Si el Chapo Guzmán volviera a nacer querría ser Hacker

Descripción

> El cibercrimen genera beneficios por 600.000 millones de dólares al año por sólo los 320.000 millones de dólares anuales que genera el narcotráfico.

Empresas de todo el mundo están inmersas en la transformación digital de sus negocios. Millones de personas se conectan, cada día a internet, ajenos de qué sucede más allá de sus dispositivos y por dónde circulan los datos que intercambian. Y mientras, los ciberdelincuentes acechan en las sombras dispuestos a darnos un mal día.

Sólo en nuestro país se reciben cerca de 40.000 ciberataques diarios (Datos 101). A nivel mundial se registra un ataque cibernético cada 39 segundos (Universidad de Mayland).

Y es que el cibercrimen es más rentable y provoca más daño que el narcotráfico. Los cibercriminales consiguen robar 600.000 millones de dólares al año a gobiernos, empresas e individuos y se estima que el impacto en la economía llegará a ser de 5,2 billones en 2023 (Foro Económico Mundial). Comparativamente, el narcotráfico es capaz de generar 320.000 millones de dólares anuales y su impacto negativo en la economía es de 2,2 billones.

Uno de los ámbitos más vulnerables está en los sistemas de control industrial donde es fácil encontrar vulnerabilidades. El 90% de éstas no requieren de condiciones especiales para provocar una brecha y, además, son fácilmente repetibles (Clarity). El 71 % de las vulnerabilidades pueden suponer un daño profundo a la empresa y el 66% ni siquiera requieren de la participación humana para provocar la brecha de seguridad.

El principal problema es que la mayoría de los ejecutivos de negocios están convencidos, erróneamente, de que sus compañías tienen integrados mecanismos resilientes ante ciberataques.

Pero no sólo afecta a las empresas privadas, sino también a la administración pública. Un ejemplo claro se encuentra en el ciberataque sufrido en marzo de 2021 por el Servicio informático del SEPE paralizando a más de 700 oficinas del Servicio Público de Empleo Estatal y poniendo en riesgo el sistema de pago de prestaciones por desempleo. Otro ejemplo llamativo sucedió sólo tres meses después del ataque al SEPE, en esta ocasión contra el Ministerio de Trabajo y Economía, dejando a unos 5.500 funcionarios parados

durante más de 15 días.

Incluso el FBI fue crackeado en noviembre de 2021, poniendo de manifiesto lo vulnerables que son las agencias estatales. De hecho, el 57% de las organizaciones europeas sufrió un ataque de ransomware que bloqueó el acceso a sus sistemas en 2021 (IDC Research).

El miedo a los ciberataques ha hecho que el sector de la ciberseguridad siga en crecimiento continuo. Este mercado sobrepasará en España los 1.749 millones de euros en 2022, un 7,7% más que en 2021, siendo la inversión en seguridad en la Administración Pública la que más crecerá.

Se estima que en 2023 el 55% de las organizaciones asignará la mitad de sus presupuestos de seguridad (IDC Research).

Se espera que el tamaño del mercado global de servicios de ciberseguridad esté en torno a los 190.000 millones de dólares en 2028 con un crecimiento medio anual del 10,2% (Grand View Research).

Pero España, tercera en la lista de países más tacados del mundo, le siguen faltando profesionales de ciberseguridad, unos 38.000 especialistas (ISC). A nivel europeo se necesitan más de un millón.

Tal es la necesidad que incluso se ha puesto de moda el ciberdelito como servicio y la idea de ofrecer prácticas ciber delictivas de pago.

En contrapartida, han surgido muchas empresas y expertos que ofrecen servicios de hacking ético, que se centra en evaluar la seguridad informática e identificar vulnerabilidades en sistemas, redes o infraestructuras mediante acciones de hacking de cara a fortalecer las propias defesas de las compañías que los contratan.

Sin duda, tanto en el lado del ataque, como en el de la defensa, el mercado de la ciberseguridad está en crecimiento notable y así parece que seguirá unos años más.

Este articulo fue originalmente publicado en la revista ADN Emprendedores