Publicado en Madrid el 06/07/2018

Radiografía del perfil del ciberatacante, según IMF Business School

Un empleado despistado, un cliente despechado, un hacktivista o el conocido pirata informático son algunos de los responsables de la mayoría de los ciberataques sufridos, según ha analizado IMF Business School

El riesgo de sufrir un ciberataque es cada día más común. Un tercio de los españoles ha sido víctima de algún ataque online, según un estudio realizado por la empresa Norton. Informe que sitúa a España en el tercer puesto de los países que más ciberataques sufren, después de EEUU y Reino Unido.

Pero ¿quién está detrás de estos ciberataques? Para resolver esta duda, desde IMF Business School, han analizado los perfiles más comunes de ciberatacantes que existen:

El despechado. Son aquellos usuarios de Internet que tienen un conocimiento mínimo de cómo llevar a cabo un ciberataque o tienen acceso a programas o aplicaciones para hackear. Sobre todo, se trata de empleados despedidos en injustas condiciones que utilizan sus propios conocimientos de la empresa para llevar a cabo el ciberataque o clientes no conformes con una compra o devolución que buscan "vengarse".

El despistado. Se trata de aquellos ataques que han sido creados fuera de la empresa, pero que es alguien del propio equipo quién, de forma accidental, facilita su acceso: ya sea a través de un email o descarga. La falta de formación de los trabajadores sobre ciberseguridad les convierte en un blanco fácil.

El hacktivista. Es un nuevo movimiento que está tomando cada vez más poder en Internet. Su principal motivación es denunciar injusticias o abusos. Estos hacktivistas conocen a la perfección las herramientas y técnicas utilizadas por los hackers, pero las ponen en marcha por una causa política o social. Por ejemplo, dejar un mensaje visible en la página principal de algún organismo público o lanzar un ataque de denegación de servicio para interrumpir el tráfico a una web.

El pirata informático. Conocidos como "hackers de sombrero negro", tienen un gran conocimiento de programación. Su objetivo es vulnerar la seguridad de un computador o una red mediante programas como el "ransomware" y, de esta forma, perjudicar al usuario obligándolo en la mayoría de los casos a pagar para recuperar su información.

El terrorista cibernético. Generalmente, estos hackers pertenecen a grupos organizados que buscan crear el miedo en la población atacando a las infraestructuras tecnológicas críticas de países enteros o corporaciones. Rara vez se trata de ataques organizados por un solo individuo. Detrás de sus actos se encuentran creencias religiosas o políticas extremistas.

Para Carlos Martínez, presidente de IMF Business School, "la formación es nuestra mejor defensa. Necesitamos dotar a las empresas de profesionales que conozcan el entorno, las herramientas y las metodologías para prevenir este tipo de ataques. Por ese motivo, desde la escuela hemos puesto en marcha un nuevo Máster en Ciberseguridad con modalidad online y presencial de la mano de empresas expertas en el sector como Deloitte y Ametic".

Datos de contacto:
Redacción

Nota de prensa publicada en: Madrid

Categorías: Nacional Madrid Ciberseguridad