Retos actuales en Seguridad de la Información del Ministerio de Justicia

19 de febrero de 2019

María del Carmen Zarcero García-Risco
Coordinadora de área de la DTIC

Sobre nosotros…

La División de Tecnología de la Información y las Comunicaciones, dependiendo de la Subsecretaría del Ministerio de Justica tiene entre sus misiones:

- La **planificación estratégica**, la **transformación digital e innovació**n y coordinación de la **política informático** a nivel Departamento.
- **Desarrollo de sistemas de información** en el ámbito del Ministerio (AGE).
- La implantación de la **Administración Digital.**
- **Portales Institucionales y Servicios al Ciudadanos y terceros** que se relacionan con el Ministerio.
- **Centro de servicios** para otras entidades y organismos dependientes del Departamento.
- **Seguridad de la Información,** constituyendo los órganos de gobierno y aprobando normas y medidas técnicas.
- **Coordinación y supervisión en materia de protección y reutilización de datos**.

Algunas cifras…

- Formada por casi 50 funcionarios públicos y 170 efectivos externos.
- Ofrece servicios a alrededor de 1000 usuarios internos, 900 usuarios de organismos adscritos, Ciudadanos y actores terceros: Notarios, Registradores, Fundaciones, Mediadores, Entidades Religiosas, Administración de Justicia...
- 2 centros de proceso de datos clasificados entre los 20 mejores de la AGE.
- Proyectos claves para los ciudadanos: Nacionalidad, Registro Civil Digital y la completitud de la Administración Digital.

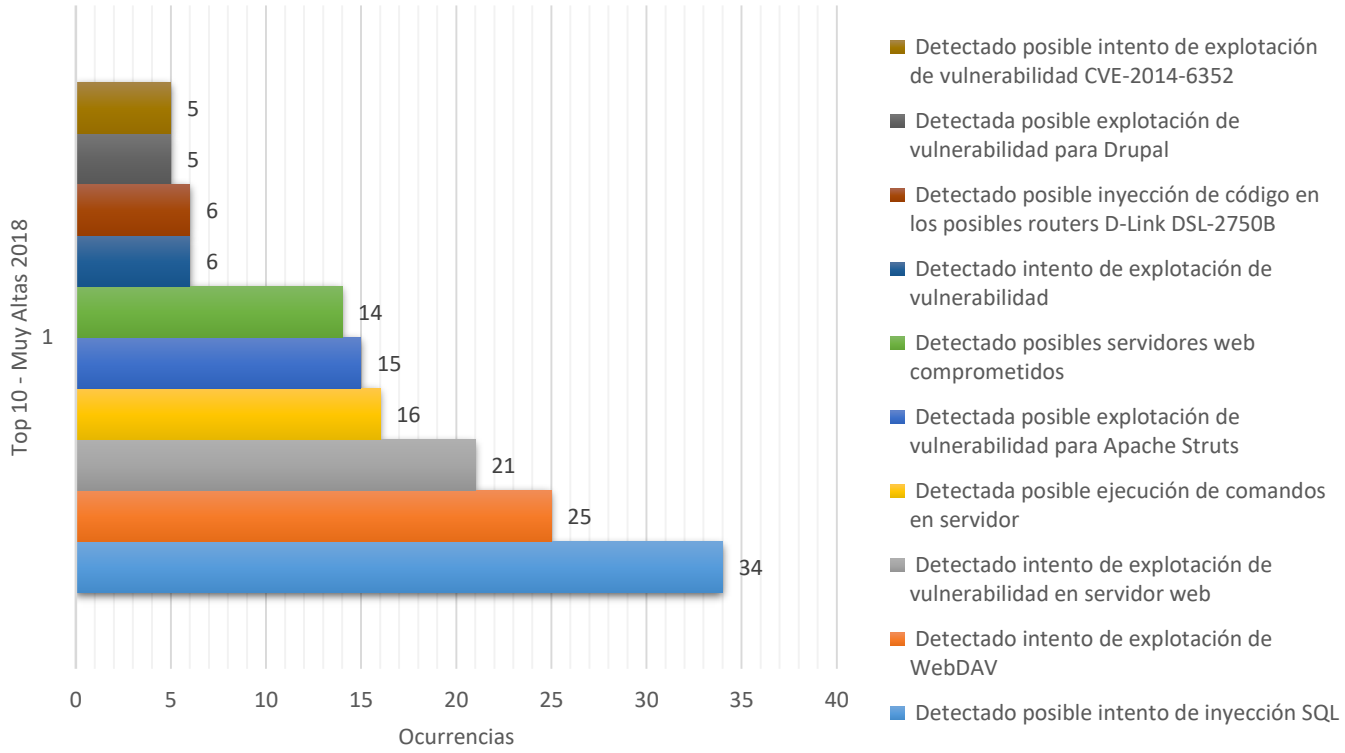
Pero para su consecución tiene grandes retos

