La ciberdefensa en los sistemas de información sanitarios militares

García-Córdoba J.[1], Herrero-Pérez L.[2]

Sanid. mil. 2020; 76 (3): 140-142, ISSN: 1887-8571

NO HAY QUE PREGUNTARSE SI OCURRIRÁ, SINO CUÁNDO OCURRIRÁ

A principios de 2019, según diversas informaciones públicas, se detectó un ciberataque contra la red de propósito general del Ministerio de Defensa (WAN PG). Por la complejidad del ataque, una de las posibilidades era que el ataque hubiera sido llevado a cabo por alguna organización o estado extranjero que quisiera robar secretos militares, sin embargo, la red que sufrió dicho ataque no contenía información clasificada. Aparentemente, el método utilizado en ésta ocasión fue mediante la descarga de un malware distribuido a través de correo electrónico en dicha WAN PG, red que cuenta con más de 50.000 usuarios conectando el Ministerio de Defensa con EMAD, Cuarteles Generales de los Ejércitos y Armada así como con todas las Unidades, Centros y Organismos dependientes de ellos y con las distintas Zonas de Operaciones en las que se está presente. El HCD «Gómez Ulla» y su sistema de información «Balmis» también se encuentran dentro de dicha red.

Este tipo de acciones son cada vez más recurrentes debido a su alto rendimiento ya que se puede conseguir un gran beneficio a un muy bajo coste, siendo en muchas ocasiones y para muchos actores la forma más rentable de ataque y, por ello, en el futuro resultará todavía más frecuente que en la actualidad.

EL CIBERESPACIO

El ciberespacio, definido como el dominio global y dinámico compuesto por infraestructuras de tecnología de la información, incluyendo Internet, redes de telecomunicaciones y sistemas de información, se ha consolidado como un entorno de relación cuyo control es prácticamente imposible. Éste control no pasa únicamente por alcanzar una suficiente capacidad de **defensa** en dicho entorno, sino que además es necesario disponer de capacidad de **explotación** para elaborar inteligencia de ciberamenazas, con el fin de obtener información de las Tácticas, Técnicas y Procedimientos (TTP) de las mismas, así como colaborar a la obtención del Orden de Batalla (ORBAT) del adversario y, finalmente, también debe alcanzar una capacidad para poder llevar a cabo acciones **ofensivas** en el ciberespacio ante amenazas o agresiones que puedan afectar al concepto global de seguridad nacional.

[1] Comandante ET. TRA. Jefe CIS del Servicio de Telemedicina HCD «Gómez Ulla». jgarcor@et.mde.es.
[2] Comandante ET. TRA. DIM. Subdirección General de Planificación y Costes de RRHH. Dirección General de Personal. lherper@et.mde.es

Recibido: 18 de agosto de 2020
Aceptado: 23 de septiembre de 2020

doi: 10.4321/S1887-85712020000300001

En las Fuerzas Armadas Españolas estas capacidades se llevan a cabo de la siguiente manera:

- Defensa: Los Ejércitos y la Armada son responsables de sus redes y sistemas específicos y el Mando Conjunto de Ciberdefensa es el responsable de las redes y sistemas conjuntos y corporativos así como de dirigir y coordinar los Centros de Operaciones de Seguridad del Ministerio de Defensa.
- Explotación: Mando Conjunto de Ciberdefensa.
- Ataque: Mando Conjunto de Ciberdefensa.

El ciberespacio se ha convertido en una nueva dimensión del campo de batalla que se verá inundado por las acciones derivadas de los conflictos que el ser humano ha ido teniendo durante siglos y que ahora se extienden a este nuevo escenario. Un conflicto no surge de la nada, ni de un momento a otro, sino que tiene unas causas y evoluciona de manera progresiva desde un estado inicial de paz hasta el de guerra declarada pasando, entre otras, por situaciones intermedias de tensión o crisis.

La denominada como «La Ciberguerra» o «3.ª Guerra Mundial» no será una guerra que se libre exclusivamente en esta nueva dimensión, sino que obedecerá a la progresión típica de un conflicto antes mencionada, y se combinará con otro tipo de acciones, inicialmente en su forma de ciberespionaje, para pasar posteriormente a ciberataques que condicionarán las tácticas que se adopten en el planeamiento conjunto de operaciones convencionales, normalmente en las fases de conflicto armado o de guerra. No obstante, un ciberconflicto o ciberataque se puede originar de forma aislada, sin necesidad de que haya una escalada de violencia.

