Cert-IST annual review for 2013 regarding flaws and attacks

1) Introduction

Each year, the Cert-IST makes a review of the previous year. The goal of this document is to sum up the major events of the 2013 year, in order to highlight the trends regarding attacks and threats, and to help readers to better protect their assets.

First, we present the most significant events for 2013 (in chapter 2). This includes the Snowden affair, the (low level) hardware attacks and the raise of offensive security. These 3 interdependent topics are the most important ones when looking at the new threats companies should consider.

Secondly, we present the main vulnerabilities and attacks seen in 2013 (in chapter3), based on the daily threat and vulnerability analysis performed by Cert-IST. This includes a summary of the Cert-IST production for 2013 (with figures on the number of advisories or alerts published), a quick review of the Alerts and Potential Danger notices, and finally a focus on some vulnerabilities and attacks.

We finally analyze how to protect companies (in chapter 4) against the main threat categories (cyber-espionage and opportunistic attacks) and the typical targets they take at aim (users, user's computer, web sites and Scada systems).

In the conclusion (in chapter 5) we drawn a global picture for the cyber-threat current situation and the challenges the companies must face with.

➢ About Cert-IST

The Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam - **I**ndustrie, **S**ervices et **T**ertiaire) is a center for alert and reaction to computer attacks and cyber threats dedicated to companies. Established in 1999, it analyzes daily the new vulnerabilities discovered, assesses their severity and identifies the possible protective measures. In the event of a security incident impacting one of its members, the Cert-IST can assist in the investigation and the resolution of this incident and allow a fast return to secure operational state.

2) The most significant events for 2013

2.1 The Snowden Affair changes the perception for « cyber-espionage » risk

The Edward Snowden revelations about surveillance programs of the NSA are the most significant event of 2013. Following is the timeline for these revelations:

- June: first Snowden revelation. It concerns the existence of the **PRISM program** that allows the NSA to access to subscriber data in major American Service Providers (Google, Facebook, Yahoo, etc ...) and Telcos (Verizon).
- August: revelation about the **Xkeyscore** program. This shows that NSA (and other states such as UK) performs massive surveillance over IP networks using a large set of eavesdropping sites located all around the world. From the captured network traffic, they can then reconstruct conversations of Internet users (e.g. Facebook or emails exchanges).
- September: revelation about various **programs aiming at breaking or circumvent encryption** of data communications. This includes for example the "Bullrun" program or the voluntary weakening by NIST of the cryptographic algorithm Dual_EC_DRBG.
- December: publication of **the NSA ANT catalog**. This catalog, which seems to date back from 2008, lists around 50 tools made available to the American secret services to achieve offensive operations. For example, it includes backdoors for Cisco, Huawei and Juniper network equipments.

All together, these revelations highlight the fact that NSA (and probably also equivalent services in other countries) has been intensively using cyber-weapons for several years and that expertise in this field is more advanced than what we estimated so far.

None of the elements brought by Snowden revelations is actually new, but the underlying threats were up to now considered as theoretical or hypothetical. The Snowden affair shows that in the last ten years, governments have been actively working to develop an offensive cyber-arsenal. This arsenal actually exists (at least since 2008), it is used in real attacks, and the number of attacks seen is soaring. There is every reason to believe that these offensive techniques are developed by all countries, and not only by the United States.

The "Snowden" event is similar to the discovery of "Stuxnet" in 2010: it changes a theoretical risk into a demonstrated fact.

The consequences are of several kinds:

- For organizations that need to protect themselves against governmental attacks (e.g. NSA attacks), it is necessary to reassess the effectiveness of the measures already in place. And this is a difficult task because NSA attack capabilities, as shown by the Snowden affair, are very advanced. The physical isolation of sensitive projects seems here a requirement, but it clearly has a cost and limitations (because complete isolation is impossible).
- Other organizations should also ask the same kind of questions, but with a lower level of requirement. They should for example ensure that all outgoing communications are encrypted or that the infection of a single workstation does not give access to all the IT system of the company. It should also be aware that sophisticated attacks, that today mainly targets strategic industries and are performed by a limited set of attackers, will democratize and will be more broadly used in a near future.

More anecdotally, the NSA should also review its internal organization to understand how a leak of this magnitude could have happen. But apparently this task is already well engaged.

