Security Disciplines | by Rich Whyrick, MCP, ITIL, Security+

Ah, security. Network security. Information Security. Endpoint security. Configuration security. Cloud security. Physical security. All different but depending on the size of your institution or your role within it, you may have a hand in each of these security areas. And while it may not seem important to the casual observer, it is important that anyone managing any aspect of these knows the differences between them.

When I decided after six years in IT that security was where I wanted to focus, I dove in head-first, never really considering that there are subtle but real differences in each of these terms. People used to ask what I did for work, and I'd go off on a long rant about using firewalls, antivirus, intrusion detection, data-loss prevention and other tools in an effort to protect the network from all kinds of nastiness. Eventually, I was able to satisfy most of those asking with the elevator pitch, "I protect data." And when you really cut to the chase, isn't that the point of all the tools and measures in place? Sure, with physical security you're also protecting physical assets, trying to ensure someone doesn't make off with your PCs, printers, and whatever other valuable pieces of equipment you may have, but each of those devices likely has some information on their hard drives that you wouldn't want walking out of the protections of your building.

I want to point out that the information below is by no means an exhaustive list of every possible protection; that would take volumes, and this blog will be plenty long enough already. With that said, let's dive into each and see what differences there are.

Network Security

This usually encompasses the heavy hitters of the security world: firewall, intrusion detection/prevention system (IDS/IPS), Network Access Control (NAC), and so on. These are the devices that are used to try to keep the bad guys out of your network; or, if they've already managed to infiltrate your network, to notify you that there is suspicious traffic flowing out of your network, unknown devices on your network, or that sensitive data is being exfiltrated. Another example would be antispam/antivirus for email, trying to prevent scammers from phishing your users and gaining access to their accounts, or getting them to go buy gift cards at Best Buy and sending them the numbers off the back. This can also include other systems, like antivirus, user and entity behavioral analytics (UEBA), and web content filtering. Last, but certainly not least, are your authentication services. Almost everyone uses Microsoft Active Directory Domain Services, so you're already enforcing some network security by requiring that people login to the network to gain access to resources. If you're logging the proper audit controls, then you have a trail of who logged in when and what they accessed, which is very important. Equally important are, "how did they get there?" and "what did they do with it after they accessed it?"

Information Security

One thing you'll note is there tends to be some overlap between the different security disciplines. Consider your firewall and IDS/IPS; they are traditionally viewed as the gatekeepers of the network, blocking known bad traffic based on access-control lists and/or signature files. However, with the advent of next-generation firewalls (NGFW), traffic can now be decrypted and inspected before it enters or leaves your network, giving you an opportunity to inspect traffic that historically was something of a blind spot. They can provide web content filtering, preventing your users from surfing to known bad sites. NGFW's can filter based on application, allowing you to permit your marketing department to post to Facebook while nobody else can. Data-Loss Prevention (DLP) systems are another information security tool, for reviewing data at rest (on a file share or in a database), data in motion (data traversing in and out of, or within your network) and data in use (data that's being used on an endpoint) to ensure data you have deemed sensitive is not being used in ways it was not intended. Some antivirus solutions also include a form of DLP, as do some firewalls.

Endpoint Security

This one is fairly self-explanatory; as opposed to network security, which is almost always a hardware (or virtual) device sitting somewhere in a rack in the data center, endpoint security is usually a software agent installed on PCs, laptops and servers. Whether it's antivirus, UEBA, or a DLP agent endpoint security is your last line of defense if something manages to evade all the other tools mentioned so far. Suppose a hacker has managed to gain access to your network - they will start off their reconnaissance slowly at first, only starting to get a little bolder after an extended amount of dwell time. UEBA on all of your endpoints will notice very subtle changes in behavior and could alert you to their presence much more quickly. Some may say it's redundant to have antivirus on your firewall and on your PCs. But what about portable drives that invariably get plugged in? No firewall is going to catch that. Or maybe you want to prevent those devices from being plugged in. Several antivirus solutions also provide device control to prevent those drives from being mounted. There are so many more reasons to have *defense in depth* (AKA *layered security*) than not. And yes, there is a cost associated with having layered security, but is it more expensive than having a breach? Depending on the extent of the breach that's an emphatic NO!

