rediffmail enterprise

Rediff Security

Information Security and integrity has been integral part of the Rediff services. We store and transmit very sensitive user data. We understand the huge repercussions of this data getting in to wrong hands. We have built all our services and applications to comply with highest security standards. We have designed our security infrastructure to mitigate the risks even at granular levels. We cover the security risks at physical, operations, network as well as application levels.

Physical security

Rediff pioneered the establishment of Data Centers in India. The datacenters location selection is based upon proximity to the international internet landing stations to reduce latency and most reliable power supply. The datacenter is guarded 24x7x365 and multiple level of checking is done to ensure only the authorized personnel have access to storage location. Datacenter is equipped with biometric scanner and surveillance cameras as it also hosts the national interconnect facility.

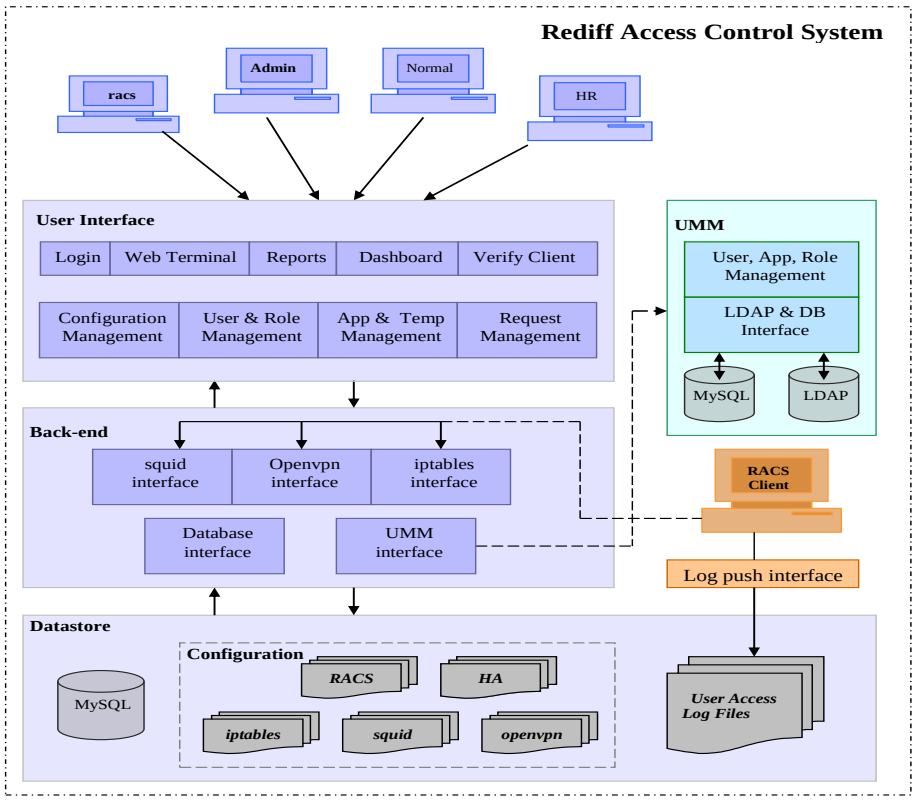
Operational Security

Rediff access control system

The Remote Access Control is a web based application aimed at providing the access to remote servers at Rediff Network with various access control options. The tool provides option to control the access to the remote servers and can collect the necessary access logs from remote servers. The generated access logs would help to create reports and would represent the data with various filter options. This data would help the user to analyze the access details of remote servers. The report would have further detailed reporting option to diagnose the operations executed on the remote servers.

The high level architecture of Rediff access control system is given below

© 2016 Rediff.com



The Application also contains a User Management facility to effectively manage users of the system and a local database for effective data management. It has three main components

1. RACS (Rediff Access Control System): The core application which controls the remote server access. The remote servers are controlled at various levels command level, directory level and application level.
2. UMM (User Management Module): This is a centralized user management and user authentication server. This system manages the centralised user database, which is accessible by other applications in Rediff network. Each application has to be registered in the UMM system to access the user database.
3. RACS Client: RACS clients are remote servers (Linux). All the servers are configured with the RACS client setup. These servers interact with RACS server to validate the system access and also to push the access logs generated on the server to RACS server.

Audit trails

The data center operation processes are audited every year by independent auditors. Also we follow mandatory sand box testing and maker-checker policy for any change on production system.

© 2016 Rediff.com

Maintaining and analyzing log of every activity and password randomization policies ensures against any breach of security.

Systemwide backup

We have very evolved backup policy which comprises of backup schedules and restoration exercises carried out across code, data and configurations. On the code front, we have a central CVS repository which is access controlled and is backed up on a daily basis with backup stored offline. On the configuration front, the key configurations are automatically backed up on the central backup server which is backed up on tapes. On the data front, the data in files are replicated across data center in realtime to ensure business continuity and databases are backed up daily and stored offline on tapes. The entire process is audited every quarter and is SOX / IT-GCC compliant.

