RedShield's Approach to Information Security

White Paper
January 2019

Introduction

From more than a decade of testing networks for security weaknesses RedShield was formed to actively protect web applications from known attacks. This history in Information Security produced a company that has, from inception, been designed and operated to provide a secure service.

The RedShield founders and operational teams are aware of the complexity of this domain and make concerted efforts to elevate its client's levels of security. RedShield employs operating practices that safeguard its client's information whilst at rest and in flight. It operates in a niche area of cyber security and strives to work alongside its clients in a transparent and open manner, this way RedShield can be a trusted vendor in your cyber defence.

This article presents RedShield's approach to Information Security and gives an overview of some of the methods employed to secure its environment, and your data.

Organisational Security

RedShield has adopted best practice approaches and aligned with ISO 27000 standards in its management of the organisation. An ongoing audit programme ensures alignment to these requirements and that it is able to make continual advancements to established processes.

Personnel Security

All RedShield resources (contractors or full-time employees) comply with our organisations personnel practices, these apply to all people that have access to RedShield's internal information systems and / or unescorted access to RedShield's offices. All staff are required to understand and follow internal policies and standards.

Before gaining access to RedShield systems, all workers must agree to confidentiality terms, pass a background screening, and attend security training. Training covers privacy and security topics, including device security, acceptable use, physical security, data privacy, account management, and incident reporting. Upon termination of work at RedShield, all access to RedShield systems is removed immediately.

Security and Privacy Training

RedShield has developed a series of training courses, each developed specifically for RedShield staff, these map directly to our internal policies, Standards, and Guidelines. Annually staff complete a refresher of our core policies. Additional courses are required for staff that perform key roles in the organisation, for example Incident Response, or for those that work with Credit Card processing environments.

Our staff are required to report security and privacy issues using our processes to appropriate internal teams. Any failure to comply with acknowledged policies may result in consequences, up to and including termination of employment.

Security Resources

RedShield has defined roles and responsibilities in the organisation that are responsible for operating the various aspects of the Information Security Management System (ISMS).

With security as a core discipline every member of the RedShield team has responsibility for safeguarding our services and the operational environment. Central to the administration of the ISMS is the Chief Information Security Officer (CISO) who owns and is responsible for its management and enforcement, he is supported by the Information Technology Security Manager (ITSM) and representatives from each business division.

Infrastructure Team

This team are responsible for the following RedShield activities.

- Build and operate security-critical infrastructure including RedShield's public key infrastructure, event monitoring, and authentication services
- Maintain all environments patch and update levels
- Maintain a secure archive of security-relevant logs
- Consult with operations personnel to ensure the secure configuration and maintenance of RedShield's production environment
- Respond to alerts related to security events on RedShield systems
- Manage security incidents and vendor vulnerability notifications

Risk and Compliance

To respond to compliance requirements and to maintain a level of operational abstraction, RedShield utilise a dedicated Risk and Compliance Lead that concentrates on the following activities.

- Coordinate penetration testing
- Manage vulnerability scanning and remediation
- Coordinate regular risk assessments, and define and track risk treatment
- Manage the security awareness program
- Coordinate audit and maintain security certifications
- Respond to customer inquiries
- Review and qualify vendor security posture

Policies and Standards

RedShield maintains a set of defined policies, standards, procedures and guidelines that describe for the various teams how to fulfil their obligations in respect of security and the operation of RedShield's ISMS. RedShield security documents include the following.

- Acceptable uses of information systems
- Classification, labelling, and handling rules for all types of information assets
- Practices for worker identification, authentication, and authorisation for access to system data
- Secure development, acquisition, configuration, and maintenance of systems
- Workforce requirements for transitions, training, and compliance with ISMS policies
- Use of encryption
- Description, schedule, and requirements for retention of security records
- Planning for business continuity and disaster recovery
- Classification and management of security incidents

- Control of changes

RedShield has implemented a system to ensure that these documents are updated when necessary and are available to all employees (the RedShield Intranet hosts the core documents).

