

CLIPPING
JORNADA SOBRE
CIBERSEGURIDAD



Club Diálogos
para la Democracia

Medios impresos



Los ciberataques se disparan: afectan ya a 3 de cada 4 empresas en España

CIBERSEGURIDAD España es el tercer país del mundo que más ataques informáticos recibe. En 2016 se detectaron 115.000 incidentes, de los que 480 afectaron a hospitales y aeropuertos, entre otros.

Imma Benedito Madrid

La ciberseguridad, igual que el cambio climático, es tan alarmante como intangible. Tres decada cuatro empresas españolas ha sufrido un ciberataque en los últimos cinco años. Sin embargo, apenas el 3% tiene un plan de respuesta a incidentes de este tipo. A nivel mundial, el coste de los ciberataques a empresas asciende a un total de 265 millones de euros. En el caso de España, nos encontramos con que es el tercer país con más ofensivas a nivel mundial, después de Reino Unido y Estados Unidos.

La escalada es exponencial y, las cifras, alarmantes. En 2016, el Instituto Nacional de Seguridad (Incibe) detectó más de 115.000 ciberincidentes, de los cuales más de 110.000 afectaron a ciudadanos y al sector privado, y 480 a infraestructuras críticas -aeropuertos, hospitales, centrales eléctricas o plantas de agua-, sólo en el primer trimestre de este año. España recibió 50.000 ciberataques, 247 en estructuras críticas. A ese ritmo, podríamos alcanzar las 150.000 ofensivas a finales de este año. El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% amenazas y coacciones.

"Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos. Muchas veces no valoramos lo que tenemos dentro de un dispositivo y no hacemos lo posible por protegerlo", explicó ayer José Antonio Nieto Ballesteros, secretario de Estado de Seguridad del Ministerio del Interior, en una jornada sobre Ciberseguridad organizada por el Club Diálogo para la Democracia.

El "negocio" es rentable. Actualmente supone cerca del 0,8% del PIB mundial, es decir, mueve más dinero que la mayoría de crímenes, como es el caso de tráfico de estupefacientes. Por la parte de la ciberseguridad también, alcanzando los 76.000 millones de euros al año en el mundo. "La magnitud del problema está todavía lejos de entenderse por una mayoría. No se está respondiendo ni con la seriedad ni la contundencia que se

256
Millones de euros

Es el coste total de los ciberataques a empresas durante el último año, a nivel mundial. La mayoría de las empresas (52%) no disponen de ciberseguros.

115.000
Ciberataques

Detectados en España en 2016 por el Incibe. De los cuales, 110.000 afectaron a ciudadanos y al sector privado y 480 a centrales eléctricas, hospitales, aeropuertos, etc.

66.586
Denuncias

El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% fueron amenazas y coacciones.

debe", señaló Enrique Cabeiro Cabello, jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa. Es el gran problema de lo intangible, que hace que no terminemos de creerlo lo que no vemos.

Pero del virus hemos pasado a la epidemia y del pasado a la plaga. En diciembre de 2015, el trojan BlackEnergy provocó cortes en el suministro de electricidad a más de 600.000 hogares ucranianos en pleno invierno. Las ofensivas contra estructuras críticas son las más preocupantes. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. El pasado 12 de mayo, el incidente del ransomware WannaCry afectó a más de 25 hospitales. Ante la imposibilidad de acceder al sistema informático, muchos de ellos tuvieron que trasladar a pacientes graves a otros hospitales cercanos. En los dos últimos años, más de 4.000 ataques cibernéticos se identifican con el tipo ransomware -se caracteriza por secuestrar la información y



El dinero que mueven los ciberataques supone cerca del 0,8% del PIB mundial.

AUMENTO EXPONENCIAL DE CIBERATAQUES EN ESPAÑA



Fuente: INCIPE

exigir un rescate". Se trata del principal malware en Europa. WannaCry afectó a más de 300.000 equipos de 180 países. En España, fueron 1.200 equipos. "La reacción fue rápida y se pudo controlar el impacto de manera inmediata", explicó ayer Antonio Gavilanes Dumont, presidente del Club Diálogo para la Democracia. El caso más sonado fue Telefónica, aunque José Luis Gilpérez, director ejecutivo

de Administraciones Públicas, Defensa, Seguridad y Big Data de Telefónica, aseguró ayer que "el impacto real de WannaCry ha sido cero". El grupo de telefonía aumentó sus ingresos en el área de seguridad un 22,7% en 2016, hasta 341 millones.

"Esto es un trabajo de todos los agentes públicos y privados", señaló Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Incibe.

Después del incidente, Reino Unido ha decidido invertir 13.000 millones de euros en ciberseguridad. En España no hay una partida definida de la Administración Pública, aunque Nieto aseguró que "tenemos herramientas para prevenirlo y una implicación altísima de los técnicos y de la iniciativa privada para conseguir que España sea una materia de seguridad virtual como lo es física".

El fiscal Moix renuncia por su empresa familiar en Panamá

Expansión Madrid

Manuel Moix renunció ayer su cargo al frente de la Fiscalía Anticorrupción después de la polémica sobre su participación en una sociedad familiar radicada en Panamá, una decisión que aplaudieron las asociaciones de fiscalía que para la oposición llega tarde y es insuficiente. Con un mandato de tres meses, Moix se ha visto obligado a presentar su renuncia irrevocable después de esa última polémica, aunque su escaso trimestre en la dirección de la Fiscalía Anticorrupción no ha estado exento de críticas a su gestión desde un amplio espectro de lapolítica y la judicatura.

Ya se esperaba anteayer su renuncia, pero finalmente decidió hacerlo ayer. Ante el fiscal general del Estado, José Manuel Maza, dejó claro que él no habría pedido la dimisión y que en el comportamiento de Moix no ha existido "ninguna clase de ilegalidad, irregularidad o incompatibilidad". "Tras hablar con él, y puesto que ha insistido en que lo hace de manera irrevocable, no he podido conculcarle. Ha ejercido el cargo a plena satisfacción, pero no puedo obligar a quien alega motivos personales", justificó.

El diario *Infórbre* publicó que Moix posee el 25% de una sociedad constituida en el paraíso fiscal de Panamá en 1988 y propietaria de un chalet en Collado Villalba (Madrid) valorado en 550.000 euros. Moix y sus hermanos heredaron la sociedad tras el fallecimiento de sus padres y la han mantenido tras declararla a Hacienda. El fiscal dijo haberse enterado de la existencia de dicha sociedad cuando fallecieron sus padres, pero el mismo diario ha publicado datos que contradicen esa versión.

El Gobierno, que pasó del apoyo público a Michel Salvendy, el presidente del Ejecutivo, Mariano Rajoy, ni se refirió ayer a él, dejó al ministro de Justicia, Rafael Catalá, la reacción al caso, en unas declaraciones en las que expresó su respeto por esa decisión "personal" a la vez que coincidió con Maza en sus apreciaciones.

Junto a Moix aspiraron en su día al puesto de jefe Anticorrupción: Belén Suárez, Antonio Romeral, María Teresa Gilber, Carlos Alba y Alejandro Lonzani, a vez que Moix lo hagan de nuevo.

Los ciberataques se disparan: afectan ya a 3 de cada 4 empresas en España

CIBERSEGURIDAD España es el tercer país del mundo que más ataques informáticos recibe. En 2016 se detectaron 115.000 incidentes, de los que 480 afectaron a hospitales y aeropuertos, entre otros.

Imma Benedito, Madrid
La ciberseguridad, igual que el cambio climático, es tan alarmante como intangible. Tres decada cuatro empresas españolas ha sufrido un ciberataque en los últimos cinco años. Sin embargo, apenas el 37% tiene un plan de respuesta a incidentes de este tipo. A nivel mundial, el coste de los ciberataques a empresas asciende a un total de 265 millones de euros. En el caso de España, nos encontramos con que es el tercer país con más ofensivas a nivel mundial, después de Reino Unido y Estados Unidos.

La escalada es exponencial y, las cifras, alarmantes. En 2016, el Instituto Nacional de Seguridad (Incibe) detectó más de 115.000 ciberincidentes, de los cuales más de 110.000 afectaron a ciudadanos y al sector privado, y 480 a infraestructuras críticas -aeropuertos, hospitales, centrales eléctricas o plantas de agua-, sólo en el primer trimestre de este año. España recibió 50.000 ciberataques, 247 en estructuras críticas. A ese ritmo, podríamos alcanzar las 150.000 ofensivas a finales de este año. El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% amenazas y coacciones.

"Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos. Muchas veces no valoramos lo que tenemos dentro de un dispositivo y no hacemos lo posible por protegerlo", explicó ayer José Antonio Nieto Ballesteros, secretario de Estado de Seguridad del Ministerio del Interior, en una jornada sobre Ciberseguridad organizada por el Club Diálogo para la Democracia.

El "negocio" es rentable. Actualmente supone cerca del 0,8% del PIB mundial, es decir, mueve más dinero que la mayoría de crímenes, como es el caso de tráfico de estupefacientes. Por la parte de la ciberseguridad también, alcanzando los 76.000 millones de euros al año del mundo. "La magnitud del problema está todavía lejos de entenderse por una mayoría. No se está respondiendo ni con la seriedad ni la contundencia que se

256
Millones de euros

Es el coste total de los ciberataques a empresas durante el último año, a nivel mundial. La mayoría de las empresas (52%) no disponen de ciberseguros.

115.000
Ciberataques

Detectados en España en 2016 por el Incibe. De los cuales, 110.000 afectaron a ciudadanos y al sector privado y 480 a centrales eléctricas, hospitales, aeropuertos, etc.

66.586
Denuncias

El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% fueron amenazas y coacciones.

debe", señaló Enrique Cabeiro Cabello, jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa. Es el gran problema de lo intangible, que hace que no terminemos de creerlo lo que no vemos.

Pero del virus hemos pasado a la epidemia y del pasado a la plaga. En diciembre de 2015, el trojan BlackEnergy provocó cortes en el suministro de electricidad a más de 600.000 hogares ucranianos en pleno invierno. Las ofensivas contra estructuras críticas son las más preocupantes. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. El pasado 12 de mayo, el incidente del ransomware Wannacry afectó a más de 25 hospitales. Ante la imposibilidad de acceder al sistema informático, muchos de ellos tuvieron que trasladar a pacientes graves a otros hospitales cercanos. En los dos últimos años, más de 4.000 ataques cibernéticos se identifican con el tipo ransomware -se caracteriza por secuestrar la información y



El dinero que mueven los ciberataques supone cerca del 0,8% del PIB mundial.

AUMENTO EXPONENCIAL DE CIBERATAQUES EN ESPAÑA



Fuente: INCIBE.

exigir un rescate. Se trata del principal malware en Europa. Wannacry afectó a más de 300.000 equipos de 180 países. En España, fueron 1.200 equipos. "La reacción fue rápida y se pudo controlar el impacto de manera inmediata", explicó ayer Antonio Gavilanes Dumont, presidente del Club Diálogo para la Democracia. El caso más sonado fue Telefónica, aunque José Luis Gilpérez, director ejecutivo

de Administraciones Públicas, Defensa, Seguridad y Big Data de Telefónica, aseguró ayer que "el impacto real de Wannacry ha sido cero". El grupo de telefonía aumentó sus ingresos en el área de seguridad un 22,7% en 2016, hasta 341 millones.

"Esto es un trabajo de todos los agentes públicos y privados", señaló Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Incibe.

Después del incidente, Reino Unido ha decidido invertir 13.000 millones de euros en ciberseguridad. En España no hay una partida definida de la Administración Pública, aunque Nieto aseguró que "tenemos herramientas para prevenirlo y una implicación altísima de los técnicos y de la iniciativa privada para conseguir que España sea una materia de seguridad virtual como lo es física".

El fiscal Moix renuncia por su empresa familiar en Panamá

Expansión, Madrid
Manuel Moix renunció ayer su cargo al frente de la Fiscalía Anticorrupción después de la polémica sobre su participación en una sociedad familiar radicada en Panamá, una decisión que aplaudieron las asociaciones de fiscalías que para la oposición llega tarde y es insuficiente. Con un mandato de tres meses, Moix se ha visto obligado a presentar su renuncia irrevocable después de esa última polémica, aunque su escaso trimestre en la dirección de la Fiscalía Anticorrupción no ha estado exento de críticas a su gestión desde un amplio espectro de lapolítica y la judicatura.

Ya se esperaba anteayer su renuncia, pero finalmente decidió hacerlo ayer. Ante el fiscal general del Estado, José Manuel Maza, dejó claro que él no habría pedido la dimisión y que en el comportamiento de Moix no ha existido "ninguna clase de ilegalidad, irregularidad o incompatibilidad". "Tras hablar con él, y puesto que ha insistido en que lo hace de manera irrevocable, no he podido conculcarle. Ha ejercido el cargo a plena satisfacción, pero no puedo obligar a quien alega motivos personales", justificó.

El diario *Infórbre* publicó que Moix posee el 25% de una sociedad constituida en el paraíso fiscal de Panamá en 1988 y propietaria de un chalé en Collado Villalba (Madrid) valorado en 550.000 euros. Moix y sus hermanos heredaron la sociedad tras el fallecimiento de sus padres y la han mantenido tras declararla a Hacienda. El fiscal dijo haberse enterado de la existencia de dicha sociedad cuando fallecieron sus padres, pero el mismo diario ha publicado datos que contradicen esa versión.

El Gobierno, que pasó del apoyo público a Maza al nombramiento de Moix como fiscal, Mariano Rajoy, ni se refirió ayer a él, dejó al ministro de Justicia, Rafael Catalá, la reacción al caso, en unas declaraciones en las que expresó su respeto por esa decisión "personal" a la vez que coincidió con Maza en sus apreciaciones.

Junto a Moix aspiraron en su día al puesto de jefe Anticorrupción: Belén Suárez, Antonio Romeral, María Teresa Gilber, Carlos Alba y Alejandro Luzzi, y es previsible que lo hagan de nuevo.

Los ciberataques se disparan: afectan ya a 3 de cada 4 empresas en España

CIBERSEGURIDAD España es el tercer país del mundo que más ataques informáticos recibe. En 2016 se detectaron 115.000 incidentes, de los que 480 afectaron a hospitales y aeropuertos, entre otros.

Imma Benedito Madrid

La ciberseguridad, igual que el cambio climático, es tan alarmante como intangible.

Tres decada cuatro empresas españolas ha sufrido un ciberataque en los últimos cinco años. Sin embargo, apenas el 3% tiene un plan de respuesta a incidentes de este tipo. A nivel mundial, el coste de los ciberataques a empresas asciende a un total de 265 millones de euros. En el caso de España, nos encontramos con que es el tercer país con más ofensivas a nivel mundial, después de Reino Unido y Estados Unidos.

La escalada es exponencial y, las cifras, alarmantes. En 2016, el Instituto Nacional de Seguridad (Incibe) detectó más de 115.000 ciberincidentes, de los cuales más de 110.000 afectaron a ciudadanos y al sector privado, y 480 a infraestructuras críticas -aeropuertos, hospitales, centrales eléctricas o plantas de agua-, sólo en el primer trimestre de este año. España recibió 50.000 ciberataques, 247 en estructuras críticas. A ese ritmo, podríamos alcanzar las 150.000 ofensivas a finales de este año. El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% amenazas y coacciones.

"Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos. Muchas veces no valoramos lo que tenemos dentro de un dispositivo y no hacemos lo posible por protegerlo", explicó ayer José Antonio Nieto Ballesteros, secretario de Estado de Seguridad del Ministerio del Interior, en unas jornadas sobre Ciberseguridad organizada por el Club Diálogos para la Democracia.

El "negocio" es rentable. Actualmente supone cerca del 0,8% del PIB mundial, es decir, mueve más dinero que la mayoría de crímenes, como es el caso de tráfico de estupefacientes. Por la parte de la ciberseguridad también, alcanzando los 76.000 millones de euros al año en el mundo. "La magnitud del problema está todavía lejos de entenderse por una mayoría. No se está respondiendo ni con la seriedad ni la contundencia que se

256
Millones de euros

Es el coste total de los ciberataques a empresas durante el último año, a nivel mundial. La mayoría de las empresas (52%) no disponen de ciberseguros.

115.000
Ciberataques

Detectados en España en 2016 por el Incibe. De los cuales, 110.000 afectaron a ciudadanos y al sector privado y 480 a centrales eléctricas, hospitales, aeropuertos, etc.

66.586
Denuncias

El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% fueron amenazas y coacciones.

debe", señaló Enrique Cabeiro Cabello, jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa. Es el gran problema de lo intangible, que hace que no terminemos de creerlo lo que no vemos.

Pero del virus hemos pasado a la epidemia y del pasado a la plaga. En diciembre de 2015, el trojan BlackEnergy provocó cortes en el suministro de electricidad a más de 600.000 hogares ucranianos en pleno invierno. Las ofensivas contra estructuras críticas son las más preocupantes. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. El pasado 12 de mayo, el incidente del ransomware WannaCry afectó a más de 25 hospitales. Ante la imposibilidad de acceder al sistema informático, muchos de ellos tuvieron que trasladar a pacientes graves a otros hospitales cercanos. En los dos últimos años, más de 4.000 ataques cibernéticos se identifican con el tipo ransomware -se caracteriza por secuestrar la información y



El dinero que mueven los ciberataques supone cerca del 0,8% del PIB mundial.

AUMENTO EXPONENCIAL DE CIBERATAQUES EN ESPAÑA



Fuente: INCIBE

exigir un rescate. Se trata del principal malware en Europa. WannaCry afectó a más de 300.000 equipos de 180 países. En España, fueron 1.200 equipos. "La reacción fue rápida y se pudo controlar el impacto de manera inmediata", explicó ayer Antonio Gavilanes Dumont, presidente del Club Diálogos para la Democracia. El caso más sonado fue Telefónica, aunque José Luis Gilpérez, director ejecutivo

de Administraciones Públicas, Defensa, Seguridad y Big Data de Telefónica, aseguró ayer que "el impacto real de WannaCry ha sido cero". El grupo de telefonía aumentó sus ingresos en el área de seguridad un 22,7% en 2016, hasta 341 millones.

"Esto es un trabajo de todos los agentes públicos y privados", señaló Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Incibe.

Después del incidente, Reino Unido ha decidido invertir 13.000 millones de euros en ciberseguridad. En España no hay una partida definida de la Administración Pública, aunque Nieto aseguró que "tenemos herramientas para prevenirlo y una implicación altísima de los técnicos y de la iniciativa privada para conseguir que España sea una materia de seguridad virtual como lo es física".

El fiscal Moix renuncia por su empresa familiar en Panamá

Expansión Madrid

Manuel Moix renunció ayer su cargo al frente de la Fiscalía Anticorrupción después de la polémica sobre su participación en una sociedad familiar radicada en Panamá, una decisión que aplaudieron las asociaciones de fiscalía que para la oposición llega tarde y es insuficiente. Con un mandato de tres meses, Moix se ha visto obligado a presentar su renuncia irrevocable después de esa última polémica, aunque su escaso trimestre en la dirección de la Fiscalía Anticorrupción no ha estado exento de críticas a su gestión desde un amplio espectro de la política y la judicatura.

Ya se esperaba anteayer su renuncia, pero finalmente decidió hacerlo ayer. Ante el fiscal general del Estado, José Manuel Maza, dejó claro que él no habría pedido la dimisión y que en el comportamiento de Moix no ha existido "ninguna clase de ilegalidad, irregularidad o incompatibilidad". "Tras hablar con él, y puesto que ha insistido en que lo hace de manera irrevocable, no he podido conculcarle. Ha ejercido el cargo a plena satisfacción, pero no puedo obligar a quien alega motivos personales", justificó.

El diario *Infórbre* publicó que Moix posee el 25% de una sociedad constituida en el paraíso fiscal de Panamá en 1988 y propietaria de un chalet en Collado Villalba (Madrid) valorado en 550.000 euros. Moix y sus hermanos heredaron la sociedad tras el fallecimiento de sus padres y la han mantenido tras declararla a Hacienda. El fiscal dijo haberse enterado de la existencia de dicha sociedad cuando fallecieron sus padres, pero el mismo diario ha publicado datos que contradicen esa versión.

