Universidad de Talca
Facultad de Ingeniería
Departamento de Ciencias de la Computación

Seguridad Informática

Tarea 2

Erik Regla
eregla09@alumnos.utalca.cl

11 de mayo de 2020

1. Enunciado

Definir una Política de Utilización de Dispositivos Celulares para una empresa.

2. Desarrollo

2.1. Contexto

Vamos a tomar el ejemplo de una empresa pequeña de consultoría de software con un área de ventas y un área de desarrollo, para así tener una diferenciación entre los niveles de privilegios globales. La empresa está basada en el uso de software Microsoft por lo que es necesario restringir en lo posible las herramientas a dicho ecosistema.

Una empresa que trabaja con software Microsoft (el cual es la mayoría del mercado en este momento), por lo general utiliza OneDrive/Sharepoint como herramienta de colaboración, Office365 para productividad y Azure para infraestructura. Estos tres recursos tienen un alto valor dependiendo del negocio y las politicas de seguridad implementadas para la segregación de contenido. Para efectos de este desarrollo se considera que existe una alta segregación de los privilegios.

El componente con el nivel de valor más alto de manera inmediata es el repositorio de documentos (OneDrive/Sharepoint) que es utilizado por el equipo de ventas. Si bien es de esperarse que el mismo repositorio tenga información sensible de clientes para el area de desarrollo, en el caso del área de ventas por lo general suele ser compartido con la gerencia y tienen información relativa a todos los clientes de la empresa (a diferencia de un área de desarrollo, la cual por lo general maneja solo información de sus clientes asignados). Debido a esto, nos vamos a centrar en una política centrada en esta unidad en específico.

2.1.1. Vulnerabilidades detectadas, probabilidad de ser explotada y costo

- Factores humanos: Es de esperarse que el área de ventas no tenga un conocimiento profundo en temas de seguridad y suelen tener un comportamiento más relajado que sus pares en otras unidades. La probabilidad de ser afectado por los mismos errores que son cometidos en un ambiente de trabajo son extremadamente altos, el almacenaje de contraseñas dentro del dispositivo, transferencia a medios locales de información sensible, etc.
- Factores físicos: La posibilidad de el robo de el dispositivo es alta como también el de su pérdida. Si bien en este último caso es responsabilidad del usuario, la intervención física del dispositivo es una realidad, por lo cual es necesario tener mecanismos para prevenir la exfiltración de información en caso de emergencias.
- Factores culturales: La cultura chilena es bastante pobre en términos del trabajo, ya que a muchos nos gusta *sacar la vuelta*. Esto deja a los dispositivos expuestos a su uso como unidades de entretenimiento, nevegación, etc en las cuales el riesgo de recibir información infectada es alta.

2.2. Políticas

2.2.1. Declaración de autoridad y alcance

Esta politica es diseñada por parte del SOC (security operations center) de la organización para velar por la seguridad de TI de dispositivos moviles del área comercial de la empresa.

2.2.2. Política de uso aceptable

- El usuario tiene prohibido extraer información de su dispositivo personal a otro medio físico.
- El usuario no puede utilizar otra SIM que no sea la provista por la empresa.
- El usuario no puede utilizar aplicaciones externas o fuera del ecosistema utilizado por la organización.
- No esta permitido realizar cambios al sistema operativo, hardware o estructura interna del dispositivo entregado.
- El dispositivo no podrá ser desconectado de su enlace a InTune bajo ninguna circunstancia.

2.2.3. Política de identificación y autenticación

- Para poder ingresar a sus dispositivos será necesaria la utilización de un PIN numérico de minimo 8 caracteres al momento de iniciar el equipo para luego ser autenticado por medio de su huella digital.
- Todos los usuarios deben contar con autenticación de doble factor y dos pasos.

- Todos los usuarios deben contar con un acceso a una VPN de privilegios y alcance restringido.
- Todos los dispositivos no deben presentar medios para poder establecer cambios al sistema operativo ni a su entorno. Esta medida consta pero no está solo restringida a uso de puertos como solo carga, eliminación de bootloader y mecanismos de recovery para particiones.
- Todos los dispositivos deben contar con encendido automático cada cierto número de horas.

2.2.4. Política de acceso a internet

- Todas las conexiones hacia los recursos de la empresa deben ser realizadas por medio de una conexión 4G y una VPN, no teniendo permitido el uso de redes IEEE802.11 diferentes a la de la misma empresa.

2.2.5. Política de acceso

- Para poder iniciar sesión en los recursos de la empresa es necesario proveer de la contraseña de la cuenta corporativa y una verificación de dos pasos por medio de Office365 S2-E5.
- Las conexiones a recursos de la empresa solo pueden ser ejecutadas por medio de las aplicaciones stand-alone correspondientes.

2.2.6. Política de acceso remoto

- El acceso remoto solo está permitido por medio de el uso conjunto de una VPN y la red inalámbrica.
- Las conexiones a recursos de la empresa solo pueden ser ejecutadas por medio de las aplicaciones stand-alone correspondientes.

2.2.7. Políticas del manejo de incidentes

En caso de robo o pérdida del equipo:

- Se debe dar anuncio inmediato a el SOC para iniciar el procedimiento de traza y de ser necesario de borrado de información.
- El SOC debe dar anuncio inmediato del evento a las autoridades pertinentes e iniciar los trámites necesarios para la obtención del equipo. El individuo afectado también deberá concurrir junto con el SOC para tales efectos.
- La gerencia debera gestionar la entrega de un nuevo dispositivo en un plazo no mayor a 5 días hábiles.
- De no ser posible la recuperación del dispositivo, se debe iniciar un procedimiento de eliminación e inhabilitación remota por medio del encendido automático.

En caso de mal uso:

- En caso de detectarse mal uso el SOC deberá emitir una carta de amonestación a la persona, la cual deberá acusar su recibo con su jefe directo. Esta carta solo será entregada como máximo tres veces, luego de esto será considerado una violación al código de seguridad de la empresa.
- En caso de reiteradas violaciones al código de conducta, el caso será derivado a la gerencia de recursos humanos para sus respectivas medidas o sanciones que estimen pertinentes.

En caso de ser victima de un ataque informático u sospecha del mismo:

- La persona afectada deberá dar cuenta al SOC de sus actividades y sospechas para que este pueda investigar en el problema.
- Se deberá hacer un security assesment para poder identificar los posibles afectados y comenzar con mitigaciones.
- De ser necesario afectado deberá hacer entrega de sus equipos digitales para ser examinados por el SOC y esclarecer el origen del problema y sus mitigaciones.
- El SOC deberá pasado el proceso de examen entregar los equipos limpios a su usuario para que este pueda retomar sus funciones.
- El incidente deberá ser archivado dentro de los registros del SOC. Dependiendo de la gravedad del incidente, este reporte puede ser elevado a otras unidades de la organización o bien a entes gubernamentales en acuerdo a la ley de protección de datos vigente actualmente en el país.