Securing Operating System

Information Protection Technology

Anonemis Research
Simenona Martinez
AnonemisResearch.com

Securing Operating System

Information Protection Technology

Overview

Information technology department testing, vetting and secured procedures for new operating system.

Ethical hacking and Penetration testing: Sending malware, viruses, DoS, and socially engineered malicious links to see how the operation system and individually tested application respond to the same method. Assessing the potential damage: how, where, and why the application and operating system reacted to the infected sources and how calculating recovery effort both, monetarily and timespan wise. System response is an essential element in testing because users rely on safe system to navigate throughout the day-to-day, long term, personal, business, domestic, foreign, remote and as well as base. General and maintenance security testing can perform more efficiently with this groundwork of initial security testing.

Password retrieval from suspicious addresses and hostile takeover as an administrator (Remote take over) on the backend. Testing all the primary administration functions in the event of compromised using ethical hacking and penetration. For example, what is an accessible risk from the remote hacking: internal, external, domestic, and foreign. It is important that this methodology of testing be extended to both foreign and domestic because Microsoft is international brand.

Vulnerability scanning. Assessing which applications require regular updating and patches. This would be essential in possible partnerships with existing security companies such as Norton or MacAfee as well setting the Microsoft framework for user assurance. Posture assessment can be better catered when testing is a precise but board scope in spectrum within cybersecurity, especially in big corporation and government settings. These layouts tend to have a vast spectrum of vulnerabilities that require an "all things considered" approach. Utilizing this capacity of depth in cybersecurity testing will be of an asset for initial product roll out and continual standard practices regarding future updates, patches, and configuration.

Ethical Hacking and Social Engineered Attacks. Vulnerability scanners examining malicious content found on web apps from the outside to identify cross-site scripting, SQL injections, command injections, insecure server configuration, etc. is essential testing because that's where user are most at-risk for downloading and accepting infected data. Again, these layouts tend to have a vast spectrum of vulnerabilities that require an "all things considered" approach. Utilizing this capacity of depth in cybersecurity testing will be of an asset for initial product roll out and continual standards for updates, patches, and configuration.

Security is the result of negative goals seeking positive outcomes and positive goals which seek to deter negative outcomes. It is important to seek negative outcomes which render the most effective results because that’s the mode of operation for many attackers. It is important to consistently keep in mind that the application of attaining negative goals is always on a distributional foundation that is a spectrum, as

sometimes the most damaging attacks require little to no sophistication. The attacker maintains the ideology of being more about accessibility than the actual scheme.

The positive goal in tactical operation in the negative outcome being that it affords you an allowance to patch, repair, and reconfigure your structure and vulnerabilities that may be present, thus, producing a positive outcome in terms of defense.

The inherent challenge within security which creates this dynamic is that the intention of attackers is always negative and therefore, agents must maintain this mindset within the scope of a present positive reality. Like so many other multifaceted areas in cybersecurity, it is about achieving an equilibrium in the space that is an ever-evolving spectrum. 100% security is extremely difficult to obtain because this is an industry of innovation to idlers.

Enforcing administrative controls based on job responsibility and skillset. Time limitation and location separation is enforced to ensure further security as well as monitoring user logs in his folder accessed regardless of restrictions, both granted and revoked.

There is certainly a segregation of access in terms of administrative roles vs. executive staff. Technical and Security teams monitoring the usage in both and the primary administration observing the overall oversight of the operation.

Restriction and regulation is contingent upon roles and necessity. All access being time restricted is essential in oversight, particularly within the areas concerning efficiency and security.

The executive, administrative and technical teams are the top tier without the organizational. However, the technical and security structure would be to maintain a more depth access which would be strategically isolated from administrative and executive, not only for privacy but to decrease the possibility of compromised within ones enterprise.

Administrative controls> Access Controls>> Guest User

- The primary access as administrator is restricted and encrypted.

Running the guest user on an external hard drive that is completely separate from the administrative back end.

The functional goals are the daily structure of operation and the functionality as well as the practicality of its baseline. Security goals are intended for both being protected and protecting the functional goals and vice versa. The functional goals are the cake, and the security is the icing. They essentially require each other to operate efficiently and are needed for an enterprise to prosper.

As with any element within an enterprise it’s about formulating a model that can operate individually as well as simultaneously. Researching to establish which department are most at risk for both internal and external attacks. Staging attacks is a tactical measure which will allow you to observe and execute a line of defense that is most useful.

Achieving C.I.A in the scope of usability comes down to understanding the role of each team member, their function and ensuring that they can achieve those goals with both efficiency and precision. The use of the NIST framework, applying comprehensive levels of classification, coding, and the encryption of such is

non-negotiable. Building a system where access is both restricted and readily available upon contingency of organizational positioning. For example, a company manual can only be edited by primary administrative staff but the document is viewable by employees that can be limited during training session and for a specific allotment of time. This example tackles and ensures ***confidentiality, integrity,*** and ***availability.***

In the quest of supporting cases, the operational systems, and structures, the effectiveness is dependent upon the understanding of how the contrasting elements work and how to apply them accordingly based on need. The importance of knowing what works based upon research but most importantly, practical and functional real-world experience when applied.

Establishing which department requires access to information with both the why and how in mind. In the case of universal policy within your enterprise, like for example, a code of ethics, all employees are required to adhere by the same standards. However, departments such as accounting requires system controls that should only be accessible with the ability to edit within the confines of the financial department, whereas, the executive levels have access to the same information but employees outside of that departmental tier would not have access to that information. Restricting what folders and contents are available depending upon department and respective roles.

