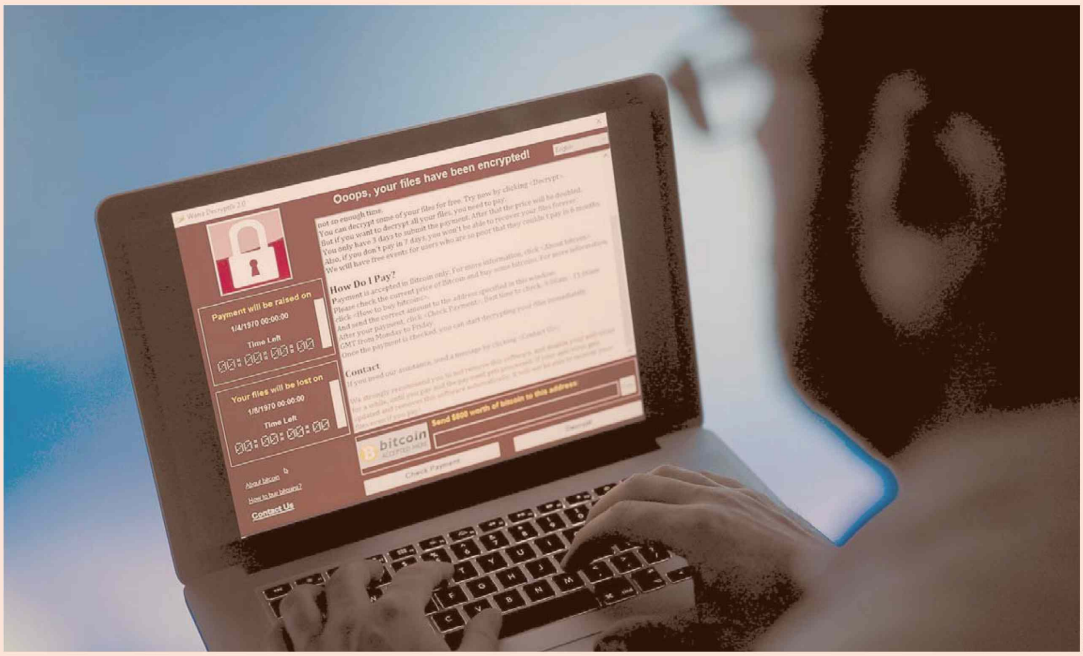
LITORALPRESS MEDIA DE INFORMACIÓN http://www.litoralpress.cl

Fecha: 31/10/2017
Fuente: DIARIO FINANCIERO (SANTIAGO-CHILE)
Pag: 8
Art: 2
Título: CENTROS DE SALUD Y CIBERATAQUES

Tamaño: 29,2x19,0
Cm2: 552,7

Tiraje: 30.000
Lectoría: 42.230
Favorabilidad: No Definida



BLOOMBERG

CENTROS DE SALUD Y CIBERATAQUES

Cinco claves para no bajar la guardia

Infor Cono Sur identifica cinco formas para implementar herramientas de ciberseguridad en las empresas, donde se incluyen los servicios de salud:

1. Contar con una política de seguridad informática. Esta tiene que reconocer la presencia de dispositivos y tener la capacidad de verificarlos antes de que puedan tener acceso a la red de la organización.

2. Tener sistemas de IDS/ISP, especialmente dedicados a plataformas móviles.

3. Implementar sistemas y soluciones que integren la protección antivirus de los dispositivos encriptando datos sensibles y teniendo medidas antirrobo basadas en contraseña maestra, reconocimiento facial y dactilar, entre otros.

4. Administrar el ciclo de vida de los dispositivos. De esta forma, las actualizaciones de sistemas de ciberseguridad se aseguran y no quedan obsoletas.

5. Limitar el almacenamiento de la información empresarial a dispositivos y activos de la empresa y de ninguna manera permitir el acceso de cuentas personales o que no pertenezcan a las corporativas.

LITORALPRESS MEDIA DE INFORMACIÓN http://www.litoralpress.cl

Fecha: 31/10/2017
Fuente: DIARIO FINANCIERO (SANTIAGO-CHILE)
Pag: 8
Art: 3
Título: CENTROS DE SALUD Y CIBERATAQUES

Tamaño: 17,0x18,5
Cm2: 315,0

Tiraje: 30.000
Lectoría: 42.230
Favorabilidad: No Definida

Hospitales y clínicas guardan en sus computadores información sensible que podría ser de alto interés para un hacker. ¿Están preparados estos establecimientos? Acá, expertos comentan las preocupaciones y los resguardos necesarios que se deben implementar para minimizar los riesgos.

Por María Ignacia Medina.

En lo que va del año, Chile ha experimentado un 40% de aumento en los ataques informáticos, de acuerdo a datos entregados por NovaRed. Dentro de esos incidentes, el *malware* -o software que busca infiltrarse o dañar un computador o dispositivo móvil- concentra el 37,6% de los ataques, mientras que el *ransomware* -un programa dañino que restringe el acceso a sistemas o archivos para pedir un rescate a cambio- ocupa el 28% de las ciberagresiones en 2017.

