MARSH

PERSPECTIVAS | OCTUBRE 2020

Adaptación de los planes de respuesta ante los incidentes cibernéticos para teletrabajadores

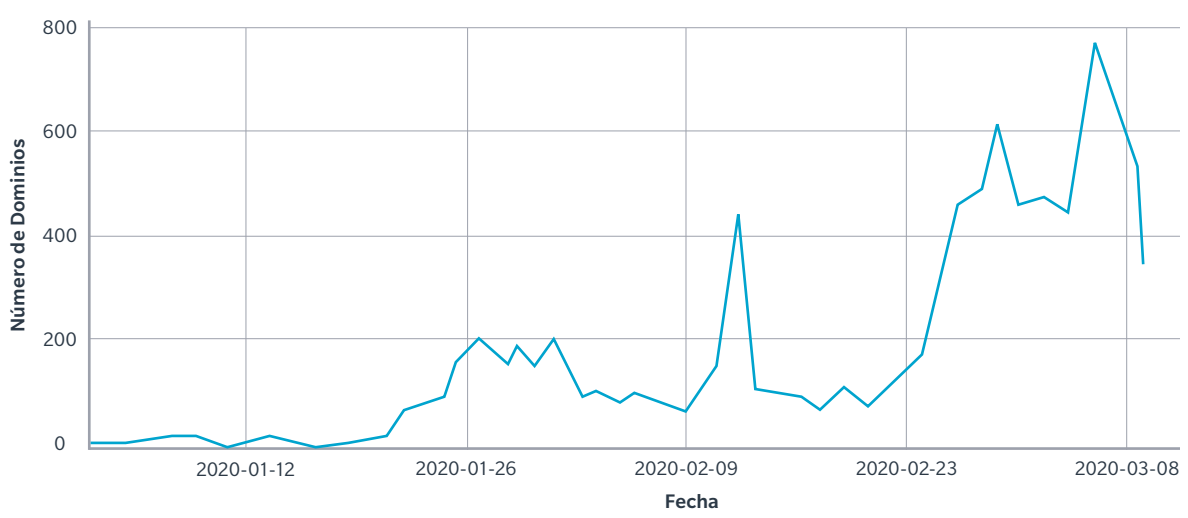
La pandemia de COVID-19 ha llevado a muchas organizaciones a saltar al plano digital con una fuerza de trabajo remota, lo que a menudo requirió que los equipos informáticos ampliaran rápidamente el ancho de banda disponible de la red y modificaran el modelo operativo "normal" para mantener el negocio en funcionamiento. Al prestar un mayor apoyo a los teletrabajadores, los equipos informáticos han podido pasar por alto algunos de sus procesos y procedimientos habituales, de forma que se infrinjan, debiliten o eliminen sus políticas informáticas y de seguridad.

Al aplicar sus soluciones de trabajo a distancia, las organizaciones han aumentado sin ser conscientes de ello sus riesgos operativos, especialmente en materia de ciberseguridad. Los actores más deshonestos no han pedido el tiempo a la hora de capitalizar estos riesgos, explotando las vulnerabilidades más comunes de la VPN, poniendo en marcha campañas de phishing dirigidas a los usuarios de las plataformas de comunicación y colaboración más populares, apuntando al Protocolo de escritorio remoto (RDP) de Microsoft y erigiendo infraestructuras de apoyo a las campañas maliciosas (véase la Figura 1 a continuación).

FIGURA 1

Dominios relacionados con COVID-19 creados a diario

FUENTE: *RECORDED FUTURE*.



MARSH & McLENNAN COMPANIES

Debido a que el entorno que abarca a esa fuerza de trabajo a distancia es más amplio, ¿debería su organización reconsiderar cómo responder a un incidente cibernético? Sí, y aquí está el porqué.

Los planes de respuesta ante los incidentes cibernéticos antes de la pandemia asumían que la mayoría de los empleados trabajarían in situ, en entornos controlados por la empresa. Ahora, muchos de ellos —si no la mayoría— de los empleados están teletrabajando en una amplia variedad de entornos. Estos entornos fuera de empresa pueden suman a la ecuación una gran cantidad de nuevas amenazas para las que los equipos informáticos y de ciberseguridad deben prepararse.

A medida que los equipos informáticos y de ciberseguridad refuerzan la ciberseguridad de sus organizaciones, es posible que no hayan tenido en consideración estos factores en sus planes de respuesta ante los incidentes cibernéticos (CIBR, por sus siglas en inglés) y cómo adaptarlos a la "nueva normalidad", así como a los incidentes cibernéticos que todavía pueden producirse.

