10 Steps to Creating a Secure IT Environment

March 13, 2020 |

Every day, as a part of my work at AlienVault, I talk to prospective clients. Many of them are trying to put together a security plan for their business. Most of the people I talk to are IT professionals who, like everyone else, are learning as they go.

During my time in IT and the security industry, I have seen almost every type of network you could imagine. Most of them made sense and could be explained and I could understand why they were built the way they were. Some, not so much. During the last 10 years especially, I have started compiling network drawings and information on the many ways that networks are designed and deployed.

The following list of bullet points are my recommendations to an IT manager or business leader if they consulted me on how to put together information technology for their business. Please remember this is a fairly generic list and there are tons of deviations to take into consideration when building a network and then protecting it.

1. Policies and Procedures

Policies and procedures are the cornerstones of your IT governance. This is the “what is going to happen and how is going to happen” of your security posture, and from the big picture your entire IT infrastructure. Creating a solid policy and procedure document or documents will provide your organization with an IT and security blueprint for your initial build, maintenance, management and remediation of issues. Solid policy and procedure manual(s) will also prepare the environment to work within any framework and meet compliance requirements.

2. Gateway Security

Gateway security is essential to keeping the bad guys out. There are a number of popular firewalls on the market that will provide excellent security at the gateway. The needs of the environment will dictate which firewall will work best.

For example, a high throughput environment with a large internal IP count might require a Next Generation Firewall (NGF) that runs only a few services on board and reserves the majority of resources for ingress-egress traffic. On the other hand, an environment that requires a very high level of security but has limited WAN bandwidth may be better suited for a UTM (Unified Threat Management) firewall which runs a number of services onboard. Traditionally it also utilizes significant resources for services like deep packet inspection (DPI), data loss prevention, (DLP), gateway antivirus, website filtering, email filtering and other high-end security services.

3. End Point Security

As the old saying goes… AntiVirus is DEAD!!! Not really.

Actually, antivirus is evolving and morphing like your favorite advanced persistent threat (APT) malware. A few years back the InfoSec industry started to break new ground on digging deeper into threats and breaches using threat intelligence in real-time to actively pursue malware based on heuristic data. Heuristic data became important as technology progressed to utilize behavioral analysis based on up-to-date threat intelligence.

These progressions in the industry gave rise to Endpoint Detection and Response (EDR), which is quickly morphing into a formidable companion to traditional antivirus and antiMalware protection. The very minimum that should be deployed into an environment includes a good reputable antivirus with antimalware capabilities, however, to get a definite head start on any compromises within the environment EDR is highly recommended.

4. Identity and Access Management (IAM) / Multi-Factor Authentication (MFA)

IAM and MFA are two entirely different technologies, and for good cause. As so many tech manufacturers are trying to get rid of the password, setting up good IAM services which work as initial authentication and then a reputable MFA service that is authenticated separately from the IAM service is essential.

IAM services range from Active Directory and LDAP (Lightweight Directory Access Protocol) Cloud LDAP, and authentication services like those provided with AWS IAM services, Microsoft Azure Active Directory services, and Google Directory services. There are tons of IAM services to choose from, and the environment will dictate the type of IAM services to utse.

The other part of the equation is MFA. The industry is full of MFA providers, from Google Authenticate to Yubikey and many others. Whether it’s token based, hardware or biometric-based, MFA it is important to understand that the second form of authentication needs to be separate from the initial authentication system and it needs to be secure. For example, biometric authentication is very popular, but if it is simply used as a shortcut to enter an insecure password then it is not a secure solution.

Soft tokens that are received through Short Messaging Service (SMS), though very popular, do not provide the level of security that is often marketed. SMS in and of itself is insecure. Traditional SMS messages are sent in clear text and are subject to being intercepted or even having the SMS service broker hacked and the unencrypted messages being stolen and used to hack other larger targets. There have also been instances of “man in the device” attacks that have been used to steal tokens as they come in from the SMS broker.

IAM and MFA are probably the most important aspects of any threat posture, because not only does it control ingress authentication from the WAN, but it also validates and authenticates internal users requesting access to various resources.

