An experiment in security at the University of Poitiers

Ollive Franck

Université de Poitiers, France

Preface

For several years, the University of Poitiers has gradually realized the strategic value, inescapable and irreversible, of the use of information processing. The mass of information dealt with and the number of users relying daily on this support require a reliable and performing infrastructure. Although they were the object of a moderate interest at the start, the problems resulting from how to make secure the information circulating between the users have been largely taken into account for the last four years at the highest level of the university. This growing awareness of the leading executives of the university has removed a lot of obstacles and has directed the security objectives very close to the needs of the users. However, one should not hide the problems that have been run into: most of the times they were net of a technical order. Indeed, it is necessary to define correctly the role played by the actors of the securisation and have it accepted and respected by all.

There is no miracle recipe to implement an efficient security system. However, one necessary element is to define clear and accurate objectives. It is methodically and by drawing conclusions from past experiences that the university can make progress in the field of security.

1 Introduction

The university of Poitiers has the double peculiarity of being one of the oldest universities of France and of being scattered over about fifteen sites. It is therefore not easy to implement the securisation of the information systems so as to insure a minimum risk level. Indeed we are quickly faced with several determining factors in the choice of a policy of risk managements. Those are: the distance between the sites, the safeguard of the scientific patrimony, the freedom of expression of the personnel, the range of action granted to those responsible for the security, the habits of the users, the financial problems....

Before 1997. the security of the information systems, at the university of Poitiers as in many other establishments. was considered as a minor problem concerning only other people. Unfortunately, the reality was quite different and quickly forced the decision-makers to change opinions. Indeed, following several visits of the Home Security Branch of the Police in our premises to enquire about bounces, the people in charge became aware that it was necessary to ensure a protection. An objective was set up : to prevent bounces from being possible. Once more, reality required that the restrictive objective should be revised. When intruding into the field of the security of information systems, a great amount of our prejudices became obsolete (such as protecting only the main sites with a filler box ....). One had to realize that it was necessary to set up a policy of risk management bound to the information systems by defining administrative / technical as well as preventive measures and personnel training.

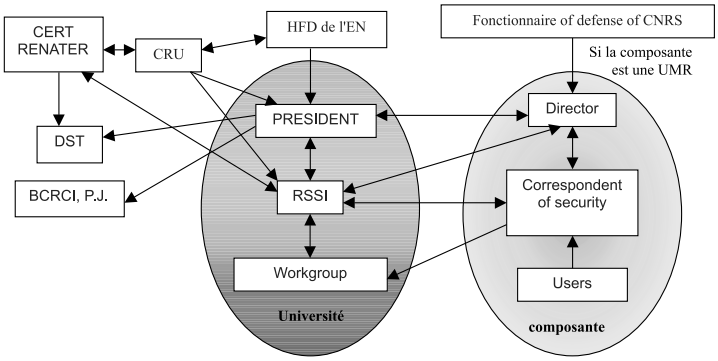
The next chapter will deal with management and administrative aspects. The prevention of risks and personnel training will be described in the third chapter. The fourth will state the choices and technical achievements and the last one will give a financial balance.

2 Administrative organisation

One of the clues for the smooth working of a university is to set up an administrative and organizational scheme which the users can rely on and find the requisite references to bring to fruition the missions they are trusted with. This is the rule we have applied to define all the regulations governing the people that have to deal with the security of the information systems of the university of Poitiers. It is however important to keep in mind that the established regulations must only be a reference mark for the user and in no way bring additional constraints. The basic principle we have adopted is that it is not possible to implement safety measures without the agreement of the users. Otherwise, they will find a means of getting round the safety measures.

2.1 The agents of security

The safety of information systems cannot be summed up in the installation of a material solution. The securisation of a university is the prerogative of a team that must be operational every day. We have started our reflection by defining all the persons and groups that come into play in our safety-ensuring process.



Source [1]

National level

In France, the security of the university information systems is represented at the level of the Ministry of National Education by a higher civil servant of the Defense Ministry (HFD). This person conveys the recommendations to the Presidents of the universities. He

is helped in his job by the advice and actions of the security cell of the Network Committee of the Universities (CRU). One of the most important recommendations as far as administration is concerned is the appointment, in each university, of a person responsible for the security of the information systems (RSSI) who, hierarchically, depends directly front the President of the university.

The majority of universities houses mixed research units where both researchers and university personnel can be found. Within this context, the problem of securisation is more complex because of a shared sponsoring at 50 %. Indeed, because he belongs to the National Center of Scientific Research (CNRS), it is the Defense Civil Servant (fonctionnaire de défense) of CNRS who conveys these recommendations to the Laboratory Directors. However, the latter use the university web and, therefore, must take the policy of the university site into account. On the grassroots, the exchanges between actors exist as it is the interest of each one of them to evolve in the same direction. However, it can be noted that the lack of partnership clearly defined as for as security is concerned makes the exchange depend depend on the goodwill of the persons.

