CHINK IN THE ARMOUR

IT security professionals have to find frailties in external security systems before cybercriminals seek to exploit them. Cybercriminals can inflict devastating damage, and the speed in which they can accomplish their task is only getting faster. With that in mind, it is paramount that security professionals are aware of common weak points.

F “Cybercriminals will exploit any weak point of a network to gain entry – rather than targeting a specific area, they will attack the whole network hoping to find their way in,” says Latik Gupta, Head, Jumbo Enterprise. “These are known as blended attacks and use an array of malware to break in and access data.”

This blanket approach to attack is an equally accurate representation of the reality of security defence; if attackers have the determination, they can and will find a way in. Although IT leaders are waking up to the reality that their defences are not impenetrable, they still need to remain vigilant in order to identify their own weak points that attackers will seek to exploit. Gartner’s prediction that Middle East and North Africa IT spending will hit $1 billion in 2014 is certainly an indication that region-wide, the need for a proactive rather than reactive security approach is being acknowledged.

David Flower, Managing Director, Bit9 + Carbon Black, EMEA, believes that the advancement of attacks requires a security rethink. “Given how unpredictable and sophisticated these attacks are, antivirus, or signature-based threat prevention solutions are no longer sufficient,” he says. “It is important therefore to invest in more advanced security approaches that do not depend solely on simple signatures and known blacklists of IP addresses or files. The proper integration of security tools is also as important to make it easier to detect attacks across multiple layers.”

Stephan Berner, Managing Director, Help AG, is mindful of the importance of a fresh security base that can position organisations to protect their assets. “The thing is that the existing systems and technologies already implemented bring big risks because they need to be continuously maintained, updated and upgraded,” he says. “Organisations have to build an information security baseline which is the foundation to increase their security posture gradually and then they can stack advanced initiatives without falling short in results.”

IT’s transition to the third platform heralds a new age in the way that technology will drive business value, as well as define citizens’ day-to-day lives. However, the increase in the number of endpoints also increases the breadth of attack possibilities. Although a large number of security concerns have been raised around the pitfalls of public cloud, the unavoidable tide of mobility, and Bring Your Own Device culture is perhaps the greatest threat to enterprise security that the third platform brings. The lure of greater productivity, and being able to allow employees to work anytime, anywhere is an impending reality that even the hardest-nosed CIO cannot ignore. But with this promise comes the need for sharpened vigilance and fresh security strategies.

> ” Since the weakest security link can often be humans, companies must incorporate privacy and security training and instill the culture of data privacy within all employee groups. It is important to ask your employees to change their behaviour in regards to how they use their IT systems.”
>
> Anas Ali Al Naqbi, Senior Security Consultant, eHosting DataFort

“The ongoing trend of BYOD means that any device that has malware on it can then be introduced in to the enterprise network once connected,” says Gupta. “This malware can find its way onto a device through unsecured Wi-Fi connections, and can remain on the device for extended periods of time without interrupting usability. Once connected to the enterprise network, the malware can then be passed on and gain access to data.”

If ill-prepared, organisations risk allowing hackers to target mobile devices by circumventing traditional security layers. However, establishing and enforcing IT policies, particularly in terms of managing employee-owned devices that are connected to the network, will mean taking a big step towards a more secure IT environment.

Inextricably linked with the risks that mobility brings is the slippery issue of employee naivety, which always has the potential to be the poisonous sting that compromises an organisation's integrity. Whether downloading malicious attachments, clicking unsecure pop-up windows or leaving mission-critical passwords written on scraps of paper, individuals who contribute so much to a business can easily create a string of problems for IT arms via their corrosive security habits.

Anas Ali Al Naqbi, Senior Security Consultant, eHosting DataFort, believes that employee education is paramount in plugging what is perhaps the most widespread of security threats. "Since the weakest security link can often be humans, companies must incorporate privacy and security training and instill the culture of data privacy within all employee groups," he says. "It is important to ask your employees to change their behaviour in regards to how they use their IT systems. They may have to stop downloading new software from the Internet, and start using stronger passwords on all of their devices, especially on their smartphones."

Flower thinks that formal designations will cement this mentality among staff. "Your employees must be well informed of the potential threats to customer data as well as the legal requirements for securing them," he says. "One of the best measures is to designate an employee as an information security coordinator to oversee the company's security efforts. Another is having a clear data security policy to guide employees on the proper use of data to help create a more secure environment."

An inconvenient truth perhaps, but the reality of flawed, decade-old architectures is a key factor in rendering businesses of all sizes susceptible to security breaches. Accepting this predicament is perhaps the most prudent thing an organisation can do to combat external threats, rather than burying its head in the sand and wishing unavoidable issues away.

> "Organisations need real-time visibility into what is happening in the enterprise IT environment, with intelligent IT analytics automatically generated to reveal risk factors and exposure, indicators of compromise and data exfiltration activities."

Maged Eid, Regional Director, Nexthink

> "My advice to customers is that attackers will always go after the lowest hanging fruit. By hardening their IT infrastructure, organisations can make themselves a far less attractive target."

Stephan Berner, Managing Director, Help AG

"Traditional security simply cannot protect against the complex malware types we are seeing today," says Berner. "Take firewalls for example, which are an essential part of network security. They are very limited in their features and lack the ability to close unnecessary ports, dynamically route packets and protect against denial-of-service attacks. They also lack the ability to analyse packets for malware and identify if an attack is taking place on the network. Without these measures in place, an organisation is a prime target. My advice to customers is that attackers will always go after the lowest hanging fruit. By hardening their IT infrastructure, organisations can make themselves a far less attractive target."

Although the underlying issue of incomplete infrastructures could take years to resolve, Maged Eid, Regional Director, Nexthink, believes that a proactive approach involving Big Data analytics is the most efficient way to combat existing weaknesses. "In today's world of custom attacks, traditional security solutions are ineffective because they do not sense unusual activities and usages that should be detected," he says. "It is important to focus on the detection of current threats and damage mitigation rather than relying solely on defences that are supposed to prevent them from occurring in the first place. Organisations need real-time visibility into what is happening in the enterprise IT environment, with intelligent IT analytics automatically generated to reveal risk factors and exposure, indicators of compromise and data exfiltration activities." ■