Crisis de Identidad (Gestión)

La evolución de los conceptos de identidad

Este artículo ha sido desarrollado por Debra Shinder, y fue traducido al español por Enrique Dutra previa autorización de TechGenix Ltd.

La versión original se puede encontrar en Windows Security. Acceder a la parte I, II, III

Introducción

El robo de identidad, gestión de identidad, protección de la identidad son términos que observamos o escuchamos últimamente, y vemos que la identidad es un elemento crucial en la mayoría de los mecanismos de seguridad informática. Los controles de acceso dependerán de la identificación de los usuarios o dispositivos que se les permita ver o utilizar los recursos. Se nos pide "probar" nuestra identidad cada vez que vamos a bordo de un avión, en un hotel,al hacer una compra a través de un cheque o una tarjeta de crédito, o ingrese a una computadora o un sitio web seguro. Sin embargo, la valoración de la prueba suele ser muy baja, y en el mundo de las TI, parece que tenemos una idea equivocada acerca de lo que la identidad es en realidad y cual es el caso de que no lo es.

En este artículo, serie de tres partes, en primer lugar vamos a observar cómo el concepto de identidad se ha convertido - particularmente en los ámbitos legales y tecnológicos. En la segunda parte, vamos a demostrar por qué todo lo que usted piensa que usted sabe acerca de identidad está mal. Luego en la tercera parte, vamos a ver las soluciones de TI comunes de gestión de identidades, donde no logran cubrir las expectativas o necesidades, y cómo se podría mejorarlo.

Identidad: ¿Qué significa eso realmente?

"Identidad" tiene diferentes significados, dependiendo del contexto en el que se lo utiliza. Se trata de un concepto filosófico, un concepto psicológico, un concepto jurídico, incluso un concepto religioso - y luego está ovbiamente, la forma en que se lo utiliza en TI. En términos filosóficos, simplemente se refiere a lo que hace que una entidad reconocible y distinguible de otras entidades. En psicología, se trata de la propia imagen de una persona, los roles sociales y las características de la personalidad, y hay una gran cantidad de teorías y modelos que van desde la ruptura freudiana de la psique en ello, el yo y el super yo, con el marco Eriksoniana para separar la identidad personal y social o cultural. En la teología, se trata del alma.

Eso es todo muy interesante, pero voy a dejar esos debates a la gente que está especializada en estas disciplinas. Más pertinente para aquellos que tiene que ver con el crimen cibernético es lo que significa la identidad en un sentido legal, y cómo ve el mundo de TI y de los intentos de "manejar" la identidad. Sin embargo, una breve mirada a la historia y la evolución de la sociedad de definiciones de la identidad es útil en la comprensión de la ley y su correspondiente práctica.

Historia y evolución de la identidad.

Cuando usted entra en una relación con alguien - de negocios o personales - siempre es importante saber con quién estás tratando. Los seres humanos se diferencian de muchas maneras. Antes de desarrollar el lenguaje, podemos asumir que la gente se identificaban con otras personas por el aspecto que tenían, como se comportaban; sonaban (bajos gruñidos agudos frente a altos tonos?), incluso por su olor. Sabemos que muchos animales hoy en día, como los perros, se basan en la nariz para interpretar el mundo y esto incluye el reconocimiento de personas y otros animales por la forma en que huelen.

Con la palabra hablada y escrita fue la práctica de dar nombres a objetos y personas. En una población pequeña, los nombres podrían ser únicos para que cuando se habla de "John Smith", todos sabían de quien se estaba hablando. Las poblaciones tempranas también fueron en general menos móviles (la gente no se iba de la ciudad), por lo que todos en el pueblo no sólo sabía quién era John - que lo habían conocido desde su nacimiento y estaban familiarizados con todas las características que definieron a "Juan", como su voz, su modo de andar, los gestos divertidos que hizo con sus manos y sus comportamientos generales. Las personas fueron identificadas a menudo no sólo por sus nombres y características, sino también por su ascendencia: por ejemplo, John Smith, hijo de Robert y Mary Smith.

A medida que la población se hizo más grande y más móvil, los nombres se duplicaron y la gente entraba y salía de la ciudad. Ellos fueron identificados a veces por sus lugares de origen: es decir, Joe Jones, de Riverside. Pero a medida que más y más extranjeros llegaron a la ciudad, no teníamos la historia con ellos y no había manera de identificarlos, excepto por los nombres y otra información que proporcionaban, lo que podría o no podría ser su "verdadero" nombre. Por lo tanto hemos desarrollado la necesidad de credenciales de identidad.

