NOTA INFORMATIVA CIBERSEGURIDAD – GENERALITAT VALENCIANA – 4/AB/2020

De: informagv_5-bounces@listserv.gva.es [mailto:informagv_5-bounces@listserv.gva.es] **En nombre de** Nota informativa Ciberseguridad
Enviado el: sábado, 4 de abril de 2020 0:01
Para: informagv_5@gva.es
Asunto: Ciberseguridad en tiempos de la COVID-19

Resumen
Las autoridades han advertido de una campaña de ataques cibernéticos especialmente dirigidos contra el personal e instalaciones sanitarias que podría llegar a alcanzarnos. Las amenazas son reales. El impacto que podría tener un incidente grave en las actuales circunstancias sería enorme. La solución no puede ser sólo policial ni tecnológica. Necesitamos que permanezcáis atentos ante cualquier intento de fraude o engaño, especialmente por correo electrónico, y que hagáis un uso seguro de la información y de los medios tecnológicos. Para estos asuntos, la Oficina de Seguridad de la Información de la conselleria y CSIRT-CV estamos a vuestra disposición.

CiberCOVID-19

Las bandas cibercriminales no descansan. Las autoridades de todo el mundo encargadas de la vigilancia de las redes han detectado un recrudecimiento de los ataques especialmente dirigidos contra el personal y las instalaciones sanitarias. En los últimos meses han afectado a varios hospitales españoles y al Departamento de salud de EEUU. En Chequia han llegado a paralizar el hospital de Brno, el mayor del país, en plena crisis de la COVID-19.

En la Conselleria hemos detectado un pequeño incremento en el número de ataques (menos del 10%) y la situación en este aspecto es de relativa normalidad. Hasta ahora hemos intervenido a tiempo y los incidentes que han llegado a producirse son los habituales y de orden menor. Otros hospitales de nuestro entorno y de la Comunidad de Madrid no pueden decir lo mismo y en los últimos meses han sufrido incidentes que han afectado gravemente a su funcionamiento.

Ante esta situación es fundamental darse cuenta de la gravedad de la amenaza y adoptar las medidas de protección adecuadas, entre ellas las que se refieren al comportamiento del personal. Para entenderlas mejor y saber cómo y por qué debemos actuar conviene recordar cómo se produce un incidente.

El origen de la mayoría de incidentes

La manera habitual de lanzar un ataque es mediante el envío de mensajes por correo electrónico. Pueden ser indiscriminados o selectivos, dirigidos a un colectivo o a una persona concretos. Estos últimos son los más peligrosos porque suelen estar bien hechos y a la medida de la víctima (recuérdese el todavía reciente fraude millonario a la EMT de Valencia). Esos mensajes incluyen ficheros o enlaces a sitios infectados.

Si el receptor de uno de tales mensajes abre el fichero o hace click en el enlace, produce la descarga de un programa malicioso que infecta el equipo. Este programa hace varias cosas: se oculta, se multiplica e intenta propagarse en todas direcciones, pudiendo infectar todos los dispositivos conectados al equipo y todos los equipos de la misma red. Seguidamente, el programa despliega su actividad maliciosa, que puede ser de naturaleza muy variada: cifrar la información y pedir un rescate para recuperarla (ransomware), espionaje y robo de información,

utilización de la capacidad de cómputo del equipo para otras actividades (cryptojacking, o minado de criptomonedas), etc.

Lo que tiene de particular esta campaña es que los mensajes maliciosos son más sofisticados, están diseñados para engañar al personal sanitario y, a diferencia de ocasiones anteriores, están aceptablemente escritos en español o en valenciano/catalán. Los delincuentes saben que en esta situación de emergencia sanitaria somos más vulnerables a los engaños y hacen cuanto pueden para aprovechar la oportunidad.

