EUROPEAN RISK MANAGEMENT SEMINAR 2018

8-9 OCTOBER 2018
ANTWERP, BELGIUM

Corporate responsibility & sustainability

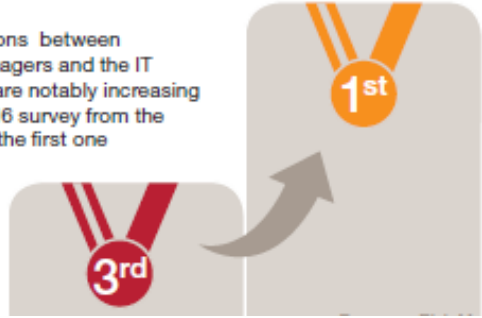
Applying lessons learned

cyber

EUROPEAN RISK MANAGEMENT SEMINAR 2018

European Risk Manager Survey 2018

The interactions between the Risk Managers and the IT department are notably increasing since the 2016 survey from the third rank to the first one




EUROPEAN RISK MANAGEMENT SEMINAR 2018
8-9 OCTOBER 2018
ANTWERP, BELGIUM
Corporate responsibility & sustainability
Wannacry learnigs
cyber

EUROPEAN RISK MANAGEMENT SEMINAR 2018

Europol

Europol: "Hay que elogiar a Telefónica por su trasparencia sobre el ciberataque"

El jefe del Centro Europeo de Ciberdelincuencia dice que tanto las empresas como los particulares deben protegerse mejor.

16 mayo, 2017 - 05:23

EN: EUROPOL TELEFÓNICA CIBERATAQUES CIBERSEGURIDAD

Juan Sanhermelando • • Bruselas

Telefónica también fue la única gran empresa española que reconoció haber sido afectada. ¿Hizo bien? ¿Es la transparencia la respuesta en estos casos?

Esta es absolutamente la forma correcta de actuar. La industria y las fuerzas de seguridad deben cooperar y tiene que haber esta transparencia. Cuanta más información tengamos de todas las partes posibles, más fácil será que podamos detener a los responsables del ataque. Así que hay que elogiar a Telefónica por su transparencia.

España ha dado una respuesta muy profesional al ataque. Fue uno de los primeros países en comunicarse con Europol.

EUROPEAN RISK MANAGEMENT SEMINAR 2018

Actualización informativa sobre los ciberataques producidos (/sala-prensa/notas-prensa/actualizacioninformativa-los-ciberataques-producidos)

Publicado el 14/05/2017

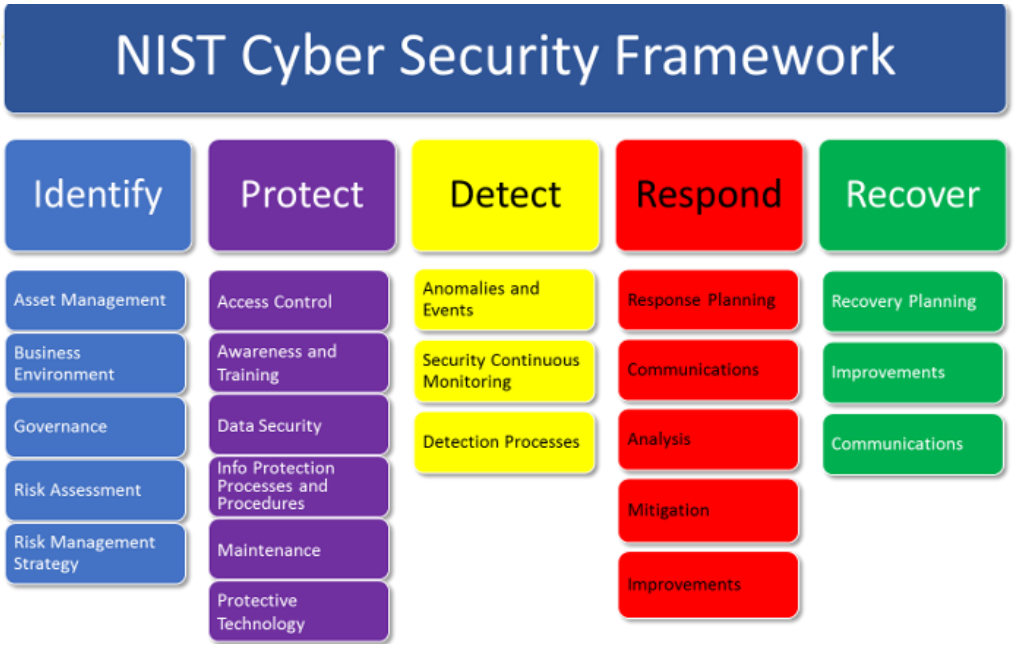
El Ministerio de Energía, Turismo y Agenda Digital informa a través del Instituto Nacional de Ciberseguridad (INCIBE) que el Centro de Respuesta a Incidentes de Seguridad e Industria (CERTSI), operado de forma coordinada por INCIBE y el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), continúa trabajando con las empresas afectadas por los ciberataques que empezaron a producirse el viernes 12 de
mayo.

Telefónica, una de las primeras compañías en detectar la amenaza, ha sido clave para acotar y minimizar el impacto del ataque en otras empresas y organismos. Gracias al trabajo conjunto con las entidades afectadas y en particular con Telefónica, el equipo del CERTSI ha podido confirmar y analizar que existen al menos dos variantes del virus informático.

