Francesc Pla

Los avestruces no saben de ciberseguridad

> «Los usuarios suelen ser el eslabón más débil de la cadena, sea por posibles actos maliciosos o por desconocimiento y falta de concienciación»

Uno de los cambios más profundos de las sociedades modernas es el que ha provocado la irrupción de las tecnologías de la información y comunicación (TIC). Es una obviedad que internet ha cambiado la vida de las personas del mundo desarrollado y las condiciones en las que deben trabajar para aumentar su competitividad en los distintos sectores económicos. No es el objeto de este artículo glosar las oportunidades que ofrecen estas tecnologías, que son muchas, sino analizar y reflexionar sobre las nuevas obligaciones y responsabilidades que comporta la implantación de un cambio tan radical.

En esta última década, las oficinas de farmacia se han visto obligadas a incorporar las TIC de forma relevante en su operativa diaria. La implantación extensiva y exhaustiva de la receta electrónica en toda España ha significado un punto de inflexión en la tendencia alcista del grado de tecnificación del sector, lo que a su vez ha implicado que su dependencia de las TIC, tanto desde el punto de vista profesional como desde el empresarial, se haya incrementado de forma exponencial.

©alphaspirit/123RF

Cualquier análisis de las responsabilidades de las oficinas de farmacia en este ámbito deberá tener en cuenta que, como establecimiento sanitario que son, el manejo de sus datos deberá ajustarse a los estándares estrictos que dicta la nueva normativa europea en materia de protección de datos del Reglamento General de Protección de Datos de la UE (RGPD, 2016/679), y a la vez, como empresa altamente tecnificada que también es, deberá velar por el buen funcionamiento de sus infraestructuras informáticas y por la integridad de los datos necesarios para la correcta gestión de la empresa.

La penetración intensiva de las TIC en el quehacer diario de las farmacias ha generado nuevos sistemas de relación entre farmacias, colegios profesionales, asociaciones empresariales, administraciones, mayoristas y proveedores en un teatro de operaciones llamado «ciberespacio», integrado por el conjunto de sistemas de información, sistemas e infraestructuras de telecomunicaciones, internet, redes sociales y por los usuarios que interactúan con ellos. Este mundo «hiperconectado» abre, aún más si cabe, las puertas a la explotación de las vulnerabilidades de todas estas tecnologías con fines maliciosos. Tanto para la seguridad de la propia farmacia, como para las instituciones y empresas con las que las farmacias están permanentemente conectadas.

La explotación de las posibles vulnerabilidades de los sistemas de información, cada vez más expuestos a posibles ataques (tanto desde el exterior como desde el interior de las propias farmacias), puede conllevar importantes perjuicios económicos, sanciones, así como graves deterioros en la reputación frente a los clientes y a la Administración.

A nuestro entender, con demasiada frecuencia se oyen voces (sobre todo entre los usuarios domésticos y también entre los profesionales autónomos y las pequeñas y medianas empresas, a diferencia de las grandes corporaciones, que, de forma mayoritaria y sistemática, dedican recursos importantes a blindar sus sistemas de información) que proclaman la idea de que lo natural es convivir en un estado de inseguridad.

«La inseguridad en el ciberespacio es inevitable.» Es peligroso que esta afirmación se convierta en un mantra que consolide la creencia de que la inversión en ciberseguridad es un gasto superfluo y que el único método posible para afrontar esta situación es cruzar los dedos. Existe una diferencia crucial entre afirmar que la seguridad absoluta no existe (por lo que las ofertas de servicios que lo aseguren no son creíbles) y asumir como algo inevitable la vulnerabilidad. No saber diferenciar entre lo uno y lo otro puede derivar en perjuicios muy importantes para las farmacias.