Configuration Security

OK, what's this? This is by far the easiest and least expensive security option you have available to you, yet invariably it's what gets overlooked and leads to so many breaches. When you get a new firewall, a new printer, a new PC, what's the first thing you should do? Well, duh - plug it in and turn it on! But high up on the list of priorities should be renaming default user accounts and changing their passwords. Don't need the account after you've done some initial configuration? Disable it. Then harden that OS; disable unnecessary services, uninstall unnecessary software, disable unneeded network protocols, remove all unnecessary user accounts, and apply all necessary patches and service packs. Then scan it with a vulnerability scanner like Nessus or Qualys, both internally and externally if it's Internet-facing, address any noted vulnerabilities, then scan it again to ensure you've locked that thing down tighter than Fort Knox (while still permitting your users the necessary access).

Cloud Security

This one is rapidly becoming prevalent, and as more organizations move to cloud-based services (e.g., AWS, Google Cloud, Microsoft Azure, etc.) the more opportunities there are for bad guys to try to get access to sensitive data. In my experience, configuration is the number one problem organizations face with cloud services, largely due to the fact that they think building a server in the cloud will be no
different than it is in the data center, less the time spent racking it. Unfortunately, that's rarely the case; if you haven't taken the time to learn what security options are available, what's enabled by default and what isn't, and what the cloud provider does to secure your environment vs. what's expected of you, chances are you're not going to have a very good week. Before you dive into cloud computing, be sure you have done your diligence and know exactly what you have and what you don't. This also includes Microsoft 365 (and other similar cloud offerings). It includes antispam, antivirus, encryption and some advanced threat protection options, but you should read what others have to say about those offerings before putting all your eggs into that one basket.

Physical Security

We've already discussed this a little bit, but this is everything from ensuring you have a lock on your front door to ensuring you're monitoring for temperature, humidity and water in your data center (think "Availability" in the CIA triad). Unless you've made the move to cloud or your data center is hosted by a third-party, chances are good that a lot of sensitive data resides on your servers and losing any or all of it for an hour, a day, or forever is going to make for a bit of hand-wringing. So, ensure you're monitoring the environment; have all of your systems supported by UPS and

generator; make sure your backups are encrypted and stored a reasonable distance away from your datacenter; keep a log of anyone who enters your data center; ensure there are cameras on all ingress/egress points; and lock up any unused tokens or hard drives.

So, you're employing all these different security measures. How can you possibly keep track of all this information? This is where a security information and event monitoring (SIEM) is going to be your friend. It can consume the logs from all these disparate security sources, aggregate them and correlate them to see certain patterns, as well as provide a "*point-in-time*" snapshot of an event or possible incident. Yes, you could certainly do all of this yourself, but it can take hours to piece all the information together for a single incident, where a SIEM can do it in seconds.

Consider this quote: "Poker isn't just about calibrating the strength of your beliefs. It's also about becoming comfortable with the fact that there's no such thing as a sure thing—ever. You will never have all the information you want, and you will have to act all the same. Leave your certainty at the door." Maria Konnikova, Ph.D. in Psychology and Champion Poker Player

This quote is what prompted me to write this blog. I don't even remember what the article I found it in was about, but this struck me as the way security professionals ought to approach every day, and I wish I'd found this twenty years ago. No matter how hard any of us tries there will always be an opportunity for bad guys to find a crack in the wall and get inside. All any of us can do is the best that we can by applying our knowledge of the different security disciplines, keeping abreast of the latest trends and attack vectors, ensuring that we are following hardening guidelines, consistently patching and scanning, and monitoring as much as you possibly can.

Bottom line: Don't sweat the small stuff until it's all that's left. Good luck, and happy hunting.