Enhancing information systems security in an academic organization

François Morris

Université Pierre et Marie Curie & CNRS

Preface

The Centre National de la Recherche Scientifique (CNRS) is the biggest public research institute in France. The activity fields cover a large spectrum from social science to mathematics including physic and biology. Some laboratories are directly managed by the CNRS but many others are joint structures with a university or even a private company. With 1300 laboratories the CNRS is a split organization.

The author manage the information system in a laboratory shared between the CNRS and a university. He participates to actions engaged by the CNRS to improve the security in its laboratories.

1 Context

1.1 An unfavourable environment

The common paradigm that applies even to multinational corporations is to have a private network for all the data traffic pertaining to the organization and few very well controlled gateways for exchanging with the outside world. For academic research the situation is very different. Often a scientist has more exchanges with people living on another continent than with people in his own laboratory. Each site, campus, laboratory is directly connected to the Internet. There is no private network (Intranet) excepted sometimes for the administration needs. The security cannot be performed at the border because there is no true border. So the controls must be located very close to the user's computer.

People have various statuses. Many are temporary (students, interns, visitors, guests). Even permanent people in the same laboratory belongs to (and are paid by) different organizations. Added to the fact that people in this environment are individualistic if not libertarian, it is very difficult to enforce a security policy. When there is no real hierarchical power, persuasion must be used.

The academic research was involved in the Internet development since the beginning. Apart from the common situation where the web an e-mail represent the great majority of uses, here all sorts of protocols and applications are used and there are justified reasons to do so. Practically there is no difference between the Internet and an Intranet. The situation vas adapted at the heroic beginnings when every one tried to do his best effort to have a working network. Today this position is clearly not sustainable and we have to protect from malicious intruders.

Sure, for any security concerned people, it is a true nightmare.

1.2 Several advantages

The technical staff, especially in information systems, is generally competent, motivated and capable of initiatives. The creativity allows developing innovative and efficient solutions despite the weakness of the budgets.

The practice of exchanges, open-mindedness, dialog, co-operation is a serious advantage compared to more closed structures.

Compared to other places the instruction level is high and the users are generally well skilled.

1.3 Target

It must be said. In this context a perfectly secured information system cannot be achieved. We have to be satisfied with a limited, realistic target that can be aimed.

2 Evaluating the threats

Before defining any security policy the first thing to do is evaluating he threats. Depending on the representation of the world we have, we can put an index in a scale from friendly to hostile. If anybody is considered as a friend there is no need to implement security controls. If the whole world is considered as hostile the only possibility is to keep isolated. In the real world the situation is between these two extremes. We can trust some people, we must protect from other ones.

We must determine the assets to be protected. The information system which is now a very important tool for many scientists must be keep in a working state. Some data must be preserved from destruction, theft, and alteration. Among these data are research results, papers to be submitted, and contracts… The respectability of the organization must also be considered very seriously. The diversion of a web server to display pornographic images is anecdotal compared to the spreading of false scientific results without the knowledge of the organization by people having a cause to defend. If the systems are hacked and used to perpetrate attacks to outside systems the responsibility can be engaged. In order to develop partnership the information system must be trusted.

The direct and indirect costs of a security incident have to be evaluated. There is obviously no need to implement expensive solutions in order to protect from attacks of benign consequences. But often the analysis shows that security related incident can have disastrous effects. It is a strong incitation to define a security policy.

3 Defining and implementing a security policy

The security is first an organizational problem before being a technical one. To install a firewall is not a panacea.

3.1 People

The laboratory manager, as in many other domains, is the authority responsible for information systems security. If the management is not aware of the security problems and not strongly committed to cope with them nothing serious can be done. The manager takes consults, assigns tasks to execute but he must initiate the security policy.

The technical staff has to implement the security policy. In a so rapidly changing field a key point is to maintain the skills of the people. Education, training is the first action to do. The experience, the competence is spread among many people in the community. It is very useful these people co-operate, communicate in a supporting network. The organization role is to promote education operations, to stimulate the co-operations between the people.

