# Ransomware y sesgos cognitivos: porqué los empleados hacen clic y abren la puerta a los ciberdelincuentes

nexus aggity

En los últimos años el ransomware se ha convertido en uno de los incidentes de ciberseguridad que más afectan y preocupan a las empresas, independientemente de su tamaño y el sector en el que operan. Y es que, a medida que las empresas se vuelven más digitales, se abren nuevas oportunidades para que los ciberdelincuentes. Prueba de ello es que el 54% de los ciberataques denunciados por empresas de todo el mundo durante 2020 fue causado por ransomware, según una investigación de Bitsight con datos de la Universidad de Cambridge.

De acuerdo con un estudio de EY, más del 90% de incidentes de ciberseguridad tiene su origen en un error humano, fundamentalmente debido a la sencillez con la que ciberdelincuentes se aprovechan de las vulnerabilidades humanas al conocer cómo funcionan los sesgos cognitivos, un fenómeno psicológico de la mente, principalmente inconsciente.

"Todas las empresas nos encontramos ante un nuevo escenario que nos obliga a formar concienzudamente a nuestros trabajadores, a ponerlos a prueba, a hacerlos conocedores de las últimas tendencias en ciberdelincuencia, y siempre a través de recursos más originales y realistas huyendo de los típicos y denostados powerpoints o charlas poco atractivas". según indica Daniel Puente Pérez, CISO en Cirsa.

Según reflejan algunos estudios e investigaciones, las personas tomamos alrededor de 35.000 decisiones de media al día de las cuales solo 91 son conscientes.

El resto las toma nuestro cerebro con atajos mentales o sesgos cognitivos, entre los que se encuentran hacer o no clic en un enlace malicioso en un correo que recibimos.

## Ser conscientes y protegernos de nuestros sesgos cognitivos para hacer frente al ransomware

Los sesgos cognitivos forman parte de la naturaleza humana y de nuestra evolución como especie, por ello no podemos eliminarlos de nuestros equipos y organizaciones, pero sí podemos dominarlos.

Porque como señala Antonio Fernandes, Hacker y Divulgador en ciberseguridad, "Cuándo un grupo criminal escoge un objetivo, ha existido detrás una investigación de ciberinteligencia de la compañía, un perfilado de sus empleados y un estudio de cómo trabajan para, entre otras cosas, definir cómo puedan aumentar las posibilidades de éxito".

Conocer cómo funciona nuestro cerebro y cuáles son sus principales vulnerabilidades a través de los sesgos abre una nueva dimensión en la detección y desarrollo de comportamientos.

En este sentido, el primer estudio sobre Sesgos Cognitivos y Ransomware de Aiwin ha encontrado más de 30 sesgos cognitivos concretos que demuestran que "pensar antes de hacer clic", como parte de la cultura de ciberseguridad de una empresa, no es tan sencillo como recordárselo una y otra vez al empleado.

Estos son algunos de ellos:

### Efecto de verdad ilusoria

A nuestro cerebro le resulta más sencillo procesar información que hemos experimentado con anterioridad. Esto crea una sensación que nos puede llevar a malinterpretar una señal como un contenido verdadero. De esta forma, los ciberdelincuentes pueden realizar ataques de phishing aprovechando el principio de colaboración, reciprocidad y confianza.

## Sesgo de percepción selectiva

Se da cuando la persona recibe una información y, en función de sus expectativas, selecciona automáticamente un objeto de atención y desatiende la parte restante para no saturarse. Con su activación, se puede caer en prácticamente cualquier técnica de ingeniería social.

## Efecto Bandwagon

Tiene lugar cuando el cerebro hace decisiones basadas en emociones y en el impulso de grupo. Por ejemplo, se activa cuando seguimos lo que hacen nuestros compañeros asumiendo que es seguro o sensato hacerlo. Si alguien envía un enlace a un chat de trabajo y más personas están reaccionando a él, el temor a perderse algo y quedarse "fuera" puede superar a su formación sobre ciberseguridad y puede hacer clic en el enlace.

## Sesgo de automatización

Se da cuando nuestro cerebro confía más en la información que da un sistema automatizado que la que ofrece un sistema no automatizado, como la recopilada por una persona, incluso aunque sea correcta. Con ello se puede caer en prácticamente todas las técnicas de ingeniería social, pero especialmente en las que aprovechan el principio de urgencia.

## Sesgo de optimismo o ilusión de invulnerabilidad

El cerebro humano está programado para ser optimista en general y, a menudo, subestima la probabilidad de que se produzcan eventos adversos. En nuestra vida cotidiana puede ser beneficioso, pero en ciberseguridad se necesita justo lo contrario, es decir, estar siempre alerta. Un buen ejemplo de los efectos de este sesgo es cuando un empleado piensa "la empresa nunca va a ser vulnerada por un clic que yo haga en un correo".

Estos son solo 5 sesgos cognitivos que están influyendo de manera automática e irreversible en las 35.000 decisiones que tomamos al día, incluidas abrir correos, hacer clic en enlaces ransomware o dar información confidencial a los ciberdelincuentes.

Fuente de información:
https://www.revistacloudcomputing.com/