DOCUMENTO TÉCNICO

PRINCIPIOS FUNDAMENTALES DE CIBERINTEGRIDAD EN CUANTO A CLOUD Y MOVILIDAD

vmware | intel

Índice

Introducción

La ciberseguridad es uno de los principales problemas a nivel directivo en las administraciones públicas y las empresas de todo el mundo. Ahora más que nunca, los altos cargos de administraciones públicas y empresas (desde senadores y diputados hasta directores ejecutivos y consejeros) están profundamente comprometidos con la implantación de estrategias de ciberseguridad eficaces en organismos públicos y empresas.

No obstante, pese a que la inversión en ciberseguridad aumenta, se siguen produciendo vulneraciones con una frecuencia alarmante. Hay algo que no va bien. ¿Qué es? ¿Y cómo se soluciona? Existen muchas teorías sobre cómo actuar, desde atenerse a los nuevos marcos de control, hasta desarrollar nuevos productos y servicios.

En VMware, somos de la opinión de que no se va a mejorar la eficacia de la seguridad de la información por implantar nuevos marcos de trabajo o por comprar un producto en particular. La respuesta reside en volver a los principios básicos de una informática con privilegios mínimos, además de integrar la seguridad en la propia arquitectura, en lugar de añadirla «a posteriori». Esto ha sido un aspecto intrínsecamente complicado para las organizaciones, sin embargo, gracias a las nuevas funcionalidades que incorpora la informática de cloud y móvil, ahora es algo que resulta viable por no decir fundamental.

Para adoptar un enfoque de seguridad más eficaz, se deben seguir dos pasos fundamentales: implementar una ciberintegridad básica y centrarse en proteger las aplicaciones esenciales para la empresa, es decir, las «joyas de la corona».

En este documento, proponemos los **cinco principios fundamentales de la ciberintegridad** como valores de referencia universal, es decir, como los aspectos más importantes y elementales que deberían tener en cuenta las organizaciones. Los conceptos no son nuevos, pero son fundamentales para avanzar hacia una seguridad más efectiva. Tienen su origen en marcos de trabajo muy consolidados como, por ejemplo, el marco de trabajo de ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST) estadounidense, y brindan un enfoque de neutralidad tecnológica. Tenemos la firme convicción de que si se hubieran aplicado estos principios eficazmente, las cosas habrían sido muy diferentes en el caso de las vulneraciones de datos más graves de los últimos años, como las de Target, Sony o la Oficina de Administración de Personal (OPM) de los Estados Unidos.

DEFINICIÓN DE «CIBERINTEGRIDAD»

Este término tiene diversos significados. Lo utilizamos para referirnos a los aspectos básicos que deberían implantar las organizaciones para la ciberdefensa.

Este concepto difiere de otra visión común de la ciberintegridad, que se refiere a lo que hacen los consumidores en línea para proteger de infecciones sus actividades en la red.

En cualquier caso, no resulta fácil implementar los principios fundamentales de ciberintegridad de forma efectiva, y las organizaciones llevan años teniendo problemas para conseguirlo. Aunque sea difícil ponerle peros a las ventajas de la informática con privilegios mínimos (o de «confianza cero») en lo que a seguridad se refiere, muchos consideran que resulta imposible implantarla desde el punto de vista operativo. Por tanto, también sugerimos a las organizaciones que centren sus iniciativas de seguridad en la protección de las aplicaciones, en particular, las aplicaciones empresariales esenciales, que son sus «joyas de la corona» y donde resulta más sencillo llevar un control de los comportamientos. Por otra parte, se recomienda emplear los modernos métodos de macrodatos y aprendizaje automático para consolidar comportamientos adecuados, en lugar de dedicarse a perseguir actividades malintencionadas.

El propósito de este documento es ayudar a los responsables de administraciones públicas y de empresas a entender los problemas específicos de las estrategias de ciberseguridad actuales y cómo adoptar un enfoque mejor. Se ha concebido para responsables de empresas que están involucrados en cuestiones de ciberseguridad, pero que no son necesariamente expertos técnicos. Para los profesionales de la seguridad y otras personas que estén interesados en detalles más técnicos, ofrecemos una serie de apéndices que incluyen sugerencias prácticas para la implementación.

