Resumen Ejecutivo

CENTRO DE ESTUDIOS ESTRATEGICOS DE LA ACADEMIA DE GUERRA

REC N° 8/2020

Título del resumen ejecutivo	**:**	**La resiliencia cibernética de los sistemas de salud durante la pandemia de coronavirus.**
Título del documento original	**:**	**Addressing the Cyber Resilience of Healthcare Systems During the Coronavirus Pandemic.**
Autor (a)	**:**	Rebecca Lucas and Sneha Dawda, The Royal United Services Institute (RUSI)
Fecha	**:**	28 April 2020.
Contenidos	**:**	

El incremento de la utilización de la infraestructura digital que sustenta los sistemas de salud durante esta pandemia es una excelente razón para aumentar su seguridad

La seguridad cibernética del sector de la salud, tanto en el Reino Unido como en el extranjero, es un problema de larga data que persistirá después de que esta pandemia haya pasado. La pandemia ya ha alertado sobre los peligros de ignorar las debilidades de las plataformas de atención médica en cuanto a la resiliencia cibernética, habiéndose registrado múltiples incidentes, como el ataque de denegación de servicio al Departamento de Salud y Servicios Humanos (HHS) de los EE. UU. y varios ataques a hospitales checos. Sin embargo, la actual crisis de salud puede representar una oportunidad para que los gobiernos desarrollen resiliencia cibernética tanto en la asistencia sanitaria pública como privada.

La salud era y es vulnerable a los ataques cibernéticos

La infraestructura de salud digital ha sido históricamente vulnerable a numerosos tipos de ciberataques debido a que, por la naturaleza del sector, las organizaciones de atención médica son unas de las más propensas a conservar datos personales, siendo éste un problema de naturaleza global (los datos personales de 1,5 millones de ciudadanos de Singapur fueron robados en un ataque contra su infraestructura de salud el año 2018).

A lo anterior se agrega el que las compañías de atención médica destinan una proporción de los presupuestos de TI a la seguridad significativamente menor que otras industrias

(alrededor del 5% en EE.UU), pese a que el 83% de las organizaciones de atención médica de ese país informaron un aumento en los ataques cibernéticos en 2019.

En el Reino Unido, el daño causado por el ataque del ransomware WannaCry[1] 2017 evidenció las insuficiencias en los procesos de TI actuales, originando la adopción de medidas de seguridad, incremento de controles y mayor asignación de recursos. Aun así, el 67% de las organizaciones de atención médica en el Reino Unido experimentaron un incidente de seguridad cibernética en 2019.

Coronavirus enfatiza las vulnerabilidades actuales

Con el coronavirus actualmente dominando la vida diaria, la dependencia de la sociedad del sistema de salud nunca ha sido tan grande. Si bien algunos actores y grupos de amenazas han dicho que se abstendrán de atacar los servicios de atención médica, otros se han aprovechado de esta dependencia. La Interpol emitió un aviso de alerta para advertir sobre la avalancha de ataques cibernéticos en instituciones de salud críticas en medio de la pandemia mundial. Lo que complica aún más el problema es la división entre la infraestructura de salud pública y privada. En tiempos de crisis, no solo es imprescindible la seguridad cibernética de la infraestructura de salud pública, sino que también la resiliencia de la salud privada, por lo que debe tratarse en su conjunto.

Priorización de la resiliencia cibernética en atención médica

La mayor atención creada por la pandemia de coronavirus ofrece una oportunidad para que los encargados de formular políticas identifiquen vulnerabilidades en la infraestructura de salud pública bajo una tensión significativa, verificando cómo funciona la atención médica en tiempos de crisis. Por otra parte, la inversión cibernética y la gestión de riesgos no deben ser descuidadas por los proveedores privados de atención de salud, debiendo los gobiernos considerar las opciones de políticas para inducirlos a la inversión y la acción, ya sea a través de la regulación, la orientación o las normas.

La inversión en ciberseguridad en un mundo posterior al coronavirus está potencialmente en riesgo ante la previsión de una recesión económica importante y posibles recortes presupuestarios. El aumento de la atención pública combinado con la naturaleza crítica del sistema de atención médica brinda una justificación para concentrar los fondos y los recursos en un sector que ha sufrido significativamente los ataques cibernéticos.

Un sistema nacional de salud es tan resiliente como todos sus componentes. La seguridad cibernética en el sector de la salud seguirá siendo crítica mucho después de que se haya mitigado el daño del coronavirus.

JCVM/CEEAG

[1] Los ataques **Ransomware de la variedad WannaCry**, son ataques informáticos que usan el criptogusano conocido como WannaCry dirigidos al sistema operativo Windows de Microsoft.