1-1-2023

Capítulo 16 Ciberseguridad

Shambhavi Roy

Clinton Daniel
University of South Florida

Manish Agrawal
University of South Florida

Pablo Brescia
University of South Florida

Clara Olivia Ocampo

See next page for additional authors

Ciberseguridad

16

CONTENIDOS DEL CAPÍTULO

> *Si la seguridad fuera lo único que importara, las computadoras nunca se encenderían, y mucho menos se conectarían a una red con literalmente millones de intrusos potenciales.*
>
> — Dan Farmer, investigador y programador de seguridad informática.

Panorama: ¿qué es la ciberseguridad?

El Instituto Nacional de Estándares y Tecnología (NIST, siglas en inglés de National Institute of Standards and Technology), fundado en 1901, forma parte del Departamento de Comercio de EE. UU. y apoya la misión estadounidense de promover las innovaciones y la competitividad industrial actuales. Esta misión se logra mediante el avance de mediciones y estándares en ciencia y tecnologías que mejoran la seguridad económica y la calidad de vida. NIST define la ciberseguridad como:

> Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no rechazo.[249]

En el centro de la ciberseguridad está la motivación para proteger la información y los sistemas que la gestionan. De hecho, la ley estadounidense, 44 USC 3552, define la seguridad de la información como "proteger la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados con el fin de proporcionar integridad…, confidencialidad…, y disponibilidad…".[250]

En la práctica de la ciberseguridad, esto se conoce comúnmente como la tríada CIA, donde **C** significa confidencialidad, **I** integridad y **A** disponibilidad. Lo notable aquí es que la ciberseguridad tiene que ver con la información y los sistemas que respaldan su gestión. Nuestra información y nuestros sistemas están cada vez más frecuentemente bajo el ataque de adversarios poderosos que quieren robar los datos para obtener ganancias. Por lo tanto, comprender la ciberseguridad es importante para proteger el futuro de las personas, los recursos y las sociedades. Nuestro viaje hacia esta comprensión comienza con la exploración del pasado para saber cómo hemos llegado al presente. Luego, exige que volvamos nuestra atención a estudiar hacia dónde nos dirigimos en el futuro.

Antes de comenzar a comprender cómo llegamos al clima actual de ciberseguridad, primero establezcamos algo de contexto con la tríada CIA. Esto nos ayudará a comprender qué motiva a los actores de la ciberseguridad en el pasado, presente y futuro.

Confidencialidad

Según 44 USC 3552(b)(3)(B): " Confidencialidad…significa preservar las restricciones autorizadas de acceso y divulgación, incluidos los medios para proteger la privacidad personal y la información de propiedad exclusiva". La ley reconoce el derecho de los individuos a la privacidad, y dicho derecho se

249 NIST, Computer Security Resource Center (CSRC), Information Technology Laboratory, https://csrc.nist.gov/glossary/term/cybersecurity (consultado en mayo del 2024).

250 44 USC 3552(b)(3), https://www.law.cornell.edu/uscode/text/44/3552 (consultado en mayo del 2024).

extiende a la información que, de hacerse pública, podría causar daño a la persona. Es responsabilidad de los custodios de la información preservar esa privacidad de las personas cuya información tienen en su poder. Por ejemplo, la gente confía en los bancos para proteger la privacidad de la información de sus tarjetas de crédito. La expectativa es que los bancos (los custodios de la información) no permitan que la información de las cuentas de sus clientes quede expuesta a quienes no requieren su acceso.

Los bancos han implementado servicios modernos de ciberseguridad para custodiar la privacidad de la información de sus clientes. Dichas prácticas incluyen servicios como alertas de fraude a los clientes cuando las tarjetas de crédito se utilizan de manera inusual. Estos servicios brindan a los consumidores la oportunidad de congelar su tarjeta de crédito para que no pueda ser utilizada por alguien que haya violado su información confidencial. A esta respuesta normalmente le sigue cambiar la tarjeta de crédito comprometida para que los datos robados ya no sea útiles y disputar todos los cargos no deseados a dicha tarjeta.

Integridad

La ley 44 USC 3552(b)(3)(A) define la integridad como: "Integridad…significa proteger contra la modificación o destrucción inadecuada de la información, e incluye garantizar que no se rechace y la autenticidad de la información".

Cuando se extraen datos de un sistema de información, por ejemplo, las calificaciones escolares o el extracto mensual de una cuenta bancaria, se cuenta con que la información proporcionada sea confiable y procesable. Por ejemplo, cuando el banco informa el saldo de una cuenta corriente, en general los dueños de la cuenta no creen necesario calcular ellos mismos los totales de créditos, débitos e ingresos por intereses para verificar el monto. Más bien, esperan que el banco haya hecho los cálculos correctos. Imagínate lo compleja que sería la vida si no se pudiera creer que la información que se recibe de los sistemas de TI sea precisa. La integridad es el aspecto de la seguridad de la información que evita que eso suceda.

Veamos el siguiente ejemplo: has trabajado muy duro durante todo el semestre para tener buenas calificaciones en todas tus clases. Ahora es el momento de las boletas de calificaciones y esperas obtener A en todas tus clases. Abres tu boleta de calificaciones y esta muestra que has reprobado todas tus clases. La situación podría ser devastadora y quizás arruinaría tus posibilidades de ingresar a la universidad de tu elección. Este es el impacto que tiene la integridad. Tu expectativa es que el sistema que administra tus calificaciones en la escuela mantenga su integridad para que puedas ser recompensado por tu arduo trabajo. Entonces, al darte cuenta de que la información se ha modificado de alguna manera, deberás disputar las calificaciones y la escuela deberá investigar cómo se ha violado la integridad de tus datos de las calificaciones. Un sistema de información sin integridad no sirve para ningún trabajo serio.

Disponibilidad

La disponibilidad según lo definido por 44 USC 3552(b)(3)(C): "Disponibilidad…significa garantizar el acceso oportuno y confiable a la información y su uso".

Cuando inicias sesión en una clase virtual, esperas que esté en línea. Eso en esencia es la disponibilidad. La relevancia de la disponibilidad para la seguridad de la información se explica por sí misma. Un

sistema de información que no esté disponible no es útil. La mayoría de los virus afectan la disponibilidad; normalmente eliminan archivos importantes, lo que provoca una pérdida de disponibilidad. Incluso si los archivos finalmente se pueden recuperar a partir de sistemas de respaldo u otras fuentes, el tiempo perdido en la recuperación de esos archivos representa tiempo no invertido en hacer un trabajo útil, es decir, una falta de disponibilidad.

El 4 de octubre de 2021 hubo una falta de disponibilidad que se hizo famosa. Facebook, Instagram, WhatsApp y Oculus no estuvieron disponibles a nivel mundial durante un período (Ilustración 253). Este problema de disponibilidad provocó una interrupción global de los servicios de información, que afectó a muchas personas y a empresas diferentes que dependían de la infraestructura de Facebook para sus negocios.

Aunque no se confirmó que la falta de disponibilidad de Facebook y sus servicios fuera un ataque de ciberseguridad, esto demostró el impacto de cómo la no disponibilidad de recursos de la Internet puede causar rápidamente perturbaciones en las sociedades globales dependientes de la información. La Ilustración 254 es una captura de pantalla tomada por este autor el 4 de octubre del 2021, que demuestra con qué rapidez eventos cibernéticos como este de la disponibilidad de información pueden volverse perturbadores y causar miedo y pánico entre las personas.

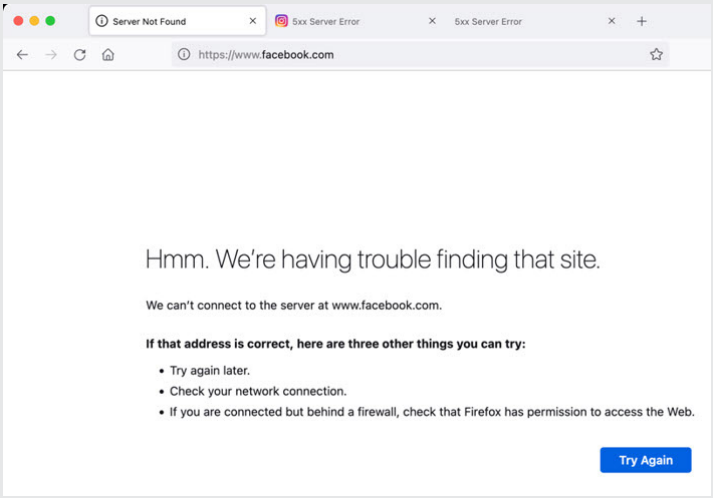


Ilustración 253 — Los sitios web pueden estar "inactivos" por muchas razones, desde técnicas hasta intencionales.

