La autenticación fuerte: Un requisito indispensable para el uso nómada de las TIC

T13:Uso nómada de las TIC

Dr. José Domingo Carrillo Verdún

Profesor Titular de Universidad

Director Académico de los Masters de Seguridad y Auditoría Informática UPM-ALI

Universidad Politécnica de Madrid

Facultad de Informática

Índice

1. Introducción
2. La seguridad en los sistemas nómadas
3. Los sistemas de autenticación fuerte en el control de acceso
4. Implicaciones legales de estos sistemas
5. Conclusiones

Las demandas del nomadismo

- Conectividad 24x7
- Facilidad de acceso y soporte a todas horas
- Acceso a múltiples sistemas desde distintos dispositivos utilizando múltiples aplicaciones

- Seguridad en el control de accesos
- Gestión de Configuraciones
- Planificación de la Capacidad
- Diagnóstico Remoto
- Resolución de Problemas

2 – La seguridad en los sistemas nómadas

¿ Qué políticas de seguridad deben ser modificadas y reforzadas?

- Protección de Datos
  - Los dispositivos móviles son un objetivo fácil para los ladrones.
  - Los dispositivos móviles se pierden y dañan con frecuencia.
  - Los datos pueden ser destruidos o comprometidos
- Protección ante virus y ataques.
  - Dificultad para actualización de antivirus en ubicaciones remotas (visualización de los dispositivos)
  - Necesidad de actualizar virus en dispositivos fuera de la red
  - Escasa robustez de los dispositivos para resistir ataques de troyanos, phishing… (sistemas operativos, criptografia, programas …)

3 – La autenticación fuerte en los sistemas de control de acceso

Principios de diseño

- No deben mantenerse sistemas estáticos de acceso basados en una identificación del usuario y palabra clave fijas
- Procedimiento de autenticación obligando a que el Cliente se identifique a la Empresa y la Empresa al Cliente
- La autenticación debe ser fuerte haciendo uso de un doble factor de autenticación
- Impedir que el Cliente conozca todas las credenciales a intercambiar en la autenticación fuerte hasta que se haya autenticado la Empresa ante el Cliente.
- Las credenciales que se utilicen en la autenticación mutua deben ser de un solo uso (OTP) de forma que no puedan ser utilizada en operaciones posteriores

3 – La autenticación fuerte en los sistemas de control de acceso

Ejemplo de funcionamiento

- El Cliente dispone de un dispositivo de claves, proporcionado por la Empresa, cuyo contenido es conocido únicamente por dicha Empresa.
- Las claves son de un único uso (OTP) sin posibilidad de reutilización.
- El Cliente, cuando quiere identificarse frente a la Empresa, envía su identificador junto con una primera clave OTP proporcionada por su dispositivo de claves.
- La Empresa envía al Cliente una segunda clave, pareja de la primera clave recibida del Cliente, que la permite autenticarse frente al Cliente.
- Únicamente el Cliente, por medio de su dispositivo de claves, puede saber cuál es la segunda clave con la que la Empresa le debe responder.
- El dispositivo de claves proporciona una tercera clave al Cliente únicamente después de haber verificado la exactitud de la segunda clave recibida.
- Únicamente el Cliente puede saber cuál es la tercera clave que responde a la recibida de la Empresa por lo que su envío a la Empresa le permitirá autenticarse frente a ella.

4 – Implicaciones legales de estos sistemas

- La Ley Orgánica de Protección de Datos (LOPD) (Artículo 9).

Seguridad de datos : "El responsable del fichero, y, en su caso, el encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural."

- El estado de la tecnología antifraude ha evolucionado.
- ¿Cómo siguen existiendo sistemas críticos que se basan en un código de usuario y clave únicos?
- ¿Los sistemas antivirus y de detección de ataques de phishing realmente están impidiendo el acceso a los datos personales?

5- Conclusiones

- Los sistemas nómadas incorporan una gran complejidad , riesgo y responsabilidad a la gobernanza y gestión de la Seguridad.
- Se requiere una revisión profunda y estricta de la Política de Seguridad en muchas organizaciones.
- Deben incorporarse sistemas de autenticación fuerte en estos tipos de sistemas
- La Agencia de Protección de Datos debería analizar las implicaciones de los sistemas de autenticación actuales en los sistemas que pueden comprometer datos personales.
- La tecnología actual de autenticación tiene actualmente soluciones sólidas para evitar los fraudes como el phishing, troyanos o Man in the Middle.
- Las empresas, para la autenticación de sus clientes, deben aplicar estos sistemas de autenticación fuerte potenciando la seguridad y la confianza en los sistemas frente a la mal entendida comodidad del cliente.

Muchas gracias