Database and Server Access Security Policy

For:
SEC625
Information System Security

By:
Megan E. Cutler

October 23, 2009

Table of Contents

Introduction

Every company has critical data which it does not want to fall into the hands of competition. Any company which also collects private information from its customers is also required by law to protect that sensitive information and protect it from any who would use it for malicious means. It is for this reason that the Database and Server Access Security Policy is being introduced; in order to create a more secure environment in which to store critical company data and sensitive customer information. The Database and Server Access Security Policy focuses on the company database where this information is stored, as well as the server on which it is housed and the network hardware which is used to access the database on a daily basis. It is our hope that by implementing this policy and dedicating ourselves to adhering to the measures herein, we can provide a more excellent service to our customers as well as ensure a more secure and efficient work environment for our employees.

Purpose

Security of confidential information, both related to our business and our customers, is of the utmost importance. The Database and Server Access Security Policy is being implemented for this reason. While the current state of operations allows ease of access to company resources, it does not take into account the security of valuable company resources. In order to comply with laws which mandate the protection of customer information obtained and stored by our company, measures must be taken to secure the hardware and software used in customer transactions.

Because we are liable for loss or theft of customer information protected by privacy laws, we must make every effort to ensure no harm comes to this sensitive data. Not only are we interested in protecting customer information, but also confidential internal data with contents regarding internal operations. It is important to implement policy regarding protection of sensitive information before an electronic attack can take place.

Adherence to this policy will benefit the company on many levels. Increased productivity and efficiency are achievable short term goals. Future company expansion will also be easily accommodated with the implementation of this policy. The most crucial benefit, however, is the protection of sensitive company and customer data in adherence with all privacy protection laws. Not only will this ensure our company a long and successful life, but will ensure the continued trust of our loyal customers.

Scope

Everyone is involved in security. In order to get the most benefit, everyone must be dedicated to the policy's implementation, from the users to the administrators. For this reason, the Database and Server Access Security Policy applies to everyone, even the business owner. There are no exceptions. Strict adherence to the policy is the only way to ensure the safety of critical business operations and private customer data.

The primary focus of the Database and Server Access Security Policy is on the internal company database which houses the information gathered from customers during the ordering process. However it is impossible to secure the database without taking into consideration a much wider range of company resources. The policy contains details regarding the server which houses this critical database, as well as the network hardware used to connect to the server, including the router which provides access to the server inside the office. Further details document the isolated DMZ which will act as a part of the internal network to protect the server from outside attacks, as well as the VPN which will allow users to securely access company data from remote locations.

While all users must adhere to the policy, it is most critical for those implementing and maintaining the systems described here in to understand the terms laid out in the policy. The interoffice computer technician must be familiar with all aspects of the policy regarding the office equipment which he maintains, including the router which provides network access in the office. Likewise the remote technician who administers and maintains the servers must be familiar with aspects of the policy devoted to server operations. Finally the Administration Clerk must understand those aspects of the policy which govern the access and maintenance of the company database which he is responsible for maintaining.

Policy Statements

The following statements make up the Database and Server Access Security Policy and will be adhered to on a daily basis by all employees of the company in order to maintain the highest level of security possible in regards to critical company data and sensitive customer information. Any change or update to the policy must be approved by management and the policy statement redistributed before it can be put into effect.

Network Policy

A firewall will be present and active at all times on the internal office router which provides access for employees to company resources. The firewall will be configured according to a secure network firewall policy which is designed to actively block potentially malicious network traffic. (Please see the reference section for guidelines on creating a secure firewall policy.) The firewall policy will be actively maintained by the onsite computer technician. Regular audits of firewall log activity must take place to determine if malicious network activity is present.

A new password will be issued for the office router which complies with strong password standards. (Please see the reference section for guidelines on secure password practices.) The password will only be known to those who must administer the network hardware, such as the onsite computer technician. Default passwords are insecure and must never be allowed to remain on an active network device.

