SPANISH BEST PRACTICE ON CYBERSECURITY

HOW BUSINESSES IN SPAIN COLLABORATE WITH LEAS IN FIGHTING CYBERCRIME

WHO AM I

- DIRECTOR OF SPANISH CENTRE OF EXCELLENCE ON CYBERSECURITY (CNEC)

UAM UNIVERSIDAD AUTONOMA DE MADRID

CNEC
CENTRO NACIONAL
EXCELENCIA EN CIBERSEGURIDAD

Collaborators

- Guardia Civil
- Cuerpo Nacional de Policía

CNEC ORIGINS

- CREATED BY AND TO LEAS
- HAND IN HAND BOTH SECURITY BODIES AND A **PRIVATE COMPANY, EXPERTS ON CYBERSECURITY**
  - THEY CAME LOOKING FOR THE UNIVERSITY TO PARTICIPATE

CNEC
CENTRO NACIONAL
EXCELENCIA EN CIBERSEGURIDAD

- Universidad Autónoma de Madrid
- Guardia Civil
- Cuerpo Nacional de Policía
- A Private Company

But… it really didn't work

- Five years Later …
- It is a UAM initiative, with the participation of LEAs
- Why it didn't work for the private company?
  - They saw it as an opportunity to SELL products and training to LEAs.
  - So they were not really willing to share (and much less give)

A MUCH BETTER APPROACH

- ONE OF THE CNEC ACTIVITIES IS A MASTER ON DIGITAL EVIDENCE, DESIGNED FOR LEAS
- THIS YEAR WE HAVE MORE THAN 30 *GUARDIAS CIVILES* ATTENDING IT
- THEY ARE FUNDED BY GUARDIA CIVIL AND … A PRIVATE COMPANY
  - WHY A COMPANY IS WILLING TO "SPEND" MONEY ON LEAS TRAINING?

WIN-WIN SITUATION

- A couple of years ago the company has a "cyber issue"
- They called GC and asked for help
- Of course they got it, because is GC responsibility to protected Spanish Citizens and their Companies
- Now, the company understands that Inverting on GC Training is as cost-effective (even more?) as training its own personnel.

Fighting cybercrime

- Most experts agree that sharing intel is basic for reducing cybercrime.
- However, admitting my company was "hacked" does not seem the best promotion strategy
  - The government is asking me to report security incidents
  - But the can penalyze me in the next public bidding

THE PROPER WAY OF LOOKING AT IT

- WHO WOULD YOU CALL?

Do not fool ourselves

- We all are in war (at least a digital one)
  - I would call it "Cold War 2.0"
  - The "towers" to be defended are our **Information Assets**
- So what more logical that a (very close) collaboration between **State** and **Companies**

Spanish Strategy for National Cybersecurity

- One (out of 4) of the basic Principles: **Shared Responsibility**
  - All the agents, both public and private (including citizens) should be implied
  - … Suitable public-private cooperation, able to promote information interchange

Spanish Strategy for National Cybersecurity (II): Goals

- Goal 4 (out of 6): To **raise awareness** on Citizens, Professionals, Private Companies and Public Administrations about cyber-risks

Spanish Strategy for National Cybersecurity (III): Action Lines

- Line 5 (out of 7): Security and Resilience of ICTs on the Private Sector
- Line 6: Knowledge, Skills and I+D
- Line 7: Cybersecurity Culture

Spanish organization: agencies

- CCN-CNI: is the CERT for the public administration, but also provides
  - Information
  - Guides
  - Tools
  - Incident Handling: "Always **<u>under strict confidentiality from both sides</u>**, the CCN-CERT provides technical and operative support, for detecting, reacting, deterring and removing potential (cyber) threads"

