La Ciber-Pandemia

Ataques informáticos contra el sector sanitario

pandasecurity.com

panda

Desde siempre se le ha reconocido un carácter muy noble al sector sanitario. Tanto es así que, incluso en tiempos de guerra, su naturaleza humanitaria le concede el respeto y la protección de toda la sociedad. Quizá es por eso que se hace difícil pensar que pueda convertirse en el objetivo de algún tipo de ataque.

Pero el dinero es uno de los motores que mueve el mundo, y el anhelo por tenerlo no entiende de sectores. Es también la principal motivación de unos ciberdelincuentes que han encontrado en el sector sanitario un filón muy rentable.

Despreocupado por su condición social y su excelente posición en la comunidad, el ámbito sanitario ha descuidado durante años la seguridad de sus sistemas. Nos encontramos ahora con una industria tecnológicamente muy avanzada pero con un abandono en seguridad muy preocupante.

Un historial comprometedor

Que el ransomware haya convertido en una de las amenazas más populares hoy en día, es solo un ejemplo más de que el lucro económico se ha convertido en el leitmotiv de los ciberdelincuentes.

Un ataque que busca a víctimas con información valiosa, y dispuestas a pagar por recuperarla, convierte a las empresas en el objetivo perfecto.

Pero también hay ataques diseñados contra una industria en concreto. De hecho, en determinados sectores como el financiero, el interés es más que evidente. Aquí, cuando el objetivo es una cuenta bancaria particular, la finalidad del atacante es retirar todo el dinero y dejarla a cero. Y aun cuando la víctima es la propia entidad bancaria el objetivo se mantiene, como vimos con el caso del Banco Central de Bangladesh.

Otros sectores sin embargo, no sufren el robo de dinero de forma directa. Pero el objetivo sigue estando muy claro. Grandes almacenes, servicios y hoteles, como documentamos en el whitepaper “El Ciberexpolio Hotelero”, en todos aquellos casos los ciberdelincuentes iban a por la información de las tarjetas de crédito infectando los Terminales de Punto de Venta.

Saqueo de cuentas bancarias, suplantación de identidad o robo de datos de tarjetas de crédito, no parecen ser objetivos rentables en el sector sanitario. De hecho, en una gran cantidad de países no es habitual utilizar tarjetas de crédito para pagar por los servicios, ya sea porque estén cubiertos por el Estado o por seguros de salud privados. A pesar de que propósito no sea tan evidente, hospitales, clínicas, laboratorios y todo tipo de centros asistenciales son objetivo continuo de ataques a gran escala.

¿Por qué la industria sanitaria?

De acuerdo con la Office of Civil Rights de Estados Unidos, **durante 2015 se produjeron unos 253 agujeros de seguridad en el sector sanitario que afectaron a más de 500 personas con el robo de más de 112 millones de registros**. Esta industria sufrió más ataques que cualquier otra en 2015, según IBM.

Todo el sector está en plena revolución tecnológica y ahora toda la información se almacena en formato digital, algo muy beneficioso para el paciente. Toda esta información se encuentra además disponible a través de la red así, en caso de cambio de médico, por ejemplo, el facultativo puede acceder de forma sencilla al historial del paciente. Es este mismo adelanto el que genera un serio problema de seguridad para la industria sanitaria. La información médica es muy valiosa, por lo que quien logre hacerse con ella puede obtener suculentos beneficios.

En algunos países incluso, se puede comerciar con esta información de forma legal, y hay empresas muy interesadas en hacerse con ella, desde centros de investigación a compañías aseguradoras.

Por no hablar del mercado negro, donde un historial clínico puede ser varias veces más valioso que una tarjeta de crédito.

Estos registros contienen una gran cantidad de información personal, lo que puede convertirse también en una llave maestra para llevar a cabo ataques dirigidos. Pensemos en personas clave en puestos de responsabilidad que cuidan especialmente su privacidad y son muy reservadas a la hora de mantener online su información personal. Por muy cuidadosas que sean no pueden evitar que sus historiales estén registrados en sus centros médicos, y si estos caen en manos equivocadas, su intimidad puede dejar de ser tan privada.

