**#Designing Malware Protection Policy**

##What’s the first step in designing a Malware protection Policy?

When working with Malware, you need to know how we can protect against malware. What is the first step in any battle? Know your enemy. As a computer security specialist, you will be tasked with knowing your enemy's approaches to getting access to critical and well-protected information in any organization. So what resources are at your disposal?

There are two resources that I can safely say will be of utmost importance in any field concerned with cybersecurity. (NIST)[https://www.nist.gov/cybersecurity] and (MITRE)[https://attack.mitre.org/], the cybersecurity community loves acronyms.

###What is NIST?

* The NIST site contains a cybersecurity page that you can use to help develop a cybersecurity policy that stretches across multiple facets: Cryptography, Cybersecurity Measurement, and Trustworthy platforms are just a few of the fundamental subjects that the NIST covers. They are a government-operated organization that develops cybersecurity policies for both the private and public sectors.[^1]

###What is MITRE ATT&CK?

* MITRE is a collection of cyber security-based knowledge that strives to meet the stringent needs of the many different cybersecurity corporations and is at the forefront of cyber attack-based knowledge. Using their database lists attacks that cover a wide range of attacks such as Reconnaissance, Defense Evasion, Credential Access, and Exfiltration. Entities can use these techniques in a combination of ways to create different and unique attacks that can penetrate even the best security defenses.[^2]

##What are the main ways that Malware causes damage to corporations?

When it comes to viruses spreading in Corporate America, quite a few manage to get through. Still, with such an abundance of resources, the question that we as cybersecurity personnel are left with is, “Why is it so damaging?”

There’s a simple reason. It’s the development of new methods and the constant need for people to adapt to what these viruses are capable of. As we’ve covered earlier, there are a variety of different viruses. Still, their effects can be all-encompassing or achieve the singular purpose that they are designed to do. These purposes include:

* Interrupting and disabling services by breaking down the network of an organization.[^3]
* Retrieving and spoofing personal information, acting as an authorized user to access information that would otherwise be restricted.[^4]
* Controlling and executing applications on a device, thereby causing programs to give up sensitive information. It seems like it came from a computer so no one would expect it. [^5]

One way to combat this is to regularly have your information, vulnerabilities, and protections audited by outside sources. To quote Davidoff, “A risk assessment is critical for prioritizing your cybersecurity ‘game plan’.”[^6]

##The Policy should cover six fields:

* Purpose: This field is the purpose that your policy is trying to achieve. This field means that your policy should list the goal. If the goal is to limit unauthorized access to the network infrastructure by creating a policy in which everyone who accesses it needs to gain administrative approval, the policy must establish that.
* Scope: This field defines what it means to achieve the goal you are setting out to accomplish with the implementation of the policy. It describes the work you are going to do, the upkeep and updates you will perform, and the degree to which you will continue maintaining a service long after the first threat has been dealt with.
* Definitions: This section of the policy should define all the acronyms and jargon used about the policy. These words or acronyms will be job-specific and will more often than naught directly correlate to the role that this policy is supporting.
* Policy: This portion is the actual policy itself. The length of the policy can vary as there is no set standard for policy length, but it should be long enough to account for variations in the situations that the policy may encounter.
* Violation of Policy: This simply outlines what happens if the policy is violated. This portion should be concise but give a fair estimate of how much punishment should be doled out to people who violate the policy.
* Enforcement: This will be a portion of the policy that gives information on the enforcement of the policy. This enforcement will be left up to the person issuing the punishment more often than not but should give appropriate guided actions to help an entity enforce apropos repercussions.

#Works Cited

[^1]Hernandez, P. (2022, March 15). *Cybersecurity*. NIST. Retrieved April 14, 2022, from https://www.nist.gov/cybersecurity

[^2] MITRE. (2015). *Mitre ATT&CK®*. MITRE ATT&CK®. Retrieved April 14, 2022, from https://attack.mitre.org/

[^3][^4][^5]Digintrude. (2018, December). *Malwares and Its Impact on Business*. Malwares and its impact on businesses. Retrieved April 14, 2022, from https://www.digintrude.com/malwares-and-its-impact-on-business.html

[^6]Davidoff, S. (2017). CYBERSECURITY AUDITS Getting to Good. *GPSolo*, *34*(4), 56–59.