SEADE

Cómo contrarrestar la futilidad de la seguridad de las redes

Frank Konieczny
Teniente Coronel Eric D. Trias, PhD, USAF
Coronel Nevin J. Taylor, USAFR

No podemos resolver nuestros problemas con la misma forma de pensar que usamos cuando los creamos.
—Albert Einstein

Los medios de comunicación actuales están llenos de historias de ciberataques que hacen que se produzca una pérdida de confianza por parte del público, dimisiones de oficiales superiores y un impacto significativo a corto y largo plazo en nuestra nación. Muchas de estas violaciones se derivan de vulnerabilidades conocidas en la arquitectura de seguridad de la red existente, que presenta un peligro diferenciado para nuestros intereses nacionales vitales. Estas vulnerabilidades, que varían en refinamiento, podrían ser tan sencillas como usar claves débiles (por ejemplo, valor predeterminado, series numéricas sencillas o la palabra *clave* misma). Los ataques ligeramente más refinados hacen uso de intentos de suplantación de identidad mediante correo electrónico o ingeniería social, diseñados para suscitar acciones peligrosas o información que permitan a los adversarios un acceso no autorizado.

La noción de "defensa en profundidad" ha sido considerada por organizaciones de seguridad principales (que se basan en el Instituto Nacional de Normas) como base según la cual la estructura de seguridad se puede desarrollar para salvaguardar nuestras redes. La profundidad incluye

protecciones de seguridad físicas (muros, puertas, cerraduras, protectores y jaulas de computadoras) y medidas de seguridad lógica (cortafuegos de redes y detección de intrusiones). No obstante, sea cual sea el número de capas de protección de redes perimetrales empleado, los adversarios siguen superando las defensas mediante el uso de una variedad de contramovimientos o explotando malas prácticas de seguridad cibernética.

Además, los ciberataques con éxito resaltan el hecho de que es necesaria pero no suficiente una higiene cibernética disciplinada para prevenir todos los posibles ataques. Los sistemas simplemente son demasiado complejos para aplazar la aplicación y la seguridad de datos a los aparatos de defensa e infraestructura de la red de apoyo. Por lo tanto, proponemos que, desde su incepción, se deben diseñar aplicaciones para protegerse como entidades independientes con seguridad integrada y con una dependencia de seguridad mínima en aparatos de seguridad de redes (por ejemplo, cortafuegos).

Como anunció el Secretario de Defensa Ashton Carter durante un discurso de la Universidad de Stanford, para mantener la seguridad de los sistemas, debemos construir "una arquitectura de seguridad sencilla que sea más defendible y capaz de adaptarse y evolucionar para mitigar las amenazas cibernéticas actuales y futuras".[1] Proponemos que la siguiente evolución sea un paquete de seguridad de "diseño" a nivel de aplicación: arquitectura de aplicaciones encapsuladas de seguridad y enclave de datos (SEADE) compuesta por un centro de datos de aplicaciones virtuales (VADC) y seguridad a nivel de empresa (ELS). SEADE redistribuirá la responsabilidad de un perímetro de seguridad de redes a nivel de empresa para cada aplicación. Se comportará como un recipiente virtual asegurado por separado que ofrece a los usuarios un mejor acceso de datos y produce un paquete de aplicaciones que es muy difícil de penetrar y fácil de transferir; además, SEADE requiere poco mantenimiento.

Defensa de redes perimetrales insuficiente

En el pasado, las empresas estratégicas en esta área se concentraban en salvaguardar la información que reside dentro de nuestras redes formando muros cada vez mayores y más gruesos alrededor de nuestras *joyas de la corona*, poniendo guardas en las puertas que interrogan a todo el que entra o sale y estableciendo múltiples puntos de verificación. Estos esfuerzos tratan de mitigar la capacidad de acceso, que es la propia capacidad para la que se han diseñado nuestras redes modernas. Claramente, esta ha sido una propuesta inoperante, ya que el costo de estas redes excede con mucho la asociada con los ataques y su penetración. Críticamente, también impide un acceso sin obstrucciones y un acceso oportuno a nuestras fuerzas a la información que tan críticamente necesitan.

El modelo de defensa del enclave de la red actual es paralelo a estas defensas perimetrales clásicas que limitan la capacidad de acceso a usuarios o transacciones aparentemente válidos. No obstante, hace poco por definir el fin detrás del esfuerzo. Así, sin entender claramente lo que hay que defender, nos queda la enorme tarea de defender toda nuestra "casa/fuerte" sin tener ninguna oportunidad de dar prioridad a un esfuerzo específico, como los que tendrán el máximo impacto en nuestra capacidad para llevar a cabo la misión.

Es esencial observar que nuestro método tradicional de protección usando solamente límites de redes es inútil cuando un adversario ya está dentro de la red. Según unos eventos recientes y dados los niveles actuales de complejidad de las redes, es poco probable que los adversarios aparezcan a través de ataques de rechazo de servicio concentrado como fue antes el caso. En vez de eso, llegaríamos a concluir que dichos enemigos ya existen en nuestras redes. En la realidad, tratan más de ocultar su presencia para lograr información que representa la savia de nuestras compañías, planes y propiedad intelectual. En consecuencia, las tres consideraciones principales que deben regularse por medidas de seguridad son (1) capacidad de acceso, (2) confidenciali-

dad (incluida la determinación de que los datos sean correctos y no se han alterado) e (3) integridad (que se relaciona con la esencia de nuestra confianza y dependencia de la información usada en el proceso de toma de decisiones). La complejidad de los ciberataques recientes realmente ha aumentado. Aunque en el pasado se concentraron en robar o manipular datos, dichos ataques tratan ahora no solo de robar datos críticos sino también de socavar su uso dentro de los centros de mando y control operacionales. De hecho, las amenazas que han permanecido latentes hasta que fueron accionadas por un evento específico (por ejemplo, ataques de día cero) pueden tener consecuencias devastadoras en los momentos más inoportunos durante las operaciones militares. Por lo tanto, debemos elevar nuestro conocimiento de dichas amenazas y gestionar el riesgo asociado determinando lo que debe defenderse, cómo se llevarán a cabo dichas defensas, qué objetivo se cumplirá y por qué es importante. Por último, las redes que continúan ofreciendo acceso sin límite (aunque es una cualidad que merece la pena) no podrán asegurar la propiedad intelectual que domina el entorno de información actual. Claramente, pues, debemos dar un paso atrás y preguntarnos lo que debemos defender. ¿Debemos proteger las carreteras y autopistas (es decir, la red) utilizadas por usuarios y adversarios al mismo tiempo o debemos proteger los datos y la propiedad intelectual internos?

Condición actual de la defensa de la empresa

Las defensas perimetrales de hoy están instrumentadas para análisis basados en tráfico de redes que suponen que no va a ocurrir nada malo en las aplicaciones/datos si esas defensas impiden transacciones de software malicioso en la entrada. La solución —basada en el reconocimiento rápido y uniforme de estas transacciones corruptas— da buen resultado si se saben y entienden *todas* las transacciones aceptables de modo que el complemento pueda caracterizarse como inaceptable (es decir, prohibiciones de tráfico de redes indeseable).

Otro método defensivo consiste en aislar la aplicación desde canales de acceso externos, pero los requisitos comerciales obligan el acceso a áreas dentro del perímetro para la colaboración (reparto de datos), interacción (servicios de la red), acceso móvil/remoto (red privada virtual), y enlaces intercomerciales. De ahí que sea muy difícil determinar qué tráfico hay que bloquear debido a múltiples excepciones que deben adaptarse para que funcione el negocio. Las prohibiciones se han hecho lentas y difíciles de mantener y no aumentan de escala bien, especialmente con la creciente adopción de IPv6.[2] Las listas de aprobación a nivel perimetral se han hecho imposibles de controlar debido a las miles de entradas para mantenerlas. El hecho de que los *muros* tengan que permitir un superconjunto de todas estas excepciones crea un perímetro poroso. Además, al añadir nuevas excepciones o eliminar otras existentes se pueden causar efectos inintencionados en otras aplicaciones, normalmente descubiertos solo después de la implementación. Para complicar aún más la situación está la continuación del requisito de mantenimiento —por ejemplo, persisten excepciones obsoletas en configuraciones debido a que no se notifica a los administradores a que hagan las actualizaciones.