O supongamos que conseguimos acceso a información confidencial sobre estudios farmacéuticos, la competencia pagaría a precio de oro la oportunidad de quitarle de las manos una patente mil millonaria a sus rivales. O algo menos pretencioso, consigamos la ficha completa de algún facultativo médico y podremos recetar cualquier medicamento en su nombre.

Historiales médicos, direcciones de email, contraseñas, números de la seguridad social, información confidencial de empleados, pacientes y empresas; **datos todos ellos con un valor increíblemente alto que están rodeados de la última tecnología pero protegidos con un sistema de seguridad que se ha quedado obsoleto**.

Un historial de ataques muy lucrativos

Cruz Roja Americana

En 2006, un empleado de la Cruz Roja Americana en San Luis accedió a los datos de más de 1 millón de donantes de sangre, y llegó a robar la identidad y a utilizar la información de 3 de ellos.

Más de 1 millón de datos de donantes fueron comprometidos

Temple Street Children's University Hospital

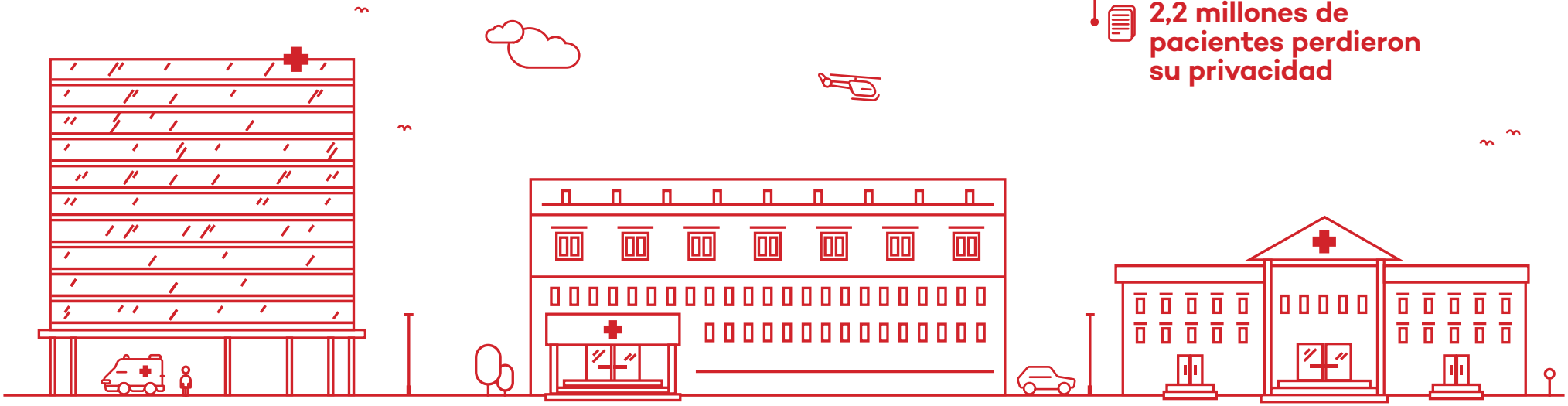
Un año después, 2 servidores que contenían datos de casi 1 millón de pacientes fueron robados del Children's University Hospital de Temple Street, en Irlanda. Entre la información sustraída se hallaban datos de los pacientes, incluyendo nombres, fecha de nacimiento y motivo del ingreso.

Se robaron datos de más de 1 millón de pacientes

The University of Utah Hospitals & Clinics

En 2008, la University of Utah Hospitals & Clinics anunció que los datos de 2,2 millones de pacientes habían sido robados. Los datos estaban en unas cintas de backup guardadas en el coche de un empleado de una empresa externa con la que habían subcontratado el almacenamiento. En este caso el empleado incumplió los protocolos establecidos para el transporte de información y millones de personas vieron sus datos comprometidos.

2,2 millones de pacientes perdieron su privacidad



Hasta ahora solo hemos hablado de casos puntuales, y no de ataques a gran escala. Sin embargo, con el paso de los años, el panorama ha cambiado de forma radical. Según un estudio publicado por el Ponemon Institute, **en los últimos 5 años los ataques a este sector han aumentado un 125%, convirtiéndose en su principal causa de pérdida de información**.

