LA CIBERSEGURIDAD EN TIEMPOS DEL COVID-19, MÁS IMPORTANTE QUE NUNCA

- **Hogares y negocios cada vez dependen más de la tecnología.**
- **Las ciberamenazas explotan el miedo y la incertidumbre durante esta pandemia.**
- **El aumento de horas en el hogar se traduce en un comportamiento online más arriesgado.**

A medida que la pandemia del coronavirus continúa poniendo a prueba los sistemas mundiales de salud, económicos, políticos y sociales, hay otra amenaza invisible en aumento, el riesgo de ataques de ciberseguridad que aprovechan nuestra mayor dependencia de las herramientas digitales y la incertidumbre de la crisis provocada por el confinamiento forzoso en nuestros hogares.

Hemos incrementado nuestra dependencia de la tecnología

Los casos de coronavirus reportados en el mundo abarcan más de 150 países, y la obligatoriedad del confinamiento lleva a las personas y empresas a tener una mayor dependencia de las comunicaciones por medios digitales. Internet se ha convertido en el casi único canal para la interacción y como medio de trabajo.

Hemos incrementado nuestra **dependencia de la tecnología**, las empresas, tanto del sector privado como público, continúan como pueden su labor incentivando el teletrabajo, y las comunicaciones entre personas prácticamente se reducen a las llamadas y videoconferencias, chats y los mensajes en las redes sociales. Del mismo modo, una buena parte de los servicios y de la información que ofrecen las diferentes organizaciones gubernamentales son accesibles por medios online.

En este contexto tan novedoso como poco común, un ataque por parte de ciberdelincuentes que limitara a los usuarios y empresas el acceso a sus dispositivos, sus datos o simplemente a Internet, sería devastador porque supondría la paralización de las operaciones.

Y poniéndonos en el peor de los casos, un ataque de este tipo podría causar fallos en las infraestructuras que pueden afectar incluso a ciudades, paralizando,

info@bcsc.eus | 945 010 059

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz

por ejemplo, la función de los sistemas de atención médica o a los servicios públicos en general.

Amenazas que explotan el miedo y la incertidumbre

Los ciberdelincuentes buscan imprudencias humanas para entrar en los sistemas. Cuando una situación de crisis se prolonga en exceso, tal y como está ocurriendo en la actualidad, la gente suele cometer errores que no habría cometido en circunstancias normales.

Se calcula que el 98% de los ataques se deben al uso de métodos de ingeniería social, y la creatividad de los ciberdelincuentes aumenta día a día con tal de acceder a contraseñas y datos personales o de especial interés. Para ello, se usan temas de actualidad para tentar a los usuarios y conseguir que cometan errores a la hora de pinchar en un enlace o abrir un mensaje adjunto en un correo electrónico.

Hemos vivido los casos de phishing y distribución de malware suplantando al Ministerio de Salud chino o la campaña de suplantación a la Organización Mundial de la Salud (OMS) en la que se solicitaba una donación que debía realizarse en forma de Bitcoins, con el objetivo de contribuir a la investigación de una cura contra el COVID-19.

Los casos de **extorsión** afectan incluso a los hospitales, con la constancia de un ataque a un hospital de la República Checa, así como mensajes dirigidos a personas de edad avanzada con amenazas de contagio si no se transfiere una cantidad de dinero determinada.

Y las **estafas vía web** proliferan sobre la compra de kits de prueba de virus, páginas fraudulentas orientadas a la recogida de donaciones para la investigación en una vacuna, o portales que ofrecen y venden todo tipo de productos en los mercados de Darknet.

Las imprudencias en materia de ciberseguridad se disparan

Por otro lado, no es algo consciente, pero **estar más tiempo conectados online**, nos lleva a **comportarnos de forma más arriesgada**. Por ejemplo, no es raro buscar accesos gratuitos a páginas web poco recomendables o buscar un software sin disponer del licenciamiento oficial, con lo que se abre una puerta a posibles ataques y a la instalación de malware.

No olvidemos que también puede haber riesgos ocultos en las tareas habituales relacionadas con la tarjeta de crédito o en la instalación de aplicaciones especializadas.

Normalmente es peligroso pulsar en enlaces de poca confianza, pero durante la pandemia esta acción puede ser realmente destructiva y tener un coste económico muy alto para quien la realice o para la organización en la que trabaje.

Concienciación y precaución, los mejores consejos de seguridad

El COVID-19 ha obligado a cambiar nuestros hábitos y rutinas diarias, pero también exige un cambio en nuestro comportamiento online:

- En la situación actual, donde en numerosos casos se utilizan dispositivos domésticos propiedad del empleado para acceder remotamente a redes de empresa, cobra especial relevancia que nuestros hogares sean ciberseguros.
- Hay que tener especial cuidado de a quién le cedemos la información personal propia. Conviene **tomarnos nuestro tiempo para comprobar** lo que estamos leyendo, lo que nos piden y dónde vamos a acceder.
- Por último, pero no menos importante, la mejor forma de actuar pasa **por mirar todo con lupa** y confiar solo en aquellas empresas, personas o instituciones de credibilidad solvente, así como en las agencias gubernamentales nacionales o locales.

Con el objetivo de ayudar a la protección de todos, desde el **Basque Cybersecurity Centre** hemos creado una sección específica sobre los riesgos relacionados y amenazas relacionadas con el coronavirus, y un kit de sensibilización con consejos, infografías específicas y una serie de documentos que contribuyan a prevenir la exposición frente a las ciberamenazas.

Y por supuesto, ante cualquier sospecha de haber sido víctima de un ciberataque, puedes ponerte en contacto con nuestro **servicio de asesoramiento frente a incidentes de ciberseguridad**, disponible las 24 horas del día, a través del número de teléfono gratuito 900 104 891 o enviando un e-mail a incidencias@bcsc.eus.

Recuerda que **el comportamiento personal responsable** es sin duda la llave para evitar la propagación de todo tipo de infecciones, tanto las físicas como las del mundo digital.

info@bcsc.eus | 945 010 059

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz