Asociación de Seguridad Informática

EuskalHack

INFORME SECTF 2019

Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

www.euskalhack.org

ACERCA DE EUSKALHACK

La Asociación de Seguridad Informática EuskalHack es una organización sin ánimo de lucro constituida en Donostia y conformada por diversos profesionales vinculados a la investigación de seguridad informática e informática forense.

Su objetivo es promover la comunidad y la cultura en materia de seguridad digital a cualquier tipo de público interesado, ya sean de carácter público o privado, mediante la promoción y difusión de conocimiento principalmente técnico.

Fomenta actividades como es la organización de seminarios y congresos, donde difundir y compartir avances e investigaciones alcanzadas en el sector nacional e internacional. Asimismo, impulsa la colaboración entre el público asistente, aproximando empresas y particulares en relaciones de Networking.

El valor de sus asociados es esencial, siendo el pilar fundamental de esta asociación, pues su empeño y entusiasmo facultan el adecuado desarrollo para el cumplimiento de este reto. EuskalHack Trabaja por ser una organización abierta y dinámica, siendo nuestros Órganos de Gobierno la Asamblea General y la Junta Directiva.

AUTORES

Angel Alonso

Miguel Ángel Hernández

Roberto Casado

CONTENIDO

INTRODUCCIÓN

La IV edición de EuskalHack Security Congress celebrada los días 21 y 22 de junio de 2019 en la ciudad de Donostia-San Sebastián, acogió el primer CTF de Ingeniería Social (SECTF) de Europa, actividad organizada y tutelada por EuskalHack.

Cabe reseñar que hasta la fecha de celebración del SECTF únicamente se había llevado a cabo en los EE.UU., dentro de las conferencias de seguridad informática DEF CON y DerbyCon, dónde es ampliamente valorado y reconocido.

Resulta evidente el aumento que se está produciendo en el uso de las técnicas de ingeniería social. Estas técnicas, si bien no acostumbran a ser casos de estudio, han sido una parte fundamental de muchos de los ciberataques con mayor impacto en los últimos años.

Precisamente, dado el grado de exposición de organizaciones y ciudadanos frente a los ataques de ingeniería social, y el limitado desarrollo de competencias profesionales en esta materia, surge la idea de albergar esta iniciativa en el congreso de ciberseguridad de EuskalHack.

La iniciativa se planteó con los siguientes objetivos:

- Generar concienciación sobre las técnicas de ingeniería social y sus posibles consecuencias.
- Conocer el nivel de exposición de la información de las empresas en fuentes públicas.
- Conocer el nivel de efectividad de las técnicas de ingeniería social sobre las empresas.
- Dar la oportunidad a que los participantes puedan poner a prueba sus habilidades de ingeniería social en un entorno real, y de forma segura.
- Compartir conocimiento en materia de ingeniería social.
- Generar un informe con las conclusiones obtenidas tras un profundo análisis sobre el desarrollo de SECTF, poniéndolo a disposición de cualquier persona u organización interesada.
- Promover la cultura en materia de ingeniería social con la intención de impulsar la investigación en esta área.

AGRADECIMIENTOS

Queremos agradecer expresamente su colaboración a las siguientes entidades:

Basque Cybersecurity Centre

LegalConsulTech

Christopher Hadnagy

EuskalHack

De la misma forma, queremos agradecer su colaboración a los participantes y a todas aquellas personas anónimas que han facilitado la realización del SECTF colaborando con EuskalHack en diferentes ámbitos.

DESCRIPCIÓN DEL SECTF

El SECTF es una competición de tipo “Capture the Flag” (Captura la Bandera), donde a los participantes se les proponen una serie de desafíos de seguridad informática (en este caso de Ingeniería Social) que tienen que superar. Estos retos suelen tener una duración determinada, tras los cuales se suelen publicar los solucionarios (Writeups) del reto, dando a conocer las técnicas utilizadas por los jugadores.

El objetivo de los participantes pasaba por obtener diferentes piezas de información (flags) para lo que debían emplear:

- Fuentes públicas de información (OSINT) en la primera fase.
- Llamadas telefónicas en directo en la segunda fase.

Cualquier persona mayor de edad que estuviese interesada, independientemente de su grado de conocimiento sobre ingeniería social, dispuso de un periodo de dos meses para registrarse a este reto a través del formulario publicado en la web del congreso.

El hecho de llevar a cabo la fase de llamadas en directo, y bajo la supervisión de los jueces, impuso ciertas restricciones de logística, que obligaron a seleccionar un número limitado de participantes.

Tras analizar las solicitudes, se seleccionaron aquellos 5 participantes cuyas motivaciones estuvieron más alineadas con los siguientes criterios:

- Aprender y compartir el conocimiento, por encima obtener el primer puesto en la competición.
- Predisposición a enfrentarse a nuevos retos y desafíos.
- Ganas de pasar un buen rato en compañía de otros miembros de la comunidad.

A cada participante se le asignó una empresa como objetivo, además de un listado con las flag, un informe de ejemplo, y el horario en el que debían realizar las llamadas el día del congreso.

A partir de ese momento dio comienzo la primera fase (OSINT), con una duración de tres semanas, y el objetivo de obtener y analizar tanta información expuesta (de carácter público) sobre las empresas objetivo como les fuera posible.

Antes de la fecha de finalización de esta fase, cada participante debía entregar un informe (Writeup) con las conclusiones obtenidas tras analizar la información recabada, dependiendo gran parte de la puntuación final de la calidad de este informe.

Durante la segunda fase, celebrada el día 21 de junio en el propio congreso, los participantes dispusieron 20 minutos en el horario que les había sido asignado, para realizar llamadas a la empresa objetivo e intentar conseguir todas las flags que les fuera posible.

Reseñar que esta fase tuvo lugar en el interior de una cabina insonorizada a fin de evitar distracciones a los participantes. Además, tuvieron la posibilidad de utilizar un identificador de llamada personalizado para cada una de las comunicaciones con el objetivo.

De la misma manera, la organización optó por realizar la fase de llamadas en un entorno restringido exclusivamente a los participantes de esta iniciativa, buscando garantizar la completa confidencialidad y seguridad de las empresas objetivo.

No obstante, se está analizando si es posible mejorar esta parte del aspecto divulgativo en futuras ediciones.

Finalmente, con la información obtenida durante ambas fases y tras un riguroso análisis, se ha redactado el presente informe que da por concluida la actividad en 2019.

Empresas seleccionadas

En esta primera edición se seleccionaron empresas con sede en la Comunidad Autónoma Vasca.

Estas empresas provenían de diferentes sectores, con importancia estratégica para el desarrollo de la economía de la comunidad como denominador común.

Atendiendo a su criticidad se descartaron empresas de sectores sensibles o estratégicos como educación, sanidad, gobierno, telecomunicaciones o banca.

A continuación, se facilitan algunos datos genéricos sobre las empresas que han participado en la iniciativa:

Estos datos son aproximados para preservar la identidad de las empresas participantes, aunque suficientes para comprender el tipo de organizaciones que han participado en la iniciativa.