La situación se complica aún más al aumentar la escala de las defensas de la red a miles de millones de transacciones. La respuesta normal para mantenerse al día con demandas de rendimiento ha sido aumentar el refinamiento y la escala de los aparatos de defensa. Desgraciadamente, estas "mejoras" significan más gastos generales y causan una mayor latencia (a pesar de parecer más rápidas o más robustas) y no siempre producen sistemas más efectivos.

Tiene que haber una forma mejor. Para defender mejor nuestra información, no solamente necesitamos reconocer ese hecho y tener en cuenta los adversarios entre nosotros, sino que también debemos continuar operando dentro de este entorno disputado. Como nuestros adversarios cibernéticos nos han hecho saber su presencia, debemos encontrar nuevas formas de defender la información vital (las joyas de la corona de hoy) que nos permita mantener nuestra ventaja

competitiva, a la vez que aceptar la idea de que operará en un entorno disputado. A medida que nos concentramos en nuestra propiedad y establecemos perímetros de seguridad más ajustados, también desarrollamos la capacidad de aumentar rápidamente la escala de nuestros métodos y de superar amenazas cada vez mayores.

Antes, la arquitectura de enclaves aislados era el diseño inicial de la red —cada grupo tenía su propio enclave sin conectividad exterior. El deseo de compartir información condujo a conectarse con estos enclaves, lo que generó cierta preocupación, pero existía un acuerdo de confianza entre ellos. A medida que los enclaves se conectaron cada vez más, el nivel de confianza se degradó aún más, especialmente cuando se perdió el control y se generalizó la anonimidad dentro de la World Wide Web. Volver a ganar esta confianza consistía en emplear defensas perimetrales de la empresa para controlar el acceso a la información y restringir la disponibilidad de datos para mantener cierto nivel de confidencialidad.

Aunque este problema se ha reconocido desde hace mucho tiempo y se han propuestos muchas alternativas, solamente se ha logrado un cierto éxito para salvaguardar la propiedad intelectual. La alternativa evidente es construir capas múltiples de defensas perimetrales de redes que proporcionen una confidencialidad adecuada de datos estratégicos. Sin embargo, este método requiere que se establezcan distintos ajustes, configuraciones o conjuntos de herramientas en cada punto en la defensa por niveles. Por último, dicha acción aumenta la carga de mantenimiento y produce demoras en el flujo de transacciones, la combinación de las cuales impide la diseminación oportuna de información vital.

Identificación/Reacción de incidentes

Al considerar que las defensas perimetrales de la red generan registros/alertas para miles de millones de transacciones en una gran organización, ¿cómo se analizan estas en una imagen coherente? Incluso mejor, ¿cómo se puede detectar en "tiempo real" que hay software malicioso presente y que puede prevenirse un incidente? Este problema es difícil porque existe poca información para determinar a qué aplicación pertenece una transacción específica a menos que las defensas adicionales de la red estén colocadas en múltiples ubicaciones en la empresa, normalmente cerca de centros de datos, para registrar y analizar todo el tráfico de la red. Por supuesto, esta situación genera incluso más datos para el análisis, y se acaba buscando la proverbial aguja en un pajar. Una solución evidente consiste en usar herramientas de análisis de "grandes datos" de fines especiales como técnicas de análisis predictivas, análisis de intercorrelación, y así sucesivamente, con gran capacidad de almacenamiento para transacciones históricas. Evidentemente, este análisis de gastos generales añade más costos y recursos para los esfuerzos de defensa. Tiene que haber una forma mejor.

Una forma mejor

Como se siguen produciendo ataques a pesar de nuestras mejores defensas perimetrales de redes, ¿qué pasaría si empezamos con la suposición de que los adversarios ya están en nuestras redes? En consecuencia, debemos ajustar nuestro modelo de amenaza y pensar de forma diferente para proteger nuestros datos y propiedades intelectuales. ¿Qué pasaría si disminuimos la superficie de ataque a nivel de aplicación o datos con las mismas capacidades de seguridad usadas actualmente para la defensa perimetral pero especializada para la aplicación o datos particulares? Esta visión radica en el núcleo de concepto de SEADE, que desactiva la superficie de ataque general de portales que protegen el perímetro de la red de la empresa a miles de enclaves de seguridad individuales especializados. La multitud de enclaves, consistentes en múltiples productos y configuraciones especializados, forzará al atacante a aumentar su esfuerzo para pene-

trar en una sola aplicación. Como cada enclave de seguridad se especializa en una aplicación específica, el atacante debe adaptar los ataques por cada aplicación en vez de concentrarse en penetrar el perímetro para exponer toda la red. Así, ya no será posible para los adversarios existir dentro de nuestras redes sin ser retado.