Mejorar la ciberseguridad es una de las prioridades en las agendas de administraciones públicas y empresas. Como expertos en tecnologías de cloud y movilidad, para nosotros es un orgullo participar con nuestra perspectiva única en la mejora de la ciberseguridad. Gozamos de una posición privilegiada y práctica desde la que poder afrontar los desafíos de seguridad. Aportamos nuestra capacidad de ver las cosas desde un punto de vista distinto.

El problema de la ciberseguridad

El gasto global en seguridad no deja de aumentar, y se estima que la tasa de crecimiento anual compuesta hasta 2020 se situará en el 8,7 %.[1] Con todo, la cifra anual de vulneraciones de datos en Estados Unidos alcanzó un récord histórico el año pasado.[2] Empresas y administraciones públicas de todo el mundo pierden cerca de 500 000 millones de dólares al año debido estas vulneraciones de datos.[3] A todas luces, hay algo que no funciona. ¿Qué es? ¿Qué se puede hacer al respecto?

No es por falta de orientación

Las carencias en ciberseguridad evidentemente no se deben a una falta de orientación sobre los procedimientos que deben seguir las organizaciones para proteger la información. Existen numerosas normas empresariales y de la administración pública ampliamente aceptadas sobre la seguridad de la información en Estados Unidos y en todo el mundo, como NIST, ISO y SANS, entre otras. Todas ellas remiten a una lista exhaustiva de prácticas recomendadas y consensuadas.

La complejidad es abrumadora

La complejidad de los enfoques actuales dificulta enormemente la implementación de unas prácticas recomendadas exhaustivas en todo el entorno de TI. La variedad de herramientas de seguridad que deben gestionarse es muy amplia: cortafuegos, antivirus, sistemas de prevención de intrusiones y sistemas de detección de amenazas, por nombrar algunas de ellas. Cada herramienta incorpora una cantidad ingente de reglas que también se deben gestionar. Cada una de ellas debe configurarse para que aplique políticas de control de acceso o de protección de la información en todo el ámbito de la empresa, para todos los usuarios y sistemas de la organización. En algunos casos, esto puede suponer millones de reglas. Configurar todo es abrumador. Además, el panorama de las amenazas no cesa de cambiar, lo que complica mucho las cosas.

Cambios constantes

Por otra parte, no basta con configurar las herramientas de seguridad una sola vez y después olvidarse de ellas. Los sistemas deben actualizarse constantemente para seguir el ritmo de la actividad empresarial y proteger frente a las vulnerabilidades que se han detectado recientemente.

La automatización es inalcanzable

El método DevOps y los métodos utilizados en las aplicaciones modernas siguen aumentando el ritmo de cambio de las aplicaciones y de la infraestructura. A pesar de que esto es un facilitador empresarial extraordinario, complica aún más los procesos de seguridad. Con demasiada frecuencia la seguridad se considera un impedimento a la hora de distribuir aplicaciones e infraestructuras modernas según las necesidades. Pese a que las organizaciones disponen de muchas herramientas para automatizar las tareas de seguridad, no las utilizan de forma coordinada con la automatización de las infraestructuras.

Las organizaciones deben adoptar la automatización como una forma de configurar las políticas de seguridad, en lugar de contemplarla como un problema para la seguridad. La mayoría de las herramientas de automatización de infraestructuras disponen de manifiestos extremadamente declarativos que describen el estado deseado de la infraestructura y de las aplicaciones; además, se pueden utilizar como método para aplicar las directrices de privilegios mínimos y mantener el ritmo de los cambios sin necesidad de realizar ajustes manuales en las reglas.

[1] «Worldwide Semiannual Security Spending Guide», IDC, marzo de 2017

[2] «Data Breach Report 2016», Identity Theft Resource Center (ITRC), 2. Identidad

[3] «Net Losses: Estimating the Global Cost of Cybercrime», Center for Strategic International Studies, junio de 2014

Dar respuesta a las alertas es un proceso laborioso

Otra dificultad es la carga de trabajo que supone hacer un seguimiento de las alertas de seguridad. Cada una de las herramientas de seguridad de una organización envía miles de alertas al día, en algunos casos, cada hora. Los clientes de mayor tamaño confían en los sistemas de gestión de eventos e incidencias de seguridad (SIEM) para correlacionar estas alertas y eventos, y establecer prioridades de investigación. Sin embargo, si no se dispone del contexto suficiente resulta difícil establecer la prioridad de las alertas, y la mayoría de las veces se convierte en un proceso demasiado manual. Por ejemplo, una herramienta de detección puede indicar que se está desarrollando una actividad sospechosa en la red, pero no explica cuáles son los sistemas afectados, el nivel de riesgo o las posibles medidas que se deben tomar.

Las organizaciones dependen de las personas para llevar a cabo funciones de seguridad, pero no hay personal suficiente formado en ciberseguridad.

Seguridad más efectiva en dos pasos

Gracias a los recientes avances en informática de cloud y móvil, ahora es posible simplificar y automatizar más la seguridad. Existen dos pasos fundamentales que se deben seguir: implementar la ciberintegridad y centrarse en proteger las aplicaciones esenciales para la empresa, es decir, las «joyas de la corona».

Paso 1: implementar los principios fundamentales de la ciberintegridad

Se trata de los principios más importantes y básicos que deberían adoptar las organizaciones.

La base: la formación

Se debe implantar un proceso obligatorio de formación para todos, desde profesionales de TI y responsables empresariales a empleados y trabajadores externos.

- Los profesionales de TI deberían comprometerse a integrar la seguridad en el diseño de los sistemas.
- Los desarrolladores deben adquirir un mínimo de conocimientos sobre la seguridad del código.
- Los arquitectos de sistemas deben comprometerse a conseguir resultados en materia de seguridad. El nivel de conocimientos básicos en cuestiones de seguridad debería ser similar al nivel de conocimientos sobre recursos informáticos, redes o almacenamiento.
- Los usuarios finales deben ser conscientes de los riesgos y de sus responsabilidades a la hora de proteger la información. Los aspectos básicos de la seguridad deberían entenderse tan bien como acceder a un sitio web o comprobar el correo electrónico.

MICROSEGMENTACIÓN:

La protección del entorno de TI fraccionándolo en porciones más pequeñas es similar al uso de compartimentos estancos en un barco. Hace que resulte más sencillo proteger el barco. Si el barco resulta dañado en una zona, el daño solo afectará a esa zona.

Los principios fundamentales

Con un plan de formación bien definido, estos cinco principios son fundamentales para lograr una seguridad más efectiva:

1. Informática con privilegios mínimos	Las aplicaciones deben ejecutar exclusivamente los componentes mínimos necesarios para realizar sus funciones y nada más (control de aplicaciones y lista blanca). Las cuentas de usuarios o sistemas en las máquinas de centros de datos deben ocuparse de las funciones mínimas necesarias para llevar a cabo su cometido y nada más.
2. Microsegmentación	La red debe dividirse en pequeñas porciones para que resulte más sencillo protegerla y para limitar el daño si una parte está en peligro (vea la columna izquierda).
3. Cifrado	En cuanto a los procesos empresariales esenciales, se deben cifrar todos los datos cuando se almacenen o transmitan. Si se produjera una vulneración de datos, los archivos esenciales robados solo contendrían datos ilegibles.
4. Autenticación multifactor	La identidad de los usuarios y los componentes del sistema debe comprobarse mediante varios factores (no únicamente contraseñas) y de forma proporcional a los riesgos que entraña la función o el acceso que se haya solicitado.
5. Aplicación de parches	Los sistemas deben estar actualizados y sometidos a un mantenimiento continuo. Los sistemas esenciales que no están actualizados representan un riesgo importante para la seguridad.

Principios bien establecidos

Estos principios fundamentales no son conceptos nuevos. Se basan en principios muy consolidados. Por ejemplo, se corresponden con diversas funciones del CSF del NIST (vea el apéndice 1).

Estos principios solo representan una pequeña parte de los aspectos que cubren el CSF del NIST y otros marcos de trabajo. Sin embargo, se trata de principios clave que permitirán la adopción de un enfoque más sencillo y automatizado.

Si estos cinco principios se aplican de forma correcta y sistemática, será más difícil llevar a cabo ciberataques y estos serán menos dañinos. Incluso en el caso de las vulneraciones de datos más graves de los últimos años, creemos que si se hubieran aplicado estos principios eficazmente, las cosas habrían sido muy diferentes (véase más abajo).

