FEATS OF STRENGTH

PROFILES IN SECURITY

VOLUME 2 / ISSUE 1

PUBLISHED BY K LOGIX

Be Confident

The Importance of Being Prepared

K logix

Be Confident

Three Pillars of Confident Security Programs

WHAT IS A CONFIDENT DATA SECURITY PROGRAM?

At K logix, we believe that the future of data security is here. It is time to move beyond the fear, uncertainty, and doubt that has been the driver for the IT security industry. Let's face it, cyber attacks and exposures have been a surefire way to get budget for security investments. But this approach positions security as tactical, reactive, and non-strategic. It does nothing to engender trust or respect amongst executives.

We are working with our clients to create prepared security programs that align with business objectives. These programs move security from a reputation as a cost center to an organization that has a positive impact on business direction.

A STRONG PLAN

Thinking strategically about data security and aligning with business goals enables the organization to move from a reactive to a proactive security program. A proactive program accounts for the most critical data, is aware of data as it moves through and outside of the company, and accepts that attacks will inevitably occur. A strategic security plan prepares you to effectively mitigate threats, address issues, and understand the impact on performance and revenue. Importantly, a prepared security posture creates a confident security team that is certain of its ability to positively impact business goals.

REPUTATION & RESPECT

Across our clients, we see that the most successful security organizations have strong reputations with the executive team. When you have a strong reputation among executives, you have more power, which means more budget and authority to make the right security investments. You will not engender respect from executives, without a strong plan, that's why creating a strategic three to five year plan is paramount.

RESOURCES & PREPARATION

Successful security teams are fully-staffed, highly-trained, and constantly expanding their knowledge base to react to changes in the business environment, the threat landscape, and technology improvements. A team with the right resources is able to think more strategically about the security program and its impact on company performance. A well-prepared security team is a confident team, and one your organization will be confident in as well.

What this means for you...

>> Be Confident Leaders <<

IT security organizations have the opportunity to truly impact business performance with sophisticated programs that provide critical advantages in revenue, reputation, and strategic direction.

We are proponents of this evolution of IT security. Let us show you how to take your organization to the next level.

K logix eBook:
5 Tips for Security Product Optimization

K LOGIX DIRECTOR OF TECHNICAL SERVICES RICK GRIMALDI EXPLAINS TIPS TO OPTIMIZE FUNCTIONALITY AND PERFORMANCE OF YOUR SECURITY TOOLS.

A common problem for large enterprise companies is poor security system optimization. The typical enterprise organization has more than 50 security products in their environment, but with over-burdened and under-trained teams, they effectively leverage only 10-20% of those technologies.

1. Don’t Let Workplace Politics Impact Policy

When it comes to protecting your data, policy is just as important as the technologies in place. The policies will govern how technology is used, who can access information, and how they may interact with that data. An out-of-date policy or an ignored policy is not effective.

2. Train Your Admins Appropriately

It is important to invest annually in product training for administrators to ensure they are skilled to best leverage the technology to meet the business objectives and make updates as changes in the environment dictate them.

3. Change is in the Air

Vendors make important updates to product functionality as they respond to threats and vulnerabilities as well as network performance issues. It is important to review these changes to ensure they consistently align with policy.

4. Have a Rapport with Reports

The most under-utilized functions of any security product are the report and log features. It is best to work with a systems integrator to identify the best reports to leverage and how to take actionable steps based on reported information.

5. Take the Longview

According to a survey done by Crossbeam Systems, over half of all companies report they only evaluate performance needs less than one year in advance. As a result, companies are implementing technologies that may not serve long-term business goals. It is necessary to annually assess how a product supports business goals each time goals are set.

50+

Security Systems in Most Enterprise Organizations

<5

Number of fully leveraged security systems in most companies

$12B

Wasted

PER **YEAR** ON

UNUSED TECHNOLOGY

INTERESTED IN OPTIMIZING YOUR SECURITY INVESTMENTS? WE CAN HELP.

