Chapter 1

Attacks on IT Systems:
Categories of Motives

Georg Disterer
University of Applied Sciences Hannover, Germany

ABSTRACT

Attacks on IT systems are deliberate acts with the determined aim of destroying, damaging or misusing a company's IT systems. This type of risk is growing significantly in the last years. Today it must be assumed that the greatest dangers for IT systems no longer emanate from individuals, but rather from mafia-like structured, organised crime. Knowing categories of motives and attributes of actors can support the discovery, investigation and persecution of attacks and malicious activities. The categories make it easier to develop preventive and reactive policies and measures to mitigate the risks of computer crime.

INTRODUCTION

For a long time now, operators of IT systems have had to reckon with their systems being attacked and, as a result, being subjected to unauthorised use, and misuse. Early cases are chronicled for 1961, for instance, when the clearing procedure at MIT's (Massachusetts Institute of Technology) mainframe computer was compromised by special programs, so that the programmers could use systems capacities without having to pay the costs (Cross, 2008). In those days, such hackers (in the sense of burglars), with their technical skills, also switched off telephone system controls and phoned free-of-charge. And, for all intents and purposes, they triggered quite positive associations among the general public, since they out-manoeuvred big companies and monopolies, perceived as over-powerful. In films of the 70s and 80s, hackers were stylised as representatives of resistance against the establishment.

But still, financial damages have also been noted since the 60s, through manipulations of IT systems with which salary or invoice payments

DOI: 10.4018/978-1-61350-507-6.ch001

have been diverted, or the status of accounts has been altered (Dannecker, 1996). Thus, the abuse of IT systems is to be regarded as an attack, which is very difficult to prevent as long as attackers weigh up possible advantages to be gained for themselves against the effort necessary, plus the risk of being caught and the penalty, and come to the conclusion that their activity seems to be worth the risk. The definition of "attacks" covers all deliberate acts with the determined aim of destroying, damaging or misusing a company's IT systems. The concentration on attacks as deliberate and purposeful acts excludes from the discussion two categories of threatening influences on IT systems: erroneous actions (perhaps user mistakes in handling or operating, a lack of skill, or inability), or inadvertent actions (perhaps handling or operating errors through inattention or carelessness). Further threats, moreover, and the resulting damages are also excluded from the discussion: the use of IT systems can hold immense risks for companies if faults in operating processes and the shut-down of IT systems are the result. Currently, for example, so many unwanted incoming e-mails (SPAM) are received by companies that identifying and processing them at best causes costs, and at worst causes the e-mail server to grind to a halt. Information on the portion of unwanted mails vary: a mere 13 to 15% of all incoming mails are regarded as „wanted" (Messaging Anti-Abuse Working Group, 2008)—for the German Administration Offices a portion of 1.5% of wanted mails is assumed (BSI 2009). Since the majority of these mails advertise products, SPAM mails won't be spoken about here under the section "attacks", since their aim is not foremost one of the purposeful destruction (damage or misuse) of the IT systems (in this case, e-mail server) of the companies concerned.

Further essential threats of IT systems which do not fall under the category of a threat are natural incidents and catastrophies like floods, lightning and earthquakes, acts of war, technical defects and technical failure (through material fatigue, material defects, quality faults, or wear and tear and old components), function faults (e.g. through development or production faults), or organisational faults (lack of responsible staff and competencies, inconsistent deputising arrangements, insufficient controls and lack of resources for protective measures). There are classic politics and measures against these threats, like the redundant design of technical systems (e.g. CPUs and storage devices), additional dedicated devices (e.g. emergency power generators), further education/courses/training, and organisational or technical controls.

Types of Attacks

Attacks as intentional and purposeful acts to destroy, to damage or to misuse IT systems are major threats against the security objectives availability, integrity and confidentiality of information processing.

During the preparation phase of an attack, vulnerabilities of IT systems are explored by various techniques. Scanning or probing Web sites and applications attackers get information about the structure and parameters of the systems and the underlying technical infrastructure. Scanning the target systems for known vulnerabilities in applications, systems software (like web server, database, middleware, operating system), and hardware configuration. With knowledge about the IT systems attackers may try use known vulnerabilities or default settings to exploit the system.

Access systems can be attacked by programs that discover passwords and therefore enable abusing user accounts. Password-cracking programs can test a huge number of possible and even complex passwords using dictionaries; the high processing speed of their computer give attackers a chance to break into systems with these kinds of brute-force attacks.

With eavesdropping techniques attackers monitor network traffic and data transmission like wiretapping. With sniffing programs they can