Network security

We have created a mesh of interconnected network by peering with major ISPs. This has helped us immensely to provide seamless and always available services to our remotest user.

At the same time, such a large network operations exposes us to wide array of hackers and the users with malicious intent. We have mitigated all the network security risks by implementing the best industry standard practices in place. We have done the due diligence of hardware hardening to allow only the legitimate traffic to flow from our infrastructure. All the data transmission of sensitive data to and fro our data center is completely secure. We have also deployed TLS1.2 protocol to support this secure data transmission.

The datacenter network is a private network beyond firewall and it can be accessed only through VPN network. We have deployed multiple levels of network security checks and Intrusion detection systems.

DDoS Attacks

DDoS attacks occur when hackers flood a network with spam email or deny network access to customers, making it impossible to complete transactions. DDoS attacks have serious repercussions—bringing operations to a halt, losing revenue opportunities, decreasing productivity and damaging business reputations.

© 2016 Rediff.com

We have taken at most care to isolate our infrastructure from DDoS attack. Is it done by monitoring and analysing customer traffic in real time, on a 24x7x365 basis. We get proactive alerts once the root cause of traffic changes, such as a usage policy violation, worm outbreak or DDoS attack is analysed by system called Arbour. This attack traffic is then filtered automatically before any of our network component is impacted, resulting in optimum bandwidth utilisation.

DNS poisoning

We have done all the due diligence to make sure that users are not spoofed via DNS poisoning. DNS Cache Poisoning occurs when the legitimate IP address of a Web site is replaced with a fraudulent IP address, resulting in end users who log on to a targeted Web site being taken instead to a different, often malicious Web site even though they typed the correct address into their browser.

We avoid the DNS poisoning risk to an extent by performing secure zone transfers from the master name server and uploading the zones to multiple content distributed network's cache name servers.

SIEM

SIEM stands for Security Information and Event Management (SIEM) System for advanced network and infrastructure monitoring.

- Real-time data aggregation : Log management aggregates data from many sources, including network, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events
- Correlation: looks for common attributes, and links events together into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information
- Real-time file integrity check to monitor critical OS and application files
- Alerts: Real-time alerts to notify critical issues if any after correlation of the data for immediate remediation
- Dashboard : For showing the event data into charts for the patterns
- Reports: For compliance and auditing process

© 2016 Rediff.com

Application security

VRAD (Vulnerability Radar and detection)

Increase in use of smart phones and tablets has a dark side effect. Consumers fall prey to enticing apps and end up downloading malware on their devices. Unsecured wifi connections has only helped in increasing the malware footprint. With malware on your device, passwords can be key logged and thus accounts can be compromised. As a service provider, we need to protect our customers' data at all times.

A home grown real time vulnerability detection framework, VRAD analyses aberrations in access patterns of services like authentication, SMTP, blogs, etc. Access logs are aggregated and analysed in real time and outliers are isolated. The outliers are passed through a rule engine which determines the extent of the aberration. Each consumer's access pattern is analysed separately and equated against his historical data. This helps eliminate false positives and identify the offenders who are blocked. The authorized person is alerted about the vulnerability and asked to take corrective measures, including change of authentication information.
All this happens in near real time in less than 4-5 min from the beginning of the attack and arrests any further damage.

VAPT (Vulnerability Assessment and Penetration Testing)

VAPT is a process in which networks, servers, Operating Systems and Application Software are scanned and tested for vulnerabilities. It does a comprehensive Testing for Applications and Networks and identifies the weakest link in the chain. It also eliminates false positives and prioritizes real threats and secures against business logic flaws. We have used many Open-Source and reputed proprietary tools to implement VAPT.

Appscan

- Automated dynamic—known as black box—security testing for emerging web vulnerabilities including web services, Web 2.0 and rich Internet applications such as JavaScript, Ajax and Adobe Flash.

© 2016 Rediff.com

- JavaScript Security Analyzer for advanced static—known as white box— analysis of client-side security issues, such as DOM-based, cross-site scripting and code injection.
- Enhanced support for web services and service-oriented architecture (SOA) including SOAP and XML.
- Customization and extensibility with the IBM Security AppScan eXtensions Framework, which allows the user community to build and share open source add-ons.
- Scans websites for embedded malware that links to malicious or undesirable sites.
- Performs comparisons with an IBM X-Force® maintained database.
- Simplifies the process of interpreting scan results with scan-specific descriptions and explanations of each issue.
- Offers an adaptive test process that intelligently mimics human logic. It learns the application, down to the level of each specific parameter and adjusts to perform only relevant tests.
- Provides tools for manual testers, including advanced utilities for custom security testing using Pyscan scripts.
- Provides streamlined remediation that fixes high-priority problems first.
- Offers explicit remediation steps with code examples to implement fixes quickly.
- Provides advanced remediation capabilities, including a helpful task list.
- Includes regulatory compliance reporting templates with over 40 ready-to-use compliance reports, including Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), ISO 27001 and ISO 27002 and Basel II.
- Helps meet key compliance standards such as PCI DSS by supporting application security testing on an ongoing basis.
- Integrates with IBM Security AppScan Reporting Console for enterprise-wide visibility into risks and continuous updates on remediation progress.