Encryption assures that data being sent across the network is safe from the prying eyes of others. To ensure that no one is eavesdropping on network communication with the internal servers which host sensitive information, encryption will be enabled on the router for all network traffic.

The router will be configured to provide network addresses on a separate subnet for internal communication. This will ensure that only devices which are located in the office will be able to communicate with the server which hosts the company database.

A secure VPN will be available for all users who must access the company database remotely. The VPN connection will require the user to login with a unique PIN code and a secure ID token. This will ensure that only authorized personnel are able to access protected company resources. This will also provide a secure connection over which company data can be viewed.

All external communication with the company database will be conducted through a secure, isolated DMZ system. The isolated DMZ will receive regular updates from the internal server to ensure that it has the most recent up to date information. However, no external request will be able to directly modify the internal database. This will keep the database safe from external attacks. All communication between the web server and the internal database will take place though the secure DMZ in order to ensure that no attack can be made against the database through the company's own website.

The company database, which contains critical business information and sensitive data gathered from customers, will be hosted on its own server which contains no active services which require access to the Internet or any other external network. This server will remain separate from the server which manages the company website and email. This server will only be accessible by internal network or secure VPN. It will not be reachable by the Internet or any other external network.

The web server which manages the company website and the email server will remain together on a second server. This server will be able to access the Internet and other external networks. Likewise external networks will be able to access this server so that customers will still be able to access the company website and receive emails regarding their orders.

Access Policy

Only those who require access to the company database in order to do their jobs will be allowed to access the database. Anyone not requiring information from the database will not be provided with an account for database access.

Each employee who requires access to the internal database will be provided their own unique account for use in accessing the database. Each employee's username and password must be unique. Passwords for these accounts should follow secure password practices. (Please see the reference section for guidelines on secure password practices.)

Each user account will only be provided as much access to the database as is required for each user to do their job. If a user only requires the ability to read and update data, they will only have read and update access to the database. Only the Administrative Clerk, who maintains the database, will have administrative access to the database.

Roles and Responsibilities

In order to ensure that all security measures in the policy achieve their full potential, the following people are responsible for maintaining the company's computer systems in accordance with this policy and should be contacted in regards to issues in their stated area of expertise:

Requirements for Individuals

The interoffice computer technician will be responsible for managing all internal network equipment, including the network router. It will be his responsibility to maintain the firewall configuration as well as the working state of the hardware. If the router password is compromised, the inter office technician will update the password and notify those who must be aware of the change.

The owner, technician and administrative clerk who remotely maintain the servers will be responsible for maintaining security on the servers as well as keeping them in working order. They will be responsible for maintaining database user accounts as well as maintaining security on the database.

All users will be responsible for maintaining their own database and VPN accounts. Users will make sure that their passwords are secure and updated regularly according to the implemented password policy. All passwords must be strong passwords. (Please see the reference section for guidelines on secure password practices.) Passwords must never be shared or written down.

Requirements for Technology

Security systems left to their own devices for too long will quickly become out of date. To ensure that the company continues to benefit from the policy, all technologies listed here must be maintained so that they remain up-to-date and secure.

The firewall on the internal router must be regularly updated with the latest vendor patches. The configuration should also be updated to include conditions for any major security warnings which are released. All updates to configuration must occur in a timely fashion to ensure that the company is not at risk from newly identified vulnerabilities.

Similarly, the internal servers must have vendor patches and security updates applied in a timely fashion. These updates must occur in such a way that they do not disrupt services required for regular business operation. As such, it is best they occur during off-hours and with minimal server down time.

The DMZ must also be properly maintained so that it remains secure. Updates to the DMZ will also occur during off-hours. It is best if the DMZ is updated at the same time as the servers in order to insure minimal interruption to service, especially the online services accessed by customers.

The VPN system which allows access from remote locations must also be kept securely up-to-date by applying all vendor related patches. It may be necessary to update the VPN to the latest version. Major upgrades to the VPN which will disrupt service will be performed rarely and will be well documented before hand to warn users of any service outages.