El Gobierno, que pasó del apoyo público a Maza al apoyo "el presidente del Ejecutivo, Mariano Rajoy, ni se refirió ayer a él-, dejó al ministro de Justicia, Rafael Catalá, la reacción al caso, en unas declaraciones en las que expresó su respeto por esa decisión "personal" a la vez que coincidió con Maza en sus apreciaciones.

Junto a Moix aspiraron en su día al puesto de jefe Anticorrupción: Belén Suárez, Antonio Romeral, María Teresa Gilber, Carlos Alba y Alejandro Lonzani, y es previsible que lo hagan de nuevo.

Los ciberataques se disparan: afectan ya a 3 de cada 4 empresas en España

CIBERSEGURIDAD España es el tercer país del mundo que más ataques informáticos recibe. En 2016 se detectaron 115.000 incidentes, de los que 480 afectaron a hospitales y aeropuertos, entre otros.

Imma Benedito Madrid

La ciberseguridad, igual que el cambio climático, es tan alarmante como intangible. Tres decada cuatro empresas españolas ha sufrido un ciberataque en los últimos cinco años. Sin embargo, apenas el 37% tiene un plan de respuesta a incidentes de este tipo. A nivel mundial, el coste de los ciberataques a empresas asciende a un total de 265 millones de euros. En el caso de España, nos encontramos con que es el tercer país con más ofensivas a nivel mundial, después de Reino Unido y Estados Unidos.

La escalada es exponencial y, las cifras, alarmantes. En 2016, el Instituto Nacional de Seguridad (Incibe) detectó más de 115.000 ciberincidentes, de los cuales más de 110.000 afectaron a ciudadanos y al sector privado, y 480 a infraestructuras críticas -aeropuertos, hospitales, centrales eléctricas o plantas de agua-, sólo en el primer trimestre de este año. España recibió 50.000 ciberataques, 247 en estructuras críticas. A ese ritmo, podríamos alcanzar las 150.000 ofensivas a finales de este año. El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% amenazas y coacciones.

"Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos. Muchas veces no valoramos lo que tenemos dentro de un dispositivo y no hacemos lo posible por protegerlo", explicó ayer José Antonio Nieto Ballesteros, secretario de Estado de Seguridad del Ministerio del Interior, en unas jornadas sobre Ciberseguridad organizada por el Club Diálogo para la Democracia.

El "negocio" es rentable. Actualmente supone cerca del 0,8% del PIB mundial, es decir, mueve más dinero que la mayoría de crímenes, como es el caso de tráfico de estupefacientes. Por la parte de la ciberseguridad también, alcanzando los 76.000 millones de euros al año del mundo. "La magnitud del problema está todavía lejos de entenderse por una mayoría. No se está respondiendo ni con la seriedad ni la contundencia que se

256
Millones de euros

Es el coste total de los ciberataques a empresas durante el último año, a nivel mundial. La mayoría de las empresas (52%) no disponen de ciberseguros.

115.000
Ciberataques

Detectados en España en 2016 por el Incibe. De los cuales, 110.000 afectaron a ciudadanos y al sector privado y 480 a centrales eléctricas, hospitales, aeropuertos, etc.

66.586
Denuncias

El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% fueron amenazas y coacciones.

debe", señaló Enrique Cabeiro Cabello, jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa. Es el gran problema de lo intangible, que hace que no terminemos de creerlo lo que no vemos.

Pero del virus hemos pasado a la epidemia y del pasado a la plaga. En diciembre de 2015, el trojan BlackEnergy provocó cortes en el suministro de electricidad a más de 600.000 hogares ucranianos en pleno invierno. Las ofensivas contra estructuras críticas son las más preocupantes. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. El pasado 12 de mayo, el incidente del ransomware WannaCry afectó a más de 25 hospitales. Ante la imposibilidad de acceder al sistema informático, muchos de ellos tuvieron que trasladar a pacientes graves a otros hospitales cercanos. En los dos últimos años, más de 4.000 ataques cibernéticos se identifican con el tipo ransomware -se caracteriza por secuestrar la información y



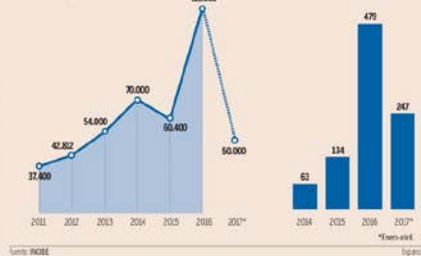
El dinero que mueven los ciberataques supone cerca del 0,8% del PIB mundial.

AUMENTO EXPONENCIAL DE CIBERATAQUES EN ESPAÑA

1 Ciberincidentes detectados

En número.

*Datos entre enero y abril.



Fuente: INCIBE.

exigir un rescate". Se trata del principal malware en Europa. WannaCry afectó a más de 300.000 equipos de 180 países. En España, fueron 1.200 equipos. "La reacción fue rápida y se pudo controlar el impacto de manera inmediata", explicó ayer Antonio Gavilanes Dumont, presidente del Club Diálogo para la Democracia. El caso más sonado fue Telefónica, aunque José Luis Gilpérez, director ejecutivo

de Administraciones Públicas, Defensa, Seguridad y Big Data de Telefónica, aseguró ayer que "el impacto real de WannaCry ha sido cero". El grupo de telefonía aumentó sus ingresos en el área de seguridad un 22,7% en 2016, hasta 341 millones.

"Esto es un trabajo de todos los agentes públicos y privados", señaló Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Incibe.

Después del incidente, Reino Unido ha decidido invertir 13.000 millones de euros en ciberseguridad. En España no hay una partida definida de la Administración Pública, aunque Nieto aseguró que "tenemos herramientas para prevenirlo y una implicación altísima de los técnicos y de la iniciativa privada para conseguir que España sea una materia de seguridad virtual como lo es física".

El fiscal Moix renuncia por su empresa familiar en Panamá

Expansión Madrid

Manuel Moix renunció ayer su cargo al frente de la Fiscalía Anticorrupción después de la polémica sobre su participación en una sociedad familiar radicada en Panamá, una decisión que aplaudieron las asociaciones de fiscalía que para la oposición llega tarde y es insuficiente. Con un mandato de tres meses, Moix se ha visto obligado a presentar su renuncia irrevocable después de esa última polémica, aunque su escaso trimestre en la dirección de la Fiscalía Anticorrupción no ha estado exento de críticas a su gestión desde un amplio espectro de lapolítica y la judicatura.

Ya se esperaba anteayer su renuncia, pero finalmente decidió hacerlo ayer. Ante el fiscal general del Estado, José Manuel Maza, dejó claro que él no habría pedido la dimisión y que en el comportamiento de Moix no ha existido "ninguna clase de ilegalidad, irregularidad o incompatibilidad". "Tras hablar con él, y puesto que ha insistido en que lo hace de manera irrevocable, no he podido conculcarle. Ha ejercido el cargo a plena satisfacción, pero no puedo obligar a quien alega motivos personales", justificó.

El diario *Infórbre* publicó que Moix posee el 25% de una sociedad constituida en el paraíso fiscal de Panamá en 1988 y propietaria de un chalet en Collado Villalba (Madrid) valorado en 550.000 euros. Moix y sus hermanos heredaron la sociedad tras el fallecimiento de sus padres y la han mantenido tras declararla a Hacienda. El fiscal dijo haberse enterado de la existencia de dicha sociedad cuando fallecieron sus padres, pero el mismo diario ha publicado datos que contradicen esa versión.

El Gobierno, que pasó del apoyo público a Mela Salvaterra al presidente del Ejecutivo, Mariano Rajoy, ni se refirió ayer a él, dejó al ministro de Justicia, Rafael Catalá, la reacción al caso, en unas declaraciones en las que expresó su respeto por esa decisión "personal" a la vez que coincidió con Maza en sus apreciaciones.

Junto a Moix aspiraron en su día al puesto de jefe Anticorrupción: Belén Suárez, Antonio Romeral, María Teresa Gilber, Carlos Alba y Alejandro Luzzi, y es previsible que lo hagan de nuevo.

Los ciberataques se disparan: afectan ya a 3 de cada 4 empresas en España

CIBERSEGURIDAD España es el tercer país del mundo que más ataques informáticos recibe. En 2016 se detectaron 115.000 incidentes, de los que 480 afectaron a hospitales y aeropuertos, entre otros.

Imma Benedito Madrid

La ciberseguridad, igual que el cambio climático, es tan alarmante como intangible. Tres decada cuatro empresas españolas ha sufrido un ciberataque en los últimos cinco años. Sin embargo, apenas el 3% tiene un plan de respuesta a incidentes de este tipo. A nivel mundial, el coste de los ciberataques a empresas asciende a un total de 265 millones de euros. En el caso de España, nos encontramos con que es el tercer país con más ofensivas a nivel mundial, después de Reino Unido y Estados Unidos.

La escalada es exponencial y, las cifras, alarmantes. En 2016, el Instituto Nacional de Seguridad (Incibe) detectó más de 115.000 ciberincidentes, de los cuales más de 110.000 afectaron a ciudadanos y al sector privado, y 480 a infraestructuras críticas -aeropuertos, hospitales, centrales eléctricas o plantas de agua-, sólo en el primer trimestre de este año. España recibió 50.000 ciberataques, 247 en estructuras críticas. A ese ritmo, podríamos alcanzar las 150.000 ofensivas a finales de este año. El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% amenazas y coacciones.

"Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos. Muchas veces no valoramos lo que tenemos dentro de un dispositivo y no hacemos lo posible por protegerlo", explicó ayer José Antonio Nieto Ballesteros, secretario de Estado de Seguridad del Ministerio del Interior, en unas jornadas sobre Ciberseguridad organizada por el Club Diálogo para la Democracia.

El "negocio" es rentable. Actualmente supone cerca del 0,8% del PIB mundial, es decir, mueve más dinero que la mayoría de crímenes, como es el caso de tráfico de estupefacientes. Por la parte de la ciberseguridad también, alcanzando los 76.000 millones de euros al año en el mundo. "La magnitud del problema está todavía lejos de entenderse por una mayoría. No se está respondiendo ni con la seriedad ni la contundencia que se

256
Millones de euros

Es el coste total de los ciberataques a empresas durante el último año, a nivel mundial. La mayoría de las empresas (52%) no disponen de ciberseguros.

115.000
Ciberataques

Detectados en España en 2016 por el Incibe. De los cuales, 110.000 afectaron a ciudadanos y al sector privado y 480 a centrales eléctricas, hospitales, aeropuertos, etc.

66.586
Denuncias

El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% fueron amenazas y coacciones.

debe", señaló Enrique Cabeiro Cabello, jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa. Es el gran problema de lo intangible, que hace que no terminemos de creerlo lo que no vemos.

Pero del virus hemos pasado a la epidemia y del pasado a la plaga. En diciembre de 2015, el trojan BlackEnergy provocó cortes en el suministro de electricidad a más de 600.000 hogares ucranianos en pleno invierno. Las ofensivas contra estructuras críticas son las más preocupantes. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. El pasado 12 de mayo, el incidente del ransomware WannaCry afectó a más de 25 hospitales. Ante la imposibilidad de acceder al sistema informático, muchos de ellos tuvieron que trasladar a pacientes graves a otros hospitales cercanos. En los dos últimos años, más de 4.000 ataques cibernéticos se identifican con el tipo ransomware -se caracteriza por secuestrar la información y



El dinero que mueven los ciberataques supone cerca del 0,8% del PIB mundial.

AUMENTO EXPONENCIAL DE CIBERATAQUES EN ESPAÑA



Fuente: INCIBE

exigir un rescate". Se trata del principal malware en Europa. WannaCry afectó a más de 300.000 equipos de 180 países. En España, fueron 1.200 equipos. "La reacción fue rápida y se pudo controlar el impacto de manera inmediata", explicó ayer Antonio Gavilanes Dumont, presidente del Club Diálogo para la Democracia. El caso más sonado fue Telefónica, aunque José Luis Gilpérez, director ejecutivo

de Administraciones Públicas, Defensa, Seguridad y Big Data de Telefónica, aseguró ayer que "el impacto real de WannaCry ha sido cero". El grupo de telefonía aumentó sus ingresos en el área de seguridad un 22,7% en 2016, hasta 341 millones.

"Esto es un trabajo de todos los agentes públicos y privados", señaló Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Incibe.

Después del incidente, Reino Unido ha decidido invertir 13.000 millones de euros en ciberseguridad. En España no hay una partida definida de la Administración Pública, aunque Nieto aseguró que "tenemos herramientas para prevenirlo y una implicación altísima de los técnicos y de la iniciativa privada para conseguir que España sea una materia de seguridad virtual como lo es física".

El fiscal Moix renuncia por su empresa familiar en Panamá

Expansión Madrid

Manuel Moix renunció ayer su cargo al frente de la Fiscalía Anticorrupción después de la polémica sobre su participación en una sociedad familiar radicada en Panamá, una decisión que aplaudieron las asociaciones de fiscalía que para la oposición llega tarde y es insuficiente. Con un mandato de tres meses, Moix se ha visto obligado a presentar su renuncia irrevocable después de esa última polémica, aunque su escaso trimestre en la dirección de la Fiscalía Anticorrupción no ha estado exento de críticas a su gestión desde un amplio espectro de lapolítica y la judicatura.

Ya se esperaba anteayer su renuncia, pero finalmente decidió hacerlo ayer. Ante el fiscal general del Estado, José Manuel Maza, dejó claro que él no habría pedido la dimisión y que en el comportamiento de Moix no ha existido "ninguna clase de ilegalidad, irregularidad o incompatibilidad". "Tras hablar con él, y puesto que ha insistido en que lo hace de manera irrevocable, no he podido conculcarle. Ha ejercido el cargo a plena satisfacción, pero no puedo obligar a quien alega motivos personales", justificó.

El diario *Infórbre* publicó que Moix posee el 25% de una sociedad constituida en el paraíso fiscal de Panamá en 1988 y propietaria de un chalet en Collado Villalba (Madrid) valorado en 550.000 euros. Moix y sus hermanos heredaron la sociedad tras el fallecimiento de sus padres y la han mantenido tras declararla a Hacienda. El fiscal dijo haberse enterado de la existencia de dicha sociedad cuando fallecieron sus padres, pero el mismo diario ha publicado datos que contradicen esa versión.

El Gobierno, que pasó del apoyo público a Michel Salvendy -el presidente del Ejecutivo, Mariano Rajoy, ni se refirió ayer a él-, dejó al ministro de Justicia, Rafael Catalá, la reacción al caso, en unas declaraciones en las que expresó su respeto por esa decisión "personal" a la vez que coincidió con Maza en sus apreciaciones.

Junto a Moix aspiraron en su día al puesto de jefe Anticorrupción: Belén Suárez, Antonio Romeral, María Teresa Gilber, Carlos Alba y Alejandro Luzzi, y es previsible que lo hagan de nuevo.

Los ciberataques se disparan: afectan ya a 3 de cada 4 empresas en España

CIBERSEGURIDAD España es el tercer país del mundo que más ataques informáticos recibe. En 2016 se detectaron 115.000 incidentes, de los que 480 afectaron a hospitales y aeropuertos, entre otros.

Imma Benedito, Madrid
La ciberseguridad, igual que el cambio climático, es tan alarmante como intangible. Tres decada cuatro empresas españolas ha sufrido un ciberataque en los últimos cinco años. Sin embargo, apenas el 37% tiene un plan de respuesta a incidentes de este tipo. A nivel mundial, el coste de los ciberataques a empresas asciende a un total de 265 millones de euros. En el caso de España, nos encontramos con que es el tercer país con más ofensivas a nivel mundial, después de Reino Unido y Estados Unidos.

La escalada es exponencial y, las cifras, alarmantes. En 2016, el Instituto Nacional de Seguridad (Incibe) detectó más de 115.000 ciberincidentes, de los cuales más de 110.000 afectaron a ciudadanos y al sector privado, y 480 a infraestructuras críticas -aeropuertos, hospitales, centrales eléctricas o plantas de agua-, sólo en el primer trimestre de este año. España recibió 50.000 ciberataques, 247 en estructuras críticas. A ese ritmo, podríamos alcanzar las 150.000 ofensivas a finales de este año. El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% amenazas y coacciones.

"Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos. Muchas veces no valoramos lo que tenemos dentro de un dispositivo y no hacemos lo posible por protegerlo", explicó ayer José Antonio Nieto Ballesteros, secretario de Estado de Seguridad del Ministerio del Interior, en unas jornadas sobre Ciberseguridad organizada por el Club Diálogo para la Democracia.

El "negocio" es rentable. Actualmente supone cerca del 0,8% del PIB mundial, es decir, mueve más dinero que la mayoría de crímenes, como es el caso de tráfico de estupefacientes. Por la parte de la ciberseguridad también, alcanzando los 76.000 millones de euros al año en el mundo. "La magnitud del problema está todavía lejos de entenderse por una mayoría. No se está respondiendo ni con la celeridad ni la contundencia que se

256
Millones de euros

Es el coste total de los ciberataques a empresas durante el último año, a nivel mundial. La mayoría de las empresas (52%) no disponen de ciberseguros.

115.000
Ciberataques

Detectados en España en 2016 por el Incibe. De los cuales, 110.000 afectaron a ciudadanos y al sector privado y 480 a centrales eléctricas, hospitales, aeropuertos, etc.

66.586
Denuncias

El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% fueron amenazas y coacciones.

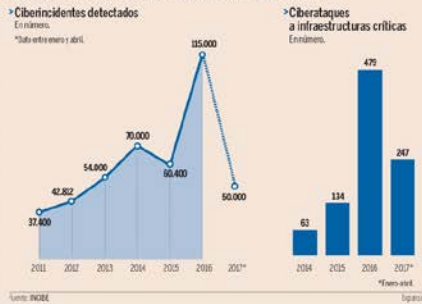
debe", señaló Enrique Cabeiro Cabello, jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa. Es el gran problema de lo intangible, que hace que no terminemos de creerlo lo que no vemos.

Pero del virus hemos pasado a la epidemia y del pasado a la plaga. En diciembre de 2015, el trojan BlackEnergy provocó cortes en el suministro de electricidad a más de 600.000 hogares ucranianos en pleno invierno. Las ofensivas contra estructuras críticas son las más preocupantes. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. El pasado 12 de mayo, el incidente del ransomware WannaCry afectó a más de 25 hospitales. Ante la imposibilidad de acceder al sistema informático, muchos de ellos tuvieron que trasladar a pacientes graves a otros hospitales cercanos. En los dos últimos años, más de 4.000 ataques cibernéticos se identifican con el tipo ransomware -se caracteriza por secuestrar la información y



El dinero que mueven los ciberataques supone cerca del 0,8% del PIB mundial.

AUMENTO EXPONENCIAL DE CIBERATAQUES EN ESPAÑA



Fuente: INCIPE.

exigir un rescate. Se trata del principal malware en Europa. WannaCry afectó a más de 300.000 equipos de 180 países. En España, fueron 1.200 equipos. "La reacción fue rápida y se pudo controlar el impacto de manera inmediata", explicó ayer Antonio Gavilanes Dumont, presidente del Club Diálogo para la Democracia. El caso más sonado fue Telefónica, aunque José Luis Gilpérez, director ejecutivo

de Administraciones Públicas, Defensa, Seguridad y Big Data de Telefónica, aseguró ayer que "el impacto real de WannaCry ha sido cero". El grupo de telefonía aumentó sus ingresos en el área de seguridad un 22,7% en 2016, hasta 341 millones.

"Esto es un trabajo de todos los agentes públicos y privados", señaló Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Incibe.

Después del incidente, Reino Unido ha decidido invertir 13.000 millones de euros en ciberseguridad. En España no hay una partida definida de la Administración Pública, aunque Nieto aseguró que "tenemos herramientas para prevenirlo y una implicación altísima de los técnicos y de la iniciativa privada para conseguir que España sea una materia de seguridad virtual como lo es física".