SEADE—Centro de datos de aplicaciones virtuales

La tecnología de virtualización, disponible en la *nube* o en centros de datos virtuales (VDC), ha hecho posible el concepto de centro de datos de aplicaciones virtuales. Un VDC es un centro de datos definido por software que es compatible con la "infraestructura como servicio" para aplicaciones. Es una materia disponible inmediatamente en muchos centros de datos de nubes comerciales y gubernamentales. Utilizamos un VDC para definir un VADC. Esencialmente, un VADC está especializado en una sola aplicación, que es compatible con la plataforma como servicio (PaaS). Consta de capacidades de monitoreo y defensa de redes virtualizadas como cortafuegos e inspección profunda de paquetes junto con su punto de acceso a la red asociado, cortafuegos de la base de datos y componentes de PaaS tradicionales de servidores de la web, servidores de aplicaciones y servidores de base de datos. El VADC de SEADE extiende este concepto para cada aplicación.

Una ventaja de seguridad significativa de esta arquitectura es que el tráfico de la red puede permanecer cifrado hasta que entre en el VADC. Solamente después de que entren los paquetes, se descifra e inspecciona el VADC. Dentro de cada VADC, el desarrollador de aplicaciones ha adaptado las defensas de inspección de la red, que se "cocinaron" desde la fase de diseño, hasta los puertos/protocolos específicos, tamaño/formato de la transacción, gama de parámetros, y así sucesivamente, para esa sola aplicación.[3] Por ejemplo, algunas aplicaciones pueden afinarse para ser compatibles con una inspección profunda de paquetes con anomalías informadas al proveedor de servicios de defensa de redes de computadoras apropiadas (CNDSP). La gestión de riesgos de aplicaciones individuales estimulará los requisitos de adaptación. El VADC mejorará los niveles de *capacidad de acceso y confidencialidad* reconociendo las amenazas específicas de inmediato e impidiendo que ocurra un incidente.

SEADE—Seguridad a nivel de empresa

ELS es un sistema dinámico de control de acceso basado en atributos desarrollado para reducir los riesgos de seguridad generales automatizando el proceso de acceso, basándose en información autoritativa relacionada con atributos.[4] Hoy, cada aplicación tiene un esquema de control de acceso configurado exclusivamente mantenido por administradores de sistemas, basado principalmente en usuarios y grupos, que pueden ser bastante laboriosos. En la Fuerza Aérea, el proceso se sobrecarga más por medio de un proceso de aprobación de acceso administrativo basado en formularios. Como nuevo paradigma, ELS automatiza el proceso de mantenimiento de autorización; convalida las condiciones preliminares de acceso, como capacitación, aprobación de seguridad, rango y así sucesivamente; y permite el acceso a una persona cuando se cumpla un conjunto de condiciones definidas por el propietario de la aplicación.

La accesibilidad a los datos es controlada por reclamaciones, basadas en los atributos de una persona (o una entidad), generada y propagada dinámicamente cuando cambian los atributos.[5] Las reclamaciones pueden ser adiciones, desaprobaciones o modificaciones a derechos de acceso existentes. Se transmiten por medio de canales cifrados, basadas en solicitudes de acceso del usuario en un símbolo de lenguaje de marcado para confirmaciones de seguridad (SAML). Un gestor estándar evalúa y convalida el símbolo (contenido, sincronización y autenticación) y pasa la reclamación al acceso a la aplicación. La conexión se produce por cada solicitud de acceso, y se envía una información de acceso errónea al CNDSP apropiado. Un gestor estándar se

asegura de que la validación de SAML y la conexión de acceso se efectúen de forma correcta, liberando aún más al desarrollador de aplicaciones para producir una capacidad similar.

ELS mejorará los niveles de *integridad y confidencialidad* impidiendo un acceso de datos no autorizado. Según se muestra en la figura de abajo, SEADE combina ambos conceptos (VADC y ELS) y se suministra con dos VDC—uno para la aplicación (VADC) y el otro para el motor de reclamaciones de ELS (que incluye el servicio de símbolo seguro, almacén de atributos de empresa y reclamaciones de SAML generadas).