Alguna vez, las credenciales podían ser cualquier cosa, desde una carta de presentación de alguien que había conocido durante un tiempo sustancial a una anotación en una Biblia de la familia. Pero los gobiernos se convirtieron en las burocracias y los burócratas les gusta llevar un registro, por lo que los documentos de identidad se convirtieron en algo común y obligatorio. Los certificados de nacimiento proporcionaban un registro escrito de un nombre, lugar / fecha / hora de nacimiento, hasta un linaje. Cuando la mayoría de los bebés nacían en su casas, muchas personas no tenían certificados de nacimiento, pero a medida que el proceso de parto se trasladó a las instituciones (hospitales), se hizo más fácil para los gobiernos para vigilar los nacimientos.

El advenimiento del automóvil tuvo la consecuencia imprevista de la creación de un modelo de documento, documento oficial de identidad, licencia de conducir. Ese documento se transformó en un pedazo de papel con su nombre, fecha de nacimiento, dirección y firma en él hasta llegar a una tarjeta de plástico con una foto, y ahora en muchas jurisdicciones se incluye una huella digital, banda magnética con información codificada, impresiones holográficas y / o transmisores de RFID.

Hoy tenemos una gran cantidad de credenciales de identidad. Además de la licencia de conducir (o tarjeta de identificación estatal/Cédula de identidad para aquellos que no conducen), tenemos credenciales por todas partes, debemos obtener una tarjeta de seguridad social o de la obra social, para nuestros hijos mucho antes de ser apto para obtener un trabajo, y a pesar de que originalmente la ley prohíbe expresamente su uso como identificación, se ha convertido en una credencial de identidad de facto que no podemos usar para obtener beneficios del gobierno y pagar nuestros impuestos, pero al tomar una clase, podemos solicitar un crédito o incluso (en algunos casos) firmar un servicio como el de televisión por cable o para el servicio teléfonico. Los que trabajan para las grandes empresas tienen tarjetas de identificación de empleados. Si pertenecemos a una organización, tenemos también tarjetas de membresía. Para viajar fuera del país, es necesario el pasaporte.

Nos estamos ahogando en un mar de credenciales de identidad.

La credibilidad de las credenciales

No todas las credenciales de identidad han sido creadas iguales. ID emitidos por el gobierno son generalmente considerados como la mejor prueba de su identidad, pero ¿lo son realmente?.Los Estados han reforzado sus procedimientos, pero tan sólo unos pocos años atrás (antes de 11 de septiembre), en muchas jurisdicciones no era tan difícil conseguir una licencia de conducir con en el nombre que uno quisiera. Recuerdo que cuando me casé en la década de 1990 y me fui a DMV para cambiar mi nombre. La persona que me atendió no me pidió mi licencia de matrimonio o cualquier otra documentación del cambio de nombre que justificara mi cambio, yo simplemente les dije cual era el nuevo nombre y diligentemente se introdujo en el sistema y emitió una nueva licencia como le solicité. Por supuesto, en aquel entonces era perfectamente legal para cambiar el nombre en Texas a través de la ley común - es decir, sólo mediante la adopción y el uso del nuevo nombre. No se requiere orden judicial (a menos que usted fuera un menor de edad).

Hoy en día tienes que saltar a través de algunos aros más para obtener una licencia o cambiar su nombre, pero no es como se lo hacen en un cheque de fondo. La adición de una huella digital a la base de datos de la licencia de conducir lo hace un poco más difícil para que Usted pueda falsificar su identidad en el DMV - si alguna vez te han tomado las huellas digitales de impresión y que estás permanezcan aún en el archivo. Sin embargo, muchas personas no tienen, a menos que hayan estado en el ejército, fue arrestado alguna vez, trabajó como oficial de cumplimiento de la ley o en una posición con la autorización de seguridad, en la que se obtiene una licencia para portar un arma oculta, etc. Un día es probable que todo el mundo tomará las huellas digitales de niños, en el momento en que aún es opcional, pero esto es alentado por muchos programas de seguridad escolar del niño.

