12 January 2024 17:03

There are many data groups that make up the different domains of the “cyber world”. When groups are able to collect and utilize massive amounts of data, they begin to amass power and influence. This data can be in the form of numbers, pictures, video, audio, or any type of data that can be digitized. These groups could become so powerful that they operate as though they are separate powers, creating separate cybersecurity domains
Companies such as Google, Facebook, and LinkedIn, could be considered to be data domains in our cyber world. Extending the analogy further, the people who work at these digital companies could be considered cybersecurity experts.
consider a domain to be an area to be protected. It may be limited by a logical or physical boundary. This will depend on the size of the system involved. In many respects, cybersecurity experts have to protect their domains according the laws of their own country.

The data collected within the Internet is considerably more than just the data that the users contribute voluntarily.
Cyber experts now have the technology to track worldwide weather trends, monitor the oceans, as well as the movement and behavior of people, animals and objects in real time.
New technologies, such as Geospatial Information Systems (GIS) and the Internet of Things (IoT), have emerged. These new technologies can track the health of trees in a neighborhood. They can provide up-to-date locations of vehicles, devices, individuals and materials. This type of information can save energy, improve efficiencies, and reduce safety risks. Each of these technologies will also result in exponentially expanding the amount of data collected, analyzed and used to understand the world. The data collected by GIS and IoE poses a tremendous challenge for cybersecurity professionals in the future. The type of data generated by these devices has the potential to enable cyber criminals to gain access to very intimate aspects of daily life.

Who Are the Cyber Criminals?

Amateurs
Amateurs, or script kiddies, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks. Some are just curious, while others try to demonstrate their skills and cause harm. They may be using basic tools, but the results can still be devastating.

Hackers
This group of criminals breaks into computers or networks to gain access for various reasons. The intent of the break-in determines the classification of these attackers as white, gray, or black hats.

White hat attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems. The owners of the system give permission to perform the break-in, and they receive the results of the test. On the other hand, black hat attackers take advantage of any vulnerability for illegal personal, financial or political gain. Gray hat attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda. Some gray hat hackers publish the facts about the vulnerability on the Internet, so that other attackers can exploit it.

Organized Hackers

These criminals include organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are usually groups of professional criminals focused on control, power, and wealth. The criminals are highly sophisticated and organized, and may even provide cybercrime as a service. Hacktivists make political statements to create awareness to issues that are important to them. Hacktivists publically publish embarrassing information about their victims. State-sponsored attackers gather intelligence or commit sabotage on behalf of their government. These attackers are usually highly trained and well-funded. Their attacks focus on specific goals that are beneficial to their government. Some state-sponsored attackers are even members of their nations’ armed forces.

Thwarting Cyber Criminals

- Creating comprehensive databases of known system vulnerabilities and attack signatures (a unique arrangement of information used to identify an attacker's attempt to exploit a known vulnerability). Organizations share these databases worldwide to help prepare for and fend off many common attacks.

CVE Databases (National Common Vulnerabilities and Exposures)

- Establishing early warning sensors and alert networks. Due to cost and the impossibility of monitoring every network, organizations monitor high-value targets or create imposters that look like high-value targets. Because these high-value targets are more likely to experience attacks, they warn others of potential attacks.

Honeynet Project

- Sharing cyber intelligence information. Business, government agencies and countries now collaborate to share critical information about serious attacks to critical targets in order to prevent similar attacks in other places. Many countries have established cyber intelligence agencies to collaborate worldwide in combating major cyberattacks.

InfraGard - partnership between FBI and other private sectors

- Establishing information security management standards among national and international organizations. The ISO 27000 is a good example of these international efforts.

- Enacting new laws to discourage cyberattacks and data breaches. These laws have severe penalties to punish cyber criminals caught carrying out illegal actions.

Using Advanced Weapons

Software vulnerabilities today rely on programming mistakes, protocol vulnerabilities, or system misconfigurations. The cyber criminal merely has to exploit one of these. For example, a common attack involved constructing an input to a program in order to sabotage the program, making it malfunction. This malfunction provided a doorway into the program or caused it to leak information.
There is a growing sophistication seen in cyberattacks today. An advanced persistent threat (APT) is a continuous computer hack that occurs under the radar against a specific object. Criminals usually choose an APT for business or political motives. An APT occurs over a long period with a high degree of secrecy using sophisticated malware.
Algorithm attacks can track system self-reporting data, like how much energy a computer is using, and use that information to select targets or trigger false alerts. Algorithmic attacks can also disable a computer by forcing it to use memory or by overworking its central processing unit. Algorithmic attacks are more devious because they exploit designs used to improve energy savings, decrease system failures, and improve efficiencies.
Finally, the new generation of attacks involves intelligent selection of victims. In the past, attacks would select the low hanging fruit or most vulnerable victims. However, with greater attention to detection and isolation of cyberattacks, cyber criminals must be more careful. They cannot risk early detection or the cybersecurity specialists will close the gates of the castle. As a result, many of the more sophisticated attacks will only launch if the attacker can match the object signature targeted.