All logs generated by security systems such as the firewall will be audited on a regular basis to determine potential threats to the company and its computer systems. Any suspicious activity should be dealt with according to the response plan determined by the company.

Enforcement

What to Do in the Event of Policy Violation

As part of our continued dedication to security it is vital that all violations of the policy be reported and dealt with in a timely manner. Violations should be reported according to the area in which they occurred. Any violation which relates to network hardware, software or internal computer systems should be reported to the onsite computer technician. Any violation which relates to the company database and the data contained therein should be reported to the Administration Clerk who monitors and maintains the database. All violations should then be reported by their respective administrators to the business owner so that proper action can be determined. To ensure the security of the company, it is vital that all violations are reported immediately.

Penalties for Policy Violation

Penalties for violations to the security policy will be determined on a case-by-case basis at the discretion of the business owner, or the respective administrator of the system. Any violation which results in the loss or exposure of sensitive customer data at risk or liability of the company will result in termination.

References

Guidelines on Creating a Secure Firewall Policy

Provided by SANS, this document contains information on how a proper firewall policy can be prepared and what should be taken into consideration when writing that policy. It includes a sample policy draft in the appendix.

http://www.sans.org/reading_room/whitepapers/firewalls/the_firewall_has_been_installed_now_what_developing_a_local_firewall_security_policy_810

Guidelines on Secure Password Practices

Provided by SANS, this policy contains useful information in regards to creating and maintaining secure passwords. The policy is offered freely by SANS and states directly that it can be modified to suit a company's needs if desired. It makes an excellent guide for creating a secure password policy. http://www.sans.org/security-resources/policies/Password_Policy.pdf

Contact Information

Any questions or concerns related to the policy and the statements contained therein should be directed to the currently active business Owner, Computer Technician or Administrative Clerk.

Any issues which cannot be resolved internally can be directed to the author of the policy at: mecutler@learn.senecac.on.ca.

Glossary

DMZ

Short for “Demilitarized Zone”, “Data Management Zone” or “Demarcation Zone”, DMZs are used to create a “perimeter network” for an internal network. A DMZ marks the place where the company's internal network and resources meet external networks, such as the Internet. DMZs are put into use in order to protect internal resources from outside threats. They do this by sitting between the external network and the internal one. In the case of an “isolated DMZ”, the DMZ system receives regular updates from the internal network, but cannot actually make any changes to internal systems at the request of someone from an external network. The DMZ also listens to requests from the external network and sends an answer to all queries from the information which it has received, but never actually passes the request to the internal system. This allows information to pass from the company database to the outside world (for example, a customer checking on the status of their invoice via the company's website), but prevents an attacker from being able to modify or delete vital data.

Encryption

The process by which information or data is hidden from everyone except those who we wish to read it. This is accomplished by an algorithm (known as a cipher) which transforms the data into something which is unreadable. Data is usually encrypted before it travels across the network so that an attacker will be unable to read any data which is intercepted. This ensures the confidentiality and integrity of

documents. When a document reaches its destination, the reverse process (known as decryption) is applied so that the data once again becomes readable.

Firewall

Part of a computer system or network which is designed to block unauthorized access to network resources, while still allowing authorized communications. A firewall sits between the internal network and the external network. It ensures that legitimate communications with the internal network are allowed to pass but blocks any potentially malicious activity so that it cannot reach the internal network.

Subnet

Short for "Subnetwork". A subnet is a subdivision of a network. A subnet is usually a network which is formed by breaking down a group of IP address networks and assigning the resulting network a specific task. In this case, only the subnetwork created for the internal office will be allowed to access internal devices. All other IP addresses will be blocked.

VPN

Stands for "Virtual Private Network". A secure connection which allows the user to connect to secure systems, such as an internal company network, via the Internet. A VPN provides the encryption which is needed to prevent an outside attacker from viewing the data being sent to and from the internal network if they are able to intercept it.