k_Street Consulting

WHITE PAPER

Best Practices for Protecting Your Cyber Kingdom

k_Street

Defending your business from data leaks and hackers is much like protecting your kingdom from an advancing enemy. Defenses have to be manned along the path up to your castle wall and even past it.

The following is an outline of several possible lines of defense to be considered when determine your cyber security program. This list is not intended to be all-inclusive of all available security controls, nor are all measures listed below needed in order to be considered secure; rather this is a general list to help develop a mindset for how you may view your defenses and where controls may be inserted.

At the end of this list, we will educate on how to determine what controls are reasonable for your business and budget.

Please note these recommendations apply only to general corporate data access and resources. Governmental or classified data, as well as employee or customer financial data, personable identifiable information, private health information and information related to citizens of the European Union may require greater security measures than discussed here.

The Internet is the path that all data, visitors, and criminals follow to gain access to your kingdom. Along this path we can put various sentries to monitor this traffic.

Content Filtering

This is a service or appliance that monitors what websites your employees access. When a user accesses a website, they are opening a path both outbound and inbound to your network. Accessing a compromised or questionable website may allow for threat vectors to gain access and execute malicious code. A content filtering service will help prevent access to such sites.

Anti-Phishing

Phishing is one of the most common vectors for stealing data or causing malicious code to be introduced into a network. An anti-phishing service will help train and test your user base how to detect and avoid phishing emails.

Before entering your network castle, there are a couple of guards you should have to inspect the data coming in.

E-mail anti-virus

Your email service or a third party service should have a pre-virus scan of all emails before reaching the end user. The end user will still have their own anti-virus application, but this pre scan will help block the email based virus before the user even has a chance to accidently trigger. It should be noted these are not 100% full proof. Anti-viruses can only stop known viruses, but it is still critical to have these scans performed.

Anti-spam

You email service and / or a third party service should be incorporated to cut down the amount of bulk email traffic or spam mail your staff receives. Often these spam messages not only consume time and labor disposing of, but can be vectors for more malicious activity. Also, anti-spam services can be a preventative measure for some phishing emails as well.

E-mail redundancy services

These are a variety of features your firm may find useful such as:

"Spool-and-suspend" which allows you to pause email transport. This service will collect all inbound email and hold delivery to your email server during outages such as down service or migrations.

"E-mail Compliance Archive" which maintains a separate copy of all inbound and outbound email for compliance purposes such as is needed by regulation in financial services.

"E-mail Continuity" which is a secondary email service that you can access to send and receive email should your primary service go down.

It is critical for your network to have a secured perimeter surrounding your resources. On an average day, every network connected to the Internet will experience hundreds of automated port scans from bots looking for low hanging fruit to exploit. But just like your skin protects you from daily contact with germs, industry standard forms of network security will protect your network.

Firewalls

By far, this is one security device that is a must have for every network. At a minimum firewall services must be provided by your Internet Service Provider's on premise equipment such as the Internet router or modem, but, it is highly recommended using a standalone firewall appliance for this function. Internet routers protect your network by only saying yes / no for if simple types of data are allowed in or not. Firewalls are better at protecting your network because they take an active role in inspecting the type of data traffic as it comes in. An Internet router may say email data is allowed in, but a firewall will look at that data to make sure it really is email data and not a hacker disguising themselves as email data. This is called "deep packet inspection" and most industry standard firewall do this.

Next Generation Firewalls

These are firewalls with advance features over standard firewalls. Some of these next gen firewall appliances now have the ability to "sandbox" Internet connections. This is where, in real time, each time a user connects to a website or receives data from a website, the connection is played out in a virtual sandbox first before being delivered to the end user. This allows for any malicious code to be executed before it has a chance to cause harm without any lag time.

IDS / IPS

Intrusion Detection and Intrusion Prevention Systems do just that, detect- or detect and prevent- an attempt at intrusion into your network. The way these work above and beyond your firewall is by looking for known techniques and attack procedures. Whereas the firewall is looking for malicious data or unauthorized access, an IDS or IPS is looking for malicious activity. A firewall blocks someone from coming in by locking the door, an IDS / IPS looks for someone trying to come in by pretending they are a repair man. An IDS will only detect and you will need to take action once the intrusion is detected. People use this to limit action taken on false positives. An IPS will actively work with your firewall to create rules on the fly when an intrusion occurs. Some firewalls have this feature built in, and there are standalone appliances you may implement. Our general recommendation is to use a third party service that has the ability to manage your firewall. These services provide live persons monitoring your network 24/7 and can instantly start the prevention process while notifying you of the occurrence.

