



Developing, Applying, and Maintaining a Security Program

Written by Steve Hall - IT Manager & Services Consultant for World Data Products, Inc.

Have you ever heard the statement, “Networks evolve”? Discover tips on developing, applying, and maintaining a security program that will evolve as your company evolves.

Page 2: Developing a Security Program

Page 5: Designing and Applying Security Policies to your Network

Page 7: Maintaining and Monitoring the Security on your Network

Developing a Security Program

Have you ever heard the statement, “Networks evolve”? Ask any System Administrator whether they think this statement has merit and most will agree. The company grows, and one server turns into two which turns into ten; or, one location turns into five, and before you know it, your network has evolved into its own entity.

As this entity grows, the administrator’s time is consumed, causing some priorities to take a back seat. One area I have seen take a hit is security. As threats change, having a solid security program is important to helping identify and react to these threats, and when your bandwidth is stretched, it is easy to let security slip to the back burner. However, security is much too important to any organization to not keep it a priority.

This whitepaper is intended to give you examples and provide reasons why a sound security plan is so important. The following will provide you with an outline for how to develop and implement a secu-

urity program for your organization and/or clients.



Business Needs and Risks

When developing a security program, there are some initial critical facts you must identify:

Company’s position on security - You need to find out the business’s stance on security. As a security professional, it is your responsibility to inform the

decision-makers on the risks and the cost/benefits related to bolstering the company’s security vs. doing nothing. At the end of the day, security is ultimately a business decision. The acceptable level of risk tolerance must be defined by the company’s decision-makers.

Company’s ‘crown jewels’ - Identifying the company’s most valued assets and what it is willing to spend to protect those assets is critical. For example, a sales organization would place a high value on customer contacts whereas a medical device manufacturer may place inventions or R&D projects at the core of what must be protected. I’ve noticed the answer to this question may vary depending who you ask in the company. For example, a VP of Finance may place accounting data at the top of the list while the Director of Operations may identify people as the number one asset.

It is your job to encourage those people to talk together and decide what is most important to the

organization as a whole. Once you know what keeps your decision-makers up at night, you will have a starting point to know where to focus your efforts when planning and designing your security program.

Risk assessment - A good way to identify a company's priorities is to do an assessment. This will help define the top high risk issues in your environment. Furthermore, it will allow you to take bite-sized chunks out of a potentially overwhelming situation. It's a lot easier to remediate the top twenty issues and feel like you are making headway as opposed to trying to tackle all of your security woes at once. Finally, a risk assessment will give the stakeholders a view into the state of the security on the network.

The end result of this step should help identify the company's security goals and define a project list for your security fixes. In other words, you should have a blueprint to assist you in designing a secure network and business sponsorship to address the top priority issues.

Compliance requirements - Compliance is yet another business driver when developing your security program and will shape many of your business and design decisions for you. De-

pending on what regulatory compliance your company falls under, your security design will vary.

It is important to work with your compliance team to thoroughly understand your obligations before defining your security program. If you are regulated by some type of compliance, don't stop securing once you have met compliance. In many cases, compliance is a baseline or a minimum of what the company requires. Meeting the requirements doesn't automatically make you secure. Use common sense, consider the data you are protecting and consult your decision-makers to reach the best decision for the organization.

Policies

Once you've gathered your initial facts, it's time to sharpen the pencil and develop your security policies.

Create your team - Define a security policy team to write the policies. Members of this team may include the Security Administrator, IT Staff, Management, HR, Legal/Compliance and representation from employee users. These stakeholders help the company create and endorse the direction of security. If you don't



have legal counsel available on staff, you should have your company's legal advisors review your policies before rollout.

Develop a flexible framework - When writing your security policy, consider creating a frame-

work that will allow for flexibility. A modular approach, in other words, splitting one large policy into smaller policies, will allow you flexibility as business needs change. Below is a list of some key policies that are essential to a good security policy:

- Acceptable Use Policy
- Privacy Policy
- Remote Access Policy
- Network Maintenance Policy
- Incident Handling Policy
- Monitoring Policy and more!

Whether you utilize a third party vendor to help you build your security program or develop the program in house with existing staff, there are many resources on the web related to policy development.

Plan Completion & Rollout

Communicate policies to your users - Once you have completed your security policy, you now need to educate and inform your users. You should have your users sign a consent/ acknowledgement form, recognizing that they have read, understand and agree to abide by the policies. If your company should experience a security breach as the result of a user, you then have a policy in place to take performance action as needed.

Review! - Just because you create your policy doesn't mean that you can now forget about it! Reviewing the policy is necessary especially as the company grows and experiences change. An effective security program is cyclical in nature and will require a re-assessment both annually and as incidences happen. Always reserve the right to change policy if your current policy does not effectively meet your company's business needs. You should also note that changes made to any of the policies should be proactively communicated to your users.