If you share confidential information with am untrusted source, the technical department should be notified immediately, and damages should be assessed accordingly.

Depending upon the industry, research would incorporate the most impactful security breaches and the monetary loss to assemble best practices and insurance. Researching high risk areas and behaviors which led up to these said breaches.

I would the NIST framework to provide guidance on how to prevent, detect, and respond to cyberattacks. In a 2016 survey, 70% of respondents recognized NIST CSF as a popular security best practice. D*etect, protect, and respond* has been proven to be most effective.

Precision and effectiveness is key when classifying categories. As different industry requires more invasive encryption but NIST framework incorporates the best straightforward practice and policy by far. Policy and Procedure can only be as effective as its application in real, real-time business practice. Establishing who and what access to what files, controls, content and when but most importantly, how and where that information is being used and applied to establish behaviors both normal and abnormal. This is key in the prevention of both external and internal breaches.

- Protected
- Confidential
    - Policy
    - Procedure
    - Legal
- Secret
    - Policy
    - Procedure
    - Legal
- Top Secret

Providing adequate training and verifying that all practices meet standards and regulation. Contracting and/or employing a compliance and enforcement officer. Policy requires constant

updating as well as procedural measures. Hiring the most qualified applicants and engaging in regular drills to mandate expectation and standard of execution. The enforcing of best practice and standards for both long term and short-term protection. Researching other models and framework employed by other operations. Establishing the who, what, where and how all possible threats can affect a security structure.

Maintaining flow charts for each category of security structure, ensuring the equilibrium of your security foundational needs, as it changes and upgrades within industry. Putting to use both practical and learned knowledge in the field. Researching further into the mechanics and engineering of who and what the industry's leading cybercrimes/criminals are using to carry their attacks. This research is key to the breaking down of the mechanics criminal enterprises and the divide and conquering in the realm of any discourse of business, most effectively as it relates to cybersecurity. Cyber-attacks are unavoidable but cyber-mapping and restricting areas where there are higher incident rates can be instrumental in protection, research, and detection. These are essentials elements required to sufficiently, *detect, protect, and respond.*

What are the classification categories? Examples as follows:

Helpsystems has a comprehensive data structure which is as follows: **Policy, Internal >> PII Present, Confidential > Legal Hold and finally Confidential >Project Alpha and metadata.** This system is both automated and manually driven.

How does the system allow you to identify and codify critically sensitive or important data sets? *Helpsystems* classification system is organizational chart based. Safeguarding policy and internal information data at the foundation and upmost priority of it's system. Further confidential information and legality data guarded in mid-range with critical safeguarding, followed by a co-operated system with the option of further user customization.

How would you apply the system? When applying this system setup, the layers are an allowance for critical data which allows a barrier and protection to be allotting before an attacker can reach crucial data which would compromise a system further. Access to policy can be used as a first line of defense as a primary offensive line.

How would you enforce the system or train the team to implement it? Training all employees to be aware and alert of what a cybersecurity breach looks like in the order of it's undependable compromization. Enforcing a system which incorporates an up-to-date security policy and procedures for the security task force. Something as critical as the proper team to escalate a possible breach could be the difference of millions of dollars. It is essential that labeling, classifying of data, both correctly and organizationally positioned and the appropriate reactive response is key in the effectiveness in risk management.

Does the system also include policy elements or guidelines for use? *Helpsystems* understands that policy and guidelines are the foundation to any effective planning in a cybersecurity construct.

Ensuring constant and effective training of employees, entry-level or executive, is essential and critical. Current firewalls and anti-virus systems being up-to-date is the baseline. Implementing policy; pre and post operational structure response to incidents is crucial in prevention and learning post incident. Including fire drill type structure training, engaging in ethical hacking to gage team response, effectiveness, skill assessments regarding agents, response time, accumulation of mock damages occurred pre/post and ultimately preparedness. Insurance.

Using defensive software that operates by using algorithms which tracks each employee and the entire organization operational systems usage, workflow, and behavior analysis. This will aide in the early detection of abnormal behaviors, files, commands, downloads, ports, packets, email links, social engineered infringement, and duplication of data in rapid flow which will signal system alarms, thus, early detection. This algorithm would also track the path of the infection and auto lock and effectively power off devices remotely. Alerting the necessary chain of command of possible breach with auto generated reports when detection is verified.

Training is key and assures that your organization is confident and comfortable in situations regarding these inevitable attacks. The most effective way to achieve this uniformity is to instill confidence in the training, applying obtain knowledge and skillset, implementing effectively precise planning, engaging in constant but random ethical hacking for assessing preparedness, and discussing/analyzing post evidence in proper organizational order. Learning and researching from past security breaches can be an effective in the operational response guide, while always reviewing data from a current trend standpoint regarding cybersecurity. Big Picture.

After reviewing the post incident reports throughout the chain of command, implement drills and depending upon budget or industry establishing a cyber breach research teams is essential. Reviewing and understanding the data at hand, the who, when, where, why and how. Comprehending the fundamental of the source and ultimately the trail of the attacks, software can aide in this process. Establishing the response of each employee and their effectiveness in their roles during the incident and as well the chain of commands response as well as repair. Insurance is essential if he budget permits.

Anonemis Research
Simenona Martinez
AnonemisResearch.com