Pensamos en los métodos de alta tecnología de hoy de identificar a las personas como superiores a las de años pasados, pero ¿son realmente?. Como ya hemos mencionado, la base de la verificación de la identidad antes de que todas estas tarjetas de fantasía y los métodos científicos

fuera certificado. Es interesante, vamos a regresar en torno a ver el valor de un mundo donde las credenciales de papel, plástico y electrónicos pueden ser fácilmente falsificadas.

El enfoque de TI a la identidad

Si tenías la mayoría de edad en la época de cuando la PC de IBM era el rey, es probable que recuerden arrancar el sistema operativo y empezar a trabajar. Usted no tenía que identificarse con el sistema (a menos que un software especial se hubiera cargado y te lo exigiera). Los primeros ordenadores domésticos eran compartidos por lo general por todos los miembros de la familia, y nadie tenía cuentas de usuario.

Pero en un entorno empresarial, es importante identificar quién está usando una computadora, aunque sólo sea para saber quién era responsable si el sistema estaba mal. Configuración de cuentas de usuario separadas, bien se logró esto, pero los usuarios no tenían manera de probar su identidad cuando se lo despidió y sus cuentas quedaron huérfanas, en donde cualquier persona podría utilizar cuenta de otra persona (y a menudo lo hicieron). Por lo tanto la obligación de proporcionar las credenciales para demostrar que eras realmente el usuario propietario de esa cuenta era subjetivo.

El uso de contraseñas (o "códigos secretos") para verificar la identidad ha estado por mucho más tiempo que las computadoras. Por lo tanto, era lógico (y fácil) para utilizar el sistema de contraseñas para la autenticación de los usuarios de computadoras. Los PIN son sólo el equivalente numérico de las contraseñas alfabéticas. Sin embargo, los problemas con las contraseñas y números de identificación como un mecanismo de autenticación son leyenda. Si las contraseñas son breves y sencillas, son fáciles de romper con un ataque de fuerza bruta. Si son largos y complejos, los usuarios las olvidan y/o las escriben en algún lugar simple para recordarlas. Las frases proveen más complejidad al mismo tiempo dejan de ser relativamente fácil de recordar, pero no resolvemos del todo el problema.

La necesidad de un mecanismo de autenticación mejorado es llevado al concepto de autenticación de múltiples factores. Además de "algo que usted sabe" (PIN, contraseña o frase de contraseña), los usuarios pueden ser obligados a proporcionar algo de lo que tiene: una tarjeta inteligente o token, o un teléfono celular que se identifica por un número de serie único o una señal generada por el software . El sistema de tarjeta / token tiene sus propios inconvenientes, sin embargo, la credencial de física se puede dejar en el hogar, perdidos o robados.

Información biométrica se ha considerado el Santo Grial de la autenticación, porque se dice que se basa en "algo que se" - características fisiológicas o de comportamiento que se cree que son exclusivos de una persona en particular y que no cambian. Sin embargo, incluso los datos biométricos no ofrecen un método infalible para verificar la identidad. Las huellas dactilares se pueden reproducir a través de los moldes (o siendo más dramático, al estilo Hollywood, un tipo malo solo podría cortar el dedo y utilizarla para tener acceso). La enfermedad y las lesiones pueden causar cambios en las características fisiológicas - huellas dactilares, patrones de la retina, voz, modo de andar, etc. Existe la posibilidad en minutos, pero real, de la duplicación, por lo

menos en la medida utilizada para declarar un partido en la base de datos. Por ejemplo, un sensor de huellas digitales, como cualquier pieza de equipo electrónico, pueden fallar. El software utilizado para procesar la impresión y la comparamos con otros en la base de datos podría tener errores. Los falsos positivos son posibles. Lo mismo es cierto para otros métodos biométricos.

No hay ningún medio perfecto e infalible de la autenticación de la identidad de un usuario. Y esto es complicado por factores que vamos a discutir en la segunda parte.

Nombres no es lo mismo que Identidad

Los nombres son el principal medio por el cual la mayoría de nosotros identifican a las personas (como a los objetos también). En el idioma Inglés (en Español se definen de la misma manera)(1), los nombres que identifican a determinados individuos o entidades se llaman "nombres propios". La investigación ha demostrado que incluso algunas especies no humanas (como los delfines) aparece el uso de nombres, de una especie, para diferenciarse entre uno y otros. En algunas sociedades, los nombres están muy bien guardados y solo se confían a personas cuando las mismas son de confianza.

(1) Referencia del traductor.

