Introducción a la identidad - Parte 2: Administración de acceso

Por Pamela Dingle

Tabla de contenidos

Resumen

¿Quién eres y qué tienes permitido hacer? En un sistema digital estas preguntas son el dominio de la Administración de Identidades y Accesos (IAM, por sus siglas en inglés). Los sistemas de administración de acceso proveen los mecanismos para decidir quién es quién y para evaluar y ejecutar las decisiones sobre quién debe tener acceso a qué. Esta segunda parte de la introducción de la identidad del Cuerpo de Conocimiento de IDPro aborda un panorama general de la administración de acceso desde una perspectiva histórica. Por lo tanto, en este artículo encontrarás algunas recomendaciones, mucho contexto y un pantallazo general de lo que hacemos en la administración de accesos y por qué nuestras contribuciones son importantes.

Terminología

- Ceremonias - Son interacciones predecibles que los usuarios ocasionalmente afrontan en espacios bien vigilados.
- Infraestructura de autorización delegada - Es un marco de control de acceso que separa la autenticación de la autorización, permitiendo que la contraseña se mantenga local y protegida.[1]
- Identidad federada - Son los medios para enlazar la identidad electrónica y atributos de una persona, almacenados en múltiples y diferentes sistemas de administración.[2]
- Mínimo privilegio - También conocido como el principio de mínimo privilegio. Es un principio por el cual un recurso, como un usuario, puede acceder únicamente a los recursos (como aplicaciones, datos, etc.) que son necesarios para el cumplimiento de su función.[3]
- Federación de confianza - Es un marco de confianza entre múltiples entidades para usar información de identidad y de administración de accesos de manera controlada.
- Confianza cero - De acuerdo con el Borrador de la Publicación Especial NIST 800-207, "La confianza cero implica que no hay ninguna confianza garantizada en un recurso o cuenta de usuario basándose únicamente en su ubicación física o de red (por ej. redes locales versus Internet)."[4]

Introducción

¿Qué es la administración de acceso y por qué es tan interesante? El momento en que se toma una decisión es emocionante y apremiante: una puerta se abre y un recurso valioso se pone a disposición de un extraño. ¿Habilitamos a la persona correcta para que ejecute su trabajo o cometimos un peligroso error? Una buena administración de acceso depende de buena información de identidad; también requiere políticas que estén en concordancia con las reglas corporativas, una correcta comprensión de los factores del entorno y contexto actuales y herramientas que se ejecuten en función de una tolerancia de riesgo definida. Se necesita mucha preparación y ponderación de las decisiones diarias que se toman durante la ejecución y que operan con todo tipo de granularidades en la infraestructura, *middleware* y capas de aplicación.

---

[1] Raible, Matt, "¿Qué diablos es OAuth??" *DZone Security Zone*, 28 de abril de 2018, https://dzone.com/articles/what-the-heck-is-oauth.

[2] Contribuyentes de Wikipedia, "Identidad federada," Wikipedia, La Enciclopedia Libre, https://es.wikipedia.org/wiki/Identidad_federada (consultado el 6 de junio de 2020).

[3] Contribuyentes de Wikipedia, "Principio de mínimo privilegio," Wikipedia, La Enciclopedia Libre, https://es.wikipedia.org/wiki/Principio_de_m%C3%ADnimo_privilegio (consultado el 6 de junio de 2020).

[4] Rose, Scott, y Oliver Borchert, Stu Mitchell, Sean Connelly, "Arquitectura de confianza cero (2do borrador)," SP 800-207 (borrador), Instituto Nacional de Estándares y Tecnología, febrero de 2020, https://csrc.nist.gov/publications/detail/sp/800-207/draft.

Si eres un profesional de la identidad con experiencia, habrás visto nuestras herramientas evolucionar - pero si recién comienzas, es importante que tengas un poco de perspectiva sobre por qué las cosas son como son. Abróchense los cinturones: esta introducción no es ni remotamente objetiva, pero ofrecerá una perspectiva sobre cómo llegamos hasta aquí y sobre cómo los conceptos que abordaremos más adelante en el artículo evolucionaron hacia nuestro panorama actual de la administración de acceso.

