Security Whitepaper:
Bloomtools

Bloomtools
growing business

Security Whitepaper:
Bloomtools

Table of Contents

Introduction 2
Overview 2
Security Policies 2
Internal Protocol and Employee Education 3
Physical and Environmental Security 3
Operational Security 4
Systems Development and Maintenance 5
Security Feature Customisation 6
Policy enforced security features 7
Disaster Recovery and Business Continuity 7
Conclusion 7

Introduction

Bloomtools understands that the confidentiality, integrity and availability of our customers' data is vital to their business operations and, as a result, security is an integral part of Bloomtools' cloud computing applications, as well as a core element of Bloomtools' development processes. This document will outline how the Bloomtools platform and infrastructure secures its customers' data and is correct at the time of writing.

Overview

Bloomtools' security policy is designed to protect all of our clients' data by constantly monitoring and improving our applications, systems and process to meet the ever-changing demands and challenges of security. The strategies that we employ include:

- Security policies
- Internet Protocol and Employee Education
- Physical and environmental security
- Operational security
- Systems development and maintenance
- Security Feature Customisation
- Policy enforced security features
- Disaster recovery and business continuity

Security Policies

The foundation of Bloomtools' commitment to security is its security policies that cover physical, account, network and computer systems, application services, system services, change management, incident response and data centre security. These policies are reviewed on a regular basis to help ensure their continued effectiveness.

In addition to the requirement that all employees follow these policies, employees are educated on the important aspects of informational security, such as safe use of the Internet, working from remote locations safely and how to handle sensitive data.

Internal Protocol and Employee Education

All employees are required to conduct themselves in a manner consistent with Bloomtools' guidelines regarding confidentiality, business ethics, appropriate usage and professional standards.

Upon hire, each employee's individual education and previous employment is checked. Bloomtools may conduct criminal or other security checks dependant on the role of the individual.

Employees are then required to execute a confidentiality agreement and to then read and understand the company's code of conduct. This document deals with Bloomtools' expectations that every employee will conduct themselves with ethics, integrity and within the law.

Physical and Environmental Security

Power

Bloomtools' systems are accessable 24 hours a day, seven days a week. Power supply to the servers that run the Bloomtools operating system are maintained through a minimum N+1 redundancy, while the main power is supplied via two 33kV dedicated incomers, a diverse A&B power supply distributor at 11kV via a rotary UPS and multiple ring main circuits. In the event of utility outages, an on-site diesel power generator can support the centre at a full capacity for 24 hours. This generator is also backed up by 24 hours a day, seven days a week fuel delivery contracts to ensure the continued running of the generator in the event of a long, persistent power outage.

Climate and temperature

As with any hardware, heat is produced by operational servers and computing hardware. To maintain an optimum operating temperature for the hardware a sophisticated air cooling system is used. This system uses both normal and emergency electrical systems to power the air conditioning units. By maintaining an optimum climate and temperature for the hardware, Bloomtools is reducing the possibility of overheating and the consequential server outages.

Fire detection and suppression

In the event of fire in the Bloomtools server room, a sophisticated automatic fire detection and suppression system will activate and minimise damage to the computing hardware. This system is comprised of fire detection units and flame suppressors in all areas as well as dry pipe sprinklers in technical areas, dry risers to all floors and a smoke and gas clearance system. Manually operated fire extinguishers are located throughout all the data centres and staff are regularly retrained in their use as well as other fire safety proceedures.

Operational Security

Network Security

Bloomtools uses a number of defence mechanisms to protect the network perimeter from external attacks. In order to traverse Bloomtools' internal and external networks, services and protocols must meet our stringent security requirements.

The components that make up the network security are as follows:

- Access to servers via shell connections is not possible except to authorised locations and personnel.
- All traffic is routed and monitored through commercial grade redundant firewalls.
- Network segregation is enforced using private network switches.

Operating System Security

Bloomtools uses proprietary software, which means that is has been fully developed by Bloomtools' own team of programming experts. The team uses a hardened, enterprise version of Linux specifically designed to only use the features and functionalities required of the Bloomtools system. This means that all others funtionalities of the system are disabled, allowing Bloomtools to retain complete control over the system and what it is capable of performing.

The Bloomtools security team are constantly researching new security measures and threats and updates are performed on a regular basis.

Access and Authentication

Each Bloomtools employee accesses the Bloomtools system using a two-factor authentication system comprised of a unique RFID key and a password. All passwords used comply with Bloomtools' strong password policy which requires a minimum password length, the inclusion of numbers and symbols, regular password resets and a Word Verification feature when multiple unsuccessful login attempts have been made.

Individuals are not aware of any of the passwords required to access Bloomtools' systems. At the end of a person's employment, their unique RFID key is returned to the employer and their access is fully disabled.

Authorisation Controls

Employees of differing roles are given different access rights based on their job inclusions and responsibilities. In the event that an employee requires additional access rights for a duration, a formal request for extended access permissions needs to be made by the employee, approved by Bloomtools Security Management and then disabled when the access right is no longer required by the employee.

