

Security in organizations course
Digital Security group,
Radboud University Nijmegen

Alternative assignment 4 for Kerckhoffs students, August 30 2010

Goals:

- Performing a technically oriented risk analysis.
- Reporting on technical issues to management

Background

A hospital provides its clients (e.g., patients) on-line access to their medical records in an application called MEDFILE. This application uses HTTPS as a basic communication protocol and a two-factor authentication mechanism. One factor is a user / name password and the other factor is an SMS sent from MEDFILE to the patient each time the user wants to access its records.

Recently Govcert published a warning ('Afluisteren van GSM-communicatie dichterbij'; <http://www.govcert.nl/download.html?f=154>) on (near) future attacks on GSM security that might have its ramifications for SMS security too. Govcert recommends that organizations perform a risk assessment related to these attacks and to come up with additional controls if necessary.

Task

You are the security officer of the hospital and you are asked by your management to perform such a risk assessment and treatment. The risk assessment needs to be in conformance with the steps in ISO 27005.

In line with this the following questions are posed by the management:

1. Do some internet research and give a short description of the vulnerability and an indication of what it will take to exploit it.
2. Given an prediction of the time before 'open software' will be on the internet that will allow exploitation of the vulnerability (e.g. such as Airsnort for WEP).
3. Give an indication of the required hardware and related cost required to exploit the vulnerability, given the 'open software'.
4. Give an indication of the threats (who, motive) that could exploit this vulnerability (i.e. using the 'open software') and the possible impact of that.
5. Give an indication of the probabilities that the identified threats will become manifest.
6. Summarize the risks (based on threats, impact, probabilities): what do you think is the biggest risk when the 'open software' is available?
7. Describe three controls to mitigate the risks.
8. Should the hospital immediately stop using the SMS based authentication method in MEDFILE and change it for something else?
9. Give an estimate on how long the hospital can proceed with the current SMS solution.
10. Give a roadmap for dealing with this vulnerability.

Report on the nine points above in a PowerPoint presentation (or the open office variant of it) meant to be used for a presentation for your management. Your management has basic knowledge on IT and security but are not experts; your presentation should take that into account.

This document is freely distributable as long as it is unmodified in any way.