Para comenzar este recorrido, a continuación, encontrarás algunas realidades fundamentales a tener en cuenta en el mundo de la administración de acceso.

Los recursos necesitan estabilidad

Los secretos de empresa, las transacciones financieras y las comunicaciones personales son solo algunos de los ejemplos de los recursos valiosos que los profesionales de la identidad están encargados de proteger. Los recursos pueden ser divulgados mediante Interfaces de Programación de Aplicaciones (API, por sus siglas en inglés), interfaces web o aplicaciones móviles nativas. Incorporar capacidades de administración de acceso externalizadas a un único recurso es relativamente fácil, pero incorporarlas a cientos o miles de recursos es agobiante. Los dueños de aplicaciones rara vez quieren realizar cambios y menos aún quieren realizarlos con frecuencia. Después de la primera vez que te toque programar una actualización en una aplicación de administración de acceso para cientos de aplicaciones diferentes, pensarás igual.

Los recursos no deben realizar una administración de identidad local

Si cada recurso que despliegas realiza sus propias funciones lógicas, es casi imposible garantizar que se cumplan las mejores prácticas como las detalladas en NIST 800-63B o que se lleven adelante políticas corporativas consistentes.[5] Cuando muchas aplicaciones almacenan credenciales, protegen una página de inicio de sesión y garantizan un proceso de recuperación de cuenta seguro cada una por su lado, se genera una superficie de ataque enorme y los usuarios son más propensos a reutilizar contraseñas a lo largo de las distintas aplicaciones. Este patrón arrastra el peligro de que, si un atacante descubre la contraseña, tendrá acceso a una credencial que puede reproducir para acceder a otras aplicaciones...y no tienes forma de medir el alcance de este daño, es decir de saber qué aplicaciones pueden ser o fueron afectadas.

Los humanos necesitan desafíos, pero no obstáculos

Mientras que los recursos necesitan estabilidad y consistencia, los humanos necesitan empatía. Obligamos a los usuarios a interactuar con sistemas informáticos para que

[5] Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, y Justin P. Richer. 2017. Directrices de identidad digital: autenticación y gestión del ciclo de vida. Reporte técnico. Publicación Especial NIST 800-63B.

demuestren que son el operador correcto de la cuenta digital de la que reclaman tener derecho a acceder; este proceso debiera ser fácil para un usuario legítimo y difícil para un impostor. La mejor práctica es crear "ceremonias" - es decir interacciones predecibles poco frecuentes que los usuarios pueden abordar en un entorno bien vigilado. Si bien la autenticación es la ceremonia más conocida, hay muchas otras situaciones en las que los humanos están obligados a interactuar como en el registro o la recuperación de una cuenta de manera autogestionada, en respuesta a notificaciones o para aprobar transacciones. Queremos que los usuarios estén informados cuando ocurre una ceremonia fuera de lo común porque podría estar alertando de un fraude. Las ceremonias cambian siempre porque los nuevos ataques obligan a los administradores a probar técnicas nuevas o adicionales que incluyen cambios en la experiencia de usuario (UX, por sus siglas en inglés), en los factores de autenticación y en la detección de riesgos. Si bien es importante mantener los ataques a raya, la experiencia de los usuarios legítimos es extremadamente importante. Al verse enfrentados a un problema difícil, los humanos suelen comportarse de forma predecible y esta predictibilidad es un vector de ataque en sí misma. Si como administrador le complicas la vida a los usuarios, tú te conviertes en el problema: los usuarios van a intentar a toda costa evitar los controles que implementaste para protegerlos.

