CIBERRISCOS I COMPLIANCE

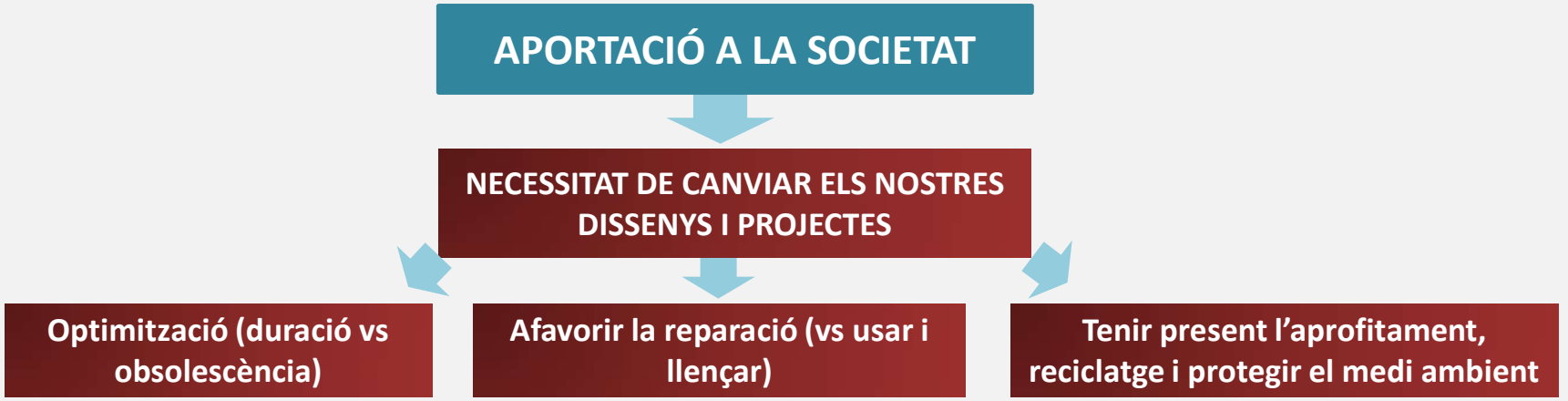
EN L'ENGINYERIA PER A LA TRANSICIÓ

la mútua dels enginyers

iGenium 2019
8th enginyering meeting point

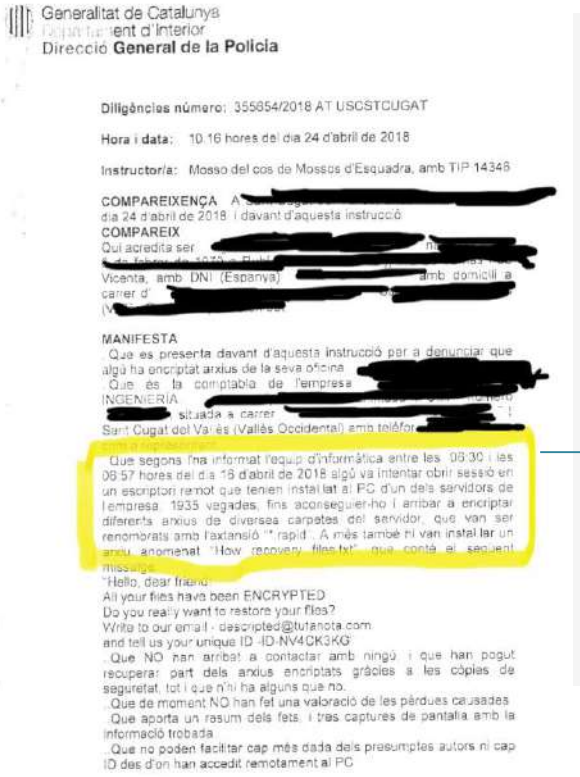
ANDREU MINGOTE
22/10/2019

ENGINYERIA PER A LA TRANSICIÓ:



NOUS REPTES: amb tecnologia i saber fer de les seves empreses.
NOUS RISCOS: ciberriscos i responsabilitat penal empreses.

