CC5327-1 Introducción a la Seguridad Computacional
Profesores: Alejandro Hevia A. y Eduardo Riveros Roca
Auxiliar: Sergio Rojas H.
Estudiantes: Andrés Calderón, Nicolás Arancibia, Martín Bahamonde y Martín Rojas

Caso de Estudio 4

Ransonware

P1. ¿Cuáles son las mayores ciber amenazas que pueden afectar su organización?

Una de las principales amenazas es el acceso a la información que está disponible en el computador robado, en especial considerando la falta de soporte ofrecido por el sistema operativo, de forma que sería posible obtener acceso a todas las plataformas y la arquitectura utilizadas por la empresa y que fueran accesibles por el empleado al que se le robó.

Del punto anterior se deriva otro problema, lateral phishing, dado que sería posible realizar phishing desde la cuenta de dicho empleado al que le robaron el computador.

P2. ¿Cuáles son los procesos de tecnologías de la información más críticos?

- Información pasajeros
- Información laburadores
- Sistemas de compras online
- Información aviones
- Backups

P3. ¿Cómo debería guardar tu organización sus respaldos? ¿Qué tan seguido? ¿Por cuánto tiempo deberían guardar respaldo? ¿Dónde deberían estar esos respaldos? ¿Cuánto tomaría restaurar los respaldos? ¿En qué formatos deben ser guardados?

Los backups deberían estar encriptados, de forma que no sea posible acceder a esta información desde dispositivos externos en caso de robo de computadores de algún empleado.

Los backups deberían realizarse cada mes, principalmente por datos importantes como las reservas y estos se deberían mantener durante 3 meses para tener suficientes respaldos.

Deberían estar guardados en un servidor central con acceso limitado a empleados capaces, sin acceso a red a menos que se requiera acceder a estos mismos por situaciones de urgencia.

Debería tomar a lo más unas pocas horas para mantener la continuidad del servicio.

El formato dada la cantidad de datos que maneja la empresa debería ser en alguna base de datos SQL para mantener acceso eficiente a los datos.

P4. ¿En qué temas entrenarías a los empleados de tu organización para prevenir los efectos de incidentes de ciberseguridad? ¿Cada cuánto tiempo deben completar el entrenamiento? ¿En qué momento debería hacerse el primer entrenamiento? ¿Cómo debiese cambiar el entrenamiento si el usuario tendrá privilegios administrativos? ¿Qué métodos de entrenamiento encuentras más efectivos?

Capacitaríamos a los empleados periódicamente sobre el phishing, para que puedan reconocer las formas de este (emails falsos o cuentas comprometidas), con ello, cuando detecten un mail puedan verificar su autenticidad, y si sus pc son comprometidos entrenarlos para que alerten a la organización posibles riesgos ASAP.

Depende de lo critico de la información manejada, pero sin saturar a los empleados, cada 6 meses es un buen periodo para hacer un modulo capacitador. Por otro lado el primer entrenamiento debería hacerse en las primeras 2 semanas entrado a la organización, como parte de su capacitación inicial.

Con privilegios administrativos, el entrenamiento debería ser similar al del trabajador inicial, mas algún modulo especial dedicado a sus permisos, para darle énfasis a que mientras mas escale en la organización mas crítica es la especialización (dependiendo sobre todo del cargo), en resumen, la capacitación es similar a la de los otros empleados pero con mayor enfasis para que el administrador adquiera una preocupación mayor.

Módulos de videos con cuestionarios al final del video donde se alerte a jefes de departamento si algún trabajador tiene un performance negativo, así los trabajadores tienen que prestar atención y responder a conciencia. Además de simulaciones de phising para que los trabajadores estén alerta (al menos 1 vez en el año en distintos periodos para no saturarlos).

P5. ¿Qué opinas del impacto de los ejercicios de phishing que hacen las empresas a sus empleados? ¿Qué debería hacer el departamento IT cuando correos sospechosos son reportados? ¿Cómo debería entregarse retroalimentación a los empleados que reportan phishing?

Son buenos en términos generales, puesto a que generan impacto en el empleado que fue victima de un posible ataque de pishing haciéndolo mas atento a ataques futuros.

El departamento de TI debería reportar al emisor del correo sospechoso a lo largo de la empresa y a la vez debería flagearse dentro de un sistema interno que el correo es posible emisor de pishing dentro de un futuro.

Debería hacerse un reconocimiento a los empleados para fomentar buenas practicas.