White Paper

HOLDING THE FORT–SECURING YOUR NETWORK WITH APP-AWARE FIREWALL TESTING

The Business Case for Testing Security

August 2012

Rev. A 08/12

SPIRENT

1325 Borregas Avenue
Sunnyvale, CA 94089 USA

Email: sales@spirent.com
Web: www.spirent.com

AMERICAS 1-800-SPIRENT • +1-818-676-2683 • sales@spirent.com

EUROPE AND THE MIDDLE EAST +44 (0) 1293 767979 • emeainfo@spirent.com

ASIA AND THE PACIFIC +86-10-8518-2539 • salesasia@spirent.com

Securing Your Network with App-aware Firewall Testing

The Business Case for Testing Security

CONTENTS

EXECUTIVE SUMMARY

The news is littered with stories of enterprises that have suffered costly downtime and damaging lawsuits as a result of security breaches. Even high-profile names such as LinkedIn, Sony, and RSA are not immune. Lack of security is costly, but how much should an organization spend to address their security issues?

Unlike a typical ROI, which determines the ratio between the number of dollars you spend to the number you gain in return, when it comes to security, you're comparing how much you spend to how much you can avoid losing. In essence, you're spending money to lower risk, much like spending money on the legal department to reduce your liability.

But simply installing a security solution is no guarantee of protection against a breach. With the new breed of nex-gen firewalls, the problem becomes more complicated. Testing is the key to effective security, but inadequate testing causes more problems than not testing by creating a false sense of security. A test platform with the power to create realistic tests and the use of industry best-practices, developed over time through experience and expertise, allow organizations to test and deploy security solutions with confidence.

THE COST OF INSECURITY

Gartner estimates the low end of the range of hourly cost of downtime for computer networks at $42,000. For a financial services company that trades on Wall Street, the cost could be ten times that or more. Even a short outage can rack up significant costs. The loss of HIPAA data due to a breach has cost some companies as much as $1,000 per record in the resulting lawsuits.

June, 2012: A study released by Guardian Analytics and McAfee documents the progress of Operation High Roller[1], an ongoing server-based automated attack of at least 60 financial institutions in Europe, Latin America, and the United States that began in 2011. The attackers have processed thousands of attempted transfers, totaling at least $78 million, from high-value commercial accounts and high net worth individuals. The attack targets organizations of all sizes, including credit unions, large global banks, and regional banks, with individual transfers as high as $130,000. Since the attack is still ongoing, no actual damage numbers have been released.

[1] http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

June, 2012: Over six million LinkedIn user passwords were leaked on a Russian website[2], causing the company to advise their users to change their password immediately.

October, 2011: Sutter Health had a breach that compromised unencrypted HIPAA data for over 4 million patients, prompting a $1 billion class action lawsuit[3]. The company was in the process of encrypting their data at the time of theft, starting with hand-held devices.

June, 2011: A group of hackers known as LulzSec used a SQL injection attack to get into the Sony Pictures website and compromised over 1 million accounts, including password, email address, home address, and date of birth [4]. None of the data was encrypted. The damage extended to network admin details, including passwords, 75,000 music codes, and 3.5 million music coupons. They published information from 150,000 of the one million compromised records online.

April, 2011: The Sony PlayStation Network was compromised, exposing the credit card numbers and other personal information of 77 million users, creating a 24-day outage[5]. The outage cost Sony over $24 billion.

March, 2011: Cyber criminals broke into the Fidelity National Information Services (FIS) network and obtained twenty-two legitimate ATM cards[6]. They altered the cards so that they could be used to withdraw an unlimited amount of cash, made copies, and shipped them to Greece, Russia, Spain, Sweden, the Ukraine, and the United Kingdom. In 24 hours, a total of $13 million was taken from accounts.

March, 2011: A cyber attack cost EMC $66 million when attackers compromised the SecurID hardware token solution sold by EMC's security division, RSA[7]. EMC replaced the tokens of one third of the 40 million users of the security solution. The attackers used stolen SecurID information to launch attacks against numerous defense contractors, including Lockheed Martin, who detected the attack early and was able to prevent any data loss from their systems.