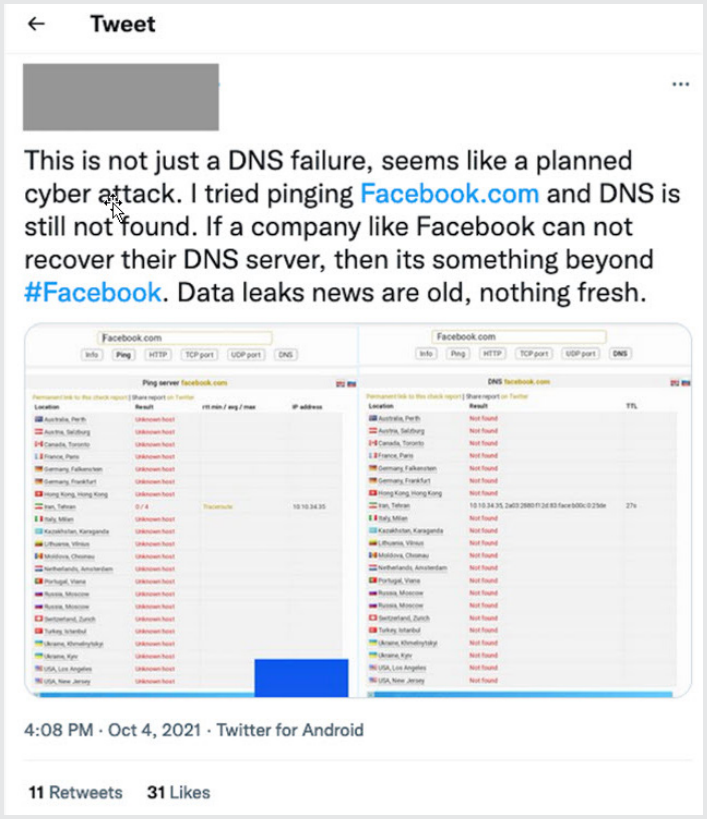


Ilustración 254 — El acceso global a la información permite discusiones en tiempo real sobre los sucesos.

Actualización por parte de Meta sobre la interrupción del 4 de octubre del 2021[251]

¿Qué pasó?

La interrupción del 4 de octubre se produjo debido a un comando emitido por un ingeniero durante el mantenimiento de rutina que de manera involuntaria cortó todas las conexiones de nuestra red troncal, desconectando efectivamente los centros de datos de Facebook de la Internet a nivel mundial. Nuestro blog de ingeniería de Facebook proporciona una explicación más detallada sobre qué causó esta interrupción y el porqué de la demora en restaurar nuestros servicios. No se les cobró ni cobrará a los anunciantes por la publicidad que no se publicó durante el tiempo que nuestros servicios estuvieron fuera de línea. Sin embargo, hemos escuchado de clientes que sus campañas experimentaron volatilidad cuando nuestros servicios se restablecieron.

Por otra parte, el 8 de octubre, un cambio de configuración provocó que algunas personas y empresas tuvieran problemas para acceder a algunas de nuestras aplicaciones y productos durante un período más corto. Tras descubrir el problema, nuestros equipos pudieron resolverlo rápidamente y restaurar el acceso a nuestros servicios.

Breve historia de eventos de ciberseguridad

Para comprender mejor cómo funciona el ámbito de la ciberseguridad en el mundo corporativo actual, es útil conocer incidentes específicos que han ocurrido en el pasado y cómo han influido significativamente en el entorno empresarial. La lista de incidentes que sigue no pretende ser exhaustiva. Pero tiene excelentes ejemplos de preocupaciones sobre la seguridad de la información en el momento en que ocurrieron. Estos incidentes también desempeñaron un papel importante en el establecimiento de algunas de las leyes y organizaciones importantes relacionadas con la ciberseguridad. A medida que leas estos diversos eventos de la historia, notarás cómo nuevos términos y conceptos de la tecnología o ciberseguridad se introducen gradualmente en nuestro léxico diario.

1981—*Desarrollo de las tecnologías centrales de la Internet (TCP e IP)*: Las tecnologías centrales de la Internet se finalizaron en 1981. No se mencionó la seguridad en sus inicios, lo que indica que en ese momento el mundo de la informática no estaba preocupado por la ciberseguridad. Dado que TCP e IP estaban disponibles de forma gratuita, se convirtieron en las herramientas de red preferida para los sistemas UNIX, ampliamente utilizadas en universidades y diversas organizaciones como hospitales y bancos. Sin TCP/IP, es probable que no hubiera redes, y sin redes habría pocos riesgos de ciberseguridad.

251 La información de esta sección proviene de "Update About the October 4 Outage" por Meta, https://www.facebook.com/business/news/update-about-the-october-4th-outage (consultado en mayo del 2024). En español "Actualización sobre la interrupción del servicio del 4 de octubre" https://es-es.facebook.com/business/news/update-about-the-october-4th-outage (consultado en diciembre del 2023).

1982–1983—*La pandilla del 414*: las intrusiones informáticas comenzaron poco después de que TCP e IP se integraran en los equipos industriales. El incidente más publicitado de esta época fue la pandilla del 414, un grupo de seis adolescentes, que obtuvieron su nombre del código de área telefónica de Milwaukee donde vivían. A estos adolescentes les pareció emocionante entrar a sistemas que se suponían fuera de su alcance.

Utilizando computadoras domésticas, líneas telefónicas y contraseñas predeterminadas, este grupo pudo acceder a aproximadamente 60 sistemas informáticos de alto perfil, incluidos los de Los Alamos Laboratories y el Memorial Sloan-Kettering Cancer Center en Nueva York. El incidente recibió una amplia cobertura, incluido un artículo de portada de *Newsweek* titulado "Cuidado: jáquer jugando". Se cree que este es el primer uso del término "jáquer" (*hacker* en inglés, pirata informático) en los principales medios de comunicación dentro del contexto de la seguridad informática. Si bien los adolescentes no causaron ningún daño, fue evidente para la industria ver que las técnicas simples utilizadas por los muchachos podrían ser replicadas fácilmente por otros. Como resultado, el Congreso de los Estados Unidos realizó audiencias sobre seguridad informática. Después de más incidentes de este tipo, el Congreso aprobó la Ley de Abuso y Fraude Informático de 1986, que tipificaba como delito la entrada no autorizada a sistemas informáticos federales o comerciales.

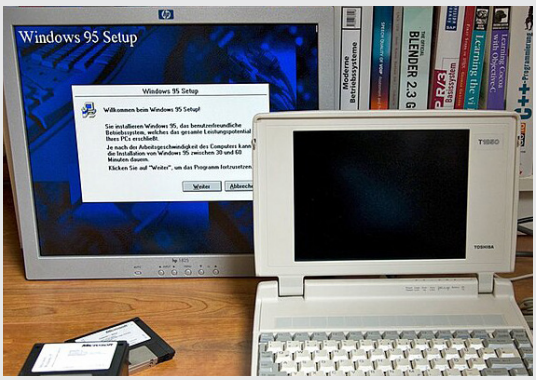
1988—*Gusano Morris*: Robert Morris, entonces estudiante de posgrado en Cornell y ahora profesor de Ciencias de la Computación e Inteligencia Artificial en el MIT, lanzó un programa autorreplicante de 99 líneas el 2 de noviembre de 1988 para medir el tamaño de la entonces naciente Internet. Como resultado de una característica del diseño del programa, derribó muchos sistemas que infectó y logró varios hitos en el proceso. Se considera el primer gusano de la Internet. En términos porcentuales, se estima que derribó la mayor fracción de la Internet jamás registrada (10%). También resultó en la primera condena bajo la Ley de Abuso y Fraude Informático de 1986. Robert Morris fue sentenciado a libertad condicional, servicio comunitario y una multa. El gusano Morris impulsó al gobierno estadounidense a establecer el CERT/CC (centro de coordinación CERT)[252] en la Universidad Carnegie Mellon como un punto único para coordinar la respuesta de la industria y el gobierno a las emergencias de la Internet. El profesor Morris también fue cofundador de Viaweb, una empresa de comercio electrónico comprada por Yahoo y rebautizada como "Yahoo! Store".

Padre e hijo

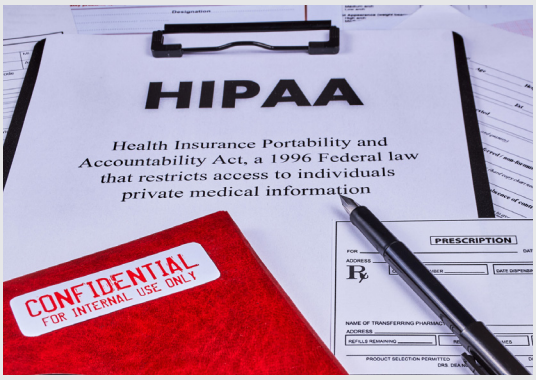
Como anécdota interesante, el padre de Robert Morris, Bob Morris, diseñó el método de cifrado de contraseñas para el sistema operativo UNIX que todavía se utiliza en la actualidad. Aún más interesante es que, en el momento de este incidente, Bob Morris, el padre, era el científico jefe del Centro Nacional de Seguridad Informática (NCSC, por sus siglas en inglés) de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés),[253] la agencia federal responsable del diseño de computadoras seguras.[254]

252 Si bien CERT normalmente significa Computer Emergency Response Team (en español: Equipo de respuesta a emergencias informáticas), CMU ha registrado el nombre como marca de servicio en la Oficina de Marcas y Patentes de EE. UU.

1995–1998—*Windows 95/98*: Microsoft lanzó Windows 95 el 24 de agosto de 1995. El sistema operativo tenía una interfaz gráfica y fue diseñado para ejecutarse en computadoras relativamente económicas. El lanzamiento contó con un fuerte impulso de mercadeo y, en muy poco tiempo, se convirtió en el sistema operativo de mayor éxito jamás producido. Windows 95 fue diseñado principalmente como un sistema operativo de escritorio independiente para un solo usuario y, por lo tanto, casi no tenía precauciones de seguridad. La mayoría de los usuarios utilizaban Windows 95 sin contraseñas y casi todas las aplicaciones ejecutaban Windows 95 con privilegios administrativos para mayor comodidad. Sin embargo, Windows 95 admitía TCP/IP, llevando así TCP/IP a las empresas convencionales. Esta combinación de una tecnología de red (TCP/IP) carente de seguridad combinada con un escritorio empresarial igualmente vulnerable creó un entorno fértil para que florecieran riesgos para la seguridad de la información. En las conferencias, los expertos en seguridad a veces se refieren a este entorno TCP/IP-Windows 95 como el lugar de nacimiento de la profesión de seguridad de la información.[255]



1996—*Ley de Responsabilidad y Portabilidad del Seguro Médico (HIPAA*, siglas en inglés de Health Insurance Portability and Accountability Act): Esta ley, que se centró principalmente en proteger el seguro médico de los trabajadores estadounidenses cuando cambian o pierden trabajo, también tuvo importantes implicaciones para la seguridad de la información. Muchos líderes gubernamentales creían en ese momento que los registros médicos electrónicos (EHR, siglas en inglés de Electronic Health Records) eran un instrumento importante para reducir los crecientes costos de atención médica en Estados Unidos. Por lo tanto, la ley también impulsó los registros médicos electrónicos. Dado que se empezaba a reconocer que la seguridad de la información era una preocupación importante, la ley incluía disposiciones para responsabilizar a las organizaciones de mantener la confidencialidad de los registros de los pacientes en la industria de la atención médica que ahora se ha trasladado completamente a EHR, creando una demanda significativa de seguridad de la información dentro de la industria de la salud.