Basura entra, basura sale

Las partes más visibles de la administración de acceso son las decisiones que se toman en el momento. Estas decisiones no salen de la nada. Antes de que cualquier decisión sea tomada, alguien tiene que establecer reglas digitales y políticas que estén en concordancia con los objetivos de negocio de la organización (vea "Introducción a la gestión de proyectos IAM" para más información sobre la gestión de proyectos IAM).[6] El contexto de usuario, de grupo y de rol debe existir al igual que una combinación con el contexto de dispositivo, de red y de riesgo. Toda la información que deba considerarse en una decisión de acceso debe estar disponible al momento que el usuario intente acceder a un recurso determinado. Nunca olvides que: si las decisiones se basan en entradas incorrectas, no importa lo buena que sea tu infraestructura de administración de acceso.

Ahora vamos a la parte divertida

Los profesionales de la identidad terminan enfrentándose a problemas ancestrales. Tenemos recursos que proteger, usuarios que quieren accederlos y atacantes que quieren lo mismo y son muy difíciles de diferenciar de los usuarios legítimos. Necesitamos un sistema que sea preciso pero ningún sistema es 100% preciso y es por eso por lo que el sistema debe seguir el principio de confianza cero, otorgando el mínimo privilegio. Para detectar fraudes, debemos autenticar los usuarios resolutivamente y haciendo uso del

[6] Graham Williamson y Corey Scholefield. Introducción a la gestión de proyectos IAM para proyectos IAM. Cuerpo de Conocimiento de IDPro, volumen 1, edición 1, 31 de marzo de 2020. https://bok.idpro.org/article/id/25/.

contexto del entorno. Debemos aplicar políticas consistentes a lo largo de un panorama de recursos diverso. Y debemos verificar constantemente que nuestros sistemas estén funcionando como esperamos que lo hagan.

La administración de acceso como evolución

Este Cuerpo de Conocimiento te dará todo tipo de información sobre los conceptos básicos implicados en un régimen de administración de acceso - pero ¿por qué existen estos mecanismos? Fueron desarrollados para dar respuesta a las necesidades de negocio y amenazas a la seguridad. Los administradores se encontraron con una falta de control y crearon las mejores prácticas para facilitar la administración a escala y dificultar los ataques a escala.

La proliferación de contraseñas nos dio los directorios

Cuando los negocios comenzaron a acumular programas de negocio en su red privada, cada programa nuevo requería la creación y eliminación de cuentas de usuario. Cada programa solicitaba a cada usuario que estableciera una contraseña. A medida que los negocios crecieron hasta tener cientos y miles de programas, los usuarios llegaron al tope de la cantidad de nombres de usuarios y contraseñas que podían memorizar. Algunos programas permitían que los usuarios eligieran sus nombres de usuario y como resultado los nombres de usuario variaban mucho de programa en programa. Las políticas de contraseña también variaban mucho entre programas. Era tierra de nadie y de esa tierra de nadie nació el concepto de "directorios". En lugar de tener cientos de programas almacenando separadamente nombres de usuario y contraseñas, las aplicaciones empezaron a usar un directorio externo de usuarios, a menudo utilizando el Protocolo Ligero de Acceso a Directorios (LDAP, por sus siglas en inglés).[7],[8] De pronto, los usuarios podían usar una única contraseña en todos lados y los administradores no tenían que mantener miles de aplicaciones individualmente. Todo estuvo bien...por un tiempo.

La fatiga de contraseña nos dio la Gestión del Acceso Web

El lado positivo de los directorios de usuarios y del LDAP era que los usuarios solo tenían que recordar una contraseña. El lado negativo era que aun cuando todas las aplicaciones estaban dentro del mismo perímetro de red e integradas con LDAP, el usuario estaba obligado a introducir su contraseña cada vez que usaba una nueva aplicación - lo cual en el transcurso de un día se torna cansador. Esto dio lugar a la innovadora técnica de administración de acceso llamada "Gestión del Acceso Web" (WAM, por sus siglas en

---

[7] Contribuyentes de Wikipedia, "Protocolo ligero de acceso a directorios," Wikipedia, La Enciclopedia Libre, https://es.wikipedia.org/wiki/Protocolo_ligero_de_acceso_a_directorios (consultado el 6 de junio de 2020).

