# 20

# Introducción a la Seguridad Operacional

La última parte de este libro está dedicada a aterrizar de una manera más práctica nuestra estrategia de ciberdefensa personal. Las partes previas podemos tomarlas como un ejercicio exploratorio sobre todo aquello a tener en cuenta para proteger nuestra identidad digital y nuestros datos. Ahora toca aterrizar nuestra estrategia de una manera más concreta y estructurarla teniendo en cuenta también aquellas amenazas particularmente avanzadas.

En el capítulo 5 se introdujo el concepto de modelado de amenazas, distinguiendo entre indiscriminadas, oportunistas, dirigidas y avanzadas. En capítulos posteriores hablábamos de cómo algunas de nuestras tácticas son útiles frente a algunas de estas amenazas, pero inútiles frente a otras. Por ejemplo, una autenticación reforzada basada en la recepción de códigos por SMS puede ser suficiente frente a amenazas indiscriminadas, pero a la vez insuficiente frente a ataques dirigidos o avanzados. Además, estas tácticas de ciberdefensa personal pueden ser robustas, pero requieren también que adoptemos una cierta disciplina y comportamientos específicos en el mundo físico. Por ejemplo, de nada sirve tener contraseñas robustas o bloquear nuestro dispositivo si permitimos frecuentemente que otros vean como tecleamos nuestro PIN en lugares públicos. También pueden requerir que adoptemos disciplina en el ámbito social. De nada sirve utilizar una plataforma con cifrado de extremo a extremo para proteger una foto sensible de ojos indiscretos si luego la enviamos a decenas de contactos que no cuentan con nuestra plena confianza. Esta combinación de

tecnología y comportamiento conforman una estrategia de Seguridad Operacional.

El concepto de Seguridad Operacional (abreviado *OpSec*) proviene del argot militar. Según las definiciones más ortodoxas OpSec se refiere al proceso sistemático y probado para evitar que potenciales adversarios obtengan acceso a información sobre nuestros planes o actividades [199]. Otros autores más elocuentes como *The Grugq* definen el OpSec como el arte de «conseguir que no nos pillen» [200]. En términos de lo que nos puede interesar como lectores de este libro, OpSec es una disciplina interesante porque nos enseña a adaptar y enriquecer las tácticas vistas hasta ahora según sea nuestra circunstancia particular. En este caso no estaremos planeando operaciones militares o de espionaje a otros estados enemigos, pero bien podemos encontrarnos necesitando protección de amenazas avanzadas que buscan comprometer nuestra identidad o nuestros datos. En términos similares al de un enfrentamiento entre estados esto sería el equivalente a realizar operaciones de contraespionaje. Además, según el perfil de amenazas al que nos enfrentemos, podemos necesitar estrategias de grado militar para garantizar que nuestro OpSec esté a la altura.

En ocasiones, debido a nuestra posición social y exposición pública, podemos llegar a pensar que estamos constantemente en el foco de atención. La paranoia puede volverse fuerte en nuestras mentes mientras pensamos que absolutamente toda nuestra actividad online está siendo monitorizada por adversarios con las capacidades suficientes. La realidad es que por mucha exposición que tengamos y salvo casos excepcionales, es raro que incluso los adversarios más avanzados estén constantemente monitorizando nuestra actividad digital. Incluso los periodistas más perseverantes, los fans más obsesivos y los gobiernos con mejores programas de vigilancia y espionaje tienen sus limitaciones. Tarde o temprano el coste de oportunidad les obliga a tener éxito o a tener que desviar su foco, aunque solo sea temporalmente.

Distinguir entre periodistas, adversarios, fans y gobiernos autoritarios es también relevante, pues sus capacidades para probar la robustez de nuestra OpSec varían mucho en intensidad y profundidad. Estrategias preparadas para resistir amenazas que utilizan prismáticos pueden ser inadecuadas contra aquellas que utilizan microscopios, y viceversa. Como vimos en el capítulo 5 es importante no perder nunca la referencia de nuestro modelo de amenazas. De lo contrario es fácil perder el foco y la consistencia al mantener nuestra estrategia de ciberdefensa personal. En particular, cuando en nuestro modelo entren las amenazas avanzadas y persistentes, nuestra OpSec debe ser ortodoxa y rigurosa, con poco espacio para equivocaciones. Cuando las amenazas sean indiscriminadas u oportunistas, quizá tengamos más margen de error.

