SUGERENCIA 05/2021: *RANSOMWARE*

El ransomware es una amenaza real y creciente para cualquier institución o empresa, especialmente para aquellas que manejan datos de carácter personal. Recientemente hemos visto a entidades estatales del nivel del SEPE perder miles de solicitudes del paro y la gestión de los ERTE tras un ciberataque protagonizado por el ransomware *Ryuku* y pese a la traumática experiencia volver a tener un Ministerio paralizado por idénticas razones semanas después. Y no se trata únicamente de la pérdida de acceso a los datos, si no que en algunas variantes actuales el ransomware además de cifrar los datos del equipo que ataca es capaz de hacerse con ellos para posteriormente utilizarlos como extorsión en caso de que los datos extraídos sean sensibles. Por tanto es una cuestión seria que podría acarrear problemas muy graves frente a la que un Colegio Profesional tiene que estar preparado. Para ello redactamos este decálogo que puede servir para prevenir un ataque de estascaracterísticas y minimizar sus consecuencias en caso de ocurrir.

1. **Mantenerse conscientes del problema**. Es vital conocer las dinámicas básicas referentes a los cibertaques en general y los de tipo *ransomware* en especial (por ejemplo: se estima que más de la mitad de los ataques se inician desde ingeniería social, accediendo a lugares maliciosos, a través de spam, adjuntos no solicitados en correos electrónicos, *phishing*, etc.) y hacer conscientes de ellas a las personas más expuestas a dar paso a estos ataques en el Colegio: personal administrativo, secretarías técnicas y en general cualquiera que emplee servicios online desde equipos que contengan datos de carácter personal referentes a la entidad.

2. **Política de Seguridad**. Vinculado a lo anterior, es necesario que los Colegios elaboren unas directrices fundamentales que rigan todas las acciones relacionadas con la Seguridad de la Información dentro de la entidad. Sería deseable que esas directrices estuviesen plasmadas en un documento marco (que debería constar al menos mencionado dentro del documento de **Análisis de Riesgos**) y el contenido del mismo estar en conocimiento de todo el personal que pueda ser considerado como especialmente vulnerable a compromisos relacionados con la seguridad de los datos de carácter personal.
3. **Plan de Actuación**. Dentro de la Política de Seguridad mencionada, debería constar igualmente un plan de acción específico frente al escenario derivado de un ataque de *ransomware* en el que se especifiquen de forma clara los pasos a dar, tanto desde el punto de vista técnico (desconexión preventiva de los equipos afectados, desconexión a Internet y aislamiento de equipos en la red local, preparación de copias de seguridad, etc.) como organizativo (puesta inmediata en conocimiento del responsable informático, aviso a trabajadoras/es para evitar la expansión del malware, comunicación urgente al DPD en caso de compromiso de datos de carácter personal, etc.).
4. **Sistemas actualizados**. El software que empleamos es fundamental para evitar el riesgo de ser atacados. Nuestros sistemas operativos deben estar regularmente actualizados con los últimos parches de seguridad conocidos Por último debemos valorar el uso de sistemas menos vulnerables: evidentemente el uso de un sistema operativo como Microsoft Windows tiene una superficie de ataque mucho mayor que un GNU/Linux o un MacOS.
5. **Utilizar soluciones de seguridad preventiva**. Se deberían implementar medidas adicionales de protección como cortafuegos, antivirus o lineas de defensa (IDS/IPS) que también se han de mantener continuamente actualizadas. Adiconalmente siempre es una buena inversión contratar los servicios de profesionales de seguridad informática para que nos orienten e implementen medidas específicas adaptadas a nuestras necesidades concretas.
6. **Cifrado en origen de datos sensibles**. Los datos de carácter personal y especialmente aquellos que puedan ser sensibles deben protegerse siempre que sea posible con sistemas de cifrado que ofusquen su contenido para los atacantes. De esta forma estaremos protegiendo a los titulares de los mismos al tiempo que estaremos protegiendo al propio colegio de ulteriores extorsiones por parte de los ciberatacantes o incluso de demandas frente a las Autoridades de Protección de Datos en caso de fuga o brecha de seguridad.
7. **Redes Privadas Virtuales**. En la medida de lo posible sería muy recomendable emplear sistemas de conexión VPN para aquellos

accesos remotos que podamos estar haciendo en situaciones de teletrabajo a datos alojados en el colegio. De esta forma garantizamos un extra de protección en aquellos casos en los que tengamos que hacer uso de datos personales en contextos de red que pueden ser vulnerables a ataques. En ningún caso es recomendable emplear alternativas populares pero mucho más inseguras como accesos de escritorio remoto estilo Teamviewer y mucho menos manejo de contenidos e información por grupos de *WhatsApp*, adjuntos por correo sin cifrado o similares.

8. **Navegación segura**. Dado que muchos ataques de ransomware se inician también a través de la navegación web, es importante aplicar medidas que refuercen la seguridad en el navegador, como *add-ons* bloqueadores de *JavaScript* que impidan la ejecución de scripts maliciosos alojados en páginas web. En ese sentido es necesario evitar visitar páginas de contenido dudoso donde se pueden estar alojando Web Exploit Kits que dañen nuestros sistemas, básicamente haciendo un uso prudente de la navegación. Del mismo modo es fundamental mantener al día el software de nuestro navegador web.
9. **Sistemas de respaldo**. En caso de ser atacados por un malware de las características del ransomware, la única garantía para sobreponerse es poder recuperar eficientemente la información comprometida, por tanto es fundamental contar con un sistema robusto y eficaz de copias de seguridad, especialmente aquellos que se refuerzen con la conocida **Regla 3-2-1**: "*al menos 3 copias de seguridad, al menos 2 en soportes diferentes, al menos 1 fuera de la entidad.*"
10. **No ceder a la extorsión**. Aún cuando la situación sea desesperada, pagar el rescate y ceder al chantaje no es una buena idea, para empezar porque el pago no garantiza en absoluto la recuperación de los datos y abre las puertas a otros abusos posteriores y en segundo lugar porque llegados a ese caso antes de plantearse tal cosa es necesario consultar con un profesional que nos oriente en opciones alternativas, tanto desde el punto de vista técnico como jurídico.

Como véis es posible ser proactivos en la prevención del riesgo y hay mucho que se puede hacer para estar preparados frente a esta grave amenaza.

Enlaces de interés

- https://www.incibe.es/sites/default/files/contenidos/guias/doc/guiaransomwaremetad.pdf
- https://www.incibe-cert.es/blog/ransomware-ekans-prevencion-deteccion-y-respuesta
- https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware
- https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html
- https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/9476-ccn-cert-av-07-20-vulnerabilidad-en-teamviewer.html
- https://www.osi.es/es/search/node/ransomware
- https://www.osi.es/es/search/node/ransomware