30 de marzo de 2020

Ciberseguridad en época de pandemia

Desde que el COVID-19 llegara a nuestras vidas, primero como noticia lejana, después como una realidad aterradora, ha sido ingente la cantidad de información que hemos recibido y estamos recibiendo. Las empresas, especialmente las Pymes, pero también las grandes, se han visto afectadas en gran medida: ERTES, cierres, adaptaciones de los puestos de trabajo, problemas de abastecimiento, bajas, etc. Una avalancha de cambios y emergencias que se han intentado solventar de la manera más rápida posible, y como suele pasar, la improvisación y el desconocimiento no han dejado actuar con certeza y uno de los aspectos que se ha descuidado ha sido la seguridad, la ciberseguridad.

Desde la AEI de Ciberseguridad y Tecnologías Avanzadas nos vemos en la obligación de advertir sobre estos riesgos, tanto a empresas como a ciudadanos para **evitar que la crisis sanitaria y económica se vea agravada por una crisis de seguridad**. Por ello, nos hacemos eco de los medios oficiales como el Grupo de Delitos Telemáticos de la Guardia Civil, el Instituto Nacional de Ciberseguridad – INCIBE-, o la Policía Nacional, todos ellos expertos en detectar ciberataques y localizar ciberdelincuentes, y que estos días están trasladando numerosos consejos de gran utilidad. Además, contamos con la información aportada por las entidades miembro de la AEI, los grandes expertos en materia de ciberseguridad en este país.

Dadas las circunstancias hay tres áreas sensibles que están siendo el objetivo de los ciberdelincuentes para tratar de desestabilizar aún más la situación y beneficiarse con la obtención de datos: el **sistema sanitario**; el **Smart Working** (teletrabajo), que según datos de la Encuesta de Población Activa (EPA), sólo estaba disponible para 4% de las personas trabajadoras antes de esta crisis; y la **información relativa al COVID-19**, tanto a través de portales web que informan sobre la evolución del virus, como de Fake News, emails o incluso memes que corren de un usuario a otro.

Como muestra, podemos destacar algunas noticias que leíamos hace unos dias *"La policía detecta un ciberataque al sistema informático de los hospitales. Los autores querían secuestrar la información colándose en correos electrónicos enviados a sanitarios y pedir un rescate para recuperarla"*, o *"Interior alerta de una quincena de ciberestafas que utilizan como señuelo el coronavirus"*. Afortunadamente, también podemos leer *"El CNI lanza una operación para blindar la ciberseguridad de hospitales y el Gobierno"*.

En cuanto a la implantación del teletrabajo, se ha detectado que numerosas empresas han implantado medidas de teletrabajo sin la seguridad necesaria, sin firewall, redirigiendo puertos desde el router a servidores y ordenadores de la red local dejando importantes vulnerabilidades en el acceso remoto a sus sistemas, que pueden ser aprovechados para accesos no controlados. Desde la AEI aconsejamos que las empresas que requieran de estos servicios lo hagan a través de especialistas dedicados a la ciberseguridad, con una trayectoria contrastada, que garanticen las conexiones y los accesos a sistemas remotos.

Algunas de las medidas más importantes para evitar riesgos, tal y como explican INCIBE o el Centro Criptológico Nacional (CCN CERT) son utilizar una red privada virtual (VPN) para acceder a los sistemas de información de la empresa, priorizar los dispositivos corporativos, conectarse a redes wifi privadas, actualizar los sistemas operativos, antivirus y aplicaciones, utilizar contraseñas robustas y doble factor de autenticación o realizar copias de seguridad periódicas. El informe "Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia" elaborado por CCN CERT recoge una serie de pautas que permiten garantizar la seguridad de todas las herramientas y soluciones utilizadas en el teletrabajo para seguir manteniendo la confidencialidad, integridad y disponibilidad de la información, como si se estuviese en la oficina.

Otra de las grandes vías de riesgo es toda la información relativa al COVID-19. En un momento en que toda la población está ávida de recibir información, la poca prudencia o el desconocimiento hace que noticias falsas circulen por la red sin límites, teniendo como consecuencia un efecto de alerta o pánico innecesario o dando lugar a ciberestafas, robos de datos o pérdida del control de los dispositivos. Para muestra, algunas noticias: "Interior alerta de una quincena de ciberestafas que utilizan como señuelo el coronavirus. Los expertos policiales destacan la peligrosidad de una web que ofrece falsos diagnósticos de la enfermedad"; "Esta falsa app del coronavirus bloquea tu smartphone y pide un rescate".

Es importante trasladar a los ciudadanos algunas recomendaciones para aprender a distinguir una fuente fiable de la que no lo es, identificar aplicaciones fraudulentas o ciberestafas recibidas vía email. En su web, INCIBE cuenta con numerosos consejos a este respecto que os animamos a consultar.

Después de esta pandemia la vida no será igual, y como siempre existe algo positivo en cada situación, quizá a partir de ahora comprenderemos un poco mejor nuestras limitaciones y podamos abordarlas, seremos más conscientes de nuestras vulnerabilidades y podremos corregirlas en alguna medida, aprenderemos de los errores

y viviremos más alerta, seremos menos confiados, y por tanto un poco más seguros, ciberseguros.

Desde la AEI de Ciberseguridad, nos comprometemos con las empresas y los ciudadanos a trasladar información veraz y útil acerca de esta crisis y cómo sobrellevarla en cuanto a ciberseguridad en general y medidas dirigidas a empresas se refiere, contando con las aportaciones de todos nuestros socios, demostrando una vez más que unidos somos más fuertes.

Fuentes de información fiables recomendadas:

- **INCIBE – Instituto Nacional de Ciberseguridad**
  www.incibe.es/cibercovid19
  Teléfono 017. La línea de ayuda de INCIBE para incidencias de ciberseguridad
  Facebook: @incibe | Twitter: @INCIBE

- **OSI (Oficina de Seguridad del Internauta)**
  www.osi.es | Facebook y Twitter: @osiseguridad

- **CCN-CERT – Centro Criptológico Nacional**
  www.ccn-cert.cni.es | Twitter: @CCNCERT

- **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)**
  www.aepd.es | Twitter: @AEPD_es

- **GUARDIA CIVIL**
  Grupo de delitos telemáticos www.gdt.guardiacivil.es
  Twitter: @GDTGuardiaCivil y @guardiacivil
  Facebook: @GrupoDelitosTelematicos

- **POLICIA NACIONAL**
  www.policia.es | Twitter @policia | Facebook: @PoliciaNacional