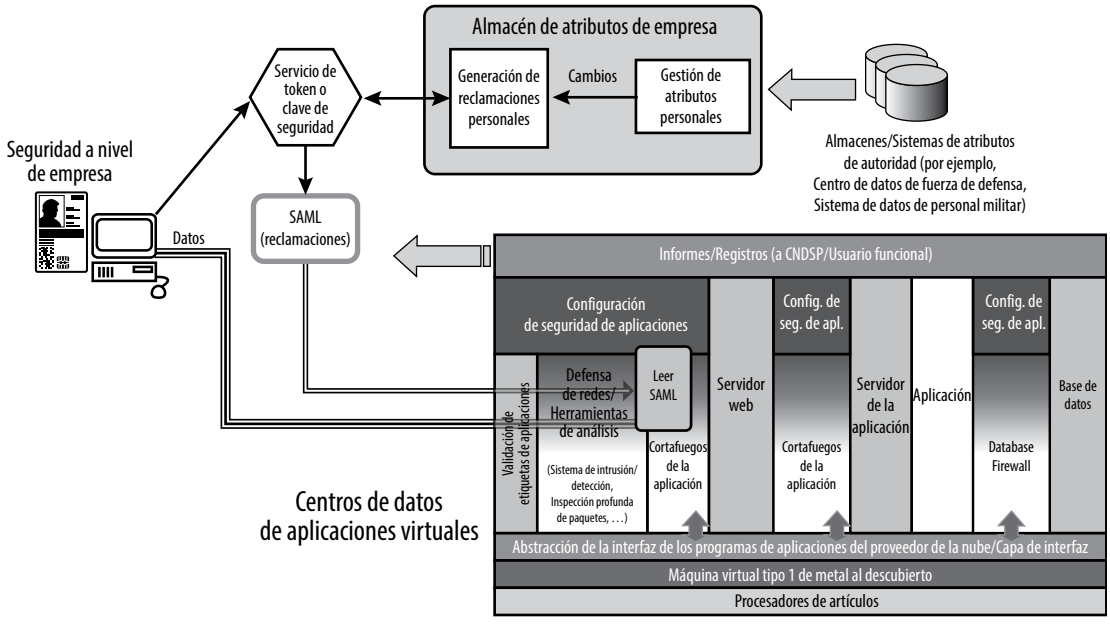

Diagrama de SEADE

Ventajas de SEADE

Al emplear SEADE en una operación a nivel de empresa grande se generan las ventajas siguientes:

- *Permite la transferencia de aplicaciones.* SEADE promociona dicha portabilidad permitiendo ejecutar aplicaciones en cualquier entorno virtualizado. Así, los propietarios tienen la libertad de maniobrar aplicaciones donde se necesitan para cumplir requisitos de operación y resistencia.
- *Acelera el despliegue de aplicaciones.* Múltiples empleos de SEADE en toda la empresa disminuirán significativamente la fuerza de trabajo asociada con el desarrollo y el despliegue de una aplicación. Como se incluyen defensas de redes y aplicaciones en un entorno PaaS estándar, la aplicación misma sigue siendo la lógica del programa al heredar todos los controles de seguridad del PaaS. Esta arquitectura ha disminuido de forma demostrada el tiempo de producción de meses a semanas. Como se puede usar un gestor de ELS están-

dar para el símbolo de SAML, el desarrollador de aplicaciones necesita un solo código de interfaz del programa de aplicaciones del gestor de ELS, disminuyendo más el tiempo de despliegue.

