CONSEJOS DE CIBERSEGURIDAD EN LA ERA DE TRABAJO REMOTO

Como se destaca en los informes recientes, los ciberdelincuentes y los actores de los estados nacionales ya están aprovechando este momento de pánico y desinformación para usar métodos de piratería tradicionales para robar datos, desde el uso de mapas interactivos con estadísticas de infección por Coronavirus para plantar malware en dispositivos hasta estafas de phishing donde los hackers se hacen pasar por oficiales de la CDC. Si bien la respuesta a COVID-19 se ha centrado correctamente en su costo humano, y mientras las organizaciones toman medidas para enfrentar la amenaza que representa COVID-19, también deben prepararse para el aumento en los riesgos de ciberseguridad que estamos viendo. A continuación se presentan consejos prácticos que se pueden implementar rápidamente sin la necesidad de reconstruir su infraestructura de TI o volver a redactar pólizas (lo que probablemente no será factible en el término inmediato).

- **Recuérdele a sus Empleados los Peligros de Phishing**. El termino phishing define una táctica bien conocida que los hackers han usado durante años, pero es una herramienta particularmente poderosa durante una pandemia global cuando las personas tienen más preguntas que respuestas. Los ciberdelincuentes ya han utilizado estafas de phishing para explotar sentimientos de inseguridad y pánico, y las personas corren un mayor riesgo de ser víctimas de tales esquemas en medio del caos y la irregularidad de sus nuevos arreglos laborales. Debería considerar enviarles a sus empleados un recordatorio para estar alertas ante intentos de phishing y recordarles que estén atentos a correos electrónicos externos y solicitudes inusuales de sus credenciales.

- **Instruya a sus Empleados Sobre las Mejores Prácticas de Trabajo Remoto**. Es posible que muchos de sus empleados no tengan una oficina en casa, una conexión a internet de banda ancha confiable o acceso a una impresora. Esto presenta riesgos de seguridad únicos que necesita abordar. Aquí hay algunas áreas en las que debería considerar brindar orientación.

    - *Redes WiFi Públicas*: A diferencia del ambiente de oficina, no podrá controlar cómo los empleados acceden a internet desde su hogar u otros lugares. Los empleados pudieran usar redes inalámbricas no seguras para hacer su trabajo. Para mitigar el riesgo de acceso no autorizado a la información de su organización, es posible que desee proveer a sus empleados instrucciones para

asegurar su red inalámbrica personal, por ejemplo, protegiéndola con una contraseña, restringiendo el acceso de red a dispositivos específicos y actualizando su enrutador de firmware regularmente. Si es posible, los empleados deben conectarse al entorno corporativo utilizando una red privada virtual, y configurar una para su organización toma menos tiempo de lo que cree.

- *Información Comercial Confidencial*: Recuérdele a sus empleados el manejo adecuado de la información comercial confidencial mientras realizan la transición al trabajo remoto. Si su empresa tiene datos confidenciales, es probable que no desee que sus empleados reenvíen correos electrónicos del trabajo a sus cuentas personales o que envíen información confidencial a una imprenta local para su impresión. Si un empleado ya tiene información confidencial en una copia impresa, debe considerar recomendar que se guarden las copias impresas hasta que puedan eliminarse adecuadamente cuando sea posible regresar a la oficina o utilizando una trituradora doméstica si hay una disponible.

- *Instalación de Software*: A medida que más empresas cambien a autorizar el trabajo remoto, los empleados y las empresas descubrirán una variedad de herramientas de software (para llamadas de conferencia y videoconferencias, por ejemplo) diseñadas para facilitar el teletrabajo. Debe tener cuidado. Considere designar cuales herramientas son las herramientas preferidas y aprobadas para tener cierto control sobre cómo se maneja y comparte su información.

- **Considere su Enfoque Hacia los Dispositivos BYOD ("bring your own device", en castellano "trae tu propio dispositivo")**. Permitir que sus empleados trabajen de forma remota supone que tienen los dispositivos para hacerlo. No todas las organizaciones emiten computadoras portátiles a los empleados, y los arreglos de trabajo remotos pueden requerir que las compañías permitan que sus empleados usen sus dispositivos personales para fines relacionados con el trabajo. Su organización deberá ser consciente de los riesgos de dicho enfoque BYOD. Al decidir si permitir dicho acceso, considere el riesgo que enfrenta su organización en vista de, entre otras cosas, la necesidad de que los empleados accedan a su red de forma remota, las protecciones de seguridad establecidas para permitir dicho acceso y el riesgo potencial de daño resultante de un compromiso de sus datos.

  - Una vez que haya estabilizado sus operaciones, puede considerar otros pasos para permitir el acceso seguro desde dispositivos personales como entornos de escritorio virtual y sistemas de administración de dispositivos móviles.

- **Asegúrese de que su Equipo de TI Pueda Responder a Incidentes de Forma Remota**. Su equipo de TI puede estar limitado en cuanto a cómo puede ayudar a sus empleados. Es posible que su equipo de TI en el sitio tenga que trabajar de forma remota e, incluso hasta si no tiene que hacerlo, con más empleados que no son de TI trabajando de forma remota, es posible que el equipo de TI no pueda proporcionar el mismo nivel de soporte que a los empleados presente en la oficina. Prepárese para estas limitaciones ahora. Debe asegurarse de que sus protocolos de respuesta a incidentes sean claros, que los incidentes continúen siendo marcados y escalados de manera apropiada según corresponda, y que el equipo de respuesta a incidentes pueda comunicarse utilizando comunicaciones fuera de banda si es necesario. Para lograr esto, necesita canales de comunicación claros y confiables para las partes internas y externas.

- **Revise y Actualice su Póliza de Teletrabajo**. Aunque la actualización de las pólizas puede no ser su primera prioridad entre los muchos pasos que deberá tomar para preparar a sus empleados para el trabajo remoto, debe considerar si los pasos de emergencia que está tomando son consistentes con su póliza de teletrabajo y dejar en claro que las excepciones a la póliza están siendo autorizadas debido a las circunstancias inusuales. Cuando el tiempo lo permita, y con el beneficio de las lecciones que ha aprendido de la respuesta inicial de su organización a COVID-19, querrá revisar su póliza de teletrabajo y asegurarse de que refleje con precisión sus prácticas y las mejores prácticas de ciberseguridad.