Un último punto antes de continuar. Compartir técnicas sobre seguridad operacional puede ayudar a delincuentes a no acabar en la cárcel. Aunque este libro no busca ser un manual para ayudar a los malos a evitar que los buenos les pillen, estas técnicas pueden también ayudar a personas con malas intenciones. Detrás de la poca divulgación popular sobre OpSec puede existir una motivación para justo evitar publicar alegremente este tipo de información como si fuera una receta para fabricar explosivos con ingredientes caseros. Desgraciadamente esta falta de divulgación perjudica más a aquellas personas con buenas intenciones que necesitan aprender y mejorar su OpSec. La gente con buenas estrategias de seguridad operacional no habla de ellas. Ni siquiera admite tenerlas. Si bien la seguridad operacional exige siempre un componente introspectivo para adaptar artesanalmente los principios generales a cada situación personal, estos principios tampoco es fácil encontrarlos. La literatura disponible sobre estos temas oscila entre largos manuales poco prácticos hasta guías más cabales, pero de alcance más limitado [201].

Con la intención de compartir con el lector una iniciación a la OpSec lo más completa posible, en los siguientes capítulos trataremos de presentar sus fundamentos principales. Su necesaria adaptación a

las circunstancias de cada persona quedará patente con algunos casos prácticos que introduciremos a continuación.

## Elenco de Personajes

El aprendizaje basado en casos prácticos puede ser una herramienta muy potente para afianzar conceptos y plantear situaciones simuladas (basadas en casos reales o no) donde poder aplicar los conocimientos adquiridos. Ya hemos visto que tácticas como activar la autenticación reforzada, bloquear nuestros dispositivos y borrar periódicamente nuestro historial de actividad son pilares comunes de cualquier estrategia de ciberdefensa personal. Pero mejorar aún más nuestro juego mediante el uso de tácticas de seguridad operacional requiere comenzar a modificar estas estrategias con más atención al detalle.

A continuación, presentaremos diferentes casos prácticos que nos permitirán aterrizar en los próximos capítulos estrategias de ciberdefensa personal que incorporen la seguridad operacional como parte integrante. Cada caso está estructurado de la siguiente forma:

- Quién - una descripción de la persona y de su actividad.
- Activo - aquello que busca proteger, por ejemplo, su anonimato.
- Amenazas - los adversarios que buscan comprometer el activo.
- Retos - dificultades a las que debe enfrentarse la persona para proteger su activo.

## Un cantante

Larry es un cantante de éxito global. Sus fans se cuentan por millones y sus giras por las grandes capitales movilizan cientos de miles de personas llenando estadios durante varios días consecutivos.

Larry no puede pasear por la calle como una persona normal. Información cotidiana sobre su vida como en qué restaurante comerá o en qué lugar estará puede movilizar a cientos de personas en muy corto

espacio de tiempo. Las fotos y vídeos que captura con su teléfono móvil, en particular aquellas que intercambia con su familia y amigos más cercanos, pueden resultar de interés para muchas personas. Además, puede estar iniciando una relación sentimental con una persona mucho menos expuesta y cuya privacidad debe preservarse a toda costa.

Larry se enfrenta a hordas de fans allá donde viaja, especialmente en ciudades donde su gira tiene alguna parada. Estos harán todo lo posible por averiguar su ubicación actual o próxima. Los paparazzi le esperarán a la salida de su casa, de las tiendas y restaurantes que frecuente. Cuando consiga evitarlos, cualquier persona que le identifique puede sacarle una foto en un lugar público y compartirla en redes.

Larry no tiene mucho tiempo para configurar adecuadamente sus cuentas ni entiende bien cómo funciona el permiso para acceder a su localización en un smartphone. Puede disponer de escoltas que le acompañen en el mundo físico e incluso quizá alguien que le gestiona sus cuentas online [202]. Sin embargo, no confía tanto en ellos como para darles acceso a sus mensajes privados o fotos sensibles. Activar la autenticación reforzada puede crearle problemas ya que cambia de número de teléfono con mucha frecuencia [203]. Cuando comparte contenido con sus contactos, siempre tiene la duda de si puede confiar en que no lo reenvíen a otras personas.

## Una alta directiva de una multinacional

Rosa lidera una de las verticales de negocio de una de las 50 empresas más grandes del mundo. Proviene de un entorno humilde y mantiene una vida alejada de los excesos que frecuentemente caracteriza a otras personas de su posición social y poder adquisitivo. Trabaja mucho. Durante largas temporadas trabaja los fines de semana al menos la mitad del día. Su ritmo frenético de trabajo le obliga a atender decenas de llamadas a la semana, así como cientos de chats o correos.