[8] "La historia más completa de servicios de directorio que jamás haya encontrado," blog, *Easy Identity*, 13 de abril de 2020, https://idmdude.com/2012/04/13/the-most-complete-history-of-directory-services-you-will-ever-find/ (consultado el 12 de junio de 2020).

inglés).[9] Con la gestión del acceso web, los usuarios se autenticaban una sola vez con sus contraseñas y luego se generaba una cookie de sesión de dominio (generalmente encriptada) que podía ser leída por múltiples aplicaciones. En lugar de hacer una asociación LDAP, la aplicación podía verificar que el usuario tenía una cookie válida. Por aquel entonces se desarrollaron otras técnicas para lidiar con la fatiga de contraseña, como por ejemplo Kerberos.[10] Estas tecnologías finalmente trajeron un poco de alivio a los usuarios; un usuario podía iniciar sesión una sola vez y acceder a múltiples aplicaciones. El concepto de un solo inicio de sesión para acceder a múltiples aplicaciones fue luego llamado "Inicio de Sesión Único" (SSO, por sus siglas en inglés).

Las limitaciones de perímetro nos dieron la federación

En la medida que los negocios operaban dentro de los perímetros de su red, las funciones de administración de acceso como Kerberos y WAM fueron convenientes y seguras. Pero Internet estaba creciendo y muchas empresas empezaron a querer otorgar acceso no solo a sus empleados sino a sus socios y clientes. Los negocios querían crear relaciones de confianza con otros negocios y habilitar a sus usuarios a acceder a las aplicaciones del otro. El Lenguaje de Marcado para Confirmaciones de Seguridad (SAML, por sus siglas en inglés) vino a satisfacer ese deseo.[11] Con SAML, los negocios preestablecen una "federación" de confianza entre dos dominios y luego solicitan una presentación segura cuando un usuario quiere acceder a un recurso. SAML y otras especificaciones de identidad federada permitieron que los negocios mantuvieran el control sobre las actividades de sus usuarios tanto en sus dominios como en otros. La identidad federada sigue siendo la columna vertebral de la administración de acceso y SAML aún es el mejor estándar para la administración de acceso entre dominios.

La innovación móvil & API nos dio OAuth y las infraestructuras de autorización delegada

La federación y SSO son lo que en la industria llamamos escenarios de "usuario presente". Podemos saber que el usuario está presente en una solicitud de federación porque la actividad ocurre utilizando un navegador y los navegadores no tienen cerebros - son clientes "pasivos" y alguien tiene que estar ahí apretando los botones y cliqueando los enlaces. Para el año 2007, la mayoría de las entregas de aplicaciones de negocio se hacían a través de un navegador - pero con el surgimiento del primer "teléfono inteligente" el juego cambió. Justo cuando las plataformas en la nube se estaban popularizando, las

---

[9] Contribuyentes de Wikipedia, "Gestión de acceso web," Wikipedia, La Enciclopedia Libre, https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_acceso_web (consultado el 6 de junio de 2020).

[10] Contribuyentes de Wikipedia, "Kerberos" Wikipedia, La Enciclopedia Libre, https://es.wikipedia.org/wiki/Kerberos (consultado el 6 de junio de 2020).

[11] Contribuyentes de Wikipedia, "Lenguaje de Marcado para Confirmaciones de Seguridad," Wikipedia, La Enciclopedia Libre, https://es.wikipedia.org/wiki/Security_Assertion_Markup_Language (consultado el 6 e junio de 2020).

aplicaciones móviles comenzaron a poder ser descargadas desde una tienda de aplicaciones y a renderizar información accedida en API en la nube. De pronto, los *softwares* de cliente "activo" comenzaron a considerarse como una forma deseable para comunicarse con los usuarios.