El fiscal Moix renuncia por su empresa familiar en Panamá

Expansión, Madrid
Manuel Moix renunció ayer su cargo al frente de la Fiscalía Anticorrupción después de la polémica sobre su participación en una sociedad familiar radicada en Panamá, una decisión que aplaudieron las asociaciones de fiscalía que para la oposición llega tarde y es insuficiente. Con un mandato de tres meses, Moix se ha visto obligado a presentar su renuncia irrevocable después de esa última polémica, aunque su escaso trimestre en la dirección de la Fiscalía Anticorrupción no ha estado exento de críticas a su gestión desde un amplio espectro de lapolítica y la judicatura.

Ya se esperaba anteayer su renuncia, pero finalmente decidió hacerlo ayer. Ante el fiscal general del Estado, José Manuel Maza, dejó claro que él no habría pedido la dimisión y que en el comportamiento de Moix no ha existido "ninguna clase de ilegalidad, irregularidad o incompatibilidad". "Tras hablar con él, y puesto que ha insistido en que lo hace de manera irrevocable, no he podido conculcarle. Ha ejercido el cargo a plena satisfacción, pero no puedo obligar a quien alega motivos personales", justificó.

El diario *Infórbre* publicó que Moix posee el 25% de una sociedad constituida en el paraíso fiscal de Panamá en 1988 y propietaria de un chalet en Collado Villalba (Madrid) valorado en 550.000 euros. Moix y sus hermanos heredaron la sociedad tras el fallecimiento de sus padres y la han mantenido tras declararla a Hacienda. El fiscal dijo haberse enterado de la existencia de dicha sociedad cuando fallecieron sus padres, pero el mismo diario ha publicado datos que contradicen esa versión.

El Gobierno, que pasó del apoyo público a Maza al nombramiento de Moix como presidente del Ejecutivo, Mariano Rajoy, ni se refirió ayer a él, dejó al ministro de Justicia, Rafael Catalá, la reacción al caso, en unas declaraciones en las que expresó su respeto por esa decisión "personal" a la vez que coincidió con Maza en sus apreciaciones.

Junto a Moix aspiraron en su día al puesto de jefe Anticorrupción: Belén Suárez, Antonio Romeral, María Teresa Gilber, Carlos Alba y Alejandro Lonzani, y es previsible que lo hagan de nuevo.

Cuponísimo
MÁS OFERTAS Y AHORROS

Compra esta oferta y muchas más en:
cuponismo.laprovincia.es



Amorlie
MÁS AHORROS

RECUPERA LA JUVENTUD DE TU ROSTRO CON 1 O 3 SESIONES DE MASAJE FACIAL RELAJANTE O EFECTO LIFTING CON AROMATERAPIA CDESD 25€

25€ **RECUPERA LA JUVENTUD DE TU ROSTRO CON 1 O 3 SESIONES DE MASAJE FACIAL RELAJANTE O EFECTO LIFTING CON AROMATERAPIA CDESD 25€**

¡No lo dudes, entra ya y no te quedes sin esta oferta!

cuponismo.laprovincia.es

Reservar esta oferta en:
Cuponismo.laprovincia.es
Para publicar tus ofertas:
comunicacion@cuponismo.laprovincia.es
91 353 81 93

Cuponísimo LA PROVINCIA

Ecología

Suman 10.000 firmas para declarar El Hierro Parque Nacional Marino

La organización ecologista World Wildlife Fund destaca la riqueza biológica de la zona y el compromiso por la sostenibilidad de la isla

LA PROVINCIA / DLP

World Wildlife Fund (WWF) sumó los grandes grupos ecologistas del planeta, hasta un total de más de 10.000 firmas para declarar en El Hierro el primer Parque Nacional Marino de España.

En las aguas de El Hierro, vertidas por la WWF para salvaguardar Parque Nacional marino, se pueden encontrar más de 12 especies de peces, moluscos, crustáceos, aves marinas, mamíferos marinos y plantas acuáticas.

Paralelamente se dio a conocer la WWF también destacó los acantilados volcánicos de más de mil metros de altura que se encuentran en El Hierro como hasta los tres kilómetros de profundidad, que como atestiguan fotos aéreas y que contienen este paisaje submarino tan único como el que se encuentra en su superficie donde se encuentran monumentos herpetológicos y de gran interés que se encuentran en la zona de la zona de El Hierro, Canarias.

Ciencia



El avión más grande del mundo

Symantec y el avión más grande del mundo creado por Paul Allen, cofundador de Microsoft, se han dado la mano para crear el avión más grande del mundo, el Boeing 747-8, que será el más grande del mundo.

Tecnología

Alianzas contra el ciberataque

Seguridad organizada por el Club Diálogos para la Democracia y Telefónica, en la que han señalado que "la resiliencia digital, la capacidad para volver a la normalidad y restaurar la operatividad de un sistema tras un ataque, es tan importante como la prevención".

Tecnología

Alianzas contra el ciberataque

Efe

MADRID

A la hora de afrontar un ciberataque no hay una "tecnología mágica", sino que hace falta una industria que trabaje de manera coordinada, con alianzas entre fabricantes y con información compartida, o "la batalla estará perdida de antemano". Así lo han señalado varios expertos en la jornada sobre ciber-

seguridad organizada por el Club Diálogos para la Democracia y Telefónica, en la que han señalado que "la resiliencia digital, la capacidad para volver a la normalidad y restaurar la operatividad de un sistema tras un ataque, es tan importante como la prevención".

Así lo suscribió el director general de Symantec para el sur de Europa, Miguel Ángel Martos, quien ha apostillado que "el mayor riesgo

es no saber cómo gestionar un ataque". Por ello, la responsable de McAfee en España, María Campos, ha hecho hincapié en actuar "puntos estratégicos", a través de la protección de terminales como ordenadores, teléfonos inteligentes o tabletas, pues el aumento del número de ataques a través de *ransomware* -secuestro de datos- obliga a contar con "un plan de defensa para remediar posibles ataques".



PROTAGONISTAS DEL DÍA



Norman Foster
Arquitecto



Solange
Cantante



Carlos Saura
Cineasta



Ariana Grande
Cantante

TENDENCIAS
CIENCIA
CULTURA
OCIO

Defendió ayer el diseño y las tecnologías limpias como "la clave del futuro" durante la inauguración del foro *Future is now*, con el que su fundación dio ayer por inaugurado su aterrizaje en la capital.

El Fórum de Barcelona abrió ayer sus puertas a la primera jornada oficial del Primavera Sound, que cuenta con la reina del neo-soul Solange o el talento de Bon Iver como principales atractivos.

Señaló que "no es ningún dictador a la hora de trabajar en el cine", ya que a su juicio, "los actores son personas muy frágiles en general" y que por ello, "hay que tratarlos con sumo cariño y cuidado".

Las entradas para el concierto benéfico en Mánchester que la cantante pop y otros artistas internacionales ofrecerán el domingo en recuerdo de las víctimas del atentado se vendieron en 20 minutos.

VIERNES
02 DE JUNIO DE 2017

EL CORREO GALLEGO

39

Las ciberamenazas no son "un cuento chino", 3 de 4 empresas son atacadas

Solo en los primeros tres meses de 2017, las denuncias subieron un 22,3% respecto al primer trimestre del pasado año

MARÍA ABASCAL
Madrid/Santiago

Altos mandos de Defensa y expertos en ciberseguridad dieron ayer un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberatque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo *ransomware* WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diplomáticos para la Democracia.

De desafío "muy serio y real" tidaron todos los especialistas estas ciberamenazas en cuyo lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado.

Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los

ponentes. Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7% más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3% respecto al primer trimestre del pasado año, lo que demuestra que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, lanzó una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la



“

"El ataque del WannaCry ha sido una muestra de que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional"

Enrique Cubeiro
ESTADO MAYOR DE LA DEFENSA

“

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes. El WannaCry fue facilon"

Marcos Gómez
INCIBE

EL DÍAS, JORNADA EN SANTIAGO

●●● El Colexio Profesional de Enxeñaría en Informática de Galicia (CPEIG) reunirá el 8 de junio, bajo el patrocinio de Emetel y la colaboración de Abanca y Symantec, un elenco de expertos en ciberseguridad. La II Jornada de Ciberseguridad en Galicia. Protoceno os Nosos Activos, pondrá a la comunidad gallega a la vanguardia de una de las principales preocupaciónes actuales del empresariado, administracións e particulares.

●●● La jornada -abierto previa inscripción-, comenzará a las 10 horas con una bienvenida institucional en la que participarán el presidente del CPEIG, Fernando Suárez, la directora de la Antega, Mar Pereira; el director general de Emetel, Manuel Lago; y Roberto Baratta, Global Executive VP and director of Loss Prevention, Business Continuity and Security de Abanca.

UE, no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, explicó Cubeiro.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no

dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8% del PIB mundial, ha resultado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (Incibe), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", avisó Gómez, que ha definido el virus WannaCry como "facilon", lo que permitió en pocas horas conocer "lo que hacia el bicho" y fabricar una vacuna.

dejar lugar a dudas: el ciberdelito supone ya cerca del 0,8% del PIB mundial, ha resultado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (Incibe), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

Viernes, 2 de junio de 2017

Diario de Teruel 33
+SOCIEDAD

El verano será más cálido de lo normal en casi toda España

El verano será más cálido de lo normal en casi toda España, más concretamente en las Península y el Baleares, según el informe de la Agencia Estatal de Meteorología (AEMET)...

Sin embargo, en las Islas Canarias las temperaturas se mantendrán dentro de lo normal, según el informe...

Respecto a las lluvias, pronostica una estación bastante "irregular" en cuanto a la cantidad de precipitaciones...

El informe también indica que el período de lluvias será más corto de lo normal, con un inicio de lluvias en mayo...

El verano será más cálido de lo normal en casi toda España, más concretamente en las Península y el Baleares...

El informe también indica que el período de lluvias será más corto de lo normal...

Respecto a las lluvias, pronostica una estación bastante "irregular" en cuanto a la cantidad de precipitaciones...

Sin embargo, en las Islas Canarias las temperaturas se mantendrán dentro de lo normal...

El informe también indica que el período de lluvias será más corto de lo normal...

Respecto a las lluvias, pronostica una estación bastante "irregular" en cuanto a la cantidad de precipitaciones...

Sin embargo, en las Islas Canarias las temperaturas se mantendrán dentro de lo normal...

El informe también indica que el período de lluvias será más corto de lo normal...

Respecto a las lluvias, pronostica una estación bastante "irregular" en cuanto a la cantidad de precipitaciones...

Sin embargo, en las Islas Canarias las temperaturas se mantendrán dentro de lo normal...

El informe también indica que el período de lluvias será más corto de lo normal...

Respecto a las lluvias, pronostica una estación bastante "irregular" en cuanto a la cantidad de precipitaciones...

Sin embargo, en las Islas Canarias las temperaturas se mantendrán dentro de lo normal...

El informe también indica que el período de lluvias será más corto de lo normal...

Respecto a las lluvias, pronostica una estación bastante "irregular" en cuanto a la cantidad de precipitaciones...

Sin embargo, en las Islas Canarias las temperaturas se mantendrán dentro de lo normal...

El informe también indica que el período de lluvias será más corto de lo normal...

Respecto a las lluvias, pronostica una estación bastante "irregular" en cuanto a la cantidad de precipitaciones...

Sin embargo, en las Islas Canarias las temperaturas se mantendrán dentro de lo normal...

El informe también indica que el período de lluvias será más corto de lo normal...

Respecto a las lluvias, pronostica una estación bastante "irregular" en cuanto a la cantidad de precipitaciones...

Sin embargo, en las Islas Canarias las temperaturas se mantendrán dentro de lo normal...

El informe también indica que el período de lluvias será más corto de lo normal...



Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Yoyos y trenes eléctricos desbancan a drones y robots como los juguetes de moda

La más alta tecnología no ha podido barrer del mapa a la madera y el colorido plástico de algunos productos

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

Algunos de los juguetes en el stand de Teruel en la feria del juguete de Salamanca.

#Antetodotú: campaña contra las drogas de los rehabilitados

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

El Ministerio de Sanidad...

Tres de cada cuatro empresas reciben ciberataques

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

Tres de cada cuatro empresas reciben ciberataques

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

El estudio...

MAYCO advertisement listing services like 'Regeneración y soluciones en control de cables, camiones y tractores' and 'Máx potencia, menos consumo y ahorro de DTC'.

Tres de cada cuatro empresas reciben ciberataques

últimas víctimas hace apenas quince días, a través de un ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que sirvió para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia. De desafío "muy serio y real" tildaron todos los especialistas...

estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, reveló uno de los ponentes. Antes, el secretario de Estado de Seguridad, José Antonio Nieto, inauguró el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000. Solo en los primeros tres meses, las denuncias se han incrementado un 22,3 % respecto al primer trimestre del pasado año, lo que demuestra que las empresas tienden a denunciar más.



Medios Online



José Antonio Nieto afirma que "España es un referente en la lucha contra el terrorismo yihadista"

Ministerio del Interior

Madrid, 01/06/2017

Imágenes (5) Vídeos (0) Audios (0)



El secretario de Estado de Seguridad participa en una conferencia sobre ciberseguridad en el Club Diálogos para la Democracia



El secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado en Madrid una jornada sobre ciberseguridad, organizada por el Club Diálogos para la Democracia

Nieto ha informado sobre el incremento de la ciberdelincuencia en España que ha crecido un 22,3% en el primer trimestre del 2017 respecto al mismo periodo del año anterior

Ha subrayado que "debemos utilizar la revolución digital en beneficio de la sociedad y que España cuenta con las herramientas y profesionales necesarios para conseguir que nuestro país sea referente en materia de ciberseguridad como ya lo es en el terreno físico"

El secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado esta mañana en Madrid, una jornada sobre ciberseguridad, organizada por el Club Diálogos para la Democracia. Foro en el que Nieto se ha referido a la "revolución digital" en el mundo, los retos en materia de ciberseguridad así como los riesgos que este desarrollo conlleva y que, ha asegurado, "supone un cambio en el paradigma de muchos aspectos, y en concreto, en el de la seguridad".

El secretario de Seguridad ha afirmado que "España es un referente para otros países en la lucha contra el terrorismo yihadista y que se está trabajando de forma intensa para que también lo sea en el terreno virtual. Tenemos -ha añadido- las herramientas necesarias y la implicación de nuestros profesionales para que nuestro país también sea referencia en materia de seguridad virtual". Por ello, ha señalado que "el mundo está virando hacia una nueva realidad y que debemos aprovechar esta revolución digital en beneficio del hombre. Consolidar la sociedad del conocimiento y potenciar el uso de internet en educación, para generar empleo y no convertir su uso en una amenaza".

Respecto a los datos de ciberdelincuencia en España, José Antonio Nieto ha destacado el crecimiento "imparable y exponencial" de este tipos de delitos que en 2016 ascendió a 66.586. lo que supone un 10,7% más que en 2015. En concreto, ha detallado que las tipologías predominantes fueron fraudes y estafas (68,9%) y, amenazas y coacciones (17,2%). En este contexto, ha explicado que la evolución de los ciberdelitos en España durante el primer trimestre de 2017 sigue la tendencia al alza al haber aumentado en un 22,3% la actividad delictiva en el ciberespacio con respecto al mismo periodo del año anterior.

Un incremento de la ciberdelincuencia que, según Nieto, "es preocupante pero tranquilizador al mismo tiempo ya que la afloración de este tipo de delitos facilita la denuncia y nos permite conocerlos más a fondo para combatirlos con más contundencia".

Giro estratégico de Daesh en las Redes Sociales

El secretario de Estado de Seguridad ha destacado que hasta hace poco no se hablaba de ciberterrorismo, y que es "Daesh quien descubre la potencialidad de la Red para explotar su mensaje de terror, consiguiendo así convertir el terrorismo en un fenómeno viral". Sin embargo, ha subrayado que la acción internacional combinada de los servicios de seguridad e inteligencia así como de las empresas de Internet ha obligado a Daesh a gestionar su propio espacio en el ciberespacio. En este sentido, ha advertido sobre "el giro estratégico" de esta organización terrorista en las Redes Sociales, que ha explicado, está empezando a desarrollar sus propias plataformas, en concreto, una página web que imita a Facebook.

Respecto a la lucha contra el terrorismo yihadista en España, el secretario de Estado de Seguridad ha afirmado que "casi en la totalidad de los casos es lucha contra el ciberterrorismo. Nosotros -ha dicho- no esperamos que se produzca un atentado porque las operaciones y detenciones se producen con carácter preventivo". En este contexto, ha destacado que desde el 11 de marzo de 2004 las Fuerzas y Cuerpos de Seguridad han realizado 230 operaciones que se han saldado con 771 detenidos y, que en lo que llevamos de Legislatura, ya son 50 las operaciones efectuadas y 81 los detenidos.

En este foro, en el que José Antonio Nieto ha desgarnado las claves de España para dar respuesta a los "retos ciber", ha puesto de relieve el incremento de la cooperación entre todas las administraciones públicas, así como el esfuerzo conjunto con el sector privado que, según Nieto, ha generado una "confianza mutua" que está permitiendo aflorar este tipos de delitos. Asimismo, ha destacado la cooperación con la sociedad civil, la comunidad educativa y el sector de las ONG.s que "nos ayuda a mentalizar a la sociedad ante la nueva realidad virtual y así combatir y prevenir las actividades delictivas en el ciberespacio".



Date: 01/06/2017
Medio: EFE

INTERIOR CIBERSEGURIDAD

Interior descarta implantar el voto electrónico por la creciente ciberdelincuencia

EFE | Madrid | 1 jun. 2017



El secretario de Estado de Seguridad, José Antonio Nieto, ha asegurado hoy que la implantación del voto electrónico es un "riesgo" que España no debe asumir ante la creciente amenaza de la ciberdelincuencia, a pesar de contar con la tecnología para cambiar el sistema de votación.

En la inauguración de una jornada sobre ciberseguridad organizada por el Club de Diálogos para la Democracia y Telefónica, Nieto ha dejado claro que hoy por hoy el voto en papel para unas elecciones ofrece "más garantías" que el electrónico.

CIBERSEGURIDAD



Los expertos piden alianzas contra los ciberataques

A la hora de afrontar un ciberataque no hay una "tecnología mágica", sino que hace falta una industria que trabaje de manera coordinada, con alianzas entre fabricantes y con información compartida, o "la batalla estará perdida de antemano".



Recurso de Archivo de una Conferencia sobre ciberseguridad nacional. EFE/Walf Hirschberger

Así lo han señalado varios expertos en la jornada sobre ciberseguridad organizada por el Club Diálogos para la Democracia y Telefónica, en la que han señalado que "la resiliencia digital", la capacidad para volver a la normalidad y restaurar la operatividad de un sistema tras un ataque, "es tan importante como la prevención".

"La resiliencia es tan importante como la prevención", ha asegurado el director general de Symantec para el sur de Europa, Miguel Ángel Martos, quien ha apostillado que "el mayor riesgo es no saber cómo gestionar un ataque".

Por ello, la responsable de la compañía McAfee en España, María Campos, ha hecho hincapié en actuar en "puntos estratégicos", a través de la protección de terminales como ordenadores, teléfonos inteligentes o tabletas.

Alianzas contra los ciberataques

En su opinión, el aumento del número de ataques a través de **ransomware** -secuestro de datos- obliga a centros e instituciones que manejan grandes bases de datos a contar con "un plan de defensa para responder y remediar posibles ataques".

Y es que "no existe una tecnología mágica", sino que hay que integrar varias medidas y herramientas en las soluciones, así como "una industria que trabaje de forma coordinada", con alianzas con fabricantes y compartiendo información contra los **'malwares'** y sus variantes, o, de lo contrario, "la batalla estará perdida de antemano", según Campos.

La digitalización empresarial ha sido otro de los temas debatidos en este encuentro, en el que el director comercial de grandes cuentas en **Fortinet**, Luis Miguel Garrido, ha subrayado que "nuestros datos van cada vez más a 'la nube', donde existen espacios con poco control".

En este sentido, Garrido ha destacado el correo electrónico como una de los principales frentes por los que un usuario o empresa pueden ser atacados, que "deben ser consciente del riesgo que entrañan las URL o los ficheros desconocidos".