Vulneraciones graves en las que no se habían implementado eficazmente los principios fundamentales

Principio	**Ejemplos de vulneraciones** Nota: Hay muchos factores que pueden explicar una vulneración de datos. Estos ejemplos muestran casos donde no implementar eficazmente alguno de los principios fundamentales ha provocado una vulneración, aunque también podrían intervenir otros factores.
1. Informática con privilegios mínimos	Si el control de las aplicaciones no se implementa con eficacia y se concede libertad a los usuarios, o a los sistemas, para ejecutar más tareas de las que necesitan, los atacantes pueden aprovecharse de un acceso tan laxo para sus actividades malintencionadas y, en muchas ocasiones, sin necesidad de utilizar programas maliciosos conocidos. Por ejemplo, en las vulneraciones de Target y Sony, los atacantes consiguieron privilegios de administrador y ejecutaron comportamientos ajenos a la actividad normal de la aplicación.
2. Microsegmentación	Si la microsegmentación no se implementa con eficacia, los atacantes pueden irrumpir en una zona de la red y, después, pasar con facilidad a otras zonas. Por ejemplo, en la vulneración de Target, los atacantes se infiltraron en el sistema de aire acondicionado y calefacción y de ahí pasaron al sistema de la red de pagos. En el caso de la vulneración de Sony, los atacantes también pudieron pasar de una parte de la red a otra. En cuanto a la vulneración de la OPM, los atacantes obtuvieron acceso a la red de área local y, posteriormente, se dirigieron al centro de datos del Departamento del Interior.
3. Cifrado	Si no se ha implementado un método eficaz de cifrado, los atacantes pueden robar datos en formato legible. Por ejemplo, después de una vulneración de datos en Royal & Sun Alliance Insurance PLC, los inspectores enviados por la administración pública determinaron que la empresa no había cifrado los datos debidamente.
4. Autenticación multifactor	Si no se ha implementado eficazmente la autenticación multifactor (MFA), los atacantes podrán obtener contraseñas y utilizarlas para acceder a los sistemas. Por ejemplo, en el caso de la vulneración de datos que afectó a la OPM, si se hubiera aplicado una autenticación multifactor adecuada al nivel de riesgo para los inicios de sesión de los trabajadores externos, la capacidad de los atacantes para utilizar las credenciales robadas al trabajador externo de la administración habría sido limitada. Con respecto a la vulneración de LinkedIn, el ataque puso en peligro las contraseñas de 100 millones de usuarios porque no estaban protegidas adecuadamente. Dado que los consumidores suelen utilizar contraseñas en muchos sitios, la MFA habría reducido los riesgos.
5. Aplicación de parches	Si la aplicación de parches no se implementa de forma eficaz, los atacantes pueden aprovechar las fisuras de los sistemas. Por ejemplo, el ataque del programa de secuestro WannaCry aprovechó una vulnerabilidad de software conocida, para la que además existía un parche. Las organizaciones que sufrieron el ataque no habían aplicado el parche correctamente.

No es fácil implementar los principios fundamentales con eficacia

Los profesionales en materia de seguridad de la mayoría de las organizaciones están muy familiarizados con estos principios, y la mayor parte de ellos no cuestiona su efectividad cuando se implementan debidamente. De hecho, incluso en las organizaciones que han sufrido vulneraciones es posible que el equipo de seguridad haya intentado (sin éxito) ponerlos en práctica. El problema es que todo esto resulta muy difícil de lograr debido al enfoque actual que utilizan la mayoría de las organizaciones, con las herramientas y técnicas de las que disponen.

«Joyas de la corona = aplicaciones esenciales»

Paso 2: centrarse en proteger las aplicaciones esenciales *individuales*

El paso siguiente es centrarse en proteger las aplicaciones esenciales individuales. De esta forma, resultará más sencillo implementar eficazmente los principios fundamentales de la ciberintegridad.