En IT, los nombres se requieren a menudo para obtener acceso a un recurso. Los nombres de cuenta de los usuario son una parte del conjunto de la información necesaria para iniciar sesión en una computadora o tener acceso a un recurso protegido en el sistema o a través de la red. Los nombres de los servidores pueden ser necesarios para localizar un recurso de red. La combinación de nombre de servidor, nombre de dominio y el nombre del archivo está obligando a acceder a una página web - aunque a veces no están obligados a proporcionar toda la información, por ejemplo, si apuntamos un navegador web para www.mydomain.com, que han proporcionado el nombre del servidor Web (WWW) y los nombres de dominio (mydomain y com.) pero no tiene que escribir el nombre del archivo (por ejemplo, default.htm o index.html), ya que se supone que si no lo hacemos, puede entrar en otro nombre de archivo.

En el "mundo real", muchas personas diferentes pueden tener exactamente el mismo nombre, escrito de la misma manera. Todos los John Smiths por ahí puede ser fácilmente confundido con otras personas. En un sistema de TI, los nombres de las cuentas de usuario se requieren generalmente para ser único dentro de ese sistema. Vemos, pues, los nombres de usuario, tales como jsmith392.

Tan importante como son los nombres, es importante recordar que un nombre en realidad es sólo un descriptor. Ya sea que se refieren a mí como "Debra Shinder", como "el autor de Crisis de Identidad (Gestión)" o como "el 5'4 "mujer pelirroja de suéter verde", que estamos hablando de la misma persona. Sin embargo, sólo dos de las tres descripciones son específicos (no es probable que sean muchas las mujeres que usan 5'4 "suéteres verdes en el mundo en un día determinado"). Sólo uno de ellos es permanente - que podría teñirme el pelo, o incluso cambiar legalmente mi nombre, pero una vez que he escrito este artículo, siempre voy a ser el autor. Sólo uno es "oficial",

en el que está en mis documentos emitidos por el gobierno. Los nombres se pueden cambiar - a través de una orden judicial, a través del matrimonio, o en algunas jurisdicciones en común, sólo mediante la adopción y el uso de uno nuevo. El punto es que su nombre no es usted.

En TI, los nombres de usuario también se puede cambiar. En la mayoría de los sistemas, esto se puede hacer con bastante facilidad, precisamente porque, aunque el nombre es la información que usan los humanos para identificar la cuenta, no es lo que utiliza el sistema. El sistema utiliza generalmente una cadena alfanumérica de caracteres subyacente, que en los sistemas Windows se llama el SID o el identificador de seguridad. El nombre asociado con el SID es sólo una de sus propiedades y se puede cambiar.

Las credenciales de autenticación no es igual a Identidad

Lo que comúnmente se denomina como "robo de identidad" en general es realmente el robo de credenciales que se asocian con una identidad particular. Robar tu contraseña no constituye realmente el robo de tu identidad - pero permite al ladrón hacerse pasar por Usted. Esto sólo funciona con un sistema sofisticado / sin saber que se basa únicamente en esas credenciales para identificarse y hacer la suposición de que Usted es el único que podría saber la contraseña.

Volviendo a la comparación del mundo real, si alguien utiliza su nombre y tal vez tiene una de sus tarjetas de crédito en su posesión, un comerciante no sabe por que razón puede tener la tarjeta o si la misma ha sido robada y la considera válida. Un comerciante más consciente de los riesgos, puede pedir una identificación con una foto, junto con la tarjeta de crédito, para verificar que realmente es Usted. Un comerciante que en realidad sabe que no es Usted, sabrá de inmediato que no es usted, incluso si el ladrón de la apariencia física en general es similar a la suya o no.

Incluso si una persona tuvo una cirugía plástica para él/ella se mira igual que Usted, sus amigos cercanos y miembros de la familia sabrán que no es la persona que dice ser, al menos después de un poco de interacción, porque esa persona podría tener todos sus recuerdos, o recordar todas las experiencias compartidas, y demás que componen una relación.

Un sistema de autenticación de TI sofisticado debe exigir algo más que el nombre y la contraseña correcta. Usted probablemente ha notado que recientemente, ciertos sitios web protegidos han empezado a utilizar otros métodos, adicionales para verificar su identidad junto con las credenciales habituales. Le puede solicitar la respuesta a una pregunta personal, como el monto de su pago hipotecario mensual. Puede ser que hayan seleccionado una foto que usted tendrá que escoger de un grupo de imágenes cada vez que se inicie la sesión. Hay muchas maneras diferentes de hacer el proceso de verificación de identidad más difícil para un impostor se pueda hacer pasar como Usted. El truco es hacer que sea muy difícil para un impostor, pero muy fácil para el "verdadero yo". En la Parte 3, vamos a estar mirando a los diferentes métodos y la forma de determinar cuál funciona mejor en una situación determinada.