Los centros de salud no están exentos de eso. A mediados de este año, WannaCry, uno de los ataques más masivos en la historia de los *ramsonware*, atacó a gran parte del mundo y llegó a afectar directamente a 61 entidades del Sistema Nacional de Salud del Reino Unido, según Kaspersky Lab. Y es que cuando los servicios hospitalarios comenzaron a introducir tecnología y aplicaciones para hacer más eficiente su sistema, las preocupaciones en esa área cambiaron poco a poco y los hospitales y clínicas, con cada uno de sus servicios, comenzaron a entender que eran vulnerables a virus, hackers y ataques cibernéticos.

Para el gerente de Informática de Red de Salud UC CHRISTUS, Hugo de la Rosa, debido a que se ha incrementado el uso de la tecnología para almacenar y acceder a historial clínico de un paciente, tener acceso a resultados de exámenes inmediatamente, contar con información para investigación y educación, además de controlar el uso de los medicamentos en pos de la seguridad, entre otros temas, el nivel de exposición que tienen los hospitales, clínicas, consultorios y todos los servicios relacionados con el cuidado de la salud es mucho más alto que antes.

A juicio del gerente comercial de Infor Cono Sur, Rubén Belluomo, Chile está dentro de los países más propensos en la región a sufrir un colapso tras una emergencia como un ataque cibernético debido a que está por delante en el uso de tecnologías como computadores y sistemas.

"Se deben desarrollar sistemas integrales para reducir los riesgos, reforzar la privacidad y seguridad cibernética de la información de salud, al tiempo que se promueve la seguridad de los pacientes", explica, agregando que, pese a que este es un tema muy relevante, no siempre recibe la atención adecuada, ya que la seguridad en el sector salud no está muy desarrollada.

Más allá de todas las áreas que se podrían ver afectadas en los servicios

LITORALPRESS MEDIA DE INFORMACIÓN http://www.litoralpress.cl

Fecha: 31/10/2017
Fuente: DIARIO FINANCIERO (SANTIAGO-CHILE)
Pag: 8
Art: 4
Título: CENTROS DE SALUD Y CIBERATAQUES

Tamaño: 18,4x19,9
Cm2: 367,0

Tiraje: 30.000
Lectoría: 42.230
Favorabilidad: No Definida

de salud en caso de un ciberataque, la privacidad de los pacientes, según los expertos, es una preocupación. Para el analista de software de IDC Chile, Jonathan Namuncura, durante los próximos años, cuatro de cada cinco empresas tendrán como prioridad la inversión en seguridad por los ataques de *ransomware* y *phishing*, donde la "vulnerabilidad de los datos y exposición de información personal son los principales riesgos ante los ciberataques en el servicio de salud", asegura.

PROTECCIÓN

El experto en ciberataques de Adexus, Héctor Kaschel, asegura que la mayoría de los problemas que enfrentan las compañías del área de salud se debe a que se adoptan medidas de prevención que, sin embargo, "muchas veces no están alineadas bajo normativas, estrategias y tecnologías de securización de sus activos". Por ello, asegura, la clave para resguardar la información "es implementar normas y políticas de seguridad formalizadas, que evidencien una política vinculada con el tema, alineada a los requerimientos del negocio y apalancada con tecnología para la protección de sus activos".

Dentro de las organizaciones, asegura el gerente de ingeniería de Consultora TI Vector, Eduardo Parada, se está trabajando en la revisión de sus procedimientos, respaldos, alfabetización digital de sus usuarios internos y en la incorporación de herramientas tecnológicas de detección temprana. "Todo esto, guiado por una consultoría integral, es capaz de minimizar las probabilidades de ataques y disminuye la exposición de la información de las instituciones", comenta.

Y es que los cibercriminales han ido cambiando la forma de aproximarse a sus víctimas. "Antes, los ataques se dirigían donde había grandes volúmenes de dinero, pero hoy esto ocurre donde hay menos control de la información", advierte el director de Desarrollo Digital de la Fundación País Digital, Marco Terá, debido también a la mala configuración de, por ejemplo, los accesos que son fáciles de identificar, lo que lleva por consecuencia a la fácil penetración de los canales y a la vulnerabilidad de éstos.

"Lo más crítico de los ataques es que pueden afectar todos y cada uno de los pilares de la seguridad, y todos ellos afectan la continuidad", comenta la directora de la Escuela de Tecnologías de la Información de la Universidad de Las Américas, Tania Gallardo, quien distingue dos áreas que podrían ser las más afectadas: la información de pacientes, debido a la vulnerabilidad de la confidencialidad, y la continuidad de los servicios, ya que se involucra directamente con la vida de las personas. Por eso, parece completamente relevante saber actuar de manera eficiente ante un ataque.

Gallardo cree que, independiente de todo lo que se pueda hacer, el mayor problema que está asociado a estos ataques es que "no existe forma de garantizar la protección".

Por eso, la demanda de las organizaciones por seguridad informática es una tarea que está siendo abordada por todos los sectores, ya sean privados, servicios públicos, proveedores tecnológicos y gobiernos.