La pólvora y la dinamita han empezado a perder importancia en la era de Internet, la guerra en el ciberespacio conlleva nuevas estrategias y reglas para la milicia. Ya no es tan importante quién tiene las mejores armas sino quién tiene a los mejores combatientes, los cuales necesitan un nivel de conocimientos y habilidad importante para utilizar toda esa tecnología que no es algo que se pueda lograr de la noche a la mañana. Eso sin tener en cuenta que el ejército debe competir con la industria para reclutar a los mejores.

La ciberamenaza se contempla en la estrategia de seguridad nacional como uno de los riesgos principales a los que hacer frente, estableciendo como primera premisa de desarrollo que la ciberseguridad no es específica de las Fuerzas Armadas, sino que se plantea y converge en una dimensión dual cívico-militar como principales ciberamenazas del siglo XXI (ciberguerra, ciberterrorismo, ciberespionaje, «hacktivismo», cibercrimen, etc.).

La sinergia en las acciones a desarrollar en el campo militar y en el ámbito civil (sector público, privado y los propios ciudadanos, además del sector académico) deben ser la referencia para dictar cualquier guía de desarrollo, tanto a la hora de emprender acciones propias de la ciberdefensa, como a la hora de acometer

estudios en los campos de I+D+i. El desfase tecnológico en uno de los campos, civil o militar, puede suponer una vulnerabilidad hacia el otro, ya que ofrecerá líneas de aproximación al entorno de sistemas desde uno u otro campo, y por tanto, de éxito ante cualquier ciberamenaza.

En el siglo XXI los bits y los bytes podrán ser tan amenazantes como las balas y las bombas.

CIBERATAQUES

Puesto que no todos los ciberincidentes poseen las mismas características ni la misma peligrosidad, es necesario disponer de una clasificación que ayudará a su conocimiento y posteriormente a su análisis, contención y erradicación.

Los principales agentes de la ciberamenaza que pueden afectar a los Estados son:

• Estados o Empresas que realizan acciones de ciberespionaje.

• Ciberdelincuencia organizada.

• Hacktivistas.

• Grupos terroristas, diferenciando dos vertientes.

– Uso de internet por terroristas. Por ejemplo, para intercambiar información.

– Ciberterrorismo.

• Insiders maliciosos, personal interno de las organizaciones que lleva a cabo acciones de manera intencionada.

• Ciberpatriotas, civiles que llevan a cabo acciones en el ciberespacio en apoyo a conflictos económicos, políticos o militares en los que se vea envuelto su país.

A grandes rasgos, se pueden distinguir principalmente las siguientes motivaciones para la realización de un ciberataque:

• Desafío o motivación personal, llevándose a cabo por actores individuales con el fin de ganar fama a costa de revelar información de empresas o exponer sus vulnerabilidades.

• Económicas, a través de la venta de la información obtenida o robada de datos personales e información.

• Políticas, como ataques a páginas gubernamentales o de partidos políticos o grandes empresas, con el fin de dañar su reputación y su imagen pública.

• Robo de información y espionaje, que suele ser llevado a cabo por grandes empresas o por actores estatales. Normalmente son ataques prolongados en el tiempo obteniendo todo tipo información, desde secretos industriales a secretos militares, u otro tipo de datos como pueden ser los datos médicos.

Existen muy diversos factores que podemos considerar a la hora de establecer los criterios de clasificación, como por ejemplo el tipo u origen de la amenaza, la categoría de los sistemas afectados, el perfil, posición o privilegios de los usuarios afectados, el número y tipología de los sistemas afectados o simplemente el impacto que el incidente puede tener en la organización desde los puntos de vista de la protección de la información, la prestación de los servicios, problemas legales o la misma imagen pública.

El conocimiento de estos factores es muy importante a la hora de tomar la decisión de clasificar el tipo de ciberincidente o determinar su peligrosidad y prioridad de actuación.

Teniendo en cuenta las anteriores motivaciones, los principales tipos de ataque irán fundamentalmente dirigidos a afectar a la Confidencialidad de la información, a la Integridad y a la Disponibilidad de la misma y de los sistemas que las manejan. De esta forma se distinguen distintos tipos de ataques:

• Ataques pasivos, en los que el atacante simplemente monitoriza las comunicaciones y la información que se transmite.