2000—*Virus ILOVEYOU*: El 5 de mayo del 2000, este virus fue liberado por un estudiante en Filipinas.

253 Robert Morris (cryptographer), https://en.wikipedia.org/wiki/Robert_Morris_(cryptographer) (consultado en mayo del 2024). En español: Robert Morris (criptógrafo) https://es.wikipedia.org/wiki/Robert_Morris_(cript%C3%B3grafo) (consultado en mayo del 2024).

254 Para conocer otro relato muy interesante sobre Bob Morris, lea el libro increíblemente divertido de Cliff Stoll, "The Cuckoo's Egg", ISBN 0671726889.

255 Por ejemplo, Dan Geer (director de seguridad de la información de In-Q-Tel, la rama de capital de riesgo de la CIA) se refirió a esto en su charla en la reunión de la AISS en Tampa, en diciembre del 2011.

El virus eliminaba las imágenes en las computadoras infectadas y se enviaba automáticamente como un archivo adjunto de correo electrónico a todos los contactos de Outlook de las computadoras infectadas. Este virus contagió millones de computadoras en todo el mundo y causó daños por miles de millones de dólares. Los creadores del virus, Reomel Ramores y Onel de Guzmán, fueron localizados pocas horas después de la liberación del virus. Sin embargo, los investigadores se dieron cuenta muy rápidamente de que Filipinas no tenía ninguna ley contra la creación de virus informáticos y tuvieron que retirar todos los cargos contra los estudiantes.[256] Este incidente llevó a la comprensión de que la seguridad de la información era un fenómeno global y provocó un impulso por parte de los países desarrollados para alentar a los países en desarrollo a modernizar sus leyes de seguridad de la información. Sin embargo, aún hoy existen diferencias significativas entre los países en cuanto a las leyes de seguridad de la información. Por ejemplo, mientras que crear un virus puede conllevar multas de hasta 250.000 dólares y 10 años de prisión en Estados Unidos, el castigo en Filipinas puede oscilar entre 100.000 pesos (unos 2.500 dólares) y una cantidad proporcional al daño y hasta tres años de prisión. Estas diferencias internacionales son un desafío constante para la ciberseguridad en sociedades dependientes de la tecnología.

2002—*Ley Sarbanes-Oxley*: Durante el período del 2000–2002, Estados Unidos fue testigo de muchos incidentes desagradables de fraude corporativo que involucraron a empresas tan legendarias como Enron, Tyco y WorldCom. Por ejemplo, Enron declaró ingresos de más de 100 mil millones de dólares en el 2000 y se declaró en quiebra el año siguiente. MCI-WorldCom reveló en 2002 que había exagerado sus ganancias en más de 72 mil millones de dólares de los últimos cinco trimestres. Estos fraudes fueron posibles gracias a la manipulación fraudulenta de los sistemas contables, que, se especula, fue a instancias del liderazgo de las firmas. Sin embargo, durante los juicios, los directores ejecutivos intentaron sistemáticamente escapar de la culpa alegando ignorancia de los procedimientos contables y afirmando que confiaban ciegamente en sus subalternos bien pagados y con alto nivel educativo. Dado que las jubilaciones de la mayoría de los estadounidenses se invierten en grandes empresas que cotizan en bolsa, su caída en valor afecta a muchas familias estadounidenses. Obligó al gobierno a actuar ante estos devastadores fraudes corporativos y a garantizar la exactitud de los informes financieros, el Congreso promulgó la Ley Sarbanes-Oxley en el 2002. La ley se centró en responsabilizar personalmente a los ejecutivos clave de la exactitud de los informes financieros presentados por las empresas que cotizan en bolsa. La ley tiene tres disposiciones principales. El artículo 302 exige que el Director ejecutivo y el Director financiero de las empresas firmen una declaración de conocimiento personal de toda la información en los reportes anuales. El artículo 906 impone sanciones penales que incluyen penas de prisión de hasta 20 años por certificación incorrecta. El artículo 404 requiere que la certificación del artículo 302 se base en controles internos formales. El artículo 404 ha tenido un gran impacto en la profesión de seguridad de la información porque exige a las empresas que cotizan en la bolsa establecer procesos formales de seguridad de la información. Esto ha llevado a importantes inversiones en controles internos sobre la información financiera en empresas que cotizan en la bolsa y al correspondiente crecimiento en la demanda de profesionales de ciberseguridad.

2005–2007—*Ataques a minoristas*: en diciembre del 2006, T.J.Maxx informó que sus sistemas informáticos, que procesaban pagos con tarjeta de crédito, habían sido vulnerados. Tras la investigación, se descubrió que la violación había comenzado en julio del 2005, un año y medio antes de su descubrimiento, y que se habían robado más de 45 millones de números de tarjetas de

256 Arnold, W. "TECHNOLOGY: Philippines to drop charges on e-mail virus", New York Times, agosto 22, 2000.

crédito y débito. Resultó que el líder del grupo involucrado en la violación era Albert González,[257] un informante del Servicio Secreto de Estados Unidos y, de hecho, González estaba cooperando con el Servicio Secreto en relación con otro caso en el momento de estos ataques. Las investigaciones también revelaron que el grupo además había pirateado los sistemas de otros minoristas como BJ's Wholesale Club, DSW, Office Max, Boston Market, Barnes & Noble y Sports Authority. El *modus operandi* del grupo era conducir por la Ruta 1 de los Estados Unidos en Miami y buscar una tienda con redes inalámbricas desprotegidas para ingresar a las redes corporativas. Posteriormente, el grupo mejoró su metodología y utilizó ataques de inyección SQL para ingresar a las redes de Hannaford Brothers y Heartland Payment Systems, una empresa de procesamiento de pagos con tarjetas de crédito. Se estima que se robaron más de 125 millones de números de tarjetas de crédito de Heartland y la empresa estimó los daños en más de 12 millones de dólares. En marzo del 2010, Albert González fue condenado a 20 años de prisión. También se le confiscó más de 1,65 millones de dólares que había ganado vendiendo tarjetas de crédito falsas basadas en la información robada. Estos incidentes pusieron de relieve que incluso las grandes empresas tenían evidentes deficiencias en la seguridad de la información que podían provocar graves situaciones embarazosas y pérdidas. Los ataques de inyección SQL, en particular, crearon conciencia de la necesidad de prestar atención a la seguridad de la información durante el desarrollo de software e introdujeron el término "SDLC seguro" en el léxico de TI.

2008—*Ataques de denegación de servicio en Georgia*: Coincidiendo con la guerra militar entre Georgia y Rusia en 2008, Georgia fue víctima de masivos ataques de denegación de servicios de distribución. Los ataques dañaron los sitios web de muchos medios y organizaciones gubernamentales, limitando su capacidad de comunicar sus puntos de vista sobre la guerra a sus ciudadanos. Muchos expertos creen que los ciberataques fueron provocados por Rusia como parte de una estrategia de guerra. De ser así, estos fueron los primeros incidentes conocidos de ataques cibernéticos utilizados como instrumento de guerra.

Junio del 2009—*Establecimiento del Comando Cibernético de EE. UU.*: En abril del 2009, el *Wall Street Journal* informó que unos intrusos habían irrumpido en las redes informáticas de los contratistas de defensa que desarrollaban el Joint Strike Fighter, también llamado F-35 Lightning II. El proyecto de 300.000 millones de dólares fue el programa de armas más costoso realizado por el Departamento de Defensa y utilizó 7,5 millones de líneas de código informático. Los intrusos habían robado terabytes de datos relacionados con el diseño y la electrónica del avión. Se cree que el robo ayudaría a los enemigos a planificar sus defensas contra el avión. Los contratistas involucrados en el proyecto eran Lockheed Martin, Northrop Grumman y BAE Systems. Además, en abril el *Wall Street Journal* informó que la red eléctrica estadounidense había sido penetrada por espías de China, Rusia y otros países. Los espías también insertaron software informático en la red que podría usarse para causar daños por control

257 La revista New York Times publicó un perfil detallado de Albert Gonzales, destacando el lado intensamente personal de la ciberseguridad. James Verini, The Great Cyberheist, revista The New York Times, 10 de noviembre del 2010, accesible en https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html (consultado en mayo del 2024).

remoto.[258] Poco después, el 23 de junio del 2009, se creó el Comando Cibernético de EE. UU. para defender las redes informáticas militares estadounidenses contra ataques de adversarios. El Comando Cibernético de EE. UU. también es responsable de responder en el ciberespacio según sea necesario.