Enforcement - Policy enforcement is a very critical piece of the plan. Why invest the money and time in developing a program if you have no intention of following through with it? Again, remember what your decision-makers identified as the company's 'crown jewels.'

You can enforce policies any number of ways. For example, in your Acceptable Use Policy, you can state that the users are not permitted to access adult websites or other inappropriate sites. How you enforce this part of the policy could be done both automatically and/or manually:

- You can achieve enforcement by using web filter tools to create compliance.
- You could conduct a manual solution of random checks of local machines.

Your method of enforcement will vary based on your budget & available staff/resources. The point, though, is to enforce your policy consistently. Policy development is important for the security professional because it gives him/her a baseline or something to measure against..

A policy also helps develop and shape the company's security design considerations. Now that your policy has been defined, you have a good blueprint and starting point on where you need to go from a design perspective!

Designing and Applying Security Policies to your Network

Now that you have identified policies and the company's responsibilities for security, you can start your design. It is not likely you will get a clean slate to design whatever you want. It is more likely you have inherited the network, and it is not ideally setup the way you would like it to be. In either case, you can add value by bolstering the security or designing from scratch. There are many different methodologies from various vendors, but most of the methodologies all touch on a key foundation... Defense in Depth. Civilizations have understood the concept of Defense in Depth for ages.

Militaries have often designed their defenses in a layered approach. For example, aircraft carriers have destroyers that provide a perimeter and act as an early warning system. Obviously the carriers are the "crown jewels", however, the destroyers, even

though they are expensive, are more agile and made to detect threats and take action in order to protect the carriers.

This concept can easily be applied to designing networks and network security. Like the destroyers that surround the carriers, network design and security form a perimeter of defense.

Defining/securing your perimeter

Defining network perimeter in today's business environment can be challenging with remote work forces, remote vendor management and client extranets, or federations with partners.

In order to get a good starting point, consider areas of responsibilities and devices that you have direct

control over. Also ask if you will be utilizing a DMZ for hosted public servers.

Once you have a defined line drawn in the sand you can then start to document what traffic equals normal traffic or expected traffic. I highly recommend documenting traffic flow diagrams so you have a base line of what the traffic should look like on your network.

Once you have these items identified you can now select the products that fit your company's requirements such as firewall, IPS, Content Filtering, web application firewalls and anti-virus. Consider vulnerabilities and risks that could be exposed with the technology being used and work to eliminate or reduce the attack surface of your devices.

Inside the Perimeter

Once the perimeter is secure, secure the network routers and switches. Always harden these devices as they handle all of your network traffic. If there was a compromise or a man in the middle on your default gateway, it is game over.

There are open source and commercial software that will allow you to run your configurations through a check to ensure they are secure and correct. The Center for Internet Security also has resources and guides for hardening and configurations.

Servers and workstations should also be hardened. Minimize the attack surface by uninstalling and shutting off any unnecessary services. If you have an active directory, you can use group policy to deploy many security features globally.

You may be stuck with some legacy systems that are not tolerant to patching, or they are simply too old to have any support for patching. In cases like these you can use isolation with VLAN's and monitoring to help reduce risk of these systems that cannot be decommissioned.

Physical Security

Don't forget about the physical security of your network. Someone with physical access to your internal systems can be game over! Coming from the inside, a trusted source can put the company at a severe disadvantage. Whenever possible consider mantraps, card access, biometrics, video surveillance, and locking accessible switch ports down to only known devices.



Staying Healthy

Having a patch management process is yet another important aspect of keeping a healthy environment and mitigating your exposure to new threats. Staying patched on all software, and not just operating system software, is also very important. There are many third-party applications that may be overlooked for patching. One thing I notice a lot is that administrators do not proactively monitor logs. Only when some-

thing happens do logs get reviewed and, by that time, it is too late.

In many cases proactive monitoring of logs can head off potential problems. If there is budget, make sure to add a monitoring solution. Even if you don't have a budget for it, there are open source solutions (depending on your company's stance on open source). All of the devices on your network should be able to talk SNMP, SYS-LOG or WMI. By having all your devices report these logs to your management server, you will be able to proactively manage your network, which will help with long term reporting and trending.

Detect + Response = Exposure

The goal is to make sure your protection outlasts your detection and response; but remember, the closer your exposure time gets to zero the higher the costs. These are all considerations to keep in mind when deciding what network design is right for your company.

Although there are many more aspects that I haven't touched on, this will start you down the right path of completing your design, and implementing it. Check with your vendors on their security practices and get their recommendations on securing their software/hardware.

Maintaining and Monitoring the Security on your Network

Now that your design and implementation are complete, you will transition to maintenance and monitoring mode. This is the day-to-day functioning and maintenance of your systems.