EXEMPLE PRÀCTIC: DENÚNCIA REAL D'UN ATAC INFORMÀTIC A UNA SOCIETAT D'ENGINYERIA AL 2018



Generalitat de Catalunya
Departament d'Interior
Direcció **General de la Policia**

Diligències número: 355854/2018 AT UCSTCUGAT

Hora i data: 10.16 hores del dia 24 d'abril de 2018

Instructor/a: Mosso del cos de Mossos d'Esquadra, amb TIP 14346

COMPAREIXENÇA A [redacted] dia 24 d'abril de 2018 i davant d'aquesta instrucció

COMPAREIX

Qui acredita ser [redacted]

Vicenta, amb DNI (Espanya) [redacted] amb domicili a carrer d' [redacted]

MANIFESTA

.Que es presenta davant d'aquesta instrucció per a denunciar que algú ha encriptat arxius de la seva oficina [redacted]

.Que és la comptable de l'empresa INGENIERIA [redacted] situada a carrer [redacted] Sant Cugat del Vallès (Vallès Occidental) amb telèfon [redacted]

.Que segons l'ha informat l'equip d'informàtica entre les 06:30 i les 06:57 hores del dia 16 d'abril de 2018 algú va intentar obrir sessió en un escriptori remot que tenien instal·lat al PC d'un dels servidors de l'empresa. 1935 vegades, fins aconseguir-ho i arribar a encriptar diferents arxius de diverses carpetes del servidor, que van ser renombrats amb l'extensió '*.rapid'. A més també hi van instal·lar un arxiu anomenat "How_recovery_files.txt", que conté el següent missatge:

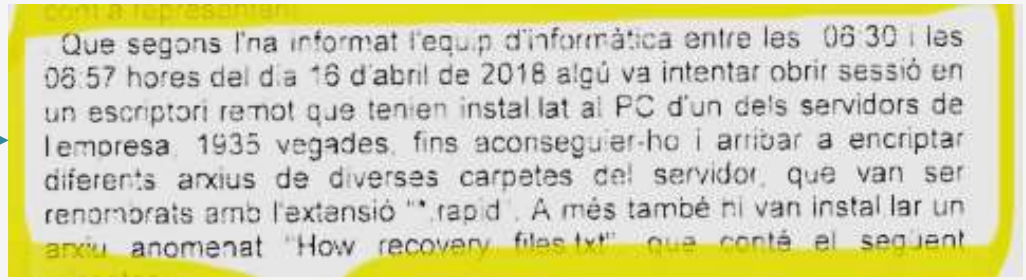
"Hello, dear friend.
All your files have been ENCRYPTED
Do you really want to restore your files?
Write to our email - descripted@tutanota.com
and tell us your unique ID "ID-NV4CK3KG"

.Que NO han arribat a contactar amb ningú i que han pogut recuperar part dels arxius encriptats gràcies a les còpies de seguretat, tot i que n'hi ha alguns que no.

.Que de moment NO han fet una valoració de les pèrdues causades

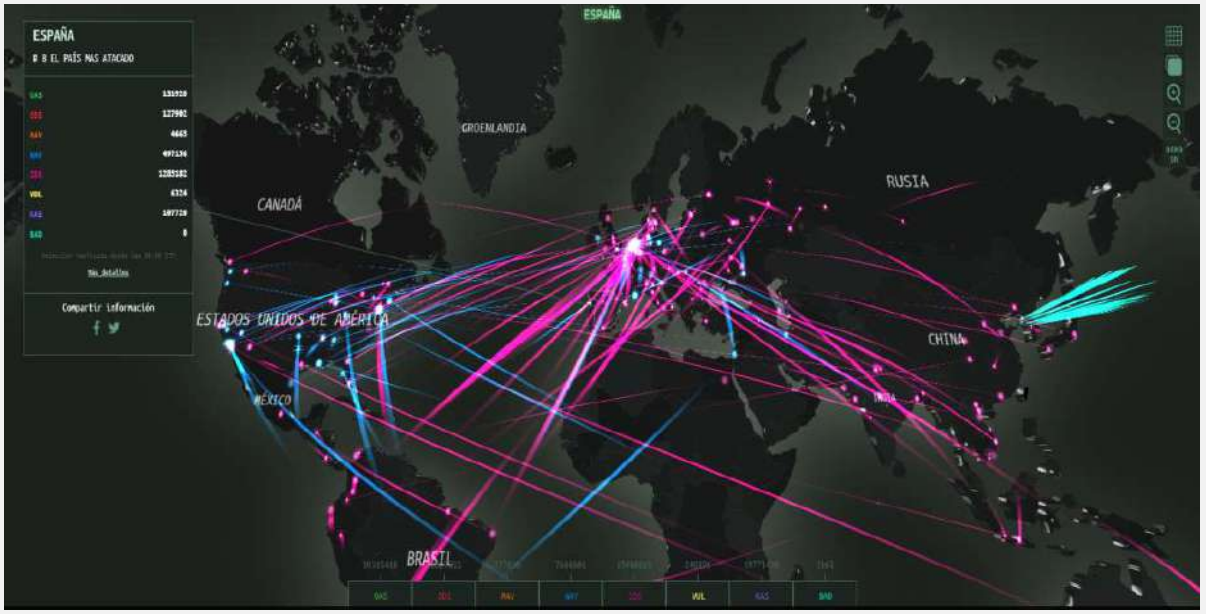
.Que aporta un resum dels fets, i tres captures de pantalla amb la informació trobada