Third Party Audits

RedShield regularly evaluates the operation of its ISMS for compliance with internal and international standards. We engage credentialed assessors that perform our external audits, these occur annually. The findings from the audits are tracked through our change and development processes to resolution.

RedShield operate a comprehensive information security program that addresses the majority of the requirements of international security standards. Initially these audits have concentrated on the NZ market, but processes and standards are based on PCI and ISO standards.

As part of our commitment to the NZ Government's Telecommunications as a Service (TaaS) framework RedShield has completed a full certification audit against the requirements of the New Zealand Information Security Manual (NZISM).

Penetration testing

RedShield engages independent parties to conduct regular application-level and infrastructure-level penetration tests. RedShield's Infrastructure Team reviews and prioritises reported findings and these are tracked to resolution.

Legal compliance

RedShield employs a legal and compliance team with extensive expertise in data privacy and security.

Data requests

In the process of its business RedShield may be required to provide information about its clients to law enforcement authorities. In compliance with local laws and regulations RedShield will provide requested information. However, this will only be in the instance where legal procedure has been followed i.e. relevant court orders are presented. Additionally, RedShield will notify users if a request of this nature has been made, unless a specific legal request is made that prevents this.

Secure Code

RedShield assesses the security risk of software development projects according to our Operational Development (OPDEV) programme. This programme includes reviews by Technical Management, Engineering, and Governance Risk and Compliance (GRC).

All code is checked into a version-controlled repository. Code changes are subject to peer review and automated code reviews.

Protecting Customer Data

The focus of RedShield's security program is to safeguard the confidentiality, availability, and the integrity of the shielding solution. This includes preventing unauthorised access to any customer data that may be held.

RedShield has developed a security programme that works with each internal team which helps identify and mitigate risks in the environment, implement best practices, and evaluate ways to improve.

Data Encryption in Transit and at Rest

By default, RedShield transmits data over public networks using strong encryption. This includes data transmitted between RedShield clients and the RedShield service. RedShield supports the latest recommended secure cipher suites to encrypt traffic in transit, including use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures, as supported by its clients. RedShield monitors the changing cryptographic landscape and upgrades cipher suite choices as the landscape changes. For the shielding service itself clients are free to specify cipher requirements.

The RedShield service is hosted in data centres maintained by industry-leading service providers. Data centre providers offer state-of-the-art physical protection for the servers and related infrastructure that comprise the operating environment for the RedShield service. These service providers are responsible for restricting physical access to RedShield's systems to authorised personnel.

Network Security

RedShield operates separate systems to protect more sensitive data, and the reliable operations of the Production network. Separate systems supporting testing and development activities are provided to safeguard against inadvertent changes to the production environment.

Administrative access to RedShield systems within the production network is limited to those with a specific business need. Access to the production environment from any public network (e.g. the internet) is restricted and requires Multi-Factor Authentication (MFA) for access. This ensures that any changes to RedShield's production network configuration are restricted to only authorised personnel

Only the network protocols that are essential for operational support of the shielding service are open at RedShield's perimeter.

RedShield retains an inventory of its hardware, software and data assets which is updated continually to maintain correct data, this is essential for monitoring and reporting of patching and software maintenance updates.

Access Control

To minimise the risk of data exposure, RedShield adheres to the principle of least privilege, in which staff are only authorised to access devices and data that they need to in order to fulfil their role responsibilities. To achieve this level of restriction, RedShield uses the following measures:

All systems used in the provision of the RedShield service require users to authenticate, users are granted unique identifiers specifically for that purpose.

Using our orchestration solution each user's access permissions are reviewed regularly to ensure the access granted is appropriate for the user's role responsibilities.

Requests for all access follow a documented process and which requires approval of the immediate manager.

Authentication

To reduce the risk of unauthorised access to data further, RedShield employs multi-factor authentication for access to the production network. Where possible RedShield uses SSH key based authentication. For example, all access to production servers requires staff to connect using both an SSH key, associated with their unique identifier, as well as a password.