El dilema de la Identidad múltiple

Una cosa que complica la gestión de identidad es el gran número de identidades que cada uno de nosotros puede asumir en el curso legítimo al momento de vivir nuestras vidas. En la vida real, aunque la mayoría de nosotros usamos el mismo nombre para la mayoría de nuestras interacciones, jugamos muchos roles diferentes en función de dónde estamos y con quien estamos interactuando.

A veces estas diferencias son tan extremas que las descripciones de la misma persona en diferentes situaciones nos llevaría a creer que usted puede ser tímido y reservado en casa, pero extrovertido y bullicioso en público "No debemos estar hablando de la misma Mary Smith." - O viceversa. Usted puede ser formal y correcto delante de sus padres, pero provocativo u ofensivo, incluso después de unas copas en un bar.

Algunas personas incluso viven de verdad una "doble vida", no sólo actúan de manera diferente, pero usan oficialmente distintas identidades. Todos lo hemos visto en las películas - por lo general la participación de un espía del gobierno o agente de espionaje corporativo. Hemos leído los artículos periodísticos sobre el vendedor afable que tiene esposas y familias en diferentes ciudades. Y, por supuesto, no es la condición psiquiátrica, lo que se llamó una vez "doble personalidad" o "trastorno de personalidad múltiple" y que ahora se denomina "trastorno de identidad disociativo", en el que una persona muestra "alterna" - distintas personalidades separadas, cada una con su propias percepciones del mundo.

La mayoría de nosotros tenemos muchas identidades diferentes - que generalmente se traduce en muchos conjuntos de nombres de usuario y contraseñas (y / u otras credenciales de autenticación). Tenemos un nombre y una contraseña para iniciar sesión en nuestros ordenadores, otro para el registro en los equipos de trabajo, otro para la línea de sitios Web bancarios, otro para el pago de nuestra factura de electricidad, uno para comprar cosas de Amazon, uno para compartir con los amigos en las redes sociales, y sigue y sigue y sigue. No es nada raro tener veinte o más cuentas diferentes en línea para la gestión de los diferentes aspectos de nuestras vidas digitales.

Sólo la gestión de todas sus identidades personales puede ser un desafío. Los departamentos de TI tienen más de un desafío, con la necesidad de gestionar cientos o miles de identidades de los usuarios. Algunas personas toman el camino más fácil, y usar el mismo nombre y la contraseña para todas sus cuentas. Simplifican las cosas, pero plantea una gran amenaza a la seguridad: Si el conjunto de las credenciales se ve comprometida, todas sus cuentas están en riesgo.

Otros utilizan un método improvisado de "niveles" de credenciales. Es posible que tenga un nombre de usuario/contraseña que utiliza para las cuentas no muy importantes, como el inicio de sesión en un sitio de noticias para leer sus historias o de TI en el foro para hacer/responder a las preguntas de alta tecnología. Entonces usted tiene otra cuenta que se utiliza para los sitios de alta seguridad, tales como Facebook o Google (en el que compartir información personal). Esa contraseña puede ser mayor y más compleja. Usted podría tener otro conjunto de credenciales,

más difícil como contraseña/frase, para los sitios de banca o en los que debe introducir la información de tarjetas de crédito u otros datos financieros.

Una identidad para gobernarlos a todas

Single Sign-on es considerado por algunos como el Santo Grial de la gestión de la identidad. Esto se refiere a la capacidad de iniciar sesión una vez y acceder a múltiples sistemas. Esto difiere de utilizar las mismas credenciales para varias cuentas en que hay:

1. Credenciales idénticas, usted todavía tiene que iniciar sesión en cada sistema por separado, simplemente no tiene que recordar múltiples nombres y contraseñas.

2. Inicio de sesión único, usted todavía tiene unas credenciales distintas para cada uno de los sistemas, pero todos estos son almacenados por el sistema de SSO y entró automáticamente en el sistema adecuado después de haber iniciado sesión con su cuenta "maestra" de SSO.

