**Privilegios sin control: la vulnerabilidad oculta que pone en riesgo a las organizaciones**

*Por Christian David López Chavero\**

Para que una persona realice su trabajo del día a día, requiere tener acceso a ciertas aplicaciones y sistemas de manera directa, rápida y segura. Un director de finanzas debe trabajar con información altamente sensible, que esté fuertemente protegida, un representante de ventas necesitará acceder a un sistema de gestión de relación con clientes (CRM) y utilizar sistemas especialmente diseñados para levantar pedidos, mientras que un empleado requiera trabajar únicamente con algunas plataformas administrativas y aplicaciones en la nube.

Determinar quién tiene acceso a qué y las acciones que puede realizar es un trabajo que involucra a diversas áreas de negocio tales como recursos humanos, seguridad de la información, áreas operativas y de TI, quienes se deben apoyar en la gestión de privilegios. Esto es, delinear el control de acceso por usuario, aplicación o regla, de modo que los usuarios tengan derechos específicos para ayudarles a realizar su trabajo, para brindar seguridad y optimizar la productividad.

No obstante, no son pocas las organizaciones que operan con una pobre o, incluso, nula administración de privilegios. En la práctica, es común asignar privilegios innecesarios en lugar de detenerse a realizar un análisis de roles y privilegios basado en el principio de la "necesidad de saber" (*need to know*), lo que ayudaría a disminuir el riesgo de acceso no autorizado.

En consecuencia, se descuida la ciberseguridad y, por comodidad, se asignan permisos más allá de los requeridos para usuarios técnicos y de negocio, dejando a la organización vulnerable a diversos tipos de amenazas. En un entorno empresarial, el director general y el director de recursos humanos deberían de tener derechos y atribuciones distintas y perfectamente delimitadas.

Se suma, además, una pobre cultura de ciberseguridad en la que los colaboradores comparten sus credenciales de acceso a diferentes sistemas, lo que puede potencialmente poner en riesgo procesos críticos o información sensible.

El escenario anterior representa, en muchos casos, una "enfermedad silenciosa" para las organizaciones. Mientras detener un proceso operativo crítico es algo notorio, ya que sus efectos se hacen evidentes en la continuidad del negocio, una administración deficiente o nula de privilegios puede estar teniendo impactos no tan visibles. Es sólo cuando se produce un ataque, un fraude o un error que vemos las consecuencias devastadoras de haber sido negligentes al no contar con una adecuada administración de privilegios.

**Seis preguntas que hacerse para medir el riesgo**

Contar con una gestión y gobierno de privilegios adecuados puede ser una tarea compleja y demandante. También es importante señalar que tener una herramienta especializada de gestión de identidades y accesos no garantiza que los controles establecidos sean efectivos. Un diseño deficiente, errores en la configuración o no aprovechar adecuadamente sus capacidades pueden conducir a los mismos problemas que cuando se carece de dichos controles.

Cada organización, de acuerdo con la industria en la que opera, su tamaño y sus propias necesidades, requiere una estrategia a medida que le permita minimizar efectivamente los riesgos asociados. Para ello, es fundamental que se planteen preguntas básicas que les pueden ayudar a conocer su posición en lograr afrontar dichos riesgos.

* ¿La organización cuenta con procedimientos establecidos y aprobados por el área de seguridad y/o cumplimiento para asignar privilegios?
* ¿Existe trazabilidad de qué privilegios se asignaron a qué recurso y quién autorizó dichas asignaciones?
* ¿Se definen y ejecutan procesos periódicos de certificación de accesos, así como la correspondiente remediación de las desviaciones encontradas?
* ¿Se han definido roles en función de las necesidades del negocio de la organización?
* ¿Existen matrices de segregación de funciones para minimizar el riesgo de fraude?
* ¿La administración de privilegios se está llevando a cabo de manera efectiva?

Si las preguntas anteriores se responden negativamente, es un indicio de que es necesario prestar atención a la administración de privilegios, a la vez que alerta a no caer en una falsa sensación de seguridad basada en el hecho de que "nunca ha pasado nada".

En resumen, la organización debería ser capaz de responder, en cualquier momento, quién o qué tiene acceso a qué recurso, cuándo y desde dónde, así como la razón por la que se les ha asignado determinado acceso.

Sobre el autor

*\*Christian David López Chavero\** es líder de la Unidad de Negocio de Digital Identity para Minsait México. Por más de una década, Christian ha sido un referente en proyectos de ciberseguridad, con un enfoque destacado en la gestión de identidad y acceso (IAM). Su experiencia se ha moldeado a lo largo de roles clave, desde posiciones técnicas y escalando hacia funciones de liderazgo y asesoría para definir estrategias de gestión y gobierno de identidades & accesos para diversas entidades.