/Carey

Marzo de 2020

CIBERSEGURIDAD Y TELETRABAJO BAJO LA PANDEMIA DEL COVID-19

El COVID-19 y las restricciones de circulación que ha aparejado esta emergencia sanitaria, han acelerado de manera sustantiva la implementación teletrabajo por parte de las empresas en Chile y el mundo.

Sin perjuicio de los muchos aspectos positivos del otorgamiento de esta herramienta de flexibilidad laboral, estas decisiones deben necesariamente ir acompañadas de la evaluación, por parte de las empresas, de los niveles de protección de su información, y el análisis del inevitable aumento de los riesgos de ser objeto de ataques cibernéticos.

Con el teletrabajo, la información a la que normalmente acceden los trabajadores desde las instalaciones corporativas se ve diseminada a través de distintos medios que dependen de las herramientas tecnológicas con las que cuentan sus empleadores. Así, algunos trabajadores podrán llevarse los equipos portátiles que normalmente utilizan en sus empresas para trabajar desde sus casas; existirán aquellos que tengan a su disposición herramientas de conexión remota desde sus equipos personales; o en otros casos los trabajadores solo tendrán la opción de recolectar información relevante para dar continuidad a sus funciones, por medio de dispositivos portátiles como pendrives o a través de programas de almacenamiento en la nube, en cuyo caso almacenarán localmente en sus equipos personales la información para llevar a cabo sus compromisos laborales.

Desde el punto de vista de la ciberseguridad, no es indiferente qué tan preparadas están las empresas para llevar a cabo estos desafíos y qué mecanismos se están utilizando para ejecutar el teletrabajo. Las herramientas y medidas lógicas de protección que posee una red y un computador doméstico serán mucho menos robustas que las establecidas a nivel corporativo, como antivirus, firewalls, programas para detectar correos de phishing, bloqueo de sitios, entre otros; y en este escenario se hace indispensable desarrollar protocolos

Esta alerta legal es proporcionada por Carey y Cía. Ltda. con fines educativos e informativos únicamente y no pretende ni debe interpretarse como asesoría legal.

Carey y Cía. Ltda.
Isidora Goyenechea 2800, Piso 43.
Las Condes, Santiago, Chile.
www.carey.cl

informativos y obligatorios relativos a las medidas de seguridad (tanto lógicas como organizacionales) mínimas asociadas a las actividades de los trabajadores que están hoy desempeñando sus funciones desde sus casas.

Por otra parte, la pandemia del COVID-19 ha generado que las empresas hayan alterado profundamente los hábitos de tráfico de internet en sus servidores corporativos, volviendo más difícil detectar aquellos comportamientos inusuales que podrían corresponder a un hackeo. Si antes las empresas monitoreaban sus redes internas y las conexiones que entraban y salían desde aquellas redes, el teletrabajo les ha exigido el desafío de monitorear muchas conexiones que vienen desde afuera, ampliando intempestivamente su campo de control y aumentando por tanto los riesgos de ataques.

Adicionalmente, no podemos ignorar el componente humano de esta contingencia y cómo se han visto afectados emocionalmente los trabajadores. La preocupación y distracción de los trabajadores por el contexto del COVID-19 será un factor que facilitará comportamientos desacertados como la apertura de correos maliciosos, la instalación de aplicaciones riesgosas, errores en el ingreso o divulgaciones indebidas de contraseñas, entre otros; los que en conjunto crean un escenario vulnerable y atractivo para ataques. Esto se replica también en aquellas industrias que están operando bajo presión y altos niveles de estrés, como los clínicas y hospitales. Se han reportado preocupantes ataques de ransomware a hospitales en el mundo, como el que afectó recientemente al Brno University Hospital en República Checa, causando la interrupción de sus operaciones y la suspensión de las atenciones a pacientes. La razón de esto, es que los atacantes asumen que los hospitales estarán tan presionados para operar en su máxima capacidad, que tendrán altos incentivos para pagar los rescates exigidos, convirtiéndose en las víctimas perfectas en tiempos de crisis sanitarias.