Patch/Change Management

I mentioned patch management in the design and implementation section, but this becomes a task in the day-to-day management of your systems as well. Depending on your systems, it is likely you will be patching them off-hours or during maintenance windows. Either way, before deploying your patch, you should always test the patching on a test system. Also, be sure to remember there are many pieces of software that could be overlooked.

Microsoft OS and application patches are more

commonly done because they make it easy for the user. Microsoft has the biggest target on them, so by proxy, they have gotten really good at the process of rolling out their fixes. True, sometimes it feels like the patching will never end, but it beats the alternative or having a vendor not patch their systems when there are known issues. Now set aside the OS and consider all the other applications that are installed on your systems...Adobe Reader, Adobe Flash, CD Burning software, Firefox, iTunes and many others. There are solutions out there that will help you do patching above and beyond Operating System patching.

Change management is another function that is a routine or day-to-day function. Organizations vary on the formality of change management processes. Some are very formal, while others may not have

anything formal at all. In all cases it is good to have some checks and balances of your change management program or process. If you are a small organization you may simply have something like a spreadsheet or helpdesk software in which you document what was changed on key systems. This helps you keep track of changes. It can also help you pinpoint problems in the event of a change breaking something in a production system.

If you are in a larger organization, you may have forms that have to be filled out which detail the changes to be made, the impact, the estimated downtime and the back out procedures. Even after all that you still may need approval by a change management committee. Although most find this process painful, it can really help track changes and minimize unnecessary downtime.

Monitoring/Testing

Proactive care of your network includes Monitoring and Testing. The types of questions that you should continue to ask are:

- Are my systems working as designed? Are they protected against intruders? How do I know?
- Are my Policies effective? Are they being enforced? How do I know?
- Are my systems secured? How do I know?
- Was the response enough for a given security event?
- Are we compliant? How do I know?

Monitoring and Testing your systems and processes will help you tune your security program. Many organizations are required to have third-party penetration testing done in order to test their systems. Some organizations are not required to do third-party testing, yet they still will, or they will do their own internal testing.

The organization has to determine if they have the competency in-house, or if they need to hire an outside organization to help with testing. Also they may have the skill set but not the time. Even if a third party is used for testing, it is still a good practice to do your own internal

testing. There are many pieces of software, commercial and open source, that can assist you in performing an effective internal test.



Security Awareness & Continued Training

Having some type of awareness program is also critical. A well-informed user community makes the organization more secure.

A suggestion would be to send email updates of current security threats in the wild, replayed in laymen's terms. It's true some will just delete the email and not read it, but some will read it and benefit from the effort. Intranet sites as well as security updates or tips at departmental or quarterly meetings are also some good

ideas. The goal is to raise awareness however you can. This will help you as a security professional and will also increase the company's overall security in the long run.

In addition, organizations need to invest in their security personal by helping them stay up to speed with security training or allowing them to go to trade shows focused on security. The better informed everyone is, from the typical end-user to the security administrator, the better your chances are for a secure environment.

Rinse and Repeat

Throughout the whole process you should be evaluating your process, systems and procedures and fine tuning them. When designing, and then implementing, a program like this you will find that sometimes what you originally decided in a process or procedure may not function like it was intended. Continual tuning with help your program evolve and develop into a finely tuned security program.

About World Data Products, Inc.

Since 1987 World Data Products has been a market leader acting as a partner for thousands of enterprise and government customers providing OEM quality refurbished server, storage, and networking solutions “on demand” and at substantial savings.

We provide leading lines of hardware plus a full range of spare parts, maintenance, financing, lifecycle management, and asset redeployment services which increase our customers’ return on their IT investment and improve the manageability while reducing the risk and complexity of their IT operations.

We can deliver “factory fresh” and fully serviceable refurbished hardware with great value for our customers.

We are one of the largest global secondary market makers in refurbished high end IT equipment and have been since our earliest days.

Every product we deliver to our customer has been

fully reconditioned and tested at our Corporate Technical Center to meet or exceed original factory performance specifications, and every system we ship is guaranteed to qualify for third party maintenance.

World Data Products helps enterprises and governments increase the yield and useful life of their IT investment and improve IT asset manageability. This is achieved in three key ways: first, by providing fully tested refurbished, used, and new hardware solutions; second, by facilitating the economical acquisition of system components and parts, upgrades and replacements; and third, by purchasing surplus hardware, thereby maximizing residual returns for customers.

Unlike new IT equipment vendors, World Data Products is driven exclusively by customer requirements, responding to customer-triggered requests to source or dispose of specific systems. World Data Products customers can extend the lifecycle of existing installations and more flexibly manage, even

delay upgrades, increasing return on investment (ROI) and reducing total cost of ownership (TCO).



Our staff of hardware specialists is ready to help you save money and gain control throughout your hardware product lifecycle.

Call us today at 1.888.210.7636 or email us at info@wdpi.com for more information.