.Que no poden facilitar cap més dada dels presumptes autors ni cap ID des d'on han accedit remotament al PC



Que segons l'ha informat l'equip d'informàtica entre les 06:30 i les 06:57 hores del dia 16 d'abril de 2018 algú va intentar obrir sessió en un escriptori remot que tenien instal·lat al PC d'un dels servidors de l'empresa. 1935 vegades, fins aconseguir-ho i arribar a encriptar diferents arxius de diverses carpetes del servidor, que van ser renombrats amb l'extensió '*.rapid'. A més també hi van instal·lar un arxiu anomenat "How_recovery_files.txt", que conté el següent

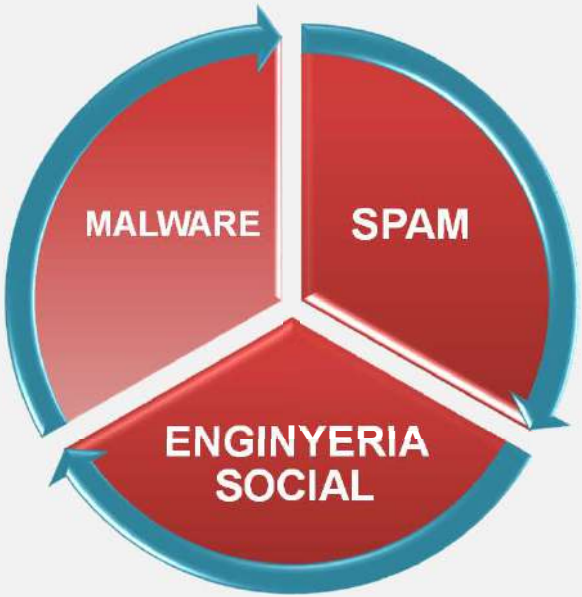
ELS CIBERRISCOS ARRIBEN PER A QUEDAR-SE: ENS ATAQUEN!



Webs on es poden veure mapes de ciberatacs on-line:
https://cybermap.kaspersky.com/es/ o **http://www.norse-corp.com/map/**

LES AMENACES ATAQUEN ELS NOSTRES PILARS DE SEGURETAT INFORMÀTICA

ELEMENTS PRINCIPALS DE LA CIBERDELINQÜÈNCIA



MALWARE

Són programes maliciosos (*malicious software*), també anomenats *badware*, codi maligne. Té com a objectiu filtrar-se o danyar el nostre PC o sistema d'informació sense el consentiment del propietari.

- Virus
- Adware
- Worms
- Hoax
- Hijacker
- Keylogger
- PUP, PUM
- Rogueware
- Ransomware
- Dropper
- RAT
- Dialers
- Stealer
- Riskware
- Rootkit
- Spyware
- Sniffers
- Backdoors
- Exploit
- Drive-by Download – Drive-by Exploit
- Troyano
- Botnets
- APT
- ScreenGrabbers

Podem descarregar una guia de Glosari amb terminologia del CNI-CERT:

https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

SPAM

També denominat correu brossa o no desitjat i fa referència als missatges no sol·licitats, no desitjats o amb remitent no conegut (correu anònim), habitualment de tipus publicitari, generalment enviat en grans quantitats (inclús de manera massiva) que perjudica d'alguna manera o diversa al receptor.

Pot manifestar-se a través de correus, finestres emergents, texts en la web... També es pot fer a través de mòbils amb sms.