2.2 Hardware attacks are becoming a real threat

For several years, publications on low-level attacks have multiplied. For example:

- SMM attacks (System Management Mode) against Intel processors that lead to BIOS level attacks (See this presentation at SSTIC 2009 conference in French or this English translation).
- Attack against network card firmware (for example, see this CansSecWest 2010 presentation).
- DMA (Direct Memory Access) attacks that allow an extension card plugged to the computer board bus to get access to the central memory (for example, see this presentation in French from the SSTIC 2011 conference and this English translation).
- Etc.

In 2013, several new publications were also published in that field:

- An experiment to implement a backdoor in hard disk firmware (see this publication from Eurecom in December 2013).
- The IPMI and BMC vulnerabilities (see this Cert-IST article in September 2013).
- The BadBIOS malware (see this article from ErrataSec in October 2013). Even if this malware does not actually exists (up to now), it aggregates a set of advanced features which are all theoretically possible.

All these publications are research works or prototypes. On the other hands, the secret ANT catalog of the NSA (that we already mentioned in the previous chapter), that was discovered in late 2013, shows that the NSA already has operational hardware backdoors since 2008. This catalog includes:

- Backdoors for hard disk firmware,
- Backdoors at BIOS level,
- Backdoors embedded in PCI cards.

If the ANT catalog is genuine (but there no element that could make think it is not), the risk of hardware attacks is then no more theoretical.

> The evolution of research shows that for several years the hardware level attacks are possible (BIOS backdoor, PCI attacks …). In 2013 this threat has crossed over a significant step. In particular, the secret catalog of the NSA, which was revealed in late 2013, shows that since 2008 the NSA has access to this kind of attack tools. And it is probably the same for other governments.

2.3 Offensive security is increasingly present

In recent years, the offensive security has gradually emerged in the IT security landscape. And 2013 marks an important step in this evolution with the following events:

- The offensive cyber-security has been acknowledged by French government as being a integral part of the National Defense (see the French "Livre blanc" released in April and the "Loi de Programmation Militaire" in November). Similar initiatives exist as well in other countries.
- The research and selling of 0-day vulnerabilities (and associated exploit code), as practiced for example by the French company Vupen, are now widely accepted.

This trend is understandable. This is the result of the multiple attacks against national or private interests seen during these last years. For a country, it is now unimaginable to not master cyber security topics, on defensive but also on offensive aspects.

However, it is clear that the offensive security should remain a prerogative of governments and has no place at business level. But, the rise of interest on these topics will also probably raise vocations, and there is a risk that more and more companies will offer offensive services for all. Although this does not seem a priority for the current governments, a strict and precise legislation should be defined to control this type of activity. It may be noted on this aspect that in late 2013, the French government has put in place restrictions on the export of eavesdropping systems for IP networks (see this Numerama article in French).

3) Vulnerabilities and attacks seen in 2013

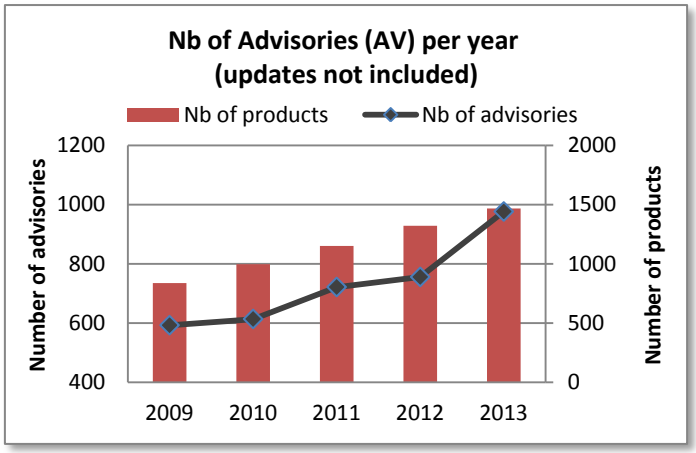
3.1 Figures about Cert-IST 2013 production

