9/18-22

Zero-days, Patches and new Regulations

As we enter another week down, let’s look at a few things that we have learned this week in the world of Cyber-Security. As always, this is not meant to encompass everything that is going on but give you a brief look.

Although Zero-Day attacks and vulnerabilities are not an uncommon thing, they can become scare, as any new thing can be, as the discovery of the flaw is something that is brand new and defending against the unknown is near impossible. Trend Micro and Apple both release patches and hotfixes for multiple Zero-Day vulnerabilities this week. The unfortunate news for Trend Micro users is that these exploits were actively used in the wild. While the attack vector requires the threat actor to already have administrative control of the target system, it is imperative to move quickly when patches are released. While patching the production is extremely important, ensuring that patches are applied to the backups can become just as important. As a current workaround, Trend Micro suggests that customers limit access to the product’s administrative console to trusted networks. Apple is in a similar place however they did not release much information regarding the exploits aside from acknowledging that they may have been exploited in the wild. Please see the full list of versions to ensure that your system is protected.

Taking a step back, it may not always be a Zero-Day vulnerability being exploited. Many companies, both hardware and software will release patches and work on better solutions for known vulnerabilities. GitHub released some of these that help to prevent threat actors from injecting malicious pipelines into codes. The original implemented fix came out in August but security researcher Johan Carlsson was able to find a way around this fix. This is just one example to show that even if a security fix has been implemented, that does not mean that the system is good and you don't have to worry about it anymore.

While regulations can be a good thing to help the public have a better understanding and work to keep companies honest, the landscape for new regulations can become murky with the use of legal verbiage that can bring ambiguity to how it is implemented and enforced. With the new regulations regarding Security breaches for companies goes into effect, looking at how some of the first companies file these findings can be important to formulate how you will disclose these findings if or when they happen to you. Creating the plan before an event happens will only ensure that you stay a step ahead and help to get through the unfortunate times with as much ease as possible. The first of these filings comes from the Clorox breach. While there will be MANY more of these to come, creating the policy for if it happens to you and continuously improving on that will only ensure that you can navigate the storm.

While keeping up with the news on what is going on, knowing the who, how and when to implement changes can make the difference between a detrimental outage and a minor annoyance. Always remember that this is an ever present war against the attackers. Know your systems that you use, keep up with releases and fixes and ensure that you have an incident response plan in place ahead of time.