• Ataques activos, que implican algún tipo de acción contra los sistemas y contra la información transmitida. Estos ataques se podrían dividir en varias categorías:

– Ataques de disponibilidad: ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones (denegación del servicio, fallo de hardware o software, error humano o sabotaje).

– Suplantación de identidad: el intruso se hace pasar por una entidad diferente, con el fin de engañar al sistema o la persona, para acceder a recursos a los que no podría acceder normalmente.

– Alteración de información o de los mensajes transmitidos: tienen el fin de lograr un objetivo no deseado por la víctima, como podría ser alterar un expediente médico o provocar que a un paciente se le administrase un medicamento o una dosis inadecuada.

– Obtención de información de manera activa: ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.

Para llevar a cabo los ataques, los atacantes usarán diferentes vectores de ataque, entre los se pueden destacar:

• Malware: software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas (virus, gusanos, troyanos, spyware, rootkit, adware, ransomware o herramienta para acceso remoto).

• Exploits: son programas o fragmentos de código que aprovechan una vulnerabilidad para provocar un comportamiento no deseado a nivel software o hardware.

• Ingeniería social o phising: es la práctica de obtener información o lograr que un usuario ejecute una acción, mediante la manipulación de usuarios legítimos y situaciones cotidianas y aparentemente inofensivas.

• Keyloggers hardware: son dispositivos que se conectan entre el teclado y el ordenador, con el fin de robar la información tecleada por la víctima, entre la que se encuentran contraseñas e información sensible. Este ataque se suele dar en ordenadores expuestos en zonas públicas o en sitios poco vigilados en ciertas organizaciones, a los que tenga acceso el público general o las visitas.

• Memorias USB: aparentemente perdidas u olvidadas, pero dejadas por un atacante con el fin de que sean conectadas en un equipo de una red. Una vez que se conectan pueden realizar distintas acciones, tales como instalar algún malware o abrir una conexión con un atacante externo.

Atendiendo a la clasificación realizada y al número de incidentes producidos anualmente en España, los más importantes en nuestro país son los siguientes:

• Ransomware: consiste en un malware que entra a un ordenador o a un sistema para cifrar los datos que contiene y pedir un importe económico a cambio de liberar el bloqueo y poder acceder de nuevo a los archivos. Se trata de una de las prácticas

de ciberataques más frecuente y hay muchas formas de introducir un ransomware, aunque la más común es la que se produce a través de email mediante archivos adjuntos o enlaces trampa de supuestas instituciones de confianza.

• Adware: es otro tipo de malware que afecta sobre todo a personas individuales, que introduce en cualquier dispositivo electrónico publicidad en lugares donde no debería haberla, como en ventanas emergentes o en ciertos tipos de programas. Aunque no entraña un gran peligro para la seguridad informática, si analiza los hábitos de navegación y provoca el abuso de inserción publicitaria personalizada en los dispositivos afectados.

• Phishing: es un ejemplo de ingeniería social, generalmente vía correo electrónico o mensajería instantánea, en el que el atacante se hace pasar por una entidad de confianza para conseguir que la víctima proporcione información sensible, como datos personales, números de tarjetas de crédito, cuentas bancarias o contraseñas, o bien que descargue y ejecute una aplicación que generalmente será algún tipo de malware. El modus operandi siempre suele repetirse: el usuario recibe una comunicación en la que se le pide incluir algunos datos personales. La página web a la que deriva suele ser una copia exacta de la página de la empresa original.

• Wifi Hacking: consiste en aprovechar una vulnerabilidad en la seguridad de una red wifi para acceder a la red interna, a partir de ese momento el atacante tendrá acceso a la información transmitida y podrá realizar acciones dentro de la red con el fin de entrar a distintos equipos y obtener más información.

• Intrusión física a instalaciones: en determinadas ocasiones simplemente basta un dispositivo para copiar información y acceder por un breve momento a la fuente.

Cada tipo de ataque está orientado a conseguir un objetivo distinto, sin embargo, al margen de las consecuencias prácticas que se pudieran llegar a producir, es indiscutible que cualquiera de estos ataques, sean del tipo que sean, son capaces de generar una sensación de inseguridad y desconcierto tanto en los ciudadanos como en las economías, por lo que el gasto en ciberdefensa se ha multiplicado en los últimos años.