ÚLTIMA HORA 30/01/2017 12:36

Disponibles los vídeos de las ponencias de las X Jornadas CCN-CERT

NIVEL DE ALERTA

MUY ALTO

Inicio > Definición del nivel de alerta

Definición del Nivel de Alerta

NIVEL DE ALERTA

BAJO

NIVEL DE ALERTA

MEDIO

NIVEL DE ALERTA

ALTO

NIVEL DE ALERTA

MUY ALTO

NIVEL DE ALERTA

CRÍTICO

CARMEN

Herramienta de Detección de APTs

CCNDroid

Herramientas de Seguridad para Android

CLARA

Auditoría de Cumplimiento ENS/STIC en Sistemas Windows

INES

Informe de Estado de Seguridad en el ENS

LUCIA

Sistemas de Gestión Federada de Tickets

PILAR

Análisis y Gestión de Riesgos

REYES

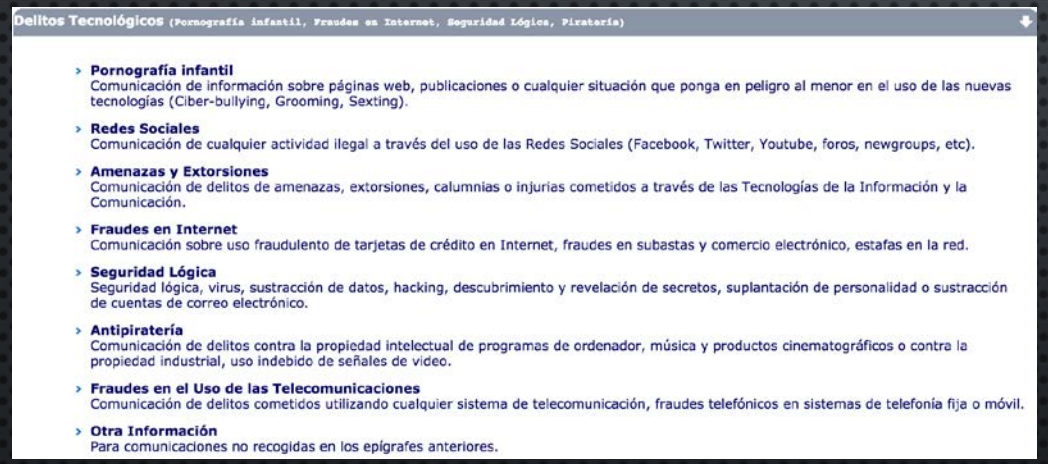
Intercambio de Información de Ciberamenazas

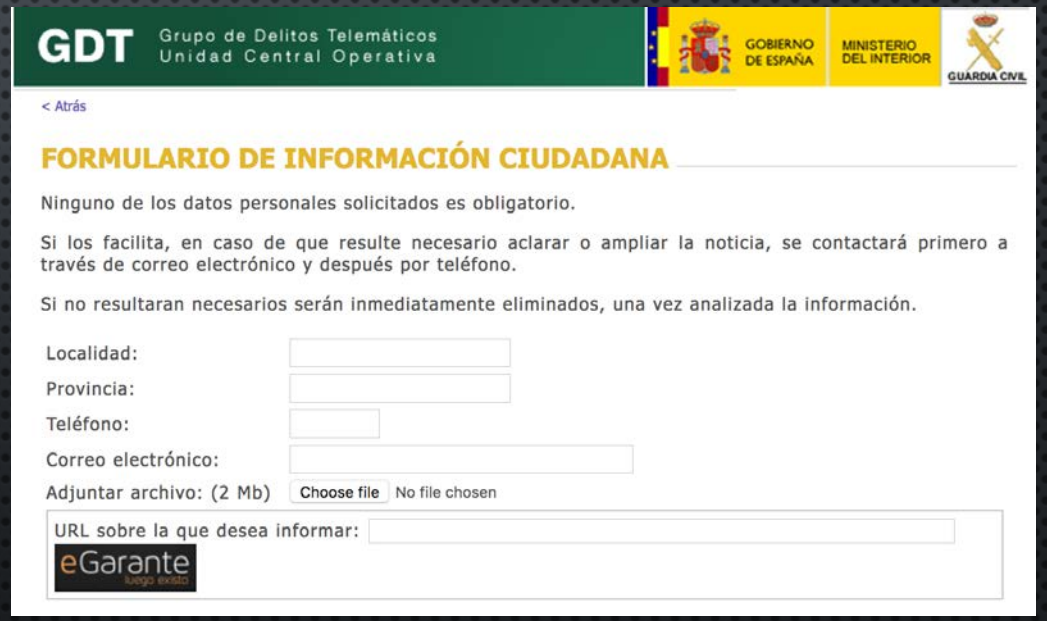
SPANISH ORGANIZATION: AGENCIES

- TRAINING, GUIDES, AWARENESS, TOOLS FOR SME'S AND SELF-EMPLOYED PROFESSIONALS

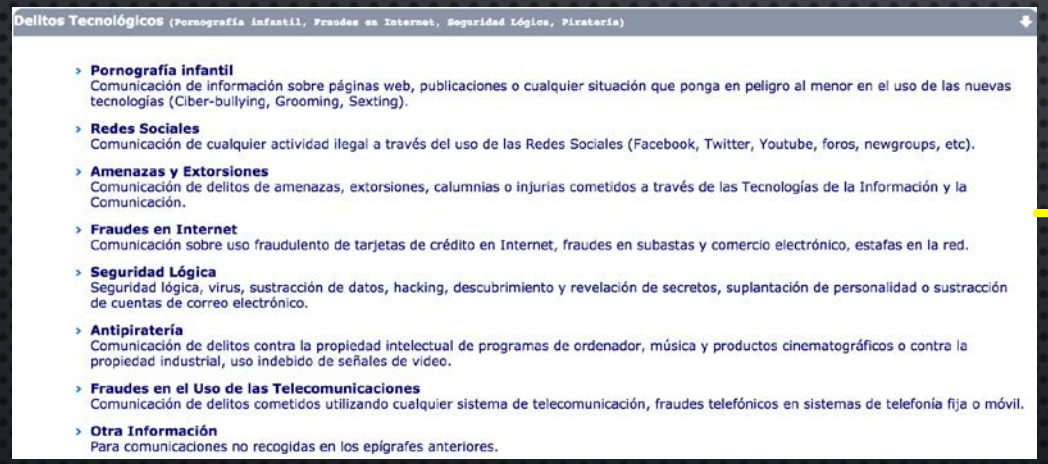
- HTTPS://WWW.INCIBE.ES/PROTEGE-TU-EMPRESA

BOTH GC AND CNP HAS SPECIFIC WEBSITES FOR CYBERCRIME REPORT / COMPLAINT





BOTH GC AND CNP HAS SPECIFIC WEBSITES FOR CYBERCRIME REPORT / COMPLAINT



Delitos Tecnológicos (Pornografía infantil, Fraudes en Internet, Seguridad Lógica, Piratería)

- **Pornografía infantil**
  Comunicación de información sobre páginas web, publicaciones o cualquier situación que ponga en peligro al menor en el uso de las nuevas tecnologías (Ciber-bullying, Grooming, Sexting).
- **Redes Sociales**
  Comunicación de cualquier actividad ilegal a través del uso de las Redes Sociales (Facebook, Twitter, Youtube, foros, newgroups, etc).
- **Amenazas y Extorsiones**
  Comunicación de delitos de amenazas, extorsiones, calumnias o injurias cometidos a través de las Tecnologías de la Información y la Comunicación.
- **Fraudes en Internet**
  Comunicación sobre uso fraudulento de tarjetas de crédito en Internet, fraudes en subastas y comercio electrónico, estafas en la red.
- **Seguridad Lógica**
  Seguridad lógica, virus, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidad o sustracción de cuentas de correo electrónico.
- **Antipiratería**
  Comunicación de delitos contra la propiedad intelectual de programas de ordenador, música y productos cinematográficos o contra la propiedad industrial, uso indebido de señales de video.
- **Fraudes en el Uso de las Telecomunicaciones**
  Comunicación de delitos cometidos utilizando cualquier sistema de telecomunicación, fraudes telefónicos en sistemas de telefonía fija o móvil.
- **Otra Información**
  Para comunicaciones no recogidas en los epígrafes anteriores.

- Child pornography
- Social Networks
- Threads and Extortions
- Internet Fraud
- Digital Security
- Piracy
- Teleco Fraud
- Other...

At the end of the road

- We are all realizing that our companies are our country
- And that these companies are in the front line of the battlefield of this **UNDECLARED WAR**

THAN YOU VERY MUCH!

ALVARO.ORTIGOSA@UAM.ES