Edición No. 8 – julio 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

Ciberamenazas contra entornos corporativos

¿Alguna vez te has preguntado qué sucedería si los ciberdelincuentes tuvieran acceso al correo electrónico corporativo, al sitio web o que simplemente toda la información de la clínica no pudiera ser accesible a causa de una infección por *malware*? La respuesta es simple, la capacidad de la clínica para continuar con su actividad y la confianza de los pacientes y proveedores se podrían ver seriamente afectada, y por lo tanto su continuidad. Además, ciertos incidentes de seguridad, como aquellos que afectan datos personales, podrían suponer consecuencias legales y sanciones por parte de las administraciones competentes.

Es importante conocer las principales ciberamenazas que pueden afectar a las Clínicas se hace vital para poder identificarlas activamente y por lo tanto poder evitarlas. Te mostraremos las principales ciberamenazas

¿Qué es la ingeniería social?

La ingeniería social consiste en **utilizar diferentes técnicas de manipulación psicológica** con el objetivo de conseguir que las potenciales victimas revelen información confidencial, o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente, como revelar información confidencial o instalar *software* malicioso.

En la mayoría de ocasiones **los ciberdelincuentes atacan al eslabón más importante en la cadena de la seguridad, los empleados.** Esto se debe a que los ataques basados en ingeniería social requieren mucho menos esfuerzo que otros tipos de ataques, y por lo tanto el beneficio es mayor.

Los ataques basados en ingeniería social se pueden categorizar en dos tipos diferentes en función del número de comunicaciones que debe realizar el ciberdelincuente hasta conseguir su objetivo:

Hunting

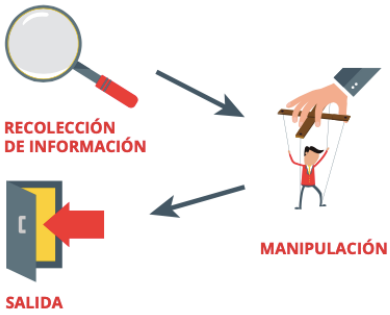
Mediante una **única comunicación** los ciberdelincuentes buscan obtener su propósito. Generalmente la técnica del *hunting* es utilizada en ataques de *phishing* o campañas de distribución de *malware*. Este tipo de campañas maliciosas son enviadas por los ciberdelincuentes de manera masiva, es decir, sin objetivos concretos.

Farming

En este caso los ciberdelincuentes emplean **más de una comunicación** con la víctima hasta conseguir su objetivo. El *farming* comúnmente es utilizado en campañas de sextorsión, fraude del CEO o de RR.HH.

Fases de un ataque de ingeniería social

Todos los ataques basados en ingeniería social comparten ciertas características que hacen que el ciclo de vida sea similar para todos ellos. Saber cuáles son puede marcar la diferencia a la hora de identificar uno de estos ataques. Pueden distinguirse tres fases: **Recolección de información, Manipulación y Salida**



Edición No. 8 – julio 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

El correo electrónico, principal medio de comunicación fraudulenta

Los ciberdelincuentes necesitan un medio de comunicación para propagar sus campañas fraudulentas, siendo el correo electrónico su preferido. Esto se debe principalmente a que **la gran mayoría utilizamos el correo electrónico como herramienta de trabajo.** Esta frecuencia en su uso es lo que vuelve a esta herramienta peligrosa, ya que en muchas ocasiones las tareas se realizan de forma mecánica. La falta de ciertas medidas de seguridad es aprovechada por los ciberdelincuentes para elaborar campañas de correos electrónicos fraudulentos más sofisticadas.

Pautas para identificar un ataque de ingeniería social

- **Remitentes desconocidos** Uno de los métodos más fiables y simples para comprobar si un correo puede ser fraudulento, es analizar la dirección del remitente.
- **Remitentes falseados** La dirección del remitente puede ser falseada suplantando a la entidad legítima. Comprobar si una dirección ha sido falseada es posible analizando las cabeceras del correo y comprobar minuciosamente el nombre de dominio ya que una simple letra podría ser el origen de un incidente de seguridad. Ejemplo, el dominio **"@grupobancolombia.com"** puede ser falseado con el dominio **"@grupobamcolombia.com"**.
- **Comunicaciones impersonales** por ejemplo "Estimado cliente, usuario, etc.". Las comunicaciones legítimas suelen ser personales, indicando el nombre de la persona o entidad a la que van dirigidas.
- **Adjuntos sospechosos** Se debe comprobar previamente la extensión del fichero adjunto, teniendo especial cuidado con las siguientes extensiones .exe, .vbs, .msi, .vbs, .docm, .xlsm o .pptm
- **Mala redacción** La presencia de faltas de ortografía o errores gramaticales es un síntoma de comunicación fraudulenta, una entidad legítima suele cuidar mucho que las comunicaciones estén bien redactadas.
- **Enlaces falseados** Antes de acceder a un enlace, se debe verificar la web a la que redirige. Para ello, si se sitúa el ratón encima del vínculo se mostrará en la parte inferior de la pantalla el sitio al que realmente dirige.
- **Firmas y otros elementos en la plantilla del correo** Cuando se está acostumbrado a los correos de una entidad en concreto, es fácil identificar elementos comunes, si esta firma o párrafo legal es diferente o directamente no está, podría ser un síntoma de que dicha comunicación probablemente sea fraudulenta.

***Fuente*: https://www.incibe.es**

"Los ataques de ransomware conocidos últimamente pueden ser catastróficos para un Hospital: no solo por la disrupción de su operatividad o la incapacidad de contar con información esencial del paciente, sino también por el coste económico que supone restaurar sistemas y copias de seguridad, así como el daño reputacional que el centro atacado puede sufrir a partir de estos eventos".

Mario Chao - VP Healthcare everis Americas