A medida que los usuarios se emocionaron con el poder de las aplicaciones móviles, los profesionales de la identidad se encontraron con el siguiente problema: las aplicaciones solicitaban API incluso cuando los usuarios no estaban presentes y, peor aún, muchas aplicaciones móviles querían consumir y desplegar información de plataformas en la nube a las que no estaban asociadas. Si una aplicación móvil quería acceder a una plataforma en la nube no asociada, la única respuesta posible era solicitar al usuario su contraseña y luego reproducirla en cada *API fetch*. Como resultado se generó algo llamado el **anti-patrón de contraseña**: los usuarios comenzaron a acostumbrarse a dar sus contraseñas de plataformas en la nube a cualquier cliente que las solicitara y esos clientes estaban obligados a guardar las credenciales de los usuarios en el caché de dispositivos móviles para poder ejecutar las llamadas API en la ausencia del usuario.

SAML no encajaba perfectamente en el contexto móvil. Los parsers o analizadores XML no fueron desarrollados para plataformas móviles y sus requisitos criptográficos eran pesados. El paradigma resultante de la administración de acceso fue OAuth 1.0, una "infraestructura de autorización delegada" que podía plegarse a los protocolos federados. OAuth aborda el escenario del "usuario no presente": las aplicaciones solicitan y reciben un "*token* de acceso" que no es introducido por el usuario; por otra parte, los *tokens* de acceso otorgan la capacidad de acceder en nombre de un usuario a un conjunto de datos y servicios delimitado con precisión.

Es posible que los *tokens* de acceso no parezcan la gran cosa, pero cuando tienes en cuenta que puedes entregar *tokens* de acceso a las API en lugar de credenciales primarias, el resultado es significativamente diferente. Puedes asegurarte de que los puntos finales API jamás recopilen ni validen credenciales primarias de usuario, eliminando así múltiples vectores de ataque relacionados con la filtración de información, con ataques por intervención (*man-in-the-middle-attacks*) y con administradores solitarios que recolectan credenciales. Dado que el mecanismo para autorizar API está desacoplado del mecanismo de autenticación de usuarios, se abre una puerta hacia un mundo donde los usuarios puedan autenticarse con otros factores que no sean una contraseña sin que esto implique más trabajo para aplicaciones. Los *tokens* de acceso actúan como una divisa estable que puede ser implementada en la arquitectura central y desplegada de forma escalable.

La Autenticación de Múltiples Factores (MFA) es, fue y será otra vez

En medio de todos los disparates y artimañas mencionados arriba, los administradores de identidades eran acechados por los ataques de contraseña. Para intentar mantener a los atacantes fuera de las cuentas que no les pertenecían, se desarrollaron todo tipo de

convenciones: obligamos a las personas a cambiar sus contraseñas regularmente; los obligamos a establecer contraseñas más largas y complejas; diseñamos nuestros directorios LDAP y formularios de inicio de sesión para que dejen de responder en el caso que se realicen demasiados intentos fallidos. A pesar de todos estos intentos de mitigación del riesgo, casi cualquier contraseña que un humano pueda establecer y recordar sin ayuda, es un blanco fácil de ataque. Si no me crees, lee el artículo escrito por Alex Weinert (@alex_t_weinert) "Your Pa$$word doesn't matter" (tu contraseña no importa).[12] Prepárate para llorar.

El descubrimiento que las contraseñas son esencialmente débiles no es nuevo y data al menos de los años 70 cuando se llevó a cabo una nueva investigación sobre cómo prescindir del cerebro humano en el proceso de autenticación.[13,14] En este artículo desarrollamos la noción básica de que las contraseñas son "algo que sabes" pero también describimos otras opciones para validar que un humano es propietario de una cuenta digital como "algo que tienes" o "algo que eres". La idea no es que validar "eso que tienes" reemplace "algo que sabes" sino más bien combinar algo que tienes, eres y sabes. Esto complica un posible ataque dado que el atacante debe lograr comprometer información tanto digital como física. La autenticación de múltiples factores de última generación usada hoy en día es muy sofisticada. Cada vez más usuarios protegen sus móviles con información biométrica, confirman una transacción usando un mensaje SMS o utilizan una Contraseña de Un Solo Uso (OTP, por sus siglas en inglés) para mejorar la seguridad, todo esto sin la necesidad de tener que comprender los principios subyacentes.

