TLP: WHITE

Ciberseguridad

Comunicado Urgente de la Situación actual

GOBIERNO DE ESPAÑA
MINISTERIO DE JUSTICIA
SECRETARÍA DE ESTADO DE JUSTICIA
SECRETARÍA GENERAL PARA LA INNOVACIÓN Y CALIDAD DEL SERVICIO PÚBLICO DE JUSTICIA
DIRECCIÓN GENERAL DE TRANSFORMACIÓN DIGITAL DE LA ADMINISTRACIÓN DE JUSTICIA
AGENDA 2030

1 COMUNICADO URGENTE DE LA SITUACIÓN ACTUAL

1.1 Ciberguerra

La definición de la situación actual en el ámbito informático y de comunicaciones, es la **ciberguerra**.

Además de las noticias que recibimos cada día en los medios de comunicación sobre la guerra en Ucrania, en el ciberespacio también se está librando una guerra paralela, la ciberguerra.

Hay multitud de ataques contra webs e infraestructuras críticas, tanto de instituciones como empresas de Ucrania, intentando desestabilizar aún más el país.

Los grupos que hay detrás de estos ataques son viejos conocidos de las agencias encargadas de la ciberseguridad de países de todo el mundo. Se trata de expertos con altísimas capacidades, como la de alterar los teléfonos Android que utilizaba la artillería ucraniana, y así poder localizar la ubicación exacta de estas unidades de artillería.

Pero no sólo son objetivo las webs ucranianas, también las de países de la OTAN y de la Unión Europea, por tanto entre los países afectados está España, y con ello el Ministerio de Justicia como posible Administración objetivo de los ciberataques.

1.2 ¿A qué estamos expuestos?

En 2021 se produjeron multitud de ciberincidentes dirigidos tanto a organismos e instituciones de la Administración, como a empresas prestadoras de servicios de la Administración.

Ejemplos de lo anterior son el ciberincidente que impidió trabajar al SEPE al 100% durante casi un mes, o el del Ayuntamiento de Castelló.

El modus operandi siempre es similar; mediante el engaño el atacante consigue instalar un programa malicioso en el ordenador de la víctima, este programa logrará extenderse por la red a otros ordenadores, robará información, y posiblemente cifrará todos los datos. El atacante pedirá un rescate y si no se paga ese rescate, los datos no se descifrarán y además como en el caso del Ayuntamiento de Castelló se filtran a la dark web datos sobre víctimas de maltrato o de menores (la dark web o web oscura es utilizada para la actividad cibernética ilegal).

El engaño a la víctima puede venir por distintas vías como el correo electrónico, un pendrive USB o incluso una llamada telefónica. Cada mes los sistemas de correo del Ministerio eliminan unos 8 millones de correos maliciosos, usted como usuario, habría recibido 540. Nuestros sistemas antivirus analizan unos 38 millones de documentos eliminando aquellos que contienen algún tipo de software malicioso.

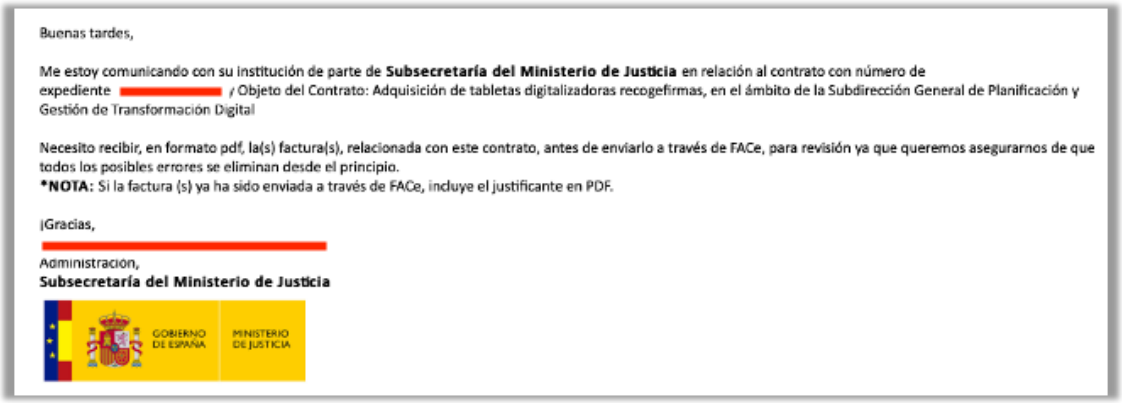
Pero no es suficiente con las medidas técnicas, hay que aprender a detectar que nos están engañando, para lo que es muy importante seguir los consejos de las píldoras de las campañas de concienciación. Debemos mantener una actitud vigilante y activa de cara a no caer en los diferentes engaños a los que nos vemos sometidos.

1.3 ¿Somos objetivo?

Sí, somos objetivo.

