AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

Primo Piano - *The means to manage cyberspace and the duty of security*

Roma - 26 nov 2021 (Prima Pagina News) **Over and above the ethical concepts regarding the near future, it is also good to focus on the present. Governments are required to protect their national resources and infrastructure against foreign and domestic threats, to safeguard the stability and centrality of human beings and political systems and to ensure modern services for civilians. Suffice it to recall the chaos that arose some time ago in the Lazio region for the well-known health issues.**

Governments must play a key role in developing and leading the local ecosystems, but this national effort must involve many other stakeholders: local businesses, entrepreneurs, multinational companies, local and foreign investors, State agencies, Ministries and academics, people in education, professional institutions and the public at large. Furthermore, cybersecurity is a national opportunity for developing the local economy and for positioning any country in the international arena as a safe place to establish and develop economic relations between States and companies. It is also important as a regional cyber hub. Cyber strategy therefore consists in prioritising operational cyber activities with a view to optimising and monitoring the overdevelopment of cyber intelligence that could one day take such turns as to be ungovernable. This is the reason why investment in technology, local capacity building and resource allocation and concentration are required. This means providing strategic advisory services to government agencies that are seeking to advance cyber security at a strategic and operational level. It is therefore necessary to work with governments to develop their strategic and operational capabilities in cybersecurity, either at the national or sectoral level, as well as providing comprehensive cyber projects that combine cyber defence and the development of a local cyber ecosystem, based on the models tried and tested by various countries around the world, such as the People's Republic of China, Israel, the United States of America, etc. There is a need to specialise in setting up Cyber Units and Cyber Centres (SOC & Fusion Centres) and in developing Cyber Eco-Systems and Cyber Strategies. This means providing various cyber solutions, services and know-how to companies in various sectors, such as financial, industrial, energy, health, technology and many other sectors. Stable OT (operational technology) security services and strategic advice to companies in the fields of energy, manufacturing, security, medicine, transport, critical infrastructure and many others create the prerequisites for defending cyberspace. As well as helping OT-based organisations integrate cybersecurity into their processes and products. Design, develop and deliver advanced technologies and solutions to protect critical assets in OT environments, such as ICS, SCADA, IIoT, PLC, etc. In this regard there is a basic need for creating professional IT schools around the world that teach the meaning of cyberspace, and not just how to use Word and other simple Office programs. The expansion and creation of universities and institutes of cyber knowledge is a starting point from which

partnerships are launched with organisations seeking to create their own cyber schools or with academic or educational organisations offering cyber training to their students. Providing comprehensive solutions for IT schools, enables the training of IT professionals and new recruits in all IT roles, so that hackers do not remain the sole repository of digital truth. Advanced training is a solid starting point for organisations seeking to train their IT professionals. Professionals who can manage and master schemes such as Cyber Defender, Cyber Warrior, Cyber Manager, SOC Analyst, Digital Forensics, Basic Training and many others, including through the use of simulation. Leading the creation and development of the high-level cybersecurity ecosystem is a duty of States towards the citizens who elect their leaders. The same holds true for seeking and employing highly experienced experts in the various security subject matters, including strategic cyber defence, cyber warfare, cyber intelligence, cyber research and development and cyber strategy, as well as defining training policies for these branches of operation. Having examined the prerequisites for protecting cyberspace, it is worth addressing the structure of some of the risks faced by institutional network systems.One of the most typical operations made by hackers relates to the use of client/server technology to combine several computers as a platform to launch DDoS (Distributed Denial of Service) attacks against one or more targets, thus exponentially increasing damage. A malicious user normally uses a stolen account to install the DDoS master programme on a computer. The master programme will communicate with a large number of agents at any given time and the agent programmes have been installed on many computers in the network. The agent launches an attack when it receives an instruction. Using client/server technology, the master control programme can activate hundreds of agent programmes in a matter of seconds. A DDoS uses a group of controlled machines to launch an attack on a computer, be it server or client. It is so fast and hard to prevent that is therefore more destructive. If we consider that in the past network administrators could adopt the method of filtering IP addresses against DDoS, it becomes more difficult to prevent such actions today. How can measures be taken to respond effectively? If the user is under attack, defence will be very limited. If there is a catastrophic attack with a large amount of traffic pouring onto the unprepared user, it will very likely that the network will be paralysed before the user can recover. Users, however, can still take the opportunity to seek defence. Hackers usually launch attacks through many fake IP addresses. At that juncture, if users can distinguish which IPs are real and which are fake - and hence understand from which network segments these IPs come - they can ask the network administrator to change them. Firstly, the PCs should be turned off to try to eliminate the attack. If it is found that these IP addresses are coming from outside rather than from the company's internal IP, a temporary investigation method can be used to filter these IP addresses on the server or router. The solution would be to discover the route through which the attackers pass and block them. If hackers launch attacks from certain ports, users can block these ports to prevent intrusion. After the exit port is closed, all computers cannot access the Internet.A more complex method consists in filtering the Internet Control Message Protocol (ICMP), a service protocol for packet networks transmitting information regarding malfunctioning, monitoring and control information or messages between the various components of a computer network. Although it cannot completely eliminate the intrusion during the attack, filtering the ICMP