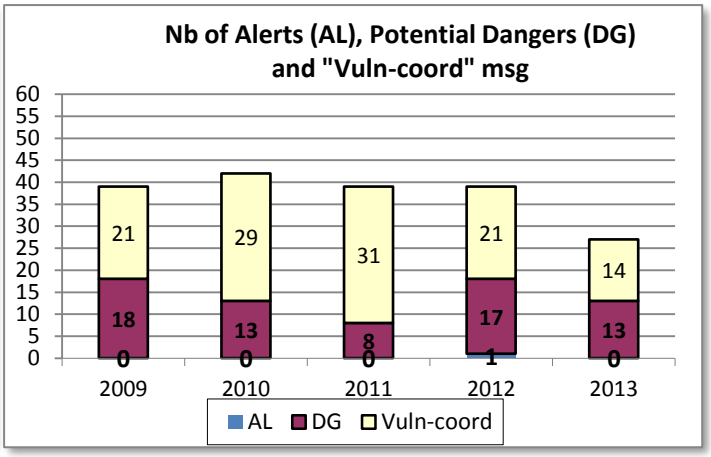
3.1.1 Daily monitoring on vulnerabilities and threats

As part of its watch activity on vulnerabilities and threats, the Cert-IST continuously monitors the different information sources about vulnerabilities (including official announces from constructors/providers, security blogs, mailing-lists, private exchanges between CERT, etc.) in order to be aware of new vulnerabilities. This information is analyzed daily to provide our members with a sorted, qualified and prioritized set of information. The Cert-IST therefore produces different types of productions:

- **Security Advisories**: they describe newly discovered vulnerabilities in the products followed by the Cert-IST. These advisories are continuously enhanced with minor or major updates. These latter typically occurs when an attack programs (aka "exploits") are released.
- **Alerts, Potential Dangers, and "Vuln-coord" messages:** Alerts from the Cert-IST are used for major threats which require an urgent treatment. Sending an alert is a rare event: for instance, the Cert-IST released in 2012 one alert for the Java JRE vulnerabilities. Potential Dangers describe significant threats, which are not imminent yet (or having a limited impact) but for which the Cert-IST recommends specific protection measures. Finally, "Vuln-coord" messages are coordination information which draws attention on particular threats which have a lower severity. These three complementary categories are focused on attack risks, whereas Security Advisories systematically identify all known vulnerability (whatever is the probability that the vulnerability is used in a real attack).

The graphs below show the production of Cert-IST over past years.





Therefore, during 2013, the Cert-IST published:

- **976 security advisories** continuously followed during the year with 2580 minor updates and 94 major updates. The number of advisories is constantly increasing since several years (see the curve above), and this phenomenon has greatly increased in 2013. This continuous increase shows that vulnerability discovery is a phenomenon which does not dry up: from year to year, vulnerabilities are found in products which constitute the company's I.T. Holding the security level then requires a regular application of the security patches on these products. On

the 31st of December 2013, Cert-IST follows vulnerabilities concerning 1466 products and 11 778 product versions.

- **No Alert, 13 Potential Dangers and 14 « Vuln-Coord » messages.** We present theses 2013 publications in the chapter 3.2 below.

3.1.2 Technological watch

Besides its vulnerability watch, the Cert-IST also releases technology watch reports:

- A daily media watch report which lists the most interesting articles found on the Internet over a sample of French and English-speaking websites about security.
- A monthly SCADA watch report presents a synthesis of the news about industrial control systems security.
- A monthly general report gives a synthesis of the month news (in terms of advisories and attacks) and deals with current subjects in articles written by the Cert-IST.

3.2 Alerts and Potential Dangers released by Cert-IST

In 2013, Cert-IST did not release any Alert. This type of publication is indeed reserved for the most severe threats and the latest Cert-IST Alert is still the one we issued in 2012 about attacks against Java JRE.

However, we have issued 13 Potential Dangers (DG), for threats less severe than Alerts. These 2013 DG break down as follow:

- 6 DG are about **Windows**, including 4 about **Internet Explorer,**
- 4 DG are about **Java JRE,**
- 1 DG for **Adobe Reader,**
- 1 DG for the **CryptoLocker** malware,
- 1 DG for the video conference system **Cisco TelePresence.**

12 of these 13 DG are for attacks targeting user's workstations. This year again, workstations reminds the asset the most exposed to attacks. Workstation is actually a target for both cyber-criminals (who try to infect individuals) and cyber-spies (who try to infiltrate companies).

Windows (and Internet Explorer) remains prime targets. A lot of the attacks seen in 2013 were targeting Internet Explorer 8 and Windows XP. These environments were still very present within companies in 2013, and the targeted attacks (which specifically aim at given companies) were consequently mainly focused against these environments.

We further comment the **Java** and **CryptoLocker** threats in the « Zoom » chapter below.

About the DG on **Cisco TelePresence System,** the issue was a default password that could have been used to take the full control of vulnerable systems.

3.3 Zoom on a few flaws and attacks

We describe here the vulnerabilities and the attacks which seem the most important to us. For those which directly concern companies and required immediate actions, we released Potential Danger notices. The other one were generally treated via articles published in our Cert-IST monthly bulletin.

- **Java vulnerabilities (from January to April 2013)**

We identified Java as the most vulnerable (therefore most dangerous) component in our annual review for 2012, and Java vulnerabilities remained very present in 2013, especially during H1. From January to April 2013:

- Oracle successively published 5 updates (whereas their annual calendar only planned 2 updates) to fix newly discovered vulnerabilities.
- We published 4 Potential Dangers to warn our members of attacks using Java vulnerabilities.

From January to April, Oracle took part in a race which seemed endless, as new vulnerabilities were discovered just a few days after the release of a fix for the previous ones. The situation calmed down at the end of April, and Oracle then only released their planned quarterly fixes. It is hard to tell if this improvement means that Java is now a secure component. It is indeed possible that vulnerability researchers (such as the Security Exploration company, who was very active on this subject) changed their targets and (temporarily?) abandoned vulnerability research in Java.

Java remains a very sensitive component, and it is the main cause of infections during web browsing. This component must be kept up-to-date to avoid these attacks.

- **Vulnerabilities in the UPnP protocol (January 2013)**

In January 2013, the Rapid7 company (which develops the MetaSploit product) released a study about the dangers related to the UPnP protocol:

- A lot of network elements are misconfigured (17.5 millions!) and allow access to UPnP services from the Internet, whereas these services should only be accessible internally.
- Major vulnerabilities exist in the most popular implementations of the UPnP protocol (**libupnp** and **MiniUPNP**).

UPnP is known for a while as a cause of security issues. This protocol is designed for residential equipments (DSL set-up boxes, multimedia servers) and should not be very present in the business environment. Yet a lot of small network equipment embeds UPnP, such as IP cameras. It is therefore very widespread: Rapid7 identified in their study that about 6900 products embedding a vulnerable UPnP stack. Furthermore, the correction of vulnerabilities on this kind of equipment is most of the times impossible because the vendor did not implement any update mechanism.

Note: These vulnerabilities were described in February 2013, in an article of our monthly bulletin.

- **DDoS attack against SpamHaus (March 2013)**

Spamhaus (an organization which fights spam) faced in March 2013 a Denial of Service attack which set records, with traffic peaks of 300 Gbits/s. The attack was performed using the « DNS amplification » technique: the attacker sends traffic towards misconfigured DNS servers which then overload the target aimed by the attacker with reply messages. At least 2 people were arrested (in Spain and in the UK) following the case opened after these events.

Note: This attack was described in an article included in our monthly bulletin of April 2013.

- **Vulnerabilities in IPMI/BMC (August 2013)**

Major vulnerabilities in the IPMI (Intelligent Platform Management Interface) and BMC (Baseboard Management Controller) were revealed in 2013: first by Dan Farmer (in early 2013), then by Rapid7 and the University of Michigan at the Usenix-Woot'13 conference (during the summer of 2013).

IPMI is a low-level protocol which allows to remotely administrate servers. It is very widespread in business environments and is known under several commercial names: HP **iLo**, Dell **iDrac**, Oracle/SUN **iLOM**, Lenovo/IBM **IMM**, etc.

As far as we know, it was the first time that a security study was conducted about this technology and (as we could expect in such a case) several major defaults were found, which allow to remotely takeover the equipments.

Note: These vulnerabilities were described in an article included in our monthly bulletin of September 2013.

- **Cryptolocker attacks (October 2013)**

CryptoLocker is a "ransomware" which enciphers files (documents, photos, etc.) on the infected workstation, and then claims for a ransom to get the files back. "Ransomware" viruses are not new, but "CryptoLocker" largely spread from October 2013 (via booby-trapped email campaigns) and causes an important data loss on the infected workstations (the cryptosystem is strong and only the payment allows to get the files back).

Note: Cert-IST released a Potential Danger to warn our members about the threat caused by the « CryptoLocker » virus.

- **Adobe attack and source code theft (October 2013)**

In October 2013, Adobe announced they faced a major attack, with a theft of 40 GB of source code of their products, and a very large amount of customer data (data such as credit card numbers and credentials). Although they were stored in their hash form, these data were spread on the Internet and malicious people can now attempt to decrypt them. Initially 2.9 million of credentials were supposed to be disclosed, but finally, it would be around 150 million accounts.