K logix Product Optimization Program

This annual service helps clients fully leverage their existing security systems. Our expert team helps you:

>> **Align Technology to Business Objectives**

>> **Maximize Value**

>> **Improve Security Effectiveness**

Understanding and Limiting Risk

K logix Security Risk Analysis Spotlight

Most Information Security teams struggle to prioritize initiatives and resource allocation. This results in an over-extended and reactive security team with limited impact on business success. When working in a reactive manner, it is difficult to communicate benefits and to gain executive mindshare. To avoid these pitfalls it is critical that organizations perform an annual Security Risk Analysis to helps align security goals with business goals.

SOLUTION

The K logix Security Risk Analysis helps clients understand their information security requirements as they relate to business-value and impact on organizational goals. The existing security program, including all controls and countermeasures, is reviewed and considered in relation to the organization's specific needs as well as industry-wide best practices. Any gaps are identified, documented, and prioritized.

Our proven process leverages our years of experience helping organizations develop successful risk management programs. This process is based on industry standards, including NIST and ISO, and is customized to meet each client's unique needs. We identify vulnerabilities, threats, and the resulting risk to the client's assets. Clients use the results report to improve performance, gain executive support, and better communicate the value of information security enterprise-wide. Our Risk Analysis process includes:

- **Business Goal Discussion** – The first step is a high-level discussion of business priorities with key stakeholders.
- **Role-Based Interviews** – Discussions with IT/IS teams, HR and legal, and senior executives determine each group's relationship with the security program, their requirements, and the knowledge of security procedures and policies.
- **Review of Assets and Business Processes** – Identify information assets and rank their impact on the business.
- **Gap Assessment** – Review current information systems security architecture, controls, processes, and policies.
- **Analysis** – Our architects analyze all of the data gathered and consider the business objectives, compliance requirements, business constraints, technical constraints, existing security program, and goals of the organization.
- **Matrix-Based Report** – This living document clearly identifies gaps that exist between business objectives and security efforts. We provide recommendations for improving security, better aligning with business goals, and prioritizing efforts.

ALIGN SECURITY
with
BUSINESS GOALS

>> MAXIMIZE IMPACT

>> MINIMIZE RISK

Learn more about the K logix Security Risk Analysis at www.klogixcorp.com or call 888-731-2314

Top SANS Critical Security Controls

Tips for Tackling Controls from our Engineers

The SANS Top 20 Critical Security Controls list breaks down the critical controls that exist in the industry. The K logix engineers provide tips and commentary on them in the K logix Blog. Let's take a look at the top 2 critical security controls analyzed by Solution Architects Kevin Murphy, Dave Tasker, and Director Rick Grimaldi.

CRITICAL SECURITY CONTROL #1

INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES

Tier: 1

Attack Mitigation: Very High

Technical Maturity: High

Having an accurate inventory of what is on your network is critical. You cannot properly secure your environment without a full understanding of what devices are connected, what applications they are running, and what data they hold. The other side to this problem is that without some form of NAC (Network Access Control) solution, employees can bring in infected devices from home and connect them to the corporate network - potentially with unrestricted access to sensitive assets. K logix engineers have the knowledge and skills to assist with planning and implementation of policies and products that address these risks.

CRITICAL SECURITY CONTROL #2

INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE

Tier: 1

Attack Mitigation: Very High

Technical Maturity: High

An effective computer-based attack method would be to exploit vulnerable software running on desktops, laptops, servers, and mobile devices. This vulnerable software can be exploited and accessed using many different techniques, some very simple to perform. Most commonly, users running vulnerable browser plugins are silently re-directed to malicious sites hosting exploit kits which then deliver malware to their systems. This tremendously increases the risk for leakage of your critical data. Knowledge of the software deployed in your environment is critical to securing your assets, data, and applications. Without the proper administrative controls and inventory of applications running on your devices, you leave your network very vulnerable. It only takes one compromised device on your network to cause significant interruption and critical data loss. IT staffs should be diligent in tracking the software running on their networks, while limiting the access levels on their devices. This will allow them to be proactive, build a strong defense against attacks, and stay ahead of malware infections.

LEARN MORE ABOUT THE OTHER SANS CRITICAL SECURITY CONTROLS

View Past Reports on the SANS Critical Security Controls on our Blog at www.klogixcorp.com/blog.