5. Mobile Protection, Remote Access, and Virtual Private Networks (VPN)

Mobile devices are more popular than ever, especially as millennials become more prevalent in the workplace. This creates an especially unique situation for InfoSec pros who are tasked with securing modern environments.

The options for securing these environments is growing on an almost daily basis. From mobile device management (MDM) to wireless networks that prevent devices from connecting to the network unless they pass authentication and a scan to ensure the mobile device meets the preset requirements. Examples include not allowing 3rd party downloads outside of the prescribed manufacturers’ store, ensuring anti-virus and anti-malware is installed and up to date and ensuring the mobile operating systems is updated to the prescribed revision range.

Something else to note more and more AV/AM and EDR manufacturers are making versions of their solutions to accommodate most mobile operating systems.

Remote access and VPN to the environment has always been a tricky topic. Anytime an employee wants to, or is required to connect to the environment for work purposes, most IT professionals pop a couple of Tylenol because they know a headache is coming.

Not all VPNs are created equally. Simple VPN connections can be made with a firewall or gateway router (even the cheap ones) with a simple handshake and a GRE tunnel to all the remote endpoints to pass traffic through the open VPN ports and into the environment. This is a minimal security solution and HIGHLY not recommended for a security-intensive environment.

The better solution would be to set up a better VPN concentrator or gateway firewall that can handle VPN tunnels. Set up IPSec connections. This is a bit more work because you have to load a security certificate on the gateway concentrator and on the IPSec software installed on the remote endpoint. However, the extra work is essential in creating a secure handshake and connection between the two devices. IPSec connections are great and they can be created with very fast speed and provide more security than a GRE connection.

However, I believe the IPSec connection running with AES256 and higher encryption over TLS are the most secure connections. It uses the most modern security type, an extremely high level of encryption, and requires a static RSA certificate to be installed on both endpoints. The same goes for static VPNs or site-to-site VPNs. The IPSec connection will create secure AES256bit or higher encryption for the SSL Tunnel as well as encrypting the payload with secure AES256 bit or higher encryption while in transit over the VPN connection.

6. Wireless Network Security

The wireless network industry has matured significantly over the last 10 to 15 years. In the old days, you set up an access point with a WEP security code and everything was great. Easy to deploy, easy to connect to and fast. Man those were the days. Then, in 2001, 3 researchers working at Berkeley produced a paper named “(In)Security of the WEP algorithm“. They found the following flaws in WEP:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- A dictionary-building attack that, after analysis of about a day’s worth of traffic, allows real-time automated decryption of all traffic.

- Furthermore, there are currently attack vectors on the TKIP. There are two attacks known against TKIP:
- Beck-Tews attack
- Ohigashi-Morii attack (which is an improvement on the Beck-Tews attack)

Both of the two attacks on the list only could decrypt small portions of data, compromising confidentiality. What they can't give you is access to the network. To give you an idea of how much data can be recovered, a single ARP frame would take around 14-17 minutes to get the plain text. Getting useful information with this type of attack is very improbable (but not impossible) considering the rate of recovery. The only attack known, besides flaws in the firmware of some routers, is brute-forcing the WPA key. Generally, the key is generated as follows:

Key = PBKDF2(HMAC−SHA1,passphrase, ssid, 4096, 256)

The algorithm takes the type of HMAC to be used, the passphrase, the ssid as salt, the number of iterations the password will be hashed and the final length of the generated hash. Considering this algorithm is meant to prevent hashed passwords from being broken, it can take a huge amount of time. The only reasonable attack would be to use a dictionary attack (hence it is important to use long passwords containing characters, numbers, and letters).

Also, note that you need to change your SSID to something very random. Rainbow tables have been generated for the top 1000 used SSIDs. Which can reduce attack time significantly.

WPA also supports AES (which can be used instead of RC4). While AES is more secure than RC4 the biggest problem of WPA is still present, namely, the integrity check is still done using TKIP-MIC.