Facturación: Entre 300 a 10.000 Millones €
Nº de Empleados: Entre 500 y 25.000
Nº de Sedes: Entre 20 y 1.500 oficinas (Nacional e internacional)

Reseñar que el SECTF se organizó con la máxima de preservar la identidad de las empresas en todo momento.

A fin de garantizar unos datos válidos para el posterior análisis, se determinó que las empresas no debían tener conocimiento previo sobre la existencia del SECTF.

En este sentido el BCSC, que ha valorado la iniciativa como positiva desde el primer momento, ayudó en la selección de empresas participantes. Igualmente, se acordó que si alguna llamada levantase evidentes sospechas, se contactaría con la organización para evitar cualquier posible crisis o inicio de protocolo de respuesta ante incidentes.

Flag

Las flag son las piezas de información que debían ser obtenidas por los participantes. En función del número de flags conseguidas y de su justificación, se determinó la mayor parte de la puntuación de cada participante en la competición.

Durante la elección de las flag se procuró establecer un equilibrio, de tal manera que la información a obtener fuese suficientemente relevante, con un adecuado nivel de dificultad y que a su vez, no fuera información sensible para la empresa.

Como punto clave, se tuvo en consideración la utilidad de esta información a la hora de planificar un ataque de ingeniería social.

El listado de flag fue el mismo para ambas fases (OSINT y llamadas), con una única excepción: inducir a que la víctima siguiese un enlace a una URL falsa, flag que por razones obvias solo se podía conseguir durante la fase de llamadas.

A continuación, se presenta el listado de flag que debía obtener cada participante:

LOGÍSTICA

¿El soporte de IT es interno o subcontratado?
¿Qué empresa de paquetería utilizan?
¿Cuál es el horario de recogida/entrega de paquetería?
¿Tienen cafetería?
¿Quién gestiona el servicio de comedor?
¿Utilizan destructoras de papel?

OTRAS TECNOLOGÍAS

¿Bloquean sitios web?
En caso afirmativo ¿Cuáles? (Twitter, Instagram, etc.)
¿Tienen WIFI? (sí/no)
En caso afirmativo ¿Cuál es el SSID?
¿Qué marca y modelo de ordenadores utilizan?
¿Qué antivirus utilizan?

PUEDE SER UTILIZADO COMO PRETEXTO IN SITU

¿Cuál es el nombre de la empresa de servicio de limpieza?
¿Cuál es el nombre de la empresa que se encarga de las máquinas expendedoras?
¿Quién se encarga de la gestión de los residuos / basura?
¿Nombre de la empresa de guardas de seguridad?
¿Qué tipo de tarjeta utilizan para acceder a la empresa? (RFID, HID, ninguna)

TECNOLOGÍA GENERAL DE LA EMPRESA

¿Qué sistema operativo utilizan?
¿Cuál es la versión de service pack?
¿Qué programa utilizan para abrir documentos PDF y que versión?
¿Utilizan servicios como wetransfer para enviar información?
¿Qué navegador utilizan?
¿Qué versión?
¿Qué cliente de correo utilizan?
¿Utilizan algún gestor de contraseñas?
¿Utilizan encriptación de disco?
URL falsa (hacer que el objetivo visite la URL: http://www.esc-support.es)

INFORMACIÓN ESPECÍFICA DE EMPLEADOS

¿Cuánto tiempo lleva trabajando para la empresa?
¿Qué día del mes se cobra?
Información del calendario de los empleados (inicio / fin de la jornada, descansos, comidas)
¿Cuál es el organigrama de la organización?
¿Qué operador de telefonía utilizan?
¿Cuál es la última vez que han recibido una formación sobre concienciación en seguridad?

Es necesario mencionar que las flag obtenidas durante la fase de llamadas puntuaban el doble que las obtenidas durante la fase OSINT.

La puntuación final dependió asimismo de los vectores de ataque plausibles debidamente justificados que pudiera facilitar el participante, y de la calidad del informe presentado en la fase OSINT.

Normativa

Los participantes de esta iniciativa estuvieron sujetos a una estricta normativa, velando en todo momento por garantizar la protección de las empresas objetivo.

Esta normativa se desarrolló a lo largo de varios meses de trabajo, teniendo como base:

- La solicitud de un informe jurídico para establecer el marco legal al que debía ceñirse la competición.
- Consultas a diversas voces autorizadas en derecho con objeto de asegurar que existía consenso al respecto.
- Asesoría con organizaciones y organismos de diferentes ámbitos con las que EuskalHack colabora habitualmente.

Todo ello a fin de tener en cuenta diferentes sensibilidades a la hora de redactar una normativa responsable y consolidada, fiel a una iniciativa que pretende aportar valor a la comunidad.

La normativa completa puede obtenerse en la siguiente URL:

https://securitycongress.euskalhack.org/SECTF/Normativa_SECTF_2019.pdf

De manera general se resume que la norma más importante de esta competición fue la de demostrar total respeto hacia todas las partes implicadas, estando tajantemente prohibido la utilización de métodos intimidatorios o denigrantes.

De hecho, el resultado del SECTF demuestra que la ingeniería social es altamente efectiva sin necesidad de utilizar técnicas poco éticas.

A continuación, se detallan algunos aspectos explícitamente prohibidos:

- Intentar obtener información confidencial o personal (DNI, números de tarjetas de crédito, contraseñas, etc.).
- El uso de lenguaje grosero o amenazador, o cualquier técnica de ingeniería social agresiva.
- Intrusión física o técnica (Red, servidores, etc.) en las empresas.
- Hacerse pasar por miembros de instituciones gubernamentales o fuerzas de seguridad.
- Suplantar a personas que existen en el mundo real.

Para preservar tanto la identidad de las empresas como la de los participantes, no se permitieron grabaciones en el emplazamiento durante la fase de llamadas, y tan sólo se realizaron fotografías con el permiso previo de los participantes.

Tanto los participantes como los miembros de la organización que participaron en el SECTF, se comprometieron mediante contrato a no revelar la identidad de las empresas objetivo.

ANÁLISIS Y RESULTADOS

Fase OSINT

A fin de buscar el máximo realismo y efectividad en esta fase, como en un proyecto real de ingeniería social, los participantes debían comenzar con un trabajo concienzudo de búsqueda de información.

La información obtenida durante esta fase resulta vital para la correcta elección de los objetivos con los que se contactará posteriormente, y para la elaboración de un pretexto a la medida de estos. El esfuerzo dedicado en esta fase, determinará en gran medida el éxito o fracaso de todo el proyecto.

Existe gran cantidad de información disponible de forma pública en Internet, pero su obtención y análisis es un arduo trabajo, por lo que para acometerlo es necesario conocer el mayor número de herramientas disponibles, además de contar con la capacidad de desarrollar herramientas propias.

