Preventing Cyber Crisis

‘Must haves’ for all organizations to secure against cyber crisis

A secure cyber space is crucial for development of any country in economic, political and social spheres. Increased adoption of digital technologies has redefined the cyber security landscape. Cyber crisis is no more a luxury that any progressive state can afford. A set of baseline requirements are suggested that all organizations must have to prevent cyber crisis.

Dependence on Information Technology to make our day-to-day tasks easier has increased with computers playing key roles in all spheres of life such as governance, transportation, health care, and banking. Cyber security is vital for protecting all of these functions as any crisis in the cyberspace will endanger one’s life and property, in letter as well as spirit. The wide spectrum of hackers, criminals, terrorists, and state actors are constantly engaged in cyber space with malevolent activities ranging from stealing money and classified information to damaging important data and denying the availability of vital services. Since the cyber warfare is a never ending one, all stakeholders involved in providing IT enabled services should be prepared to manage any crisis that emerge in their cyber domain.

Evolution of a Cyber Crisis

As in the real world, the cyber space also is filled with innumerable events happening on a regular basis. An event refers to any observable occurrence in a system or network. Browsing a webpage, logging into a system, sending a mail and sharing a file are all examples of events. The number of events taking place in a network is usually so high so that they are often counted in terms of Lac of Events per Second (EPS). While most of the events are harmless and result in a positive outcome, there are certain adverse events that can have negative consequences and even lead to disruption of service. Adverse events that pose a threat to the security of the computer or the network are called security incidents. In other words, security incidents are adverse events that breach the information security triad of Confidentiality, Integrity and Availability (CIA). Happenings like unauthorized access to a system and misuse of resources to virus attacks and violation of security policy of the organization are common examples of cyber security incident. These incidents may threaten lives, economy, national security and erode public confidence if they are not properly attended in a timely manner, resulting in what is termed as cyber crisis.

Prevention better than cure

The preliminary step in managing any kind of crisis is prevention of its occurrence, and this is more true in case of cyber crisis. Organizations of all sizes should build cyber security capabilities to safeguard its assets from cyber-attacks. Since cyber security is a continuously evolving process (and not an off-the-shelf product), organizations should inculcate a culture of cyber security

C.J. Antony
Dy. Director General &
HoG (Network Security)
antony@nic.in

in all spheres of their functioning through appropriate policies, processes and protocols. To begin with, the following baseline requirements are recommended as 'must haves' for all organizations to secure against cyber crises.

Inventory of Hardware and Software Assets

Maintaining an accurate and up-to-date inventory of hardware and software assets related to the organization is the first and foremost step for ensuring protection against cyber-attacks. A latest inventory is very essential to control the access for these solutions, besides detecting the unauthorized ones and hardening the vulnerable ones. Keeping such a record of assets deserves importance because, as the saying goes, we cannot protect what we do not know. An automated asset management system may be deployed for this purpose as newer solutions are being added and obsolete and faulty ones are getting removed on a daily basis, especially in large organizations. Obtaining a one-time-approval should be made mandatory before connecting new systems in the corporate network. A stringent Bring Your Own Device (BYOD) policy which also includes employee exit strategy may be put in place.

Secured Configuration of Hardware and Software

The configurations with which the hardware and software solutions are released by the OEMs are meant for easy and quick installation in a network. The default settings ranging from the user accounts and passwords till open ports and protocols are made to enable plug-and-play deployment of the solution with less security. It is often found that these configurations are seldom modified for lack of time, expertise and even fear of malfunctioning, leaving wider attack surfaces for the attackers. Therefore, each hardware and software component should be put in use only after proper hardening and secured configuration following the principle of zero-trust. Subsequent modifications in the settings should be done only after following a proper change management process. All the solutions should be periodically subjected to security audit to ascertain any deviation from the established security norms.

Vulnerability Assessment and Patch Management

Vulnerabilities in operating systems, development frameworks, browsers, etc. are entry points for cyber-criminals to leash out attacks. An un-patched system gives attackers an easy avenue to penetrate the network and compromise the cyber infrastructure of the organization. With novel vulnerabilities and exposures getting reported every day, organizations should make conscious efforts for vulnerability and patch management based on cyber security alerts being raised by the concerned agencies. A pro-active mechanism to identify, mitigate and patch the vulnerabilities should be established and linked with the inventory management system mentioned earlier. Client users should be encouraged to regularly avail the updates from OEMs by enabling the auto-update feature of the system and application software.

Controlled Use of Admin Privileges

Misused Admin privileges are a common cause of security breach in any network. Admin privileges must be restricted in the system and application software as well as network and security appliances. Practice and propagate the principle of least privilege, as running computer in administrator role leaves it vulnerable to security risks and exploits. Access to any system should be provided only on a Need to Know basis. Additional user accounts created on need basis should be deleted or deactivated once the requirement is over. Any temporary escalation of user privileges should be undone immediately after the proposed task is accomplished. Activities that require admin privileges should be performed by the designated system administrator only and the admin should use due diligence while using the system and privileges. Actions performed by privileged users should be constantly logged and regularly monitored to detect any adverse events.

Endpoint Protection

Endpoint of the information technology network consisting of desktops, laptops and hand-held devices are often turn-out to be the start point of a cyber crisis. Endpoints need special attention and protection to avoid any incident that may turn out to be a crisis as they are the interface where human beings usually interact. Malware is the most common attack vector that targets the endpoints. They are malicious software intentionally designed to disrupt, damage and gain unauthorized access to computer systems and networks. Security solutions that prevent the malware from entering, executing, accessing sensitive data, and infiltrating the data, should be deployed to safeguard the endpoints. As newer mutants of malware are getting generated rapidly, traditional antivirus solutions are seldom effective to counter this nuisance. Next generation solutions based on Artificial Intelligence, Machine Learning and Behavior Analysis are need to detect and mitigate fresh variants of malware.

User Awareness and Capacity Building

Many organizations tend to neglect the most important layer of defense against cyber-attacks - the end users. Human Beings being the weakest link in Cyber Security paradigm, continuous efforts need to be made to keep them aware and alert of the latest Tactics, Techniques and Procedures (TTPs) of cyber-criminals. New vulnerabilities are emerging every day and a proper understanding of the prevention, detection and mitigation techniques is very essential to remain protected. Security awareness empowers people connected with business to perform their roles by protecting the organization from potential security threats. Any investment in cyber capacity building will enhance the success rate of other policy initiatives in long-run. Thus, awareness creation is a marathon process, not a sprint race that can be accomplished in a short period of time.

Conclusion

Cyber space is an intrinsic part in the development of any country. Attacks on critical information infrastructure are continuously being leashed-out by state and non-state actors, posing threat to national security. The identity and capability of the attackers are seldom known and this often gives them an edge over the victims. With cyber-crime growing into a multi-billion-dollar industry, cyber-criminals are increasingly getting empowered and creative day-by-day. Organizations must have a strong and agile security posture to deal with these headwinds and ensure reliable and responsible service to their users.

For further information, please contact:

C.J. Antony
Dy. Director General & HoG
Network Security Group
National Informatics Centre, A-Block, CGO Complex
Lodhi Road, New Delhi - 110003

Email: antony@nic.in, Phone: 011-24305166