Cómo actuar

Por todo lo anterior conviene estar alerta y extremar las precauciones. Para no dejarse engañar, las siguientes recomendaciones son tan básicas como efectivas:

1. Presta especial atención a los mensajes que recibes. El remedio para la COVID-19 no lo recibirás por correo electrónico ni por WhatsApp.
2. Suplantar la identidad del remitente de un mensaje de correo electrónico es relativamente fácil. También es un delito.
3. Las apariencias engañan: es fácil crear un mensaje o una página web falsos con aspecto parecido al del original.
4. Si recibes un mensaje sospechoso (SMS o correo electrónico), desconfía y comprueba su autenticidad.
5. No abras los archivos adjuntos, ni hagas clic en los enlaces de mensajes sospechosos.
6. No respondas a un mensaje de origen desconocido, ni pinches en el enlace para darte de baja de una supuesta lista.
7. Desconfía de quien te solicite datos personales o actuaciones no habituales.
8. No facilites NUNCA tus contraseñas a nadie, ni siquiera al personal técnico de soporte.
9. No descargues aplicaciones no oficiales para conocer el alcance internacional del COVID-19 (¡algunas están infectadas!).
10. El CCN-CERT ha elaborado esta infografía sobre mensajes maliciosos y phishing (338 KB).
11. Evita utilizar redes WIFI abiertas. Es más seguro usar conexiones 4G/5G.
12. Usa contraseñas robustas, actualízalas regularmente y evita reutilizarlas. Una frase suele ser una buena elección.
13. Mantén actualizados el sistema operativo y el software de seguridad de tus equipos personales.
14. Crea cuentas separadas para cada persona que use tu equipo personal y no concedas privilegios de administrador.
15. Cierra la sesión VPN cuando no la utilices. Vuelve a abrirla cuando te haga falta.
16. Al terminar de trabajar de forma no presencial, cierra siempre todas las sesiones que hayas abierto (utiliza las opciones "desconectar" o "cerrar sesión").
17. Presta atención a las carpetas “Descargas”, "Papelera de reciclaje" y "Mis Documentos". Borra lo que ya no sirva o no debiera estar ahí.

Si las advertencias anteriores llegaran tarde y hubieras hecho clic en algún enlace, o descargado y abierto un fichero adjunto de un mensaje malicioso, ponte en contacto cuanto antes con CATS o con la Oficina de Seguridad de la Información.

Entre el 50 y el 70% (a veces más) de los mensajes de correo electrónico que circulan por Internet son mensajes no solicitados (spam), muchos de ellos maliciosos. Si a pesar de los filtros que aplicamos llega un mensaje malicioso a tu bandeja de entrada, notifícalo a CSIRT-CV

(csirtcv@gva.es) con copia a la Oficina de Seguridad de la Información (osi@gva.es). Tomaremos medidas para desactivar la amenaza, de modo que si en el futuro alguien cae en el engaño no tengamos que lamentar las consecuencias. Ante otros intentos de fraude electrónico o por vía telefónica, por favor ponlos también en conocimiento de estas entidades.

Recordad que por más tecnología que se ponga, las personas somos la primera línea de defensa.

Muchas gracias por vuestra colaboración.

Un cordial saludo y mucho ánimo en nombre de todo el equipo.

REFERENCIAS

Las siguientes páginas contienen información fiable y permanentemente actualizada en materia de ciberseguridad. Corresponden a entidades oficiales. En ellas alertan sobre amenazas, desmienten bulos y ofrecen consejos y utilidades para el uso seguro de las redes.

- Centre de Seguretat TIC de la Comunitat Valenciana (CSIRT-CV): https://www.csirtcv.gva.es/
- Instituto Nacional de Ciberseguridad: https://www.incibe.es/
- Oficina de Seguridad del Internauta: https://www.osi.es/es
- CCN-CERT: https://www.ccn-cert.cni.es/cibercovid19.html
- Europol: How criminals profit from COVID-19 pandemic
- Agencia Europea de Ciberseguridad (ENISA): Ciberseguridad en hospitales (video)

Una observación importante sobre estos sitios: muchas de las recomendaciones están dirigidas al público en general, no al personal de una empresa o de una Administración Pública en su puesto de trabajo. El personal de la Conselleria no tiene permitido cambiar la configuración de los equipos informáticos de su puesto de trabajo, ni instalar en ellos ningún elemento software. Esas actuaciones sólo las hace, y debe hacerlas, el personal técnico autorizado por el órgano responsable de las tecnologías de la información y las comunicaciones, según el Art. 11 del Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat.

JuanMiguel Signes Andreu
Responsable de seguridad de la información
Oficina de Seguridad de la Información
Tel: 928042 (961 928 042); Móvil corp. 486020