A veces, tener una sola identidad, incluso dentro de un único sistema, puede ser problemático. Algunas redes sociales populares, como Facebook y Google+, han recogido quejas de los usuarios acerca de sus políticas que prohíben que los usuarios tengan varias cuentas y/o requiere a los usuarios utilizar sus "reales" (legal) nombres de cuenta. Muchas personas, por ejemplo, desean tener una cuenta de compañeros de trabajo y otro para los amigos personales. Algunos quieren usar un seudónimo, como un nombre de cuenta, porque ese es el nombre con el que el público los conoce (los autores que utilizan seudónimos, los actores que tienen nombres artísticos, etc.) En algunos casos, incluso puede ser peligroso para una persona a usar su nombre real debido a las leyes dictatoriales o por las cuestiones políticas en países en los que cualquier atisbo de disidencia puede ser castigada con la muerte.

Resumiendo: Su identidad es mucho más que un conjunto de credenciales, pero la protección de sus credenciales es una parte importante para operar de forma segura en línea. En la Parte 3, vamos a ver algunas de las soluciones de gestión de identidad, y en la parte 4, vamos a terminar esta serie con algunas especulaciones sobre el futuro de la identidad en un mundo cada vez más interconectado.

Firma como prueba de identidad

En los pre-electrónicos a veces, el nombre escrito a mano es la representación legal de la identidad de una persona y la intención de un contrato u otro documento. Debido a que la escritura tiende a ser más o menos exclusivo de un individuo a otro, una firma presenta pruebas de que la persona nombrada que había creado y/o leído y aceptado el contenido del documento es la misma. Sin embargo, las firmas pueden ser falsificadas (falso).

La falsificación es un delito penal, pero contrariamente a la creencia popular, más que la firma de nombre de otra persona por lo general no constituyen la falsificación de la ley. Por ejemplo, una persona legalmente puede dar a otra persona permiso para firmar en su nombre, ya sea manualmente o utilizando un sello de firma o con una máquina, lo que es práctica común en las oficinas de negocios y agencias gubernamentales cuando la persona cuya firma es necesaria en un gran número de documentos y no pueden pasar todo el tiempo necesario para firmar personalmente.

Para ser falsificación, la firma de otro nombre por lo general debe hacerse con fines fraudulentos - es decir, para engañar a alguien y/o a expensas de otro (los elementos específicos del delito se establece en los estatutos legales que hacen que sea un delito, y pueden diferir de una jurisdicción a otra).Para verificar que una firma es de hecho realizada por la persona cuyo nombre que representa, la firma puede ser notariada. Un notario público es un funcionario público que esté habilitado por el gobierno para presenciar la firma de los documentos (entre otras cosas) y autenticar la identidad de la persona que firma, por lo general mediante el examen de documentos de identificación como una licencia de conducir, DNI o pasaporte. El notario estampará la firma propia y el sello para verificar que el firmante es quien él/ella dice ser.

Las firmas digitales

En el mundo de TI, tenemos las firmas digitales para servir con un propósito similar, en calidad de evidencia de que un mensaje electrónico o documento ha sido creado o enviado por la persona o entidad a la que parece haber venido o creado. Las firmas digitales pueden ir un paso más adelante y comprobar que el mensaje o documento no se han modificado en modo alguno desde que se firmó. Las firmas digitales han estado con nosotros, al menos en concepto, desde los años 1970 (Diffie y Hellman) y está disponible en el software comercial desde finales de 1980 (Lotus Notes). Ahora las firmas digitales son cada vez más comunes, con muchas agencias gubernamentales que los utilizan para publicar los documentos oficiales, y en muchas jurisdicciones las firmas digitales son jurídicamente vinculantes, al igual que la firma manuscrita.

Las firmas digitales utilizan el esquema de un par de claves pública/privada y por lo tanto se basan en una infraestructura de clave pública (PKI) para emitir los certificados digitales que contienen estas claves para la firma de documentos electrónicos. El papel de la entidad emisora de certificados es algo así como la del notario público - que es un tercero de confianza que le da su "sello de aprobación" para el firmante. La clave privada vinculada solamente a esa persona en particular y su uso para firmar el documento indican que la persona, y nadie más, lo hizo con la

firma. Los certificados digitales no se utilizan sólo para la identidad de las personas, sino también las máquinas, tales como servidores web.