Nuestro día a día…

GOBIERNO DE ESPAÑA MINISTERIO DE JUSTICIA

dtic División de Tecnologías de la Información y las Comunicaciones

2018: alrededor 200 incidentes categorizados muy altos y reportados por el CCN-CERT



Nuestro día a día II…

GOBIERNO DE ESPAÑA MINISTERIO DE JUSTICIA

dtic División de Tecnologías de la Información y las Comunicaciones

2018: y otros ataques detectados por medios propios

Asunto	Ocurrencias
Información de debug en eConsultas	1
Infección por virus comunes	1
Ataque web del portal desde posición en China	1
Actividad sospechosa detectada: Intentos de fuerza bruta contra servidor web y SSH	1
Intento de DDoS HTTP a portal web	1
Posible infección positiva por troyano	1
Posible virus en correo electrónico.	1
Ataque Phishing contra direcciones de correo del Ministerio de Justicia	1

VIGILANCIA DIGITAL...

GOBIERNO DE ESPAÑA MINISTERIO DE JUSTICIA

dtic División de Tecnologías de la Información y las Comunicaciones

Ataques organizados

Actualidad…

Hello #Ministerio de Justicia @justiciagob https://t.co/ykVLcyyANl
- Contact us on: digitalresearchteam@secmail.pro
- #Hacked #Pwned #Security #Justiciagob #CyberSecurity #Justicia #Email pic.twitter.com/ZToqt1HX4N

— DigitalResearchTeam (@digitalrteam) 11 de febrero de 2019

Hello @informaticaaeat https://t.co/2dFtt3CUzU
- Contact us on: digitalresearchteam@secmail.pro
- #Hacked #XSS #Security #CyberSecurity #Email #AgenciaTributaria pic.twitter.com/9rMFSLBno2

DigitalResearchTeam
@digitalrteam

Hello @justiciagob mjusticia.gob.e
- Contact us on:
digitalresearchteam@secmail.pro
- #Hacked #Pwned #Security #Justiciagob #CyberSecurity #Justicia #Email

Traducir Tweet

22:43 - 7 feb. 2019

2 Retweets **5** Me gusta

2 5

Sorteo del día 29 de enero
29 de enero de 2010
Resultado del sorteo
Documentos asociados
Resultado sorteo (XLS. 181 KB)

Actualización (14/02/2019): como señalan nuestros compañeros de Genbeta, todos los tuits de cuenta @digitalrteam que hacían referencia a esas teóricas intrusiones han sido borrados, lo que parece confirmar que todo era una farsa.

En los últimos días un grupo hacker llamado '**Digital Research Team**' ha venido publicando una serie de mensajes en Twitter para avisar del supuesto hackeo a diversos organismos oficiales, académicos o partidos políticos tanto en España como en países como Venezuela, Perú o Argentina.

es de @DigitalResearchTeam implica entre otros , el de Hacienda, el de Asuntos Exteriores, el tadística, las Universidades de Málaga, Zaragoza, tovira i Virgili o Pablo de Olavide e **incluso afecta a políticos del PSOE, CCOO y de Ciudadanos**. En todos los casos, eso sí, parece que se trata de acciones de hacking ético orientado a avisar a estos organismos de problemas de seguridad para que los resuelvan antes que "malos actores" aprovechen esas vulnerabilidades descubiertas.

Un hackeo ético masivo aún por confirmar

En un comunicado publicado en Rogue Media Labs este grupo indica que **todos sus hacks han sido éticos**, lo que significa que tienen el objetivo no de aprovecharse de esas vulnerabilidades, sino de avisar de ellas a quienes están afectados.