Durante la fase OSINT del SECTF los participantes utilizaron las siguientes herramientas:

github.com	wigle.net	TOR
domained	Zoomeye	BuscadorVM
sublist3r	Censys	Credential Breaches Dumps
knockpy	Recon-ng	Scrappers y herramientas
exiftool	DuckDuckGo	propias
SpiderFoot	Bing	Youtube.com
Google	Facebook	Infojobs.net
LinkedIn	Twitter	curriculumvitaeempresarial.com
Maltego	Instagram	DNSDumpster
Google Maps	Foca	hackertarget.com
Shodan	Fofa.so	dWatcher
Haveibeenpwned.com	WaybackMachine	pastebin.com
Whois	Tinfoleak	Raven
inteltechniques	Fireshot	Peoplecall.com
burp suite	VideoDownloadHelper	Mxtoolbox.com
www.iberley.es	VLC	www.boe.es

En esta fase del SECTF se consiguió una enorme cantidad de información de diversa índole sobre las empresas objetivo. A continuación, se muestran los hallazgos más relevantes, clasificados según su fuente:

Metadatos

Se encontraron gran cantidad de metadatos en documentos públicos, algunos de los cuales se encontraban alojados en ubicaciones que deberían ser privadas.

Este tipo de datos se obtuvieron tanto por errores en la configuración como por estar publicados de manera innecesaria.

Entre los metadatos encontrados cabe destacar:

- Sistemas operativos.
- Versiones de diferente software (Software de creación y edición de contenidos, y suites Ofimáticas).
- Nombres de usuarios.
- Direcciones de correo electrónico.
- Nombres de empleados.
- Títulos originales de los documentos.

Es importante tener en cuenta la fecha de creación de los documentos reflejadas en los metadatos, ya que ofrecen una medida de la vigencia de la información obtenida. Generalmente cuanto más actuales sean, mayor posibilidad de que la información obtenida siga vigente.

Aunque pueda parecerlo, no existe información irrelevante. En los títulos originales de los ficheros se revela multitud de información susceptible de ser utilizada durante un ataque de ingeniería social, como son los términos de uso interno, por ejemplo. Habitualmente los usuarios no lo perciben como relevante, y sin embargo pueden utilizarse por un atacante para ganar credibilidad utilizando la misma jerga que los propios empleados.

Videos e imágenes

El análisis de videos e imágenes corporativas rebeló gran cantidad de información que pasó desapercibida para la persona que los publicó, o que consideró como irrelevante.

Se obtuvo gran cantidad de información de videos e imágenes publicados por visitantes o proveedores, en ortofotos o fotografías de satélite y en Google Street View.

Entre la información que se consiguió durante el análisis de los videos y las imágenes, cabe destacar los siguientes hallazgos:

- Imágenes de acreditaciones de empleados y visitas.
- Imágenes de las tarjetas de acceso de los empleados.
- Marca y modelo de equipos informáticos.
- Software instalado.
- Nombres de usuario.
- Versiones de sistemas operativos.
- Marca de los navegadores.
- Nombres de cliente de correo.
- Sistemas para destrucción de documentos y gestión de residuos.

Sitios Web

El sitio web de la empresa objetivo y cualquier otra web asociable a la misma, son el lugar donde generalmente se inicia la búsqueda de información. A la luz da los datos obtenidos durante la fase OSINT del SECTF, resultó ser una de las fuentes donde más información se recabó.

Gran parte de los documentos de los que se obtuvieron metadatos, así como la gran mayoría de los videos e imágenes mencionados anteriormente, fueron descubiertos en sitios web pertenecientes a la empresa.

Adicionalmente a la información antes mencionada se han encontrado también:

- Números de teléfono y extensiones internos.
- Direcciones de correo electrónico.
- Información sobre la estructura jerárquica de la empresa.
- Infraestructuras de prueba.
- Portales web antiguos o en desuso y sin actualizar.
- Nombres de equipos y rutas internas.
- Manuales con nombres de usuario y contraseñas por defecto.

Como inciso, se siguen encontrando errores de programación o configuración de los servidores, ejemplo palpable de esto es que algunos de los sitios que deberían ser de acceso restringido, también estaban indexados por los buscadores.

Información de portales públicos

Diversos sitios web gubernamentales, judiciales, sindicales, de prensa o de búsqueda de empleo, también revelaron gran cantidad de información sobre las empresas objetivo.

Mucha de la información de este apartado fue extraída de pliegos de contratación, sentencias judiciales, boletines varios y artículos de prensa.

Entre la información que se encontró cabe destacar:

- Marca y modelo de infraestructura de red y equipos informáticos.
- Marca de antivirus.
- Nombre de empresas de seguridad, limpieza, comedor y logística.
- Horarios de los empleados.
- Información sobre campañas de concienciación en seguridad.
- Información sobre las características del sistema de acceso.
- Números de teléfono internos.

Proveedores

Otra fuente de información que cabe reseñar viene del análisis de los proveedores.

Es importante que una organización considere como un activo a fortificar aquellas empresas con las que mantiene una estrecha colaboración. Recordemos que la cadena siempre es tan fuerte como su eslabón más débil.

En esta fuente cabe destacar la información sobre los servicios prestados:

- Logística.
- Seguridad.
- Vending.
- Limpieza.
- Información sobre tecnología e infraestructuras implantadas en la empresa.

Redes Sociales

En este aspecto se hace constar que los informes OSINT, por deformación profesional de los participantes, se centraron especialmente en la infraestructura y la organización de las empresas objetivo y en menor medida en el análisis de los empleados, apartado que sin duda podría haberse explotado más.

Es importante destacar la importancia de la información expuesta en redes sociales sobre los empleados, ya que podría permitir a un atacante malicioso conocer detalles sobre vida personal, costumbres, comportamiento... y con ello diseñar un ataque dirigido, con un nivel de credibilidad difícil de imaginar.

A continuación, se reflejan los hallazgos realizados en redes sociales:

- Tipo de soporte de IT (Subcontratado o interno).
- Tiempo trabajando para la empresa.
- Tecnologías específicas de aplicativos y entornos de trabajo.
- Organigrama y estructura organizativa interna.
- Información sobre preferencia de ocio de los trabajadores.
- Grupos privados de Facebook sin una correcta verificación de la identidad.
- Información sobre proveedores de servicios.

Leaks de credenciales

Por último, mencionar que se encontraron cuentas de correo y credenciales pertenecientes a varias de las empresas objetivo en diversos leaks de información expuestos en Internet.

Es difícil de evaluar si son credenciales antiguas, y/o revocadas, pero debido a las consecuencias que podrían tener, se ha decidido incluir expresamente esta mención en el informe, ya que se considera importante que las organizaciones estén especialmente alerta en este aspecto.

Adicionalmente, uno de los participantes encontró un dominio que difería del dominio real perteneciente a la empresa objetivo únicamente en una letra, y que a simple vista era prácticamente indistinguible en la barra de direcciones del navegador.

Este tipo de dominios podría utilizarse, y de hecho se utilizan, en campañas de phishing, buscando el robo de credenciales o infección mediante malware.