The cost to businesses of exposing data such as Social Security and credit-card numbers climbed 7 percent last year to an average of $7.2 million per incident, according to a study of companies that experienced breaches. The most expensive incident cost an unidentified company $35.3 million, an increase of 15 percent from the costliest breach a year earlier, according to a report from Ponemon Institute LLC[8]. Malicious attacks increased 7 percentage points from last year, with the costs of such attacks jumping 48 percent, to an average of $318 per compromised record.

Clearly, lack of security can be costly. But how much should you spend to make sure you are secure?

[2] http://www.huffingtonpost.com/2012/06/07/linkedin-password-hack-check_n_1577184.html
[3] http://www.hipaatext.com/1b-suit-filed-against-sutter-health-over-data-breach/
[4] http://techland.time.com/2011/06/02/new-sony-hack-claims-one-million-user-passwords/
[5] http://www.pcworld.com/article/226128/sony_makes_it_official_playstation_network_hacked.html
[6] http://news.techeye.net/security/cyber-criminals-stole-13-million-in-a-day
[7] http://www.rsa.com/node.aspx?id=3872
[8] http://www.ponemon.org

THE TRUE COST OF SECURITY

Unlike typical return-on-investment (ROI) calculation, for security its different, as the amount of spend is compared to how much you would not lose.

ROI on security is calculated by estimating potential loss and the probability of realizing that loss. Typical types of loss include:

- **Revenue loss**: For revenue-generating systems, such as ecommerce websites, revenue-per-hour can be estimated from historical data. Anything that reduces the hours of downtime reduces your loss.
- **Productivity loss**: A virus or other malicious threat can cripple your internal network and workstations, making it impossible for your employees to conduct business.
- **Data loss**: If a malicious intruder, or even a disgruntled worker, wipes out your data, you will be down for the duration of the restore process. Assuming they didn't destroy the backups.
- **Data compromise**: The exposure of HIPAA information is costly. In addition, customers whose credit card information has been compromised may chose to do business with someone else.
- **Goodwill**: A breach affects your company's reputation, not only with existing and potential customers, but also with partners, vendors, and investors.

Once the potential loss is quantified, including the cost of recovery and remediation, the cost of protection against the loss can be compared to the cost of the loss itself. A good maximum budget for protection is thirty to forty percent of the anticipated cost of the loss, but the cost of a security solution typically falls well below the maximum.

Most likely, all of the companies in the horror stories had some measure of security in place. However, those measures obviously proved insufficient to protect them from serious exposure and loss of revenue. How can you assure yourself and the stakeholders in your organization that your security performs as it should?

Trust but Verify

Your security vendor will understandably present their products in the best light. It's up to you to make sure before you buy that the solution meets your needs and does what the vendor says it will do. Even if the vendor claims are completely accurate, their QA department cannot possibly test all combinations of features under all scenarios their customers use. To know the true performance of a device in your network, you have to know what testing is behind the numbers in the brochure.

Did they test against all of the thousands of known attacks and vulnerabilities? Did they use negative testing to benchmark processor-intensive features such as deep packet inspection (DPI) and application awareness to create the unpredictable scenarios that are frequently the cause of catastrophic and costly breaches
and failures?

In addition, a security solution not only has to protect your organization from threats, but it also has to remain transparent to the workforce, allowing employees to remain productive before, during, and after threat incidents occur. Do the throughput numbers reflect test runs with demanding features enabled? Next-gen firewalls provide many new capabilities, including app-aware features, that may come at the cost of performance. Only testing will tell the true story.

With the right test platform, your network can be modeled in the test lab, something your vendor didn't do. Placing a new device in your network could expose limits in the device, or potential security risks in your network. That is critical information you should learn through testing before purchase and certainly before deployment, not through downtime due to unexpected issues or failures.

Inadequate Testing

Clearly testing is important, but what you test and how you test it is just as important. Inadequate testing can be worse than no testing at all when it results in a false sense of security.

