Gestión de ciberincidentes durante el COVID-19

Fortaleciendo la capacidad de gestión de riesgos.

Durante un periodo de crisis como el que afrontamos en la actualidad ante la pandemia del COVID-19, es esencial que las compañías hagan hincapié en su capacidad de gestión de riesgos. Y en especial de la ciberseguridad y detección de fraudes, que pueden verse afectadas como consecuencia del teletrabajo masivo, la falta de recursos disponibles o incluso por la inoperatividad de los sistemas de control interno (automáticos o manuales).

Quizás sea innecesario resaltar que a nivel personal todos nos vemos afectados por esta situación con el pensamiento únicamente puesto en nuestras familias, nuestra salud, nuestro futuro. Pero no debemos olvidar que la naturaleza oportunista de los cibercriminales no cambia, incluso durante esta crisis. Siempre buscan vulnerabilidades y maneras de explotar debilidades: técnicas y humanas.

Lamentablemente, en la vorágine del COVID-19, ya se han detectado ciberataques específicamente diseñados para aprovechar el estado actual de las compañías. Por ello es indispensable incrementar la vigilancia y seguridad, y también la colaboración entre diferentes entidades e instituciones.

Con el objetivo de ayudar a reforzar la gestión de ciberincidentes en el marco de una crisis que afecta a todas las compañías a nivel global, es importante tener en cuenta los siguientes aspectos, que cubren no solo la prevención y detección, sino que hacen énfasis en la respuesta e investigación para que estas actividades se puedan realizar de una manera eficaz durante este periodo de incertidumbre:

Claves para mejorar la prevención y detección:

— Reforzar mensajes sobre las medidas de seguridad para el teletrabajo.

— Advertir sobre sobre el aumento de ciberataques que utilizan palabras como COVID-19 o Coronavirus, en particular ataques de phishing o en webs /apps maliciosas.

— Continuar gestionando proactivamente las actualizaciones de software/firmware, en particular de VPN, dispositivos de infraestructura de red y las aplicaciones para el teletrabajo.

— Bloquear accesos de RDP (Accesos remotos) abiertos, configurándolos por detrás del firewall y mediante VPN.

— Implementar autenticación multi-factor en conexiones remotas, incluida la VPN.

— Requerir contraseñas robustas en toda la red, con énfasis en usuarios administradores.

— Habilitar o reforzar los sistemas anti-spam y de escaneo automático de emails.

— Habilitar o reforzar las funcionalidades de detección/alerta disponibles en los sistemas.

— Reforzar la disponibilidad de sistemas de ticketing y notificación de incidentes por partes de usuarios. Considerar mecanismos alternativos en caso de una caída de red.

Claves para mejorar la respuesta e investigación:

— Contactar proactivamente con los proveedores de servicios (TI, ciber respuesta y forensic) para entender sus propios planes de contingencia y disponibilidad durante este periodo. Evaluar cobertura por bajas internas o externas y acordar medidas adicionales, por ejemplo con otro tercero.

— Acordar medidas específicas o alternas para establecer comunicaciones seguras entre el personal de respuesta (interno y externo), priorizar las tareas y la contención de incidentes.

— Revisar y actualizar los procedimientos de respuesta, considerando la necesidad de ejecutarlos en remoto.

— Repasar los protocolos de comunicación interna y externa, confirmando la disponibilidad de personas clave y métodos de contacto. Considerar mecanismos alternativos en caso de una caída de red.

— Asegurar que el personal de seguridad esté preparado para acceder y revisar remotamente los dispositivos de detección, incluyendo registros/logs de seguridad.

— Reforzar la gestión de backups, mitigando la posibilidad de su contaminación por malware y la necesidad de accederlos en remoto.

— Revisar los pasos a seguir para desconectar o aislar dispositivos/sistemas infectados, en remoto.

— Verificar la accesibilidad de los equipos de respuesta para recolectar muestras por ejemplo en caso de ransomware.

— Repasar requerimientos de preservación y análisis de evidencias con Asesoría Jurídica, en particular si se sospecha una brecha de información personal. Considerar la capacidad de banda-ancha en conexiones remotas, disponibilidad de servicios de digital forensics y funcionalidades forensic que varios sistemas ofrecen.

En tiempos de crisis, es importante compartir nuestros conocimientos y experiencia en la medida de lo posible, apoyándonos para contener y minimizar el impacto del COVID-19 en el sistema financiero y la economía en general. Los profesionales de KPMG conversan a diario con los líderes empresariales de Servicios Financieros y juntos seguiremos compartiendo nuestras perspectivas sobre cómo la industria está respondiendo a la crisis.

KPMG en Chile