Informes fase OSINT

Destacamos que la mayor parte de los informes recibidos al finalizar la fase OSINT fueron de calidad profesional.

- Perfectamente redactados.
- Con diferentes secciones bien definidas.
- Con una exposición clara y concisa de la información.

Se resalta para futuros profesionales de la seguridad informática la importancia de dedicar el suficiente esfuerzo a la hora de redactar un informe.

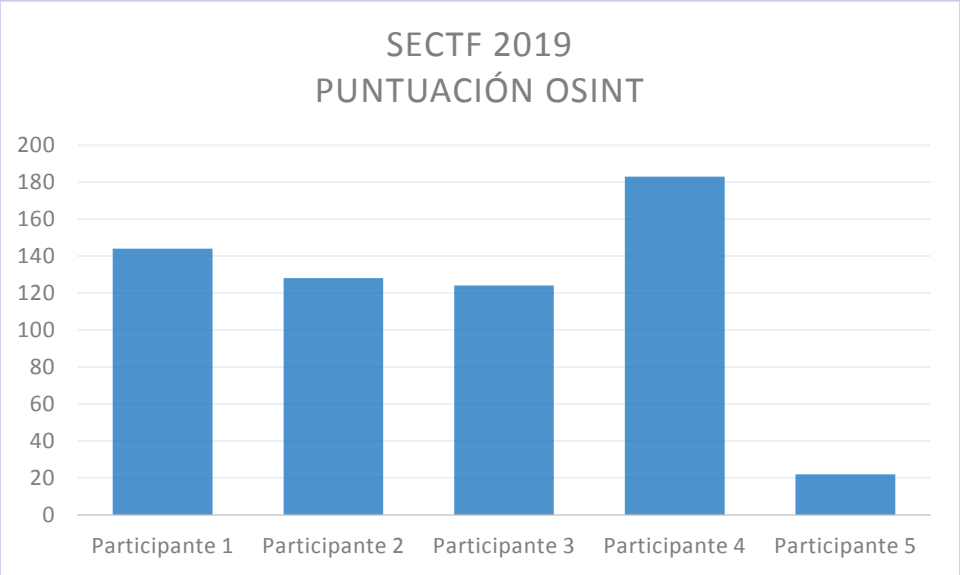

Gráfico 1: Puntuación por participante fase OSINT

Basado en la experiencia obtenida a lo largo del SECTF, a pesar de los diferentes esfuerzos de concienciación llevados a cabo por empresas e instituciones, sigue existiendo gran cantidad de información sensible accesible libremente por cualquier persona u organización que quiera consultarla.

Es importante reflexionar sobre este aspecto, ya que como se ha explicado con anterioridad, la base de la mayoría de los ataques (no sólo los de ingeniería social), parte de una fase de investigación previa. Estos resultados indican que es necesario seguir trabajando y concienciando en este aspecto.

Pretextos

En términos de ingeniería social, se considera pretexto el motivo o causa simulada, que se alega para crear un contexto que facilite la persuasión de una persona, con la intención de que revele información privada o lleve a cabo ciertas acciones. De manera simplista, podríamos decir que se trata una falsa realidad diseñada por el atacante y cuyo propósito es el de inducir al objetivo a pensar que se encuentra en una situación diferente de la real.

Resulta imprescindible una cuidadosa planificación del pretexto, basada en el análisis de la información obtenida sobre la empresa objetivo y sus trabajadores durante la fase OSINT.

Se comprobó que lo más efectivo fueron pretextos simples, coherentes con la realidad del objetivo, y con la información que se quería obtener.

Pequeños detalles, como terminología interna, referencias a empleados, o comentarios relacionados con la labor del personaje que se estaba interpretando, potenciaron la efectividad de estos pretextos.

Los pretextos más utilizados en el SECTF fueron variaciones del técnico de soporte de IT, siendo además una de estas variaciones la que mayor puntuación obtuvo.

Este pretexto les permitió utilizar conocimientos propios, lo que en la mayoría de los casos les llevó a comportarse como lo haría un técnico en la vida real, evitando de esta manera generar alerta en el objetivo, y por otro lado, ayudó a que el empleado objetivo fuese guiado sin levantar sospechas, para acceder a datos que con sus conocimientos técnicos no hubiese sabido obtener.

Otros pretextos utilizados han sido:

- La realización de una encuesta.
- Asistente de un alto cargo.
- Entrevista de un Medio digital.

Los participantes que utilizaron un pretexto poco trabajado, no coherente con la información que querían obtener o que utilizaron un guion muy rígido, tuvieron menos efectividad.

Llamadas en directo

La fase de llamadas permitió a los participantes probar sus habilidades en una situación real, sin embargo, se remarcan las diferencias con un proyecto real de ingeniería social.

En primer lugar, el tiempo es limitado, lo que añadió mucha presión a los participantes sobre todo a medida que este se agotaba.

Fueron más efectivas aquellas llamadas donde se utilizó algo de tiempo al comienzo para explicar de forma clara y concisa:

- Quien se es.
- Cuál es el motivo de la llamada.
- Convencer al destinatario de que no supone una amenaza.

También ayudó a los participantes a comenzar a solicitar la información que necesitaban rápidamente, haciendo las llamadas mucho más eficientes.

Ante una situación real en la que se dispone de más tiempo, o no se está tan enfocado en la obtención de una información tan concreta, es habitual realizar preguntas abiertas para sonsacar información que pueda ser utilizada posteriormente.

Durante el reto, se observó que los participantes que fueron más directos en este sentido tuvieron mayor éxito a la hora de conseguir las flag, evidentemente siempre y cuando el pretexto fuera sólido y coherente.

Por otro lado, hay que resaltar que las pruebas se realizaron desde el interior de la cabina insonorizada, y ante los jueces y el resto de competidores, siendo factores que añadieron presión a los participantes.

Todo ello, junto al el hecho de que para la mayoría de los participantes era la primera vez que realizaban una actividad similar, hace que sus llamadas sean un hito por el que felicitarles.

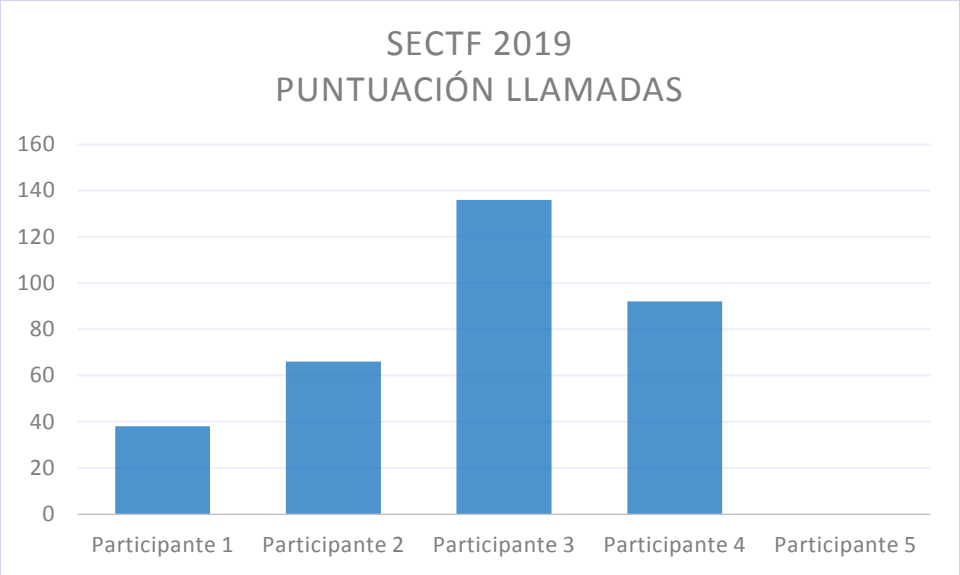

Gráfico 2: Puntuación por participante fase de llamadas

A continuación, indicamos los comportamientos observados en los participantes que han tenido mayor éxito:

- Han utilizado pretextos muy trabajados y detallados.
- Han añadido pequeños guiños de humor y conversación casual.
- Han hecho cumplidos a la persona objetivo.
- No han interrumpido a la persona objetivo y la han asistido durante la conversación.
- Han añadido detalles a la conversación que han dado solidez al pretexto.
- Han conseguido que el objetivo conecte emocionalmente con ellos.
- Han utilizado en los pretextos situaciones de las que el objetivo tenía una idea preconcebida, y han hecho que la llamada se adapte a esa idea preconcebida.
- Han utilizado el *quid pro quo* facilitando información propia o sobre terceros, lo que ha facilitado que los objetivos ofrecieran información de forma recíproca.
- Han utilizado jerga interna, o referencia a infraestructuras internas.
- Han aparentado estar tranquilos, o han conseguido justificar su nerviosismo con el pretexto.
- Han sabido asistir a los objetivos a la hora de solicitar información técnica, que no sabían obtener por sí solos.
- Han sabido elegir a sus objetivos, habiendo analizado qué perfiles o departamentos eran más vulnerables, y contactado directamente con ellos.
- Han utilizado un marco de tiempo artificial.

- Han adaptado la modulación de la voz adaptándose al tipo de voz que podía esperarse del personaje que estaban interpretando.
- En general se ha notado una relación directamente proporcional en el éxito durante la fase de llamadas con la calidad del informe OSINT.
- Tenían claro cómo encajar la información que querían obtener dentro del pretexto.
- Han sido flexibles durante la llamada y han sabido adaptarse a los imprevistos.
- Se mostraron más positivos y decididos.

A continuación, se indican los comportamientos observados en los participantes que han tenido mayores dificultades durante esta fase:

- Han utilizado pretextos poco trabajados.
- Han utilizado un esquema rígido, y han tenido dificultades cuando la conversación de se ha desviado del guion.
- Han cometido errores con los nombres y la terminología.
- Han mostrado estado de nerviosismo durante la conversación y no han sabido justificarlo.
- No han tenido confianza en ellos mismos.
- Se han justificado demasiado durante las conversaciones.
- Han pedido permiso a la hora de solicitar acciones al interlocutor como si no tuviesen autoridad para hacerlo, cuando en la situación real en la que se basaba el pretexto, no lo habrían hecho.
- Han utilizado pretextos incompatibles con la información que debían obtener.
- Han hecho un uso contradictorio del identificador de llamada.
- No han añadido marco de tiempo artificial ni, sensación de apremio cuando el pretexto lo necesitaba.
- Han sido contradictorios en diferentes momentos de la llamada.

Técnicas de influencia

Se considera técnica de influencia, el proceso por el cual se consigue persuadir a una persona para que realice una acción que de otra manera no habría realizado.

En esta sección se mencionan aquellas técnicas que han sido predominantes en cada llamada, considerando que todas las llamadas estuvieron llenas de matices, y en todas ellas intervinieron diferentes principios de influencia, en mayor o menor medida.

El principio de influencia que más se utilizó para persuadir a los objetivos fue el **principio de obligación moral**, bien la obligación moral de asistir a una persona que está solicitando ayuda, o bien la obligación moral de realizar correctamente su trabajo.

El segundo principio para influenciar a los objetivos más utilizado fue el de **ejercer autoridad**. En todos los casos en los que se ha utilizado este principio, fue ejercido en representación de una institución o un alto cargo, y no por el uso de la autoridad propia.

Otro de los principios que se utilizó, pero siempre como refuerzo de otro, fue el de **coherencia**. Este principio, se utilizó para que una vez adquirido el compromiso de colaborar por parte del objetivo, poder seguir solicitando información más allá de lo que el objetivo hubiese deseado, y a lo que accede precisamente por ser coherente con el compromiso adquirido inicialmente. Compromiso sobre el que en realidad no se había concretado demasiado.

Adicionalmente se utilizó el **principio de afinidad o simpatía**. Haciendo una buena labor en la fase de búsqueda y análisis de información, se puede elegir un pretexto relacionado con los gustos del objetivo, o interpretar un personaje que concuerde con las preferencias personales del mismo.

Si desea profundizar en el conocimiento sobre estas técnicas se recomienda que visite la siguiente dirección:

https://www.social-engineer.org/framework/influencing-others/influence-tactics/

También puede consultar el libro “Influence, the psychology of persuasion” del profesor Robert B. Cialdini.

Observaciones adicionales

- Todos los participantes salieron de manera ordenada de la conversación, aun cuando hubieron levantado alguna sospecha.

- Algunos de los participantes obtuvieron información no solicitada a los objetivos.

- Un interlocutor llegó a ejecutar un comando en el equipo a petición del participante (exclusivamente para ver la versión del sistema operativo).

- Cabe destacar, por ser la mitigación más efectiva, que en una llamada a centralita, el operador siguió el protocolo interno de su empresa (pese a que la información solicitada era aparentemente inocente), e indicó al participante que su labor consistía exclusivamente en transferir llamadas.

- Una de las llamadas despertó sospechas en la persona objetivo, perteneciente al departamento de administración, que transfirió la llamada al responsable de seguridad. (En este caso influyeron notablemente varios fallos que cometió el participante).

- Parte de los participantes pasó considerables períodos de tiempo escuchando locuciones o esperando ser transferidos, lo que acortó sustancialmente el tiempo útil en su turno de llamadas.

Observaciones sobre los Competidores

La totalidad de los competidores fueron profesionales del sector de la ciberseguridad. Su nivel de experiencia osciló desde aquellos que realizaban una llamada de estas características por primera vez, hasta los que utilizan habitualmente estas técnicas para realizar su trabajo.

Destacar que en todo momento se mantuvo un ambiente didáctico con el objetivo de aprender y compartir el conocimiento, además del máximo respeto por las empresas objetivo y sus empleados.

Agradecer especialmente el esfuerzo que se realizó para que los objetivos se sintieran tranquilos y ante situaciones que levantaron sospechas durante las llamadas, el esfuerzo que hicieron por reconducir la conversación y hacer una salida controlada de la misma, esto no es algo sencillo, y todos los participantes estuvieron a la altura.