Another actor of security at the national level is the Computer Emergency Response Team (CERT) Renater. Its role is to limit the number of unfriendly attacks through the distribution of warnings of security vulnerability to each RSSI. [2]

University level

In a university, the President represents the moral authority. To advise him in the field of information system security, he appoints a person in charge, the RSSI. The latter must imperatively agree with the highest university authority, and be supported by this authority. so that the actions undertaken may succeed.

This RSSI acts as an actual risk manager and defines the necessary structures which will enable him to set up the security procedures at every level. His range of intervention is very broad and often badly-known. If the securisation of the network and making the personnel aware of the problem seem natural enough, other points, just as primordial, are often overlooked such as the circulation of documents, telephone, telecopv, ... , the control of the movements of portables.

This person also coordinates the security audits, the intrusion tests, the test of' awareness to security. He is the one who must start the process of elaboration of security policy. On this point, his action is transversal : for instance, his advice must be sought when projects are being studied or worked out so as to ensure that the security of the university information systems is not modified or keeps the same level of securisation.

Yet, it must be noted that, because of his unique function in the university, the RSSI is often faced with a problem of administrative location which, in certain cases, can cause damage to his career. Another point that his been noted is the rather negative image the users have of this person. He is often considered as a military character, a spoil-sport. Fortunately, this bad image is gradually fading out thanks to information talks on his mission for the users. Another thing that bas been noted is that, in the majority of cases, this person responsible

for security is not sought for his advice when new projects are being established. This is mainly due to the tact that the goal must bc met as quickly as possible and very often at the expense of security. Finally it is necessary that the budget linked to security should be clearly identified and wholly managed by RSSI. This problem is often overlooked or partially dealt with because of the discharge of responsibility it implies. In spite of this difficult environment if the RSSI knows how to demonstrate the usefulness of his mission, and there exists a stray political will, then the obstacles will be overcome.

The fulfill his mission, the RSSI of the university of Poitiers relies on a network of security correspondents appointed by the persons responsible for each unit. Each security correspondent of each unit must be a member of the security cell led by the person responsible for security of the university. Indeed. it is necessary that this person should not be judge in his own case. He must succeed in keeping an objective eye on all the securisation elements. That is why he must coordinate the installations made by the correspondents but must not be the final actor of their implementation.

The security correspondent of each unit is the main element of our security chain. Indeed, he is responsible for most of the basic security job. He must know as perfectly as possible the environment of the systems he manages. He is the first to warn and keep aware the users. He implements the security policy defined by the university security officer. He is the link between the RSSI and the users. His proximity role is prominent in the system of prevention of risks. In case of emergency or if the security of the information systems is clearly imperiled, his action is well defined and can go as far as forbidding access to the machines, physically or through the network.

We did not forget to link to our system the user who is the first link of our "security" chain. Well informed and aware of the security problems he may face, he will be more careful in the daily use of information systems and more on his guard towards all suspicions behaviors.

2.2 The means

The security policy

The security policy of the information systems of the university of Poitiers has for its main function to establish the objectives, the procedures to bc followed, ..., the regulatory framework that controls the use of ail active means of information or telecommunication at the university of Poitiers. To work out such a document that records and gives the details of all the procedures is not easy. However, it is a necessity for it compels the security actors to pose concrete questions. The security policy of the university that has been written for two years has already undergone several modifications but bas never been validated by the board of trustees.

This general framework of the security objectives of the information systems that we have defined is working according to the following basic principles : availability, integrity, confidentiality, non repudiation. We are still a long way from an acceptable level of risk and the constant appearance of new services always gives us this impression of being late. Keeping ibis document up-to-date is particularly wearisorne.

The good use charter

The charter that bas been validated by the Board of Trustees defines the conditions of use and the rules of good use of the informations means of the university of Poitiers. This charter, which is displayed in the free access rooms, informs the users on the conditions of use of the information means, within the respect of laws and regulations.

So as to ensure that each user has taken notice of the charter, two measures are being set up. The first consists in having each person sign the good use charter when registering. The second one is a prevention screen containing all the charter that has to be validated by the user at each connection.

Les finances

Since 1998, a statement of expenses linked to the securisation of the university has been written. Following this statement, a specific security account bas been created and is partially managed by the person in charge of security. This situation is not simple on as daily basis and requires constant negotiations with the person who has a right of signature. This adds to the ambiguousness created by the unclear administrative position of the person in charge of security.