ENGINYERIA SOCIAL

Tècniques psicològiques/habilitats socials utilitzades conscientment i moltes vegades amb premeditació per l'obtenció de tercers. La persona objectiu no s'adona que revela informació sensible.

- **Phishing**: suplantació d'identitat per adquirir informació confidencial de manera fraudulenta.
- **Vishing**: amb trucada telefònica, veu gravada...
- **Impersonation**: fer-te passar per un altre persona per Internet (Atenció menors!: Sexting, grooming...).
- **Ransomware**: extorsió, hoax...
- **Físicament**: shoulder surfing: "xafardejar per sobre la espatlla". Robar contrasenyes o informació.

Cas: 2010: Planta enriquiment urani Iraní atacada (worm: Stuxnet). La debilitat de l'èsser humà. (1er atac cibernètic que causa danys en una estructura "real").

POLÍTICA DE SEGURETAT

L'han d'establir els màxims Òrgans de Direcció juntament amb els diferents experts i responsables de l'entitat. Tothom ha d'anar a una.

- **Objectius clau:** PREVENIR – DETECTAR - RECUPERAR

S'ha de realitzar de manera escrita i correctament documentada i posar-la a disposició de tots els empleats per al seva comprensió i aplicació.

- **Preguntes Clau:**

Que s'ha de protegir? (determinar bens a protegir)
De qui s'ha de protegir? (anàlisi de debilitats i amenaces)
Com s'ha de realitzar la protecció? (Definir mesures de protecció i monitoritzar el compliment de la política i revisar-la = GERÈNCIA DE RISCOS!)

AVALUACIÓ DEL RISC

Permet definir la freqüència i la gravetat dels perills als quals està exposada la nostra empresa.

El mètode Mosler:

Té per objecte la identificació, anàlisi i avaluació dels factors que poden influir en la manifestació i materialització d'un risc, amb la finalitat de que la informació obtinguda ens permeti **calcular la classe i dimensió del risc**.

És un mètode seqüencial i cada fase es recolza en les dades obtingudes en fases precedents.

LA RESILIÈNCIA I TRANSFERÈNCIA DEL RISC

La gerència de riscos ens ofereix també mesurar la **resiliència** de la nostra empresa, capacitat d'adaptació i poder continuar amb la seva activitat en situacions de risc.

Aquell risc que la nostre empresa no tingui capacitat de suportar **l'haurem de transferir.**

PROBLEMA EMPRESA

Arran de la reforma del Codi Penal del 2010 (Llei orgànica 5/2010), les persones jurídiques tenen Responsabilitat Penal, al marge de les persones físiques que les integren, i per tant, poden ser sancionades amb autèntiques penes, exactament per 31 delictes possibles.

PROBLEMA AUTÒNOM

Pot ser sancionat com a persona física i ha de complir amb la normativa existent. S'enfronten a un excés de regulació fora del seu àmbit de coneixement. Petites i mitjanes empreses i autònoms poden tenir veritables problemes de compliment. Poden destinar pocs recursos al compliment.

DELICTES AFECTATS COMUNS

- ✓Estafa
- ✓Insolvències punibles
- ✓Contra la propietat intel·lectual/industrial
- ✓contra el mercat i consumidors:
  - ○ Revelació secrets, desabastiment matèries primeres, publicitat enganyosa, frau d'inversions i crèdit, facturació fraudulenta, manipulació cotitzacions de mercat, abús informació privilegiada, facilitar l'accés il·legal a serveis de radiodifusió i TV, corrupció entre particulars i esportiva
- ✓Blanqueig de capitals

- ✓Contra Hisenda pública i Seguretat Social
- ✓Contra el dret de ciutadans estrangers
- ✓Suborn
- ✓Tràfic d'influències
- ✓Corrupció de funcionari estranger

- ✓Contra l' intimitat i violació informàtica
- ✓Danys informàtics, *hacking*
- ✓Ordenació del territori
- ✓Recursos naturals i medi ambient
- ✓Energia nuclear i radiacions ionitzants
- ✓Risc provocats per explosius

SENTÈNCIES I CONDEMNES PENALS CONTRA LES EMPRESES

29/02/2016 14:58:43 | REDACCIÓN NJ | RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

El Tribunal Supremo dicta la primera sentencia por responsabilidad penal de una persona jurídica

1,1K 246

El Pleno de la Sala de lo Penal del Tribunal Supremo ha dictado una **sentencia de fecha 29 de febrero de 2016 (sentencia número 154/2016, ponente señor Maza Martín)**, en la que por primera vez aprecia la responsabilidad penal de una personas jurídica.

