Language of Cyber Security

Every day, new cyber security attacks are discovered. How can we prepare for the challenge? Knowledge is the answer! Stay aware of the latest threats and vulnerabilities and familiarize yourself with the language of cyber security.

- **Vulnerabilities –** how can a cyber-attacker "get in" to cause trouble?
- **Exploits –** what do I need to watch for?
- **Mitigating Controls –** what can I do to protect myself?

Vulnerabilities –flaws in software or hardware, such as coding errors or poor design that provide a cyber-attacker with an "open door" to cause trouble. Vulnerabilities may be found in the operating system, browser and applications on your PC, Smartphone or even your car or toaster! In short, anything that relies on any type of software may be vulnerable to attack.

Exploits –a piece of code that is specifically designed by the cyber-attackers to take advantage of vulnerabilities. Typically, an exploit attempts to access information or take control of the computer or device. Common examples include product exploits in Java and Adobe Flash Player, Browser Exploits, malware and malicious websites.

Mitigating Controls – steps taken to correct vulnerabilities to protect from exploits:

✓ Ensure software on your PC, Smartphone and other devices is up to date with the latest security patches

✓ Keep anti-virus software current and perform regular scanning

✓ Avoid suspicious websites and email attachments and links

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help. Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, contact us with the code "Red Button".

Learn More at DDoS Warriors To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security