Además de los millones de correos maliciosos y los virus detectados por los sistemas antivirus, los sistemas de protección de las redes del Ministerio detectan cada día innumerables intentos de ataque y hemos de recordar que en el pasado **hemos sido objetivo de incidentes similares al del SEPE** o al del Ayuntamiento de Castellón. En 2015 se cifraron cientos de miles de documentos de las sedes de Badajoz, Ceuta y Murcia, con el consiguiente trastorno y parada de la actividad hasta que se pudo erradicar el problema.

Hay multitud de ejemplos, veamos un intento en el que **el atacante conoce perfectamente el entorno**, conoce muy bien a quien engañar (la empresa) y en nombre de quien provocar el engaño (el funcionario con capacidad de contratación).



Buenas tardes,

Me estoy comunicando con su institución de parte de **Subsecretaría del Ministerio de Justicia** en relación al contrato con número de expediente [redacted] / Objeto del Contrato: Adquisición de tabletas digitalizadoras recogefirmas, en el ámbito de la Subdirección General de Planificación y Gestión de Transformación Digital

Necesito recibir, en formato pdf, la(s) factura(s), relacionada con este contrato, antes de enviarlo a través de FACe, para revisión ya que queremos asegurarnos de que todos los posibles errores se eliminan desde el principio.
***NOTA:** Si la factura (s) ya ha sido enviada a través de FACe, incluye el justificante en PDF.

¡Gracias,

[redacted]
Administración,
Subsecretaría del Ministerio de Justicia

GOBIERNO DE ESPAÑA MINISTERIO DE JUSTICIA

Esta imagen es un correo fraudulento dirigido a una empresa que presta servicios al Ministerio para intentar obtener información de determinadas facturas o incluso modificarlas. Pretende engañar a la empresa haciéndose pasar por un funcionario del Ministerio.

A menudo se producen brechas de seguridad por las que se **roban los datos de cuentas de usuario**, por ejemplo, en abril de 2021 se robaron 500 millones de cuentas de Facebook; otros servicios conocidos como Dropbox o Phone House España (5,2 millones de cuentas) han sufrido también este tipo de incidente de seguridad.

Es imprudente utilizar la cuenta de correo del trabajo para darse de alta en servicios de Internet, ya que, si este servicio sufre una brecha, se conocerán los datos de acceso al correo electrónico del ministerio. El Centro de Operaciones de Seguridad del Ministerio

dispone de un servicio por el que se detectan robos de credenciales y se notifican al usuario que se ha visto afectado en este tipo de incidentes.

¿Le han **llamado de Microsoft** porque han detectado que su ordenador tiene virus? Evidentemente no era ningún técnico de Microsoft, estaban intentando engañarle para entrar en su ordenador.

Si no espera un documento adjunto en un correo, no lo abra; si no espera un SMS de Correos, no lo abra y sobre todo no haga clic en los enlaces.

Siempre debemos tener en cuenta que somos una Administración muy importante y la parada del servicio, por ejemplo, **sin poder celebrar juicios durante semanas causaría un grave impacto en la estabilidad del país**. Desestabilizando el país se conseguirá desestabilizar a la Unión Europea.

1.4 Incrementando las medidas de protección

Desde hace un tiempo a nivel de toda la Administración General y Comunidades Autónomas se están reforzando las medidas de protección con el fin de prevenir ciberincidentes y de detectarlos tan pronto como sucedan.

Se trata de una colección de medidas clasificadas en función del nivel de riesgo al que están expuestos los sistemas de información a causa de la situación de ciberguerra, ciberespionaje y cibercrimen.

Buena parte de estas medidas son aplicadas de manera que no apreciará cambios en su día a día. Hay, sin embargo, alguna medida que alterará ligeramente su rutina de trabajo.

Por ejemplo, el ordenador debe apagarse tras la jornada laboral; en caso de que se le olvide apagarlo, se apagará automáticamente. Esta medida evitará que se propaguen los programas maliciosos en caso de infección.

Otra medida de obligado cumplimiento es la necesidad de fortalecer el acceso cuando se trabaja fuera de la red de la oficina. Está demostrado que identificarse en un sistema simplemente con usuario y contraseña es insuficiente, ya que es fácil suplantar la identidad.

Ya desde 2020 habrá notado que para realizar compras por Internet, su banco te pide este tipo de refuerzo en la autenticación.

En el Ministerio ya llevamos un tiempo aplicando este tipo de medidas para proteger sus accesos cuando teletrabaja. Por ejemplo, proteger el acceso al correo electrónico mediante el uso de la aplicación Microsoft Authenticator en su teléfono móvil, aplicación que en ningún caso va a necesitar conocer su número de teléfono.

También existen medidas más restrictivas para proteger los sistemas que pueden ser aplicadas en función de la gravedad de los ataques y que, en todo caso, serán comunicadas a los usuarios.