Physical Security

Protecting your network is not just achieved with hardware and services. Attention must also be given to physical security. This may include requiring key access to the building, security guards requiring ID check and sign in, elevators required key access to floors, key access to office space, a receptionist to greet visitors, cameras, visitor escorts, security cables on laptops, and locked server rooms and data closets. The degree of physical security needed is dependent on the type of data you are protecting and resources. Keep in mind, much theft is targeting equipment for resell such as laptops, but, you are just as liable for the data on that equipment such as client personal information as if the data was the intended target.

Once inside the secured network, there are still several forms of protection that need to be implemented for a comprehensive security strategy.

End-Point Protection

End point protection comprises of applications on your workstations and servers for anti-virus, anti-malware, firewall, and intrusion prevention. Most industry standard applications incorporate all of these features into a single product. Once installed, make sure these applications are kept up to date and have their definitions updated frequently and automatically. Depending on the industry you are in and the type of data being protected, you may want to review the country of origin of the manufacture of the product you are choosing. Warnings have been issued concerning end point protection products made outside of the US being co-opted for nefarious purposes.

Patch updates

Insure that all operating systems and applications are getting security patch and critical updates applied on a regular basis. Same for devices and firmware. Workstations should be set to automatically update, while servers should have mandatory reoccurring update time windows in which your IT staff or provider performs patch and updates installation manually, preferably on a monthly basis, but as necessary for emergency fixes for what are called "zero day" exploits, exploits discovered by hackers who go on campaigns to utilize these discoveries before IT staff have time to patch. Automated updates can be set to directly pull updates from the developer, or you can implement a patch management solution which downloads the updates and distributes them upon your approval.

Passwords

Passwords are the keystone to all data security. All systems, devices and users should have unique login accounts with secure passwords to help limit and monitor access. Passwords should be complex, meaning having a minimum of a combination of 3 characteristics such as upper case, lower case, numbers, and special characters. Length should be no less than 8 characters but preferably 10 or more. Passwords used externally should be different than passwords used internally and these passwords should be mandatorily changed at a minimum of every 90 days. In addition to network access and systems, devices such as phones and tablets should require a pass code to access as well.

Two-Factor Authentication

Depending on the type of data needing protection, an additional level of security to passwords is the implementation of two-factor authentication. This utilizes a combination of any two forms of identification. This can be any pairing of something you know like a password or passphrase, something you have like access card or a token with a changing security code, or something you are such as a palm or eye scan.

File Rights

One of the most basic forms of data protection is that of file rights. Data should be segregated on a need to know basis in which users only have access to the data necessary for them to perform their job function. File rights should be issued using security groups and users should be added to or removed from these groups. Rights should be audited on a regular basis to prevent users from gaining or retaining rights they should not be privileged to. There are various folder structures such as common data, departmental data, user data, etc. and various rights models such as Chinese Wall, Top Down or Bottom Up that can be applied. You should first classify your types of data, determine your needs, then review your folder structure and work with a security professional to construct the best way to implement.

Internal Firewalls

Additional precautions can be taken by implementing firewalls with in your network to prevent sections or departments from one area accessing the servers or another. You may have a firewall protecting the server used for payroll or HR to prevent anyone not in that department from being able to connect to this resource. This also allows for secondary protection should the network perimeter security be breached.

File Monitoring

You may want to consider employing various file monitoring applications and services to determine if a significant amount to data is being deleted, copied or moved. These actions could be a sign of malicious or preemptive behavior such as the destruction of data or data extraction. Thresholds may be set to trigger an alarm if activity occurs on a certain amount of files within a limited amount of time. Some intrusion detection systems will notify you if a large amount of data is being extricated out of the network, but this will not detect if an internal employee is, say, copying all of their customer files to a thumb drive before resigning.

Backups

The importance of data and system backups cannot be understated. Backups are your last line of defense against crypto or ransomware impounding your data, to malicious or accidental destruction of data, to a timely recovery from any form of disaster. Backups can be handled in several ways. At a minimum, backups should be a straight file copy done once a day to some medium other than the system they are backing up. There are better forms of data backup such as only backing up the data that has changed since the last backup, to backups that maintain file rights and attributes or virtual pointers, to full images of the system itself. Frequency can also be improved to more than once a day to reduce the amount of data lost should the disaster occur after a full day's work has been done but before the following backup. The medium used to store backups should be one that can maintain at least a week's history of backups and the backups should be kept both on and off site in a secure location in case of a full site disaster.