Por su parte, el socio de **Audertis**, Óscar Bou, ha incidido en la importancia de los certificados de seguridad, "una garantía de confianza" que debe acreditar cualquier proveedor que quiera trabajar con la administración pública.

Finalmente, el socio de **Consultoría Tecnológica e Innovación de Grant Thornton**, Luis Pastor, ha recordado la importancia de la formación, capacitación y concienciación de los usuarios "para que se conviertan en una barrera, en lugar de un consumidor vulnerable". [EFE tec](#)

Interior descarta implantar el voto electrónico por el peligro de manipulación del resultado electoral

Publicado 01/06/2017 11:35:21 GMT

Ministerio Del Interior Ciberseguridad

Las denuncias por ciberdelitos crecieron un 22,3% en el primer trimestre de 2017 respecto a 2016

MADRID, 1 Jun. (EUROPA PRESS) -

El Ministerio del Interior no se plantea poner en marcha el voto electrónico en España debido al alto riesgo que existe de sufrir un ciberataque y que el resultado electoral sea manipulado, según ha revelado este jueves el secretario de Estado de Seguridad, José Antonio Nieto.

En una jornada sobre ciberseguridad, Nieto ha expuesto cómo ha cambiado la sociedad debido al uso de Internet y ha puesto como ejemplo el ámbito electoral. Según ha reconocido, las campañas electorales "no se entenderían" actualmente sin el mundo virtual, pero ello conlleva también peligros que hacen que Interior no se plantee implantar sistemas electrónicos de votación.

"Hoy estamos más lejos del voto electrónico que hace diez años porque es muy manipulable", ha confesado haciendo hincapié en que "muy pocos se atreven a garantizar la seguridad y veracidad" del resultado y se trata de "un riesgo" que, a su juicio, España "no debe asumir".

La Junta Electoral Central (JEC) recomendó hace ya siete años al Gobierno el estudio de sistemas que permitiesen en uso de sistemas electrónicos para los procesos electorales, pero Nieto ha insistido en que el incremento de los ataques cibernéticos durante los últimos años hace que se trate de un avance que no esté en la agenda a corto plazo. "La tradicional papeleta sigue siendo más segura", ha defendido.



ARTÍCULO RELACIONADO

El PSOE lleva al próximo Pleno del Congreso otra reprobación, esta vez la del 'número dos' de Interior

CRECIMIENTO DEL 22,3% EN 2017

Los denominados ciberdelitos presentan un incremento exponencial año tras año. Las denuncias por este tipo de ataques en España durante el primer trimestre de 2017 crecieron un 22,3 por ciento respecto al año anterior, según ha expuesto el secretario de Estado, que ha revelado que en 2016 se detectaron un total de 66.586 ciberdelitos, un 10,7 por ciento más que en 2015.

Estos datos son ligeramente superiores a los del conjunto de la Unión Europea porque los españoles aún deben concienciarse de la necesidad de la protección en Internet, ha explicado el secretario de Estado, que sin embargo ha destacado como aspecto favorable el aumento de las denuncias.

Nieto ha comparado esta situación con la de la violencia de género, donde sólo se denuncian el 20 por ciento de las agresiones existentes y el objetivo es aumentar estas denuncias. "La evolución del primer trimestre de los ciberdelitos denunciados muestra una tendencia al alza, pero también un aumento de las denuncias", ha celebrado.

trimestre de 2017 crecieron un 22,3 por ciento respecto al año anterior, según ha expuesto el secretario de Estado, que ha revelado que en 2016 se detectaron un total de 66.586 ciberdelitos, un 10,7 por ciento más que en 2015.

Estos datos son ligeramente superiores a los del conjunto de la Unión Europea porque los españoles aún deben concienciarse de la necesidad de la protección en Internet, ha explicado el secretario de Estado, que sin embargo ha destacado como aspecto favorable el aumento de las denuncias.

Nieto ha comparado esta situación con la de la violencia de género, donde sólo se denuncian el 20 por ciento de las agresiones existentes y el objetivo es aumentar estas denuncias. "La evolución del primer trimestre de los ciberdelitos denunciados muestra una tendencia al alza, pero también un aumento de las denuncias", ha celebrado.

Los delitos cibernéticos fueron centro de atención tras el ataque sufrido por más de 180 países el pasado 12 de mayo, al que el "número dos" del Ministerio de Interior ha asegurado que España reaccionó de forma "rápida y ágil" haciendo posible que sus efectos fueran "bastante limitados".

Según ha expuesto, la ciberdelincuencia permite la deslocalización del delito, la multiplicación exponencial de sus efectos, la ocultación del delincuente y la dificultad de la labor policial y judicial. Además, al tener casi siempre un carácter internacional, exige una cooperación policial y judicial entre países que hace "más lentas" las operaciones.

DAEHS MULTIPLICA SU ESFUERZO EN INTERNET

Uno de los focos de atención en el mundo de los delitos cibernéticos es el del terrorismo, sobretodo después de que Daesh haya demostrado una gran agilidad en su manejo para la captación y adoctrinamiento a través de las redes sociales y "la expansión de su mensaje de odio".

"El mal se desarrolla bien en las redes sociales", ha reconocido Nieto, que ha explicado que Internet ha propiciado durante los últimos años una multiplicación de su mensaje que "no tiene precedentes". Y ha expuesto que, al mismo ritmo que los terroristas pierden territorio físico en Siria o Irak están "duplicando" su esfuerzo en el mundo virtual.

En este ámbito también ha asegurado que España ha desarrollado un trabajo "de éxito", que demuestra el hecho de que todas las operaciones contra el terrorismo yihadista tuvieron su origen en seguimientos hechos en Internet. En esta legislatura, las operaciones antiterroristas se han saldado con un total de 81 detenidos.

Jefe militar de ciberdefensa alerta de su importancia para la supervivencia de una nación

Publicado 01/06/2017 13:02:00 CET

Ciberseguridad Fuerzas Armadas

MADRID, 1 Jun. (EUROPA PRESS) -

El Jefe de Operaciones del Mando Conjunto de Ciberdefensa, el capitán de navío Enrique Cubeiro, ha sostenido este jueves que la ciberdefensa y la ciberseguridad son "esenciales" para la "supervivencia" de una nación y ha alertado de que "a día de hoy" son las capacidades "más críticas".

En unas jornadas sobre ciberseguridad organizadas por el Club Diálogo para la Democracia y Telefónica, el capitán de navío ha reconocido que se están haciendo "esfuerzos" por mejorar las capacidades en esta materia, pero cree que la magnitud del problema está aún lejos de ser entendida por una gran mayoría de personas, muchas de ellas con altos cargos de responsabilidad.

En el caso de las empresas privadas, ha avisado de que deben tomar conciencia de que las mayores vulnerabilidades para su continuidad pueden llegar a través del ciberespacio. Y se ha preguntado por qué se acepta "con facilidad" invertir en seguridad física pero cuesta hacerlo en ciberseguridad. "¿Por dónde es más fácil que llegue un ataque? ¿a través de la valla o del ciberespacio?", ha preguntado.

Cubeiro ha apuntado que tres de cada cuatro empresas han sido objeto de un ciberataque durante los últimos cinco años y las pérdidas sufridas por ellos superan ya a las que provoca el crimen internacional, siendo "mortales" para muchas pequeñas y medianas empresas.

Por todo ello, ha pedido dejar de ver a los expertos en ciberseguridad y ciberdefensa como "los tipos raritos del cuarto sótano" o "cazafantasmas que persiguen figuras esotéricas" y ha defendido que se trata de un ámbito que requiere de recursos económicos y una importante masa de personal cualificado.

"Unas sólidas capacidades en ciberseguridad y ciberdefensa resultan esenciales para, no sólo la seguridad de una nación, sino incluso para su supervivencia --ha alertado--. Y a día de hoy son las más críticas".

En este punto, ha reconocido que el ataque sufrido por 180 países el pasado 12 de mayo a través del virus WannaCry puede incluso haber sido "bueno" para los expertos en este ámbito, ya que ha ayudado a concienciar sobre su importancia. "Aunque parezca increíble todavía hay personas, algunas en puestos estratégicos, que siguen considerando esto de las ciberamenazas un cuento chino", ha lamentado.

El capitán de navío ha recordado que se trata de un asunto reconocido como uno de los principales riesgos para la seguridad de la nación, pero aún no se ha culminado "ese gran paso que va de las palabras a los hechos".

ARTICULO RELACIONADO

< >

El A400M, el mayor avión de carga militar de las Fuerzas Armadas, alcanza 100 horas de vuelo con el Ejército del Aire

30 Mayo 2017

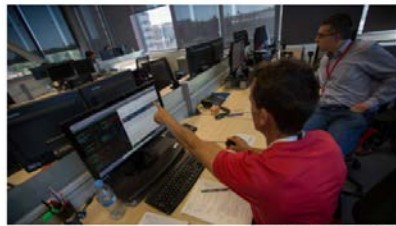
España "gasta más en vallas" que en ciberseguridad

Autoridades nacionales especializadas en la protección del ciberespacio reclaman más presupuesto para afrontar las amenazas en Internet



JULIANA OLIVERA

1 JUN 2017 - 16:33 CEST



Sede del Incibe, en León. VÍCTOR SANZ

Las denuncias por ciberdelitos en España aumentaron un 22,3% en el primer trimestre de 2017 respecto al mismo periodo del año pasado y [los ataques a infraestructuras estratégicas del Estado se han multiplicado por siete en dos años](#), según los datos del Instituto Nacional de Ciberseguridad (Incibe). El 25% del total de usuarios ha sufrido algún tipo de ciberataque, un porcentaje ligeramente superior a la media europea (21%), asegura Eurostat. A pesar de los alarmantes datos, algunas autoridades nacionales en el tema han advertido este jueves, durante una jornada sobre seguridad en Internet celebrada en Madrid, de que España no cuenta con el presupuesto adecuado para afrontar ese tipo de amenazas. Tres de cada cuatro empresas han sido atacadas en los últimos cinco años, según datos del Incibe.

Enrique Cubeiro, jefe de Operaciones del Mando Conjunto de Ciberdefensa, ha lamentado durante el encuentro que el país invierte en seguridad física, pero no en el ciberespacio. "Se invierte más en vallas que en ciberseguridad. ¿De dónde creen que vendrá el próximo ataque, de la valla o de un firewall? No se está respondiendo a esa amenaza ni con la agilidad ni con la contundencia que hace falta. Parece que están esperando a que pase algo más grave", ha lamentado al recordar el ataque a Estonia en 2007, cuando un grupo de hackers rusos paralizó los servicios básicos del país.

Con 116.000 incidencias registradas por el Incibe en 2016, España es el tercer país que más ciberataques sufre, por detrás de Estados Unidos y Reino Unido. El Gobierno británico destina aproximadamente 2.300 millones de euros para los programas de seguridad en Internet, según [los datos de 2016](#), y el [actual presupuesto estadounidense](#) para combatir esa amenaza es de 1.500 millones de dólares. El proyecto de los Presupuestos Generales del Estado de 2017 indica que el Gobierno pretende dedicar [24,3 millones de euros al Incibe](#) y 161 millones de euros al Centro Nacional de Inteligencia (CNI) para reforzar la ciberseguridad, según afirmó el pasado martes en el Pleno del Congreso la vicepresidenta del Gobierno y ministra de la Presidencia, Soraya Sáenz de Santamaría.

El secretario de Seguridad del Ministerio del Interior, José Antonio Nieto Ballesteros, que también ha participado en la jornada, ha señalado que no conoce una cifra exacta de cuánto invierte el país en ciberseguridad, porque es "un tema que está disperso en varias partidas" y ha hecho hincapié en la calidad del trabajo realizado por el Incibe y el Centro Criptológico Nacional (CCN), dependiente del CNI. "Aunque no tengamos un presupuesto de miles de millones, como Reino Unido, seguiremos haciendo lo mejor que podamos", ha afirmado.

La gestión de WannaCry

A pesar de las críticas a la falta de recursos, los expertos han destacado la actuación de las instituciones competentes en España frente al ataque global provocado por el virus WannaCry el pasado 12 de mayo, un [ransomware \(cibersecuestro\)](#) que afectó a 180 países. Nieto Ballesteros ha sostenido que la reacción fue "rápida y ágil", lo que evitó que "pasara lo mismo que en Reino Unido", donde el [ciberataque paralizó 16 hospitales](#).

Luis Jiménez Muñoz, subdirector del CCN, ha advertido, sin embargo, que parte del éxito se debió a que WannaCry era un *malware* "facilón". "Pudimos hacer una *pseudovacuna* contra ese virus en pocas horas para limitar el impacto, pero de haber sido [un software malicioso] más complejo, España hubiese sufrido más. Hemos sobrevivido, pero hay que invertir más recursos en ese tema", ha sostenido.

Para Cubeiro, quien considera que la ciberdefensa es "esencial para la supervivencia de la nación", el WannaCry sirvió para visualizar el problema de las amenazas en internet. "Mucha gente en los altos mandos estratégicos todavía ve el asunto como un cuento chino, pero la ciberseguridad es una de las capacidades más críticas para un Estado actualmente", dijo. El jefe militar ha pedido que las autoridades dejen de ver a los expertos en ese tema como "los tipos raritos del cuarto sótano" y ha defendido que ese ámbito requiere recursos económicos y más personal cualificado.

EL VOTO ELECTRÓNICO, DESCARTADO

J.O.

El secretario de Estado de Seguridad, José Antonio Nieto Ballesteros, ha afirmado que el Gobierno descarta implantar el voto electrónico debido al aumento de la ciberdelincuencia, a pesar de contar con la tecnología necesaria para hacerlo. Nieto Ballesteros ha recordado el [supuesto robo de datos al equipo de Emmanuel Macron](#) durante la campaña para las presidenciales francesas, el pasado mayo, y ha dicho que es un "riesgo" que España no debe correr.

El secretario de Estado ha recordado que pese a que la Junta Electoral aconsejó hace siete años la puesta en marcha de este sistema de votación, es difícil garantizar que ese voto electrónico no pueda ser manipulado y, por tanto, es posible que no arroje resultados veraces en unos comicios. "Hoy en día el voto electrónico está más lejos que hace diez años", ha concluido.

Interior descarta implantar el voto electrónico por la creciente ciberdelincuencia

La Junta Electoral aconsejó hace siete años la puesta en marcha de este sistema de votación



JOANA OLIVEIRA

Madrid - 1 JUN 2017 - 20:02 CEST



EL secretario de Estado de Seguridad, José Antonio Nieto. HÉCTOR MARTÍN (EFE)

El secretario de Estado de Seguridad, José Antonio Nieto Ballesteros, ha afirmado que el Gobierno descarta implantar el voto electrónico debido al aumento de la ciberdelincuencia, a pesar de contar con la tecnología necesaria para hacerlo. Nieto Ballesteros ha recordado el [supuesto robo de datos al equipo de Emmanuel Macron](#) durante la campaña para las presidenciales francesas, el pasado mayo, y ha dicho que es un "riesgo" que España no debe correr.

El secretario de Estado ha recordado que pese a que la Junta Electoral aconsejó hace siete años la puesta en marcha de este sistema de votación, es difícil garantizar que ese voto electrónico no pueda ser manipulado y, por tanto, es posible que no arroje resultados veraces en unos comicios. "Hoy en día el voto electrónico está más lejos que hace diez años", ha concluido.

El secretario de Estado ha recordado que pese a que la Junta Electoral aconsejó hace siete años la puesta en marcha de este sistema de votación, es difícil garantizar que ese voto electrónico no pueda ser manipulado y, por tanto, es posible que no arroje resultados veraces en unos comicios. "Hoy en día el voto electrónico está más lejos que hace diez años", ha concluido.

En una jornada sobre ciberseguridad, Nieto ha expuesto cómo ha cambiado la sociedad debido al uso de Internet y ha puesto como ejemplo el ámbito electoral. Según ha reconocido, las campañas electorales "no se entenderían" actualmente sin el mundo virtual, pero ello conlleva también peligros que hacen que Interior no se plantee implantar sistemas electrónicos de votación.

"Hoy estamos más lejos del voto electrónico que hace diez años porque es muy manipulable", ha confesado haciendo hincapié en que "muy pocos se atreven a garantizar la seguridad y veracidad" del resultado y se trata de "un riesgo" que, a su juicio, España "no debe asumir".

Los denominados ciberdelitos presentan un incremento exponencial año tras año. [Las denuncias por este tipo de ataques en España](#) durante el primer trimestre de 2017 crecieron un 22,3% respecto al año anterior, según ha expuesto el secretario de Estado, que ha revelado que en 2016 se detectaron un total de 66.586 ciberdelitos, un 10,7% más que en 2015.

Estos datos son ligeramente superiores a los del conjunto de la Unión Europea porque "los españoles aún deben concienciarse de la necesidad de la protección en Internet", ha explicado el secretario de Estado, que sin embargo ha destacado como aspecto favorable el aumento de las denuncias.

ABC

Date: 01/06/2017
Medio: ABC

Ciberdelincuencia

¿Está preparada España para un ciberataque?

» Expertos y autoridades aseguran que la ciberdelincuencia es, junto al terrorismo, «el gran peligro del siglo XXI» y lamentan que no se destinen más recursos a la lucha contra los peligros de la red. «Se invierte mucho en seguridad física, pero no en la cibernética. ¿Qué es más fácil, atacar cruzando una valla o por internet?», dicen los expertos

Compartir f t+ in Compartir 0 veces



La lucha contra los delitos cibernéticos es uno de los grandes problemas a día de hoy. EFE

ALEX JIMÉNEZ / [jdelgado@abc.es](#)
01/06/2017 08:28h - Actualizado: 02/06/2017 08:30h
Etiquetas: [tecnología](#)

«El siglo XXI tendrá dos grandes peligros: el terrorismo yihadista y los ciberataques». Con esta hipótesis, tan concisa como Antonio Gaitanaris, el presidente del Club Diálogos para la Democracia, la Jornada sobre Ciberseguridad organizada en la mañana de este jueves en Madrid por la asociación, en colaboración con Telefónica, que dejó patente que todavía queda un mundo entero por descubrir en la lucha contra la ciberdelincuencia.

Con las consecuencias masivas del ciberataque reciente por el secuestro de datos llamado WannaCry en la retina, los expertos y autoridades asumen las consecuencias de los peligros que tienen los ataques cibernéticos, un mal cada vez más instaurado al que es muy difícil ponerle freno, pero reclaman más inversión y presupuesto para hacer frente a futuros ataques. «El ataque del 12 de mayo de WannaCry fue muy grave y afectó a más de 180 países a niveles muy profundos», explicó el Secretario de Estado de Seguridad del Ministerio del Interior, José Antonio Nieto, que habló también de la «importancia de que exista una cooperación entre Ministerios, administraciones y países de todo el mundo para luchar contra los ciberataques».

Los peligros del voto electrónico

El peligro de la delincuencia por internet es tan alto -costuro Nieto- que desde el Gobierno no pueden plantearse instaurar el voto electrónico en España, por los riesgos de que este se vea afectado por criminales online y las elecciones se vean adulteradas. «Hoy estamos más lejos del voto electrónico que hace diez años, porque es muy manipulable por las tecnologías», señaló, añadiendo a que, si se implanta, «se asumirá un riesgo innecesario» y que sería muy complicado «garantizar la seguridad y veracidad» de los resultados electorales.

El político también incidió en la dificultad de encontrar a los responsables de los ataques. «El lucro y el anonimato están detrás de la ciberdelincuencia. Es muy difícil perseguir a los infractores», aseguró, instando antes de hablar del autodenominado Estado Islámico y de su incidencia en este tipo de delitos. «Daesh ha encontrado en la potencialidad de la red la manera de difundir sus mensajes de odio en países desconocidos».

Por otra parte, comentó que la lucha en España contra el ciberterrorismo está siendo un éxito, a pesar de que desde que arrancó 2017 «han aumentado en un 22% las denuncias por estos delitos». También comunicó que en España estaba surgiendo un nuevo perfil de agente de policía, policibotín, especializado en este tipo de delitos y que será «más importante en el futuro».