Las deficiencias de seguridad son inherentes a muchas redes domésticas, que suelen ser de tipo "Plug and Play" y están diseñadas para funcionar con pocas opciones de configuración cuando los usuarios las ponen en funcionamiento. Las cámaras de seguridad física, los electrodomésticos, los interruptores de luz, las bombillas, los componentes estéreo, los monitores para bebés y otros dispositivos comunes suelen estar configurados para conectarse automáticamente a cualquier red doméstica disponible. Estos mismos dispositivos utilizan una amplia gama de protocolos y puertos para
comunicarse con los fabricantes y los usuarios a la hora de proporcionar unos cómodos —pero inseguros— servicios. Y estas mismas redes, cargadas de aplicaciones conectadas periféricamente, son las mismas que los teletrabajadores están usando para conectar a las redes informáticas corporativas, las cuales pueden o no estar conectadas a las redes privadas virtuales (VPN).

¿Cómo puede prepararse mejor para dar respuesta a incidentes cibernéticos en entornos remotos?

A medida que el teletrabajo a gran escala se convierte en parte de la nueva normalidad, es importante que los equipos informáticos y de ciberseguridad se preparen para la posible explotación de nuevas infraestructuras remotas. Específicamente, debería tener en cuenta:

- **Identificación de sus debilidades:** Elaborar un escenario cibernético del peor caso que involucre un evento de malware para el sistema informático de un teletrabajador, y luego realizar un ejercicio de simulación en base a este escenario. Al final del ejercicio, identifique aquello que salió bien y lo que no, y asigne al personal adecuado para abordar cualquier laguna y debilidad en su plan CIBR dentro de un plazo acordado. Su plan CIBR actualizarse como corresponda.

- **Revisión de sus configuraciones de base:** Revisar la implementación de una configuración básica del sistema informático de la fuerza de trabajo remota mínima aceptable que limite las actividades del sistema informático. Por ejemplo, evalúe la posibilidad de eliminar el uso de los puertos USB o de restringirlos a usuarios específicos que puedan necesitar acceso como parte de sus funciones y responsabilidades. Una vez que se establezca y se pruebe la línea de base, implemente este modelo con su fuerza de trabajo remota.
- **Implementación de revisiones de sistemas informáticos remotos y otros registros con mayor frecuencia:** Considere la posibilidad de implementar registros adicionales del sistema informático del teletrabajador que recojan y analicen sus datos para identificar actividades no autorizadas o cuestionables que pueda requerir un análisis más en profundidad. Automatizar la recopilación y el análisis de este registro de auditoría siempre y cuando sea posible.

Cuando planifique su respuesta ante un posible incidente de su plan de respuesta ante los incidentes cibernéticos mientras su fuerza de trabajo trabaja en gran medida a distancia, es importante que:

- Elabore los procesos y procedimientos necesarios con los que poder aislar los sistemas informáticos remotos individuales —o un grupo de sistemas informáticos que puedan funcionar juntos— para dar cabida al análisis e investigación cibernéticos que sean necesarios.
- Determinar la forma en que se llevaría a cabo el análisis ciberforense de los sistemas informáticos remotos, incluidos los procedimientos de la cadena de custodia.
- Prepárese para recopilar rápidamente los registros de los sistemas informáticos remotos y las imágenes de los discos duros de los teletrabajadores.
- Considere la forma de volver a poner en línea a los teletrabajadores seleccionados lo antes posible (si fuera necesario).

La preparación, planificación y realización de ejercicios de simulación sobre ciberseguridad (tanto los ejercicios técnicos como los que atañen a los cuadros ejecutivos) ayudarán en gran medida a su organización a aprovechar los beneficios de su fuerza de trabajo remota, al tiempo que contribuyen a la preparación a la hora de tratar de forma eficiente y eficaz los incidentes cibernéticos que se produzcan.

Para más información, contacte en Marsh a:

EDSON VILLAR
Líder de Consultoría en Ciberseguridad
Marsh Advisory
Edson.Villar@Marsh.com

GERARDO HERRERA
Director Regional
Marsh Advisory
Gerardo.Herrera@Marsh.com

PAULINA VÉLEZ
Líder del Seguro de Riesgo Cibernético
Marsh
Paulina.Velez@Marsh.com

PAULA ORDÓÑEZ
Líder de Productos Financieros (FINPRO)
Marsh
Paula.Ordonez@Marsh.com