NJ OFFICE OF INFORMATION TECHNOLOGY

P.O. Box 212 www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

NEW JERSEY STATE POLICE
EXAMPLES OF CRIMINAL INTENT

The Intent of the individual is a key factor in determining the nature of the incident. (For instance, One employee's use of another person's login (with permission) to perform normal business functions because they forgot their login/password, or the first user inadvertently remained logged in after leaving, would not necessarily violate New Jersey criminal statutes).

I. CIRCUMSTANCES THAT POTENTIALLY VIOLATE NEW JERSEY CRIMINAL STATUTES INCLUDE:

A. Logging into or accessing a workstation with the owner's password to check their email or send an email from their account without their approval.

B. Locally or remotely accesses either a computer or network without explicit permission to view the contents of the system, or to copy, damage, or alter it in any way.

C. Attempts to gain access to a computer, network, or storage device the individual knows they do not have legitimate access to.

D. Preventing service (Denial of Service Attack) to a computer, network, Internet, or some other available service.

E. Without permission, remove, take, or copy data, such as personal information, computer programs, or software.

F. Attempting to login (guessing or using a password cracker) to a system, computer, or network, to make system (or any) changes. [e.g., attempting to guess administrative passwords to obtain increased rights or access (Privilege escalation)].

G. Other examples: Attempting to search your supervisor's computer, database, network, etc., in order to read his/her evaluation of the employee or a coworker.

H. Accessing someone else's email (without their knowledge or permission) to either read, copy, send, alter, delete, etc…

I. Knowingly sending a virus, worm, or other program/script that will be likely to alter, damage, copy, retrieve, or delete data/operating system, service, accessibility, etc…

This general list covers the majority of common circumstances where law enforcement intervention is appropriate. It is by no means a comprehensive list of circumstances that are violative of New Jersey statutes. If doubt exists, make contact with the Cyber Crimes Unit and the case-by-case facts will be evaluated for a potential response by unit personnel.

II. COMPUTER FORENSICS

Computer forensics is a discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

III. DEFINITIONS AND EXAMPLES OF SECURITY EVENTS AND INCIDENTS

Distinguishing between events and incidents is not always easy and personnel may not know if an event has already been reported – when in doubt, personnel should err on the side of caution and report the event to the Network Call Center as required by this policy in addition to any internal agency notification process that may be in place.

IV. SECURITY VIOLATION EXAMPLE

Mary logs into a UNIX system and notices that the “last login” message indicates that she logged in overnight from a computer belonging to a foreign university, although she knows that she did not. This may indicate a system intrusion (i.e., a security violation); therefore, Mary should immediately contact the NCC in addition to any internal agency notification process that may be in place. Mary should not change the configuration of her UNIX account, or contact anyone else at the foreign university, or take any other investigative action before contacting her respective help desk or IT staff/administrator.

V. DENIAL OF SERVICE EXAMPLE

Denial of Service is an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

An attacker sends specially crafted packets to a Web server, causing it to crash.

An attacker directs hundreds of external compromised workstations to send as many Internet Control Message Protocol (ICMP) requests as possible to the organization’s network.

Meanwhile, Sue investigates a slow enterprise mail server and discovers that a departmental mail server is sending thousands of messages infected with a virus to the enterprise server. Although the anti-virus system is correctly handling the

infected messages, the increased traffic is severely impacting the messaging system. Sue should immediately contact the NCC in addition to any internal agency notification process that may be in place.

VI. MALICIOUS CODE EXAMPLE

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

A. A virus is designed to self-replicate, make copies of itself, and distribute the copies of other files, programs, or computers. Viruses insert themselves into host programs and propagate when the infected program is executed, generally by the user interaction.

B. A computer worm is a self-replicating computer program that does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers. A worm uses a network to send copies of itself to other systems and it does so without any intervention. A worm will usually reside in a computers' memory unnoticed until the rate of replication reduces system resources to the point that it becomes noticeable.

C. Trojan horses are programs that appear to be benign but actually have a hidden malicious purpose that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

John receives e-mail from his co-worker, Nancy, with a screen saver attached as a compressed file. He asks Nancy if she sent the screen saver and she says that she did not. This e-mail message may indicate an outbreak of an e-mail worm that is not detected by current anti-virus system signatures (i.e., a computer virus infection); therefore, John should immediately contact any internal agency notification process that may be in place. John should not open or delete the e-mail message and Nancy should not make any changes to her computer's configuration until directed by the responding personnel.

An organization receives a warning from an antivirus vendor that a new virus is spreading rapidly via e-mail throughout the Internet. The virus takes advantage of a vulnerability that is present in many of the organization's hosts. Based on previous antivirus incidents, the organization expects that the new virus will infect some of its hosts within the next three hours.

An attack using a blended approach might send a virus via an e-mail attachment, along with a Trojan horse embedded in an HTML file that will cause damage to the recipient computer.

D. A blended threat typically includes:

1. More than one means of propagation -- for example, distributing a hybrid virus/worm via e-mail that will self-replicate and also infect a Web server, so that contagion will spread through all visitors to a particular site.

2. Exploitation of vulnerabilities, which may be pre-existing or be caused by malware distributed as part of the attack.

3. The intent to cause real harm (rather than just causing minor computer problems for victims), for example, by launching a denial of service (DOS) attack against a target, or delivering a Trojan horse that will be activated at some later date.

4. Automation that enables increasing contagion without requiring user actions, such as opening attachments.

VII. UNAUTHORIZED ACCESS EXAMPLES

A person gains logical or physical access without permission to a network, system, application, data, or other resource.

An attacker runs an exploit tool to gain access to a server's password file.

A perpetrator obtains unauthorized administrator-level access to a system and then threatens the victim that the details of the break-in will be released to the press if the organization does not pay a designated sum of money.

Unauthorized access is typically gained through the exploitation of operating system or application vulnerabilities, the acquisition of usernames and passwords, or social engineering. Attackers may acquire limited access through one vulnerability and use that access to attack more vulnerabilities, eventually gaining higher levels of access. Examples of unauthorized access incidents include:

A. Performing a remote root compromise of an e-mail server.

B. Defacing a Web server.

C. Guessing and cracking passwords.

D. Copying a database containing credit card numbers.

E. Viewing sensitive data, including payroll records and medical information, without authorization.

F. Running a packet sniffer on a workstation to capture usernames and passwords.

G. Using a permission error on an anonymous FTP server to distribute pirated software and music files.

H. Dialing into an unsecured modem and gaining internal network access.

I. Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password.

J. Using an unattended, logged-in workstation without permission.

VIII. SOCIAL ENGINEERING

Social engineering is a term for tricking people to give up something of value. Social engineering attacks the weaknesses in people rather than systems. Online versions of social engineering can be referred to as "phishing or pharming." Cleverly performed, hackers can use social engineering attacks to gain passwords, account numbers, etc. from unsuspecting users.

IX. OTHER EXAMPLES

Other examples of Events that may be Incidents include:

A. A caller claims to be "from technical support" and requests a user's password.

B. Unauthorized attempts (either failed or successful) to gain access to a state or agency information system or its data.

C. Unauthorized or misuse of a system for the processing or storage of data.

D. Actual or suspected loss of confidential or personal information.

E. Using information systems to commit financial crimes or cause financial loss to the State or the citizens of New Jersey.

F. Attempted or actual instances of social engineering.

G. Perpetration of hoaxes.

H. Identified weaknesses or vulnerabilities in a state or agency information system.