2010—*Operación Aurora y Google-China*: El 12 de enero del 2010, una publicación en el blog del Director Legal de Google informó que Google había detectado un intento, procedente de China, de robar su propiedad intelectual. Los ataques también tenían como objetivo acceder a los correos electrónicos de activistas chinos de derechos humanos. El gobierno de Estados Unidos pronto le prestó atención al incidente y el Congreso anunció su intención de investigar las acusaciones. El Secretario de Estado comparó la censura china de la Internet con el Muro de Berlín de la era de la información. Investigaciones adicionales rastrearon los ataques hasta dos instituciones educativas en China: la Universidad Jiaotong de Shanghai y la Escuela Vocacional Lanxiang. Jiaotong es sede de uno de los programas de informática de élite de China, y Lanxiang participa en la formación de científicos informáticos para el ejército chino.[259] China, sin embargo, ha negado la participación formal del gobierno y ha calificado los ataques simplemente como un intento de los estudiantes de perfeccionar sus habilidades informáticas. Este fue uno de los primeros incidentes de ciberseguridad presuntamente patrocinados por un estado.

17 de abril del 2011—*Sony PlayStation Network (PSN)*: Justo antes de las vacaciones de verano del 2011, Sony anunció que una intrusión externa había comprometido su servicio PlayStation Network y Qriocity, y que los piratas informáticos habían obtenido información personal de los 70 millones de suscriptores de la red. En respuesta, la empresa desconectó la red mientras intentaba garantizar que todos los rastros del software infractor se hubieran eliminado de la red. Durante ese tiempo, millones de niños de todo el mundo que habían planeado sus vacaciones de verano para ponerse al día con los juegos en línea en PSN tuvieron que encontrar formas alternativas de pasar el tiempo. Si bien la intrusión afectó a una red relativamente inocua, el impacto en las familias de todo el mundo fue enorme y casi todas las familias con niños siguieron los acontecimientos diarios en torno a los ataques. Imagínate perder todas las vacaciones de verano debido a un incidente de ciberseguridad. En realidad, esto de verdad pasó en el verano del 2011.

1 de febrero del 2013 —*Informe Mandiant APT 1*:[260] La empresa de ciberseguridad Mandiant publicó un informe alegando que una unidad militar china sospechosa, 61398, estaba involucrada en una forma novedosa de ataque de ciberseguridad patrocinado por el estado: una amenaza persistente avanzada que sucede cuando un adversario sofisticado y con muchos recursos utiliza múltiples métodos de ataque durante un período prolongado para lograr sus objetivos. Mandiant llamó a este adversario APT1. El informe atrajo considerable atención entre los líderes empresariales y gubernamentales que se dieron cuenta de que los ciberataques ya no se limitaban a individuos para obtener beneficios

258 Gorman, S. "Electricity grid in US penetrated by spies", Wall Street Journal, 8 de abril del 2009

259 Markoff, J. and Barboza, D. "2 China schools said to be tied to online attacks", New York Times, 18 de febrero del 2010, http://www.nytimes.com/2010/02/19/technology/19china.html (consultado en mayo del 2024).

260 Mandiant, "APT1, Exposing One of China's Cyber Espionage Units", https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf (consultado en mayo del 2024).

privados. Las preocupaciones aumentaron cuando las organizaciones se dieron cuenta de que los estados podían invertir recursos a escala militar para comprometer la ciberseguridad.

2014—*Ciberataque a Yahoo*: 500 millones de cuentas fueron robadas[261] por lo que se creía que el responsable era un actor patrocinado por un estado. Ciberdelincuentes contratados por agentes rusos robaron direcciones de correo electrónico, contraseñas, números de teléfono, fechas de nacimiento y nombres y atacaron a los empleados de Yahoo mediante un ataque de fraude electrónico (phishing). El phishing es una forma de ingeniería social. En este caso, un empleado de Yahoo con acceso a la red hizo clic en un enlace malicioso en un correo electrónico. Esto permitió a los piratas informáticos obtener acceso continuo a la red para obtener datos confidenciales, como preguntas y respuestas de seguridad, que Yahoo almacenaba sin cifrar. Los ataques de ingeniería social se han vuelto cada vez más sofisticados desde principios de la década del 2000. Este ciberataque a Yahoo es uno de los ataques más importantes registrados hasta la fecha. Hoy, la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) publica consejos de seguridad sobre cómo evitar ataques de ingeniería social y phishing.[262]

2021—*RockYou2021*: En 2021, un jáquer cuya identidad no ha sido revelada recopiló miles de millones de contraseñas de usuarios. Hasta la fecha, esta es la mayor colección de contraseñas jamás filtrada en línea.[263] El jáquer anónimo subió un archivo TXT (texto) de 100 GB a un popular foro de piratas informáticos que contenía aproximadamente 8,4 mil millones de entradas de contraseñas. Algunos dirían que esta cantidad de contraseñas expuestas podría abarcar varias veces a toda la población global en línea. Hoy en día, los investigadores y profesionales de la ciberseguridad suelen utilizar el archivo rockyou.txt como una lista de palabras para estudiar o recrear ataques de fuerza bruta a las contraseñas de los usuarios. Un ataque de fuerza bruta es un guion de programación diseñado para ejecutar repetidamente su código mientras intenta iniciar sesión en un sistema con una cuenta de usuario. Estos tipos de listas de palabras se administran dentro de paquetes de software que se encuentran en las distribuciones de Linux de código abierto actuales, como Kali Linux, que están diseñados para que los profesionales de la ciberseguridad evalúen la seguridad de sus sistemas.[264]

Esta breve cronología destaca cómo los ataques a la seguridad de la información han evolucionado desde pruebas de concepto técnicas hasta ataques con fines comerciales para robar información de tarjetas de crédito. Últimamente incluso se sospecha que los gobiernos persiguen sus agendas a través del delito cibernético. En Europa, una remota ciudad rumana, Râmnicu Vâlcea, se ha convertido en el punto focal del lavado de dinero cibernético global. En medio de la nada, esta ciudad tiene

261 Yahoo dice que los piratas informáticos robaron datos de 500 millones de cuentas en 2014. Se puede leer sobre esto en este artículo de Reuters escrito por Dustin Volz https://www.reuters.com/article/us-yahoo-cyberidUSKCN11S16P (consultado en mayo del 2024).

262 "Avoiding Social Engineering and Phishing Attacks", Security Tip (ST04-014), Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/uscert/ncas/tips/ST04-014 (consultado en mayo del 2024). Información en español en https://www.cisa.gov/sites/default/files/publications/active-shooter-pocket-card-spanish-508.pdf (consultado en mayo del 2024).

263 "RockYou2021: Largest Password Compilation of All Time Leaked Online with 8.4 Billion Entries", cybernews.com, 27 de julio del 2022, https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/ (consultado en mayo del 2024).

264 Kali Linux, website: https://www.kali.org/ (consultado en mayo del 2024).

concesionarios de automóviles que venden Mercedes-Benz y otros coches caros.[265] La respuesta social también ha evolucionado, desde jueces que simplemente aconsejaban a los intrusos y leyes que hacían excepciones específicas para los menores, a pesar de su conocida participación en ciberataques (los 414), hasta gobiernos que establecen comandos militares completos para ocuparse de la ciberseguridad.

El modelo básico de seguridad de la información

La seguridad de la información es un área temática muy amplia porque la mayoría de los incidentes de seguridad de la información explotan alguna debilidad nueva en una organización. Por lo tanto, mantener la seguridad de la información requiere poner atención en casi todos los aspectos de la organización. Para proporcionar estructura a estos esfuerzos, es útil organizar todas las actividades asociadas con el mantenimiento de la seguridad de la información en un modelo unificado. Un modelo se utiliza para representar un concepto que existe en el mundo real. Esto facilita comprender los motivos de los eventos de ciberseguridad. Comencemos examinando el modelo diagramado en la Ilustración 255.

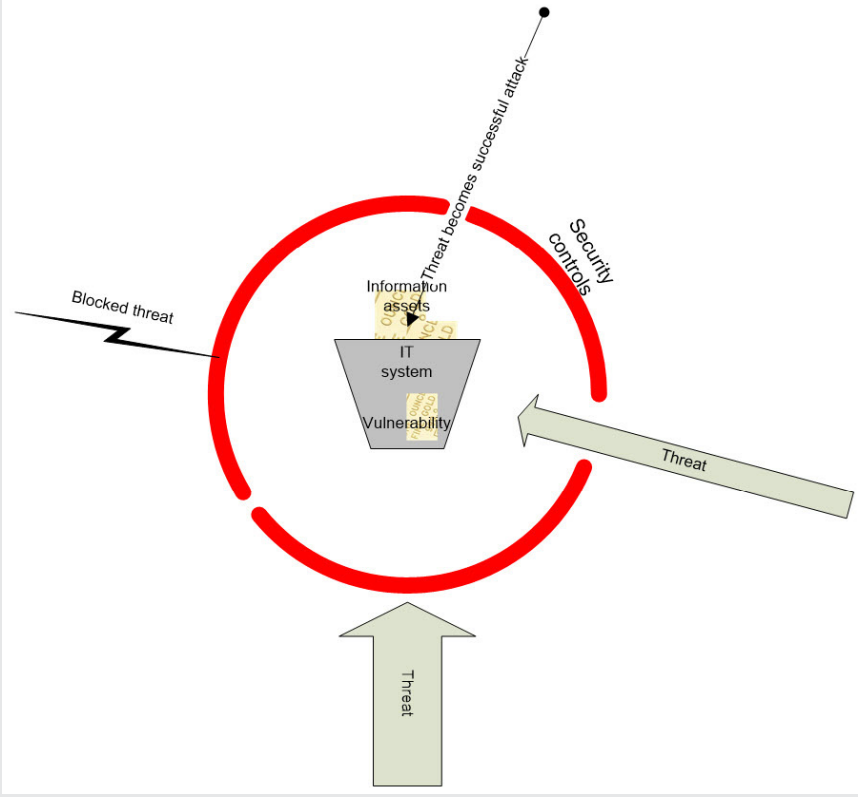


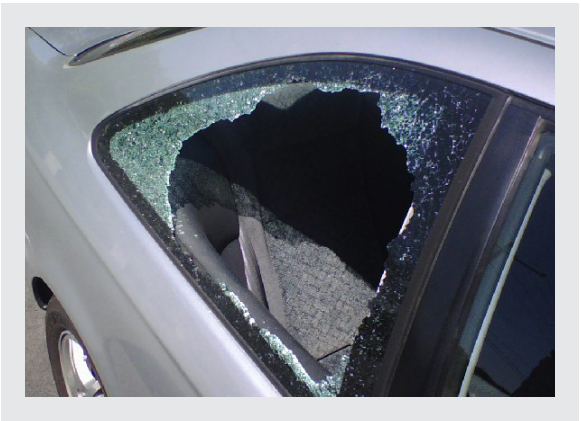
Ilustración 255 — Los sistemas y datos de TI son vulnerables desde múltiples áreas, lo que hace que el monitoreo activo sea crucial para mantener la seguridad.