La cumbre también contó, como no podía ser de otro modo, con la participación de Telefónica, una de las compañías nacionales más afectadas por el virus ransomware WannaCry, que afectó a más de 300.000 equipos de 180 países. «Nadie está a salvo de sufrir un ciberataque», advirtió el Director de Administración, Defensa, Big Data y Seguridad de Telefónica, José Luis Gilpérez.

«WannaCry no fue el primer delito de delincuencia de este tipo al que nos tuvimos que enfrentar, ni será el último al que lo hagamos. En Telefónica nos intentan atacar continuamente, pero por eso cada vez estamos más preparados», aclaró, al tiempo que recordó la importancia que tiene la constante renovación y actualización de los sistemas informáticos. «La innovación es esencial para luchar contra la ciberdelincuencia».

Asunto de estado

La lucha contra los ciberdelincuentes, por tanto, es ya un problema de seguridad nacional. Así lo remarcó también Enrique Cubeiro, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa español, que lamentó la falta de recursos destinados a la lucha contra estos ataques. «En el ciberespacio, cualquier individuo tiene armas para poder hacer daño. Es frustrante ver cómo, aunque estos ataques son reconocidos como peligrosos, no pasamos de las palabras a los hechos para tratar de combatirlos», señaló el militar.

Según Cubeiro, tres de cada cuatro empresas han sido víctimas de un ciberataque en los últimos cinco años, y califica estos delitos de «cada vez más masivos y peligrosos». «El WannaCry es solo una pequeña muestra de lo que puede hacer la ciberdelincuencia en un mundo cada vez más global», repudió. «No se está respondiendo cómo se debe. Es muy duro que tenga que pasar algo grave para que se tome conciencia de los peligros que tienen estos ataques», aseveró.

«Se invierte mucho en seguridad física, pero no en la cibernética. Y yo me pregunto, ¿qué es más fácil, atacar cruzando una valla o por internet?», refirió Cubeiro. «Hay que quitarse ese estereotipo de que la gente que ataca por la red es gente rara, que está encerrada en un cuartucho. No podemos hacer nada si no se ponen las medidas para ello y no observamos a lo que está sucediendo en nuestra historia. Y si no prestamos atención a la historia, estamos perdidos», concluyó.

En la última década, lo cierto es que los ciberataques se han multiplicado y son cada vez más peligrosos. «Hace diez años, Estonia sufrió un ataque masivo que le dejó desconectada del mundo. El año pasado, el Banco de Bangladesh perdió 100 millones de dólares tras un ciberataque. Otros países como Georgia o Ucrania, donde un ataque dejó sin suministro a más de 600.000 hogares, también se han visto muy afectados y en España los casos cada vez son más comunes», explicó por su parte Marcos Gómez, subdirector del Instituto Nacional de Ciberseguridad en España.

El mensaje del congreso, al que asistieron cerca de 300 personas, fue muy claro. Se deben poner todos los recursos posibles en luchar contra la ciberdelincuencia, con una cooperación más que necesaria entre instituciones, organismos y países y concienciando a la población de la extrema vulnerabilidad a la que está expuesta. Porque, como subrayan los expertos, nadie queda libre de poder sufrir un ciberataque.



Telefónica fue una de las empresas afectadas por WannaCry. REUTERS

Telefónica, «muy valiente» y «orgullosa» en su lucha contra WannaCry

Una de las compañías más afectadas en España por el ransomware que agitó al mundo el pasado 12 de mayo fue Telefónica. La multinacional de comunicaciones actuó denunciando públicamente que había sido víctima del virus. «Desde Telefónica fueron muy valientes», señaló José Antonio Nieto. «Estamos muy orgullosos de la manera en que actuamos. Fuimos muy transparentes, seguimos el protocolo y tomamos las medidas adecuadas para luchar contra el ataque», subrayó por su parte José Luis Gilpérez. «Lo más importante fue que no tuvo ningún impacto en nuestros clientes ni en los ciudadanos. Todos pudieron continuar utilizando sus terminales y nuestros servicios de manera normal y no se vieron afectados por WannaCry de ninguna manera. Además, nosotros no perdimos ningún tipo de información», detalló al respecto.

Elite
CONEXION

Ciberdelincuencia

¿Está preparada España para un ciberataque?

» Expertos y autoridades aseguran que la ciberdelincuencia es, junto al terrorismo, «el gran peligro del siglo XXI» y lamentan que no se destinen más recursos a la lucha contra los peligros de la red. «Se invierte mucho en seguridad física, pero no en la cibernética. Qué es más fácil, atacar cruzando una valla o por internet?», dicen los expertos

Compartir en: Facebook, Twitter, LinkedIn, Compartir 0 veces



La lucha contra los delitos cibernéticos es uno de los grandes problemas a día de hoy. EFE

ALEX JIMÉNEZ / [jdelgado@abc.es](#)
910002017-00206 - Actualizado: 09/06/2017 08:30h.
Usando en: [tecnología](#)

«El siglo XXI tendrá dos grandes peligros: el terrorismo yihadista y los ciberataques». Con esta hipótesis, tan concisa como Antonio Gualandri, el presidente del Club Diálogos para la Democracia, la Jornada sobre Ciberseguridad organizada en la mañana de este jueves en Madrid por la asociación, en colaboración con Telefónica, que dejó patente que todavía queda un mundo entero por descubrir en la lucha contra la ciberdelincuencia.

Con las consecuencias masivas del ciberataque reciente por el secuestro de datos llamado WannaCry en la retina, los expertos y autoridades asumen las consecuencias de los peligros que tienen los ataques cibernéticos, un mal cada vez más instaurado al que es muy difícil ponerle freno, pero reclaman más inversión y presupuesto para hacer frente a futuros ataques. «El ataque del 12 de mayo de WannaCry fue muy grave y afectó a más de 180 países a niveles muy profundos», explicó el Secretario de Estado de Seguridad del Ministerio del Interior, José Antonio Nieto, que habló también de la «importancia de que exista una cooperación entre Ministerios, administraciones y países de todo el mundo para luchar contra los ciberataques».

Los peligros del voto electrónico

El peligro de la delincuencia por internet es tan alto -costoso Nieto- que desde el Gobierno no pueden plantearse instaurar el voto electrónico en España, por los riesgos de que este se vea afectado por criminales online y las elecciones se vean adulteradas. «Hoy estamos más lejos del voto electrónico que hace diez años, porque es muy manipulable por las tecnologías», señaló, añadiendo a que, si se implantase, «se asumiría un riesgo innecesario» y que sería muy complicado «garantizar la seguridad y veracidad» de los resultados electorales.

El político también incidió en la dificultad de encontrar a los responsables de los ataques. «El lucro y el anonimato están detrás de la ciberdelincuencia. Es muy difícil perseguir a los infractores», aseguró, instando antes de hablar del autodenominado Estado Islámico y de su incidencia en este tipo de delitos. «Daesh ha encontrado en la potencialidad de la red la manera de difundir sus mensajes de odio en países desconocidos».

Por otra parte, comentó que la lucha en España contra el ciberterrorismo está siendo un éxito, a pesar de que desde que arrancó 2017 «han aumentado en un 22% las denuncias por estos delitos». También comunicó que en España estaba surgiendo un nuevo perfil de agente de policía, policibotín, especializado en este tipo de delitos y que será «más importante en el futuro».

La cumbre también contó, como no podía ser de otro modo, con la participación de Telefónica, una de las compañías nacionales más afectadas por el virus ransomware WannaCry, que afectó a más de 300.000 equipos de 150 países. «Nadie está a salvo de sufrir un ciberataque», advirtió el Director de Administración, Defensa, Big Data y Seguridad de Telefónica, José Luis Gilpérez.

«WannaCry no fue el primer delito de delincuencia de este tipo al que nos tuvimos que enfrentar, ni será el último al que lo hagamos. En Telefónica nos intentan atacar continuamente, pero por eso cada vez estamos más preparados», aclaró, al tiempo que recordó la importancia que tiene la constante renovación y actualización de los sistemas informáticos. «La innovación es esencial para luchar contra la ciberdelincuencia».

Asunto de estado

La lucha contra los ciberdelincuentes, por tanto, es ya un problema de seguridad nacional. Así lo remarcó también Enrique Cubeiro, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa español, que lamentó la falta de recursos destinados a la lucha contra estos ataques. «En el ciberespacio, cualquier individuo tiene armas para poder hacer daño. Es frustrante ver cómo, aunque estos ataques son reconocidos como peligrosos, no pasamos de las palabras a los hechos para tratar de combatirlos», señaló el militar.

Según Cubeiro, tres de cada cuatro empresas han sido víctimas de un ciberataque en los últimos cinco años, y califica estos delitos de «cada vez más masivos y peligrosos». «El WannaCry es solo una pequeña muestra de lo que puede hacer la ciberdelincuencia en un mundo cada vez más global», repudió. «No se está respondiendo cómo se debe. Es muy duro que tenga que pasar algo grave para que se tome conciencia de los peligros que tienen estos ataques», aseveró.

«Se invierte mucho en seguridad física, pero no en la cibernética. Y yo me pregunto, ¿qué es más fácil, atacar cruzando una valla o por internet?», refirió Cubeiro. «Hay que quitarse ese estereotipo de que la gente que ataca por la red es gente rara, que está encerrada en un cuartucho. No podemos hacer nada si no se ponen las medidas para ello y no observamos a lo que está sucediendo en nuestra historia. Y si no prestamos atención a la historia, estamos perdidos», concluyó.

En la última década, lo cierto es que los ciberataques se han multiplicado y son cada vez más peligrosos. «Hace diez años, Estonia sufrió un ataque masivo que le dejó desconectada del mundo. El año pasado, el Banco de Bangladesh perdió 100 millones de dólares tras un ciberataque. Otros países como Georgia o Ucrania, donde un ataque dejó sin suministro a más de 600.000 hogares, también se han visto muy afectados y en España los casos cada vez son más comunes», explicó por su parte Marcos Gómez, subdirector del Instituto Nacional de Ciberseguridad en España.

El mensaje del congreso, al que asistieron cerca de 300 personas, fue muy claro. Se deben poner todos los recursos posibles en luchar contra la ciberdelincuencia, con una cooperación más que necesaria entre instituciones, organismos y países y concienciando a la población de la extrema vulnerabilidad a la que está expuesta. Porque, como subrayan los expertos, nadie queda libre de poder sufrir un ciberataque.



Telefónica fue una de las empresas afectadas por WannaCry. REUTERS

Telefónica, «muy valiente» y «orgullosa» en su lucha contra WannaCry

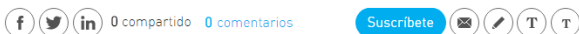
Una de las compañías más afectadas en España por el ransomware que agitó al mundo el pasado 12 de mayo fue Telefónica. La multinacional de comunicaciones actuó denunciando públicamente que había sido víctima del virus. «Desde Telefónica fueron muy valientes», señaló José Antonio Nieto. «Estamos muy orgullosos de la manera en que actuamos. Fuimos muy transparentes, seguimos el protocolo y tomamos las medidas adecuadas para luchar contra el ataque», subrayó por su parte José Luis Gilpérez. «Lo más importante fue que no tuvo ningún impacto en nuestros clientes ni en los ciudadanos. Todos pudieron continuar utilizando sus terminales y nuestros servicios de manera normal y no se vieron afectados por WannaCry de ninguna manera. Además, nosotros no perdimos ningún tipo de información», detalló al respecto.

COMPANÍAS

"Telefónica no ha perdido información debido al ataque WannaCry"



Fachada de la sede corporativa de Telefónica en Madrid. | EFE | EFE



M. PRIETO MADRID

Actualizado: 01/06/2017 14:29 horas

José Luis Gilpérez, director ejecutivo de Administraciones Públicas, Defensa, Seguridad y BigData de Telefónica, ha asegurado en su intervención en unas conferencias sobre ciberseguridad, que el impacto real del ataque WannaCry en Telefónica "ha sido cero".

Telefónica asegura que la compañía no ha perdido información debido a Wannacry, el ciberataque de *ransomware* que afectó a más de 300.000 equipos de 180 países a mediados de mayo. "No hemos perdido nada de información porque ésta no estaba en los PC sino en el *cloud* de Telefónica", ha asegurado José Luis Gilpérez, director ejecutivo de Administraciones Públicas, Defensa, Seguridad y BigData de Telefónica, en su intervención en la Jornada de Ciberseguridad organizada por Diálogos para la Democracia.

Según ha explicado el ejecutivo de Telefónica, el "impacto real de Wannacry ha sido cero. No ha tenido impacto en los servicios que prestamos a los usuarios, empresas y Administraciones Públicas". Gilpérez ha defendido la actuación de Telefónica ante el ataque. "La reacción fue ejemplar, valiente y responsable a la hora de comunicar de manera temprana que habíamos sido objetivos del incidente", según ha resaltado el directivo, quien ha señalado que "el protocolo de actuación fue el correcto y el estándar en ataques de este tipo, cuyo vector de propagación es conocido".

Los ciberdelitos crecen un 11% en 2016 en España

LOS CIBERDELITOS CRECEN UN 11% EN ESPAÑA

José Antonio Nieto, secretario de Estado de Seguridad, adelantó algunos datos del informe de anual de estadísticas sobre cibercrimen que elabora el Ministerio del Interior. Así, el año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% amenazas y coacciones. En el primer trimestre de 2017, el número de ciberdelitos ha crecido un 22% respecto al mismo periodo del año anterior. El crecimiento se explica tanto por el aumento de la ciberdelincuencia como por un mayor compromiso de denuncia por parte de los afectados.

Gilpérez ha defendido igualmente que Telefónica no hubiera desplegado el **parche de seguridad que Microsoft** había enviado en marzo y que cerraba el paso al virus. "No estamos en condiciones de aplicar de forma automática parches y actualizaciones en algunos segmentos del negocio porque tenemos que garantizar y probar que no van a causar problemas en sistemas críticos. Tenemos que primar siempre el servicio a los clientes", aseguró.

Durante las jornadas, José Antonio Nieto, secretario de Estado de Seguridad, ha destacado la actuación de Telefónica. "Demostró gran responsabilidad porque, a riesgo de su imagen, denunció el ataque y activó los mecanismos de control". Según Nieto, "Telefónica demostró resiliencia ante el ataque, que es la clave porque todos tenemos que saber que vamos a ser atacados", dijo.

COMPañÍAS

Los ciberataques afectan a tres de cada cuatro empresas en España



Pirata informático. | DREAMSTIME | EXPANSIÓN

0 compartido 1 comentarios [Suscríbete](#)

INMA BENEDITO MADRID
Actualizado: 02/06/2017 00:40 horas

España es el tercer país del mundo que más ataques informáticos recibe. En 2016 se detectaron 115.000 incidentes, de los que 480 afectaron a hospitales y aeropuertos, entre otros.

La ciberseguridad, igual que el cambio climático, es tan alarmante como intangible. Tres de cada cuatro empresas españolas ha sufrido un ciberataque en los últimos cinco años. Sin embargo, apenas el 37% tiene un plan de respuesta a incidentes de este tipo. A nivel mundial, el coste de los ciberataques a empresas asciende a un total de 265 millones de euros. En el caso de España, nos encontramos con que es el tercer país con más ofensivas a nivel mundial, después de Reino Unido y Estados Unidos.

La escalada es exponencial y, las cifras, alarmantes. En 2016, el Instituto Nacional de Seguridad (Incibe) detectó más de 115.000 ciberincidentes, de los cuales más de 110.000 afectaron a ciudadanos y al sector privado, y 480 a infraestructuras críticas - aeropuertos, hospitales, centrales eléctricas o plantas de agua-. Sólo en el primer trimestre de este año, España recibió 50.000 ciberataques, 247 en estructuras críticas. A ese ritmo, podríamos alcanzar las 150.000 ofensivas a finales de este año. El año pasado se denunciaron 66.586 ciberdelitos, un 10,7% más, de los que el 68% fueron fraudes y estafas y el 17,2% amenazas y coacciones.

"Estamos por encima de la media de ataques porque estamos por debajo en la protección de equipos. Muchas veces no valoramos lo que tenemos dentro de un dispositivo y no hacemos lo posible por protegerlo", explicó ayer José Antonio Nieto Ballesteros, Secretario de Estado de Seguridad del Ministerio del Interior, en unas jornadas sobre Ciberseguridad organizada por el Club Diálogos para la Democracia.

El "negocio" es rentable. Actualmente supone cerca del 0,8% del PIB mundial, es decir, mueve más dinero que la mayoría de crímenes, como es el caso de tráfico de estupefacientes. Por la parte de la ciberseguridad también, alcanzando los 76.000 millones de euros al año en el mundo. "La magnitud del problema está todavía lejos de entenderse por una mayoría. No se está respondiendo ni con la celeridad ni la contundencia que se debe", señaló Enrique Cubeiro Cabello, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa. Es el gran problema de lo intangible, que hace que no terminemos de creernos lo que no vemos.


Pero del virus hemos pasado a la epidemia y del gusano a la plaga. En diciembre de 2015, el troyano BlackEnergy provocó cortes en el suministro de electricidad a más de 600.000 hogares ucranianos en pleno invierno. Las ofensivas contra estructuras críticas son las más preocupantes. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. El pasado 12 de mayo, el incidente del ransomware Wannacry afectó a más de 25 hospitales. Ante la imposibilidad de acceder al sistema informático, muchos de ellos tuvieron que trasladar a pacientes graves a otros hospitales cercanos. En los dos últimos años, más de 4.000 ataques cibernéticos se identifican con el tipo ransomware -se caracteriza por secuestrar la información y exigir un rescate- Se trata del principal malware en Europa.

Wannacry afectó a más de 300.000 equipos de 180 países. En España, fueron 1.200 equipos. "La reacción fue rápida y se pudo controlar el impacto de manera inmediata", explicó ayer Antonio Gavilanes Dumont, presidente del Club Diálogos para la Democracia. El caso más sonado fue Telefónica, aunque José Luis Gilpérez, director ejecutivo de Administraciones Públicas, Defensa, Seguridad y BigData de Telefónica, aseguró ayer que "el impacto real de Wannacry ha sido cero". El grupo de telefonía aumentó sus ingresos en el área de seguridad un 22,7% en 2016, hasta 341 millones.

"Esto es un trabajo de todos los agentes públicos y privados", señaló Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Incibe. Después del incidente, Reino Unido ha decidido invertir 13.000 millones de euros en ciberseguridad. En España no hay una partida definida de la Administración Pública, aunque Nieto aseguró que "tenemos herramientas para prevenirlo y una implicación altísima de los técnicos y de la iniciativa privada para conseguir que España sea una materia de seguridad virtual como lo es física".

JORNADA CIBERSEGURIDAD (PREVISIÓN)

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

f Comparte en Facebook  Comparte en Twitter + 0

01/06/2017 15:20

Madrid, 1 jun (EFE).- Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...). Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna. EFE

Expertos piden alianzas contra ciberataques porque no hay tecnología mágica



COMENTARIOS 0

A+ A Cuerpo de letra

Imprimir noticia

ENVÍA UNA CARTA DEL LECTOR

EFE

JUEVES, 1 DE JUNIO DEL 2017 - 17:43 CEST

A la hora de afrontar un ciberataque no hay una "tecnología mágica", sino que hace falta una industria que trabaje de manera coordinada, con alianzas entre fabricantes y con información compartida, o "la batalla estará perdida de antemano".

Así lo han señalado varios expertos en la jornada sobre ciberseguridad organizada por el Club Diálogos para la Democracia y Telefónica, en la que han señalado que "la resiliencia digital", la capacidad para volver a la normalidad y restaurar la operatividad de un sistema tras un ataque, "es tan importante como la prevención".

"La resiliencia es tan importante como la prevención", ha asegurado el director general de Symantec para el sur de Europa, Miguel Ángel Martos, quien ha apostillado que "el mayor riesgo es no saber cómo gestionar un ataque".

Por ello, la responsable de la compañía McAfee en España, María Campos, ha hecho hincapié en actuar en "puntos estratégicos", a través de la protección de terminales como ordenadores, teléfonos inteligentes o tabletas.

En su opinión, el aumento del número de ataques a través de ransomware -secuestro de datos- obliga a centros e instituciones que manejan grandes bases de datos a contar con "un plan de defensa para responder y remediar posibles ataques".