MageMojo Boosts Security and Ensures Availability Using F5

THE COMPANY
A Magento e-commerce hosting provider

THE PROBLEM
DDoS attacks took the company offline on Cyber Monday, costing its e-commerce site customers significant revenue

THE SOLUTION
Big-IP AFM and Big-IP ASM on the VIPRION Chassis

THE RESULT
The company has ensured scalability and availability with reduced expenses

Magento e-commerce hosting provider MageMojo needed to improve security after a series of distributed denial-of-service (DDoS) attacks that took its site offline on Cyber Monday. Consolidating its DDoS mitigation and firewall needs in a high-performance F5 solution, MageMojo strengthened both its security posture and its business.

Business Challenges

MageMojo didn't realize it had a security problem until the worst possible time: Cyber Monday. The company hosts approximately 2,500 e-commerce sites running on the open-source Magento platform, and on one of the busiest shopping days of the year, a series of distributed denial-of-service (DDoS) attacks took out its network—and its customers' sites—for several hours.

"Our customers lost business," says MageMojo co-founder Eric Hileman, "and we lost business." Even worse, MageMojo's previously stellar reputation had been tarnished. Hileman knew they had to find a solution that would allow the company to mitigate any future attacks and regain the trust of their customers.

MageMojo maintains its own network to ensure fast page load times and boost its customers' SEO rankings.

MageMojo needed to implement a security solution that could mitigate malicious attacks and keep its customers' stores available. However, the company also had to maintain low latency and high performance—all behind a network firewall as mandated by Payment Card Industry Data Security Standards (PCI DSS).

"What we needed," says Hileman, "was a true data center firewall that scaled easily, was highly available, offered layer 7 inspection and manipulation, and was ICSA Labs certified."

Solution

To reduce the possibility of further crippling DDoS attacks and network downtime, the MageMojo team looked at several solutions, but none of them offered the complete package of DDoS mitigation, application-layer security, and scalability the company required.

After several calls with F5 engineers, MageMojo opted to implement the proposed solution, which is built upon the extremely high-performance VIPRION chassis and modular blade system to fulfill the company's needs for seamless scalability.

BIG-IP Advanced Firewall Manager (AFM) provides MageMojo with the required ICSA Labs–certified firewall, while BIG-IP Application Security Manager (ASM) delivers visibility into and control over layer 7 application-based attacks. BIG-IP Local Traffic Manager (LTM) handles load balancing and ensures low latency and high availability regardless of network conditions.

Benefits

MageMojo deployed an F5 solution portfolio that empowered the web hosting company to protect its network against DDoS attacks, improve layer 7 security and flexibility, enable rapid and easy infrastructure scaling, comply with PCI DSS regulations—and reduce costs.

DDoS mitigation ensures high availability

Built on a full-proxy architecture, BIG-IP Advanced Firewall Manager fulfills MageMojo's needs for an ICSA Labs–certified firewall, while taking advantage of the high performance of the VIPRION system.

Protects critical applications

MageMojo deployed BIG-IP Application Security Manager to protect against those layer 7 attacks with its agile, certified web application firewall and comprehensive, policy-based web application security.

BIG-IP AFM also dynamically boosts performance and helps MageMojo keep latency low with application optimization and acceleration technologies such as compression and SSL offload.

Reduces expenses through consolidation

With the F5 solution, MageMojo has all the equipment it needs to mitigate DDoS attacks, strengthen application-layer security, ensure high availability, comply with PCI DSS regulations, and scale seamlessly—in one central device.

The VIPRION system also allows the company to support large amounts of traffic, which enables it to buy bandwidth directly from the carriers in bulk—a significant cost savings. "In the end," Hileman says, "we saved over 70 percent consolidating with F5 instead of buying all the individual components or going with a third-party mitigation service."

Ensures availability with seamless scalability

MageMojo remains focused on ensuring the availability of its customers' sites. The VIPRION system allowed MageMojo to start small with a single blade and then scale quickly and seamlessly by inserting more blades into the chassis.