can effectively prevent the escalation of the aggression and can also reduce the level of constant damage to a certain extent. The DDoS attack is the most common attack method used by hackers. Some conventional methods of dealing with it are listed below. 1. Filter all RFC1918 IP addresses. The RFC1918 IP address is the address of the internal network, such as 10.0.0.0, 192.168.0.0, 172.16.0.0, etc. These are not fixed IP addresses of a particular network segment, but confidential local IP addresses within the Internet, which should be filtered out. This method serves to filter out a large number of fake internal IPs during an attack, and can also mitigate DDoS attacks. 2. Use many PCs to resist hacker attacks. This is an ideal response phase, if the user has sufficient ability and resources to enable a defence against hackers who attack and continue to access and take over resources. Before the user is fatally attacked, the hacker has little means to control many PCs. This method requires considerable investment and most of the equipment is usually idle, which does not correspond to the actual functioning of the current network of small and medium-sized enterprises. 3. Make full use of network equipment to protect resources. The so-called network equipment refers to load balancing hardware and software such as routers and firewalls, which can effectively protect the network. When the network is attacked, the router is the first to fail, but the other devices have not yet collapsed. The failed router will return to normalcy after being restarted and will restart quickly without any loss. If other servers collapse, their data will be lost and restarting them is a lengthy process. In particular, a company uses load balancing equipment so that when a router is attacked and crashes, the other will work immediately. This minimizes DDoS attacks. 4. Configure the firewall. The firewall itself can resist DDoS and other attacks. When an attack is discovered, it may be directed to certain sacrificial hosts, which are able to protect the actual host from the attack. The sacrificial hosts may obviously choose to redirect to unimportant hosts or to those having systems with fewer vulnerabilities than some operating systems and with excellent protection against attacks. 5. Filter unnecessary services and ports. Many tools can be used to filter out unnecessary services and ports, i.e. filter out fake IPs on the router. For example, Cisco's CEF (Cisco Express Forwarding) can compare and filter out Source IP and Routing Table packets. Opening only service ports has become a common practice for many servers. For example, WWW servers open only 80 ports and close all the others or use a blocking strategy on the firewall. 6. Limit SYN/ICMP traffic. The user must configure the maximum SYN/ICMP traffic on the router to limit the maximum bandwidth that SYN/ICMP packets can occupy. Therefore, when there is a large amount of SYN/ICMP traffic exceeding the limit, this means it is not normal network access, but hacking. In the beginning, limiting SYN/ICMP traffic was the best way to prevent DDoS. Although the effect of this method on DDoS is currently not widely used, it can still play a certain role. 7. Scan regularly. Existing network master nodes should be scanned regularly, checked for security vulnerabilities and new vulnerabilities cleaned up promptly. Computers on backbone nodes are the best locations for hackers to use because they have higher bandwidth. It is therefore very important to strengthen the security of these hosts. Furthermore, all computers connected to the major nodes of the network are server-level computers. Hence regular scanning for vulnerabilities becomes even more important. 8. Check the source of the visitor. Use suitable software to check whether the visitor's IP address is true. This should be done by reverse-searching the router: if it is fake,

it will be blocked. As said above, many hacker attacks often use fake IP addresses to confuse users and it is hard to find out from where they come. Therefore, for example, the use of Unicast Reverse Path Forwarding can reduce the occurrence of fake IP addresses and help improve network security. As seen above, we need experts who know more than hackers, and this is the duty that States and governments have towards their institutions, but primarily towards their citizens.

di Giancarlo Elia Valori Venerdì 26 Novembre 2021

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it