Y es que "no existe una tecnología mágica", sino que hay que integrar varias medidas y herramientas en las soluciones, así como "una industria que trabaje de forma coordinada", con alianzas con fabricantes y compartiendo información contra los 'malwares' y sus variantes, o, de lo contrario, "la batalla estará perdida de antemano", según Campos.

La digitalización empresarial ha sido otro de los temas debatidos en este encuentro, en el que el director comercial de grandes cuentas en Fortinet, Luis Miguel Garrido, ha subrayado que "nuestros datos van cada vez más a 'la nube', donde existen espacios con poco control".

En este sentido, Garrido ha destacado el correo electrónico como una de los principales frentes por los que un usuario o empresa pueden ser atacados, que "deben ser consciente del riesgo que entrañan las URL o los ficheros desconocidos".

Por su parte, el socio de Audertis, Óscar Bou, ha incidido en la importancia de los certificados de seguridad, "una garantía de confianza" que debe acreditar cualquier proveedor que quiera trabajar con la administración pública.

20
minutos

Date: 01/06/2017
Medio: 20 Minutos

< NACIONAL >

Interior descarta implantar el voto electrónico por la creciente ciberdelincuencia



Un empleado del ayuntamiento de Licking, en Ohio, muestra el funcionamiento de un ordenador para voto electrónico en EE UU. (ARCHIVO)

- "Hoy el voto electrónico está más lejos que hace diez años. Es un riesgo que no debemos asumir", afirma el número dos de Interior, José Antonio Nieto.

ECO  Actividad social ¿QUÉ ES ESTO? **24** % **58**   **0**  

AGENCIAS. 01.06.2017 - 11:26h

El secretario de Estado de Seguridad, José Antonio Nieto, ha asegurado este jueves que la implantación del voto electrónico es un "riesgo" que España no debe asumir ante la **creciente amenaza de la ciberdelincuencia**, a pesar de contar con la tecnología para cambiar el sistema de votación.

En la inauguración de una jornada sobre ciberseguridad organizada por el Club de Diálogos para la Democracia y Telefónica, Nieto ha dejado claro que hoy por hoy **el voto en papel para unas elecciones ofrece "más garantías"** que el electrónico.

Nieto ha recordado que pese a que la Junta Electoral aconsejó hace siete años la puesta en marcha de este sistema de votación y de que **España disponía del desarrollo tecnológico para hacerlo**, "muy pocos se atreven hoy" a garantizar que ese voto electrónico no pueda ser manipulado y, por tanto, a que arroje los resultados veraces de unos comicios.

"Hoy el voto electrónico está más lejos que hace diez años. Es un riesgo que no debemos asumir", ha añadido el número dos de Interior que ha citado algunos de los problemas que han sufrido países como Francia con este tipo de votación.



lainformacion.com

Date: 01/06/2017
Medio: La Información

POLICÍA Y JUSTICIA - MAGISTRATURA

Interior descarta implantar el voto electrónico por el peligro de manipulación del resultado electoral

POR EUROPA PRESS / LAINFORMACION.COM
MADRID | 01/06/2017 - 18:45



Etiquetas España, Siria, Iraq, Junta Electoral Central, Unión Europea, Ministerio del Interior, Magistratura, Terrorismo, Elecciones, Juicios, Seguridad.

Las denuncias por ciberdelitos crecieron un 22,3% en el primer trimestre de 2017 respecto a 2016

El Ministerio del Interior no se plantea poner en marcha el voto electrónico en España debido al alto riesgo que existe de sufrir un ciberataque y que el resultado electoral sea manipulado, según ha revelado este jueves el secretario de Estado de Seguridad, José Antonio Nieto.

En una jornada sobre ciberseguridad, Nieto ha expuesto cómo ha cambiado la sociedad debido al uso de Internet y ha puesto como ejemplo el ámbito electoral. Según ha reconocido, las campañas electorales "no se entenderían" actualmente sin el mundo virtual, pero ello conlleva también peligros que hacen que Interior no se plantee implantar sistemas electrónicos de votación.

"Hoy estamos más lejos del voto electrónico que hace diez años porque es muy manipulable", ha confesado haciendo hincapié en que "muy pocos se atreven a garantizar la seguridad y veracidad" del resultado y se trata de "un riesgo" que, a su juicio, España "no debe asumir".

La Junta Electoral Central (JEC) recomendó hace ya siete años al Gobierno el estudio de sistemas que permitiesen en uso de sistemas electrónicos para los procesos electorales, pero Nieto ha insistido en que el incremento de los ataques cibernéticos durante los últimos años hace que se trate de un avance que no esté en la agenda a corto plazo. "La tradicional papeleta sigue siendo más segura", ha defendido.

CRECIMIENTO DEL 22,3% EN 2017

Los denominados ciberdelitos presentan un incremento exponencial año tras año. Las denuncias por este tipo de ataques en España durante el primer trimestre de 2017 crecieron un 22,3 por ciento respecto al año anterior, según ha expuesto el secretario de Estado, que ha revelado que en 2016 se detectaron un total de 66.586 ciberdelitos, un 10,7 por ciento más que en 2015.

Estos datos son ligeramente superiores a los del conjunto de la Unión Europea porque los españoles aún deben concienciarse de la necesidad de la protección en Internet, ha explicado el secretario de Estado, que sin embargo ha destacado como aspecto favorable el aumento de las denuncias.

Nieto ha comparado esta situación con la de la violencia de género, donde sólo se denuncian el 20 por ciento de las agresiones existentes y el objetivo es aumentar estas denuncias. "La evolución del primer trimestre de los ciberdelitos denunciados muestra una tendencia al alza, pero también un aumento de las denuncias", ha celebrado.

Los delitos cibernéticos fueron centro de atención tras el ataque sufrido por más de 180 países el pasado 12 de mayo, al que el 'número dos' del Ministerio de Interior ha asegurado que España reaccionó de forma "rápida y ágil" haciendo posible que sus efectos fueran "bastante limitados".

Según ha expuesto, la ciberdelincuencia permite la deslocalización del delito, la multiplicación exponencial de sus efectos, la ocultación del delincuente y la dificultad de la labor policial y judicial. Además, al tener casi siempre un carácter internacional, exige una cooperación policial y judicial entre países que hace "más lentas" las operaciones.

DAEHS MULTIPLICA SU ESFUERZO EN INTERNET

Uno de los focos de atención en el mundo de los delitos cibernéticos es el del terrorismo, sobretudo después de que Daesh haya demostrado una gran agilidad en su manejo para la captación y adoctrinamiento a través de las redes sociales y "la expansión de su mensaje de odio".

"El mal se desarrolla bien en las redes sociales", ha reconocido Nieto, que ha explicado que Internet ha propiciado durante los últimos años una multiplicación de su mensaje que "no tiene precedentes". Y ha expuesto que, al mismo ritmo que los terroristas pierden territorio físico en Siria o Irak están "duplicando" su esfuerzo en el mundo virtual.

En este ámbito también ha asegurado que España ha desarrollado un trabajo "de éxito", que demuestra el hecho de que todas las operaciones contra el terrorismo yihadista tuvieron su origen en seguimientos hechos en Internet. En esta legislatura, las operaciones antiterroristas se han saldado con un total de 81 detenidos.

Inicio / Política

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

EFE - Madrid

01/06/2017 - 13:12h



Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

EFE 01/06/2017 (1451)

Madrid, 1 jun (EFE) - Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto, que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más. Y en esa denuncia rápida, el número dos de interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia. "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilon", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna. EFE

lca/msr

(foto) (video) (audio)

Las ciberamenazas no son un cuento, 3 de 4 de empresas son atacadas, según expertos

1/06/2017 - 15:39

Tweet Compartir G+1 0 in Share Wow! 0

Más noticias sobre: EMPRESAS MADRID RANSOMWARE PIB



ENLACES RELACIONADOS

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas (1/06)

✉ 📧 🔒 🔒

Madrid, 1 jun (EFE).- Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

01 junio, 2017



Madrid, 1 jun (EFE).- Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una Jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

01 junio, 2017



Madrid, 1 jun (EFE).- Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una Jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique CUBEIRO, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado CUBEIRO, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos GÓMEZ, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis JIMÉNEZ, ha suscrito la llamada de atención del capitán de navío Enrique CUBEIRO.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado GÓMEZ que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

01 junio, 2017



Madrid, 1 jun (EFE).- Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una Jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

01 junio, 2017



Madrid, 1 jun (EFE).- Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Teléfonica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una Jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

01 junio, 2017



Madrid, 1 jun (EFE).- Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una Jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique CUBEIRO, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado CUBEIRO, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos GÓMEZ, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis JIMÉNEZ, ha suscrito la llamada de atención del capitán de navío Enrique CUBEIRO.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado GÓMEZ que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

01 junio, 2017



Madrid, 1 jun (EFE).- Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una Jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique CUBEIRO, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado CUBEIRO, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos GÓMEZ, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis JIMÉNEZ, ha suscrito la llamada de atención del capitán de navío Enrique CUBEIRO.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado GÓMEZ que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Ciberdelincuencia

¿Está preparada España para un ciberataque?

» Expertos y autoridades aseguran que la ciberdelincuencia es, junto al terrorismo, «el gran peligro del siglo XXI» y lamentan que no se destinen más recursos a la lucha contra los peligros de la red. «Se invierte mucho en seguridad física, pero no en la cibernética. ¿Qué es más fácil, atacar cruzando una valla o por internet?», dicen los expertos

Compartir [f](#) [t](#) [v](#) [l](#) [in](#) Compartir 0 veces



La lucha contra los delitos cibernéticos es uno de los grandes problemas a día de hoy. EFE

ALEX JIMÉNEZ / [jdelgado@red.es](#)
915092517 91.281 - Andalucía - 09/06/2017 08:39L
Usando en: [tecnología](#)

«El siglo XXI tendrá dos grandes peligros: el terrorismo yihadista y los ciberataques». Con esta hipótesis, tan concisa como Antonio Gualandri, el presidente del Club Diálogos para la Democracia, la Jornada sobre Ciberseguridad organizada en la mañana de este jueves en Madrid por la asociación, en colaboración con Telefónica, que dejó patente que todavía queda un mundo entero por descubrir en la lucha contra la ciberdelincuencia.

Con las consecuencias masivas del ciberataque reciente por el secuestro de datos llamado WannaCry en la retina, los expertos y autoridades asumen las consecuencias de los peligros que tienen los ataques cibernéticos, un mal cada vez más instaurado al que es muy difícil ponerle freno, pero reclaman más inversión y presupuesto para hacer frente a futuros ataques. «El ataque del 12 de mayo de WannaCry fue muy grave y afectó a más de 180 países a niveles muy profundos», explicó el Secretario de Estado de Seguridad del Ministerio del Interior, José Antonio Nieto, que habló también de la «importancia de que exista una cooperación entre Ministerios, administraciones y países de todo el mundo para luchar contra los ciberataques».

Los peligros del voto electrónico

El peligro de la delincuencia por internet es tan alto -costuro Nieto- que desde el Gobierno no pueden plantearse instaurar el voto electrónico en España, por los riesgos de que este se vea afectado por criminales online y las elecciones se vean adulteradas. «Hoy estamos más lejos del voto electrónico que hace diez años, porque es muy manipulable por las tecnologías», señaló, añadiendo a que, si se implantase, «se asumiría un riesgo innecesario» y que sería muy complicado «garantizar la seguridad y veracidad» de los resultados electorales.

El político también incidió en la dificultad de encontrar a los responsables de los ataques. «El lucro y el anonimato están detrás de la ciberdelincuencia. Es muy difícil perseguir a los infractores», aseguró, instando antes de hablar del autodenominado Estado Islámico y de su incidencia en este tipo de delitos. «Daesh ha encontrado en la potencialidad de la red la manera de difundir sus mensajes de odio en países desconocidos».

Por otra parte, comentó que la lucha en España contra el ciberterrorismo está siendo un éxito, a pesar de que desde que arrancó 2017 «han aumentado en un 22% las denuncias por estos delitos». También comunicó que en España estaba surgiendo un nuevo perfil de agente de policía, policíbero, especializado en este tipo de delitos y que será «más importante en el futuro».

La cumbre también contó, como no podía ser de otro modo, con la participación de Telefónica, una de las compañías nacionales más afectadas por el virus ransomware WannaCry, que afectó a más de 300.000 equipos de 150 países. «Nadie está a salvo de sufrir un ciberataque», advirtió el Director de Administración, Defensa, Big Data y Seguridad de Telefónica, José Luis Gilpérez.

«WannaCry no fue el primer delito de delincuencia de este tipo al que nos tuvimos que enfrentar, ni será el último al que lo hagamos. En Telefónica nos intentan atacar continuamente, pero por eso cada vez estamos más preparados», aclaró, al tiempo que recordó la importancia que tiene la constante renovación y actualización de los sistemas informáticos. «La innovación es esencial para luchar contra la ciberdelincuencia».

Asunto de estado

La lucha contra los ciberdelincuentes, por tanto, es ya un problema de seguridad nacional. Así lo remarcó también Enrique Cubeiro, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa español, que lamentó la falta de recursos destinados a la lucha contra estos ataques. «En el ciberespacio, cualquier individuo tiene armas para poder hacer daño. Es frustrante ver cómo, aunque estos ataques son reconocidos como peligrosos, no pasamos de las palabras a los hechos para tratar de combatirlos», señaló el militar.

Según Cubeiro, tres de cada cuatro empresas han sido víctimas de un ciberataque en los últimos cinco años, y califica estos delitos de «cada vez más masivos y peligrosos». «El WannaCry es solo una pequeña muestra de lo que puede hacer la ciberdelincuencia en un mundo cada vez más global», repudió. «No se está respondiendo cómo se debe. Es muy duro que tenga que pasar algo grave para que se tome conciencia de los peligros que tienen estos ataques», aseveró.

«Se invierte mucho en seguridad física, pero no en la cibernética. Y yo me pregunto, ¿qué es más fácil, atacar cruzando una valla o por internet?», refirió Cubeiro. «Hay que quitarse ese estereotipo de que la gente que ataca por la red es gente rara, que está encerrada en un cuartucho. No podemos hacer nada si no se ponen las medidas para ello y no observamos a lo que está sucediendo en nuestra historia. Y si no prestamos atención a la historia, estamos perdidos», concluyó.

En la última década, lo cierto es que los ciberataques se han multiplicado y son cada vez más peligrosos. «Hace diez años, Estonia sufrió un ataque masivo que le dejó desconectada del mundo. El año pasado, el Banco de Bangladesh perdió 100 millones de dólares tras un ciberataque. Otros países como Georgia o Ucrania, donde un ataque dejó sin suministro a más de 600.000 hogares, también se han visto muy afectados y en España los casos cada vez son más comunes», explicó por su parte Marcos Gómez, subdirector del Instituto Nacional de Ciberseguridad en España.

El mensaje del congreso, al que asistieron cerca de 300 personas, fue muy claro. Se deben poner todos los recursos posibles en luchar contra la ciberdelincuencia, con una cooperación más que necesaria entre instituciones, organismos y países y concienciando a la población de la extrema vulnerabilidad a la que está expuesta. Porque, como subrayan los expertos, nadie queda libre de poder sufrir un ciberataque.



Telefónica fue una de las empresas afectadas por WannaCry. REUTERS

Telefónica, «muy valiente» y «orgullosa» en su lucha contra WannaCry

Una de las compañías más afectadas en España por el ransomware que agitó al mundo el pasado 12 de mayo fue Telefónica. La multinacional de comunicaciones actuó denunciando públicamente que había sido víctima del virus. «Desde Telefónica fueron muy valientes», señaló José Antonio Nieto. «Estamos muy orgullosos de la manera en que actuamos. Fuimos muy transparentes, seguimos el protocolo y tomamos las medidas adecuadas para luchar contra el ataque», subrayó por su parte José Luis Gilpérez. «Lo más importante fue que no tuvo ningún impacto en nuestros clientes ni en los ciudadanos. Todos pudieron continuar utilizando sus terminales y nuestros servicios de manera normal y no se vieron afectados por WannaCry de ninguna manera. Además, nosotros no perdimos ningún tipo de información», detalló al respecto.

EN 2016 REGISTRARON 66.680 DELITOS

Los expertos alertan que las ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

Hace 15 días se registró un ciberataque que afectó a 74 países con más de 45.000 incidentes

EFE - Jueves, 1 de Junio de 2017 - Actualizado a las 18:11h



Un periodista lee en Internet un artículo sobre el ciberataque mundial iniciado el viernes. (Efe)

Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

MADRID. Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de un ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han titulado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".



Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamanaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

EN 2016 REGISTRARON 66.680 DELITOS

Los expertos alertan que las ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

Hace 15 días se registró un ciberataque que afectó a 74 países con más de 45.000 incidentes

EFE - Jueves, 1 de Junio de 2017 - Actualizado a las 18:11h



Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

MADRID. Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de un ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han titulado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamanaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

TECNOLOGÍA**JORNADA CIBERSEGURIDAD**

Los expertos alertan: Las ciberamenazas no son un cuento, 3 de cada 4 empresas son atacadas

**0** veces compartido**Comentarios 0**

Madrid, EFE 1/jun/17 18:07 PM eldia.es



El secretario de Estado de Seguridad, José Antonio Nieto./Paco Campos (EFE)

Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

"RIESGO" INASUMIBLE

Interior descarta implantar el voto electrónico por miedo a un ciberataque

Considera que es un "riesgo" que no se debe asumir por el momento, a pesar de contar con la tecnología

EL PERIÓDICO / MADRID
01/06/2017

Compartir: [f](#) [t](#) [G+](#)



Un empleado municipal revisa una máquina de voto electrónico durante las pasadas elecciones presidenciales francesas. - AFP / FRED TANNEAU

Enviar

A- A+ 0

El voto electrónico todavía está lejos de implantarse en España. Y lo seguirá estando mientras la ciberdelincuencia continúe dando golpes como el reciente del virus Wannacry, que afectó a grandes empresas, hospitales, universidades y decenas de miles de ordenadores de particulares.

Según ha explicado este jueves el secretario de Estado de Seguridad, José Antonio Nieto, este método de votación es un "riesgo" que España no debe asumir a pesar de contar con la tecnología. Se trata, ha recalcado el alto cargo del Ministerio del Interior, de evitar que los resultados electorales puedan ser manipulados como consecuencia de un ciberataque.

"Hoy estamos más lejos del voto electrónico que hace 10 años porque es muy manipulable", ha asegurado Nieto durante una jornada sobreciberseguridad organizada por el Club de Diálogos para la Democracia y Telefónica, en la que ha dejado claro que hoy por hoy el tradicional voto en papel es el que ofrece "más garantías".

CRECIMIENTO EXPONENCIAL

En el 2010, la Junta Electoral Central (JEC) recomendó al Gobierno el estudio de sistemas que permitiesen el uso de sistemas electrónicos para los procesos electorales, pero el incremento de los ataques cibernéticos ha provocado que este avance haya desaparecido de la agenda a corto plazo.

Según datos de Interior, los ciberdelitos han aumentado en el primer trimestre del 2017 un 22,3% respecto del mismo periodo del año anterior. Un crecimiento exponencial, pues en el 2016 se registraron un 10,7% más de ciberataques que en el 2015.

"RIESGO" INASUMIBLE

Interior descarta implantar el voto electrónico por miedo a un ciberataque

Considera que es un "riesgo" que no se debe asumir por el momento, a pesar de contar con la tecnología

EL PERIÓDICO / MADRID
01/06/2017

Compartir:   



Un empleado municipal revisa una máquina de voto electrónico durante las pasadas elecciones presidenciales francesas. - AFP / FRED TANNEAU

 Enviar

    0

El voto electrónico todavía está lejos de implantarse en España. Y lo seguirá estando mientras la ciberdelincuencia continúe dando golpes como el reciente del virus Wannacry, que afectó a grandes empresas, hospitales, universidades y decenas de miles de ordenadores de particulares.

Según ha explicado este jueves el secretario de Estado de Seguridad, José Antonio Nieto, este método de votación es un "riesgo" que España no debe asumir a pesar de contar con la tecnología. Se trata, ha recalcado el alto cargo del Ministerio del Interior, de evitar que los resultados electorales puedan ser manipulados como consecuencia de un ciberataque.

