Web Application Security for GDPR

Solution Overview

RedShield Security Limited

Executive Summary

The General Data Protection Regulation (GDPR) considers data protection as a fundamental human right of an individual, which includes a "right to the protection" of their personal data. Anyone based in the EU, or anyone handling or targeting the personal data of an EU-based individual must have processes, technology, and automation to effectively protect personal data. Major provisions in the GDPR recommend or require various technological measures to protect personal data. The key GDPR data security requirements can be broadly classified into three categories: Assessment, Prevention, and Monitoring/Detection. Additionally, GDPR has stipulations, in order to meet the requirements, aimed at easing the administrative overhead of the security controls and increase the quality of protection.

Controller and Processor Security Requirements

Companies are having to assess whether they and their partners, suppliers and data processors are observing GDPR rules and have an understanding of exactly what security controls are being implementing. The penalties for non-compliance are substantial. Protection authorities able to levy fines for failing to comply with technical requirements up to the greater of €10 Million or 2% of annual revenue. Penalties are even more significant for failing to comply with key provisions as protection authorities can levy fines up to the greater of €20 Million or 4% of annual revenue.

Specific security requirements regarding all internet facing web-enabled applications accessed by employees or consumers must have industry standard tuned security controls such as a Web Application Firewall (WAF) and must be scanned and remediated using accepted industry standard for security vulnerabilities (e.g., OWASP and OWASP Top 10). Scans and remediation must first be completed prior to application launch. Post launch, and that scans will be conducted at a frequency that is appropriate for the relevant application, technology and data risk. Additionally, websites will implement and maintain accepted industry standard account and password management controls.

RedShield Security

RedShield Security offers complete vulnerability management for web-enabled applications, providing all of the tools, people and processes to ensure a secure outcome. With a history of assessing security risks and proven prevention of attacks coupled with rigorous monitoring and detection you can rely on RedShield.

Features:

- Software-*with*-a-Service - *we do it for you*
- Advanced Shield library addresses stateful business logic flaws
- No application code changes required
- Includes fully managed WAF and anti-DDoS
- Rapidly mitigate vulnerabilities discovered via scanning and penetration testing
- Full security operations service including Analysts and Engineers 24x7

Service Overview

Technical Risk Discovery & Management first requires effective risk discovery. RedShield includes weekly analyst conducted scanning of all web assets under management. These results can be supplemented by those discovered by 3rd parties via Scanning, Code Reviews, Penetration Testing, Threat detection feeds, Bug Bounties etc. Regardless of who found the issue, our analysts determine risk ratings and identify appropriate remediation options.

Web Application Threat Protection provides attack traffic visibility, DDoS and application misuse protection plus market leading application change tolerant threat mitigation. As a baseline RedShield places an expertly managed WAF in path.

With **Web Application Shielding** RedShield developers select and configure shields from RedShield's library (or develop new) to modify the application's security logic to mitigate specific code vulnerabilities. Due to our injection proxies this can be achieved without the need to modify the application source code. Whether buying time to design and remediate the application code in a managed fashion or when protecting 3rd party and legacy applications, where remediation is often not an option, this 'Shielding-AppSec' capability and approach is what makes RedShield globally unique.

Continuous Monitoring & Development by our team of analysts, engineers, pen testers and developers allows RedShield to stay in step with newly discovered vulnerabilities and exploits. The RedShield team is always watching because attacks can happen at any time and new risks are continuously discovered. Whenever a new vulnerability is released or an application issue discovered the RedShield team proactively takes action to assess the risk by understanding the problem and initiating corrective action.

Using Application Shielding To Satisfy Relevant EU GDPR Requirements

To ensure alignment, RedShield have implemented appropriate technical and organizational measures to ensure that a level of security, appropriate to the risk to any personal information it may collect or process are in place.

Our ongoing commitment to protecting the confidentiality, integrity, and availability of data and its processing systems is at the core of the service RedShield provide.

Principles

GDPR sets out a number of principles including:

> ***Article 5 : Principles relating to processing of personal data***
> *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing...using appropriate technical or organizational measures*

RedShield's primary function is to ensure that no unauthorized or unlawful processing of data occurs. RedShield's approach is to understand the vulnerabilities a system has and then shield them - fast. RedShield's fully managed "Software *with* a Service" model provides not only the technical controls but also expert staff and mature security operation processes to deliver secure web application publishing.

RedShield's Vulnerability Intelligence engine identifies and manages vulnerabilities that are discovered in web applications. Once flaws are identified traditionally the only way to remediate flaws is to modify source code on the server. With RedShield, Application Shielding code objects can be developed and placed external to the server and dynamically added to the application flow. Application messages and behavior can be transformed all without access to or modification of the source code.

RedShield can assist organizations to meet the GDPR requirements detailed in Sections One and Two of the GDPR:

Section 1: General Obligations

GDPR states:

> ***Article 25 : Data protection by design and by default***
> *The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed...*

In the context of web applications this can be interpreted as implementing fine grained authorization. Another related article is Article 29 which incorporates the idea of strong authentication:

> ***Article 29 : Processing under the authority of the controller or processor***
> *The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller...*

Many web applications have vulnerabilities related to authentication and authorization including;

- weak session management
- direct object reference
- cookie theft
- weak passwords

RedShield has a library of shield objects which can be customized for rapid deployment to mitigate all these types vulnerabilities while enforce strong authentication and fine grained authorization controls. This too is implemented without the need for access to or modification of the application code.

