Under attack: How to beat the cybercriminals

SACHIN BHARDWAJ
INSIGHT

RECENT MONTHS have seen several outrageous cyber-attacks dramatically compromise the functions and data of several businesses, governments and organisations across the globe. While hackers have been a threat for a considerable amount of time, the extent and scope of their attacks were often limited in the past — high profile cyber-attacks tended to be the ones that compromised or breached heavily defended and access restricted networks. The last two years in particular have, by contrast, witnessed attacks that are remarkable for the sheer number of networks they have compromised and the widespread geographies they have affected. The skills and services of Managed IT Security Service providers are being tested by the upswing in instances of ransomware, data theft and several other manifestations of cyber-crime. These threats can no longer be considered fringe or unlikely concerns for the average enterprise.

As IoT applications and mobile connectivity become the norm rather than exception and their advantages too favourable to ignore, the ability of hackers to compromise networks through distributed denial of services (DDoS) is becoming an ever-increasing concern for Managed Security Services. The ability of hackers to establish a 'botnet' of compromised devices to aggressively and efficiently widen the scope of their attack rapidly also presents a dynamic moving target for any remedial action, further raising concerns. While technology based solutions still form the core of the response, it is also imperative to widen the scope and purview of preventative and anticipatory strategies.

> Networks and their administrators must find a compromise between ease of access and containment of possible threats — proactively and on an ongoing basis

The Middle East has traditionally relied on geo-blocking and isolating networks to dissuade and block hackers. However, with the rise of mobile connectivity and IoT applications, such strategies are increasingly inadequate and open to being circumvented by localised device botnets. The malafide recruitment of distributed computing power in order to launch an attack is now easy to access through very few compromised devices and the wide profusion of connected devices leaves no network inherently safe — however isolated it is by traditionally accepted standards.

Managed IT Security Service providers in Dubai are no longer taking for granted that their network security filters constitute an adequate defence from hackers. The cost of launching an attack is so low, the technology so easily accessible and possible business and functional impact so severe, that far more comprehensive strategies and solutions are being put into place in response.

Concerns and solutions

A rethink regarding the layers and type of authentication involved in granting access is emerging as one of the key strategic solutions to emerging threats. Rapidly diagnosing and isolating compromised devices and network segments in real time is also a non-negotiable ability for networks now. Malware can gestate in a host network for months, familiarising itself with the ins and outs of administrative practices, mapping entire segments in the network and key data locations, before an attack is launched. It is, therefore critical that the scope, frequency and type of detection oriented practices are also adequate in the identification and isolation of threats. Once a network has been breached by malware, it is often standard everyday functions and operations that help it to spread and access other devices — it is critical that processes are rejigged to address both lean functionality and secure operations. Both legacy systems as well as the latest plethora of connected devices bring their own vulnerabilities to the table and a comprehensive response strategy requires that both types of vulnerabilities are addressed.

Essentially, networks and their administrators must find a compromise between ease of access and containment of possible threats — proactively and on an ongoing basis. While early detection and comprehensive but unobtrusive layers of network security form the core of most Managed IT Security Service providers' strategies, the involvement of the client enterprise is essential. Training of employees in best practices that optimise security, establishment of proactive standard procedures and having a comprehensive plan in place — in the event of an attack — are all initiatives that an organisation needs to take, in order to reduce the risk of vulnerability to hackers.

Conclusion

As, both, the modern network and the emerging IT security threats continue to evolve, it is essential that organisations and their Managed IT Security providers come together to address vulnerabilities. While the bulk of the strategies and technology employed to address to security concerns is likely to come from the services provider, the involvement of the organisation and its user base is a critical component. As technologies evolve and a wider array of devices are online and networked, it is important to remember that the greatest vulnerabilities are still linked to the practices and procedures involved in the everyday use of these technologies.

The writer is director marketing and business development, eHosting DataFort. Views expressed by him are his own and do not reflect the newspaper's policy.