2.3 Conclusion

The administrative measures established since 1998 have permitted an important progress in the securisation of the university.

The positive points that can be stated are : the awareness at a national level of the security problems of the universities. the appointment of a person in charge of security, the creation of a network of correspondents close to the users, the creation of a budget specifically designed for security, the establishment of documents (good use charter, security policy) and of prevention screens defining the procedures and uses linked to information systems.

Several negative aspects could be improved : the status and administrative position of the person in charge of security as well as his image within the university, the relations between the correspondents and the person in charge (no hierarchical scale between them, the person in charge has to convince the users to adhere to a project), the integration of security to the projects that use new technologies. The support of the RSSI by a strong political will is an essential condition of succes.

3 Prévention and training

The training and prevention of the actors of securisation is an essential element in the strategy adopted by the university of Poitiers. Indeed, our administrative structure is based on a network of correspondents close to the users. A good working of this organization requires that the users should trust the security correspondent of their unit. This trust can only be acquired when the correspondent is able to answer the needs of the users. This

requires, on the part of the correspondent. a solid knowledge of his working tool. Aware of the prime stake represented by the competence of the personnel, the university has made a tremendous effort for the training of correspondents and persons in charge.

3.1 Training of RSSI

To be a person in charge of security requires numerous competences in various fields. Indeed, one must : possess a good general knowledge of information systems. have a solid competence in protocols and operating systems. study in depth the securisation techniques. be trained permanently on new technologies and, therefore, on new hacking techniques, be able to manage a team of hierarchically independent correspondents, be able to overcome an important stress, lead new projects, negotiate and manage a budget, ... To find a person who possesses A these competences is difficult. That is why one of the first measures taken at the university for training concerned the person in charge of security. Bringing his competences to the level required started by a general training period in the field of security for seven weeks at the Central Service of Information System Securitv (SCSSI). Since then, the person in charge bas been attending an average of three periods of training each year. When one reads the above list of competences required by this function and the training already, achieved, one must realize that there is still much to be done to reach file required level.

3.2 Training of the correspondents on site

Since 1999, the university bas chosen as a priority the training of the unit corespondents. It appears that a huge effort is to be made because of the "click-prone generation". One notes that the majority of correspondents has a lack of knowledge as far as protocol, network working and Unix are concerned.

An average of four theoretical training periods is achieved annually to increase the competence level. For better results, we apply to training managers from outside the university.

It is important to know the theory but what the user expects is practical knowledge. We soon realized the correspondents did not apply the information obtained through the lectures. After looking in vain for a financially affordable and adapted to our environment training , we decided we would create one from scratch. This training comprises five in-depth lectures on the protocols and 23 periods of practical work. These periods are very detailed and correspond to actual requirements in administration and server securisation. Some examples of practical training : installation and use of tcpwrapper, ssh, sftp, ... This applied training has created such an interest that the students have asked for the organization of new periods of practical work. Another very positive aspect of applied training periods is the exchanges, the mutual aid and a certain collusion that is being established between the correspondents. This phenomenon creates a work and solidarity dynamism.

3.3 Personnel training for the problems of prevention

The majority of the university personnel uses the information systems without having a clue about the security problems that can crop up. That is why we are preparing a

prevention training period dedicated to the development of awareness. A first experiment showed that the end user is on the lookout for something sensational. Indeed, a simple talk explaining a range of potential dangers and recommending a way of using the systems is no longer enough. The necessary use of the fantastic, which is due to the evolution of our society, passes by demonstrations of intrusion. This is the price to be paid to make the users aware of the possibilities of hacking.

3.4 Conclusion

A majority of personnels, actors at the security level, possess a knowledge at the "Window" level and know very little at the network and Unix level. Under such conditions, a theoretical and mainly practical training becomes a necessity if you do not want to annihilate the efforts at securisation. The creation of a practical training adapted to our needs permitted a gain of time and money.

Finally. the end user needs to see intrusions to understand that the information systems are vulnerable.

4 Technical aspects

The situation of the university of Poitiers in 1997, as far as security was concerned, could not be more catastrophic. Indeed, no filtering was protecting entry to the network and the stations of the network were found, for the great majority, on the same broadcast range, no security service was used, only some mixing boxes benefited from a securised access for authorized personnel, the servers and the active materials were not on an undulating electric line, the use of a common entry for several persons was common, certain accesses were done without identification or authentication procedures ...