VULNERABILIDAD DE LOS SISTEMAS DE INFORMACIÓN SANITARIOS MILITARES

Ningún sistema de información está libre del riesgo de sufrir un ciberataque, desde este punto de vista todos son iguales, al fin y al cabo son sistemas de información con la «única» diferencia del fin para el que se utilizan y del uso que se le da a los datos que contienen. Lo que realmente hace que exista un mayor o menor riesgo de sufrir un ciberataque son los datos que contienen, el nivel de actualización de software y el nivel de seguridad con que los protejamos. En los hospitales, aunque el nivel de seguridad ha mejorado mucho, tradicionalmente ha sido bajo ya que se trata de entornos muy abiertos que utilizan muchos dispositivos diferentes de distintos fabricantes, y la mayoría bastante antiguos desde el punto de vista del software, lo que hace que sea «fácil» penetrar en ellos. La digitalización en el sector de la salud es imprescindible pero hay que crear un sistema de protección acorde y en paralelo a su implantación.

El espionaje industrial entre marcas comerciales y servir como campo de entrenamiento para hackers son dos de los principales motivos por los que los hospitales sufren ciberataques pero, como es de suponer, los motivos económicos son el principal motivo con diferencia, llevándose a cabo con malware en la mayoría de las ocasiones, buscando robar datos personales y sanitarios de los pacientes, bloquear equipos o cifrar información y posteriormente pedir compensaciones económicas para su recuperación.

Recientemente, aprovechando la situación de caos generada por la COVID-19, se han producido multitud de ciberataques de todo tipo a hospitales como los siguientes:

• En España se produjo un ataque tipo ransomware, llamado Netwalker, que consistía en un correo electrónico que contenía información sobre el virus como señuelo, enviado a personal sanitario, que intentaba acceder a los sistemas de los hospitales para inutilizarlos y posteriormente pedir una recompensa.

• En Brno (República Checa), al inicio de la pandemia se produjo otro ataque de tipo ransomware que secuestró los dispositivos electrónicos del Hospital Universitario, obligando a posponer intervenciones quirúrgicas de urgencia así como al traslado de pacientes en situación delicada a otros centros sanitarios próximos.

• En Estados Unidos, se produjo un ciberataque al sistema informático del Departamento de Salud y Servicios Humanos buscando la ralentización de los sistemas, objetivo que no alcanzaron.

• Reino Unido, en mayo de 2017, sufrió las consecuencias de un ciberataque tipo ransomware, llamado WannaCry, que no estando dirigido específicamente contra su sistema de salud afectó al menos a 16 de sus hospitales viéndose obligados a apagar sus sistemas informáticos debido a que aparecía un mensaje que exigía un rescate económico a cambio de acceder al sistema.

Debido a la información que se maneja en estos sistemas de información, tienen que estar permanentemente actualizados y ser más seguros de lo que son hoy en día; la cuestión fundamental respecto a las amenazas sobre la seguridad de los hospitales no se basa en si se va a producir una incidencia, sino más bien, en cuándo va a ocurrir y en la gravedad que ello va a suponer.

En muchas ocasiones, el factor humano, y no el tecnológico, es la clave a la hora de asegurar un nivel adecuado de seguridad. Las personas son un factor esencial en todo sistema pero al mismo tiempo también son el eslabón más débil a la hora de proteger los sistemas informáticos y las redes de datos, por lo que se le debe prestar una especial atención. Como se suele decir, los mayores agujeros de seguridad informática se encuentran sentados frente a las pantallas de los ordenadores, y dos de los errores más comunes que suelen ser riesgos de seguridad importantes, son las contraseñas débiles o apuntadas en post-its a la vista, y abrir emails sospechosos que contienen virus o troyanos. Es fundamental un programa robusto de sensibilización, concienciación y formación en toda organización, que garantice que su personal entiende su responsabilidad en materia de seguridad, las políticas de la organización en ese campo y como usar y proteger correctamente los recursos puestos a su disposición.

La seguridad total en internet no existe, pero eso no implica que no haya que buscarla por lo que hay que estar siempre alerta para minimizar las consecuencias.