): 10 THINGS TO HELP SECURITY TEAMS PREPARE

The General Data Protection Regulation (GDPR) regulates the privacy and handling of European Union (EU) citizens' personal data. GDPR replaces the existing EU Data Protection Directive, and unifies data protection laws across the EU with a single set of rules. Securing, monitoring and protecting the systems and applications that process and store personal data are key to GDPR compliance, and security teams and incident responders all have a part to play.

1. Pen tests are your friend. If you've never had one done, or it's been a while, this is a great place to start when preparing for GDPR. Attacking your systems and environment to understand your weak spots will tell you where you need to focus, and it's better to go through this exercise as a real-world scenario now than wait for a "real" attacker to get into your systems. You could do this internally using tools like Metasploit Pro, and you could employ a professional team to perform regular external penetration testing services as well. Article 32 says that you need to have a process for regularly testing, assessing, and evaluating the effectiveness of security measures. Read more about penetration testing in this toolkit.

2. Encrypt data, both at rest and in transit. If you are breached, but the Personal Data is in a render unintelligible to the attacker, then you do not have to notify the Data Subjects (see Article 34 for more on this). There are a lot of solutions on the market today—have a chat with your channel partner to see what options are best for you.

3. Have a solid vulnerability management process in place, across the entire ecosystem. If you're looking for best practice recommendations, take a look at our blog post. Ensuring ongoing confidentiality, integrity, and availability of systems is part of Article 32. If you read Microsoft's definition of a software vulnerability it talks to these three aspects.

4. Backups. Backups. Backups. Please take backups. Not just in case of a dreaded ransomware attack, but because they are a good housekeeping facet in case of things like storage failure, asset loss, natural disaster, even a full cup of coffee over the laptop. If you don't currently have a backup vendor in place, Code42 has some great offerings for endpoints, and there are a plethora of server and database options available on the market today. Disaster recovery should always be high on your list regardless of which regulations you are required to meet.

5. Secure your web applications. Privacy-by-design needs to be built into processes and systems; if you're collecting Personal Data via a web app and still using http/cleartext, then you're already going to have a problem. The latest General Data Protection Regulations require you to make code changes to your web forms and applications, so this is a good moment to ensure your SDLC is baking in security early in the cycle so you can find and fix issues faster.

6. GDPR standardises Personal Data Breach Reporting requirements, so now is a good time to review and update your Incident Response processes. If you need help setting up your incident response program, or you'd like to have a second pair of eyes review what you have today, we'd be happy to help. And if you are unlucky enough to find yourself in a potential breach situation, it's vital to engage with an incident response team. Accelerating containment and limiting damage requires fast action. Rapid7 can have an incident response engagement manager on the phone with you within an hour.

7. Detect attackers quickly and early. Finding out that you've been breached 5 months after the fact is an all too common scenario (current stats from Mandiant say that the average is 146 days after the event). If you don't know you're under attack, then you have no ability to mitigate damage. If you're in the same situation as the 60% of organisations that told us they have no way of detecting compromised credentials (which has topped the list of leading attack vectors in the Verizon DBIR for the last few years), you're more likely to find out way too late that an attacker was hiding in plain sight. User Behaviour Analytics provide you with the capabilities to detect anomalous user account activity within your environment, so you can investigate and remediate fast.

8. Lay traps. Deploying deception technologies like honeypots and honey credentials are a proven way to spot attackers as they start to poke around in your environment and look for methods to access valuable Personal Data. If you prevent a breach, you don't need to report back to the Supervisory Authority.

9. Ensure you can prioritise and respond to the myriad of alerts your security products generate on a daily basis. If you have a SIEM in place, that's great, providing you're not getting swamped by alerts from the SIEM and that you have the capability to respond 24x7 (attackers work evenings and weekends, too). If you don't have a current SIEM (or the time or budget to take on a traditional SIEM deployment project), or you are finding it hard to keep up with the number of alerts you're currently getting, take a look at InsightIDR—it covers a multitude of bases (SIEM, UBA, and EDR), is up and running quickly, and generates alert volumes that are reasonable for even the smallest teams to handle. Alternatively, if you want 24x7 coverage, we also have a Managed Detection and Response offering which takes the burden away, and is your eyes and ears regardless of the time of day or night.

10. Don't forget about cloud-based applications. You might have some approved cloud services deployed already, and unless you've switched off the internet it's highly likely that there is a degree of shadow IT (a.k.a. unsanctioned services) happening too. Making sure you have visibility across sanctioned and unsanctioned services is a vital step to securing them, and the data contained within them.

If you're looking for help with your GDPR security preparations please visit www.rapid7.com for more information or email us at info@rapid7.com