The weakest point in security matters is always the user. Is not useful to pay for expensive security measures if the password is written on paper stuck on the screen. The users must know the rules to follow. Having a charter defining the user behaviour is a first step in developing users responsibility. The large spreading of viruses or worms as ”I love you” has proved that often the users ignore the warnings and perform dangerous actions. You can use very strong cryptographic tools with 168 bits symmetric keys (triple DES), 2048 bits asymmetric keys (RSA) You can invest a lot of money and time in deploying a PKI (Public Keys Interchange). But all the efforts would reduced to quite nothing if the private key is only protected by a weak password that can be easily cracked. Recently ”man in the middle” (MITM) exploits have been proved. They require the user ingenuously accepts a fake certificate by ignoring warning messages. The cryptographic tools are very useful to increase the security but never forget the human factor.

3.2 Architecture

The security has to be considered at the first stage of a project. It is always difficult, costly to secure an existing application.

Not each machine needs a complete access to the Internet. The first thing is to establish the matrix defining the relation between the machines and the needed services. Then it is possible to define architecture, build sub-networks.

Standardizing the systems help to manage them. It is easier to replicate a system from a model than to build a new one from scratch.

If only few systems are exposed the security becomes manageable.

3.3 Technical solutions

It does not necessarily require expensive hardware and software. Implementing filters in the existing routers is the first thing to do and is a big jump in the security enhancement.

4 Measuring the security

A difficult but necessary task is to measure how the security policy is efficient.

4.1 Analysis of the reported incidents

The first idea to measure the efficiency of a security policy is to analyze the reported incidents before and after. Only a very low percentage of security incidents are detected and fewer are reported. An increase in the numbers after implementing solutions to enhance the security may simply reflect a better detection of the incidents due to the commitment of the staff. Despite the huge bias the reported incidents are an element of a security dashboard. If they are consolidated on a large scale it possible to find trends and to have proactive measures.

4.2 Intrusion simulation

Using tools to simulate known vulnerabilities produces a more reliable measure of the security level. The main interest is the pedagogic aspect. They show to the technical staff the discovered vulnerabilities and how to fix them. Unfortunately they are rather difficult to use, yield to many false alarms and need to bee very careful to avoid to stop services by simulating an attack. By using these tools on the different sides of a router it is possible to measure the efficiency of the filters. The CNRS has deployed Internet Scanner from ISSto perform this task.

4.3 Intrusion detection

Now tools have been developed that permit by continuously scanning the network traffic to recognize the attacks. Two methods are used. The first use signatures of known attacks. The is the same limitation as for antivirus, the signatures database must be regularly updated. The second is a behavioural approach. Today it is still a research project ant it may have legal implications. Such tools would be good instruments to measure the efficiency of the security if they do not yield to so many false alarms and ignore so much attacks.

4.4 Expertise

The analysis of the information system with good sense, critical spirit, accurate knowledge of existing attacks is a good mean to evaluate the security level and to suggest improvements. The only problem is to have skilled experts.

4.5 Feedback loop

Regularly a new assessment of the threats, the assets to protect, the risks must be conducted and security policy consequently adapted. The security, is a dynamic process.

5 An experience in the CNRS

To obtain a perfectly safe system cannot be considered as a realistic target. If there is no absolute measure to evaluate the security, it was obvious from reported incidents, the help of some tools and good sense that the security level was unacceptably low. In order to raise it several actions were engaged.

The first one, few years ago, was to increase the awareness of the security problems among the laboratory managers (with mixed results) and the people running the information systems. It was established a list of recipes to apply in order to improve the security. The main technical action was to implement filters in the existing routers (templates that can be easily adapted are available). A major benefit was the establishment of relationships between the actors and the setting up of a supporting network. In order to evaluate the security and consequently eliminate the vulnerabilities, Internet Scanner from ISS was deployed. If this product is rather difficult to use, it is a very pedagogic tool to show to technical staff the existing vulnerabilities, to explain their origin and gives rules to eliminate them.

The last action still in progress is to increase the skills of technical staff. No adapted curriculum was found on the education market because the needs are very specific and cover an extensive knowledge. The competencies are available in the community. So it was decide to develop the curriculum, the lectures inside the organization. A document containing about 500 pages has been written. It was a tremendous work especially for people having many other tasks to perform.

6 Conclusion

To raise the security level is a necessity. The level that can be reasonably achieved is considerably below the one that would be desirable. It must not be a reason to do nothing but to the contrary never stop to promote the security.

Never trust the vendor who wants to sell you an expensive security solution. In security matters the human factors are much more important than the technical ones. So information, training, education are the first actions to perform. Never forget that the necessary technical solutions have to be deployed by people.