La sentencia explica los requisitos para apreciar la responsabilidad de las empresas de acuerdo al **artículo 31 bis del Código Penal**:

En primer término, como presupuesto inicial, **debe constatarse la comisión de delito por una persona física que sea integrante de la persona jurídica** (en este caso eran administradores de hecho o de derecho).

En segundo término, **que las empresas hayan incumplido su obligación de establecer medidas de vigilancia y control para evitar la comisión de delitos.** "Así, la determinación del actuar de la persona jurídica, relevante a efectos de la afirmación de su responsabilidad penal, ha de establecerse a partir del análisis acerca de si el delito cometido por la persona física en el seno de aquélla, ha sido posible o facilitado por la ausencia de una cultura de respeto al derecho como fuente de inspiración de la actuación de su estructura organizativa e independiente de la de cada una de las personas jurídicas que la integran, que habría de manifestarse en alguna clase de formas concretas de vigilancia y control del comportamiento de sus directivos y subordinados jerárquicos tendentes a la evitación de la comisión por éstos de los delitos", señala la sentencia.

COMPLIANCE

Las condenas penales contra la empresa superan ya los 2.400 millones

5D

- El delito fiscal es el que provoca más sentencias contra las compañías desde 2015

Ir a comentarios

Newsletter

Aún queda mucho camino por recorrer para que el régimen de responsabilidad penal de las personas jurídicas despliegue los efectos deseados en relación a la prevención

http://noticias.juridicas.com/actualidad/jurisprudencia/10910-el-tribunal-supremo-dicta-la-primera-sentencia-por-responsabilidad-penal-de-una-persona-juridica/ 775me

https://cincodias.elpais.com/cincodias/2019/04/18/legal/1555581770_860308.htm

PROGRAMA DE COMPLIANCE

(COMPLIMENT CORPORATIU DE LA RESPONSABILITAT PENAL PER EMPRESES)

L'ADN D'EMPRESES I AUTÒNOMS

Projecte: assessorar i proveir dels serveis legals i tècnics a empreses i autònoms per facilitar el compliment normatiu que pot implicar sancions penals:

- Generar un programa de prevenció de delictes penals i/o la seva auditoria, per a empreses (des de la reforma del codi penal l'any 2015, un bon programa de prevenció pot eximir de la pena).

- Ajudar a complir amb la normativa general i no sectorial amb un programa regular per societats i professionals de l'enginyeria. Ajut a treballar de forma més segura en l'àmbit legal.

- Oferir fórmules de transferència de risc que ens protegeixin.

PROGRAMA DE COMPLIANCE…

I PER QUÈ?

QUÈ IMPLICA QUE LA EMPRESA PUGUI INCÓRRER EN RESPONSABILITAT PENAL?

Des de el 2010 les empreses són responsables penals de 31 tipus de delictes i des del 2015 un bon programa de prevenció les pot eximir.

QUINES CONSEQÜÈNCIES IMPLICA LA COMISSIÓ D'UN DELICTE?

Els administradors o consellers poden patir penes de presó o l'empresa pot ser intervinguda o dissolta, inhabilitada, obligada a indemnitzar a la víctima, sancionada...

QUAN ÉS RESPONSABLE PENAL LA PERSONA JURÍDICA?

Quan una persona de la organització comet un delicte, ho fa en nom o per compte de la persona jurídica i aquesta rep un benefici directe o indirecte.

QUI POT COMETRE AQUEST DELICTE DINS LA EMPRESA?

Persones amb poder de decisió, amb facultat d'organització i control, el representant legal, qualsevol empleat per incompliment greu del deure de control.

En una empresa, el model de negoci implica la coordinació entre els diferents actors. Establir un PROGRAMA DE COMPLIANCE aporta valor a la nostre marca i producte: EXPLICA A LA SOCIETAT EL QUE SOM I COMO HO VOLEM FER

GRÀCIES

GRUP la mútua DELS ENGINYERS

Segueix-nos!

BLOGS

Via Laietana, 39, 2n 08003 Barcelona
93 295 43 00 – 662 991 085
correu@mutua-enginyers.com
www.mutua-enginyers.com