Módulo 2

Día 7

Un aumento en tráfico DNS fuera de las horas de negocio es alertado por el sistema IDS de su institución, lo cual manda una alerta al equipo SOC. Luego de investigar los registros de sistema, el equipo SOC descubre que una cantidad considerable de datos fueron enviados desde el computador de un empleado de recursos humanos a una IP externa.

Día 9

Varios computadores de tu institución muestran una pantalla roja completa. Un mensaje de rescate aparece, indicando que se deben pagar 50 millones de pesos chilenos en bitcoin por la llave de descifrado. El mensaje también indica que los datos se harán públicos si no se recibe el pago en 48 horas.

Día 10

Una investigadora de ciberseguridad publica una serie de posts de un grupo de amenazas conocido en la Dark Web y contacta a tu organización. La investigadora cree que las publicaciones son genuinas, y que los actores de amenaza lograron acceder a datos personales y sensibles de clientes/pacientes/ciudadanos, o datos secretos (según aplique) de tu institución..

Día 11

El incidente de ciberseguridad aparece en artículos de diarios digitales. Un gran número de medios contactan al equipo de comunicaciones de tu organización haciendo preguntas sobre el incidente, como por ejemplo, si hubo o no exfiltración de datos personales.

Preguntas de discusión

1. **Discutan qué datos personales y sensibles pudo haber obtenido el atacante en su institución.**
2. **Definan un plan de ciber resiliencia para la organización y describan la infraestructura TI crítica necesaria para soportar funciones esenciales.**
3. **¿Cómo sabe su organización si hay actividad de red anómala?**
4. **¿Qué sistemas redundantes deberían existir cuando los primarios son comprometidos? ¿Qué alternativas manuales existen a procesos críticos? ¿Por cuánto tiempo se pueden ejecutar?**
5. **¿Cómo debo notificar? ¿Qué notifico?**
6. **Expliquen los pro y contras de pagar al atacante, además del valor de la información robada.**
7. **¿Cómo responde su institución a los medios? ¿Tienen mensajes prechechos? ¿Cómo comunicar a los clientes?**

8. **Luego de ejecutar lo anterior, qué desafíos identifican para mejorar la resiliencia de otras organizaciones.**