265 Yudhijit Bhattacharjee, "How a Remote Town in Romania Has Become Cybercrime Central", Wired, 31 de enero del 2011, https://www.wired.com/2011/01/ff-hackerville-romania/ (consultado en mayo del 2024).

La Ilustración 255 representa un marco para comprender la seguridad de la información. Los componentes centrales de este modelo ilustran la relación entre activos, vulnerabilidades, amenazas y controles. Estos cuatro componentes son extremadamente importantes para comprender cualquier evento o caso de ciberseguridad donde la información sea el objetivo.

Activos

Al centro de la Ilustración 255 se encuentran los activos. En el contexto de la seguridad de la información, un *activo se define como un recurso o información que necesita protegerse*. En todos los escenarios de seguridad, ya sea que estén relacionados con la protección de la información o simplemente con la protección de la propiedad personal, comienzan con un activo que se considera suficientemente valioso para tomar las medidas necesarias para protegerlo. La seguridad de la información no es diferente. Si hay cierta información o un recurso relacionado a ella que es valioso para una entidad, entonces, dicha entidad necesita hacer un esfuerzo para asegurarlo.



Sin embargo, hay dos diferencias importantes entre los activos convencionales y los activos de información: invisibilidad y duplicación. En la mayoría de los escenarios de seguridad con los que estés familiarizado, los objetos que deben protegerse se pueden ver y sentir. Por ejemplo, cierras tu auto con llave para evitar hurtos. Instalas un sistema de alarmas para evitar que roben en tu casa. En ambos casos, los activos son visibles a simple vista. Los daños también son visibles. Si alguien fuerza la entrada a tu auto o casa, los daños se ven inmediatamente. Si hay cámaras de circuito cerrado en las proximidades, se va a captar el acto de vandalismo.

Pero la seguridad de la información es diferente. Los activos en la seguridad de la información no son objetos tangibles, que se puedan ver o sentir. Más bien, son datos e información almacenados como ceros y unos en computadoras, cintas, teléfonos y otros dispositivos. Aunque los discos duros y otros dispositivos pueden verse, los valiosos datos que almacenan son invisibles. Si se roban los datos por la red, la transferencia de los datos no se ve en cámaras o aparatos de seguridad convencionales. Los ladrones pueden, incluso, operar desde otro país, a miles de kilómetros de distancia, a salvo del escrutinio de las agencias de seguridad convencionales.

La segunda diferencia importante entre los activos convencionales y los activos de información es la reproducibilidad. Continuemos con el ejemplo del auto; si te roban el auto te vas a dar cuenta de que te falta por la mañana. Esto se debe a que el auto sólo puede existir en un solo lugar en un momento dado; en cambio, la información se puede duplicar. Si te roban tus datos, no lo vas a notar hasta que te lo informen. Por ejemplo, si alguien encuentra tu computadora desatendida, podría enviarse un correo electrónico con una copia de tu tarea y luego entregarla como si fuera suya. Tú no tendrías idea del acto de plagio a menos que tu profesor te lo diga.

Estas dos diferencias entre los tipos de activos (invisibilidad y reproducibilidad), hacen que la seguridad de la información sea un reto mucho más considerable que la seguridad convencional. Los tipos de métodos de la seguridad convencional como cerraduras y guardias no son efectivos para proteger información. Por ejemplo, los cerrojos convencionales no sirven para impedir el robo de

datos por la red. El hurto de un activo convencional como el oro puede solucionarse al recuperar el oro y devolvérselo al dueño, pero los datos hurtados en red pueden copiarse en cientos de ubicaciones e inclusive, si pudieran destruirse algunas de las copias sería imposible impedirle el acceso a los datos al ladrón. Por lo tanto, los controles de seguridad de la información deben tratar de prevenir el robo en primer lugar, y detectar y bloquear hurtos a medida que ocurren, a través de un monitoreo constante.

Activos informáticos

En el escenario más común que confrontarás, los activos de información se guardan en un sistema TI. Los sistemas basados en papel simplemente no pueden proveer la densidad de almacenamiento de información que requieren las organizaciones modernas. Un sistema IT se define como *el conjunto de hardware, software y firmware, configurados para procesar, almacenar o enviar información.* En una pequeña empresa, el sistema de IT puede ser tan sencillo como una hoja de cálculo Excel.

Amenazas

Definimos una amenaza como *la capacidad, intención y métodos de ataque de adversarios para explotar o causar daño a los activos.* En el ejemplo de Excel, quizás un trabajador quiera aprovecharse de la falta de protección con contraseña de un archivo para cambiar su salario por hora. La Ilustración 255 muestra este tipo de amenazas con el uso de flechas.

Hoy día es una práctica común entre los profesionales de la ciberseguridad usar el marco de trabajo creado por Mitre, llamado "MITRE ATT&CK".[266] Mitre es una organización de investigación y desarrollo sin fines de lucro financiada con fondos federales. El Marco o Matriz Mitre incluye observaciones del mundo real a través de un inventario de conocimiento accesible globalmente que incluye tácticas y técnicas que usan los cibercriminales para explotar las vulnerabilidades de los sistemas IT. La Matriz Mitre es un gran recurso para lo que conocemos como "inteligencia contra amenazas", que el Instituto Nacional de Estándares y Tecnología o NIST (siglas en inglés para National Institute of Standards and Technology) define como: "Información sobre amenazas que se ha agregado, transformado, analizado, interpretado o enriquecido para proveer el contexto necesario en procesos de toma de decisiones".[267]

Es decir, existen recursos, públicos y privados, de inteligencia contra amenazas para profesionales de la ciberseguridad con una recopilación de información para entender las amenazas globales que buscan explotar la vulnerabilidad de los activos del sistema TI. Por ejemplo, la Ilustración 251 muestra un reporte de inteligencia de amenazas publicado por la base de conocimientos MITRE ATT&CK que

266 Página de inicio de MITRE ATT&CK, https://attack.mitre.org/ (consultado en mayo del 2024).

267 NIST, Computer Security Resource Center, https://csrc.nist.gov/glossary (consultado en mayo del 2024)

advierte de tres amenazas (Axiom, GOLD SOUTHFIELD y Hikit) que se han utilizado en campañas de fraude electrónico para obtener acceso a los sistemas IT de las víctimas.[268]

ID	Name	Description
G0001	Axiom	Axiom has used spear phishing to initially compromise victims.[1][2]
G0115	GOLD SOUTHFIELD	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines.[3]
S0009	Hikit	Hikit has been spread through spear phishing.[2]

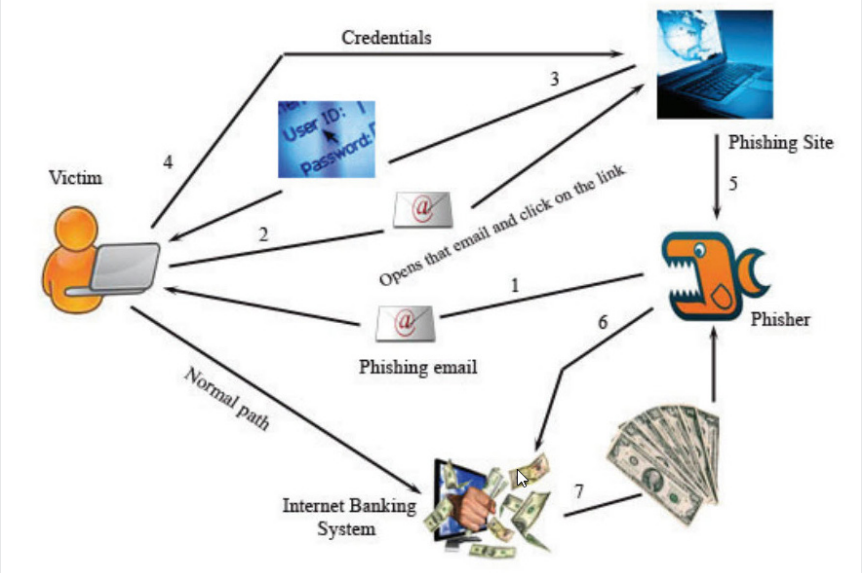
Ilustración 256 — Recursos de inteligencia de amenazas les facilitan a los analistas la tarea de referencia e identificación de ataques maliciosos.