Nuestra experiencia…

- **Amenazas globales** y ataques de denegación de servicio **DDoS.**

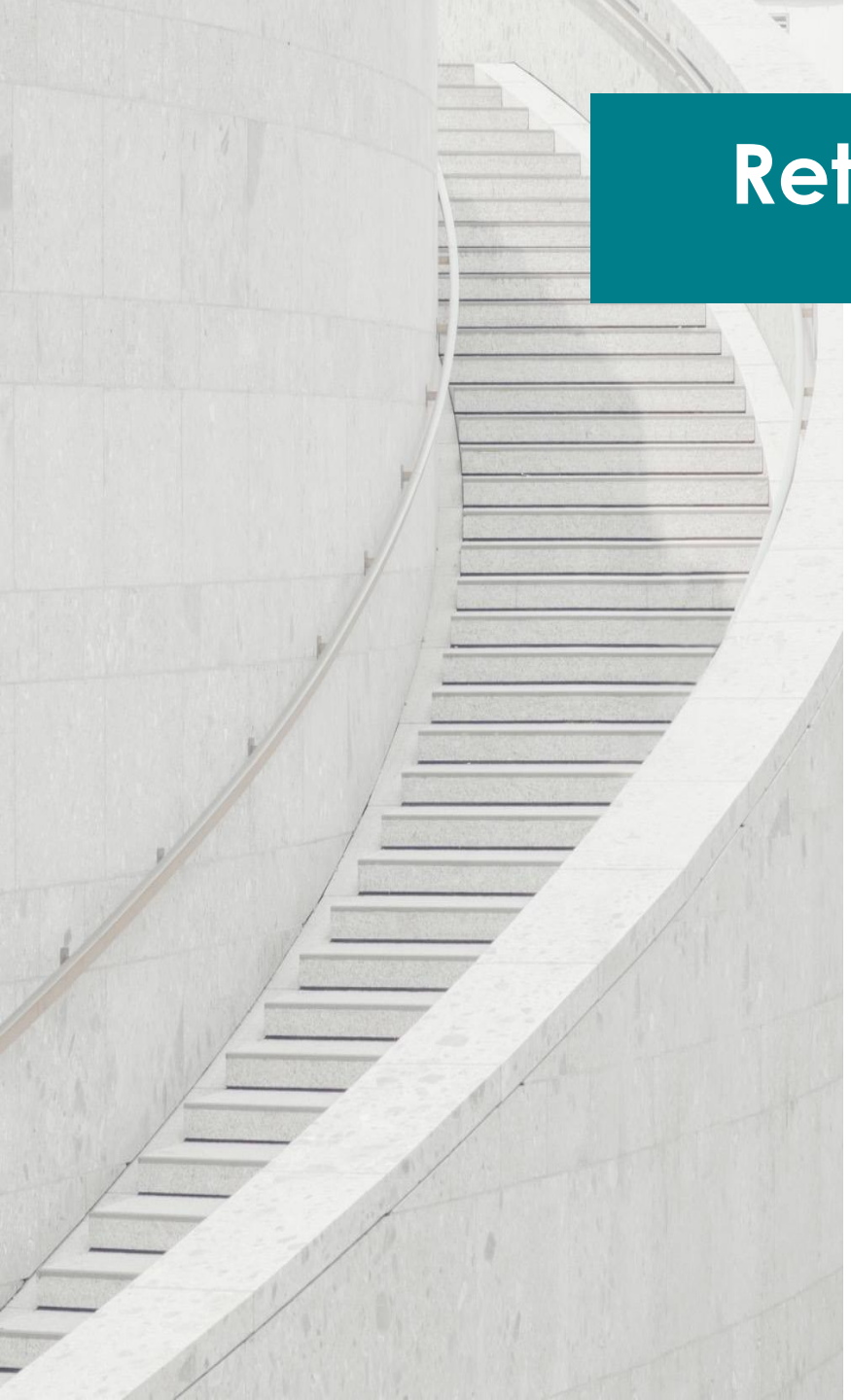
- La constante aparición de **vulnerabilidades y la publicación de exploit:** tanto para fallos en sistemas operativos, de aplicaciones, herramientas para el desarrollo tipo struts como los fallos de seguridad propios de nuestros sistemas de información.

- Desconocimiento de los usuarios de los **riesgos y consecuencias** de la ciberseguridad.

- **Ataques dirigidos** que aprovechan la ingeniería social para provocar grandes daños: **phising**, **ransomware, ataques patrocinados**

- **Nunca las medidas técnicas** son suficientes.

- **Fugas de información** intencionadas. El usuario es el eslabón más débil de la cadena.



Retos …

- **Cumplimiento de la Política de Seguridad, Instrucción de buenas prácticas** en el uso de los medios informáticos y **Cumplimiento Normativo:** adaptación RGPD y Esquema Nacional de Seguridad.

- **Mejora de medidas técnicas** a través de la automatización de la **detección de vectores de ataques**: capas perimetrales (FW, filtros de navegación y correo), Data Loss Prevention, gestión de cuentas privilegiadas, e introducción de sistemas de gestión de eventos y de información de Seguridad (SIEM) e implantación de la **seguridad en el diseño de aplicaciones y auditorías de código**.

- **Obtener Formación especializada** en materia de seguridad informática del personas TIC e introducción de **Planes de Concienciación** de usuarios finales.

- **Gestión eficiente de incidentes de Seguridad** para reducción del impacto.

- Generación de **confianza** en los ciudadanos.

Nuestra filosofía …

Algo que intentamos hacer y que nos caracteriza en la DTIC es contemplar la Seguridad desde el momento de diseño de las aplicaciones, con evaluaciones formales ENS y plan de gestión de riesgos en los principales sistemas, incorporando junto a las prioridades de negocio los evolutivos y adaptativos que refuercen la privacidad y disponibilidad, con la introducción del hardware y software específico para ciertas necesidades de seguridad y con auditorías de los sistemas dentro de un proceso muy interiorizado de mejora continua.

¡Gracias!

19 de febrero de 2019