Although the above list is far from exhaustive as there was no reflection on security, all the activities quoted eau be made more secured with time, money and a good coordination. But what is more difficult to change are habits. As there has not been any coordination for several years, a number of people have granted themselves privileges in the use of the network and have taken working habits that are not easy to change. For example, the census of services showed that. in 1998, 181 email servers were on use and, in some services, it was possible to find 8 or 9 email servers, or one for two users.

It was decided, on one hand, to make more secure the basic equipment of the outside sites of the university and to propose network services at a transversal level and, on the other hand, to improve the security of the composing units.

4.1 At the global level

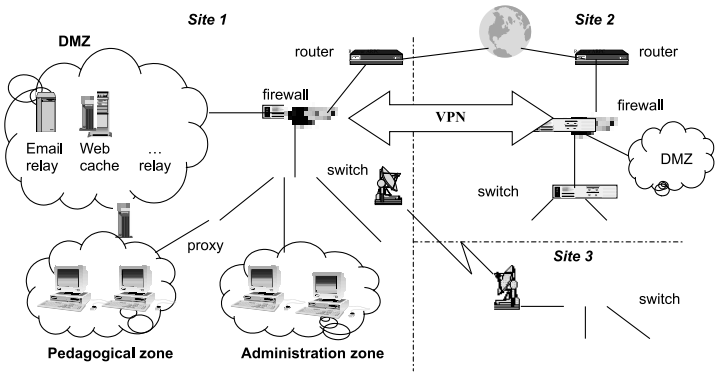
The first three actions achieved consisted in the positioning of a filter on the entrance router, a flow analysis and the segmentation of the network. If the flow writing takes only a few minutes and the flow analysis takes a few months, the segmentation required several years of work. The separation of the flows of pedagogy. administration and research by VLAN and ELAN required the modifying of the addressing plan and the renewing of the

commuters. We took advantage of complete remodeling of the basic equipment to connect several sites through 34 Mb/s hertzian links. It is important to underline that the security took advantage of the renewing of the network but that it is only one element among a group of reasons that brought about an improvement of the transit of information.

After this first series of changes. we have undertaken two basic projects. One consisted in proposing unified network services (mail, web, intranet, ...) for the whole of the university. For consulting the mail coming from outside the university, a service is proposed in securised web (https). The other is destined to ensure a better security of exchanges between the university sites and the dialogue with outside.

This last project was proposed around a firewall Netasq network. Each site is equipped with a bridge had positioned material that permits, coded exchanges through a VPN tunnel (Virtual Private Network). The various coding possibilities through the firewall do not change the performances [3] as the maximum output of the connection to Internet is 34 Mb/s. We also use the firewall to set up a public exchange zone called DMZ (Demilitarized Zone). Within this zone are positioned all the servers that will act as relays or service caches (smtp, web, ...).

Also to try and limit attempts at hacking, the pedagogical zones and free access rooms are made secure by proxies. Finally, intrusion sensors are positioned for a first level watch. These sensors are either of the commercial type, which permit the detection of 80 % of the hacking, or developed from free software and, in this case, used for pinpoint or targeted detection. The graph under shows all the actions implemented :



4.2 Unit level

At the unit level, the correspondents center their technical securisation efforts on the three following directions :

– Suppression on the stations of useless services

- Check-out of the flow and detection of hacking (Snort, . . .)
- Restriction of access to the network of the unit through filtering

4.3 Conclusion

The technical solutions that the university of Poitiers implements are on two levels. The first one is meant to prevent the hacking from outside and to ensure a vpn securised transit of the information between the different sites. The second level consists in installing on extremity stations only the services really needed by the users. A detection of the attempt at intruding and of the flow passing through the network enables to obtain markers for the security management of information systems.

5 Financial balance

Since they year 1998, a financial effort to the benefit of security has been made at the university. We are not going to give the detail of all the purchases but to visualize the outlines as for security expenses. Moreover, we have achieved an approximate evaluation, voluntarily underestimated, of the means in personnel necessary for the implementation of security.

	Common information budget	Security budget	Percentage
1998	10 075 135 F	105 194 F	1,04 %
1999	6 474 120 F	121 139 F	1,87 %
2000	9 265 846 F	1 483 797 F	16,01 %

It has to be noted that the year 2000 security budget include the firewall project generalized on all the sites. If we establish the financial ratio between the security budget and that of information technology on the period 1998-2000, one obtains 6.62 %. This results shows the awareness of the direction of the university to the security problems. However, this figure is largely overestimated because it takes only the budget of the two common information services into account. It is very difficult to know the exact amount used for information technology in all the university as the majority of the units is financially autonomous as far as information technology material purchase is concerned.

It is interesting to know the distribution by items of the security budget, without taking the year 2000 firewall project into account. In 2000, the 1 2134 297 Francs correspond only to the purchase of hardware.