La clave para confiar en una firma - ya sea manuscrita o electrónica - como una verificación de identidad en su confianza de que el tercero - un notario público o CA - da fe de ello. Si un notario es laxo en exigir documentos de identidad o no sabe cómo determinar si la identificación es válida, la autenticidad de la firma puede ser dudosa. Si los certificados de la CA tienen problemas a quien lo solicite, bajo cualquier nombre, sin ningún tipo de verificación de que el solicitante está utilizando su verdadera identidad, la firma digital no es buena.

Los certificados tipo Extended Validation (EV) son mucho más caros que los otros certificados digitales, ya que implican un trasfondo más profundo para comprobar la identidad legal de una entidad. Estos han existido desde 2007, cuando las directrices para la emisión de ellos fueron ratificados, y se utilizan para identificar sitios web seguros.Como la firma manuscrita, la firma de cada individuo debe ser presenciado por el notario. Con la firma electrónica, la autoridad competente emite el certificado y puede ser utilizado para muchas firmas diferentes. Por lo tanto, es imperativo que la clave privada se mantenga en secreto. La clave privada se guarda en un archivo que se puede guardar en el disco duro de una computadora, en una unidad extraíble, como una llave USB o en una tarjeta inteligente.

Más allá de la firma

Debido a que las firmas pueden ser copiadas o falsificadas, algo más a menudo, es necesario probar su identidad al firmar los documentos, siendo esto de especial importancia. Las agencias que emiten las licencias de conducir, algunos bancos y otras entidades puedan tomar una foto de una persona y/o requerir que él o ella proporcionen una huella digital junto con la firma. En el mundo de TI, la autenticación biométrica va más allá de una firma digital, lo que podría ser robado por un pirata informático inteligente.

Como ya comentamos en la primera parte, aunque la biometría no es un método infalible para verificar la identidad, se puede agregar otra capa al proceso de verificación. Si usted posee la clave privada correcta, su huella dactilar coincide con la almacenada para usted en la base de datos, usted conoce la contraseña, y usted es capaz de responder a algún desafío pregunta/respuesta de las preguntas con la información correcta, es muy probable que usted realmente es la persona que dice ser. De este modo, tal y como vemos en una "defensa en profundidad", la solución para la protección de nuestros sistemas de los ataque, la mejor apuesta para la verificación de la identidad es una "autenticación en profundidad" como estrategia.

¿Cuál es el problema con eso? No hay, desde el punto de vista del administrador de seguridad. Pero a los usuarios no les agradará. E incluso nosotros, los profesionales de la seguridad, si somos honestos, puede ser un poco molesto cuando los sitios de banca nos pide que cambiemos nuestras contraseñas, volvamos a introducir el número de teléfono asociado a nuestras cuentas, y el nombre del perro de la tía de nuestro primer novio de antes que nos permiten la entrada para ver nuestros saldos. Un sistema de identidad de una buena gestión debe ser transparente para el

usuario, al igual que un buen plan de seguridad global no puede sacrificar la facilidad de uso, o en última instancia, se producirá un error, como Bruce Schneier, dio a entender cuando dijo: "Mientras más seguro lo quiera hacer, se convierte en menos seguro."

Hacia una solución integral de gestión de identidad

Gestión de la identidad es algo más que sólo la autenticación de identidad, aunque la autenticación es un componente importante. El sistema de gestión de la identidad debe primero establecer la identidad de las personas o entidades (como computadoras) y luego usar esa información para controlar el acceso a los recursos del sistema.

Suena simple, pero su aplicación efectiva puede ser muy compleja. En mundo de las TI de hoy en día, es todo acerca de EaaS - todo como un Servicio. El sistema de gestión de identidad debe estar integrado para ofrecer los servicios a los usuarios a la perfección, en la demanda, mientras se determina quién tiene acceso a los servicios y en qué grado. Y va en ambos sentidos, los usuarios deben ser capaces de verificar la identidad de los proveedores de servicios.

Incluso las redes domésticas de hoy requieren de algún sistema de gestión de identidades. Los controles para padres se basan en la autenticación de identidad para dar a los padres la posibilidad de restringir los juegos que los niños puedan jugar, qué sitios web puedan visitar, cuánto tiempo podrían permanecer en línea, y así sucesivamente. A continuación vamos a mirar más de cerca los criterios para elegir una solución de gestión de identidad integral de una organización, la gestión de identidad federada, y el efecto de la nube de problemas de identidad en TI. Entonces, brevemente discutir el futuro de la identidad.