Centrarse en las aplicaciones esenciales pone el foco de atención donde debe estar: en las «joyas de la corona». En definitiva, las «joyas de la corona» de una organización son las aplicaciones empresariales esenciales y los datos que contienen. Algunos ejemplos pueden ser: una aplicación financiera empresarial que procesa datos confidenciales durante la creación de los estados financieros de la empresa; una aplicación de gestión de pedidos que cumplimenta los pedidos de los clientes, lo que incluye almacenar la información personal y los datos de tarjetas de crédito; una aplicación de recursos humanos que contiene datos confidenciales sobre los empleados; o una aplicación de investigación y desarrollo que contiene secretos comerciales. La aplicación es el mecanismo para acceder e interactuar con los datos.

Pese a que el objetivo de la seguridad de la información es proteger estas «joyas de la corona», los métodos actuales se centran en la protección de la infraestructura de TI, como los enrutadores (hardware que enruta el tráfico de una red) o los servidores (ordenadores que suministran potencia de procesamiento). Lo que es aún peor, la mayoría de las herramientas consideran que estos componentes de la infraestructura son genéricos y no aprovechan el contexto de las aplicaciones que intentan proteger. Proteger la infraestructura de TI es necesario, pero insuficiente.

Enfoque basado en los riesgos

El valor para la empresa reside en los datos y las aplicaciones esenciales. Si estos activos estuvieran en peligro, la organización correría riesgos considerables. La infraestructura proporciona los recursos que necesita la aplicación para funcionar, pero no es en sí un recurso esencial.

Sea más específico

Centrar la seguridad en la infraestructura no es suficientemente específico. Es como intentar proteger todas las casas de una urbanización poniendo alrededor una valla y una verja con llave; sería más eficaz centrarse en proteger cada casa de manera individual (vea el diagrama 1 más abajo).

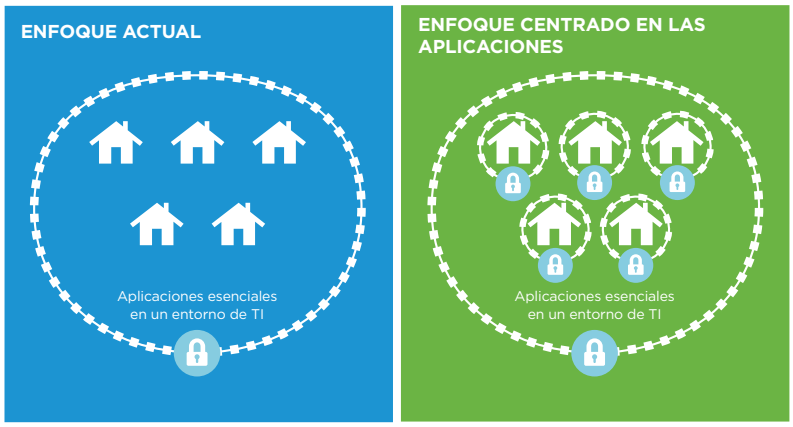

Diagrama 1: El método que se utiliza actualmente para proteger los entornos de TI es como intentar proteger todas las viviendas de una urbanización poniendo alrededor una valla y una verja con llave. Sería más eficaz centrar la atención en proteger las viviendas (aplicaciones esenciales) con vallas y llaves en cada una de ellas.

Control del acceso a cada aplicación individual

Con los métodos actuales, resulta difícil cumplir los objetivos de seguridad, como es garantizar exclusivamente el acceso mínimo necesario. Por ejemplo, un cortafuegos, por lo general, se configura en el perímetro de toda la empresa (como la valla que rodea la urbanización) para controlar el acceso a un grupo de aplicaciones que, en muchas ocasiones, puede estar formado por miles de ellas. En este caso, la efectividad de la política de cortafuegos para cualquier aplicación es igual a la de la aplicación menos protegida de ese grupo. En su lugar, debería configurarse un cortafuegos para controlar el acceso a cada aplicación esencial (como las casas individuales), de forma que solo se permitiera acceder a los usuarios y a los componentes del sistema que precisaran acceso a una aplicación concreta (una vivienda).

La seguridad también debe ser más eficiente. Imagine que los vigilantes de la entrada reciben una llamada de teléfono para avisarles de una actividad inusual en la urbanización. Es posible que los vigilantes tengan que pasarse el día buscando esa actividad inusual por toda la urbanización. Sería mucho más eficiente que los vigilantes supieran exactamente a qué vivienda acudir, si está vacía o llena de objetos valiosos, y si ese tipo de actividad es normal en la vivienda (vea el diagrama 2 más abajo).