Como puede apreciarse en la Ilustración 256, Axiom es un presunto grupo chino de ciber espionaje, mientras que GOLD SOUTHFIELD es un grupo motivado por el lucro. Ambos grupos se consideran amenazas globales a la ciberseguridad. El tercer nombre incluido en la ilustración es Hikit, un programa malicioso (*malware*) que puede conectarse remotamente a un sistema IT para crear amenazas persistentes, las cuales se utilizan para causar daños al sistema IT en cualquier momento que el actor de amenaza lo desee.

Los tipos de amenazas más populares incluyen virus, gusanos informáticos, phishing y programas maliciosos. Los virus y gusanos informáticos son *programas de computadora que dañan las computadoras y se propagan a través de la red sin el consentimiento del usuario*. La diferencia entre un virus y un gusano es que el virus usa otros programas (por ejemplo, el cliente del correo electrónico del usuario) para propagarse, mientras que el gusano se puede propagar por sí solo. Como los autores de gusanos y virus saben que la mayoría de los usuarios utilizan programas antivirus, los gusanos y virus actuales están diseñados para causar el mayor daño posible a pocos minutos de su lanzamiento.

El fraude electrónico o phishing es *un intento de comprometer a un usuario haciéndose pasar por una entidad confiable en una comunicación electrónica*. Los primeros ataques de fraude intentaban adquirir información como nombres de usuarios, contraseñas y datos de tarjetas de crédito. La mayoría de las personas recibe semanalmente al menos uno o dos de estos correos electrónicos que parecen originarse desde bancos y llevan a los usuarios a visitar un sitio web que parece el del banco; una vez allí, se les pide a los usuarios que provean su nombre de usuario y contraseña para corregir alguna información en la cuenta. Aunque los correos electrónicos y el sitio web de destino parecen legítimos, en realidad no lo son. Si nos fijamos cuidadosamente en la URL nos daremos cuenta de que el sitio está alojado en un servidor comprometido.

268 "Phishing, Sub-techniques", T1566, MITRE ATT&CK, https://attack.mitre.org/techniques/T1566/ (consultado en mayo del 2024).



Los usuarios pueden ser fácilmente víctimas de ataques fraudulentos.

Un software malicioso (*malware*) es *un término general para describir software o códigos diseñados específicamente para explotar una computadora o los datos que contiene sin el consentimiento del usuario.* Una forma muy común de un programa malicioso entrar a una computadora es a través de descargas gratuitas donde el autor del malware crea un programa que parece de gran utilidad y que distribuye gratuitamente. Cuando los usuarios desprevenidos descargan e instalan el, aparentemente útil, programa, el programa malicioso se instala con él. Esto se conoce como la Técnica del Caballo de Troya.

Vulnerabilidades

La seguridad de la información es importante porque todos los sistemas tienen vulnerabilidades. Una vulnerabilidad es *una debilidad en un sistema de información que lo hace susceptible de poner en peligro un activo.* En el caso del sistema IT basado en Excel mencionado anteriormente, dichas vulnerabilidades incluyen acceso no autorizado que puede causar pérdida de confidencialidad o integridad y fallos del disco duro que puede afectar la disponibilidad. Si alguna vez alcanzáramos un tipo de estado utópico donde no hubiera vulnerabilidades en los sistemas IT, no tendríamos que estudiar la seguridad de la información y no habría un grupo de profesionales dedicados a ella. Sin embargo, los productos de software modernos son muy grandes. Por ejemplo, para crear Microsoft Windows se necesitaron millones de líneas de código. Es difícil anticipar y eliminar todas las posibles vulnerabilidades en productos de ese tamaño.

Para enfrentar las vulnerabilidades la industria del software, en colaboración con el gobierno federal se han invertido recursos considerables para crea un inventario de vulnerabilidades de software conocidas, la lista de Vulnerabilidades y exposiciones comunes (CVE, siglas en inglés para Common Vulnerabilities and Exposures).[269] El propósito de la lista CVE es proporcionar nombres comunes e

269 Para acceso a la lista, ir a https://cve.mitre.org/ (consultado en mayo del 2024).

identificadores para todas las vulnerabilidades de software públicamente conocidas. Mitre también mantiene esta lista.

Las vulnerabilidades pueden clasificarse en categorías especializadas tales como vulnerabilidades del software. Una vulnerabilidad de software es *un error en la especificación, desarrollo o configuración del software en la que su ejecución puede violar la política de seguridad.*[270] Por ejemplo, un programador de software podría crear un sitio web que requiera la información del usuario en un cuadro de texto antes de enviar un formulario. Sin embargo, si el programador no escribe el código para validar la entrada del usuario en el formulario en la red es posible que un pirata informático inyecte Lenguaje de Consulta Estructurado (SQL siglas en inglés para Structure Query Language) en el cuadro de texto cuando se envíe el formulario. A este tipo de ataque se le conoce como Inyección SQL.

La Ilustración 257 muestra un intento de Inyección SQL en ChatGPT.[271] ChatGPT es un sitio web gratuito de Inteligencia artificial (IA) de OpenAI que le permite al usuario escribir dentro de un cuadro de texto. Luego, ChatGPT analiza el texto y trata de responderlo usando IA, de manera similar a como un ser humano contestaría una consulta verbal. Aquí, como se aprecia en la Ilustración 257, el usuario trata de inyectar SQL malicioso y ChatGPT no permite que el código se ejecute. Esto ilustra cómo los programadores de ChatGPT han escrito código que valida la entrada del usuario para impedir cualquier vulnerabilidad de software del sistema IT.

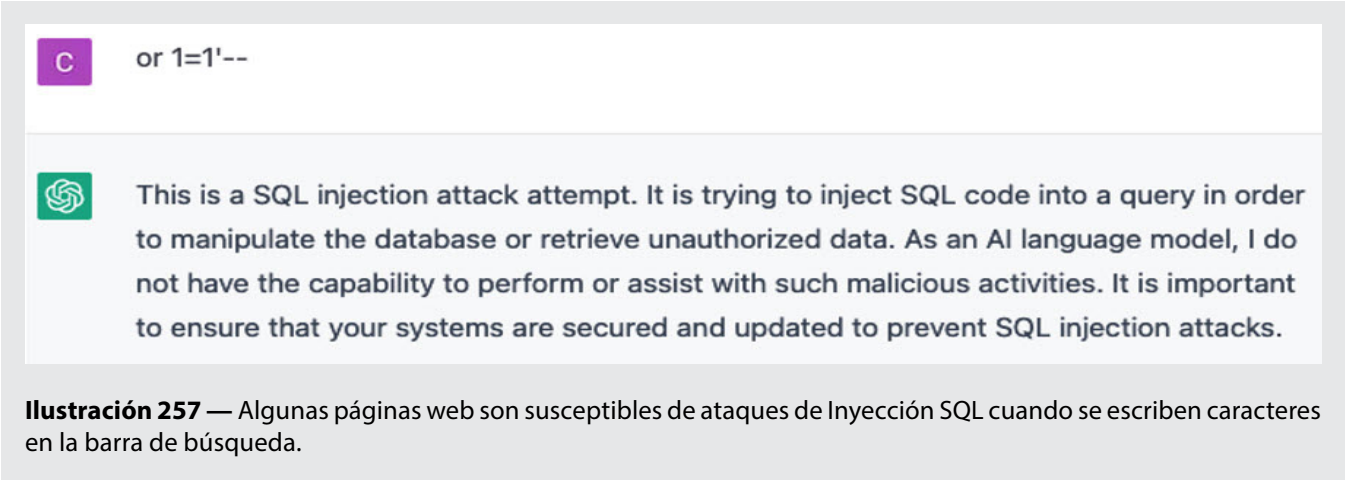


Ilustración 257 — Algunas páginas web son susceptibles de ataques de Inyección SQL cuando se escriben caracteres en la barra de búsqueda.

Controles

En un futuro próximo todos los sistemas IT serán vulnerables. Además, habrá atacantes, concentrados en explotar vulnerabilidades para lucro personal u otros motivos. ¿Qué puede hacer un administrador de sistema para defender las computadoras a su cargo?

El papel de la seguridad de la información es minimizar el impacto de las amenazas implementando controles de seguridad alrededor de sistemas IT vulnerables. Los controles de seguridad son *salvaguardas que se usan para minimizar el impacto de amenazas.* Dentro del marco de trabajo que aparece en la Ilustración 255, estos controles se representan como un anillo alrededor del sistema IT. El ancho de las flechas en la Ilustración indica la relativa frecuencia de las diferentes categorías

270 Krsul, I. "Software vulnerability analysis", disertación doctoral sin publicar, Purdue University, 1988.

271 ChatGPT por OpenAI, https://openai.com/blog/chatgpt/ (consultado en mayo del 2024).

de amenazas desde la perspectiva de una organización típica. La mayoría de las amenazas son bloqueadas por los controles que comúnmente emplean las organizaciones. Por ejemplo, la mayoría de los sistemas operativos ahora traen un cortafuegos con algunas configuraciones predeterminadas y animan a los usuarios a usar una contraseña fuerte para proteger la cuenta de usuario administrativo en sus computadoras. En el ámbito comercial, aún las empresas más pequeñas hacen copias de seguridad de sus archivos más importantes en dispositivos de almacenamiento externos o en otros servicios de Internet y mantienen sus computadoras bloqueadas para impedir el acceso no autorizado.