- *Facilita la acreditación.* Como las aplicaciones están encapsuladas con sus propias funciones de seguridad, la transferencia a nuevos entornos de servidores será mínima, incluida la justificación de las medidas de seguridad para satisfacer el proceso de acreditación.
- *Elimina las solicitudes de acceso individuales.* Se eliminará la dependencia de los procesos administrativos basados en formularios, y la carga de gestión de acceso de los administradores del sistema se reducirá de forma significativa. Ya no habrá permisos de usuarios y grupos para mantener por aplicación, reduciendo considerablemente las personas-hora requeridas para realizar esta función básica de administración del sistema.
- *Proporciona un acceso inmediato al usuario.* Los usuarios tendrán acceso inmediato a aplicaciones y datos, basándose en sus atributos (por ejemplo, posición, capacitación, ubicación del servicio, y así sucesivamente). Tan pronto como se actualice la fuente de datos con autoridad con información de su personal —por ejemplo, a una nueva asignación— entonces se otorgará a los usuarios un acceso correspondiente.
- *Incluye una seguridad "cocinada".* El desarrollo de aplicaciones cambiará fundamentalmente cocinando la seguridad desde un principio. Los desarrolladores integrarán las configuraciones de defensa de la red (por ejemplo, listas blancas) en su VADC. Además, tendrán más opciones y unas capacidades relacionadas con la seguridad más fuertes al tener diversos aparatos de la red a su disposición. Los desarrolladores deben pensar ahora de forma integrada y producir aplicaciones para responder y relacionarse con entradas definidas, válidas y reconocidas.
- *Se concentra en informes de incidentes.* En vez de hacer que los combatientes de la guerra cibernética busquen en corrientes de transacciones de la red, tratando de determinar una anomalía, los informes de incidentes se reducen a la aplicación real con información detallada, basada en el perfil de seguridad adaptado de la aplicación. El CNDSP será alertado solamente cuando se accionen umbrales.
- *Reduce el número de administradores de la red.* Los operadores de seguridad de la red ya no tendrán que hacer cambios de configuración de los aparatos de la red (por ejemplo, cortafuegos, servidores y sistemas de detección de intrusiones) para "permitir solamente" un tráfico legítimo y bloquear el tráfico malo conocido. Además, se pasará menos tiempo en reuniones de gestión de configuración para aprobar cambios pequeños a aparatos de la red.
- *Proporciona una resistencia operacional.* Como el VADC está compuesto exclusivamente de componentes virtuales, si se detecta una anomalía, la aplicación puede volver a cargarse dinámicamente a partir de una buena imagen cargada anteriormente, o instantánea, para continuar el procesamiento. Como medida de resistencia adicional, los casos de SEADE pueden generarse en múltiples lugares y numerosos entornos para obtener una mayor redundancia y un mayor control de la misión.
- *Permite la continuidad de operaciones (COOP) y agilidad.* Al hacer uso de la virtualización, se pueden suministrar aplicaciones en entornos múltiples, así como COOP en otros centros de datos, siempre que los datos se hayan descargado en el sitio de COOP. Esta capacidad de aprovisionamiento en cualquier lugar disminuye más el tiempo de aprovisionamiento y agiliza la misión de forma significativa.
- *Reduce la amenaza interior.* Este nuevo paradigma permite métodos creativos para la protección de datos. La vulnerabilidad a una amenaza interior se reducirá debido a que el ELS bloqueará el acceso no autorizado y rastreará todo el acceso a aplicaciones o datos. Esta información se puede usar para detectar o predecir actividades anómalas. Con etiquetado de acceso de datos apropiado, los datos exfiltrados serán ilegibles fuera de un entorno sin SEADE.

- *Mejora la confidencialidad, la integridad y la disponibilidad*. La combinación SEADE de capacidades de ELS y VADC aumenta significativamente la *confidencialidad y la integridad* de los datos impidiendo el acceso no garantizado y la *disponibilidad* de la aplicación (y datos) por medio de un análisis dinámico y la eliminación de amenazas de la aplicación misma.
- *Mantiene la CNDSP*. La estructura actual de la CNDSP no tiene que cambiar. Las alerta dentro de cada SEADE pueden enviarse a la unidad de CNDSP apropiada, que seguirá determinando las prioridades de las alertas de forma correspondiente.

Ventajas relativas

La ventaja relativa principal al emplear SEADE es que en vez de confiar y deferir a la seguridad perimetral de la red, los desarrolladores de aplicaciones serán responsables ahora de tener en cuenta la seguridad de la aplicación y controles de ELS durante el diseño, la prueba y el desarrollo. Los desarrolladores deben familiarizarse de forma íntima con su aplicación para tratar temas de estímulos esperados y desconocidos. Esto aumentará sin duda el costo inicial de desarrollo del sistema, pero con el tiempo ahorrará innumerables personas-hora y mejorará la protección de datos. Los desarrolladores serán responsables de cerciorarse de que la seguridad se incorpore desde el principio en vez de esperar a que los operadores traten la necesidad de forma retroactiva.