La situación es inquietante, puesto que un 91% de las organizaciones consultadas en ese estudio reconocían haber sufrido al menos una pérdida de datos como consecuencia de algún ataque durante los 2 últimos años. Y hasta un 40% reconocía haber tenido 5 o más pérdidas de información durante ese mismo periodo.

Anthem Insurance Company

Un ejemplo muy gráfico de esta situación lo protagonizó Anthem en 2015. Esta aseguradora médica, la segunda de EEUU, sufrió el robo de 80 millones de registros, con datos tan sensibles sobre los clientes como su número de la Seguridad Social.

Pero al robo de toda esta información, y su posible comercialización, se le suman los ataques de ransomware con impacto económico directo para las víctimas. De hecho, como hospitales, farmacéuticas y aseguradoras tienen tanta y tan valiosa información, este tipo de secuestros han afectado con especial virulencia a este sector. Los ciberdelincuentes se han centrado en ellos esperando contar con más posibilidades de obtener altos rescates para poder recuperar la información.

Robaron 80 millones de registros con datos de clientes

Hollywood Presbyterian Medical Center

Sin ir más lejos, el Hollywood Presbyterian Medical Center de Los Ángeles declaró una "emergencia interna" y dejó a sus empleados sin acceso a los historiales médicos de sus pacientes, al correo electrónico y otros sistemas.

Como consecuencia de esto, algunos pacientes no pudieron recibir tratamiento y algunos tuvieron que ser derivados a otros centros. El rescate solicitado por los ciberdelincuentes era de 3,7 millones de dólares. Aunque el CEO del hospital llegó a un acuerdo y finalmente pagó unos 17.000 dólares para poder recuperar los ficheros secuestrados.

Se pidió un rescate de 3,7$ millones

Baltimore MedStar Health

MedStar Health reconoció también que tuvo que desconectar algunos de los sistemas en sus hospitales de Baltimore debido a un ataque similar.

Tuvieron que desconectar los sistemas del hospital

Henderson Methodist Hospital

El Methodist Hospital en Henderson, Kentucky, ha sido otra de las víctimas.

En este caso también pagaron un rescate de 17.000 dólares, aunque se comenta que el pago pudo ser sensiblemente superior a la cifra publicada.

Pagaron 17.000$ por el rescate de su información

Prime Healthcare Management

Prime Healthcare Management, Inc. fue también víctima, con 2 hospitales atacados (Chino Valley Medical Center y Desert Valley Hospital), y muchos otros afectados por el mismo ataque.

En este caso la compañía no pagó ningún rescate.

Dos de sus hospitales fueron atacados

Lukas Hospital y Klinikum Arnsberg

Pero no sólo los hospitales norteamericanos son objetivos suculentos para los ciber-criminales, en Alemania se han visto casos similares.

Según el Deutsche Welle, varios hospitales como el Lukas Hospital en Neuss y el Klinikum Arnsberg en North Rhine-Westphalia, sufrieron también ataques de ransomware. Pero en ninguno de los dos casos se accedió a pagar el rescate.

2 hospitales alemanes también fueron atacados

Kansas Heart Hospital

De hecho, **es necesario apuntar que el pago del rescate en ningún caso garantiza la recuperación de la información**. Un claro ejemplo de esto es lo que le sucedió al Kansas Heart Hospital en mayo de 2016 que, tras sufrir un ataque de ransomware, sus responsables optaron por pagar el rescate demandado. Los atacantes comenzaron a descifrar la información pero, justo antes de finalizar, exigieron un segundo pago para devolver el resto de la información. El hospital decidió no realizar este segundo pago.

Los hackers pidieron un segundo rescate

"Es mejor prevenir que curar"

Con todos estos casos, es evidente que el sector debe aplicarse su propia máxima.

Una realidad de ciencia ficción

Los ataques han demostrado ser capaces de paralizar la actividad de un hospital, de robar miles de registros y de utilizar la información sensible como rehén de cobro.

Pero bajo todo esto, hay algo mucho más cercano que puede afectar a cualquier persona de a pie. Solo tenemos que pensar en que prácticamente todos los equipos médicos (marcapasos, escáneres, rayos X, bombas de perfusión, respiradores, etc.) están conectados en red. Pensaremos pues en casos reales y no en delirios tan fantásticos como pueden parecer.