Broader Scope and Cascade Effect

Federated identity management refers to multiple enterprises that let their users use the same identification credentials gaining access to the networks of all enterprises in the group. This broadens the scope and increases the probability of a cascading effect should an attack occur.
A federated identity links a subject's electronic identity across separate identity management systems. For example, a subject may be able to log onto Yahoo! with Google or Facebook credentials. This is an example of social login.
The goal of federated identity management is to share identity information automatically across castle boundaries. From the individual user's perspective, this means a single sign-on to the web.
It is imperative that organizations scrutinize the identifying information shared with partners. Social security numbers, names, and addresses may allow identity thieves the opportunity to steal this information from a partner to perpetrate fraud. The most common way to protect federated identity is to tie login ability to an authorized device.

The National Cybersecurity Workforce Framework

The Workforce Framework categorizes cybersecurity work into seven categories.
Operate and Maintain includes providing the support, administration, and maintenance required to ensure IT system performance and security.
Protect and Defend includes the identification, analysis, and mitigation of threats to internal systems and networks.
Investigate includes the investigation of cyber events and/or cyber crimes involving IT resources.

Collect and Operate includes specialized denial and deception operations and the collection of cybersecurity information.
Analyze includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence.
Oversight and Development provides for leadership, management, and direction to conduct cybersecurity work effectively.
Securely Provision includes conceptualizing, designing, and building secure IT systems.
Within each category, there are several specialty areas. The specialty areas then define common types of cybersecurity work.

Threats to Internet Services

There are many essential technical services needed for a network, and ultimately the Internet, to operate. These services include routing, addressing, domain naming, and database management. These services also serve as prime targets for cyber criminals.
Criminals use packet-sniffing tools to capture data streams over a network. This means that all sensitive data, like usernames, passwords and credit card numbers, are at risk. Packet sniffers work by monitoring and recording all information coming across a network. Criminals can also use rogue devices, such as unsecured Wi-Fi access points. If the criminal sets this up near a public place, such as a coffee shop, unsuspecting individuals may sign on and the packet sniffer copies their personal information.
Domain Name Service (DNS) translates a domain name, such as www.facebook.com, into its numerical IP address. If a DNS server does not know the IP address, it will ask another DNS server. With DNS spoofing (or DNS cache poisoning), the criminal introduces false data into a DNS resolver's cache. These poison attacks exploit a weakness in the DNS software that causes the DNS servers to redirect traffic for a specific domain to the criminal's computer, instead of the legitimate owner of the domain.
Packets transport data across a network or the Internet. Packet forgery (or packet injection) interferes with an established network communication by constructing packets to appear as if they are part of a communication. Packet forgery allows a criminal to disrupt or intercept packets. This process enables the criminal to hijack an authorized connection or denies an individual's ability to use certain network services. Cyber professionals call this a man-in-the-middle attack.
The examples given only scratch the surface of the types of threats criminals can launch against Internet and network services.

The Vulnerabilities of Mobile Devices

In the past, employees typically used company-issued computers connected to a corporate LAN. Administrators continuously monitor and update these computers to meet security requirements. Today, mobile devices such as iPhones, smartphones, tablets, and thousands of other devices, are becoming powerful substitutes for, or additions to, the traditional PC. More and more people are using these devices to access enterprise information. Bring Your Own Device (BYOD) is a growing trend. The inability to centrally manage and update mobile devices poses a growing threat to organizations that allow employee mobile devices on their networks.

Safety Implications

Emergency call centers in the U.S. are vulnerable to cyberattacks that could shut down 911 networks, jeopardizing public safety. A telephone denial of service (TDoS) attack uses phone calls against a target telephone network tying up the system and preventing legitimate calls from getting through. Next generation 911 call centers are vulnerable because they use Voice-over-IP (VoIP) systems rather than traditional landlines. In addition to TDoS attacks, these call centers can also be at risk of distributed-denial-of-service (DDoS) attacks that use many systems to flood the resources of the target making the target unavailable to legitimate users. There are many ways nowadays to request 911 help, from using an app on a smartphone to using a home security system.