	Training	Hardware and software	Travelling expenses	Percentage of training
1998	20 000 F	64 663 F	20 531 F	19,01 %
1999	117 013 F	0 F	4126 F	96,59 %
2000	171 095 F	72 230 F	6 175 F	68,57 %

One must note that, for the year 1998, the item "training" should be more important. Indeed, the person in charge of security has undergone a training period of 7 weeks in Paris and his training was paid by the Ministry, but for the travelling expenses. If you take this remark into account, one must notice the important effort in training of the security actors from the university.

The person in charge of security has been working full time on security for one year. In spite of this full time on security, the daily tasks (reading of the logs, checking of passwords, traffic analyses, technological wake, ...) are often put aside through lack of time, to the benefit of urgent tasks that, in most of the cases, have been put aside for quite a long time. This laborious job would require an additional person.

As an example, the following table enables to become aware of the time passed for the training periods and the generalized firewall project.

Firewall and DMZ installation; 800 hrs This concerns the installation and configuration of the 10 firewalls with the VPN tunnels, as well as the relays that can be found in the DMZ.

	heures	Commentaire
RSSI training	252 h	7 week training period at the SCSSI + 5 training periods of 3 days
Theoretical training	105 h	25 to 32 of the 45 correspondents take part in the training
Practical training	24 h	7 to 10 persons for a 24h session. Three levels of practical work are provided.
Preparation for practical work	300 h	The préparation entails the conception of practical work supports, the setting up of the room for a 24 hour session. This preparation is valid for the first session. The second one requires only the preparation of the room.
Administrative preparation of the firewall project	1200 h	Under this generic term is grouped all that concerns the tender for contract.
Firewall and DMZ installation	800 h	This concerns the installation and configuration of the 10 firewalls with the VPN tunnels, as well as the relays that can be found in the DMZ

The conclusion is that the university of Poitiers makes an important effort for the training of personnel as far as securisation is concerned, as it represents the bulk of the budget. In fact, the theoretical training represents most of the training budget. Indeed, numerous training periods are offered at affordable prices (22 000 FF for two days) but in the majority of cases the technical content is very superficial. To find a training period of a very good level, one must pay twice that price. The practical training is undertaken by the persons in charge of the university, which offers an appreciable financial benefit as it is assessed that a practical training with renewal of lectures and about 10 practical activities will cost 10 000 francs for each trainee. The investment for the realisation of practical work which does not seem paying as far as time is concerned will certainly become so on the financial level. Moreover, one must not underestimate the dynamic aspect of group work.

6 Conclusion

The implementation of the security of information systems within the university of Poitiers bas taken a decisive turn when the leaders of the university have become aware of what was at stake. This turned into the setting up of an administrative structure close to the users when a security correspondent was appointed in each unit. Very soon, limits appeared at

the administrative level (budget, positioning of the RSSI, ...) as well as at the users' level (harmonization of the network services, securisation of the stations, ...).

If the financial problems can be gradually solved, the recognition of an actual status for RSSI is quite another proposition.

At the grassroots, the priority bas been given to the training of the security correspondents of each unit and that at two levels. A theoretical training bas been undertaken by external people. Then a practical training bas been undertaken within the university. based on the securisation needs of the university.

Another grassroots problem is the development of awareness among the personnel who no longer believe in fine speeches. If is compulsory in such a case to show clearly the vulnerable points and to carry out intrusion demonstrations.

On the technical level, a project of securisation of all the sites of the university was born. It consists in a filtering at the entrance with an exchange zone between the external and internal worlds. For the transit of information between each site. It is carried out through coded tunnels. The securisation of flows of the pedagogical, administrative and research communities uses the technique of separation between VLAN and ELAN. Finally, each unit must reduce to the minimum the services open on stations and can filter the entrance to its network.

On the financial point of views, the effort made by the University is important. However, the financial management puts certain problems.

The security of information systems is at its very beginning and already shows an important delay. With the coming of new technologies and new services, the prospects for the future as far as the workload is concerned seem promising. Without a real political will of integrating in each project the security aspect and of giving oneself the necessary financial and human means, the hackers have their heydays before them.

In spite of strong pressures and an important inertia due to the structures, experience shows that with a lot of energy and a strong political will it is possible to make progress.

References

[1] Jean-Paul Leguigner: Organisation sécurité de l'Enseignement Supérieur. http://www.cru.fr/securite/1divers-ps/organisation.gif

[2] David Crochemore: Le rôle et l'experience du Cert-Renater. Actes JRES 99 P 249

[3] Society Netasq: Technical manual.