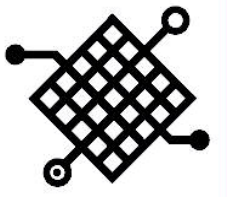
ChainLink Halo

Protecting your investment on the Web



Enterprise Web Security

Summary

While corporate Internet usage has grown significantly over the past decade, so have the number of Internet related attacks from both the inside and outside the organization and corporate enforcement of Internet usage policies and security have not kept pace. Firewalls, which control access to network resources, fall short in providing visibility into what is allowed to pass. Organizations need to deploy additional measures to monitor the content of allowed traffic.

According to the "2001 CSI/FBI Computer Crime and Security Survey", 95% of the surveyed corporations had firewalls, although 91% of those surveyed reported that they have had security breaches, and 64% had suffered financial loss as a result. The amount of loss is also on the rise. The survey found that of those suffering losses, the average loss was over $1 Million per respondent in 1999 while in 2000 it had risen to over $2 Million.

Clearly there must be a balance between restricting Internet access and securing the Internet investment that companies have nurtured and which has become and invaluable asset. It is not uncommon to allow web-based traffic to flow freely through the company Internet. This paper will discuss what challenges are faced when attempting to provide web security and how the rises ChainLink Halo to meet those challenges.

Challenge

As companies have rapidly embraced web services for research, marketing, and communication they have opened paths into their corporate infrastructure and through their Internet firewall for the web servers. Those paths onto the corporate network allow for hackers to penetrate from the outside and malicious or unacceptable use of the resources from the inside.

Vulnerabilities in web server applications allow hackers to exploit the weakness and gain control over the web site. Once access has been obtained, they can use the compromised system to access others that may have been otherwise unreachable. This sort of attack has been exploited on numerous major web sites allowing hackers to do anything from simply defacing the web site to stealing customer information as well as confidential documents. Companies are often left with little indication of how their system was compromised and find it difficult to perform meaningful forensics.

On the inside, security risks are even more critical although policies tend to be more lenient. Message boards provide an easy means for employees to communicate with others and share valuable information. The problem occurs when the information that is shared, either intentionally or unintentionally, contains confidential information or is inappropriate for business conduct. The insider threat can lead to legal and direct financial losses. Government agencies have experienced leaks of classified material through bulletin board postings. Businesses have had deals broken and law suits waged due to inappropriate employee use of the Internet. A major OS manufacturer has had their entire source code to their software leaked through the web. An intangible loss may be when your company appears on the nightly news due to a failed security policy.

When network administrators are faced with the task of monitoring a company web presence, they rely on a mixed bag of tools log traffic, monitor usage and detect intruders.

Some potential problems can be detected by inspecting web and proxy server log files. Many commercial log analyzers exist that the administrator can use to collate the log files and report on general traffic patterns. Log file analysis provides insight into the general traffic patterns of users, but it lacks the ability to reconstruct the web transaction and perform forensics.

Additional methods must be used to log web transactions and reconstruct the content of the web conversations. A common tool for monitoring network traffic is a LAN analyzer. The LAN analyzer picks up any traffic that exists on the network and saves it to a file. LAN analyzers typically perform well at the micro level, but the log files quickly grow and without very narrow filters in place, they very quickly become too big to be useful. Additionally, even if the problem transaction can be identified, making sense of the captured packets can be tiresome.

ChainLink Halo

The ChainLink Halo is a passive network appliance server, which sits quietly on any ethernet segment and collects HTTP traffic, which can be used to detect unauthorized outside intruders and inappropriate insider use of the web.

The ChainLink Halo contains three core components that combine features of the most common tools that administrators use to monitor inbound and outbound web traffic. The three components are the ChainLink WebWatcher, ChainLink WebLogger, and ChainLink WebAnalyzer. The components are packaged together in a single ChainLink Halo or can be distributed as separate agents across multiple application servers. All three components are managed through a single web application so that they can be accessed remotely.

The ChainLink WebWatcher is a packet capture component that splits apart HTTP specific data into request and response header and data streams. It records important metrics about each part of the web transaction and will save any or all pieces of the web transaction to either file or directly to the ChainLink WebLogger. All servers that are on the same LAN segment can be monitored simultaneously. The ChainLink WebWatcher aggregates all web server traffic into one central repository.

The ChainLink WebLogger is the central repository for all web traffic data. Multiple devices can log data to the ChainLink WebLogger including remote WebWatchers, ChainLink Halo data files, and proxy or web server log files. Periodic cleansing and compression as well as smart caching of identical objects minimize the storage requirements for the ChainLink WebLogger.

The ChainLink WebAnalyzer catalogs the captured web transactions into logical groupings so that the web transactions can be easily located. Each catalog has user-defined indexes and rules for filtering content as well as how long the content is to live with the catalog.

For example, one catalog could be defined to capture all known web server exploitation type viruses. One example of an exploitation type virus would be the NIMDA virus for which hackers use to gain root access to unprotected IIS web servers. The content of isolated NIMDA virus hits could be examined to determine the origin and if they caused any damage to the servers they were accessing.

A general catalog could be set up to store all html type hits (no images) originating from internal sources. Filters can be added to group the cataloged data, for example, by department, user, server. Additionally, custom filters can be created to further isolate the data. A weekly macro level

report can be created from the entire catalog and any suspect transactions can be fully inspected to determine the appropriateness of the web use.

Although many predefined filters have been included in the ChainLink WebAnalyzer, additional ones can be easily created and integrated. The ChainLink WebLogger can be accessed through JDBC/ODBC drivers so that custom reporting tools can take advantage of the data gathered.

Conclusion

Web traffic monitoring while essential enterprise web security, can be ineffective without the proper tools. As web traffic increases, the challenge of monitoring becomes even more difficult. The ChainLink Halo network-monitoring appliance provides a comprehensive set of tools, which simplify an administrator's ability to monitor the traffic on medium to large-scale web infrastructures. Additionally, the web traffic measurements gathered with the ChainLink Halo provide added value statistics to measure the effectiveness of the enterprise web investment.

ChainLink Networking Solutions, Inc.

11012 Burywood Lane
Reston, VA 20194
Phone (703) 430-5752
Email: info@chainlink.com