Otra ventaja relativa es la formación de un entorno de apoyo para servicios de SEADE. Los propietarios de aplicaciones y funcionales deben definir y regular atributos para proporcionar la granularidad necesaria para que las aplicaciones tengan el nivel correcto de fidelidad de control de acceso. Esto atributos deben provenir de fuentes de datos con autoridad conocidas que tienen que identificarse e integrarse en el almacén de atributos de la empresa para uso del ELS.

Líneas de referencia de tecnología de información de empresas consolidadas de la Fuerza Aérea

Hoy en día, la tecnología se mueve tan rápido que no se alcanzará nunca la mejor solución del 100 por cien en un tiempo razonable. El suministro de soluciones ágiles es la mejor forma de tratar un problema mediante desarrollos de software concentrados y un desarrollo espiral de modo que uno se pueda ajustar a medida que cambia la tecnología disponible. Esto permite la capacidad de aprovecharse y adquirir una ventaja estratégica de acciones ágiles y soluciones innovadoras. Desgraciadamente, este cambio de paradigma desconcierta a muchas personas que esperan requisitos predefinidos con puntos finales predestinados. No obstante, este método tradicional solo desperdicia recursos a medida que cambian el entorno y el requisito en su medio. A medida que las cosas varían constantemente en tecnología y ciberespacio, debemos poder ser adaptables y decidir aventurarnos para adoptar los cambios —a menos que nos arriesguemos a quedarnos atrás.[6] Debemos dominar y guiar este espíritu de innovación y proporcionar una estructura para insertar una nueva tecnología —de forma metódica y rápida— en nuestro entorno.

De forma correspondiente, es en esta vena que el oficial de tecnología principal de la Fuerza Aérea estableció y gestionó la estructura de Líneas de Referencia de Tecnología de Información de Empresas Consolidadas (CEIT-B) para conformar, adoptar y suministrar un entorno de tecnología de información estándar a propósito. Este esfuerzo disciplinado se conforma al paradigma ágil a medida que se desarrolla la línea de referencia del objetivo futuro.[7] SEADE es un componente sustancial de CEIT-B que trata de los requisitos de seguridad, transferencia y eficiencia. Además, la Fuerza Aérea, a través de CEIT-B, trata e informa de los requisitos del entorno de información conjunto (JIE) para requisitos de empresa a nivel del Departamento de Defensa.

Conclusión

La Fuerza Aérea, como servicio, emergió de la tecnología. Debemos seguir dominando el mismo espíritu innovador del ciberespacio que nos ha permitido dominar el aire y el espacio. La innovación es el combustible del éxito en el futuro, y debemos esforzarnos en nuevas formas de resolver nuestros problemas difíciles. SEADE, compuesta por un VADC y ELS, es un paradigma fundamentalmente diferente que cambiará la forma en que se desarrollan, despliegan y defienden los sistemas. Al proporcionar un enclave de seguridad separado para aplicaciones en un VADC, habilitado por un control de acceso dinámico ELS, podemos proteger nuestro tesoro más importante —los datos internos— a medida que continuamos operando en un entorno disputado. La arquitectura de SEADE aumentará la velocidad de acceso del usuario y el suministro de la aplicación a la misión, disminuirá la gestión diaria de la red y de las aplicaciones, y contrarrestará la inutilidad de la seguridad perimétrica de la red.❑