Virtualized Backups

A higher degree of Disaster Recovery and Business Continuity can be achieved with the next generation of backup appliances that create entire images of systems rather than individual data backup. These appliances create a virtual image of servers, then update the data as it changes from every 5 minutes to 1 hour. During a disaster, these virtual images may be powered on in place of the real server, to allow users full functionality with minimal loss of time and data while the production system is being repaired. These images can be maintained both on and off site depending on the degree of the disaster.

Disaster Recovery and Business Continuity Plans

Part of a good security posture is to have plans and remediation's in place should a disaster occur. A disaster recovery plan tells you what to do should a disaster occur such as a production server or application failing. A disaster recovery plan is part of a business continuity plan which is a plan that takes in consideration more than just the IT infrastructure. Rather, it will include all aspect of maintaining your business with topics such as phone systems, payroll, relocation of the facilities should the current location be rendered unusable, etc.

Log Monitoring

Reviewing and monitoring of system logs are often overlooked as methods of determine if a failure is imminent or if an attack is underway or has occurred. While reviewing logs from all devices such as servers and firewalls may be laborious to the point of unfeasibility, there are third party services and applications that can assist with detecting trends or raising critical warnings.

Segregation of Duties

Work functions and job duties that could result in significant damage to the firm should be segregated between more than one persons to prevent misappropriation. An example of this would be all financial transactions over X dollars requires a second signature, or any wire transfer requires additional verbal communication rather than just approval via email. This will allow an extra layer of protection from fraud or scams.

Once you have your kingdom's defenses in place there are a few other factors to take in consideration to ensure you are properly protecting your environment, that your protections are working, and that you have right level of protection for your needs.

Define Your Crown Jewels

Often business do not take the time to define what in fact, are the crown jewels of the business that need protecting. This determination needs to be facilitated as a discussion amongst all department heads. The IT person may think just their server data needs to be protected while the head of accounting knows of a specific function workstation that needs protection as well. Determine what type of data you have, what your business needs to have to function, and what level of protection these resources need.

Determine Applicable Regulations

Regulations are dependent upon the type of industry you are in and the type of data you hold. This may include customer or employee personal data, financial or health data, or information related to persons living in the European Union. Classify your data types then work with an IT security specialist or your legal counsel to determine what laws or regulations apply to your situation.

Testing

All of your preparation is only as good as regular testing says it is. Perform parodic testing and assessments of your network environment. Security baseline testing for patch levels and vulnerably scans should be run once a month or every quarter. Full penetration testing and testing of your disaster recovery plan should be held once a year. Users should be tested for security awareness and phishing examples regularly as well. After each testing, improvements and updates should be made if necessary, and vulnerability and penetration testing should produce a remediation plan.

Determine Cost Effective Solutions

Depending on the type of data you are protecting and various aspects of your business, it is most likely not cost effective to implement every level of protection technology has to offer. The mathematical formula for determining if a solution is cost effective is as follows:

Asset Value x Exposure Factor = Single Loss Expectancy

Single Loss Expectancy x Annual Rate of Occurrence = Annual Loss Expectancy

First, determine your single loss expectancy. Single loss expectancy is the value of an asset times your exposure factor. An exposure is whatever threat your deterrent is protecting against. Your exposure factor is 1 when a threat would cause a total loss, and is broken down into decimal for any loss that is a fraction less than total such as .5 for only 50% loss. An example is, if a warehouse is worth one million dollars, and if a tornado was to hit, you would expect only 50% damage, then your SLE is 1 million x .5 = $500,000.

Next, determine your annual loss expectancy by taking your single loss expectancy times the annual rate of occurrence for the risk you are protecting against. In our example, if we know that a tornado only hits once every 10 years, then our annual rate of occurrence for that threat is 1/10 or .1 giving us 500,000 x .1 = 50,000. Therefore we would not want to pay more than $50,000 a year for tornado insurance.

Thus, to determine if you should budget for a particular deterrent, determine the cost of the asset, time, labor, business, or even cost of reputation, related to the protection the deterrent can provide then multiple that by the amount of damage caused by your business being down if this event occurred. Next, with the assistance of your insurance company's actuarial tables or an IT security specialist, determine the chance of this occurring over the period of a year. If the deterrent's yearly cost is greater than it is not a cost effective solution. But if it's under then it's worth considering.

With each of these various methods of protecting your IT kingdom, you increase your chances of a safe and secure and cost effective network.

If you would like further information, or assistance with implementing any of these suggestions, please do not hesitate to contact K_Street Consulting for professional, certified, cyber security service.