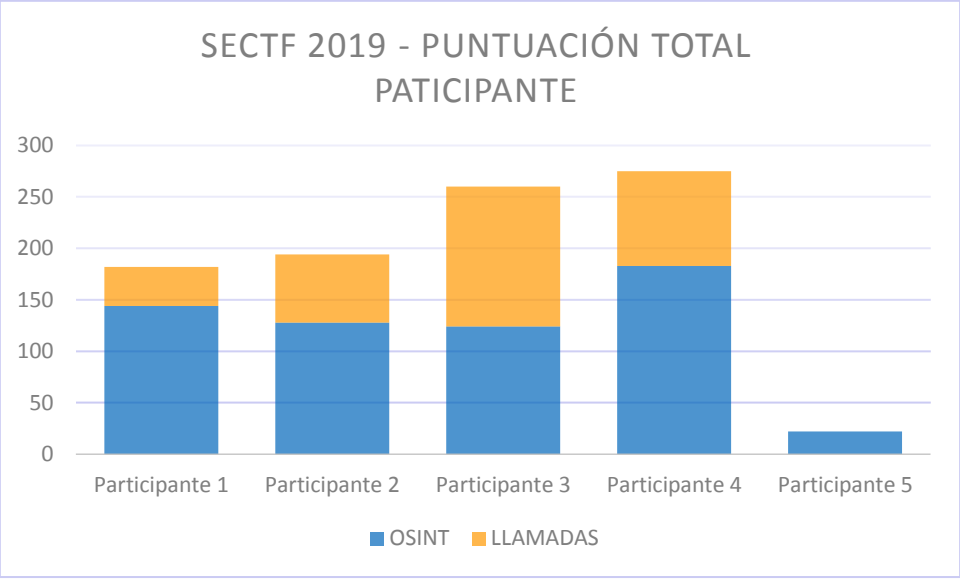

Gráfico 3: Puntuación total por participante

Una vez concluida la fase de llamadas, los jueces revisaron todas las puntuaciones arrojando el resultado final.

En el siguiente gráfico se muestra el resultado final por empresa: una mayor puntuación indica que el participante asignado a esta empresa obtuvo mayor cantidad de información sobre la misma, o información de mayor valor.

A la hora de interpretar los resultados no podemos obviar que el SECTF cuenta con ciertas restricciones en cuanto a tiempo y normativa, y que el nivel de experiencia de los participantes puede influir notablemente en el resultado, de manera que no podemos inferir que las empresas con mayor puntuación sean las más expuestas, o que las que tienen menor puntuación las más seguras.

Este ranking sirve para mostrar la efectividad de la ingeniería social, no para comparar el grado de seguridad de cada empresa.

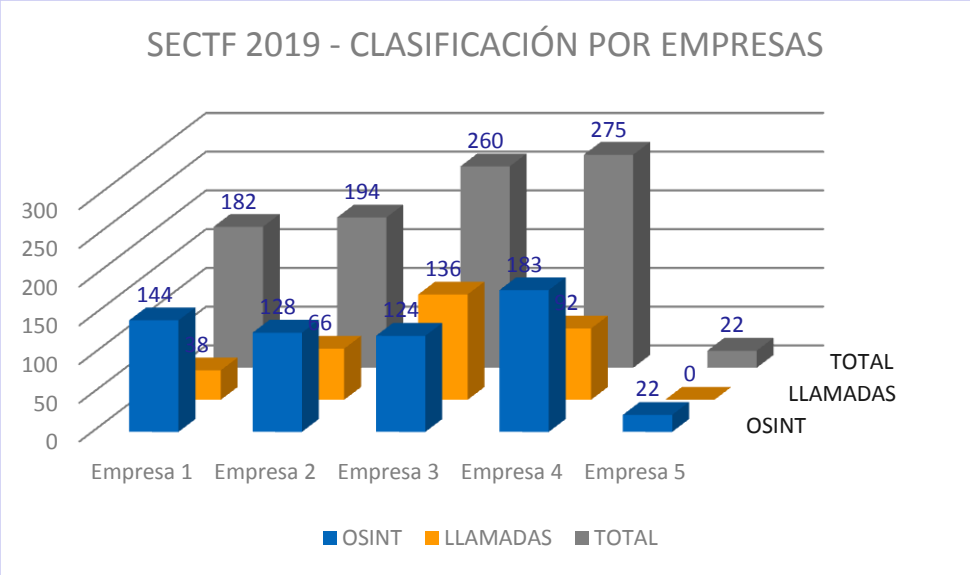

Gráfico 4: Puntuación total por empresa

A continuación, se muestra un gráfico con el número de ocasiones que se ha conseguido cada flag durante la competición.