"Hoy estamos más lejos del voto electrónico que hace 10 años porque es muy manipulable", ha asegurado Nieto durante una jornada sobreciberseguridad organizada por el Club de Diálogos para la Democracia y Telefónica, en la que ha dejado claro que hoy por hoy el tradicional voto en papel es el que ofrece "más garantías".

CRECIMIENTO EXPONENCIAL

En el 2010, la Junta Electoral Central (JEC) recomendó al Gobierno el estudio de sistemas que permitiesen el uso de sistemas electrónicos para los procesos electorales, pero el incremento de los ataques cibernéticos ha provocado que este avance haya desaparecido de la agenda a corto plazo.

Según datos de Interior, los ciberdelitos han aumentado en el primer trimestre del 2017 un 22,3% respecto del mismo periodo del año anterior. Un crecimiento exponencial, pues en el 2016 se registraron un 10,7% más de ciberataques que en el 2015.

Las ciberamenazas no son “un cuento chino”, 3 de 4 empresas son atacadas

Solo en los primeros tres meses de 2017, las denuncias subieron un 22,3 % respecto al primer trimestre del pasado año



Comentar (0) Imprimir Enviar por correo



MARÍA ABASCAL MADRID/SANTIAGO



Altos mandos de Defensa y expertos en ciberseguridad dieron ayer un toque de atención a quienes siguen creyendo que el ciberdelito es “un cuento chino”, una actitud “irresponsable” que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Teléfonica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío “muy serio y real” tildaron todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado.

Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes. Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este “cambio de paradigma” que el pasado año dejó 66.680 delitos, un 10,7 % más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 % respecto al primer trimestre del pasado año, lo que demuestra que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más. Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción “rápida y ágil” y que los efectos del ataque fueran “limitados”.

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, lanzó una advertencia: “Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE, no culminemos de las palabras a los hechos”.

El ataque de WannaCry ha sido “una pequeña muestra” del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, explicó Cubeiro.

“Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha”, ha reprochado este mando militar, antes de advertir que todavía la “magnitud” del problema “está lejos de ser entendida por una mayoría”. Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 % del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (Incibe), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

“Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes”, avisó Gómez, que ha definido el virus WannaCry como “facilón”, lo que permitió en pocas horas conocer “lo que hacía el bicho” y fabricar una vacuna.

Las ciberamenazas no son un cuento, 3 de 4 de empresas son atacadas, según expertos

Agencia EFE 1 de junio de 2017



El secretario de Estado de Seguridad, José Antonio Nieto, inaugura la Jornada sobre Ciberseguridad en España organizada por Club Diálogos para la Democracia y Telefónica, con expertos del INCIBE, del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa y del Centro Criptológico Nacional, entre otros, hoy en un hotel de Madrid. EFE

Madrid, 1 jun (EFE). - Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 68.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilon", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Digital

3 de cada 4 empresas españolas han sufrido un ciberataque en los últimos 5 años

02 Junio 2017



Tras el último **ciberataque** que afectó a miles de compañías a nivel mundial a raíz del ransomware WannaCry, entre ellas a Telefónica dejando inutilizados sus sistemas, la preocupación sobre la seguridad en la red solo ha ido en aumento.

cierto es que las cifras que ofrece el **Instituto Nacional de Ciberseguridad (Incibe)** no son demasiado halagüeñas.

Y es que reflejan que lejos de decrecer, los ciberataques en el territorio nacional no dejan de aumentar.

En los últimos 5 años 3 de cada 4 empresas españolas han sido **atacadas** mientras que, según Eurostat, el 25% del total de usuarios ha sufrido algún tipo de ciberataque, un porcentaje superior a la media europea que se sitúa en un 21%.

Además, las **denuncias por cibercrimitos aumentaron en el primer trimestre de 2017 un 22,3%**.

Pero, ¿a qué se deben estas preocupantes cifras? Según os expertos, a los bajos presupuestos destinados a la protección del entorno online. Así lo han asegurado las autoridades nacionales en una jornada sobre seguridad en internet celebrada esta semana en Madrid y que recoge el diario *El País*.

“Se invierte más en vallas que en ciberseguridad. ¿De dónde creen que vendrá el próximo ataque, de la valla o de un firewall? No se está respondiendo a esa amenaza ni con la agilidad ni con la contundencia que hace falta. Parece que están esperando a que pase algo más grave”, explicaba **Enrique Cubeiro**, jefe de Operaciones del Mando Conjunto de Ciberdefensa.

Asimismo, también ha aprovechado la ocasión para reivindicar la necesidad de invertir más recursos en un asunto de enorme importancia a pesar de que muchos lo consideren un tema menor.

“Mucha gente en los altos mandos estratégicos **todavía ve el asunto como un cuento chino**, pero la ciberseguridad es una de las capacidades más críticas para un Estado actualmente”, añadía.

La necesidad de **mayor inversión en este ámbito** es evidente si nos fijamos en las cifras destinadas a la seguridad online en nuestro país y en los de nuestro alrededor.

España se sitúa como el tercer país que más ciberataques recibe por detrás de Estados Unidos y Reino Unido pero la diferencia radica en que mientras Estados Unidos dedica 1.500 millones de dólares a la lucha contra los criminales en la red y Reino Unido invierte 2.300 millones de euros, España solamente destina 24,3 millones de euros al Incibe y 161 millones al CNI.

Estos números presentan una alarmante situación, sobre todo teniendo en cuenta la creciente amenaza que existe en la red.

Así, aunque el secretario de Seguridad del Ministerio del Interior, **José Antonio Nieto Ballesteros**, asegura que hacen lo que pueden, desde luego, no parece ser suficiente.

Las ciberamenazas no son un cuento, 3 de 4 de empresas son atacadas, según expertos

Efe | 01.06.2017 | 17:25

Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría". Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.



José Antonio Nieto, secretario de Estado de Seguridad. Efe

POLÍTICA

Interior descarta implantar el voto electrónico por la ciberdelincuencia

■ "Hoy el voto electrónico está más lejos que hace diez años. Es un riesgo que no debemos asumir", ha dicho José Antonio Nieto

Jueves, 1 de Junio de 2017 11:55

EL INDEPENDIENTE @redacion@elindpendiente.com

[f](#)
[t](#)
[in](#)
[e](#)
[Resumen](#)



José Antonio Nieto se dispone a comparecer este viernes ante la comisión de Interior del Congreso de los Diputados. EFE

El secretario de Estado de Seguridad, José Antonio Nieto, ha asegurado que la implantación del voto electrónico es un "riesgo" que España no debe asumir ante la creciente amenaza de la ciberdelincuencia, a pesar de contar con la tecnología para cambiar el sistema de votación.

En la inauguración de una jornada sobre ciberseguridad organizada por el Club de Diálogos para la Democracia y Telefónica, Nieto ha dejado claro que hoy por hoy el voto en papel para unas elecciones ofrece "más garantías" que el electrónico.

Nieto ha recordado que pese a que la Junta Electoral aconsejó hace siete años la puesta en marcha de este sistema de votación y de que España disponía del desarrollo tecnológico para hacerlo, "muy pocos se atreven hoy" a garantizar que ese voto electrónico no pueda ser manipulado y, por tanto, a que arroje los resultados veraces de unos comicios.

"Hoy el voto electrónico está más lejos que hace diez años. Es un riesgo que no debemos asumir", ha añadido el número dos de Interior que ha citado algunos de los problemas que han sufrido países como Francia con este tipo de votación.

Los ciberdelitos, una amenaza creciente en los últimos años

Sus expertos tildan su desafío de "muy serio y real" en cuya lucha se precisa personal muy cualificado



El secretario de Estado de Seguridad, José Antonio Nieto, en la jornada sobre ciberseguridad.

AGENCIAS MADRID 02/06/2017 02:50 H.

Alto mando de Defensa y expertos en ciberseguridad dieron ayer un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas. Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" tildan todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, según reveló uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, inauguró el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000. Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, dijo Nieto, que las empresas tienden a denunciar más.

advertencia a las empresas

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cibeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, lanzó una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, explica Cibeiro, crítico con la respuesta que se está dando. "Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", reprochó este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, resalta el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (Incibe), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, suscribió la llamada de atención del capitán de navío Enrique Cibeiro. "Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios" y definió el WannaCry como "facilón".



Les ciberamenaces no són un conte. 3 de cada 4 empreses són atacades

01/06/2017
MADRID »

Diuen que es necessitarà personal molt qualificat, però encara inexistent al mercat.

COMPARTEIX:

Alts comandaments de Defensa i experts en ciberseguretat han donat avui un toc d'atenció als qui segueixen creient que el ciberdelicte és "un conte xinès", una actitud "irresponsable" que dificulta la lluita contra una amenaça creixent que en els últims cinc anys han patit tres de cada quatre empreses.

Telefónica ha estat una de les últimes víctimes fa tot just quinze dies, a través d'una ciberatac a gran escala que va afectar a 74 països amb més de 45.000 incidents perpetrats pel virus del tipus ransomware WannaCry, un exemple que ha servit per il·lustrar el problema global a què s'enfronten els Estats en una jornada de ciberseguretat organitzada pel Club Diàlegs per a la Democràcia.

De desafiament "molt seriós i real" han titllat tots els especialistes aquestes ciberamenaces en la lluita es necessita personal molt qualificat, però encara inexistent al mercat. Com a dada, en una fira d'ocupació es van oferir recentment més de 2.000 llocs de treball per al sector de la ciberseguretat, però no es van cobrir ni la meitat, ha revelat un dels ponents.

Abans, el secretari d'Estat de Seguretat, José Antonio Nieto, ha inaugurat el debat sobre aquest "canvi de paradigma" que l'any passat va deixar 66.680 delictes, un 10,7 per cent més que el 2015, mentre que fa tot just quatre anys es produïen 43.000.

JORNADA CIBERSEGURIDAD (PREVISIÓN)

Expertos alertan: Ciberamenazas no son un cuento, 3 de 4 empresas son atacadas

01/06/2017 - 14:53 Agencia EFE



Altos mandos de Defensa y expertos en ciberseguridad han dado hoy un toque de atención a quienes siguen creyendo que el ciberdelito es "un cuento chino", una actitud "irresponsable" que dificulta la lucha contra una amenaza creciente que en los últimos cinco años han sufrido tres de cada cuatro empresas.

Telefónica ha sido una de las últimas víctimas hace apenas quince días, a través de una ciberataque a gran escala que afectó a 74 países con más de 45.000 incidentes perpetrados por el virus del tipo ransomware WannaCry, un ejemplo que ha servido para ilustrar el problema global al que se enfrentan los Estados en una jornada de ciberseguridad organizada por el Club Diálogos para la Democracia.

De desafío "muy serio y real" han tildado todos los especialistas estas ciberamenazas en cuya lucha se precisa personal muy cualificado, pero todavía inexistente en el mercado. Como dato, en una feria de empleo se ofertaron recientemente más de 2.000 puestos de trabajo para el sector de la ciberseguridad, pero no se cubrieron ni la mitad, ha revelado uno de los ponentes.

Antes, el secretario de Estado de Seguridad, José Antonio Nieto, ha inaugurado el debate sobre este "cambio de paradigma" que el pasado año dejó 66.680 delitos, un 10,7 por ciento más que en 2015, mientras que hace apenas cuatro años se producían 43.000.

Solo en los primeros tres meses de 2017, las denuncias se han incrementado un 22,3 por ciento respecto al primer trimestre del pasado año, lo que demuestra, ha dicho Nieto que, a pesar del propio aumento de este tipo de delitos, las empresas tienden a denunciar más.

Y en esa denuncia rápida, el número dos de Interior ha elogiado la responsabilidad de Telefónica, que puso de inmediato en conocimiento a las autoridades del problema, lo que permitió una reacción "rápida y ágil" y que los efectos del ataque fueran "limitados".

Precisamente, a los directivos de las empresas y, sin decirlo, a los responsables políticos, Enrique Cubeiro, el jefe de operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, ha lanzado una advertencia: "Es absolutamente irresponsable no tomarse en serio las ciberamenazas (...) Es frustrante que aunque ya es reconocido como un riesgo en la estrategia de seguridad de la UE no culminemos de las palabras a los hechos".

El ataque de WannaCry ha sido "una pequeña muestra" del escenario mundial cada vez más ciberdependiente en el que el ciberdelito deja pérdidas más cuantiosas que las del delito tradicional, ha explicado Cubeiro, crítico con la respuesta que se está dando.

"Están sonando las alarmas pero no se está respondiendo ni con la celeridad ni con contundencia. Parece que es necesario que pase algo muy grave para que la maquinaria se ponga en marcha", ha reprochado este mando militar, antes de advertir que todavía la "magnitud" del problema "está lejos de ser entendida por una mayoría".

Pese a ello, las cifras, no dejan lugar a dudas: el ciberdelito supone ya cerca del 0,8 por ciento del PIB mundial, ha resaltado el subdirector de servicios de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), Marcos Gómez, en tanto que el subdirector del Centro Criptológico Nacional, del CNI, Luis Jiménez, ha suscrito la llamada de atención del capitán de navío Enrique Cubeiro.

"Vamos sobreviviendo a la ciberamenaza pero hay que poner más medios y estar más vigilantes", ha avisado Gómez que ha definido el virus WannaCry como "facilón", lo que permitió en pocas horas conocer "lo que hacía el bicho" y fabricar una vacuna.

Interior descarta implantar el voto electrónico por el peligro de manipulación del resultado electoral

01/06/2017

diarioabierto.es. Las denuncias por cibercrimes crecieron un 22,3% en el primer trimestre de 2017 respecto a 2016.

El **Ministerio del Interior no se plantea poner en marcha el voto electrónico en España** debido al alto riesgo que existe de sufrir un ciberataque y que el resultado electoral sea manipulado, según ha revelado este jueves el **secretario de Estado de Seguridad, José Antonio Nieto**.

En una **jornada sobre ciberseguridad**, Nieto ha expuesto cómo ha cambiado la sociedad debido al uso de Internet y ha puesto como ejemplo el ámbito electoral. Según ha reconocido, **las campañas electorales "no se entenderían" actualmente sin el mundo virtual**, pero ello **conlleva también peligros** que hacen que Interior no se plantee implantar sistemas electrónicos de votación.

"**Hoy estamos más lejos del voto electrónico que hace diez años porque es muy manipulable**", ha confesado haciendo hincapié en que "muy pocos se atreven a garantizar la seguridad y veracidad" del resultado y se trata de "un riesgo" que, a su juicio, España "no debe asumir".

La **Junta Electoral Central (JEC) recomendó hace ya siete años al Gobierno el estudio** de sistemas que permitiesen en **uso de sistemas electrónicos** para los procesos electorales, pero Nieto ha insistido en que el incremento de los ataques cibernéticos durante los últimos años hace que se trate de un avance que no esté en la agenda a corto plazo. "**La tradicional papeleta sigue siendo más segura**", ha defendido.

Crecimiento de los ciberataques

Los denominados **cibercrimes** presentan un incremento exponencial año tras año. Las denuncias por este tipo de ataques en España durante el primer trimestre de 2017 **crecieron un 22,3 por ciento respecto al año anterior**, según ha expuesto el secretario de Estado, que ha revelado que **en 2016 se detectaron un total de 66.586 cibercrimes**, un 10,7 por ciento más que en 2015.

Estos datos son ligeramente **superiores a los del conjunto de la Unión Europea** porque los españoles aún deben **concienciarse de la necesidad de la protección en Internet**, ha explicado el secretario de Estado, que sin embargo ha destacado como aspecto favorable el aumento de las denuncias.

Nieto ha comparado esta situación con la de la **violencia de género**, donde sólo se denuncian el 20 por ciento de las agresiones existentes y el objetivo es aumentar estas denuncias. "La evolución del primer trimestre de los cibercrimes denunciados muestra una tendencia al alza, pero también un aumento de las denuncias", ha celebrado.

Los delitos cibernéticos fueron centro de atención tras el **ataque sufrido por más de 180 países el pasado 12 de mayo**, al que el 'número dos' del Ministerio de Interior ha asegurado que España reaccionó de forma "rápida y ágil" haciendo posible que sus efectos fueran "bastante limitados".

Según ha expuesto, **la cibercriminalidad permite la deslocalización del delito**, la multiplicación exponencial de sus efectos, la ocultación del delincuente y la dificultad de la labor policial y judicial. Además, al tener casi siempre un carácter internacional, exige una cooperación policial y judicial entre países que hace "más lentas" las operaciones.

Daesh multiplica su esfuerzo en Internet

Uno de los **focos de atención en el mundo de los delitos cibernéticos es el del terrorismo**, sobretudo después de que **Daesh** haya demostrado una gran agilidad en su manejo para la **captación y adoctrinamiento a través de las redes sociales** y "la expansión de su mensaje de odio".

"**El mal se desarrolla bien en las redes sociales**", ha reconocido Nieto, que ha explicado que Internet ha propiciado durante los últimos años una multiplicación de su mensaje que "no tiene precedentes". Y ha expuesto que, al mismo ritmo que los terroristas pierden territorio físico en Siria o Irak están "duplicando" su esfuerzo en el mundo virtual.

En este ámbito también ha asegurado que **España ha desarrollado un trabajo "de éxito"**, que demuestra el hecho de que todas las operaciones contra el terrorismo yihadista tuvieron su origen en seguimientos hechos en Internet. En esta legislatura, las operaciones antiterroristas se han saldado con un total de 81 detenidos.

España sufrió el año pasado 66.500 ciberataques, que han aumentado un 22% en 2017

2 junio, 2017 | España, Portada | 0 Comentarios



Nieto y Cubeiro junto a Gavilanes. / Foto: Diálogos para la Democracia

Eduardo González. 02/06/2017

Altos responsables de los Ministerios de Interior y Defensa advirtieron ayer de la necesidad de tomarse en serio la amenaza de la ciberseguridad, un problema cuya “magnitud está lejos de ser comprendida” por muchos dirigentes políticos y económicos y que se ha convertido en “la forma de alevosía más rentable de la historia de la humanidad”.

“Aunque parezca increíble, hay personas en puestos estratégicos que siguen pensando que esto de las ciberamenazas es un cuento chino”, declaró el capitán de navío Enrique Cubeiro, jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa, en el curso de la *Jornada sobre Ciberseguridad*, organizada por el Club Diálogos para la Democracia y Telefónica y presentada por el presidente del Club, Antonio Gavilanes Dumont.

A juicio de Cubeiro, es necesario “tomar conciencia de la gravedad de los ciberataques, porque sería irresponsable no hacerlo”. Se están haciendo “esfuerzos” para mejorar las capacidades, pero “no se está respondiendo con celeridad ni contundencia” ante una amenaza que “requiere de recursos económicos y de personal altamente cualificado”, advirtió. “Unas sólidas capacidades en ciberseguridad y ciberdefensa resultan esenciales para, no sólo la seguridad de una nación, sino incluso para su supervivencia”, manifestó.

En el caso de España, el capitán Cubeiro aseguró que la creación en 2013 del Mando Conjunto de Ciberdefensa ha ayudado a “consolidar” la capacidad operativa de las Fuerzas Armadas en esta materia y a encajar el denominado *quinto dominio de la guerra* (el referente al ciberespacio) en la estrategia nacional de defensa.

“España se ha adelantado en varios años a la OTAN, que no lo hizo hasta la última cumbre de Varsovia del año pasado”, cuando reconoció por primera vez el ciberespacio como “un nuevo dominio de las operaciones”, aseguró.

Defensa asegura que España se ha adelantado “en varios años” a la OTAN respecto al ciberespacio

Por su parte, José Antonio Nieto Ballesteros, secretario de Estado de Seguridad del Ministerio del Interior, precisó que en España (donde el 77% de sus habitantes son usuarios de Internet y el 48% tienen perfiles en redes sociales) se denunciaron 66.586 ciberdelitos en 2016, un 10,7% más que el año anterior.