Todos sabemos que para que la Autenticación de Múltiples Factores (MFA, por sus siglas en inglés) tenga un uso realmente extendido, se debe seguir mejorando su usabilidad. Las especificaciones como FIDO2 cambian la industria de la administración de acceso, no porque el problema se resuelva sino porque el problema se ***desacopla*** - FIDO2 (W3C WebAuthn y FIDO CTAP2) separó el problema de manejar las claves criptográficas con el de solicitar gestos a los usuarios.[15] Así, el intercambio de claves criptográficas puede mantenerse confiable mientras nos enfocamos en la innovación, y por qué no en una revolución, de las interacciones de usuarios.

---

[12] Weinert, Alex, "Tu contraseña no importa," *Azure Active Directory Identity Blog*, Corporación Microsoft, 9 de julio de 2019, https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984.

[13] Morris, Robert, and Ken Thompson. " Seguridad de contraseña: un caso histórico." *Communications of the ACM 22.11* (1979): 594-597.

[14] Feldmeier D.C., Karn P.R. (1990) Seguridad de contraseñas de UNIX: diez años después. In: Brassard G. (eds) *Advances in Cryptology* — CRYPTO' 89 Proceedings. CRYPTO 1989. *Lecture Notes in Computer Science*, vol 435. Springer, New York, NY

[15] "FIDO2:WebAuthn & CTAP," FIDO Alliance, https://fidoalliance.org/fido2/.

La mejor seguridad es invisible

Aparte de las ceremonias visibles que presentamos a quienes soliciten el acceso a recursos, muchas cosas ocurren por debajo de la superficie. Para calcular los riesgos de una transacción determinada, dependemos cada vez más del contexto para que complemente los desafíos abordados por los usuarios activos.

Algunas áreas adyacentes a la identidad se han convertido en actores cruciales para la prevención del fraude de identidad - los Agentes de Seguridad para Acceso a la Nube (CASB, por sus siglas en inglés),[16] la gestión unificada de terminales (por ejemplo, Gestión de Dispositivos Móviles o MDM, por sus siglas en inglés),[17] y el Análisis del Comportamiento de Usuarios y Entidades (EUBA, por sus siglas en inglés)[18] fortalecen nuestros sistemas de administración de acceso. Los atacantes saben cómo burlar la seguridad de procesos de administración de acceso estáticos, por eso impulsamos nuestras defensas más allá de la baja complejidad de las contraseñas: si no compruebas constante y rápidamente las contraseñas comparándolas con el conjunto de secuencias prohibidas que se actualiza a toda velocidad y que incluye las listas de nuevas contraseñas divulgadas públicamente, a la vez que te mantienes a la par de los avances continuos y en tiempo real de la inteligencia de ciber amenaza, estarás en graves problemas.

Y la moraleja de la historia es...

Todo lo anterior nos condujo a la actualidad. Los profesionales de la identidad todavía enfrentamos todos los problemas que mencionamos anecdóticamente aquí, solo que ahora tenemos herramientas y convenciones a nuestra disposición que nos permiten abordarlos de la mejor forma. Cuanto más trabajemos en conjunto para mejorar nuestra profesión eliminando el fraude, detectando abusos y llevando a nuestros usuarios a interacciones exitosas, mejor estaremos todos. Todos los que vinieron antes que tú llevaron el trabajo de sus contemporáneos un paso adelante. Ahora tú tienes la oportunidad de dar el próximo paso.

¿Cómo se verá la administración de acceso en el futuro?

¿Cuáles habrán sido nuestras contribuciones cuando, en un futuro, miremos hacia atrás y veamos el mundo de hoy de la administración de acceso? Se valorará nuestro éxito en la

---

[16] Contribuyentes de Wikipedia, " Corredor de seguridad de acceso a la nube," Wikipedia, La Enciclopedia Libre, https://en.wikipedia.org/w/index.php?title=Cloud_access_security_broker&oldid=949494699 (consultado el 6 de junio de 2020).