Incluso desde el punto de vista de la diversificación de las comunicaciones que las jefaturas tienen con sus trabajadores con motivo del teletrabajo, los empleados precavidos tendrán igualmente mayor riesgo de caer en las trampas de phishing, por ejemplo, al no tener claridad de los canales de comunicación directos con los departamentos de TI, o porque habrá mayores barreras para requerir asistencia personalmente o consultar con sus jefaturas si determinados correos son o no maliciosos. La probabilidad de que

un empleado corrobore la autenticidad de un correo podría verse menoscabada.

En Chile no existe hoy un marco normativo que regule las obligaciones de ciberseguridad de los empleadores en relación con el teletrabajo, y por tanto es responsabilidad de las empresas auto-regularse en estas materias y concentrar los esfuerzos en la inversión de medidas a corto y mediano plazo. En el actual proyecto de ley de trabajo a distancia que ya se encuentra en tercer trámite constitucional en el Congreso (Boletín 12008-13), se incorpora una obligación de ciberseguridad para los empleadores, que incluye informar a los trabajadores acerca de los riesgos que entrañan sus labores, las medidas preventivas y los medios de trabajo correctos, y los obliga a efectuar capacitaciones, previo al inicio del teletrabajo, sobre las medidas de seguridad y salud que deben considerarse para el desempeño de sus funciones.

Por todas estas razones, la oportuna y costo-eficiente implementación de medidas para mitigar riesgos del teletrabajo en materia de ciberseguridad debe ser urgente y prioritaria en todas aquellas empresas que han puesto o que planean poner en marcha este mecanismo.

En este sentido, les recomendamos consultar el Protocolo de Seguridad para Trabajo a Distancia emitido recientemente por el Equipo de Respuesta de Incidentes de Seguridad Informática del Ministerio de Interior (CSIRT).

Ejemplos de medidas para mitigar los riesgos de ciberseguridad en el teletrabajo:

• Implementar políticas de ciberseguridad que contengan medidas mínimas en el teletrabajo y protocolos de notificación de brechas de seguridad. Estas políticas deben ser puestas en conocimiento y ser fácilmente accesibles por los trabajadores, y deben mantenerse actualizadas y auditadas periódicamente.
• Implementar y mantener actualizados Planes de Continuidad de Operaciones (COOP) y Planes de Continuidad de Negocios (BCP) de la empresa.
• Mantener constantemente actualizados los equipos corporativos y exigir la actualización de equipos personales utilizados para llevar a cabo funciones de trabajo a distancia.
• Usar redes privadas virtuales (VPNs) cuando la criticidad de la información lo amerite, para asegurar la confidencialidad e integridad

de la información accedida por los trabajadores.
• Impartir la instrucción de evitar conectarse desde redes públicas de WIFI en el desempeño funciones laborales a distancia.
• Promover la actualización constante de los routers domésticos de los trabajadores y exigir contraseñas robustas y confidenciales.
• Implementar herramientas de doble autenticación para el acceso remoto de los trabajadores a los sistemas de la empresa, ya sea a través tokens físicos, de aplicaciones de seguridad instaladas en los móviles de los trabajadores, o incluso a través de herramientas biométricas, cuando aquello sea proporcional con la sensibilidad de la información accedida.
• Promover la administración de permisos y usuarios diferenciados en los casos de trabajadores que se conecten desde equipos familiares, para mitigar el riesgo de acceso de información de la compañía por miembros del grupo familiar o terceros.
• Implementar un protocolo de detección de phishing, que obligue a los trabajadores a chequear los dominios de los que vienen los correos electrónicos recibidos y otorgue canales de comunicación claros y accesibles en caso de dudas.
• Uniformar los canales de comunicación de las jefaturas con sus trabajadores para evitar la entrega y divulgación de datos personales y/o contraseñas por medio de canales no autorizados.