4) How to protect companies

There exist today 4 big categories of attackers: the amateurs, the hacktivists, the cyber-criminals and the cyber-spies. For the business, the main attacks which result of them are of 3 types:

- Advanced Persistent Threats (APT), which are mainly conducted by cyber-spies,
- Opportunistic attacks, which are led by hacktivists,
- Attacks aiming the industrial systems (SCADA).

In this chapter, we analyze these different classes of attacks and the means to protect from them.

4.1 Advanced Persistent Threats (APT)

The scenario of such attacks is well-known and was described in our annual review of 2011 :

- Infect a first workstation in the company and set up a backdoor allowing to remotely act on the computer.
- Remain invisible and survive the longest possible time on the infected system.
- Explore its environment and progress in the company by infecting new systems until the target is reached.
- Collect sensible data and exfiltrate them, or perform sabotage actions.

In this scenario, the attacker must first settle in the company by compromising a first internal workstation. To achieve this first step, he will successively try 3 vectors:

- **Social engineering,** to convince the user to open an attachment or visit a booby-trapped website.
- **Workstation vulnerability**: for instance PDF, Java or Internet Explorer flaws.
- **0-day attack** if previous methods failed and the attacker considers the target as very important.

Companies exposed to international competition should not wonder if they will be affected one day by an APT, but should rather wonder when this will happen. They should especially prepare to this event by limiting its potential impact and developing their detection and reaction capability to this type of incident.

To improve its defenses, companies must address each of these vectors:

- **Inform users** about the risk of social engineering attacks, teach them on how to recognize and treat them. And inform internal support as soon as possible when such an attack has succeeded.
- **Maintain the workstations up-to-date** from a security point of view. This applies to operating systems, but also to third party applications such as Adobe Reader or Java.
- **Include the 0-day risk** in the threat management processes of the company.

As we explained it in our annual review of 2012, the risk of a 0-day attack must not be neglected. Experienced attackers have an easy access to 0-days. They can for instance buy them from companies specialized in vulnerability research. It is therefore necessary to integrate the 0-day risk in the threat management processes of the company. This implies to consider as a certain fact, that one day, an enterprise workstation or server will be the victim of a successful attack.

Beyond the workstation protection, the fight against APTs implies broader actions:

- Adapt the architecture to limit the impact of a successful attack,
- Set up an active monitoring in the company, via a structure responsible for security supervision.
- Define a reaction procedure in case of an incident specifying how to behave and which people to involve.

4.2 Opportunistic attacks

Opportunistic attacks, such as those launched by hacktivists, aim at easy targets (the term "low-hanging fruits" is often used for these targets). Traditionally, these are poorly protected websites. In 2013, we also noticed new attacks vectors which aimed, for instance, corporate Twitter accounts.

- **Poorly protected websites**

Corporate websites are the number one targets for hacktivists' attacks. Their resistance to denial-of-service attacks, along with research for trivial flaws, is systematically performed once an attack campaign is considered.

Most of the times, trivial flaws do not exist when the website is put in production for the first time. However, they appear with the time passing because servers are not kept up-to-date by applying the security patches published by vendors. After 3 years without any security patch, the security condition of the website largely degraded as vulnerabilities were discovered in the framework used by the website (Joomla, Worpress, etc.). It is then trivial for the attacker to use these vulnerabilities to take control of the vulnerable web sites.

As for workstations (cf. § 4.1) regular updates of websites by applying the latest security patches are essential to maintain their security level.

- **Attacks on badly protected Twitter accounts**

In 2013, hacktivists found new attack vectors which exploit the human link of the chain. For instance, the SEA (Syrian Electronic Army – an hacktivist group which sides with Bashar Al-Assad) managed, thanks to phishing attacks, to steal:

- **Corporate Twitter accounts**. In April, the Associated Press Twitter account was hijacked and attackers used it to spread fake news (such as explosions at the White House) which induced a short decrease of the stock exchange markets. The same kind of attack also happened to the newspapers The Guardian and New York Post.
- **Management accounts in DNS infrastructures**. In August, the SEA managed to steal the account of an Australian domain reseller (the "MelbourneIT" registrar). This allowed the SEA to alter DNS records of several well-known domain names, such as **Twitter**, and the **New York Times**, and to alter their operation.

These are relatively unsophisticated attacks, based on social engineering, but we see that well-known targets can be victims of such attacks.
It is difficult to protect against all types of attacks. However, it is important to keep informed about new attacks vector in order to take the right measures as soon as possible to be protected:

- Inform Public Relation teams of possible attacks against the corporate Twitter and Facebook accounts, and help them to define protection rules to avoid these elementary attacks.
- Ensure that domain names providers are aware of attacks which affected their peers and check that the adequate protection measures were taken.

The consequences of such compromises are often spectacular (even if the hijackings are quickly discovered and incidents quickly resolved) and can be compared, in terms of impacts, to defacements of corporate websites home pages.

These attacks essentially exploit the human link: the attacker sends phishing emails to a set of targets (for instance Public Relation people, or domain name registration services) and manages to steal the password of some accounts. If they are lucky, they can then get access to famous accounts.

4.3 Attacks targeting industrial systems (SCADA)

Since 2010 and the discovery of the Stuxnet malware, which aimed the Iranian nuclear centrifuges, the risk of attacks on industrial systems became a major concern.

Since then, indicators show that the threat is progressing:

- In 2011, the number of flows released about SCADA systems explodes and reaches a 500% increase. SCADA vulnerability kits appeared. This is most of the times trivial flaws discovered by IT security specialists whom are not specialized in SCADA systems.
- In 2012, vulnerability research became more rigorous as specialists of the SCADA world started to actively look for flaws.
- In 2013, the number of released vulnerabilities decreased, but most of them were major flaws. For instance, “generic” vulnerabilities are discovered (as in the DNP3 protocol).

Trend-Micro released in 2013 a study which shows that when a SCADA system is connected to the Internet, then this system is attacked by hackers which specially look for this kind of equipment: see this article about the Trend-Micro presentation at BlackHat 2013 about SCADA Honeypot for further details.

As we highlighted it in our annual review of 2012: Industrial security is a field where the cyber attack threat is increasing and the security level of some installations is not satisfactory yet. This situation is worrying.

Governments are aware of this situation and are actively working on these topics. In France, significant progress was done in 2013 with the creation of a workgroup and the release in January 2014 of several hardening guides.

SCADA systems hardening remains a major priority and a strategic challenge.

5) Conclusions

During the last years, threats targeting the companies' information systems increased and got harder:

- 2010: the Stuxnet attack showed that **SCADA systems** are prime targets and that it is essential to actively protect them.
- 2011: **Advanced Persistent Threats** aiming at companies (mainly for cyber-espionnage goals) have multiplied and became a major concern. **Hacktivism** also appeared and demonstrated that opportunistic and not very sophisticated attacks can have a significant impact on the company image.
- 2012: **The multiplication of 0-day attacks** showed that no system can be immune to a successful attack and that information systems must be designed by taking into account the fact that they will be compromised someday.
- 2013: **the Snowden affair** shows that several groups (state supported groups or specialized in state-level attacks) developed **a great arsenal of attack, way more developed than what we thought until then.**

In parallel, the evolution of the society increased everyone's dependency to computers and systems interconnectivity. And there is an increased demand for a bigger connectivity and opening in companies (Cloud, BYOD, etc.).

The CISO is facing a complex situation. And to inform project owners or to take appropriate decisions they must know precisely what are the risks. The Cert-IST, via its technological watch activity and reports, gives them an enhanced vision of the threat. And from our point of view, this threat is increasing. Our role is also to remind that the proven security models are those which rely on the strict application of traditional security in depth principles (platform hardening, application of security patches, network segmentation, privilege limitation, etc.). The « 20 Critical Security Controls For Effective Cyber-Defense » guide released in the USA or the « Guide de l'hygiène informatique » released in France by the "ANSSI" in January 2013 clearly go in this way.

We think that the hardening actions must especially focus on the following topics:

- Hardening of industrial systems (SCADA).
- Informing users about the known attack schemes (especially social engineering attacks) and the right behavior to have when an attack attempt occurs.
- Maintaining the security level of IT systems by applying security patches, in particular on systems directly exposed to attacks (ex: workstations or web servers)
- Considering that the compromise of a workstation or a server is a possible event, mainly because of the 0-day risk.

To treat this last point, the following actions are essential:

- Adapt the architecture to limit the impact in case of a successful attack.
- Set up an active security monitoring within the company, via a structure responsible of the security supervision.
- Develop reaction procedures in case of intrusion and have the attacks analyzed by a specialized team.

End of the Document