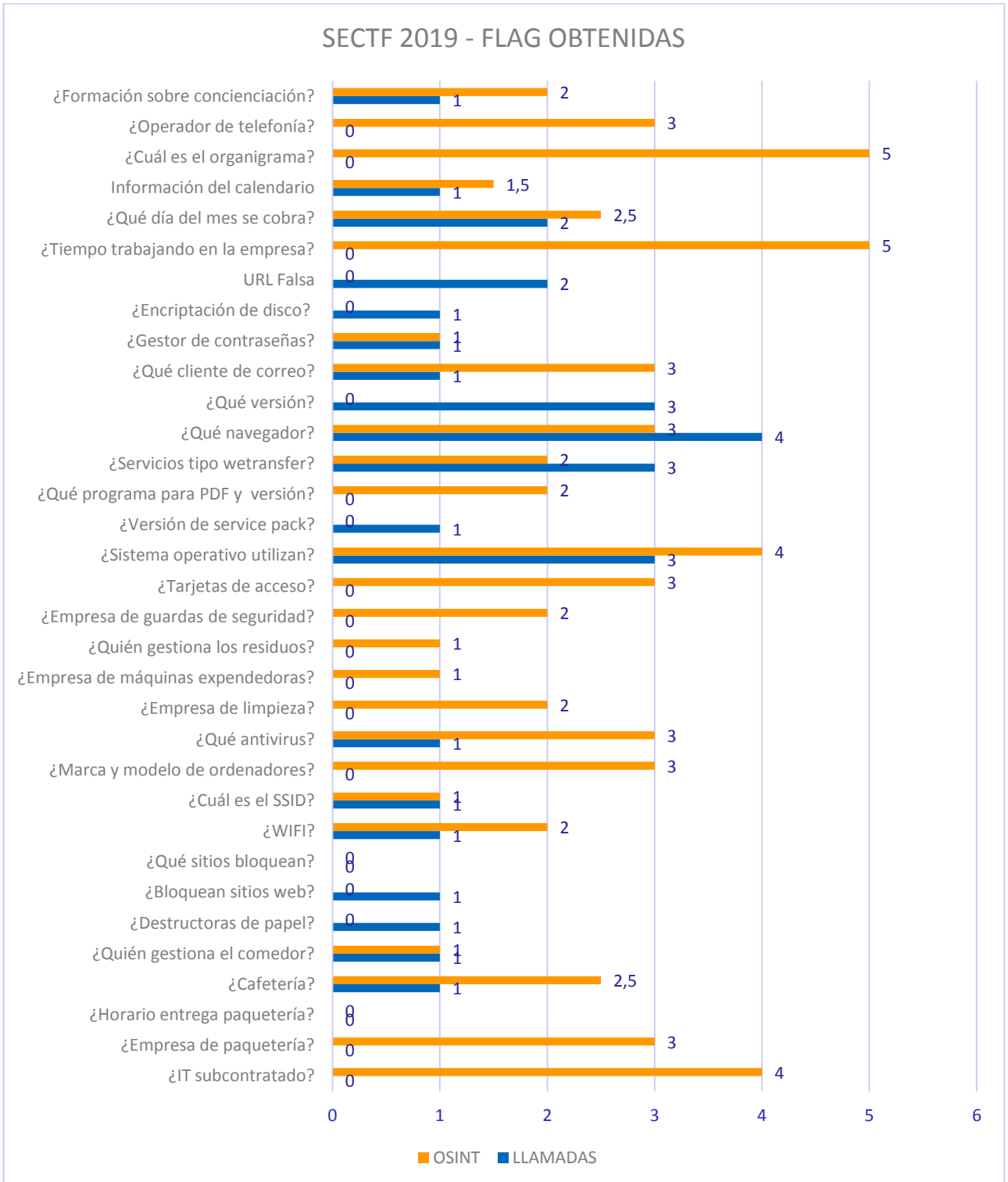

Gráfico 5: Número de flag obtenidas

Se observa que se consiguieron mayor número de flag durante la fase OSINT, que durante la fase de llamadas.

Esto se debe en parte a la diferencia de tiempo disponible para cada una de las fases, siendo el tiempo muy limitado para la fase de llamadas, lo cual que llevó a los participantes a elegir un número reducido de flags.

Finalmente, destacar que las flags “versión del navegador”, “versión de service pack del SO”, o “uso de encriptación en disco” sólo se lograron conseguir durante la fase de llamadas.

Conclusiones

En primer lugar, resaltar la cantidad de información que los participantes fueron capaces de obtener, con una dedicación limitada a su tiempo libre.

Existen tres grandes grupos de información en la fase OSINT:

- Información publicada por la propia empresa.
- Información publicada por empleados o proveedores.
- Información publicada por personas o entidades ajenas a la empresa.

Gran parte de la información disponible fue proporcionada voluntaria o involuntariamente por las propias empresas y fue localizada en:

- Contenido y metadatos de los documentos que han hecho públicos.
- Videos e imágenes corporativos.
- Sitios web propios u otros servicios.

En algunos casos se han encontrado grupos privados en redes sociales (se desconoce si son oficiales), pero que no tienen un método de validación riguroso, y que sin embargo contienen gran cantidad de información que no debería ser pública.

Otro aspecto destacable es la cantidad de medios a través de los que fue posible contactar con los empleados de las empresas. Es preocupante la facilidad con la que se pudieron obtener los números de teléfono directos de muchos empleados.

Esto hace que, ante una llamada telefónica maliciosa, la seguridad dependa exclusivamente de la capacidad de esta persona para catalogarla como una amenaza y contrarrestarla.

Aunque se hayan llevado a cabo formaciones de concienciación, y los empleados sean personas responsables, cualquier persona puede ser vulnerable a los ataques de ingeniería social en momentos puntuales o bajo circunstancias concretas.

Es digno de mención la cantidad de información que se ha podido obtener de los proveedores. En la mayoría de las ocasiones en publicaciones de marketing en las que se revela información sensible sobre los clientes.

Como se ha comentado anteriormente, la mayoría de los participantes no profundizó en la información personal disponible sobre los trabajadores, aunque en base a nuestra propia experiencia, se subraya que es el conocimiento sobre pequeños detalles y preferencias personales el que consigue en muchas ocasiones que los ataques de ingeniería social más complejos tengan éxito.

Por otra parte, existen diversos sitios de terceros que no tienen relación con las empresas, en los que se revela gran cantidad de información sobre las mismas.

Parece claro que uno de los grandes retos de cualquier organización hoy en día, es la dificultad para controlar la información pública que existe sobre la misma en Internet, incluso sin ni siquiera haber sido publicada por ella misma.

En cuanto a la fase de llamadas, la principal conclusión que se ha obtenido es la facilidad con la que la mayoría de participantes han sido capaces de obtener la información, aspecto que incluso sorprendió a alguno de ellos, ya que en muchos de los casos se consiguió obtener la información deseada, sin levantar ninguna señal de alerta en los objetivos.

Estos resultados apuntan a que los interlocutores pueden no haber recibido, al menos recientemente, formación/concienciación en la detección de ataques de vishing. Otra hipótesis es que puedan no tener clara cuál es la política de seguridad de la empresa al respecto (si es que la hubiera), o qué información es sensible, y a quién se la pueden proporcionar.

Las limitaciones debidas al tiempo y normativa impiden medir con precisión la situación de una empresa frente a este tipo de amenaza. No obstante, señalan a que si en unas pocas llamadas se ha conseguido obtener una cantidad de información considerable, el nivel de exposición de las empresas frente a ataques de ingeniería social por parte de un atacante malicioso, con objetivos económicos y disponibilidad de tiempo, podría ser bastante alto.

Mitigación

Tras analizar en profundidad el desarrollo de ambas fases, hemos dividido las consideraciones para la mitigación en tres diferentes áreas:

Medidas de protección

El primer paso a la hora de garantizar la seguridad de la información, es sin duda la de disponer de una infraestructura moderna, actualizada y fortificada:

- Activos actualizados.
- Servicios correctamente configurados y fortificados.
- Limitada exposición en Internet.
- Servicios de Intranet accesibles vía VPN.

Deberían existir **directrices claras** a la hora de publicar contenido, que eviten la publicación de información sensible, no solo en los documentos, sino también en cualquier contenido audiovisual, como videos e imágenes corporativas.

Se recomienda automatizar el **borrado de los metadatos** en todos los documentos en los que su presencia sea innecesaria, y no solo antes de publicarlos, ya que en ocasiones documentos que originalmente no han sido concebidos para su publicación, acaban siendo expuestos por medios alternativos.

En una sociedad en la que el control de la información que se publica escapa de nuestras manos, es imprescindible hacer una **monitorización sobre la información** online existente. Esta monitorización ha de ser persistente en el tiempo, lo que nos permitirá conocer qué información va apareciendo y tratar de solicitar su eliminación, en caso necesario.

Expresamente se recomienda la **monitorización de los leaks** de información que vayan apareciendo en Internet. Es posible automatizar este tipo de comprobación, para ponerse al corriente de brechas de seguridad de las que se podría no ser consciente.

Debido a la inmensa cantidad de medios de los que se dispone en la sociedad actual para comunicarse con otras personas, es posible hacer llegar un mensaje prácticamente a cualquier individuo con conexión a Internet. Este hecho pone en una notable situación de vulnerabilidad al receptor del mensaje, ya que se le puede hacer llegar directamente contenido expresamente diseñado para influenciarle.

Es por esta razón que se recomienda **limitar**, en la medida de lo posible, **los medios** a través de los cuales se puede contactar con los empleados de las empresas.

Al respecto del vishing, se recomienda en el ámbito de telefonía:

No publicar los números de teléfono directos de los empleados, ni las extensiones internas. Además del riesgo de manipulación directa, esto ayudaría a suplantar su identidad mediante el identificador de llamada.

Centralizar, en la medida de lo posible, **las llamadas** en una centralita donde una persona con formación específica para detectar los ataques de ingeniería social haga un primer filtro.

Se recomienda **desviar el flujo** de cierto tipo de solicitudes de información, como por ejemplo las encuestas o cierto tipo de entrevistas, al correo electrónico, donde se va a disponer de mayor cantidad de tiempo para analizar si procede revelar esa información, y la sensación de apremio va a ser menos acuciante que en una llamada telefónica.

Es imprescindible que a la hora de facilitar cierto tipo de información crítica, o a la hora de realizar ciertas acciones (como puede ser el cambio de un número de cuenta para realizar un pago, o la regeneración de una contraseña por parte del centro de atención al usuario CAU), **se compruebe fehacientemente la identidad** del llamante, más allá de lo que pueda indicar el identificador de llamada, que puede ser fácilmente suplantado.

En lo referente al CAU, se recomienda centralizar la gestión de las solicitudes de asistencia en un sistema que permita que el solicitante se identifique mediante unas **credenciales únicas**, y genere un número de ticket que ambas partes podrán utilizar para hacer referencia a esa solicitud en concreto. El técnico debería ser quien posteriormente contacte con el solicitante por un medio de confianza, lo que garantizará que contacte con la persona adecuada.

En caso de no disponer de un sistema de estas características, será necesario que el empleado que está abriendo una incidencia, se identifique con como mínimo con el número de empleado y DNI. Ni decir tiene, que el número de empleado es un dato a proteger, más aún si se utiliza como identificador para este tipo de situaciones.

En caso de que sea un técnico del CAU el que contacte con un empleado, siempre deberá **facilitar el número de ticket**, y en caso de que el usuario no haya abierto la incidencia, o que el técnico indique que se trata de una comprobación rutinaria, o algún pretexto similar, deberá direccionar la llamada a la persona que se encargue de gestionar el CAU, si es interna, o a la persona que lleve la relación con el proveedor si es subcontratado.

En cualquier caso, ha de quedar claro que bajo ninguna circunstancia se deberá revelar información sensible o realizar acciones comprometidas sin haber verificado la identidad de la otra persona.

Cabe señalar que muchas empresas externalizan el sistema de atención al usuario, lo que supone una complicación por la pérdida de control y visibilidad de este entorno, por no formar parte de la propia organización. En estos casos, es recomendable solicitar al proveedor **estrictas medidas de seguridad y formación** específica, así como una revisión habitual de los procedimientos de respuesta en base a los requerimientos y roles de acceso a la información.

Por último, para que todas estas recomendaciones sean efectivas, es imprescindible **definir qué información es sensible** para nuestra organización y clasificarla en diferentes niveles de criticidad, para posteriormente poder definir qué empleados deben tener acceso a cada nivel, y qué información pueden revelar, a quién, y en qué circunstancias. Debe haber una política clara al respecto, ya que en caso contrario se podría revelar gran cantidad de información sensible, por el sencillo motivo de que la persona que maneja esa información no sepa que es sensible, o no sepa a quién tiene permitido revelársela.

Auditorías, medición y seguimiento

La única forma de tener una visión objetiva del nivel de exposición de nuestra organización frente a los ataques maliciosos, pasa por realizar una correcta **evaluación de riesgos** basada en test de penetración realizados por profesionales, que en lo referente al ámbito de la ingeniería social deberán incluir campañas de phishing, vishing, e intrusión física.

Debido a la constante aparición de nuevas vulnerabilidades y técnicas para explotarlas, la posible publicación de información sensible sobre la empresa, la posibilidad de nuevos errores en la configuración de infraestructuras, o nuevas tendencias en los ataques de ingeniería social, entre otros, es necesario que los **test de intrusión** se realicen de forma periódica a lo largo del tiempo.

De esta manera nos permitirá **definir una política de seguridad** adecuada a las circunstancias de cada momento, y desarrollar **acciones de formación y concienciación** basadas en los resultados obtenidos en estas auditorías, y por tanto adaptados a las necesidades de nuestra organización.

Concienciación y formación

Es indispensable que los empleados **conozcan las políticas de seguridad** definidas por la empresa y que pueden afectar a su puesto, de manera que tengan claro qué información pueden revelar y a quien.

Se recomienda que todos los empleados reciban una formación básica sobre **concienciación en seguridad digital**, y que los perfiles más vulnerables o expuestos, que deberán ser determinados para cada organización, reciban una formación específica para hacer frente a las amenazas relacionadas con su puesto de trabajo.

Esta formación ha de ser una **formación eminentemente práctica**, estrechamente relacionada con los test de penetración, realista y coherente con la realidad de la empresa, que proporcione a los empleados la experiencia necesaria para que el día que suceda un incidente puedan tomar las decisiones adecuadas, y no se vean sobrepasados por las circunstancias.

Una forma de proporcionar experiencia a los empleados es la **realización de campañas** de phishing, vishing e intrusión física realistas, que les permitan vivir estas experiencias en primera persona y acostumbrarse a contrarrestarlas de manera natural.

Por otro lado, como hemos indicado en este mismo informe, parte de la información expuesta, ha sido publicada por los propios empleados en sus cuentas personales. Cada empleado cuenta con total libertad sobre lo que decide publicar en sus cuentas personales, siempre que se encuentre dentro del marco legal, y desde la empresa no se puede definir que puede o no publicar una persona en el ámbito privado. Sin embargo, si se proporciona a los empleados **formación sobre buenos hábitos** en la gestión de su información personal en los medios digitales, esto hará en la mayoría de los casos que sean conscientes de las consecuencias que un mal uso de los mismo pudiera tener, y adopten estos buenos hábitos en su vida privada, y por ende redunde en beneficio de los intereses de la organización.

Al igual que los test de penetración, esta formación se deberá repetir de forma periódica, de tal forma que los empleados se mantengan al día de las últimas amenazas, y cómo contrarrestarlas, evitando bajar la guardia con el paso del tiempo.

Para cualquier consulta relacionada con el SECTF o este informe puede contactar con EuskalHack a través de la siguiente dirección de email: **sectf[@]euskalhack[.]org**

Plaza de las cigarreras 1, 3ª (ImpactHub), 20012 - Donostia / San Sebastián
info@euskalhack.org
www.euskalhack.org
@euskalhack
linkedin.com/company/euskalhack