TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TIJUANA

DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN

SEMESTRE:

4TO

CARRERA Y GRUPO:

INGENIERÍA INFORMÁTICA – IF4A

MATERIA:

TALLER DE LEGISLACIÓN INFORMÁTICA

ACTIVIDAD:

CASO DELITO INFORMÁTICO

UNIDAD:

6

ALUMNO:

CASTELAN DELGADO LAKSHME RADHARANE 20212108

GARCÍA SALGADO MONCAYO NASHELLY 19211149

ROMERO DIAZ MISAEL 20212748

DOCENTE:

DANIELA ADRIANA SANCHEZ VIZCARRA

FECHA DE ENTREGA:

VIERNES 31 DE MAYO DE 2022

Alemania sufre el ataque cibernético de mayor magnitud de su historia

Por Marta Rodriguez Martinez & Jez Fielder • última actualización: 04/01/2019

Al menos un **centenar de políticos alemanes** de todos los partidos, a excepción del ultraderechista Alternativa para Alemania (AfD), han sido víctimas de **un incidente masivo de piratería informática**. Entre los datos vulnerados figura información personal como detalles de tarjetas de crédito, números de teléfono móvil y direcciones de email.

La portavoz del grupo parlamentario del partido de izquierda Linke fue la primera en confirmar que el ataque cibernético había afectado a sus miembros. "Puedo confirmar que ha habido un incidente", dijo Sarah Wagenknecht, quien añadió que **Dietmar Bartsch**, líder del grupo del partido en la Cámara baja del Parlamento alemán, estaba entre los perjudicados.

El ataque cibernético ha sido "muy aleatorio y no se dirigió a ninguna persona en particular", explicó a Euronews Sonia Giese, portavoz de prensa de Linke.

Deutsche Welle informó que todos los partidos políticos han sido blanco de ataques, con excepción del partido de extrema derecha **AfD**.

Euronews se puso en contacto con AfD, que dijo que no son responsables del ataque de piratería informática.**"¿Estás bromeando?"**, fue su respuesta exacta. Aunque parece que la información de los miembros de la AfD no ha sido expuesta, el partido dice que "aún no hemos comprobado los archivos".

La oficina de Angela Merkel fue uno de los objetivos de los *hackers*, dijo el viernes un portavoz del Gobierno, aunque, por el momento, creen que no se ha publicado información sensible de la canciller alemana. "En cuanto a la cancillería, parece que, a juzgar por la revisión inicial, no se han publicado datos e información delicada, y esto incluye (de) la canciller", dijo el portavoz en una rueda de prensa.

Un calendario de adviento con información pirateada

Una cuenta de Twitter con 17,7 mil seguidores (actualmente) ha estado publicando información personal como si se tratara de un **"calendario de adviento"**, es decir dosificando la revelación de datos pirateados cada día hasta la víspera de Navidad.

La última "puerta", la del pasado 24 de diciembre, estaba reservada para la alianza de Gobierno de centro-derecha **CDU/CSU**. Aún se desconoce si la información es comprometedora.

La **Oficina Federal Alemana para la Seguridad de las Tecnologías de la Información** tuiteó que están "examinando intensivamente el caso en estrecha cooperación con otras autoridades federales".

"El Centro Nacional de Ciberdefensa se ha hecho cargo de la coordinación central. De acuerdo con el conocimiento actual no hay preocupación de las redes gubernamentales", continuó el tuit.

Euronews telefoneó a varios políticos alemanes cuyos detalles habían sido filtrados. Una de ellas, **Jana Schimke**, del CDU, dijo que ni siquiera sabía que había sido pirateada, pero, visto que nuestro periodista había

podido hacer esa llamada con el número de teléfono publicado por el hacker, eso demostraba efectivamente que sus datos personales habían sido vulnerados.

Patrick Sensburg, también de la CDU, confirmó que su oficina había sido víctima de un ataque de *phishing*, una técnica fraudulenta que permite suplantar la identidad informática de una persona.

¿Cómo de sofisticado fue el ataque?

James Chappell, fundador y director de Innovaciones de la empresa de riesgos digitales Digital Shadows, dijo a Euronews que estaba "definitivamente en el extremo más sofisticado".

¿Qué pueden hacer las organizaciones para prevenir estos ataques?

"Los tipos de protección tienen que ser bastante amplios, si observamos los ataques al Parlamento británico del año pasado, hemos visto muchos consejos personales a los diputados sobre cómo pueden protegerse a sí mismos, sin duda eso es lo que va a suceder en este caso, aunque es una especie de cierre de la puerta del establo después de que el caballo se haya desbocado", dice Chappell.

"Se trata de educar a la gente sobre cómo estar seguros, y estoy seguro de que las BSI de Alemania centrarán muchos esfuerzos en tratar de minimizar el impacto de esto".

¿Qué pueden hacer las organizaciones para prevenir estos ataques?

"Los tipos de protección tienen que ser bastante amplios, si observamos los ataques al Parlamento británico del año pasado, hemos visto muchos consejos personales a los diputados sobre cómo pueden protegerse a sí mismos, sin duda eso es lo que va a suceder en este caso, aunque es una especie de cierre de la puerta del establo después de que el caballo se haya desbocado", dice Chappell.

"Se trata de educar a la gente sobre cómo estar seguros, y estoy seguro de que las BSI de Alemania centrarán muchos esfuerzos en tratar de minimizar el impacto de esto".

Tipos de delitos informáticos

Los tipos de delitos informáticos reconocidos por Naciones Unidas

1. Fraudes cometidos mediante manipulación de computadoras

- MANIPULACIÓN DE LOS DATOS DE ENTRADA
- MANIPULACIÓN DE PROGRAMAS
- MANIPULACIÓN DE LOS DATOS DE SALIDA
- MANIPULACIÓN INFORMÁTICA APROVECHANDO REPETICIONES AUTOMÁTICAS DE LOS PROCESOS DE CÓMPUTO

2. Falsificaciones informáticas

- COMO OBJETO
- Cuando se alteran datos de los documentos almacenados en forma computarizada.
- COMO INSTRUMENTOS: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

3. Daños o modificaciones de programas o datos computarizados

- SABOTAJE INFORMÁTICO
- VIRUS
- GUSANOS
- BOMBA LÓGICA O CRONOLÓGICA

4. Acceso no autorizado a servicios y sistemas informáticos

- PIRATAS INFORMÁTICOS O HACKERS
- REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL

Bibliografía

Seguridad informÃ¡tica - Los tipos de delitos informÃ¡ticos reconocidos por Naciones Unidas. (s. f.). Seguridad informática - Los tipos de delitos informáticos reconocidos por Naciones Unidas. Recuperado 31 de mayo de 2022, de http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Martinez, M. R. (2019, 4 enero). *Alemania sufre el ataque cibernético de mayor magnitud de su historia*. euronews. Recuperado 31 de mayo de 2022, de https://es.euronews.com/2019/01/04/un-ataque-cibernetico-masivo-a-politicos-alemanes-hace-publico-sus-datos-personales