[17] Raam, Giridhara, "El qué, el por qué y el cómo de la gestión unificada de terminales," *Integration Zone*, DZone, 8 de julio de 2019, https://dzone.com/articles/the-what-why-and-how-of-unified-endpoint-managemen.

[18] Petters, Jeff, "¿Qué es la UEBA? Guía completa para el análisis del comportamiento de usuarios y entidades," *Inside Out Security Blog*, Varonis, 29 de marzo de 2020. https://www.varonis.com/blog/user-entity-behavior-analytics-ueba/

colaboración de la adopción de múltiples factores por parte de los usuarios - pero ¿acaso lo logramos?, ¿Habremos perdido oportunidades? Mientras seamos tímidos para innovar, gran parte de nuestro futuro inmediato se desperdiciará mitigando ataques conocidos y en su mayoría prevenibles. Darle largas a la Autenticación de Múltiples Factores siendo un profesional de la administración de acceso hoy en día es como hacer *scroll* en las redes sociales sabiendo que tienes un informe pendiente que terminar (es un comportamiento lo suficientemente común como para tener su propio nombre: akrasia)[19]. Después de hacerlo, nos preguntaremos por qué entorpecimos nuestro propio camino y probablemente no tengamos ninguna respuesta válida.

Una vez que la cantidad suficiente de administradores haya adoptado MFA y eliminado los blancos fáciles que son las contraseñas de un solo factor, nuestra industria se va a hacer acreedora de un increíble premio:

¡Una nueva ola de ataques creativos!

Esto puede sonar como algo malo, pero en realidad es bueno. Hoy en día, los atacantes pueden ganarse la vida haciendo nada más que correr scripts gratuitos de *phishing* que consiguen en Internet sin casi tener que invertir tiempo o dinero. Un mundo fuertemente autenticado no está libre de los ataques *jackpot* pero sí hace que el grupo de criminales capaz de llevarse estos premios sea un grupo mucho más selecto.
Los atacantes se moverán hacia los ataques post-autenticación como el robo de *token* y el abuso del consentimiento. Y al mismo tiempo, ¡los profesionales de la identidad estarán creando cosas nuevas junto a otros! ¡Inventando mejores formas! ¡Introduciendo los recursos y la satisfacción que quieren los negocios! Asimilaremos nuestros accesorios (como los móviles) como dispositivos de seguridad, realizaremos transacciones seguras aún en lugares hostiles, haremos que la medida del menor privilegio sea aún más estricta. Seremos mejores en cumplir con lo que los productos prometen y en penalizar a los que se metan con nuestra información. Encontraremos la manera de compartir cosas privadas teniendo la confianza absoluta de que las mismas jamás serán públicas.

Lidiaremos con colapsos cuánticos y nuevas redes sociales, pero será una lucha digna de dar.

El profesional de la administración de identidades que haya llegado hasta aquí en su lectura es evidentemente un profesional dedicado y eso es algo maravilloso. Necesitamos que la nueva generación de profesionales tome la posta, cuestione todo lo aprendido y nos impulse hacia un futuro donde el riesgo sea bajo, la productividad alta y los nuevos desafíos mantengan nuestras vidas interesantes.

---

[19] Clear, James, "El efecto Akrasia: por qué no cumplimos lo que nos propusimos hacer y qué hacer al respecto," extraído de Hábito atómicos, https://jamesclear.com/akrasia (consultado el 6 de junio de 2020).

Biografía de la Autora

 Pamela Dingle forma parte del mundo de la administración de identidades desde hace mucho tiempo. Es directora del equipo de estándares de identidad de Microsoft. El equipo de estándares de identidad trabaja con organismos normativos como W3C, IETF y la Fundación OpenID en especificaciones como OAuth 2.0, FIDO, SCIM y OpenID Connect. El trabajo de Pamela consiste en asegurar que los clientes, grupos de productos y la industria toda comprendan el valor de los estándares y de otros patrones de las mejores prácticas de identidad. Pamela se desempeñó durante ocho años como arquitecta de identidad y trabajó ocho años en la oficina del CTO de Ping Identity. Pamela Dingle es fundadora de *Women in Identity*.