Vulnerabilities

Proficiency Code: A

Vulnerability is a problem, or weakness, in a computer system that allows an intruder or hacker to exploit the system's information security. *Vulnerability* is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

It is unlikely that we can ever achieve total Information System (IS) security even with the controls and safeguards we have in place. New threats and vulnerabilities continue to emerge so the Air Force is always working to identify and analyze them so we can maintain an appropriate level of protection through established safeguards based on security requirements. Air Force Network Integration Center (AFNIC) and the program manager develop and coordinate the schedules and details for network assessment. The particular details of network risk assessment depend on the system design, environment, and classification of data on that network.

Computer Security (COMPUSEC) and Information Assurance (IA) threats cause harm to information (data) or to the IS that process that data. Threats exist from natural, environmental, human, and viruses. We will discuss each one briefly.

Natural

Nature causes natural threats, which includes earthquakes, floods, hurricanes, snow/ice, tornado/windstorms, lightning, or severe storms. Every location is subject to some of these types of threats and therefore must have precautionary measures to minimize system damages.

Environmental

Environmental threats result from man-made items in the environment. These can include flaws in building construction, improper implementation of utilities, inadequate wiring and poor housekeeping practices. Program managers along with the facility management should work together to identify environmental inadequacies.

Human

Human threats can be either intentional or unintentional. Intentional threats are deliberate attacks by an individual to degrade or damage information systems, network resources, or information. Reasons for intentional attacks could include degrading system integrity, revenge, or personal gain. Unintentional threats cause inadvertent damage to ISs due to lack of training, carelessness, or accidental intrusions. A computer system is no more secure than the persons responsible for its operation are. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals or by deliberately deceiving them.

Viruses

One of the most common COMPUSEC threats is software viruses. Software viruses are software programs that destroy data on computers that contract them. They also can spread from computer system to computer system. Damages from viruses can result in: reformatting a hard disk; erasing programs and files; adding unrecognizable characters to files; or destroying disk directories and file allocation tables preventing the computer from using the tables or directories to locate files. One of the newest threats comes from spyware. Spyware is computer software that collects personal information about users without their informed consent.

Wireless services and portable electronic devices

One of the newest COMPUSEC threats comes from hand held portable electronic devices (PED) and wireless technologies. Wireless services are susceptible to interference (friendly and unfriendly) and are easily jammed resulting in no service. Proposed wireless service solutions must be coordinated with the responsible spectrum manager before finalizing a technical solution and purchasing these products using AF Form 3215, Information Technology/National Security Systems (IT/NSS) Requirements Document.

Wireless services

Wireless services (includes but is not limited to wireless devices, systems, services, and technologies) that are integrated or connected to DOD networks are considered part of those networks. All wireless comply with DOD Directive 8500.1 and 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Information Network (DODIN), meet the evaluation and validation requirements of DODI 8500.2 and be certified and accredited according to DOD Instruction 5200.40. This includes systems for joint use and Air Force systems that must interoperate directly with other service or coalition partner's networks.

Portable electronic devices

PED are any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to personal digital assistant (PDA), cellular phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

PED is a generic title used to describe the numerous amounts of small electronic items that are widely available. Nearly all of these devices have wireless telecommunications capabilities that offer tremendous advantages for government users, yet pose a security risk to classified networks. It is difficult to differentiate between these PEDs because they have similar capabilities and functions using various forms and formats.

Wireless-enabled PEDs must comply with the wireless systems requirements:

• Encrypt data transmitted through a commercial or wireless network (data-in-transit) must use National Institute of Standards and Technology (NIST)-certified cryptography such as Federal Information Processing Standards (FIPS) 140–2 validated.

• Data stored or processed by the PED requires protection against tampering, theft and loss.

• You must encrypt stored information (data-at-rest) using NIST-certified cryptography such as FIPS 140–2 validated. Use identification and authentication methods, Identification and authentication to control access to encrypted, as well as unencrypted, information.

• Use of a PED for storing or processing high impact personally identifiable information (PII) electronic records requires designated approval authority (DAA) approval.

Restrict use of PED to protected workplaces; PEDs taken outside protected workplaces require signing in and out of protected workplaces for logging and tracking procedures. PED can leave protected workplaces with the approval of a supervising official.

Computer security and Information Assurance vulnerabilities

COMPUSEC and IA vulnerabilities are weaknesses in ISs or security procedures that can be exploited by the threats we just covered.