NICOLET NATIONAL BANKS ON PALO ALTO NETWORKS™

THE COMPANY	THE PROBLEM	THE SOLUTION	THE RESULT
Since opening in 2000, Nicolet National has served the community of Green Bay, Wisconsin.	Increase application visibility for compliance reporting, enhance security and consolidate security infrastructure.	Palo Alto Networks PA-4000 Series next-generation firewall for granular visibility of threats, better control of Internet applications and lower operational costs.	Increased application security and user protocols. Improved compliance reporting. Reduced operational costs. Heightened visibility into threat landscape

Nicolet National Bank offers localized, knowledgeable decision-making, wealth management and investment services designed to create long-lasting relationships within the communities it serves. Since opening in 2000, Nicolet National has served the community of Green Bay, Wisconsin, growing in assets to $500 million.

NETWORK-CENTRIC VISION VERSUS PALO ALTO NETWORKS VISIBILITY

Nicolet National Bank was satisfied with the security level it had achieved by deploying a variety of products. For seven years firewall software from another vendor coupled with other appliances, had been employed to stop potentially hazardous Internet traffic on its corporate network. And while Nicolet National's IT staff would have preferred greater visibility into risk and real-time security events on its network, and to better understand which applications we're being used, it was pleased with its overall security posture.

Despite this, the company decided to conduct a routine competitive analysis just to see if other solutions might offer more capabilities or unforeseen advantages. During its review, Nicolet National became intrigued by Palo Alto Networks' approach to security, which differs from other vendors by wedding application and network security together in the firewall. Thus, it decided to evaluate the PA-4000 Series next-generation firewall to determine if it might deliver more visibility into their security posture, ideally with simplified management and maintenance than the bank's current multi-vendor environment required.

AN EYE-OPENING EVALUATION

The analysis of the PA-4000 Series produced several revelations for Nicolet National's IT team. Foremost, the system offered more granular information to afford Nicolet National an unprecedented view of the applications and data entering and leaving the company's network, such as attachments and zip files. "The degree of visibility allowed by the PA-4000 Series is dramatically better than that we've experienced with previous products," explains Jon Biskner, Chief Information Security Officer for Nicolet National Bank. "We really liked how we could dig down into potential threats on our network.

Impressed, Nicolet National confirmed that all of its applications are compatible with the PA-4000 Series and began to install the system. They began with an IT-only deployment, but quickly transitioned to a full-fledged firewall deployment, with all of its employees, applications, and rules running through the PA-4000 Series. The heightened network visibility and monitoring the system provides enables Nicolet National to implement application usage policies for its employees, and reduce the bandwidth and productivity drains associated with non-business applications.

The company found the PA-4000 Series superior at tracking application and network activity and making the information readily accessible. To review information in network logs, all a Palo Alto Networks user must do is log into the system. "Using the PA-4000 Series, I really like the ease with which I can review logs and gain visibility into our network," continues Biskner.

"It's kind of eerie because compliance auditors used to ask me all the time if I review our network logs. I would tell them they're crazy, we get millions of hits a day! Plus traditional firewalls don't look at applications. But now I can literally review those logs and tell anyone what's going on in minutes, which facilitates our compliance reporting."

A BANK SAVES MONEY

Nicolet National Bank is so bullish on Palo Alto Networks that it is consolidating its entire security infrastructure around the PA-4000 Series. This is enabling it to consolidate several functions into the PA-4000 Series that had been spread across multiple vendors' products in its security environment. These products include filtering appliances, an outside firewall and the tools Nicolet National currently uses to manage their network firewall logs.

"In the future, we believe Palo Alto Networks will allow us to eliminate the need for some of the programs we currently use, which will help us save on costs," says Biskner. "Moreover, we're finding the PA-4000 Series so easy to use that we don't need external engineers to help us program it. We're able to do it all on our own, which saves us even more money. Sometimes ensuring business applications are available and protecting customer and operational data are competing demands, but Palo Alto Networks helps us achieve both goals."

Did you know...

These K logix Consulting Services grew over 100% in the past year. Contact us to learn how you may benefit from these services.

Security Risk Analysis

Gap Assessment

Application Assessment Services

Project Advisory Consulting

K logix
233 Harvard Street
Suite 308
Brookline, MA 02446