2013-08-22

CiberNoticias # 14

SCProgress

www.scprogress.com

ÍNDICE

1. Las recompensas en materia de seguridad de Facebook han llegado al millón.....03
2. Hackeo de autos permite acelerar y frenar desde una PC.....04
3. Guerras cibernéticas: nerds al ataque.....06

Noticia # 01: Las recompensas en materia de seguridad de Facebook han llegado al millón.

Dos años han pasado desde que Facebook lanzase su programa de recompensa en materia de seguridad informática, desde ese momento este gigante de Internet ha desembolsado más de un millón de dólares por dichas bonificaciones. En total han sido 329 personas –desde investigadores a estudiantes, de 51 países diferentes. A destacar, que el más joven tenía 13 años y que dos de los receptores trabajan a tiempo completo en el equipo de seguridad de Facebook.

Collin Greene, ingeniero de seguridad de la red social, ha publicado estos datos en Internet y además ha hecho público que la mayor parte del millón de dólares repartido se ha quedado en Estados Unidos (20%), seguido de India, Reino Unido, Turquía y Alemania. Además, los países con más interés han sido India, Turquía, Israel, Canadá, Alemania, Paquistán, Egipto, Brasil, Suecia y Rusia. Greene, comentó que el "programa de recompensas nos permite aprovechar el talento y la perspectiva de todo tipo de personas y de todas las partes del mundo".

El precio mínimo de cada recompensa es de 500 dólares y el precio máximo no está fijado y puede ser de cualquier valor, en proporcionar a la importancia del fallo. Por ejemplo, la mayor recompensa que se ha pagado fue de 20.000 dólares y el cazador de recompensas que tiene su bolsa más llena es un investigador que consiguió obtener hasta 100.000 dólares.

Fuente: Crytex – Seguridad informática

Noticia # 02: Hackeo de autos permite acelerar y frenar desde una PC.

Los investigadores de seguridad informática Charlie Miller y Christopher Valasek revelaron métodos que descubrieron para hackear las computadoras de automóviles y obtener control de la dirección, aceleración, frenos y otras funciones importantes.

Miller, ingeniero de seguridad en Twitter, y Valasek, director de inteligencia de Seguridad en IOActive, investigaron durante 10 meses hasta que lograron irrumpir en la red de sistemas informáticos integrados, llamados unidades de control electrónico (ECU, por sus siglas en inglés), utilizados en coches modernos.

Los investigadores conectaron una laptop al sistema de comunicación de la ECU y enviaron códigos maliciosos al sistema de dos automóviles, un Toyota Prius y una Ford Escape, ambos modelo 2010.

Mediante esto, descubrieron que podían desactivar los frenos mientras el vehículo estaba en marcha, mover el volante, ajustar la aceleración y hasta dañar el motor, soltar el cinturón de seguridad, mostrar información falsa para engañar al contador y medidor de combustible, encender y apagar las luces del vehículo, así como activar el claxon.

Los investigadores también encontraron una manera de hacer ataques persistentes al cambiar el firmware de la ECU para enviar las señales equivocadas, incluso cuando no se está conectado físicamente a las unidades de control.

Fuente: Crytex – Seguridad informática

De acuerdo con la agencia de noticias IDG News Service, se entregó a los fabricantes Ford y Toyota, un documento que explica cómo se realizó el hackeo al sistema de estos vehículos.

Toyota dijo que esto no era un truco y que los esfuerzos de la compañía en materia de seguridad se han centrado en la prevención de ataques a distancia o fuera el coche, no los relacionados con el sistema de control de acceso físico.

De acuerdo con los investigadores, no hay ninguna diferencia entre un acceso local o remoto, ya que acceder a la ECU abre la puerta a toda la red y permite dar cualquier comando.

"Queremos que otros investigadores trabajen en esto, en otros coches o en los mismos autos", dijo Miller. "Nos tomó 10 meses hacer este proyecto, pero si tuviéramos las herramientas que tenemos ahora, lo habríamos hecho en dos".

Fuente: Crytex – Seguridad informática

Noticia # 03: Guerras cibernéticas: nerds al ataque.

Sin bombas y sin tanques. Basta una computadora e Internet. Los combatientes del siglo XXI ejecutarán sus planes desde una simple oficina y pondrán a muchos países a sus pies.

