Importancia de la identidad digital en el ámbito empresarial

Author : a.h.

Categories : Auditoría, Certificación y Calidad de Sistemas Informáticos

Date : 12 noviembre, 2018

En este segundo post me centraré en analizar la importancia que tiene la identidad digital en el mundo empresarial. Para ello, haré referencia a noticias y artículos que ratifiquen que el tema en cuestión es de plena actualidad.

Lo primero de todo, destacar la importancia que tienen hoy en día los datos. Estamos siendo bombardeados diariamente por términos como Big Data o IoT y esto se debe a que las empresas están comprendiendo el valor que tiene el uso de los datos. En el ámbito empresarial, los datos personales son considerados el nuevo petróleo [1]. Esto se debe a que los datos son cruciales en cualquier organización y su gestión un quebradero de cabeza para quienes tratan de garantizar la seguridad.

Precisamente hoy, 12 de noviembre, aparece una noticia en El Correo que bajo el título “Uno de cada dos robos de datos es mediante suplantación de identidad” nos muestra que el *phising* sigue siendo hoy la modalidad de ataque más sencilla y preferida por los atacantes. Mandando un email a la víctima que simula ser de su banco, pide sus credenciales y terminan apropiándose de su identidad digital. Es importante la concienciación de los trabajadores para evitar esta práctica pero también tomar acciones por parte de la empresa como configurarlos sistemas de red de manera robusta. Esto evita que los atacantes puedan obtener direcciones de correo electrónico e, incluso, nombres de usuarios [2].

Otra noticia relacionada con la identidad digital es la obra que se ha estrenado en Valencia llamada “Alexandria” que pretende hacer reflexionar al espectador sobre la información de publicamos en Internet y sus consecuencias. Es evidente que con todos los datos que cuentan de nosotros mismos los gigantes de la red, son capaces de crear perfiles de nosotros mismos. Es ahí donde la obra teatral realiza una crítica al respecto y plantea si realmente estos perfiles son una representación de lo que nosotros somos [3]. Relacionado con este último concepto de “perfil social” que se genera en Internet de nosotros mismos, el diario ABC publica que “el 35% de las empresas ha rechazado a un candidato por la imagen que ofrece en Internet” [4]. En este mismo artículo se muestra que el 83% de las organizaciones consulta las redes sociales de sus candidatos para conocer más información de ellos.

La identificación dentro de una organización puede llevarse a cabo mediante diferentes sistemas dependiendo de cuál sea el objetivo. Por un lado, existe la identificación física que se realiza mediante componentes físicos o la presencia del sujeto. Estos componentes pueden ser, por ejemplo, tarjetas de identificación RFID que funcionan mediante radiofrecuencias. Además del desgaste mínimo que sufren son muy difíciles de falsificar y pueden personalizarse para, por ejemplo, dar acceso a un empleado a un área determinado [5]. También se puede usar la identificación biométrica empleando por ejemplo la huella dactilar del empleado.

Por otro lado, el acceso a sistemas de información se realiza habitualmente mediante sistemas IAM (Identity and Access Management) que son en cuestión la mayor brecha de seguridad para una organización. Para realizar una buena gestión de este ámbito se establecen métricas en tres áreas: cobertura, actuación y comunidades de usuarios.

- La cobertura mide cómo el sistema afronta los diferentes riesgos y el impacto de los mismos.
- La actuación consiste en monitorizar los sistemas IAM y nos muestra su confiabilidad.
- Es importante que el administrador de los sistemas IAM comprenda las comunidades de usuarios presentes en la organización. Del mismo modo, debe comprender sus

respectivos perfiles de riesgo, países o hasta incluso las fuentes de datos autorizadas [6].

Por lo tanto, es esencial que los sistemas de autenticación sean meticulosos y precisos. A pesar de existir la autenticación física y electrónica, combinar ambas puede ser positivo en algunas ocasiones. Esto permitiría a los ciberatacantes no disponer de esa “llave” física. En el caso de que el atacante sea parte de nuestra entidad (insider threats) este método no solucionaría el problema pero este tema ya está siendo tratado en el Blog por uno de mis compañeros.

En los próximos post estudiaré a fondo los riesgos que conlleva este fascinante y espeluznante área de la identidad digital y analizaré qué controles existen mediante la auditoría para garantizar la seguridad de los sistemas.

---

[1] “Identidad digital - ISACA”, acceso el 12 de noviembre de 2018. https://www.isaca.org/Journal/archives/2017/Volume-6/Pages/digital-identity-will-the-new-oil-create-fuel-or-fire-in-todays-economy-spanish.aspx

[2] “Uno de cada dos robos de datos es mediante suplantación de identidad - El Correo”, acceso el 12 de noviembre de 2018. https://www.elcorreo.com/tecnologia/internet/robos-datos-mediante-20181112172924-ntrc.html

[3] “'Alexandria', una reflexión sobre la identidad digital - Las Provincias”, acceso el 12 de noviembre de 2018. https://www.lasprovincias.es/culturas/teatro/alexandria-reflexion-sobre-20181109011300-ntvo.html

[4] “Identidad digital, el factor que marca distancias en la carrera por el empleo - ABC”, acceso el 12 de noviembre de 2018. https://www.abc.es/economia/abci-identidad-digital-factor-marca-distancias-carrera-empleo-201810290301_noticia.html

[5] “¿Qué son y para qué sirven las tarjetas RFID?”, acceso el 12 de noviembre de 2018. https://www.inditar.com/blog/que-son-para-que-sirven-tarjetas-rfid

[6] “Obtain Greater Clarity Into Identity and Access Management by Establishing and Tracking Metrics - KnowledgeLeader”, acceso el 12 de noviembre de

2018.
https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/articleobtaingreaterclarityidentityaccessmanagement