Garantizar la invulnerabilidad es una exageración que puede rozar la irresponsabilidad, pero tampoco es responsable afirmar que es imposible intervenir de forma efectiva para reducir los riesgos y minimizar los perjuicios. Tampoco es acertado pensar que la oficina de farmacia no tiene

©joerf/123RF

> **“La inseguridad en el ciberespacio es inevitable”. Es peligroso que esta afirmación se convierta en un mantra que consolide la creencia de que la inversión en ciberseguridad es un gasto superfluo»**

«interés» para los cibercriminales, lo que proporciona una falsa sensación de seguridad que es un gran aliado para los que nos pueden atacar. Las farmacias y las organizaciones a las que están conectadas siempre son susceptibles de ser atacadas por los datos sensibles que manejan.

Es importante destacar que se puede y se debe actuar frente a las amenazas existentes. Las farmacias deben asumir que este escenario en el que tienen que ejercer su profesión también comporta inversiones de tiempo y dinero en el campo de la ciberseguridad, y deben buscar productos que, minimizando en lo posible su inversión, maximicen la seguridad de su entorno tecnológico.

Estrategias para maximizar la seguridad

¿Qué producto debe buscar una farmacia para lograr este objetivo? Lamentablemente, no existe un producto único o una fórmula magistral que pueda resolver todos los posibles problemas de seguridad, pero sí existen estrategias orientadas a minimizar las amenazas, a detectar posibles ataques y a disponer de mecanismos de respuesta y recuperación.

Entre las distintas estrategias que se aplican en el ámbito de la ciberseguridad, la estrategia de defensa en profun-

didad[1] es aquella que implementa diferentes mecanismos y estrategias que se complementan entre sí, con el objeto de que, en caso de vulneración de uno de los mecanismos, no se vea comprometida la totalidad del sistema.

Es recomendable establecer mecanismos que cubran las distintas capas de un sistema de información: capa física, capa de red, servidores y estaciones de trabajo, capa de aplicación, capa de datos y, finalmente, la capa humana.

Antes de implantar sofisticados mecanismos, dispositivos y herramientas, es recomendable no empezar la casa por el tejado y optar por la implantación de un conjunto de mecanismos iniciales que ayudarán a mejorar la seguridad de cada uno de los diferentes niveles.

Capa física

La seguridad en esta capa debe contemplar el conjunto de medidas que impidan físicamente el fácil acceso a los sistemas de información centrales de la oficina de farmacia (servidores, equipos de comunicaciones, equipos de seguridad...) por parte de personas no autorizadas, pero también un conjunto de equipos que garanticen la operativa de dichos sistemas.

Es recomendable que los sistemas centrales estén ubicados en una dependencia dotada de un conjunto de requisitos, como:

- Control físico de acceso.
- Vigilancia mediante la propia alarma de la oficina de farmacia y con conexión a una central receptora de alarmas.
- Sistema de climatización.
- Cuadro eléctrico dedicado.
- Sistema de alimentación ininterrumpida (SAI).

Mecanismos más avanzados contemplarían sistemas de videovigilancia remota (TVCC) y la monitorización de la temperatura y del suministro eléctrico.

> **«La peor elección frente a los ataques cibernéticos es imitar a los avestruces, porque de ciberseguridad no saben nada»**

Capa de red

Es necesario reforzar la red y su perímetro, y para ello es recomendable:

- Configurar correctamente todos los elementos de la red.
- Configurar correctamente los *switches*[2], bien mediante listas de control de accesos[3], bien mediante bloqueo de puertos[4], o bien mediante asignación de direcciones MAC[5], con el objeto de evitar conexiones no deseadas.

