BOLETÍN INFORMATIVO
Precauciones en el nuevo escenario de trabajo

Nuevo escenario de trabajo por el COVID-19

- **Nuevo escenario de trabajo por el COVID-19**
- **Riesgos y recomendaciones en el uso del correo electrónico**
- **El Teletrabajo**
- **¿Cómo podemos ayudar cada uno de nosotros?**

Durante las últimas semanas, los cibercriminales están aprovechando la **pandemia del coronavirus**, también conocido como COVID-19, para orquestar **múltiples campañas de ataques contra usuarios, empresas y organizaciones de nuestro país.** El procedimiento habitual consiste en el envío de millones de correos electrónicos falsos que pretenden hacerse creíbles aprovechando el clima social de miedo y desinformación. Esos correos persiguen o bien robar nuestras contraseñas o bien introducir "malware" que colapse los equipos y secuestre los archivos.

La necesaria implementación de sistemas de teletrabajo implica siempre una mayor exposición de los equipos informáticos y ello ha provocado un incremento inmediato en la distribución de esos virus, mayoritariamente de tipo **ransomware** a través, por ejemplo, del protocolo RDP, que es el que permite esas conexiones remotas de los usuarios. El número de conexiones y "puertos" se hace mayor, y las posibles brechas de entrada de "virus" se incrementan, especialmente al depender de equipos no corporativos con niveles propios de protección que suelen ser inferiores a los que habitualmente implementamos en los equipos corporativos.

Ante este nuevo escenario, las organizaciones, y la nuestra no es una excepción, deberán enfrentarse a estos riesgos**, asumiendo la existencia de peligros que se justifican por la necesidad de mantener operativa nuestra administración;** la adaptación continua de estrategias, herramientas y medidas de seguridad está garantizada pero el nivel de concienciación y conocimiento de los usuarios es absolutamente esencial. Del grado de concienciación de los trabajadores y trabajadoras de nuestra administración respecto al uso seguro de sus equipos informáticos depende, en parte importante, la continuidad de nuestras tareas.

Riesgos y recomendaciones en el uso del correo electrónico

Debido al envío masivo de correos que tienen como objetivo infectar los sistemas de las víctimas, se **identifica el email como el vector de ataque principal** elegido por los cibercriminales para llevar a cabo sus campañas actuales. Todo esto lleva a la necesidad de extremar las precauciones, así como a seguir una serie de prácticas a la hora de recibir correos, y muy especialmente de aquellos que en su asunto o contenido guarden relación con el COVID-19 o la pandemia.

Algunas de las **recomendaciones a seguir o datos a valorar**, para evitar o reducir los ataques son:

- Desconfiar de remitentes desconocidos: Con la implementación del teletrabajo así como el mayor uso del correo electrónico, se debe sospechar de todos los correos recibidos que no provengan de una entidad o persona de confianza, puesto que estos podrían ser malintencionados.

- Asumir que en el comportamiento concienciado de cada uno está la base para frenar la expansión de los correos infectados. Es preferible rechazar, borrar o no abrir un correo sospechoso que arriesgar nuestro equipo. Ante dudas, busque incluso confirmar con el remitente la calidad y origen del correo sospechoso.

- Prestar atención a los enlaces que figuran en los correos. Debe extremar la precaución con los enlaces recibidos puesto que no siempre son lo que parece a simple vista, por ejemplo, un correo malintencionado podría usar la URL de una entidad oficial pero el hipervínculo (visible al situar el ratón encima de la URL mencionada) podría redirigir a una página maliciosa de PHISHING o a la descarga de un fichero de malware. Ante cualquier duda, vale más no enlazar. Ojo también con los archivos adjuntos.

- No meter nunca sus contraseñas en formularios que aparezcan en una respuesta el texto del correo o en sitios webs a los que le lleven los enlaces. Recordar que todo correo con mala ortografía, idiomas extranjeros, remitentes desconocidos que parecen nombres foráneos o textos inconexos, es especialmente sospechoso. Es cierto que cada vez más cuidan ese aspecto formal, así que también un correo bien escrito puede conllevar peligro. Si además el correo incluye adjuntos, enlaces, o peticiones para que descargue archivos, su nivel de peligro aumenta.

- Los piratas informáticos han generado estas semanas muchos dominios con nombres relativos al COVID, eso implica que pueden recibir correos con asuntos que remitan a esas cuestiones y desde direcciones aparentemente legítimas, pero también son ataques camuflados.
- No podemos descartar que nos ataquen con PHISHING bien disfrazado que es aquel que hace que el remitente del correo malicioso que recibimos, usurpe la identidad de miembros de nuestra propia organización o de nuestra libreta de contactos.

El teletrabajo.