Rosa maneja información privilegiada de su compañía. Un tipo de información que podría dar un vuelco al valor de diferentes acciones y muy codiciada para inversores que busquen ganar mucho dinero

en bolsa. Rosa debe además asegurarse de que su círculo cercano de amistades o colegas no obtiene acceso a la misma para no verse envuelta en algún potencial litigio por tráfico de información.

Rosa se enfrenta a posibles adversarios que busquen acceder a la información privilegiada que ella maneja. Sus dispositivos pueden ser robados. Ataques de phishing o de malware pueden llegar a su buzón. Los metadatos que genera pueden revelar información sobre fusiones o adquisiciones próximas o sobre la apertura de nuevas líneas de negocio. También debe cuidar los accidentes o despistes que podrían permitir a terceras personas obtener información sensible.

Aunque Rosa cuenta con un equipo de seguridad en su empresa que le proporciona dispositivos debidamente configurados y consejos de ciberdefensa personal, esto puede no ser suficiente. El día a día frenético puede favorecer que sea víctima de un phishing bien preparado. Las páginas que visite o las búsquedas que realice pueden dar indicios sobre operaciones próximas en las que esté trabajando. Su familia o su jardinero podrían oír sus conversaciones mientras habla por teléfono.

## Un presentador de la TV que podría llegar a alcalde

Gunther es un presentador de TV cuya trayectoria le ha llevado a liderar un partido político local en una ciudad de aproximadamente 3 millones de habitantes. En las próximas elecciones planea presentarse a alcalde. El contexto político es muy bronco y el anterior alcalde tuvo que dimitir acusado de haber publicado hace años algunos mensajes poco afortunados en su perfil público de una red social.

Gunther presentaba un programa de humor con buenas cifras de audiencia, pero nunca ha sentido reparos en expresar sus opiniones libremente. Tampoco ha sentido nunca que su trabajo se haya visto afectado por su orientación política. Ahora, de alguna manera siente que debe protegerse de las cosas que decía hace 10 años.

Gunther se enfrenta a los recursos de los partidos políticos de la oposición y a todo aquel que desee rebuscar en su pasado en busca

de alguna información que le pueda perjudicar. Su familia y amigos cercanos también sufrirán el escrutinio de la opinión pública. Algunos medios publicarán cualquier información privada que pueda hacerle perder reputación u honorabilidad.

Gunther nunca pensó que llegaría a un cargo público con este nivel de exposición. Como presentador de TV todavía se comportaba como un ciudadano más, sin prestar atención a si alguno de sus comportamientos podía traerle problemas en el futuro. Siempre ha sido muy activo en redes sociales y ha intercambiado infinidad de mensajes privados en largas conversaciones usando múltiples plataformas. Gunther considera imposible hacer un inventario de potenciales evidencias digitales que pueden ser utilizadas por sus adversarios contra él [204].

## El whistleblower

Hiroko trabaja para el cuerpo de policía en una unidad especializada en investigar posibles casos de tráfico de influencias en las administraciones públicas. Por la naturaleza de estas investigaciones, Hiroko está acostumbrada a acceder a información muy sensible y a mantener protocolos de confidencialidad muy estrictos. Además, debe seguir procedimientos bien reglados para obtener las autorizaciones pertinentes antes de poder utilizar las herramientas que le proporcionan la información que necesita.

Hiroko ha detectado que algunos compañeros y cargos superiores de su unidad no se están comportando siguiendo los protocolos que regulan sus investigaciones. Sus métodos son poco ortodoxos y en numerosas ocasiones han abusado de su posición para acceder a información muy sensible de personas sobre las que no había ninguna investigación en curso y sin obtener previamente autorización por parte de un juez. Hiroko cree que estas prácticas suponen un abuso de poder y deben denunciarse públicamente para que puedan ser sancionadas y corregidas, pero le preocupan las posibles represalias de sus compañeros y superiores.

Una vez la historia salga a la luz, Hiroko se enfrenta a una posible caza de brujas. Si las personas afectadas por la filtración averiguan que fue ella quien acudió a la prensa, quién sabe de qué serían capaces. Su carrera profesional podría acabar, pero también podría verse envuelta en alguna contraofensiva por parte de los denunciados que podría afectar a su familia o amigos.

Hiroko debe ser capaz de encontrar un confidente que le ayude a sacar a la luz esta información y que sepa preservar su anonimato. Los adversarios que desearán saber quién filtró la historia tienen acceso a herramientas muy poderosas para investigar y romper la privacidad de todo tipo de comunicaciones electrónicas. Hiroko sabe cómo funcionan este tipo de investigaciones, pero teme poder cometer algún error que revele su identidad indirectamente.

