FEATURE

Belgian E-Security: the Start of a European Initiative?

Eddy Willems
Data Alert International, Belgium

Despite my busy schedule of consultancy work, giving presentations, analysing viruses and dealing with *EICAR* matters (as EICAR Director Information and Press), another job was thrown at me a little over two years ago.

After the VBS/LoveLetter outbreak, the Belgian Government felt that something needed to be done to protect the Belgian people and businesses against such attacks. The Belgian Minister for Telecommunications, Rik Daems, reacted promptly to the virus, introducing immediate countermeasures. After a day of brainstorming he came up with the idea of creating a website on which anyone could find virus alerts and information about other security issues.

But this was only part of the plan. The goal was to alert the Belgian people before anything else was published on the Internet and *before* a new outbreak could begin. An attractive goal and an interesting new approach – that was the idea, anyway.

In order to run the website and its associated alarm system, the minister's cabinet decided to set up a security team of relevant experts. Thus, on 5 May 2000, the e-Security team of BIPT (Belgian Institute of Postal services and Telecommunications) was established.

e-Security Team

Despite the fact that Belgium does not boast a large number of anti-virus or IT security experts, the security team was formed after just two days. Within the e-Security team there are three groups: the minister's cabinet, external specialists and the advisory team, also called external analysts. The external specialists – a group of about 30 people – comprise individuals from ISPs, some TV stations, several large corporations and two security companies.

So, where are the security experts? My employer, *Data Alert International*, volunteered me as the only anti-virus expert within the advisory team. The other security company involved in the project elected a general security expert. Other members of the advisory team include a representative from the Federal Crime Unit (Federal Police) and some members of BIPT itself. The advisory team consists of five people.

Alerting Procedure

There are eight steps involved in the alerting procedure:

1. An alarm may be initiated by members of the population (by contacting their ISP) or by the team of external specialists.
2. The call point of the e-Security team screens the alarm and determines whether it should be continued.
3. The staff of the Minister of Telecommunications are warned and the external analysts (the advisory team) are contacted by email, SMS or by telephone.
4. The members of the advisory team forward an analysis of the threat to the e-Security team, and a formal advisory is drawn up.
5. The advisory is forwarded to the staff of the Minister of Telecommunications.
6. The Minister of Telecommunications decides what action should be taken. If a press conference is appropriate, the staff of the Minister start the procedure.
7. Members of the e-Security team add information to the BIPT website: the problem, the dangers and what to do if your computer is infected.
8. The press and other media become involved. This includes the RDS system, in which programmes on the radio are interrupted for a virus announcement. Also, specially designed anti-virus banners may be added within minutes at some ISP portals (see below).

There is a timeframe of two hours for this list of actions. In my opinion, the most important part is that it is possible to use other media (i.e. radio and television) to warn the population of the potential problems. A national warning using such different kinds of media has an incredibly large impact. Can you imagine how it feels to be a system administrator driving to work and hearing between traffic alerts that ‘AnnaKournikova’ is in an outbreak situation?

Problems

Like every new system, a number of teething problems were encountered with the procedures.

For instance, at first, email was used to contact the advisory team and with that email was an attachment in the form of a *Word* document in .DOC format, containing details of the problematic new virus, worm, Trojan or hoax. Imagine how I felt when I saw the first email they sent to me! Had anyone in the chain not had adequate protection they could have sent a virus round within the email itself! Immediately, I asked that some other distribution method be used.

On receipt of the information the members of the advisory team must respond within one hour. If the process runs according to plan, an article can be published on the BIPT web page within that time, and a national security alert can be prepared – nice, if it works.

However, the details of the first message I saw were rather disappointing; it seemed that some members of the team could not tell the difference between a hoax and a virus. Neither could they distinguish whether something was of low or high importance. In fact, on one occasion I was just in time to prevent a warning being issued for a non-existent virus!

More recently, some of the alerts posted on the website have been superfluous and they vary, depending on who is responsible for editing the site at that time.

A number of links to a selection AV developer websites have been added to the site. Would it not be more helpful to point to all AV websites and select only genuine alerts? (I realise that the definition of a genuine alert is always a troublesome issue – which is something every anti-virus developer will appreciate.)

At those times when I am out of contact with the e-Security Team, the members tend to gather information about ‘problematic’ viruses direct from an anti-virus developers’ websites. The information is then consolidated and added to the official BIPT website even if it has not been verified. I am afraid I would say that, at such times, the system certainly does not act as an early warning.

Do not misunderstand me. I believe that the original concept of this early warning system has great potential – and the system has worked very well in the past. I have outlined the problems as I see them to other members of the team and improvements are being made already.

It occurs to me that the BIPT e-Security team is, in fact, more of a political game than it appears. Nevertheless, the idea behind the project should be honoured, because it is a responsive and a helpful one.

The question remains, however, could a new virus or worm with all the latest and perhaps unknown spreading techniques be quicker than this system? I think the answer is inevitable: yes, but the e-Security team can act within a defined timeframe to inform a very large number of pc-users about a potentially serious security problem.

There have been more than 100 alerts over the past two years; more than 60 of these were added to the website. Of those 60 about 20 were translated into the advisory procedure. About five alarms were given using the RDS radio system or some other notification system.

Over the Borders … the Euro Way?

The Belgian Government elaborated on their experience and chose to implement a permanent structure for an early warning system. During the Belgian Presidency of the European Union, Belgium prioritized information and network security, resulting in a resolution which was adopted at the Telecommunication Council of 6 December 2001. This resolution includes detailed measures and initiatives to be conducted by both the member states and the European Commission.

But of course this is not enough. Belgium is not an island in cyberspace and viruses don't have a sense for geographical borders. It's clear that no truly effective warning system can exist without being global, without having connections with other countries and other continents.

To that end, in September 2001, the Belgian Minister for Telecommunications signed a Memorandum of Understanding with his Singaporean counterpart. This is a formal agreement on the sharing of knowhow and information between the countries and is the framework within which joint actions can be taken. Since Singapore lies in another time zone, a virus outbreak could hit there first, or vice versa. We hope that the people of Belgium will be prepared in this situation.

Of course, involving the whole of Europe in such a project is easier said than done. A lot of political negotiation is necessary at this stage, which is why the Belgian Ministry has already started to make contact with closely related Ministries from countries like The Netherlands and Luxembourg.

The goal is to start as quickly as possible with an evolution of the e-Security Team within the BeNeLux countries to see whether it is possible to have a working solution over the borders. This could be the way to a new European e-Security platform; EICAR (European Institute for Computer Anti-Virus Research) has offered to provide advice and other input to such a system.

Of course, it may not be straightforward to realize an integrated European system like this – for example, will every 'expert' work on a voluntary basis? In Belgium it is done in this way, which is quite unique.

Bullet-Proof System

Despite my busy schedule it seems that I always have several channels open so that I can be contacted when my help is really needed.

Oops! Another SMS message from BIPT arrived on my mobile phone as I was finishing this article. By coincidence (as part of one of my consultancy jobs) I'm writing this article very close to the area where shootings between the Palestinians and Israelis are going on. Even here, the system of the Belgian e-Security Team carries on working, just as long as my mobile phone keeps working …

The BIPT website can be found at http://www.bipt.be/, where security warnings are posted in Dutch and French, Belgium's national languages.