Inclusive, los controles rudimentarios como cortafuegos y contraseñas pueden bloquear exitosamente una gran mayoría de amenazas que enfrentan las organizaciones. Sin embargo, como se muestra en la Ilustración 255, aún los mejores controles de seguridad tienen agujeros. Por ejemplo, a menudo los usuarios prefieren contraseñas fáciles de recordar en lugar de contraseñas seguras; también tienden a no realizar copias de seguridad de sus datos regularmente, aun cuando han gastado cientos o miles de dólares en sistemas de copias de seguridad. Las amenazas explotan estas debilidades en los controles de seguridad para alcanzar los sistemas IT vulnerables. En la Ilustración 255, las amenazas están representadas por la flecha a la derecha, la cual ha atravesado los controles y llegado hasta el sistema IT. Afortunadamente, es posible que muchas de estas amenazas no hagan daño, según muestra el fracaso de la flecha de abajo de alcanzar el sistema IT.

Los controles de ciberseguridad pueden clasificarse en físicos, técnicos y de procedimiento. Los controles físicos usan métodos tradicionales no-técnicos para prevenir daños. Normalmente, impiden el acceso a las instalaciones técnicas a usuarios no autorizados. Algunos ejemplos son cerraduras, extinguidores de fuego, averiguación de antecedentes y puertas. Los controles técnicos son medidas de seguridad integradas en el propio sistema informático. Los ejemplos más comunes incluyen contraseñas, cortafuegos, sistemas de detección de intrusos, actualizaciones de sistemas y programas antivirus. Los controles de procedimiento son planes de acción prescritos que regulan el uso de los recursos informáticos. Algunos ejemplos incluyen procedimientos para: adquisición de cuentas de usuario, escalada de privilegios, modificación de programas, contrataciones y requisitos de que los usuarios cambien sus contraseñas periódicamente.

Ciberhigiene

La Agencia de seguridad de infraestructura y ciberseguridad de EE. UU. (CISA, siglas en inglés de Cybersecurity & Infrastructure Security Agency), define la ciberhigiene como aquellas prácticas que reducen el riesgo de un ciberataque exitoso.[272] Hoy día es importante que las personas entiendan cómo mantener buenas prácticas de ciberhigiene para la utilización segura de los sistemas y recursos informáticos en línea. Algunas prácticas intuitivas de ciberhigiene incluyen medidas sencillas de actualizar la seguridad de los dispositivos técnicos. Por ejemplo, si tu dispositivo móvil tiene actualizaciones de su software, normalmente te envía un mensaje de alerta a la pantalla. El usuario del dispositivo móvil puede optar por ignorar las actualizaciones o dedicar tiempo a descargarlas e instalarlas. Mantener el dispositivo móvil al día es una forma excelente de mantener una buena ciberhigiene y prevenir que los cibercriminales causen daño a tu información personal.

272 Cybersecurity & Infrastructure Security Agency (CISA), "Cyber Hygiene Services", https://www.cisa.gov/cyber-hygiene-services (consultado en mayo del 2024); para una hoja suelta con información en español, ver https://www.cisa.gov/sites/default/files/publications/SPANISH-4_Things_You_Can_Do_To_Keep_Yourself_Cyber_Safe_508c.pdf (consultado en mayo del 2024)

Otros tipos de buena práctica de ciber higiene son el uso de software de protección de terminales (anteriormente llamado antivirus), y el cambio de la contraseña con regularidad. Los programas de antivirus como McAfee[273] están diseñados para proteger tu identidad, privacidad y dispositivos a través de productos diseñados para monitorear virus conocidos y otras tecnologías maliciosas en tus dispositivos.

El control de las contraseñas es uno de los medios más efectivos de practicar una buena ciberhigiene. Para mantener las contraseñas seguras se debe:

- evitar el uso de la misma contraseña para múltiples cuentas;
- cambiar las contraseñas regularmente;
- tener contraseñas de más de 12 caracteres;
- incluir una combinación de letras mayúsculas y minúsculas, además de símbolos y números;
- evitar contraseñas obvias, como números secuenciales (1234) o información personal que se pueda obtener en las cuentas de redes sociales como el nombre de una mascota o tu primer auto;
- evitar compartir las contraseñas con otras personas;
- usar un administrador de contraseñas que ayude a generar, almacenar y manejar todas las contraseñas en una sola cuenta de seguridad en línea, por ejemplo: 1Password, https://1password.com/;
- usar aplicaciones que requieran autenticación multifactorial, por ejemplo, muchas cuentas de redes sociales requieren para entrar un nombre de usuario/contraseña y además envían un código como mensaje de texto al teléfono celular para completar el proceso de iniciar la sesión;
- hacer copias de seguridad de los archivos importantes en un lugar seguro y protegido, por ejemplo, un disco duro externo o un almacén en la nube;
- no publicar información privada como la dirección doméstica o el número de teléfono en las cuentas de redes sociales;
- revisar las configuraciones de privacidad de cada una de tus redes sociales porque cada cuenta de red social es diferente y está diseñada para proteger a los usuarios cuando se usan adecuadamente las configuraciones;
- mantener los dispositivos bloqueados con una contraseña o PIN cuando no se usen;
- no utilizar sitios web o aplicaciones que divulgan información privada en un Wi-Fi público;
- hacer transacciones únicamente en sitios web que son seguros (que requieren un URL con https:// en lugar de simplemente http://);
- cambiar el nombre predeterminado del enrutador de Wi-Fi de tu casa —en otras palabras, no dejar el enrutador con el nombre que le dio el fabricante cuando lo sacaste de la caja

273 McAfee, https://www.mcafee.com/ (consultado en mayo del 2024)

- configurar una red para quienes te visitan para que la usen en lugar de la de tu uso personal;
- usar cortafuegos para prevenir que un software malicioso acceda a la red de tu casa;
- encriptar los dispositivos que contengan datos confidenciales, por ejemplo, dispositivos USB removibles; y
- borrar completamente el disco duro antes de venderlo o desecharlo.

En resumen, las personas son por lo general, el eslabón más débil para un ciberataque, muchos de los cuales están diseñados para explotar las vulnerabilidades de las personas debido a sus prácticas pobres de ciberhigiene. Por ejemplo, los actores de amenaza usan técnicas de ciberataques como la ingeniería social para hacer que las personas revelen información específica que, de otro modo, no compartirían. Dicha información, que ha sido expuesta por la pobre higiene cibernética, puede utilizarse para robo de identidad o robo bancario. Por lo tanto, a medida que la tecnología evoluciona continuará también la necesidad de que el público general se mantenga informado acerca de las mejores prácticas de una buena higiene cibernética.

Equipos en ciberseguridad

Los profesionales que trabajan en seguridad cibernética a menudo trabajan en equipo para responder o investigar un incidente de ciberseguridad, y deben de estar familiarizados con las tácticas, técnicas y procedimientos (TTP) que usan los actores de amenazas en un incidente de ciberseguridad. Mientras que una táctica se puede describir como el método básico que usa un jáquer para tener acceso a un sistema o información, una técnica se refiere a las herramientas o métodos que utiliza. Finalmente, el procedimiento se refiere a cómo el pirata informático lleva a cabo las técnicas, paso por paso.

Los equipos de ciberseguridad deben estar familiarizados con los TTP conocidos por la inteligencia de la comunidad de ciberseguridad para entender el comportamiento de un jáquer, porque es el conocimiento necesario para proteger mejor las compañías y los sistemas de ser atacados. El marco MITRE ATT&CK es uno de los repositorios de código abierto del conocimiento TTP más grandes del mundo. Los equipos de ciberseguridad lo pueden utilizar para ayudar a hacer del mundo un lugar más seguro para vivir.

Aunque las personas suelen llamar a los actores de amenazas un jáquer malicioso, no todos los jáqueres son malos. Los equipos de ciberseguridad han evolucionado con el tiempo para especializarse en diferentes áreas del comportamiento de los jáqueres. De hecho, los miembros de estos equipos especializados podrían ellos mismos considerarse jáqueres.

Esencialmente, los jáqueres se clasifican según la intención de sus acciones. Sea que sus intenciones son buenas o malas, los equipos de ciberseguridad deben de entender todos los tipos de comportamiento de un jáquer.

A continuación, se resumen los dos tipos comunes de equipos especializados en TTP que se usan en un incidente de ciberseguridad:

> **Equipo rojo:** Consiste en operadores que usan herramientas y técnicas típicamente utilizadas por actores de amenazas para atacar un sistema o su información. Si fuera un deporte, podríamos pensar que el Equipo rojo es la "ofensiva". Los ataques de ciberseguridad que ejecuta el Equipo rojo se conocen como campañas. El propósito del operador de un Equipo rojo (jáquer) es

ayudar a las compañías a entender cómo un actor de amenazas puede explotar las debilidades (vulnerabilidades) de su seguridad, para ayudar a que las compañías mejoren sus prácticas comerciales y tecnológicas y así proteger mejor sus sistemas de futuros ataques.

Equipo azul: Se enfoca en la defensa constante de sistemas e información manejada por las organizaciones. Es común que las empresas trabajen con Centros de operaciones de seguridad (SOC, siglas en inglés de Security Operation Centers), que consisten en múltiples Equipos azules dedicados a vigilar de cerca todos los sistemas importantes para realizar sus operaciones comerciales diarias. Los Equipos azules están capacitados para utilizar herramientas diseñadas para proteger, capturar, analizar y responder a un incidente de ciberseguridad. Por ejemplo, en caso de que el sistema de una compañía sea atacado por un actor de amenazas o por *malware* el Equipo azul investiga lo sucedido. Una vez que entienden el mecanismo, recomiendan una respuesta mitigadora para evitar que se repita la situación.

En resumen, se puede considerar a la ciberseguridad como un "deporte de equipo", porque requiere que se trabaje en equipo para entender infinitamente la ofensiva y defensiva de los TTP que usan los jáqueres en todo el mundo. A fin de cuentas, a estos jáqueres buenos los motiva la pasión de prevenir que los jáqueres malos hagan daño a la seguridad de la información y a la gestión de sistemas importantes.

