BOLETÍN INFORMATIVO

001-2022

CONCIBER

Comité Nacional de Seguridad Cibernética

Limitación de Responsabilidad

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Comité Nacional de Seguridad Cibernética - CONCIBER puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

Aviso Legal

Contenido

Comité Nacional de Seguridad Cibernética – CONCIBER:

Este boletín informativo destaca la importancia que los Gestor de Comunidad implementen medidas de ciberseguridad desde un enfoque para la autenticación digital en el cual el nombre de usuario y la contraseña de un usuario final son gestionados por un tercero. Así como recomendaciones de ciberseguridad para su prevención.

En la actualidad los Gestor de Comunidad deben conocer los riesgos que acechan en el mundo digital, como la suplantación de identidad a través de técnicas de phishing, el registro malintencionado del dominio por parte de terceros o los ataques de denegación de servicio distribuido (DDoS).

Si bien es cierto que la presencia de las organizaciones en las redes sociales como Facebook, Twitter, Google+ e Instagram les reporta efectos positivos, existen diferentes amenazas que pueden generar impactos negativos en su imagen y reputación online, que muchas veces son irreparables.

Los Gestor de Comunidad trabajan con diferentes cuentas al mismo tiempo. Para su desarrollo profesional estos profesionales deben contar con algunos filtros de seguridad.

La ciberseguridad es uno de los campos esenciales en el desarrollo profesional de un buen Gestor de Comunidad. Es necesario estar advertidos ante ataques cibernéticos.
La reputación online del cliente recaerá en sus hombros como Gestor de Comunidad. Es preciso amplíe las precauciones al conectarse a Internet.

Implementación de medidas de prevención

BYOI (Lleve su propia identidad)

Este es un proceso mediante el cual las credenciales de inicio de sesión emitidas por un tercero otorgan al usuario acceso a múltiples servicios en línea. Con BYOI, el usuario inicia sesión en un proveedor de credenciales, que luego transmite un token de acceso (pero no las credenciales reales) al proveedor de servicios o al sitio web.

BYOI se ha convertido en el factor de autenticación de sitios web brindando una nueva experiencia de usuario. En lugar de solicitar a los navegantes crear un nuevo registro, el sitio web permite que se utilicen sus identidades sociales existentes como Facebook, Twitter, Google+ para iniciar sesión.

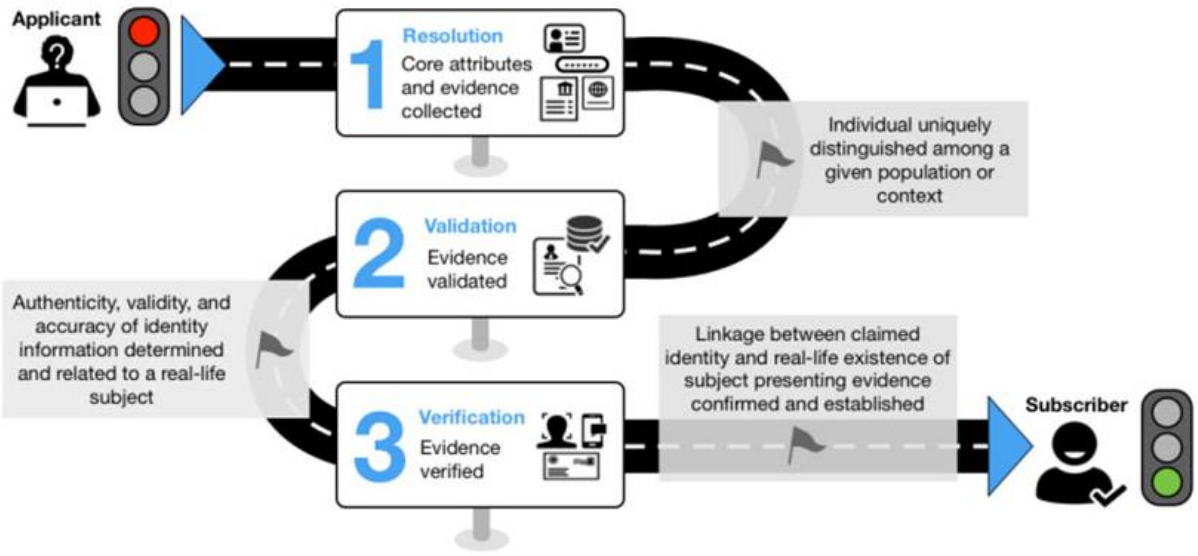

Figura 1
El proceso de prueba de identidad, según lo diagramado por NIST. (Instituto Nacional de Normas y Tecnología).

El Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) establece pautas para las agencias federales que utilizan pruebas de identidad en la Publicación especial 800-63A , definiendo tres niveles de garantía de identidad (IAL).

IAL1 exige "ningún requisito para vincular al solicitante con una identidad específica de la vida real". Por ejemplo, una cuenta de Twitter requiere solo una dirección de correo electrónico que funcione, y una cuenta de Google solo un número de teléfono móvil que funcione.

IAL2 exige algún tipo de identificación gubernamental, directamente o no. Cuando crea una cuenta bancaria en línea, generalmente está vinculada a una cuenta que creó en persona en el banco y para la cual proporcionó una prueba sólida de identidad.

IAL3 es el más estricto y exige algún tipo de presencia física. Registrar una cuenta en línea con el Servicio de Impuestos Internos de EE. UU. requiere no solo escanear una identificación del gobierno, sino también una videoconferencia con un representante de la compañía de prueba de identidad contratada por el IRS.

Medidas de Ciberseguridad

Si se desarrolla profesionalmente como Gestor de Comunidad debe tener en cuenta las siguientes recomendaciones. Como profesional manejara diferentes cuentas y administradores de contenidos así que es importante lleve un orden y siga algunas reglas relativas a la ciberseguridad:

1. Evite mantener cuentas en redes sociales o plataformas de publicación que no se utilicen y que puedan ser fácilmente vulneradas. Las cuentas olvidadas son en muchas ocasionas la fuente de mayor problema.

2. Incorpore mecanismos de doble autenticación en aquellos servicios en los que vaya a publicar algún tipo de información para reducir la posibilidad de suplantación. Establezca una periodicidad en el cambio de passwords para reducir riesgos.

3. Evite la unión de identidades que compartan credenciales a la hora de autenticarse en cuentas en las que publica contenidos.

4. Dado el caso, utilice dispositivos registrados y controlados desde los que realiza su función. No utilice dispositivos personales o no seguros (lo de utilizar el móvil personal para dar de alta una publicación es muy peligroso).

5. Monitorice la posibilidad de que existan cuentas suplantadas en la red que puedan estar actuando en contra de la imagen de la organización (phishing, fake news, etc.).

6. Verifique las condiciones de privacidad de cada cuenta que utilice, sea de una red social, una herramienta o un servicio corporativo de la organización para la que trabaja.

7. Limite y controle el número de cuentas que pueden actuar como Gestor de Comunidad dentro de la compañía. Supervise las acciones en redes de los empleados de la organización que tengan relación con la imagen corporativa.

8. Compruebe la integración de sus contenidos en portales, redes sociales asociadas, etc., para que no puedan ser manipulados sin su consentimiento.

9. Establezca niveles de control en las publicaciones para que nada aparezca en Internet sin haber pasado todos los procedimientos de autorización requeridos.

10. Defina una política de actuación en la que se recoja como notificar y actuar cualquier intento de atentar contra la imagen corporativa.

11. Realice auditorías periódicas sobre los recursos y los contenidos que publica, así como de las herramientas, procesos y procedimientos de trabajo.

Conclusión

BYOI tiene su lado complicado ya que el tema de seguridad a muchos podría preocupar por que se tiene que simplificar de una manera transparente y clara, el cual está en constante mejora. El usuario al usar identidades sociales para entrar a diferentes sitios webs, corren el riesgo de algún ciberdelincuente pueda acceder a todas estas cuentas si llega a desencriptar una de ellas.

Como en todo hay recomendaciones básicas para no involucrar BYOI con aplicaciones bancarias y financieras donde siempre será recomendable el uso de autenticación de doble factor.

Fuente de referencia:

https://www.scmagazine.com/resource/identity-and-access/bring-your-own-identity-and-the-need-for-robust-identity-proofing
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf
https://www.ubisecure.com/authentication/what-is-byoi-the-meaning-of-bring-your-own-identity-how-to-use-it/
https://niixer.com/index.php/2020/10/18/que-es-byoi/
https://searchsecurity.techtarget.com/definition/BYOI-bring-your-own-identity