- La primera de ellas, WannaCrypt.A[1] realiza, como primer paso antes de comenzar a cifrar los documentos del equipo, un intento de conexión a una página web codificada internamente. Si consigue realizar la conexión con éxito, no cifra ningún documento. Si, por el contrario, no consigue realizar la conexión a la página web, comienza el cifrado de los documentos y solicita el pago del rescate de los documentos cifrados.
- La segunda variante, WannaCrypt.B, comienza inmediatamente con el cifrado de los archivos para posteriormente solicitar el pago del rescate de los documentos cifrados.

EUROPEAN RISK MANAGEMENT SEMINAR 2018

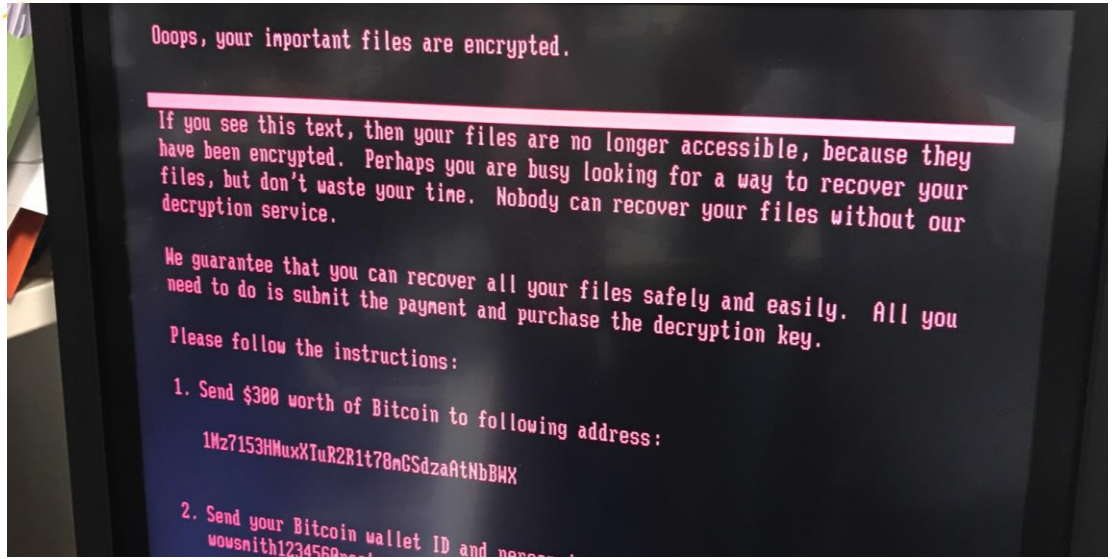
Resilience



EUROPEAN RISK MANAGEMENT SEMINAR 2018

8-9 OCTOBER 2018
ANTWERP, BELGIUM

June 27th 2017
Cyber-attack



EUROPEAN RISK MANAGEMENT SEMINAR 2018

Background to the malware
NotPetya

> *"The superficial resemblance to Petya is only skin deep. Although there is significant code sharing, the real Petya was a criminal enterprise for making money. This [latest malware] is definitely not designed to make money. This is designed to spread fast and cause damage, with a plausibly deniable cover of ransomware."*
>
> Computer security veteran, The Grugg

- Ukrainian power generation in December 2016, then US power generation in February 2017
- Targeted at Ukraine with a desire to disrupt a national holiday and delay tax

To put it plainly, this code was built to destroy, not extort

03

The cyber-attack
The impact

ON 27 JUNE A. P. MOLLER – MAERSK, AMONGST MANY GLOBAL COMPANIES, WERE HIT BY THE **MALWARE NOTPETYA**

49,000
LAPTOPS INFECTED

ALL
PRINT CAPABILITY INACCESSIBLE

1200
APPLICATIONS WERE INACCESSIBLE

1000
APPLICATIONS WERE DESTROYED

FILE SHARES
UNAVAILABLE

EUROPEAN RISK MANAGEMENT SEMINAR 2018

The root cause

The causation

The default software for submitting tax returns in Ukraine is called MeDoc

The software company that produces this was compromised and ‘back doors’ were put into the product giving the ‘hackers’ access to all companies that used the software – including Maersk

The software automatically updates itself and in the June update it pulled the virus into our network

Once on our network it looks to move from system to system, but it can not jump from one network to the other, meaning our customers and partners that connect to us remained safe

Reflections & lessons learned

Integrate CM, BCM, ERM & Insurance

Crisis Management	· Competences
	· Communication
	· Ressources available
Business Continuity	· Tested recovery plans
Governance Internal Audit	· CISO, CIO and
Risk Identification	· Risk Quantification
	· Frequency, severity and impact
Risk Mitigation	· Segregation of risk
	· Risk Culture
	· Risk Transfer
Risk Reporting	· Risk Owners
	· Action plans
	· Key Risk Indicators

Key Learnings

Key Learnings

- A framework: Telefonica applied a cyber resilience methodology based on five pillars: identify, protect, detect, respond and recover.
- Transparency: Telefonica decided to communicate quickly and regularly with the Spanish security and cyber authorities and its business customers. Telefonica was not just a good business partner but also part of the solution.
- Integrate Crisis Management, Business Continuity Management, and Enterprise Risk Management & Insurance into a comprehensive structure.

Thank you for your attention