Glosario

[1]**Estrategia de defensa en profundidad.** Estrategia de seguridad basada en definir los mecanismos de control teniendo en cuenta la infraestructura tecnológica sobre la que se soportan los servicios.
[2]***Switch.*** Equipo conmutador donde se conectan los diferentes elementos de la farmacia conectados en red, principalmente ordenadores, así como otros elementos conectados en red: dispensador, cámara de videovigilancia, cajas registradoras, puntos de acceso wifi, etc.
[3]**Listas de control de accesos.** Listado de equipos/puertos de confianza a los que se permitirá conexión a la red o a los servicios informáticos (al resto se le denegará).
[4]**Puertos.** Puertas virtuales por la que se envía y recibe información entre los ordenadores de la farmacia e internet.
[5]**Direcciones MAC.** Número de identificación individual de que dispone cada equipo que se puede conectar a una red de comunicaciones, similar al «DNI» de cada equipo, ordenador, teléfono móvil, etc.
[6]**VLAN.** Red local virtual. En una funcionalidad de los *switches* que permite separar de forma virtual elementos conectados a un mismo *switch* que no tienen por qué intercambiar información entre ellos, aumentando así la seguridad.
[7]**Mecanismos de filtrado entre subredes.** Segmentación entre redes confiables y no confiables y las comunicaciones permitidas entre ellas.
[8]**VPN.** Red privada virtual. Se basa en la creación de una conexión segura y cifrada para comunicaciones entre equipos que se conectan a internet, emulando una conexión a nivel de red local, más segura.
[9]***Passwords* por defecto.** Contraseñas fáciles de recordar y conocidas en el mundo TIC que los proveedores de servicios suelen configurar de fábrica en los equipos. Estas contraseñas son muy comunes y no suponen en la práctica ninguna capa de seguridad si no se modifican.
[10]***Firewall.*** Es un equipo o aplicación diseñado para filtrar las comunicaciones con redes externas a la red local de la farmacia, generalmente internet. Según su parametrización, decide qué comunicaciones o accesos se permiten y cuáles se bloquean.
[11]**IDS/IPS.** Es un equipo o aplicación diseñado para detectar y prevenir posibles intrusiones a la red local de la farmacia, a partir de firmas de tipos de ataque conocidas y de comportamientos sospechosos.
[12]**Firmas de ataque.** Registro forense que deja un ataque en el registro de un sistema atacado.
[13]***Pentesting.*** Realización de una auditoría o test de intrusión con el objetivo de conocer posibles vulnerabilidades en la red o servicio, complementado con la verificación práctica del efecto que tendría el uso malicioso de las mismas (ejemplo: verificar cómo un atacante podría conseguir acceso a una red wifi, y contrastar qué sería capaz de hacer una vez dentro).
[14]***Bug.*** Fallo de programación que podría convertirse en una potencial vulnerabilidad de seguridad.
[15]***Antimalware.*** Aplicación específica diseñada para prevenir, detectar y mitigar el *malware*, es decir, aplicaciones y *software* en general pernicioso para los sistemas informáticos, como pueden ser virus informáticos, troyanos, etc.
[16]**Servicios.** Un servicio o servidor informático es una aplicación centralizada que utilizan los diferentes usuarios conectados a la red de la farmacia (ejemplos: el servicio de impresoras, el servicio de correo electrónico, etc.).
[17]**HIPS.** Es un sistema de prevención de intrusión (IPS) especializado en el control de un equipo o aplicación.
[18]**Ingeniería social.** Técnica de engaño utilizada por atacantes informáticos centrada en explotar el factor humano para vulnerar los mecanismos de seguridad (ejemplo: conseguir que un usuario corporativo facilite sus credenciales de acceso a partir de una llamada/correo electrónico engañoso).
[19]***Phising.*** Suplantación de servicios y aplicaciones que el usuario utiliza habitualmente con el objetivo de conseguir de forma fraudulenta información de acceso de usuarios legítimos del sistema.

- Segmentar la red de la oficina de farmacia mediante VLAN[6] (redes virtuales) y aplicar mecanismos de filtrado entre subredes[7], de manera que dispositivos no autorizados, bien vía wifi, bien vía ADSL particular, etc., no tengan acceso a los equipos con información sensible.
- Configurar el acceso wifi, en caso de que se disponga de él, de manera profesional, satisfaciendo todas las medidas de seguridad inalámbrica.
- Los accesos remotos al servidor o a las estaciones de trabajo, bien por parte del titular, bien por parte de los proveedores (empresas de informática, programas de gestión, etc.), deben ser gestionados mediante conexiones seguras y cifradas, tipo VPN[8].
- Modificar los *passwords* por defecto[9] de los diferentes elementos de la red y actualizar las versiones de *software* de los mismos.

Asimismo, sería recomendable incrementar los niveles de seguridad mediante otras medidas:

- La implantación de un equipo *firewall*[10] o cortafuego (FW), debidamente configurado con listas de acceso (ACL) pa-

ra controlar el tráfico entre la red de la oficina de farmacia y las redes externas, a partir de un conjunto de reglas establecidas.
- Mecanismos de detección y prevención de intrusiones (IDS/IPS)[11], monitorizados de manera permanente, con el objeto de detectar o predecir accesos no autorizados mediante el reconocimiento de firmas de ataques[12].
- Auditorías permanentes de la superficie expuesta mediante técnicas de *pentesting*[13]. Dada la continua aparición de vulnerabilidades y de nuevas versiones, de poco sirven las auditorías anuales o semestrales.

Capa de servidor/es y estaciones de trabajo

En esta capa son recomendables las siguientes medidas:
- Mantener los diferentes aplicativos actualizados con la última versión del fabricante, dado que muchas de ellas solventan *bugs*[14] de seguridad publicados y de fácil explotación.
- Disponer de un buen *software antimalware*[15], también permanentemente actualizado.
- Realizar un uso profesional de las estaciones de trabajo, accediendo a webs profesionales y seguras.
- Evitar mantener abiertos servicios[16] por defecto, no necesarios, que son normalmente vías de posibles ataques.

©nicoelnino/123RF

Asimismo, sería recomendable incrementar los niveles de seguridad del servidor mediante sistemas de prevención de intrusiones (HIPS)[17] debidamente monitorizados.

Capa de aplicación

En esta capa son recomendables las siguientes medidas:
- Mantener los diferentes aplicativos actualizados con la última versión del fabricante.

- Asegurar una correcta configuración de los protocolos, como smtp, dns...
- Implantar una adecuada política de autentificación mediante contraseña y un segundo factor de autentificación. La efectividad de los sistemas de seguridad basados sólo en usuario y *password* es claramente mejorable.
- Minimizar los privilegios, de manera que cada elemento disponga únicamente de los privilegios necesarios para su operativa. No todos los usuarios necesitan utilizar todos los servicios del sistema.

Capa de datos

Dada la sensibilidad de algunos de los datos, así como la criticidad de otros necesarios para garantizar la continuidad de la operativa de la oficina de farmacia, es recomendable:

- Realizar un estricto control de acceso a los datos, de manera que sólo sean accesibles desde dispositivos y aplicaciones autorizados.
- Proteger los datos mediante técnicas de encriptación.
- Realizar diariamente copias de seguridad encriptadas, debidamente monitorizadas, en infraestructuras externas (CPD, Cloud...).

Capa humana

Los usuarios suelen ser el eslabón más débil de la cadena, sea por posibles actos maliciosos o por desconocimiento y falta de concienciación. Son normalmente uno de los puntos más vulnerables y fáciles de atacar, mediante técnicas de ingeniería social[18], *phising*[19], etc.

Es fundamental la formación y concienciación de los usuarios en materia de seguridad, dado que el sistema es tanto más seguro cuanto más lo sea su eslabón más débil.

De nada sirve todo lo anterior si los usuarios que se conectan a la red de la oficina de farmacia tienen sus portátiles infectados con *malware*, con *software* no seguro o Apps no seguras en sus dispositivos móviles.

A grandes rasgos, éstas son las recomendaciones generales que una oficina de farmacia debería seguir para aumentar de forma sensible su seguridad. Es cierto que la especificidad del sector desde el punto de vista profesional y empresarial dificulta que los productos estandarizados existentes en el mercado se adapten a ella, por lo que es necesario que los proveedores hagan un análisis inicial de esas especificidades para diseñar productos y servicios adecuados, útiles y competitivos en precio.

El peligro de ataques cibernéticos es real. La percepción del peligro que representan para el buen funcionamiento es una cuestión personal del responsable de la farmacia, y las decisiones sobre el riesgo que es capaz de asumir cada farmacéutico son intransferibles, pero lo que es incontestable es que la peor elección frente a esa realidad es imitar a los avestruces, porque de ciberseguridad no saben nada. ●