Notas

1. Cheryl Pellerin, "Carter Unveils New DoD Cyber Strategy in Silicon Valley" (Carter revela la nueva estrategia cibernética del Departamento de Defensa en Silicon Valley), Departamento de Defensa de EUA, 23 de abril de 2015, http://preview.defenselink.mil/news/newsarticle.aspx?id=128659.
2. IPv6 (Protocolo de Internet versión 6) es el último protocolo estándar de Internet que usa 128 bits en vez de los 32 bits actuales de IPv4. La nueva versión tiene capacidad para que cada habitante de la Tierra tenga miles de millones de direcciones de Internet asignadas personalmente. Por lo tanto, el bloqueo por dirección individual o gama de direcciones dejará der ser efectivo o eficiente.
3. "Cocinado" se refiere a integrar características de seguridad deseadas en la etapa inicial de diseño y desarrollo en vez de añadirlas después de haber publicado el producto.
4. Vincent Hu, Adam Schnitzer y Ken Sandlin, "Attribute Based Access Control Definition and Considerations" (Definición y consideraciones de control de acceso basadas en atributos), Publiación Especial del Instituto Nacional de Normas y Tecnología 800-162, n.d., http://csrc.nist.gov/projects/abac/july2013_workshop/july2013_abac_workshop_abac-sp.pdf.
5. Coimbatore S. Chandersekaran y William R. Simpson, "A Uniform Claims-Based Access Control for the Enterprise" (Control de acceso uniforme basado en reclamaciones para la empresa), *International Journal of Scientific Computing* 6, no. 2 (diciembre de 2012): 1–23.
6. Spencer Johnson, *Who Moved My Cheese? An Amazing Way to Deal with Change in Your Work (¿Quién me ha movido el queso? Una forma asombrosa de enfrentarse a los cambios en su trabajo)* (New York: G. P. Putnam's Sons, 1998).
7. SAF/CIO A6 CTO, *CIET-B, Target Baseline 2.0*, 2015, https://intelshare.intelink.gov/sites/afceit/TB/default.aspx.

Frank Konieczny (BS, MS, Universidad of Illinois–Chicago; MAS, Universidad de Alabama–Huntsville), ejecutivo de nivel superior, es el oficial en jefe de tecnología de la Fuerza Aérea, Oficina de Dominio de Información y oficial en jefe de información, Oficina de la Secretaría de la Fuerza Aérea, Pentágono, Washington DC. Antes de asumir sus responsabilidades actuales, adquirió gran experiencia en la industria, donde trabajó como analista de sistemas, programador jefe, director de proyectos y gerente de unidades comerciales, incluidas posiciones como científico y oficial jefe de tecnología.

Teniente Coronel Eric D. Trias, PhD, USAF (BS, Universidad de California–Davis; MS, Instituto de Tecnología de la Fuerza Aérea [AFIT]; PhD, Universidad de New Mexico) es el jefe en funciones, División de Arquitectura de Empresas de la Fuerza Aérea, Directorio de Estrategia y Política Ciberespaciales, Secretario de la Fuerza Aérea, Oficina de Dominio de Información y Oficial en Jefe de Información, Pentágono, Washington, DC. Encargado de regular, desarrollar y mantener la arquitectura de la empresa de la Fuerza Aérea, también sirve como oficial subjefe de tecnología de la Fuerza Aérea, ayudando a evaluar y definir futuras normas de tecnología de información y límites de implementación para la infraestructura de empresas de tecnología de información de la Fuerza Aérea. El Teniente Coronel Trias ha servido como profesor ayudante en AFIT, comandante de un gran destacamento, y subcomandante de escuadrón desplegado. Ha ocupado varias posiciones de liderazgo en un escuadrón de comunicaciones de base, escuadrón de control de ejercicios y escuadró de comunicaciones de combate.

Coronel Nevin J. Taylor, USAFR (BS, Universidad del Estado de New York; MS, Universidad Capella) es personal de aumento de movilización individual (IMA) del director de estrategia y política ciberespaciales, oficial subjefe de tecnología para programas especiales y Miembro de la Junta Estratégica de la Fuerza de Tarea Cibernética en la Oficina de Dominio de Información y Oficial Jefe de Información, Oficina de la Secretaría de la Fuerza Aérea, Pentágono, Washington, DC. Es un profesional del espacio con 10 años de experiencia y del ciberespacio con 20 años de experiencia con más de una experiencia de mando y una plétora de diversos conocimientos expertos operacionales únicos, incluido combate, comunicaciones fijos y espaciales, apoyo de la misión, adquisiciones, política, estrategia, planificación, ciberespacio y espacio. Entre las asignaciones conjuntas del Coronel Taylor se incluyen director de Reservas de Componentes, Mando de Componentes Funcional Conjunto para el Espacio, Mando Estratégico de EUA; ayudante militar superior del subsecretario adjunto de defensa para la integración de políticas; y jefe de estado mayor así como IMA del subsecretario de política del Departamento de Defensa en la Secretaría de Defensa.