Security Lab – Analysis of the MELANI Report

1 Introduction

MELANI[1] is the "Reporting and Analysis Centre for Information Assurance" of the Swiss Confederation with the task to protect ICT infrastructure in Switzerland from abuse, attacks and outages.

One of the most interesting «products» of MELANI is the semi-annual report *Information Assurance – Situation in Switzerland and internationally*, which is produced in collaboration with the Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK[2]).

In this lab, you are working with the latest (newest) edition of the report. Get the English version of this report as follows:

- Browse to *http://www.melani.admin.ch/dokumentation*
- Select *EN* at the top right
- Download the report listed at the top

The report to be used for this lab is also available on OLAT.

2 Task

The goal of this lab is to get a good impression of the current state with respect to cyberattacks and that you can analyze security-relevant information and extract important information.

Your task is to analyze the report. We recommend reading the entire report because it provides you with a good overview of the current situation. However, the focus of the analysis is on chapters 4 and 5, the situation of the national and international ICT infrastructure.

Some of the subchapters 4.x and 5.x describe actual attacks and sometimes also accidental disruptions (e.g. due to operational mistakes during maintenance work, software defects, or errors during software updates) that have happened. For these attacks or accidental disruptions, you should think about the following:

- Which (one or more) of the security goals (Confidentiality, Integrity, Availability) has been violated and in what way?
- What was the motivation of the attacker?
- What mistakes were made that allowed the attack to be carried out successfully? Were there any vulnerabilities (e.g. software defects or operational shortcomings) exploited? Was human error involved? In any case, try to explain the problem(s) that allowed the successful execution of the attack.
- What would you do to prevent the problem from happening again? Try to provide reasonable and practical solutions. In the case of vulnerabilities, try to explain how they could be fixed.

During your analysis, take the following into account:

- Besides information about actual attacks or accidental disruptions, chapters 4 and 5 also contain further information. This includes reports about security requirements for specific companies, legal verdicts, political activities with respect to security, new security technologies, general activities of hacker groups, general information about attacks and attack vectors, malware trends, discovered vulnerabilities, etc. Read this information as well, but you should focus your analysis and corresponding answers (see below) to the topics that describe actual attacks or accidents that have happened.

1 http://www.melani.admin.ch
2 http://www.cybercrime.admin.ch

- In some cases, you won't get enough information to unambiguously answer the questions (for instance, details about the underlying vulnerability are often missing). Nevertheless, try to provide reasonable answers in any case, even if you have to be a bit creative in some cases.
- We have only just started with the module and you likely don't know yet very much about vulnerabilities and security measures. But that shouldn't be a problem because it's not the primary goal of this exercise to provide 100% correct answers in all cases. What's important is that you are thinking in detail about the described attacks and that you try to give reasonable answers.

3 Example

As an example, we use an attack from a previously published semi-annual report and provide a reasonable answer of the analysis of the attack.

3.1 Attack

4.7 "Here you have" computer worm – "Iraq Resistance"

On 9 September 2010, a previously unknown computer worm began to spread on the Internet, disrupting the e-mail traffic of several American companies. The worm sent e-mails with the subject line "Here you have" and the e-mail body "This is The Document I told you about, you can find it Here" or "Just For you" and the e-mail body "This is The Free Download Sex Movies, you can find it Here". The "Here" included a link to the malware. The link supposedly referred to a document or video file, but in fact clicking on it would download the malware to the computer, and the user was requested to execute the file. The worm then spread through shared drives and sent the e-mail with the link to contacts in the victim's address book. Other than spreading and causing excessive amounts of e-mail that overloaded some servers, the worm did not cause any particular damage.

Authorship was admitted by a person with the *nickname* "Iraq Resistance" who claimed to be affiliated with a previously unknown group "Tariq bin Ziyad Brigades for Electronic Attack (TbZBEA)". But the author's goal was not to cause as much damage as possible. Claiming responsibility on YouTube, the author said he was not a terrorist.[39] The action was to be understood as a protest: firstly against the US invasion of Iraq, and secondly against the Quran burning announced for 11 September 2010 in the US (which was ultimately not carried out, however because of other reasons).

The method of picking off address books on infected systems and employing an e-mail body with a clickable link is a simple but very effective form of *social engineering*. These e-mails are trusted, since the sender is known, and the body of the message is general enough that it may sound plausible to many recipients. In 2000 ("I LOVE YOU" virus) and 2001 ("Anna Kournikova" virus), similar computer worms were circulated which were spread using comparable methods. An important rule in dealing with e-mails is therefore that one should as a rule treat unexpectedly received messages (even from known senders) including links or attachments with caution, and in cases of doubt one should check with the sender whether the message is legitimate. Attachments used recently as infection vectors have increasingly been PDF documents. Even by simply clicking on a link to a prepared website or by opening a file, the computer may become infected.

The "Here you have" worm used here was circulated for politically and religiously motivated cyber protest. If, in addition to its spreading mechanism, it had also included instructions to damage widespread data, then the story could have had a far worse ending for some companies.

3.2 Answer

4.7 "Here you have" computer worm – "Iraq Resistance"	
Security Goal(s):	Availability: E-mail availability was reduced by e-mail flood and overloading the mail server.
Motivation:	Protest against the US invasion in Iraq and announced Koran burnings.
Mistake(s)/ Vulnerability(es):	Lack of security awareness: Users click a link in a questionable e-mail message and in addition execute the downloaded file. (Remark: Based on the attack description, no software vulnerability appears to have been involved.)
Solution:	Increase security awareness of users, e.g. by training within companies. Use malware scanners (on mail server and user computers) to detect the received e-mail message or the downloaded file as malware – assuming the scanners know the corresponding malware signatures.

Lab Points

For **2 Lab Points** you must document your answers as in the example above and submit your solution by e-mail to the instructor and use *SecLab - MELANI - group X - name1 name2* as the subject, corresponding to your group number and the names of the group members. You can submit either pdf or doc(x) formats, and of course it's also OK if you scan and submit a handwritten solution. Please use entire sentences in your solution, individual keywords won't be accepted.

You get 2 points if you provide reasonable and complete answers as in the example above for *at least 5 different attacks* (1 point for 3 answers). In addition, the following rules apply:

- Sometimes, a topic in 4.x or 5.x summarizes several similar attacks or accidents. In this case, consider it as *one* event and also provide only one answer according to the format above. Also, if two topics are very similar (e.g. two phishing attacks using the same method with basically the same goal), then use only one of them in your answers.
- Solutions that were obviously copied from others won't give any points.