Passwords are required to be complex (it is recommended that they are auto-generated to ensure uniqueness, longer than 8 characters, and not consisting of a single dictionary word, among other requirements).

RedShield requires staff to use an approved password manager. Password managers generate, store and enter unique and complex passwords. The use of a password manager helps avoid password reuse, phishing, and other behaviours that can reduce security.

System monitoring, Logging, and Alerting

RedShield monitors the servers and devices that provide the shielding service in order that it can record a comprehensive view of the security state of its infrastructure. Administrative access and use of privileged commands on servers in RedShield's shielding network are logged.

RedShield's Infrastructure Team collects and stores logs for analysis. Logs are protected from modification and retained for at least two years. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel.

Incident Response

RedShield has established policies and procedures for responding to potential security incidents. RedShield has defined the types of events that must be managed via the incident response process. Incident response procedures are tested and updated at least annually.

Data Sanitisation and Media Disposal

Should RedShield acquire personal information of any kind we will take steps to remove it securely from the environment. Currently, RedShield has no direct business use for this kind of information.

RedShield follows industry best practices and advanced techniques for the destruction of data.

RedShield has defined standards that require media to be properly sanitised once it is no longer in use. RedShield employ hosting providers who are responsible for ensuring the removal of data from devices that have been allocated to RedShield's use before they are repurposed.

Workstation Security

All workstations issued to workers are configured by RedShield to comply with our security standards, they all operate with approved operating systems that are not prone to malware infections. Our standards require that workstations are properly configured and kept updated. RedShield's default configuration sets up workstations to encrypt data, have strong passwords, and lock when idle.

Change Management

To minimise the risk of negative events in the production network, either availability impacts or confidentiality breaches, RedShield controls changes using a formal change process. Our regular business as usual (BAU) changes to the shielding service are not change managed which allows RedShield to be agile in the instance that a client requires a change, all other changes follow a strict process of risk assessment and approval.

Our change management requirements are designed to ensure that changes which could potentially impact the Shielding service availability, or Customer Data, are documented, tested, and approved before they are enacted.

Server Hardening

New servers deployed to our production environment are hardened by disabling unneeded and potentially insecure services, removing default passwords, and applying RedShield's custom configuration settings to each server before use. RedShield has adopted the work performed by the Center for Internet Security (CIS) to assist in this area.

RedShield utilise an automated orchestration system that enforces the baseline Standard Operating Environment (SOE) configuration, monitors for changes and reverts in the instance that an approved change is not in place.

Business Continuity and Disaster Recovery

RedShield utilises services provided by its hosting provider to distribute its production operation across multiple separate physical locations. These locations are within multiple geographic regions which allows clients the flexibility to choose where and how their individual services are processed and served from.

These additionally protect RedShield's service from loss of connectivity, power infrastructure and other common location-specific failures. Production configurations are replicated among selected operating environments, to protect the availability of RedShield's service in the event of a catastrophic incident.

Third Party Suppliers

To run its business efficiently, RedShield relies on third party organisations. Where these can potentially impact the security of RedShield's service we take appropriate steps to make sure that our core values are maintained.

RedShield establishes agreements that require service organisations adhere to confidentiality commitments RedShield has made to its users. RedShield monitors the effective operation of the organisation's safeguards by conducting reviews of its service organisation controls before use and are reviewed annually for audit purposes.

Conclusion

RedShield take security very seriously, it's at the core of the service that we provide. Safeguarding our client's data and the availability of our shielding service is a critical responsibility for us and we work hard to maintain it.

References

For more information on GDPR and RedShield's Privacy Policy refer to:

- RedShield's GDPR Approach http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- RedShield's Privacy Policy https://redshield.co/privacy

ABOUT REDSHIELD

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 ensure the right shields are deployed quickly minimizing application downtime and costly remediation delays.

Get ahead and stay ahead of cybersecurity risk with RedShield. Shield First.