Los equipos informáticos del Principado han logrado organizar con gran celeridad una arquitectura de máquinas, permisos y accesos, que facilita el teletrabajo; de su buen funcionamiento depende que mantengamos operativas tareas esenciales para los ciudadanos. Pero el teletrabajo tiene características y riesgos que hay que conocer…

- Utilización de recursos personales (dispositivos, equipos, internet particular), más vulnerables a los ciber-ataques al presentar niveles de seguridad inferiores a los corporativos.
- Uso de sistemas corporativos que no estaban inicialmente diseñados para esta coyuntura y que tienen que reconfigurase o incrementarse con toda urgencia para soportar el nuevo tráfico y el uso remoto de aplicaciones y servicios. Todo ello puede derivar que en ocasiones aparezcan peores rendimientos o caídas.
- Los cibercriminales saben que el teletrabajo, y la deslocalización inusual de las personas, debilita nuestra seguridad; por ello intentan penetrar en los sistemas, robar datos, interferir en las videoconferencias, usurpar contraseñas o encriptar archivos. De todos los ámbitos el más atacado será siempre el de SANIDAD, dado que los datos que se mueven son

- El teletrabajo en la circunstancia actual de emergencia nacional llevará consigo ataques de ingeniería social; hemos hablado antes del PHISHING como riesgo esencial. **El Principado al igual que otras administraciones ya tiene encima varias campañas de correos fraudulentos intentando engañar a sus usuarios del ámbito sanitario. Nuestra seguridad ha bloqueado cientos de esos correos o desactivado sus archivos adjuntos infectados, pero seguirán entrando con asuntos como "datos del virus", "recomendaciones para COVID" o cualquiera otro que parezca un cebo "atractivo".**

- El teletrabajo obligará a algunos empleados a desplazarse por motivos de trabajo, ello puede incrementar el riesgo de robos o pérdidas de dispositivos. Igualmente en casa hay que controlar que, por error, familiares usen impropiamente esos equipos o accedan a nuestras contraseñas.

- El teletrabajo puede derivar, si no se ejecuta correctamente, en fuga o pérdida de información, al aumentar las posibilidades de conversaciones confidenciales en sitios inapropiados o al usar tecnologías a las que no estamos habituados. Evite usar WIFIs públicas para su teletrabajo y sea precavido a la hora de utilizar recursos como las videoconferencias.

- El teletrabajo no puede equivaler nunca a dejar de atender normas que nuestra Política de Seguridad impone.

Recuerde que:

La Administración del Principado de Asturias ha habilitado dos mecanismos de teletrabajo a sus empleados:

- Accesos a través de la plataforma proporcionada por el sistema de virtualización (CITRIX).
- Accesos a través de redes privadas virtuales (VPN).

Cada trabajador ha recibido manuales explicativos de las acciones a acometer para poder configurar sus ordenadores personales y así trabajar desde sus casas.

Se han de tener en cuenta que estos mecanismos posibilitan el acceso a recursos de la Organización que han de ser protegidos debido a la sensibilidad de la información en ellos contenida. **Hay que hacer un uso responsable y ello es incluso más necesario en los casos en que se accede a otras herramientas de trabajo utilizando el navegador WEB. Sea consciente de que los niveles de seguridad son inferiores a los que disfruta habitualmente desde la oficina.**

¿Cómo podemos ayudar cada uno de nosotros?

- Atendiendo a comunicados como este, dado que la concienciación es necesaria. Estemos alertas. Recuerde que las recomendaciones usuales relacionadas con la no difusión de información sensible, la protección y no compartición de contraseñas, o el uso de copias de seguridad o archivos cifrados son ahora totalmente aplicables. Pero no improvise o experimente en su equipo, si tiene dudas consulte con el CGSI.

- No proporcione información o archivos a contactos desconocidos o sospechosos y sobre todo no entregue nunca sus contraseñas como respuesta a un correo o una llamada telefónica.

- Estar en teletrabajo no le faculta para que comience a distribuir o guardar información corporativa en nubes, almacenamientos o aplicaciones, salvo aquellas que la informática del Principado pueda habilitar o permitir.

- Procure no mezclar las tareas del teletrabajo con las de ocio en su equipo personal, ni tener abiertas infinidad de pestañas y aplicaciones. No use su contraseña de trabajo también para tus redes sociales o cuentas de correo privadas

- Al finalizar el trabajo cierre todas las conexiones y sesiones abiertas, las pestañas de navegación, intente borrar incluso el historial de navegación y deje el equipo apagado.

- No dude en seguir informando de incidencias o sospechas al CGSI, que se mantiene a su disposición, pero entienda que las urgencias deben priorizarse. Y desde luego ante cualquier correo malicioso que detecte, por favor, avise de inmediato.

- Evite, si hace teletrabajo, las conexiones poco fiables (WIFI abiertas, redes públicas, equipos compartidos).

- Sea cauto cuando entre en videoconferencias y recuerde que las normas de protección de derechos de usuario siguen presentes y por tanto las grabaciones o difusiones se deben hacer con permisos y aplicando las normas rigurosamente.

- Organismos fiables, y con los que nuestra administración colabora, son el Centro Criptológico Nacional o el INCIBE. Durante estos días publican información referida a los ciber-ataques y a buenas prácticas en teletrabajo; es información de calidad que puede ser interesante conocer.

- No instale en su equipo, del cual depende ahora la calidad de su teletrabajo, software sospechoso o procedente de páginas y tiendas dudosas Se debe evitar instalar software o aplicaciones de las cuales se desconozca su legitimidad, para evitar que contengan ficheros maliciosos que infecten el sistema.