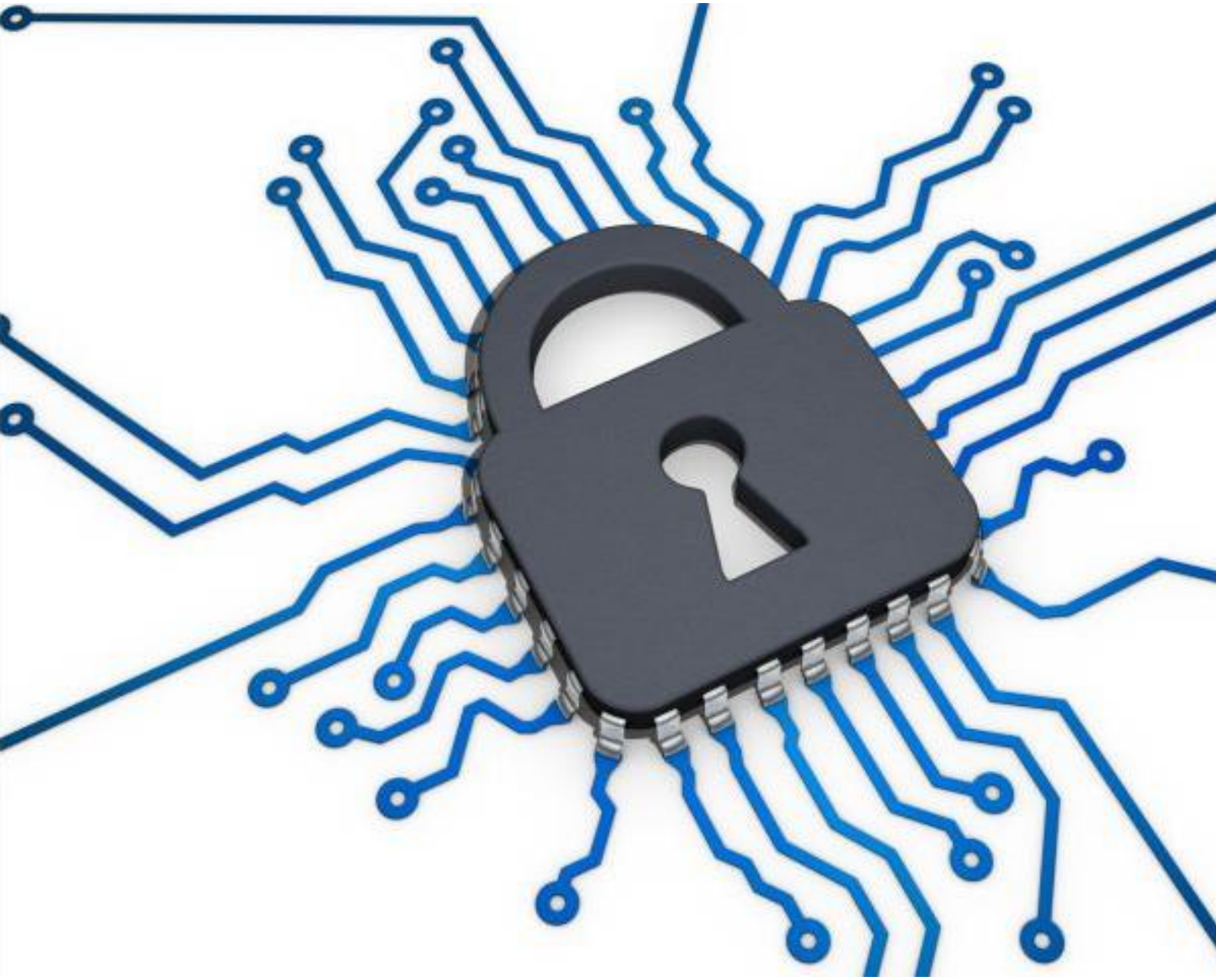

CYBERSECURITY IN THE ENERGY SECTOR:

An Introduction

Carlos Alberto Serrano Redondo

INTRODUCTION

The energy sector is globally recognized as an industry of special importance to the National Security since it preserves basic rights, freedoms, the social welfare system for all citizens and it ensures the provision of essential services and resources as well. The generation and distribution of energy is a crosscutting activity that affects the entire functioning of a country offering competitive advantages within global markets. Operators of these services and companies dedicated to developing solutions for their own protection believe that the greatest risk comes from the side of information security, because that is precisely the most vulnerable aspect of infrastructures.

In this sense, all damages to computer systems security in the energy sector may affect negatively on the economic and national security interests of all nations. A good example was the accidental outage of a power plant in August 2003 that left without electricity for 29 hours the entire northeast coast of the United States and southeastern Canada. The blackout affected 50 million people and cities like New York, where a state of emergency was declared, plunged into chaos. Normality was reestablished three days later and losses were estimated at about 3000 million dollars a day.