Bloomtools employees are only granted a limited set of permissions to access client data. If the employee requires further access to client data, the client must approve this access prior to the employee accessing the client's data. Access rights to the client's data will be terminated when the employee no longer requires the client's data to perform their role.

Audit Logging

Bloomtools logs all access to the Bloomtools production system and data in order to monitor any unauthorised access of the system. These logs are reviewable by Bloomtools security staff on an as-need basis.

Physical Security

The Bloomtools datacentre is one of the most sophisticated in the world and employs a range of strategies to ensure that Bloomtools' systems are keep at high security. These strategies include:

- Management and patrolling of the building by highly trained control staff 24 hours a day, seven days a week.
- Multiple closed circuit TV points.
- Secure entries and exits to the building in addition to limited access areas.
- All access to the facility is logged and recorded.

Monitoring

All Bloomtools servers are monitored 24 hours a day, seven days a week by two teams, one in Sydney and the other in Texas. These teams are dedicated to monitoring the traffic for any suspicious behaviour, security threats or any other activity that may compromise the security of the Bloomtools system and its associated data. Both monitoring teams are bound by a five minute live response time to server incidents and outages.

Systems Development and Maintenance

Multi layered Development

Most of the Bloomtools system is engineered to be run off a central set of core functionality that has been designed to avoid certain classes of vulnerabilities. For instance, the database access layers of Bloomtools are designed to be inherently robust against query language injection vulnerabilities, or HTML template frameworks with built-in defenses against cross-site scripting vulnerabilities.

Some of the security risks solved with this approach include;

- Injection Attacks (SQL, XSS, Command, Remote Code)
- XSRF Attacks
- Session Security
- Secure File Uploads
- Creating Secure Configurations
- Password Security

- Sandboxes & Tarpits
- Security through Obscurity
- Security Implications for AJAX
- Filtering for Charsets

Revision Control

To reduce the probability of human error or oversight in our development process, developers are required to use revision control systems to maintain current and historical versions of their source code. Once an engineer has completed code, it is submitted to a test server where the quality assurance team test the code.

Coding Reviews

Bloomtools' engineering team are required to partake in a peer-review process on a scheduled basis. These reviews are driven by Bloomtools' culture of quality engineering and integrity and are used to identify possible quality issues of individuals that may result in future security compromises.

The reviews focus on several aspects of an engineer's skills and performance including:

- Adherence to coding standards
- Adherence to style guidelines
- Quality control
- Multi-layered security testing

Security Feature Customisation

One of the inherent challenges with security is that as you start to tighten the security of an application, you also start to remove some of its flexibility. As a result the software is written with certain features that allows a customer's domain administrator to dictate their level of security.

Password Strength and Length

Administrators can set password length requirements for their users. They can also visibly determine the strength of a password using a colour coded indicator when entering in their proposed password.

Login Location Restrictions

Administrators can restrict access to the system to certain IP addresses, such as the IP address associated with their office. This will help prevent login from unauthorised locations that may compromise the system security.

Maximum Login Attempts

In order to restrict the success of a brute-force-attack (where a script is designed to try all possible password combinations for a user), administrators can tell the system to lockout users for a predetermined period of time after a designated number of failed login attempts. In addition to this, users can activate Captcha (otherwise known as Word Verification) which prevents scripts from logging into a user's account. Captcha can be activated after a set number of failed login attempts have been made against a user name.

Sessions Timeouts

Administrators can set the system to automatically log a user out if they have not been active on the system for a set amount of time. This helps prevents the hijacking of a user account if someone has left their computer for a duration of time without logging out of the Bloomtools system.

Session Identity

In order to restrict session hijacking, users can indicate the level of security that indicates that their session has not been hijacked. This can be checked against their IP address and their web browser headers.

Policy enforced security features

Secure Browser Connections

Bloomtools users are required to use Hypertext Transfer Protocol Secure when accessing the system. Information is then encrypted from the moment it leaves the user's computer until it reaches Bloomtools.

Disaster Recovery and Business Continuity

Bloomtools has developed a multi-layered disaster recovery program in the event of service interuption due to a security breach, hardware failure, or natural disaster. The main principle of this system is that there be no single point of failure so that, in the event that an entire server stops operating, there will be no service interuption to any individual using the Bloomtools system.

In addition to this, customer data is replicated on multiple hard drives within the one server (Raid 5 hard drive configurations) as well as across multiple individual servers. Data is backed-up off-site to multiple locations and a history of each backup going back up to one month is also recorded.

Conclusion

Bloomtools is committed to keeping information stored on its servers safe and secure and has developed a comprehensive security policy to ensure this happens. By developing policies around security, Internet Protocol and Employee Education, Physical and environmental security, Operational security, Systems development and maintenance, Security Feature Customisation and Disaster recovery and business continuity, Bloomtools can assure users that their privacy, confidentiality and data is extremely well protected.