## Un administrador con privilegios en una plataforma sensible

Anand trabaja desde hace 20 años como ingeniero de bases de datos para una de las aseguradoras más grandes de su país. Su mercado más fuerte son los seguros de salud. Para desempeñar sus funciones, Anand tiene acceso privilegiado como administrador a la práctica totalidad de bases de datos y aplicaciones de gestión que utilizan el resto de los empleados de la compañía. Es capaz de operar sin restricciones sobre todas esas plataformas, lo que le permite poner en valor toda su experiencia y conocimiento histórico para resolver problemas y así mantener todos los sistemas funcionando correctamente. Los jefes valoran mucho el trabajo orientado a resultados de Anand y siempre le han dejado trabajar sin dejar que nadie supervisara sus métodos.

Las cuentas de usuario que Anand utiliza tienen un montón de privilegios en la infraestructura tecnológica de la empresa. La mayoría de los servicios críticos de los que depende la aseguradora se verían seriamente afectados si alguien con malas intenciones consiguiera robar la cuenta de empleado de Anand. Los clientes también se verían afectados, pues Anand tiene acceso a los datos de salud de todos ellos.

Anand se enfrenta a la posibilidad de que alguien consiga robar sus credenciales, acceder a la infraestructura de la empresa y realizar un ataque de ransomware de doble extorsión. Estos ataques primeramente roban los datos disponibles para luego cifrarlos y solicitar un rescate a cambio de recuperarlos (primera extorsión). Adicionalmente los malos avisan de que, en caso de no pagar el rescate, los datos robados se filtrarían al público (segunda extorsión).

Anand es una persona con grandes conocimientos técnicos que considera que los ataques de ransomware solo afectan a personas poco preparadas o despistadas. Además, no considera problemático que sus cuentas personales tengan acceso a todas las bases de datos, pues a diferencia de otros profesionales menos cuidadosos, él necesita esos privilegios en su día a día y cree que no debería tener que rendir cuentas a nadie por su uso.

## Un inversor en Bitcoin

Michal trabaja en un banco de inversión gestionando carteras multimillonarias de renta variable. En su ámbito privado, además de tener una modesta cartera de acciones donde tiene buena parte de sus ahorros, Michal tiene una suma muy sustancial de activos en forma de Bitcoins fruto de su estrategia de inversión en activos exóticos.

Michal descubrió la existencia de Bitcoin como inversión a largo plazo gracias a un amigo personal que le introdujo al mundo de los cripto activos en el verano de 2016. Desde entonces, el precio de Bitcoin se ha disparado, multiplicando la inversión inicial hasta llevarla a un valor actual de varios millones de euros.

Michal se enfrenta a la posibilidad de ser atacado por mafias que busquen robar bienes de fácil venta. Los ataques posibles empiezan por los puramente digitales que buscan comprometer el billetero digital donde las guarda para transferir los activos de manera no autorizada. Pero también debe enfrentarse a potenciales ataques físicos en los que su integridad o la de su familia pueden estar en riesgo. Secuestros,

extorsiones o torturas pueden ser amenazas perfectamente posibles cuando tus enemigos creen poder robarle varios millones de euros.

La naturaleza de las criptomonedas las hace objetivos muy suculentos para los ladrones. Mover fondos a la otra punta del mundo es mucho más fácil y rápido que con transferencias de divisas tradicionales. Además, seguir su rastro puede ser una tarea costosa tanto para la víctima como para las fuerzas de seguridad del estado. Si algo caracteriza la tarea de custodiar criptomonedas es la poca tolerancia a fallos que existe. Una única operación no autorizada y todos los fondos desaparecen instantáneamente con casi ningún margen de maniobra para correcciones o recuperaciones.

## ¿Por dónde empezar?

Cada uno de los personajes que acabamos de presentar tiene unas necesidades y contexto muy diferentes. Las amenazas a las que se enfrentan son también muy distintas entre sí y los retos que se les plantean van desde la mera falta de conocimiento de Larry, las limitaciones en conocimiento técnico de Rosa y Gunther hasta la falta de humildad de Anand. Pero encontrar la solución más adecuada para cada una de estas historias invita previamente a recorrer dos estaciones:

1. Entender el estado actual del ecosistema de amenazas en base a la historia reciente. Muchas de las amenazas que antaño parecían sacadas de guiones cinematográficos se han ido desvelando como reales gracias a periodistas e informantes anónimos.

2. Entender la filosofía y técnicas más adecuadas para cada caso particular. Tomando como punto de partida las lecciones de las partes previas del libro, las adaptaremos según las necesidades de cada personaje y aplicaremos diferentes principios de seguridad operacional.