Incidents like this give an idea of how much is cross the energy sector and the effects it can have for a whole country a simple power supply failure.

GLOBAL THREAT

Among the attacks that have hit the energy sector in recent years, it is important to highlight the Slammer worm attack to a nuclear plant in Ohio (US) and the Night Dragon attack to US energy companies in order to obtain confidential information.

Laziok is the new Trojan that threatens the energy sector. During the months of January and February in 2015, different companies within the energy sector (including companies in the Oil & Gas sector located in the Middle East) suffered from several attacks perpetrated by this Trojan which allows to hackers to get confidential information stored on machines that have been hacked.

Flame has a very advanced functionality to steal, store and communicate information, as well as advanced mechanisms to spread from one computer to another. The program has been used to carry out cyber espionage attacks in Middle Eastern countries and infected about 1000 machines.

Gauss was discovered at the end of 2012 and is able to spy on bank transactions, steal login information to social networks or email and attack critical infrastructures. Gauss seems to have been used to steal authentication information from people in the Middle East, particularly in Lebanon.

Duqu, a variant of *Stuxnet* which appeared in late 2011, seeks information that could be useful to attack industrial control systems such as SCADA, although it seems that it is not meant to destroy but to spy; but it is possible that the extracted information is then used to create highly specialized attacks.

Stuxnet is the name of a malicious code discovered in July 2010 capable of spying and damaging the controlled infrastructure without the administrative staff being able to recognize damages in time. There are many indications that *Stuxnet* was explicitly designed to delay the launch of the Bushehr nuclear plant in Iran. For example, most contaminated computers by *Stuxnet* were there.

The *Madi* Trojan was identified in more than 800 victims across several countries, including people related to critical infrastructure projects in Iran and Israel, Israeli financial institutions and engineering students from the Middle East, but also people in the energy sector and foreign consulates in the U.S. Certainly, measures to be taken have to be as global and sophisticated as threats.

RISK MANAGEMENT

Cyber risks, as all risks, cannot be completely eliminated, but must be managed through decision-making processes. The aim is to reduce the likelihood and impact of a cyberattack on operations, assets and workers in an organization. The application of risk management procedures in the energy sector should be directed from a common and global approach, which would facilitate a better information exchange between organizations and other stakeholders including the private sector, states and federal agencies across international borders.

Everyone in the organization is responsible for cybersecurity, however, regardless of the size or type of organization, governing boards are responsible for the impact of such risks on the business process. The increasing number of vulnerabilities and the interconnection of systems can cause serious damage to organization's properties of the energy sector, and may even endanger the power supply.

In this sense, the Industrial Cyber Security Center identifies four major attack vectors:

- Cutting remotely the electric supply of an user, a group of users or industry.
- Leaving counters out of service in order to prevent the collection of data by the distributor.
- Capturing data from counters in order to get economic benefit from their use.
- Modifying the consumption of data by listening traffic techniques.

Understanding and management of cybersecurity risks is a strategic capability and allows an efficient, effective and sustainable management of the core objectives in all organizations within the energy sector.

CYBERSECURITY IN SPAIN

The Spanish energy sector is accelerating the implementation of projects to increase cybersecurity since the rise of sophistication in threats to critical infrastructures. The main reason, among other factors, is the incorporation into distribution networks potentially targeted components such as, for example, new smart meters.

In fact, according to the latest researches from the Industrial Cybersecurity Center, the number of incidents reported by all of the critical infrastructures in Spain amounted to 134 during 2015 and the highest percentage affected the energy sector, followed by the water and food sector. It is important to note that while the power grid is gaining in efficiency thanks to new technologies, the number of actors integrated into the infrastructure have also increased with a subsequent increase in potential entry points and therefore the risks.

The Managing Director of Iberdrola states that 40% of threats come from outside and 60% come from the employees themselves who know the company´s resources and its operations. In addition, threats have an impressive technical sophistication that exceeds capabilities of the companies themselves.

The key to an effective response is to balance the objectives of the Spanish and European energy policy with the fight against deliberate attacks on infrastructure. It is also essential collaboration between administrations, local agents and operators as well as international cooperation. In this regard, in Spain there is a specific section, within the Department of Infrastructure and Monitoring for Crisis Situations (DISSC) under the Ministry of the Presidency, responsible for coordinating the actions in this field.

CONCLUSION

In recent decades, the energy sector has become very dependent on digital technology in order to reduce costs, increase efficiency and maintain a reliable functioning. However, information technology and industrial control systems are vulnerable to malicious attacks and misuse. In conclusion, we should highlight that security strategies applied to critical infrastructures should be based on cooperation, coordination and trust between the public and private sectors, deploying safe and effective communication channels.

In addition, it is essential to recognize and promote the private sector as is the one that assumes responsibility for the facilities and make senior managers aware of the importance of safety. In this sense, it is also essential regulate the legislative framework in order to establish appropriate response mechanisms to possible incidents and attacks on systems.