“En el primer trimestre de 2017 han aumentado un 22,3% respecto al mismo periodo del año anterior”, puntualizó. El 25% de los usuarios de nuestro país han sufrido ataques, por encima del 21% de la media de la UE, lo que revela que “los niveles de protección de equipos en nuestro país están por debajo de la media europea”, alertó.

No obstante, según el secretario de Estado, el ataque masivo efectuado el pasado 12 de mayo con el virus *Wanna Try* tuvo unos efectos “muy limitados” en España gracias a que se “reaccionó con rapidez y agilidad”.

Interior asegura que la reacción de España en el ciberataque hizo que 'los efectos fueran limitados'

Seguridad 01 JUN 2017



Durante la Jornada sobre Ciberseguridad, organizada por el Club Diálogos para la Democracia, José Antonio Nieto Ballesteros, Secretario de Estado de Defensa en el Ministerio del Interior, ha hecho una valoración del ciberataque de WannaCry.

José Antonio Nieto Ballesteros, Secretario de Estado de Defensa en el Ministerio del Interior, ha asegurado, durante su intervención en la Jornada sobre Ciberseguridad que ha organizado Diálogos para la Democracia, que el panorama de la seguridad está cambiando con la llegada de las Nuevas Tecnologías.

En este sentido, Nieto Ballesteros ha hecho referencia al ciberataque de WannaCry, asegurando que éste tuvo "un impacto en extensión y en profundidad" al [afectar a 180 países y más de 300.000 ordenadores](#).

El Secretario de Estado de Defensa defendió el nivel de preparación de nuestro país ante amenazas de este tipo asegurando que, en el caso concreto de WannaCry, "España reaccionó con rapidez y agilidad" lo que hizo que "los efectos fueran muy limitados".

Asimismo, también se refirió [a la actuación de Telefónica](#), una de las primeras grandes compañías en comunicar que estaba siendo víctima de un ciberataque. "Telefónica demostró que la mejor manera de hacer frente a un ciberataque como el de WannaCry es no ocultarlo".

Antonio Gavilanes Dumont, presidente del Club Diálogos para la Democracia, también se refirió al ataque de WannaCry, remarcando la importancia que está adquiriendo la ciberseguridad y recordando que una de las "víctimas" más preocupantes fue el sistema de salud británico, al ser un servicio básico para los ciudadanos. "Debemos adoptar estrategias de prevención ya que se van a producir más ataques de este tipo".

José Antonio Nieto, Interior: 'Queremos que España sea un referente en seguridad digital'

Seguridad | 01 JUN 2017



José Antonio Nieto Ballesteros, Secretario de Estado de Defensa en el Ministerio del Interior, ha analizado la evolución de la ciberdelincuencia asegurando que ésta crece día a día. La intención del Ministerio es lograr que España sea un referente en seguridad digital, al igual que lo es en seguridad física.

Durante la Jornada de Ciberseguridad, organizada por el Club Diálogos para la Democracia, José Antonio Nieto Ballesteros, Secretario de Estado de Defensa en el Ministerio del Interior, ha explicado que nos encontramos ante una nueva realidad digital que ya se encuentra al mismo nivel "que el resto".

En este sentido, ha recordado que hay 7.395 millones de personas en el mundo, de los que el 46% se conecta a Internet, "lo que supone que hay más gente con acceso a la Red que con acceso a agua potable"; el 31% utiliza redes sociales; el 51% dispone de un teléfono móvil, y el 27% de la población mundial se conecta a Internet desde sus dispositivos móvil. Ante estos datos "nuestro mundo está virando. [La sociedad se está adaptando a una nueva realidad](#)".

En opinión de José Antonio Ballesteros, "hay que utilizar la revolución digital en beneficio de la humanidad. Necesitamos potenciar el uso de Internet para la educación y no convertirlo en una amenaza".

En este punto, el Secretario de Estado de Defensa del Ministerio del Interior ha asegurado que "es necesario que las administraciones se adapten" de tal manera que "no se dejen grietas para las ciberamenazas".

[La ciberdelincuencia](#) "permite la deslocalización y dificulta la labor policial", ya que "en casi todas sus acciones existe un componente internacional que dificulta el conocimiento". A todo esto, hay que unir que "el acceso a herramientas básicas de hacking cada vez es más sencillo", lo que está provocando que "se esté incrementando el número de la ciberdelincuencia en el mundo". No en vano, el *cryptovare* "es el principal tipo de malware en Europa". La ciberdelincuencia cada vez comete más acciones "como el robo de identidad, el fraude financiero, el robo de datos en redes sociales o la explotación infantil".

Es tal la preocupación que ha alcanzado que la UE ya ha incorporado el ciberterrorismo o el crimen organizado "en su variante cibernética" a su estrategia de seguridad.

Datos en España

En el caso de España, en 2016 se produjeron 66.586 ciberdelitos, un 10,7% más que en 2015, siendo el fraude y las estafas y las ciberamenazas los principales actos delictivos denunciados. "En el primer trimestre de este año, el número de ciberdelitos se ha incrementado en un 22,3% en comparación con el mismo periodo del año anterior" y "el 25% de los usuarios de Internet en España ha sufrido ataques de algún virus".

Para luchar contra este tipo de delitos José Antonio Nieto Ballesteros aboga por la cooperación pública de todos los Ministerios y comunidades autónomas; la cooperación pública privada con sectores sociales y la cooperación internacional.

En el primer punto "la Secretaría de Estado de Defensa del Ministerio del Interior colabora estrechamente con la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, así como con organismos como INCIBE o el CERT". La colaboración se extiende a otros Ministerios, como el de Justicia, "que nos está permitiendo reformar el código penal".

Este clima de cooperación "está haciendo que España se proteja y se proteja bien" ya que "lo que es seguro es que nos van a atacar".

Además de cooperación, José Antonio Nieto Ballesteros aboga por "educar a la sociedad civil", si no "es imposible que venzamos".

"La revolución digital es un hecho, no lo vamos a frenar y no la queremos frenar, pero hay que saber aprovecharla de manera segura". José Antonio Nieto Ballesteros ha finalizado destacando que "igual que España es una referencia en materia de seguridad física, queremos que lo sea en materia digital".



Por qué descarta Interior el voto electrónico

Por Redacción

Jueves 01 de junio de 2017, 18:00h

Me gusta 1 Compartir

G+ 0

Twitter

En la inauguración de una jornada sobre ciberseguridad organizada por el Club de Diálogos para la Democracia y Telefónica, Nieto ha dejado claro que hoy por hoy el voto en papel para unas elecciones ofrece "más garantías" que el electrónico.

El secretario de Estado de Seguridad, José Antonio Nieto, ha asegurado este jueves en una jornada sobre ciberseguridad, que la implantación del voto electrónico es un "riesgo" que España no debe asumir ante la creciente amenaza de la ciberdelincuencia, a pesar de contar con la tecnología para cambiar el sistema de votación.

Nieto ha recordado que pese a que la Junta Electoral aconsejó hace siete años la puesta en marcha de este sistema de votación y de que España disponía del desarrollo tecnológico para hacerlo, "muy pocos se atreven hoy" a garantizar que ese voto electrónico no pueda ser manipulado y, por tanto, a que arroje los resultados veraces de unos comicios.

"Hoy el voto electrónico está más lejos que hace diez años. Es un riesgo que no debemos asumir", ha añadido el número dos de Interior que ha citado algunos de los problemas que han sufrido países como Francia con este tipo de votación.

■ Economía



JORNADA SOBRE CIBERSEGURIDAD

“En España existe una implicación altísima de los técnicos y de la iniciativa privada para conseguir que sea tan segura virtualmente como ya lo es físicamente”



Destacan que en caso de ciberataque es importante la “ciberresiliencia”, es decir, disponer de un marco de defensa que nos permita llevar a cabo una respuesta rápida para actuar en tiempo real

By REDACCIÓN

MÁS ARTÍCULOS DE ESTE AUTOR

Viernes 02 de junio de 2017, 10:44h

Me gusta 0

+1 0

Twitter

El Club Diálogos para la Democracia y su presidente, Antonio Gavilanes Dumont, han organizado esta mañana, con la colaboración de Telefónica y el patrocinio de Audertis, McAfee, Fortinet, Symantec y Grant Thornton, una jornada sobre Ciberseguridad. Han participado como ponentes D. José Antonio Nieto Ballesteros, Secretario de Estado de Seguridad del Ministerio del Interior; D. Enrique Cubeiro Cabello, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa; D. Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Instituto Nacional de Ciberseguridad (Incibe) y D. Luis Jiménez Muñoz, Subdirector del Centro Criptológico Nacional.

El acto también ha contado con la participación especial como ponentes de D. José Luis Gilpérez, Director de Administración General del Estado, Defensa, Big Data y Seguridad de Telefónica, D. Óscar Bou, socio de Audertis, Dña. María Campos, Country Manager de McAfee; D. Acacio Martín, Director Regional para España y Portugal de Fortinet; D. Miguel Ángel Martos, Country Manager de Symantec; y Luis Pastor, socio de Consultoría Tecnológica e Innovación de Grant Thornton.

Celebrado en el Hotel Westin Palace de Madrid, ante un auditorio de 240 personas y la representación de más de 15 países, D. José Antonio Nieto Ballesteros, Secretario de Estado de Seguridad del Ministerio del Interior ha destacado que “la revolución de la tecnología de la información y comunicación es un hecho, no se puede frenar, no la vamos a frenar y no la debemos frenar, pero tenemos la obligación de utilizarla y aprovecharla en beneficio de la seguridad”. Y ha asegurado que en nuestro país “tenemos herramientas para poder hacerlo y una implicación altísima de los técnicos y de la iniciativa privada para conseguir que España sea tan segura virtualmente como ya lo es físicamente”.

Por su parte, D. Enrique Cubeiro Cabello, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa, ha querido transmitir la visión militar sobre Ciberseguridad. Cubeiro ha definido el ciberespacio como el “quinto dominio de la guerra”. El peligro reside en que se trata de un espacio en el que “no existe ningún tipo de control armamentístico y la infinidad de grupos, organizaciones e individuos aislados con muy diversas motivaciones tienen la capacidad de provocar daños muy graves en la sociedad”. Por lo tanto, “coloca el corazón de una nación en primera línea de combate”. Sin embargo, aunque las ciberamenazas son reconocidas como uno de los principales riesgos para la seguridad de la nación, “aún no hemos conseguido culminar ese gran paso que va de las palabras a los hechos”.

Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Instituto Nacional de Ciberseguridad (Incibe) ha informado durante su intervención de que “hay un hecho constatable y es que en el ciberespacio hay grandes oportunidades de todo tipo: sociales, económicas... Pero también hay ciberamenazas y riesgos, y por lo tanto hay que seguir trabajando en la detección y mitigación de los mismos”. Y ha concluido asegurando que “esto es un trabajo de todos los agentes públicos y privados”.

Y cerrando la mesa institucional, D. Luis Jiménez Muñoz, Subdirector del Centro Criptológico Nacional, ha destacado que para prevenir la “ingeniería social” que desarrolla los virus del tipo del ya famoso WannaCry, lo primero que hay que hacer es “concienciar a los usuarios del problema del uso de la tecnología de la información y de sus riesgos”. A continuación, “hay que formarles, dotarles de conocimientos, habilidades y práctica”.

Por otro lado, D. José Luis Gilpérez, Director de Administración General del Estado, Defensa, Big Data y Seguridad de Telefónica, ha destacado durante su discurso que lo más importante en materia de ciberseguridad es “poder anticiparnos a ataques dirigidos y detectar las vulnerabilidades que nos hacen estar más expuestos”. En Telefónica cuentan con cuatro pilares básicos para afrontar la situación: “Experiencia, infraestructuras robustas, excelencia operativa y mejora continua”. Y ha concluido advirtiendo que “tenemos que estar muy preparados y la innovación es algo fundamental”.

Y para finalizar, en la mesa empresarial en la que han participado D. Óscar Bou, socio de Audertis, Dña. María Campos, Country Manager de McAfee; D. Acacio Martín, Director Regional para España y Portugal de Fortinet; D. Miguel Ángel Martos, Country Manager de Symantec; y Luis Pastor, socio de Consultoría Tecnológica e Innovación de Grant Thornton, han coincidido en que la clave para estar protegidos reside en la cooperación entre los fabricantes, compartir la información para que todos sus clientes puedan estar seguros en todo momento. También se han mostrado de acuerdo con el hecho de que en España “necesitamos más profesionales con conocimiento y experiencia en el campo de la ciberseguridad, porque no somos capaces de cubrir toda la oferta”. Por último, en caso de ciberataque, han reiterado que la importancia de la “ciberresiliencia”, es decir, disponer de un marco de defensa que nos permita llevar a cabo una respuesta rápida para actuar en tiempo real.

Jornada de la Fundación Círculo

A. Conde: "Es una prioridad avanzar hacia una infraestructura integral de información"



Foto: Fundación Círculo

02/06/2017 | Madrid

B. Carrasco

El secretario de Estado de Defensa, **Agustín Conde**, defendió esta semana que una de las prioridades del **Ministerio de Defensa** para esta legislatura es "avanzar hacia una única *Infraestructura Integral de Información para la Defensa (I3D)*".

Durante una jornada organizada por la **Fundación Círculo**, bajo el título *Arquitectura global del Ministerio de Defensa, un modelo nacional de normalización e interoperabilidad*, Conde explicó que el ministerio impulsó el pasado mes de noviembre una nueva red integral de *Sistemas y Tecnologías de Información y Comunicaciones (CIS/TIC)* de Defensa.

A este respecto, el secretario apuntó que en el ámbito de las telecomunicaciones y la información el ministerio tiene tres objetivos "conseguir una única infraestructura integral de información para la Defensa, consolidar el desarrollo de la seguridad de la información, y adaptar, en el marco del proceso de transformación digital de la Administración General del Estado, los procesos internos del departamento".

Conde destacó que el empleo de tecnologías avanzadas en las Fuerzas Armadas produce "un efector multiplicador en su acción" y, para ello, la **Secretaría de Estado de Defensa** debe proporcionar "los medios materiales y los recursos financieros adecuados".

En este punto recordó que "tenemos que estar en continua actualización y adaptación, para evitar que los ataques cibernéticos como el ocurrido hace unos días con el *Ransomware WannaCry* pueda llegar a afectarnos".

Arquitectura global

Sobre el nuevo concepto de arquitectura global, explicó que "proporciona la referencia técnica para llevar a cabo el desarrollo normalizado de todas las capacidades *CIS/TIC* que precisa el departamento y es el instrumento que da la coherencia necesaria a la aplicación de la política para establecer la infraestructura *I3D*".

Entre sus características, añadió, "ha de asegurar la interoperabilidad de sistemas en dos ámbitos de actuación, en el marco de nuestros aliados de la **OTAN** y de la **Unión Europea**, y en el marco de la administración digital de la *Administración General del Estado*, y es en esta última donde tenemos que ser pioneros y vanguardia por nuestra experiencia adquirida".

140 millones de euros

Dentro de este proceso, el **Consejo de Ministros** autorizó a primeros de mayo una partida de casi 140 millones de euros para la contratación de los servicios e infraestructura de telecomunicaciones de la *Infraestructura Integral de Información para la Defensa (I3D)* del Ministerio de Defensa.



El jefe militar de ciberdefensa alerta de su importancia para la supervivencia de una nación

- Cree que la magnitud del problema está aún lejos de ser entendida por una gran mayoría de personas, muchas de ellas con altos cargos de responsabilidad
- En el caso de las empresas privadas, ha avisado de que deben tomar conciencia de que las mayores vulnerabilidades para su continuidad pueden llegar a través del ciberespacio

informacionsensible.com

01 de Junio del 2017 a las 15:41



Puntúa esta noticia: ★ ★ ★ ★ ★

El **Jefe de Operaciones del Mando Conjunto de Ciberdefensa**, el capitán de navío **Enrique Cubeiro**, ha sostenido este jueves que la ciberdefensa y la ciberseguridad son "esenciales" para la "supervivencia" de una nación y ha alertado de que "a día de hoy" son las capacidades "más críticas".

En unas jornadas sobre ciberseguridad organizadas por el Club Diálogo para la Democracia y por Telefónica, el capitán de navío ha reconocido que se están haciendo "esfuerzos" por mejorar las capacidades en esta materia, pero cree que **la magnitud del problema está aún lejos de ser entendida por una gran mayoría de personas**, muchas de ellas con altos cargos de responsabilidad.

En el caso de las empresas privadas, ha avisado de que deben tomar conciencia de que **las mayores vulnerabilidades para su continuidad pueden llegar a través del ciberespacio**. Y se ha preguntado por qué se acepta "con facilidad" invertir en seguridad física pero cuesta hacerlo en ciberseguridad. "¿Por dónde es más fácil que llegue un ataque? ¿a través de la valla o del ciberespacio?", ha preguntado.

Cubeiro ha apuntado que **tres de cada cuatro empresas han sido objeto de un ciberataque durante los últimos cinco años** y las pérdidas sufridas por ellos superan ya a las que provoca el crimen internacional, siendo "mortales" para muchas pequeñas y medianas empresas.

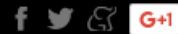
Por todo ello, ha pedido dejar de ver a los expertos en ciberseguridad y ciberdefensa como "los tipos raritos del cuarto sótano" o "cazafantasmas que persiguen figuras esotéricas" y ha defendido que se trata de un ámbito que **requiere de recursos económicos** y una importante masa de personal cualificado. "Unas sólidas capacidades en ciberseguridad y ciberdefensa resultan esenciales para, no sólo la seguridad de una nación, sino incluso para su supervivencia --ha alertado--. Y a día de hoy son las más críticas".

En este punto, **ha reconocido que el ataque sufrido por 180 países el pasado 12 de mayo a través del virus WannaCry puede incluso haber sido "bueno" para los expertos en este ámbito**, ya que ha ayudado a concienciar sobre su importancia. "Aunque parezca increíble todavía hay personas, algunas en puestos estratégicos, que siguen considerando esto de las ciberamenazas un cuento chino", ha lamentado.

El capitán de navío ha recordado que se trata de un asunto reconocido como uno de los principales riesgos para la seguridad de la nación, pero aún no se ha culminado "ese gran paso que va de las palabras a los hechos".

España descarta implantar el voto electrónico por la creciente ciberdelincuencia

ESPAÑA CIBERSEGURIDAD | 01 de Junio de 2017



Madrid, 1 jun (EFE).- El secretario de Estado de Seguridad español, José Antonio Nieto, aseguró hoy que la implantación del voto electrónico en el país es un "riesgo" que no se debe asumir ante la creciente amenaza de la ciberdelincuencia.

El ciberataque global "WannaCry", que tuvo lugar el pasado 12 de mayo, aprovechó una vulnerabilidad de sistema operativo Microsoft Windows para secuestrar datos procedentes de más de 200.000 ordenadores en 150 países, entre ellos España, donde una de las empresas afectadas fue Telefónica.

En dicho ataque, se exigió un pago en la moneda digital bitcoin para recuperar el acceso a los ordenadores y el contenido digital de las víctimas, que permanecía como "rehén" hasta que se pagara el rescate.

Nieto hizo esa declaración en una jornada sobre ciberseguridad organizada en Madrid, y destacó que a día de hoy el voto en papel para unas elecciones ofrece "más garantías" que el electrónico, ya que "muy pocos se atreven" a garantizar que sea un sistema exento de manipulaciones.

En Latinoamérica, Brasil fue el primer país en empezar a automatizar sus elecciones, seguido de Ecuador y Perú, pero "en España hoy el voto electrónico está más lejos que hace diez años", según explicó Nieto, quien mencionó algunos de los problemas sufridos en Europa con este tipo de votación.



El secretario de Estado de Seguridad, José Antonio Nieto, inaugura la jornada sobre ciberseguridad en España organizada por Club Diálogos para la Democracia y Telefónica, con expertos del INCIBE, del Mando Conjunto de Ciberdefensa del Estado Mayor de la Defensa y del Centro Criptológico Nacional, entre otros, hoy en un hotel de Madrid. EFE

¡GRACIAS!



Elite CONEXIÓN | C/ Padilla, 82 | 28006 Madrid
Publicidad no convencional | Comunicación | Eventos |
Relaciones públicas | Patrocinio | Gabinete de Prensa