Teletrabajo: Las diez medidas que deben adoptarse para protegerse de los ciberataques en tiempos del COVID-19

Madrid, 26 de marzo de 2020 - La industria de la ciberseguridad asiste a un momento sin precedentes para demostrar que es un facilitador de seguridad indiscutible en el actual entorno digital al que se han visto abocados muchas empresas para combatir el COVID-19. Ahora, más que nunca, las organizaciones deben apostar por la ciberseguridad para proteger la multitud de información confidencial a la que acceden y comparten en su ejercicio diario y que en estos días se ha convertido en el principal valor de las organizaciones para poder continuar operando a través del teletrabajo. EY (antes Ernst & Young) ha elaborado una guía con las medidas de protección que deben adoptar los empleados y las compañías en el actual contexto empresarial y económico derivado del impacto del COVID-19.

Elena Maestre, Socia responsable de Consultoría de Riesgos y Ciberseguridad de EY, afirma: "Las organizaciones deben dar pasos adicionales en materia de Ciberseguridad, con la implantación de medidas más robustas, para evitar que el teletrabajo sea aprovechado por los ciberdelincuentes para llevar a cabo campañas maliciosas".

1. **USO DE ORDENADORES: Los trabajadores deben utilizar los equipos de la empresa (equipos maquetados con las medidas de seguridad adecuadas) al considerarse que son la opción más segura. Si no fuera posible, se recomienda verificar con el departamento de IT la posibilidad de utilizar otros ordenadores personales.**

2. **ACTUALIZACIONES CRÍTICAS: El empleado debe instalar regularmente las actualizaciones de seguridad relativas a sistemas operativos, versiones del navegador de Internet y las extensiones y complementos. Es necesario extremar el cuidado con software obsoleto y, por tanto, fuera de soporte.**

3. **USO DEL CORREO ELECTRÓNICO: Se recomienda no utilizar medios establecidos como inseguros y extremar las precauciones en el envío de correos electrónicos externos a la organización.**

4. **ACCESO A LA INFORMACIÓN: Las organizaciones deben mantener en el nuevo entorno de teletrabajo la protección de la información de la compañía, fomentando el uso de herramientas colaborativas seguras, mientras que los empleados deben comprometerse a no descargar, ni almacenar información corporativa en equipos o medios personales -siempre que sea posible-, así como a no compartir información sensible de la organización en esta nueva situación de teletrabajo.**

5. **SOLUCIONES DE SEGURIDAD: Las empresas deben establecer reglas sólidas de seguridad y monitorizar escrupulosamente todos los accesos y conexiones (tanto de administrador como usuarios) para identificar cualquier posible actividad anómala.**

6. **CONTRASEÑAS ROBUSTAS: Se recomienda fijar contraseñas robustas, que sean poco identificables y solo conocidas por el empleado, y cambiarlas periódicamente.**

7. **CONEXIÓN REMOTA: El trabajador debe conectarse a los sistemas de la organización usando sólo los mecanismos establecidos para ello, siendo a través de una Red Privada Virtual (VPN) lo más recomendable.**

   En el caso de conexiones realizadas desde casa, es necesario asegurarse de configurar el acceso WI-FI a través de una contraseña fuerte (nunca la que viene por defecto) y de no conectarse nunca a través de redes WI-FI públicas de procedencia desconocida.

   Asimismo, se debe proteger con contraseñas los envíos de ficheros con información sensible, a través de los mecanismos que la organización pone a tu disposición (WixAip, ZipMail, entre otros) y evitar tener conversaciones de trabajo en lugares públicos o en presencia de dispositivos inteligentes y asistentes virtuales.

8. **ANTIVIRUS: Es necesario tener activos los programas antivirus en los equipos y asegurarse de su frecuente actualización.**

9. **PHISHING Y SOFTWARE MALICIOSO: Se debe evitar abrir correos y enlaces de origen desconocido o sospechoso, así como desconfiar de cualquier petición de datos personales o credenciales de acceso y descargar aplicaciones móviles exclusivamente desde páginas o tiendas oficiales. Para todo ello siempre es recomendable reforzar el Plan de Concienciación.**

10. **FAKE NEWS: En los momentos de incertidumbre se prodigan las noticias falsas con el objetivo de provocar desinformación y alarma social. Por lo tanto, se recomienda no divulgar información que no provenga de fuentes oficiales y asegurarse de la veracidad de la información antes de difundirla.**