Tan es así que el ex-vicepresidente de EEUU Dick Cheney, en 2013 reveló que sus doctores habían deshabilitado la comunicación inalámbrica de su marcapasos porque resultaba creíble la amenaza de que alguien tratara de realizar un ataque remoto para atentar contra su vida.

De hecho un año antes, Barnaby Jack el famoso hacker neozelandés, **demostró a los asistentes a su conferencia cómo podía manipular remotamente un marcapasos para que emitiese un shock eléctrico potencialmente mortal**. Barnaby diseño un ataque que podía afectar a todos los marcapasos en un radio de 15 metros.

El propio Barnaby, había demostrado anteriormente cómo podía alterar de forma remota una bomba de insulina portátil, utilizada por diabéticos, de tal forma que podía dar la orden de inyectar una dosis letal de insulina a todos los aparatos en 90 metros a la redonda.

Jack murió una semana antes de poder demostrar como hackear corazones artificiales. En la conferencia Black Hat 2013 hubiese revelado cómo podía alterar el ritmo de estos implantes a su antojo.

Rayos X, Escáneres, Respiradores,...

Multitud de dispositivos permanecen desprotegidos.

Un marcapasos fue hackeado

para que emitiese un shock mortal.

Un ataque contra bombas de insulina

emitiría una orden letal a estos aparatos.

Richard Rios también hizo de las suyas para poner en evidencia las vulnerabilidades de estos aparatos. Un pólipo en el tracto respiratorio postró a este investigador en una cama del Stanford Hospital durante dos semanas. En ese tiempo Rios se percató de que su cama estaba conectada a un ordenador. También lo estaban las correas que elevan sus pies y la bomba de perfusión que le inyectaba diariamente su medicación. Investigó y encontró hasta 16 redes y 8 puntos WiFi sin moverse de su habitación.

Después de pasar varios días encamado, salió al pasillo para estirar las piernas y encontró un dispensador de fármacos informatizado. El encargado de la distribución de todos los medicamentos de la planta era un ordenador al que los doctores y enfermeras accedían con una tarjeta de identificación codificada. Antes de ver ese aparato, Richard ya había averiguado que ese sistema tenía una vulnerabilidad: una contraseña incrustada en el código fuente del programa (hard-coded password) que le permitiría "jugar" con el dispensador de fármacos. A partir de ese descubrimiento, Rios se obsesionó con la seguridad de los dispositivos en el ámbito sanitario.

Durante los siguientes meses y junto con su socio Terry McCorkle, Richard identificó más de 300 dispositivos vulnerables en unas 40 empresas del ámbito socio-sanitario. El nombre de estas empresas nunca se hizo público pero Rios asegura que, a día de hoy, aún no han corregido esas vulnerabilidades.

En su afán por mostrar el peligro que suponen estos agujeros de seguridad, **Richard Rios llegó a demostrar cómo podía manipular de forma remota las bombas de medicación utilizadas en los hospitales de todo el mundo**. Así, hackeó varios de estos dispositivos alterando el suministro de la medicación hasta poder aplicar dosis letales de fármacos. Rios advirtió que podría hacerlo en más de 400.000 de estos dispositivos que permanecen vulnerables en todo el mundo.

Casi al mismo tiempo, unos analistas de TrapX Security en California, comenzaron a rastrear dispositivos vulnerables en más de 60 hospitales. **Infectaron cientos de dispositivos con un programa que reemplazaba el sistema original de la máquina en cuestión**. Los aparatos infectados seguían totalmente operativos, por lo que nadie se percató del problema, pero durante 6 meses permitieron que TrapX monitorease todos los movimientos de los hospitales a través de la red.

Entre los dispositivos a los que llegaron a tener acceso se encontraban aparatos de radiografía, herramientas para el análisis de sangre, bombas de perfusión, equipos de cirugía y, por supuesto, ordenadores del equipo sanitario. Muchos de estos aparatos funcionaban bajo sistemas antiguos y desprotegidos como Windows XP o Windows 2000. Precisamente, la protección antivirus de la mayoría de aquellos hospitales, limpiaron rápidamente el rastro de los ordenadores de los facultativos, pero parece ser que aquellos dispositivos no estaban tan bien protegidos y permanecieron infectados hasta que TrapX Security dio la voz de alarma.

Un dispensador de fármacos sin control
que permitía jugar con la distribución de medicinas.

400.000 Bombas de medicación alteradas
pudiendo variar su flujo de suministro.

Cientos de aparatos infectados
que permanecieron así durante meses.

¿Cómo podrían haberse evitado estos ataques?

Hemos visto cómo los delincuentes llevan a cabo ataques para robar información sensible, historiales médicos, estudios farmacéuticos o datos de asegurados. Cómo acceder a direcciones de emails, contraseñas y números de la seguridad social no les supone mayor problema. O cómo los ataques con ransomware pueden paralizar la actividad asistencial de todo un complejo hospitalario para llegar a obtener el rescate solicitado.

Evitar estos ataques tan rebuscados no es una tarea sencilla. De hecho implica que un conjunto de acciones, recursos y políticas sea diseñado específicamente para salvaguardar la seguridad de dispositivos, datos y personas.

La primera recomendación es básica y crucial: **contar con una solución de ciberseguridad que tenga funcionalidades de protección avanzada pero que cuente también con la capacidad de detectar y remediar las posibles amenazas**.

Pero el punto en común de la mayoría de estos ataques es algo tan sencillo de explicar cómo complicado de conseguir efectivamente: la falta de control sobre lo que ocurre en los sistemas de todos los equipos.

Por tanto, la siguiente recomendación es **contar con un modelo capaz de controlar todos los procesos activos en todas las máquinas conectadas a la red corporativa**. Una visibilidad total de lo que está ocurriendo te permitirá controlar cualquier anomalía y actuar antes de que se produzca el daño.

Adicionalmente, las empresas que manejen información tan sensible **deben revisar sus políticas de personal y sistemas de control para ajustar las exigencias de privacidad y adaptarlas a la tecnología de la que disponen**.

Por último, un consejo que siempre repetimos y que por más sencillo que parezca, pocas veces se completa: **debemos mantener actualizados los sistemas operativos y programas de todos los dispositivos de la empresa**. De este modo, cerraremos las puertas de las vulnerabilidades evidentes gracias a los parches de corrección que liberan los propios fabricantes. Para esto **es bueno contar con una política de actualizaciones y un control de los equipos disponibles**. En esa gestión, nos pueden ayudar herramientas de monitorización e inventariado que hacen que el mantenimiento de los equipos y sistemas sea más efectivo, uniforme, centralizado y seguro.

La solución

Una protección contra amenazas avanzadas y ataques dirigidos, e incluso, que sea capaz de detectar comportamientos extraños. Un sistema que pueda asegurar la confidencialidad de los datos, la privacidad de la información, el patrimonio y reputación empresarial.

Esto es Adaptive Defense 360, **el único sistema de ciberseguridad avanzado que combina protección de próxima generación y la última tecnología de detección y remediación con la capacidad de clasificar todos los procesos en ejecución**.

Adaptive Defense 360 clasifica absolutamente todos los procesos activos en todos los endpoint, garantizando la protección contra el malware conocido y contra amenazas avanzadas del tipo Zero-Day, Advanced Persistent Threats y Ataques Dirigidos.

Gracias a la clasificación del 100% de los procesos en ejecución, es capaz de detectar malware y comportamientos extraños o no comunes de los que el resto de sistemas de protección del mercado no se percatan.

Como sabemos exactamente todo lo que pasa con cada uno de los procesos y de los archivos, podemos realizar un estudio pormenorizado del flujo de la información y representar gráficamente todo el progreso desde cómo ha intentado entrar el malware, por dónde, desde dónde viene, qué pretendía hacer o quién y cómo intenta llevarse información.

Averigua quién y cómo accede a tus datos y controla la fuga de información, la que intente realizar un malware o la que realicen tus empleados.

Descubre y soluciona las vulnerabilidades de los sistemas y de los programas instalados y previene la utilización de los no deseables (barras de navegación, adwares, add-ons,...).

Adaptive Defense 360: visibilidad sin límites, control absoluto.

Más información en:

pandasecurity.com/spain/enterprise/solutions/adaptive-defense-360/

Más información en:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Contacta:

900 90 70 80

panda

Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

pandasecurity.com

panda