Términos y definiciones del capítulo

Activos (*Assets*): Información o recursos que deben ser protegidos.

Actor de amenaza (*Malicious Actor*): Alguien o algo que causa daño en el ámbito digital.

Amenazas (*Threats*): Capacidades, intenciones y métodos de ataque de los adversarios para explotar o causar daño a los activos.

Ataques de denegación de servicio (DoS) (*Denial of Service Attacks*): Actos donde más de una computadora en red abruman una red con tráfico fraudulento.

Ataques de fuerza bruta (*Brute Force Attacks*): Guiones de programación diseñados para ejecutar repetidamente sus códigos mientras se intenta iniciar sesión en un sistema con una cuenta de usuario.

Ciberhigiene (*Cyber Hygiene*): Prácticas que reducen el riesgo de un ciberataque exitoso.

Ciberseguridad (*Cybersecurity*): Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicos, servicios de comunicaciones electrónicos, comunicaciones por cable y comunicaciones electrónicas—incluyendo la información contenida en ellos—para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no rechazo.

Controles (*Controls*): Medidas de seguridad utilizadas para minimizar el impacto de las amenazas.

Gusano (*Worm*): Programa de computadora que puede propagarse por sí mismo y afectar negativamente a las computadoras, extendiéndose a través de la red sin el consentimiento del usuario.

Ingeniería social (*Social Engineering*): Utilización del engaño para hacer que una persona revele información privada o proporcione acceso no autorizado a un sistema informático o red.

Jáquer (*Hacker*): Persona que desea obtener acceso a un objetivo identificado para conocer más sobre él y explotarlo con fines de ataque.

Phishing (*Phishing*): Intento de comprometer a un usuario haciéndose pasar por una entidad confiable en comunicaciones electrónicas.

Seguridad de la información (*Information Security*): Proteger la información y los sistemas de información contra el acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción, con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

Tríada CIA (*CIA Triad*): Provisión de confidencialidad, integridad y disponibilidad, al proteger la información y los sistemas de información contra el acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción.

Virus (*Virus*): Programa de computadora que utiliza otros programas para propagarse y afectar negativamente a las computadoras, reproduciendo a través de la red sin el consentimiento de los usuarios.

Vulnerabilidad (*Vulnerability*): Debilidad en un sistema de información que contribuye a una amenaza con la oportunidad de poner en peligro un activo.

Caso del capítulo

Los operadores del Equipo rojo

Según NIST un "Equipo rojo" es un grupo de personas autorizadas y organizadas para imitar las capacidades de ataque o explotación de un potencial adversario contra la postura de seguridad de una empresa. El objetivo del Equipo rojo (también conocido en inglés como Cyber Red Team)[274] es mejorar la ciberseguridad empresarial demostrando los impactos de posibles ataques y señalando qué estrategias funcionan para los defensores (es decir, el Equipo azul) en un entorno operativo. En la ilustración que sigue, dos operadores del Equipo rojo tratan de explotar cualquier vulnerabilidad del Departamento de Recursos Humanos de Widget Inc. (HR siglas en inglés de Human Resources)

Damian Hatter, operador número 1 del Equipo Rojo, pasó de largo del Departamento de Recursos humanos de Widget Inc., miró por varias ventanas y se fijó en la disposición general de la habitación antes de entrar. Notó que solo había un recepcionista sentado ante un escritorio y que había varias estaciones de trabajo en el salón protegidas por las paredes de los cubículos. Hatter entró a la oficina, se le acercó al recepcionista y le preguntó si podía llenar una solicitud de empleo. El recepcionista le pidió que se sentara en una de las estaciones de trabajo y que hiciera clic en el ícono de acceso directo en la PC de escritorio para comenzar el proceso de solicitud. Hatter siguió las instrucciones y se sentó en una de las estaciones mientras el recepcionista se quedó en su puesto.

Tras sentarse en la estación, Hatter comenzó a buscar las vulnerabilidades de la PC. Su meta principal era implantar una puerta trasera[275] y mantener la persistencia de la red[276] a través de un servidor de Comando y control remoto (C2).[277] Para lograrlo,

274 National Institute of Standards and Technology (NIST), Computer Security Resource Center, "Red Team", https://csrc.nist.gov/glossary/term/red_team (consultado en mayo del 2024).

275 "Backdoor (computing)", TechTarget, August 2017, https://www.techtarget.com/searchsecurity/ definition/back-door?Offer=abMeterCharCount_var3 (Consultado en mayo del 2024). Para información en español sobre puertas traseras en informática ver https://masterenciberseguridadonline.es/internet/que-es-una-puerta-trasera-en-informatica/ (consultado en mayo del 2024).

276 Maloney, Sarah, "What Is an Advanced Persistent Threat (APT)?" Cybereason, 1/9/2018, https://www.cybereason.com/blog/advanced-persistent-threat-apt (Consultado en junio del 2023). Para una definición en español, leer https://es.wikipedia.org/wiki/Amenaza_persistente_avanzada (consultado en mayo del 2024)

277 "Command and Control Server", TechTarget, January 2017, https://whatis.techtarget.com/definition/command-and-control-server-CC-server (consultado en mayo del 2024). En español, ver https://es.linkedin.com/pulse/red-teaming-instalaci%C3%B3n-de-un-servidor-comando-y-control-fonsal%C3%ADa-9u43f (consultado en mayo del 2024).

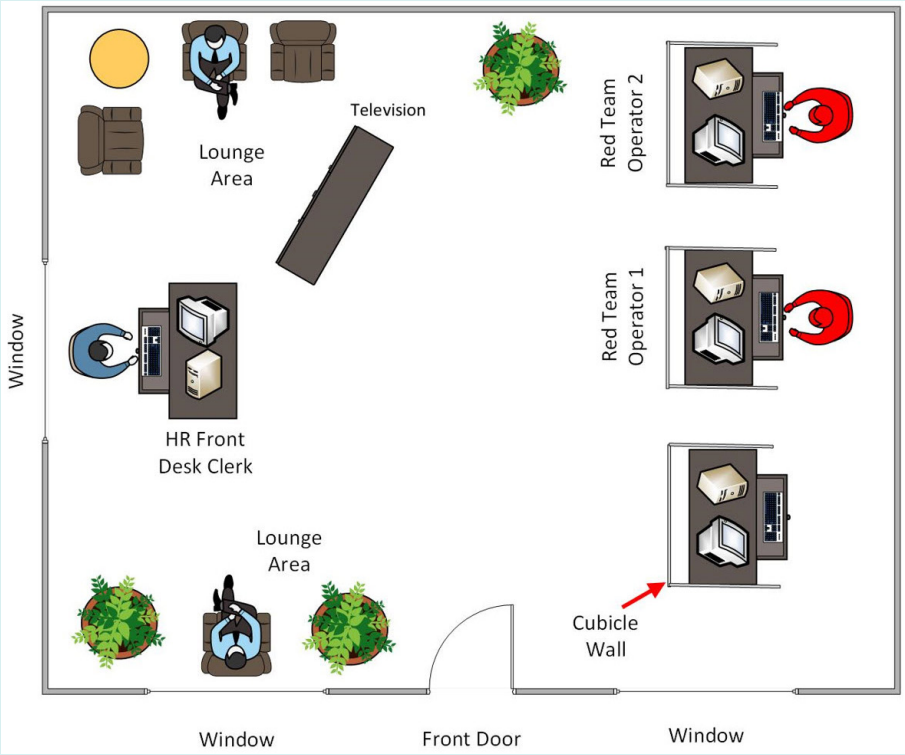
Caso del capítulo (continuado)

comenzó por verificar que pudiera usar uno de los puertos USB abiertos de la PC. Sacó de su bolsillo una unidad flash USB y la insertó en el puerto disponible. El sistema operativo Windows respondió inmediatamente confirmando que el puerto USB estaba habilitado. Tras la confirmación, Hatter abrió su unidad flash y ejecutó un programa malicioso que había instalado anteriormente en su oficina. El programa malicioso en su unidad flash finalmente se comunicó con el C2 de Hatter que operaba desde un sistema remoto localizado fuera de Widget Inc. Su objetivo se cumplió cuando comprobó que su C2 podía comunicarse con el programa malicioso ejecutado desde una PC dentro de la red de Widget Inc. Entonces, Hatter sacó su unidad flash USB, la guardó en su bolsillo y salió de la oficina de Recursos Humanos.

Tan pronto como Hatter salió de la oficina de recursos humanos, Wanna Bee, Operador 2 del Equipo rojo, entró y fue directamente a una estación de trabajo sin consultar con el recepcionista. Apenas se sentó, usó un navegador para ir al sitio web que ya había configurado en un servidor web remoto con el propósito de descargar software malicioso. La configuración de la cuenta de usuario en la PC tenía suficientes privilegios para descargar y ejecutar aplicaciones directamente de la Internet. Tras descargar y ejecutar exitosamente el software malicioso, Bee se pudo comunicar con el sistema C2 remoto.

Hatter y Bee habían conseguido acceso persistente no autorizado a la red de Widget Inc. Lo habían logrado gracias a la explotación de puntos de entrada físicos y técnicos inseguros.

Caso del capítulo (continuado)



Ilustra una operación del equipo rojo en el Departamento de Recursos Humanos de una compañía.

.....

Pregunta 1: ¿Qué vulnerabilidades crees que existen en el Departamento de Recursos Humanos?

Pregunta 2: Identifica todos los controles de ciberseguridad que puedas que deben añadirse al Departamento de Recursos Humanos según este caso. Asegúrate de incluir controles físicos, técnicos y de procedimiento.