

Application Security

OVERVIEW

Several security issues must be addressed when securing critical business processes whether the application is on the Internet or residing within a local network. Threats to business processing and data can be environmental, physical, or electronic. Environmental threats include natural disasters. Physical threats include the risk of equipment failure. Electronic threats can be wide-ranging, but the most potential risk comes from malicious users, or “hackers,” who target the network or application data. There are a number of points of vulnerability that must be bolstered with a comprehensive security policy that incorporates the latest technologies in encryption, redundancy, intrusion detection, access control, auditing, authentication, and network management.

eTapestry is committed to providing outstanding service and diligence in meeting your concerns about data integrity and application availability. To this end, eTapestry has partnerships with industry-leading hosting centers that bring Internet expertise and Internet performance that is unrivaled in the industry.

THE CHALLENGES OF SECURING AN APPLICATION

The keys to any successful security policy are a combination of technology and people dedicated to providing a level of service that reflects a serious commitment to the responsibility of hosting an enterprise application and its data. A security policy must be in place for any critical business application whether running on an internal, self-managed network, or using a hosted web application.

Issues of data security, accessibility, redundancy, and disaster recovery must be examined and addressed. Unfortunately many of these issues are overlooked when systems are installed and managed locally on internal hardware. A false sense of security often exists with an internally run application resulting in software that is susceptible to any number of security and disaster situations. This can also be the case when organizations lack the resources — in equipment, money, and expertise — to properly implement a security policy. eTapestry’s investment, expertise, and resources are unparalleled when compared to the alternative of a self-managed fundraising application.

SITE PROTECTION

Data centers are physically secured server facilities designed to keep your corporate information safe. Facilities have keycard entry, palm scanners, video surveillance and are staffed by technical support people 24 hours a day, 7 days a week. The physical servers are

+ Executive Summary

The privacy and security of donor data is critical to all nonprofit organizations. eTapestry understands the importance of security and the responsibility that comes with hosting an organization’s data. This white paper examines the different security issues and how eTapestry addresses them.

123 Contents

Executive Summary	1
Overview	1
The Challenges of Securing an Application	1
Site Protection	1
Catastrophic Event & Equipment Failures	2
Continuation of Service Plans	2
Over the Wire Transmission of Data	2
Conclusion	3

encased in locked cabinets that have access restrictions. Only those authorized employees with a need to administer the physical machines are allowed access to the actual servers.

CATASTROPHIC EVENT & EQUIPMENT FAILURES

9/11 revealed the devastation that can be caused by a single malicious event. However, threats to an enterprise application and data are not always of malicious intent, but can also stem from nature. A flood, fire, or earthquake can be devastating in the damage they can inflict on facilities and equipment. eTapestry provides backup and disaster recovery options to ensure maximum availability and integrity of the application data.

Our data centers provide a fully redundant network architecture with high-speed connections. Uninterruptible power supplies backed up by diesel generators at data centers ensure that power is continuous. The application architecture is designed so that processing can be redirected to other available servers in the event of a server failure. Furthermore, the use of Java as the server application language ensures full portability to any type of machine.

eTapestry provides daily incremental file system backups, with a full disk backup weekly. Database backups are rotated offsite as added means of recovery if needed. Production servers have mirrored drives, multiple power/cooling modules and peripheral power supplies. CPU, memory, and I/O boards are all hot swappable.

The on-call support staff is available 24 hours a day, 7 days a week, and 365 days a year to ensure that any service problems are handled promptly. eTapestry has a comprehensive disaster recovery plan in place should our primary physical site become inoperable.

CONTINUATION OF SERVICE PLANS

A critical area to consider is the continued operation of any application and the accessibility of data should the business enterprise cease to operate. eTapestry customers are always 100% owners of their data. Data downloads are available at any time in a standard format that can be used with MS Excel or MS Access. This process allows organizations to maintain a local, usable backup of their data. The eTapestry software code is escrowed and a sophisticated continuation plan is in place should anything happen to eTapestry.

OVER THE WIRE TRANSMISSION OF DATA

One of the key areas to address with an Internet application is the simple transmission of data between the host server and the client workstation. The Internet works by sending information from computer to computer until the information reaches its destination. When data is sent from Point A to Point B, every computer in between these points has an opportunity to look at what is being sent. eTapestry employs a Server Digital Certificate and the Secure Sockets Layer (SSL) Protocol to encrypt all data traffic between our server and the client PC.

Furthermore, SSL also protects the contents of messages exchanged between our Internet server and the client PC from being altered en route. SSL technology is the standard used by online banking, stock brokerages, and retailers for securing their online transactions.

Intrusions

Intrusions usually take one of two forms. One form can be an attempt to gain unauthorized access to data or the application. Another form can be an attempt to deny service to other users by tying up server resources or disabling the server.

Unauthorized Access

Authentication via username and password provides assurance that a client requesting information is the entity it claims to be. Access Control settings limit the functionality available and types of information that users can access after being identified as an authorized user on the system. Database activity logs record all transaction activity by user. This data can be used for accountability purposes and can be reviewed at any time by the system administrator.

Denial of Service

Monitoring of the eTapestry application and the hosting equipment is performed 24 hours a day. This, combined with the latest technologies in detecting and thwarting denial of service attacks, insures you will have uninterrupted service.

CONCLUSION

Critical examination of application security should be made for both internal operations and externally hosted applications. eTapestry is committed to earning client trust and keeping that trust by our implementation of technology and by our staff's integrity, diligence, and expertise as well as our strategic partnerships to provide a robust and scalable hosting solution.



About eTapestry

Since its release as the first web-based fundraising software for nonprofits in 1999, eTapestry has grown to a leadership position with over 5,000 nonprofit customers worldwide. eTapestry provides On-Demand fundraising solutions, including a donor database, website development, ecommerce, and advanced email. For more information, visit www.etapestry.com or call 888.739.3827. eTapestry is a Blackbaud Company.

Blackbaud®

© 03 2009, eTapestry, Inc.
This white paper is for informational purposes only. Blackbaud makes no warranties, expressed or implied, in this summary. The information contained in this document represents the current view of Blackbaud, Inc., on the items discussed as of the date of this publication.

All Blackbaud product names appearing herein are trademarks or registered trademarks of Blackbaud, Inc. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.