Other things to consider when deploying a network system are things like:

- Ease of management
- Centralized or cloud-based management
- How the rogue AP detection works. Does it go after non-system-based AP's as rogue or does the system utilize logic to decide which AP's are rogue and which AP's may be legally active depending on activity, SSID names and perhaps MAC addresses? ***Please note there are FCC regulations against rogue AP detection and destruction***
- Every manufacturer has their own unique functionality around rogue AP detection and many other security functions. Iit is advised that the purchaser and IT department perform due diligence before making a decision.
- Other things to look at are authentication types, 802.1x, Active Directory, LDAP, AAA services are some of the more popular authentication types.

- Lastly, it may be important to ensure that the system employs a guest WiFi authentication system. This will prevent, or at least deter, spoofing of the guest network as well as giving the WiFi owner an opportunity to collect information on every asset that connects to the guest WiFi. This is great for marketing and accountability purposes.

7. Back up and Disaster Recovery

Backup and disaster recovery (BDR) services are essential to an organization's incident planning to stay up and running in the event of a major catastrophe. BDR consists of backup and recovery of key IT systems and planning for the continuance of operations in the event that the organization encounters catastrophic events. Such events may that cause the corporate or remote locations to become inoperable, destroyed or infected with destructive malware such as ransomware. There is an entire industry built around just back up and disaster recovery operations. It has been said about the growth of the industry as "this ain't your Daddy's old tape drive anymore".

When choosing a BDR service you absolutely need to ensure that they will meet the organization's needs 100%. Ensure that they provide a Service Level Agreement (SLA) of a minimum of 99.999% reliability. They should have a plan to return your data expeditiously. Lastly, the BDR firm must have a training and test plan to ensure the first time data is recovered for your environment is *not* during the catastrophe.

8. Environment Visibility

Security information and event management (SIEM) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. The acronym SIEM is pronounced "sim" with a silent e.

A good SIEM system will provide the security team with detailed network and asset visibility, aggregation and parsing of all log files within the environment, and the ability to organize and search the log files in an organized way. The ability to do forensics in the event of an environment compromise is also required.

An exceptional system will provide all of the above-listed functions as well as threat Intelligence from a reputable threat intelligence community. The ability to correlate log files against threat intelligence to identify real-time threats within the environment is required.

There are many SIEM vendors on the market today, and each one has its own unique features and functions. No SIEM is a one-size-fits-all type of system. Some provide very granular functions but require a very high level of technical skills to deploy, setup, tune and maintain. Others may be much easier to set up, maintain and provide lots of features but may not be as granular.

In any case, great care should be taken when performing due diligence as the price point may vary - most SIEM systems are pretty expensive depending on a number of variables. SIEM systems are required for almost every major compliance requirement in the United States and many other countries. A SIEM could be the most powerful security tool in your arsenal and should make security analysis and remediation easier and faster, not difficult and more cumbersome.

9. Technical Training

Every website in the security industry has several articles about the shortage of good technical talent for the security industry.

Organizations now recognize that investment in security is a necessity. Yet with a current estimated 350,000 open cybersecurity positions in the US, and a predicted global shortfall of 3.5 million cybersecurity jobs by 2021 — according to Cybersecurity Ventures — the industry clearly has a massive problem regarding supply and demand.

As the old saying goes “it is better to hire attitude and train than to hire training and suffer the attitude”. If you want your operation to run optimally, then you have to train your people to make it do so. It is a smart move all the way around.

10. End User Security Awareness Training

Last but definitely not least. If you ask any security professional, IT person and most managers what the weakest link in any environment is - their answer will be a resounding “The End Users”.

So how do you fix that? 90% of all end users want to do the right thing but they just don’t know how. Most people do not come with the built-in skepticism to doubt everything and look for proof. Therefore you have hundreds of thousands of breaches each year, simply because an unknowing end user clicked on a link that downloaded a virus, malware or botnet. Train your end users and it will make your life easier.

While this is not a definitive or granular list of steps to take to deploy a very safe environment, it will definitely put you on the road to creating a secure environment that will enable the organization’s IT and security staff to be proactive and shorten remediation times on almost any issue that they encounter.

IT is hard. Secure IT is even harder.