Seguridad de Sistemas Informáticos - práctica 1

Conceptos básicos de Seguridad

1. Califique el nivel de seguridad de los sistemas explicados en las siguientes narrativas, entre muy bajo, bajo, alto o muy alto. Indique para cada caso como se tratan cada uno de los 4 principios de la seguridad (integridad, confidencialidad, disponibilidad, irrefutabilidad). Indique luego si considera que el nivel de seguridad es adecuado o no adecuado para cada uno de los escenarios. Justifique su posición.

   a) Control de horario de personal I

   Cada trabajador debe firmar un registro al entrar o al salir de la empresa, indicando la hora a la que el evento ocurrió. El registro se toma como declaración jurada, por lo que es responsabilidad del trabajador poner datos certeros en el mismo. En caso de ser descubierta una irregularidad, el trabajador es penalizado. No se hace ningún tipo de control para verificar la veracidad del registro. La empresa tiene 5 trabajadores.

   b) Control de horario de personal II

   Cada trabajador debe pasar una tarjeta magnética y su dedo pulgar por un lector de huellas digitales al entrar o salir de la empresa. La información obtenida se carga en el sistema informático y solo está disponible para los que trabajan en personal. La empresa tiene 20 trabajadores. El lector de huellas requiere que el trabajador tenga las manos limpias y calientes para funcionar correctamente.

2. Haga el mismo análisis que se propuso en el ejercicio anterior para los métodos de autenticación multifactor expuestos en el apunte que lleva ese nombre y acompaña a este práctico.

3. Mencione dos ejemplos de Seguridad por Oscuridad.

4. Mencione dos ejemplos de Seguridad Paranóica.

5. Mencione dos ejemplos de Falsa Seguridad.

6. A partir de los siguientes textos, identifique (y cuantifique) amenza, vulnerabilidad, impacto y riesgo.

   a) “Se ha reportado una falla en el Software XX que puede permitir a un atacante predecir una clave generada automáticamente por el sistema. La falla se produce por una debilidad del generador de números pseudo aleatorios utilizado para la generación de claves. Esta falla puede ser utilizada por un atacante que en combinación con otros tipos de ataques puede, por ejemplo, ser explotada para recuperar las claves de administrador generadas automáticamente.”

   b) “Una falla en el Software YY podría permitir la ejecución remota de código arbitrario si un usuario visualiza un sitio web especialmente modificado. Si el usuario se encuentra acreditado con permisos de administración en un sistema afectado, un atacante podría tomar control total del mismo. Luego, el atacante podría instalar programas, visualizar, modificar, o borrar datos; o crear cuentas nuevas de usuario con todos los permisos. Aquellos usuarios cuyas cuentas no poseen permisos de privilegio en el sistema se ven menos impactados que aquellos que ejecutan actividades de privilegio.”

7. Mencionar 4 ejemplos de medidas que se pueden tomar para incrementar la seguridad de un sistema, calificándolas de precavidas, reactivas o preventivas/proactivas.