SQLMAP

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

© 2016 Rediff.com

- Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB and HSQLDB database management systems.
- Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
- Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
- Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.
- Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack.
- Support to dump database tables entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
- Support to search for specific database names, specific tables across all databases or specific columns across all databases' tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass.
- Support to download and upload any file from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
- Support to execute arbitrary commands and retrieve their standard output on the database server underlying operating system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
- Support to establish an out-of-band stateful TCP connection between the attacker machine and the database server underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user's choice.
- Support for database process' user privilege escalation via Metasploit's Meterpreter getsystemcommand

Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

© 2016 Rediff.com

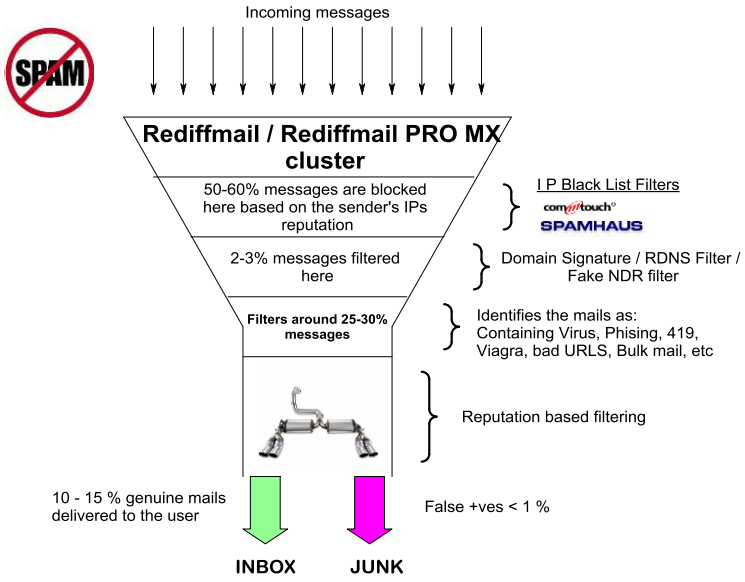
- An intercepting Proxy, which lets you inspect and modify traffic between your browser and the target application.
- An application-aware Spider, for crawling content and functionality.
- An advanced web application Scanner, for automating the detection of numerous types of vulnerability.
- An Intruder tool, for performing powerful customized attacks to find and exploit unusual vulnerabilities.
- A Repeater tool, for manipulating and resending individual requests.
- A Sequencer tool, for testing the randomness of session tokens.
- The ability to save your work and resume working later.
- Extensibility, allowing you to easily write your own plugins, to perform complex and highly customized tasks within Burp.
- NMAP for port scanning
- Wireshark for network protocol analysis
- Testing by Internal team and external partners for diversity in attack patterns
- Reports for compliance and auditing process

Anti SPAM and Virus

According to recent statistics, around 90-95% of email traffic around the world is spam.

The disruptive impact of spam and other email abuse has resulted in two types of approaches to deal with the menace. The first approach focuses on detecting and filtering problem messages. This is done by techniques that attempt to identify bad mails using pattern detection and based on other facts about the contents in the email. A complementary, but quite different approach, seeks a basis for trusting a message rather than for mistrusting it. This is done by profiling and identifying the sender and validating the sender's authenticity.

© 2016 Rediff.com



We use a combination of both the techniques to filter out unwanted mails and keeps the users mailbox free from spam. Different modules in the Rediffmail enterprise spam control system are IP based filtering, Domain Signatures / RDNS and Fake NDR filters, Content based filtering, and Reputation based filtering.

Smart TFA

The Smart 2FA framework attempts to block vulnerabilities in real time at the time of access. The system relies on the "Something You Know + Something you have" philosophy. As a part of the sign up process, consumers are made to supply their mobile number and alternate email ids. A reputation database of all users has been built which maps the relationship between various facets of access details of users. Some of the facets that are considered are: users' location, ISP, device type, device ID, service being used, browser details & time graph of access. Each relationship is mapped separately. So for instance, a consumer accessing web mail from a particular ISP from some location and using a particular device is maintained separate from the same consumer accessing some other service from the same ISP and same location and using some other device. A rule engine evaluates each users request separately at the time of access and assigns a severity score to it. Depending on the severity level, the system alerts the authorized user through SMS and blocks all suspicious request. Users can then either authorize the request or keep blocking them

© 2016 Rediff.com