Section 2: Security of Personal Data

Section 2 of the GDPR states:

> ***Article 32 : Security of processing***
> *...the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *...*
>
> *(a) the ability to ensure the ongoing confidentiality, integrity and availability and resilience of processing systems and services*
>
> *...*
>
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing*
>
> *...in assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.*

RedShield not only provides Application Shielding but also provides Denial of Service (DoS) mitigation as a service. Application Shielding specifically addresses the requirement for confidentiality and integrity. The denial of service mitigation service alongside the distributed global architecture of RedShield ensures availability and resilience.

Vulnerability Intelligence in RedShield not only provides regular scanning for vulnerability discovery and management but also proactively tests deployed shields in the same manner as an attacker to ensure they are effective.

Account and Password Management Controls

Traditionally in the case where accepted industry standard account and password management controls are not implemented in the application the only way to address the issue is to modify the application source code. With Shielding, code objects can be developed and placed external to the server and dynamically added to the application flow. Application messages and behavior can be transformed all without access to or modification of the application source code.

RedShield is able to use this architecture to solve a vast array of problems, including the following password management requirements that are often missing from older and poorly coded applications:

1. Passwords must meet certain minimum complexity requirements related to length and character sets.
2. Passwords must be stored in a non-reversible form;
3. Users must re-authenticate after a period of inactivity;
4. Accounts should be locked after a number of unsuccessful login attempts;
5. User IDs, passwords and personal identifying information must not be displayed in a URL;
6. Passwords and personal identifying information must not be stored in persistent client side storage (eg web browser caches) or in cookies, Javascript or other web tracking technology.

If you'd like any additional information with regards to account and password management and our approach review the, RedShield WhitePaper, "*Account and Password Management using Application Shielding.*"

Advanced Shielding Options

Number 1: Password Complexity

RedShield is able to enforce password complexity requirements by rewriting the requests and responses that make up the login and password change functionality present in all web applications.

For example, RedShield can detect weak passwords on login attempts and redirect the flow of the application to force users to change their passwords. During this process RedShield can enforce complexity requirements. by rewriting server responses.

Number 2: Password Storage

Even if your application does not currently encrypt credentials RedShield can provide a customized advanced shield to migrate plain text credentials to a secure salted hash form.

- Prompts user to change their password.
- RedShield salts and hashes a password and passes to the server for storage.
- On subsequent logins RedShield hashes client supplied password, sends to the server for comparison.

Number 3: Inactivity Timeout

RedShield can maintain session state for users even if your application does not. RedShield user sessions management shield features include failed login responses, inactivity timeouts, hard timeouts and random session cookies.

Number 4: Account Lockout

On top of RedShield user session management shield features mentioned above, this statefulness allows for additional controls to be applied, so now for instance, offending IPs can be blocked if a threshold for a number of page requests within a specific timeframe is exceeded.

Number 5: No user IDs, passwords or personal information in the URL

Sensitive information can be removed from the URL easily as RedShield can rewrite server responses as well as user requests.

- Sensitive information is removed from the URL and associated with a random cookie
- RedShield maintains a table of cookies and associated information
- Information can be reinserted into the URL in the format the server is expecting upon subsequent client requests

This information now only passes between RedShield and the server and so does not leak to the outside world through proxy logs or client browser histories.

Number 6: No user IDs, passwords or personal information in persistent local storage

Information to be stored on the client locally can be rewritten and sensitive information can be removed easily as RedShield can rewrite server responses as well as user requests. Similar to sensitive URL parameters.

- Sensitive information is removed from the response and associated with a random cookie
- RedShield maintains a table of cookies and associated information
- Information can be reinserted into the response in the format the server is expecting upon subsequent client requests

This information is now only stored temporarily in RedShield memory and only passes between RedShield and the server.

Conclusion

Given the broad nature of the GDPR requirements it's clear that only a comprehensive and process driven approach to application security can be used to satisfy its provisions. GDPR will be among the most comprehensive information protection regulations released to date and it will usher in a new era of responsibility for organizations with respect to personal data. Failure to comply, followed by a data breach, carries with it a hefty penalty that looks to rewrite companies' commitments to personal data security.

With web applications still by far the largest entry point for data breaches, web application security has never been under greater scrutiny. Complete web application vulnerability management is built into the RedShield DNA. RedShield has been dedicated to this security as a process approach since its inception making it ideally suited to help companies prepare for and comply with the forthcoming GDPR requirements.

RedShield is the world's first and only web application shielding-with-a service cybersecurity company. The RedShield shielding-with-a-service offering combines superior web application shielding software with industry-leading cybersecurity services. Powerful vulnerability intelligence, exploitation research and a prolific database of known exploits that ensure fast vulnerability mitigation thereby minimizing exposure and costly remediation delays. RedShield is challenging the status quo in web application security and currently secures vulnerable applications for government agencies, banks, telcos, healthcare systems, power sector and eCommerce platforms around the globe, lowering costs and accelerating time-to-market.

We are ready to do the same for you…

References

For more information on GDPR and the notes in this document, refer to:

- EU Data Protection Page http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
- GDPR http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- RedShield's Privacy Policy https://redshield.co/privacy.html

Definitions

Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data...
Data Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person