While it is tempting to economize when designing a test environment, using test tools that are incapable of recreating the target environment increases the likelihood of ending up in the headlines.

- **Using a production network during off hours**: Nothing like the target environment. Can't be configured for repeatable testing or troubleshooting.
- **Using homegrown scripts**: No plan for sustainability. Script-based tools running on a CPU don't have the power or sophistication to recreate the diversity and complexity of the production network.
- **Using open-source freeware**: Useful for troubleshooting problems, fine tuning protocol settings, and basic functional and throughput tests, but not designed to test the DPI and app-aware features of the latest security devices.
- **Using a packet blaste**r: Line-rate device performance and basic functional testing. Not designed or intended to test performance, availability, security, and scalability of a solution.

You don't want a security solution built on shortcuts.

Proper Testing

Beyond the tool is the question of how to use it to accurately evaluate performance, availability, security, and scalability. Realistic testing means re-creating the environment that the solution lives in, from the provider to the end user.

There are three essential elements of test realism.

- **Real user behavior**: Realistic testing means the flexibility and sophistication to emulate a wide range of user behavior, both benign and malicious. For security testing, this includes emulating the thousands of known attacks using real application traffic with the full range of versions and possible endpoints.
- **Real converged traffic**: Realistic testing means the power to create fully-emulated, stateful traffic across hundreds of ports. For security testing, this includes the ability to use fuzzing and custom tests for proprietary protocols to stress DPI, application awareness and other processor-intensive capabilities.
- **Real network conditions**: Realistic testing means the power and complexity to create the dynamic, time-varying conditions found on deployed, production networks. For security testing, this includes the extreme congestion typical of DDoS attacks

Testing with realism is where expertise makes the difference.

TIPS FOR CHOOSING A TEST PLATFORM

When it comes time to select a test platform to verify that your security solution will actually protect your organization there are several things to consider.

- Testing should be a core competency of the vendor, not an open-source freeware or an ad hoc solution offered on request. This means the partner is an established global name in the test and measurement industry with verifiable experience and expertise.
- The test platform must have the power and sophistication to support all the elements of test realism—real user behavior, real converged traffic, and real network conditions to stress the performance, availability, security, and scalability of the device or system under test.
- Verify that the test platform specifically stresses known software vulnerability triggers with a library of the thousands of known attacks, and that the library is updated regularly as new threats emerge.
- The platform must have the power to replicate known and potential DDoS attacks at the scale of the internet, and the flexibility to test DPI even on proprietary protocols, including support for negative testing through fuzzing.
- The system should support the latest automation tools and built-in GUI-based tools for simplifying and automating standards-based and customizable test cases.

CONCLUSION

When it comes to security, economizing and half measures can be costly. Due diligence goes beyond choosing a vendor based on the specifications in a data sheet or the response to an RFP. Real-world testing is required to validate vendor claims, verify the suitability of the solution for your unique organization and network, and quantify the degree of protection you can expect when you go live. Because testing is the key to knowing how much you can trust your security solution, the choice of the test platform is just as important as the choice of the security vendor.

ABOUT SPIRENT

Spirent Communications is a global leader in test and measurement and offers an extensive portfolio of solutions to test data centers, cloud computing environments, high speed Ethernet networks and services, 3G/4G wireless networks and devices, network security and global navigation satellite systems.

Spirent solutions for security testing include:

- **Traffic Detection and Classification**: Verify that the latest applications and protocols are detected
- **Application Control**: Validate the ability to control detected applications through features like white listing, connection/rate limiting, application QoS, URL filtering and data loss prevention/data exfiltration
- **Congestion Management**: Confirm bandwidth and connection-rate control capabilities
- **Policy Enforcement**: Ensure that applications do not evade application signatures
- **Scalability and Performance**: Validate the ability of the network security components (e.g., IPS/IDS, ALG, proxy and NAT) to handle millions of users running real applications
- **Security**: Verify the detection and prevention of malware, spam, DDoS and known attacks, and the effectiveness of fuzz testing and application white/black lists


TESTED
WITH
SPIRENT