Nadie sabe por qué sale agua sucia del grifo. No hay electricidad y resulta muy difícil explicar qué está pasando. Hay accidentes por toda la ciudad, los semáforos dejaron de funcionar. La gente comenta el último problema que ha tenido la central nuclear. Así podría ser una guerra cibernética: un ataque masivo efectuado y controlado desde una computadora. No habrá bombas ni soldados con tanques, tampoco granadas ni chalecos antibalas; sino simplemente poderosas computadoras, un buen programador informático y una conexión a Internet.

Fuente: www.dw.de

Protección inadecuada

Sandro Gaycken, especialista en seguridad informática.

"Afortunadamente estamos viviendo un período pacífico, así que por el momento no debemos tener miedo a este tipo de ataques", explica Sandro Gaycken, un experto en seguridad informática de la Universidad Libre de Berlín. Pero si la situación geopolítica cambiara, Alemania se encontraría no muy bien protegida: "La infraestructura básica alemana tiene un nivel de protección muy bajo en muchos aspectos. Si alguien quisiera atacarnos con métodos cibernéticos, podría hacerlo".

Diariamente hay ataques cibernéticos en algún lugar del mundo: son ataques pequeños y dirigidos a infraestructuras gubernamentales, oficinas militares o simplemente compañías. Nadie sabe quién está detrás de ellos. La verdad se conoce solo varios meses o incluso años después. Generalmente, los hackers buscan espacios digitales desprotegidos y se dedican a ver cómo pueden utilizarlos para causar daño. En ocasiones, son los mismos gobiernos los que planean estos ataques.

Fuente: www.dw.de

Stuxnet: un virus contra el programa nuclear de Irán

Stuxnet fue un virus creado para desestabilizar el programa nuclear de Irán.

Uno de los casos más conocidos de los últimos años fue el virus Stuxnet. Se cree que fue el responsable de que las plantas nucleares de Irán se salieran de control. Según la información disponible, el virus manipuló la frecuencia de rotación de las fuerzas centrífugas que permitían el enriquecimiento del uranio. De acuerdo con The New York Times, el virus fue desarrollado por el servicio secreto de Estados Unidos, la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) y agentes israelíes.

El presidente de Estados Unidos, Barack Obama, ha pedido una lista con todos los posibles ciberataques que podrían perpetarse en las oficinas estadounidenses ubicadas en el extranjero. Así lo ha señalado una información clasificada como "confidencial" y revelada por el diario británico The Guardian.

Fuente: www.dw.de

La OTAN crea directivas

¿Pero se pueden considerar estos ataques como actos de guerra? ¿Cómo podría responder un Estado a un ataque similar? Una unidad de la OTAN especializada en delitos cibernéticos ha creado un manual con más de 95 reglas que orientan a sus Estados miembros en caso de que hayan sido víctimas de un ataque cibernético. Estas propuestas no son vinculantes.

El experto en derecho internacional Wolff Heintschel von Heinegg, de la Universidad Europea en Frankfurt (Oder), contribuyó a la creación del manual. "En términos legales no existe ninguna diferencia entre hacer estallar un proyectil de artillería o provocar un ataque cibernético", dice a Deutsche Welle.

Fuente: www.dw.de

Una peligrosa amenaza

Un ataque cibernético podría causar daños importantes en la economía de un país.

Al mismo tiempo, no sería legítimo responder a cada ataque cibernético como si se tratara de un arma de destrucción y utilizar el argumento de la autodefensa. "Es necesario que el daño sea particularmente severo", dice von Heinegg. Si ese fuera el caso, la víctima podría responder con armas convencionales como bombas, por ejemplo.

El experto en Tecnologías de la Información Gaycken no ve factible ese escenario. Piensa que los ataques cibernéticos son más bien una peligrosa amenza económica: "Se pueden sabotear aspectos muy concretos de industrias claves, como por ejemplo, la automovilística o la aérea. Si estas presentaran fallas tendrían que retirar su productos y eso podría hacerles perder credibilidad".

Tanto el espionaje industrial como los ataques cibernéticos podrían causar daños importantes a la economía de un país y, a largo plazo, llevarla al colapso.

Fuente: www.dw.de