Supervisión lo más cerca posible de la aplicación

Los sistemas de supervisión de la seguridad, por lo general, envían una alerta que indica que se produjo una intrusión en la red o en una parte de ella sin especificar la aplicación. El equipo de ciberseguridad debe invertir mucho tiempo en investigar. Sería mejor si se evaluara inicialmente el evento en busca de una posible actividad malintencionada en el entorno más cercano a la aplicación antes de remitirlo al sistema central de gestión de eventos. De esta forma, las alertas serían muy fiables ya que indicarían qué aplicación se ha visto afectada, la gravedad de la intrusión, y si la actividad que se detectó era legítima en esa aplicación.

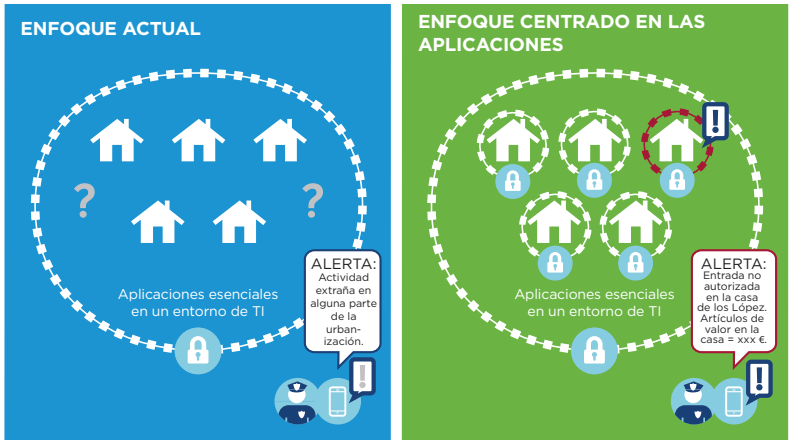

Diagrama 2: La supervisión actual de los entornos de TI se basa en un enfoque que se asemeja al del vigilante que recibe un aviso sobre una actividad extraña en algún lugar de la urbanización. Sería más eficaz si el vigilante supiera exactamente de qué casa (aplicación esencial) se trata y qué ha ocurrido.

APLICACIONES MODERNAS: SISTEMAS DISTRIBUIDOS Y DINÁMICOS

- Cada aplicación individual es un «sistema» de componentes.
- Las funciones (o servicios) de software utilizan un depósito de recursos de redes, procesamiento, memoria y almacenamiento.
- Los recursos se diseminan en el entorno de TI (probablemente en la totalidad del propio centro de datos de la organización y los proveedores de cloud).
- Muchas aplicaciones comparten depósitos de recursos.
- El uso de los recursos cambia rápidamente a lo largo del tiempo.

¿Por qué no lo han adoptado aún las organizaciones?

Si centrarse en las aplicaciones esenciales de forma individual con ciberintegridad mejora la efectividad de la seguridad, habría que preguntarse por qué las organizaciones no lo están haciendo. Dadas las tecnologías y técnicas que utiliza actualmente la mayoría de las organizaciones, sencillamente esto no es viable.

Los métodos actuales no permiten definir claramente las aplicaciones individuales

Las aplicaciones modernas se han diseñado a modo de sistemas distribuidos y dinámicos. Los servicios que distribuyen las aplicaciones se encuentran diseminados en múltiples máquinas, con funciones de software que utilizan un depósito de recursos compartidos que va cambiando con el tiempo (véase la columna izquierda). Con los métodos actuales, las herramientas de seguridad no son capaces de identificar ni de entender estos servicios, ni la manera en que forman parte de las aplicaciones.

Con los métodos actuales, las herramientas de seguridad:

- No pueden identificar que «estos servicios» forman parte de la «Aplicación A».
- No saben qué usuarios deben tener acceso a la «Aplicación A».
- No saben con exactitud cuál de las infraestructuras es responsable de distribuir los servicios de la «Aplicación A».
- No saben cómo deben permitir que los servicios se comuniquen entre sí como parte de la «Aplicación A».
- No pueden llevar un seguimiento de los cambios en la «Aplicación A» como, por ejemplo, cuando el software utiliza los distintos recursos de hardware.

Las aplicaciones no dejan de evolucionar

El ritmo al que las aplicaciones migran a este enfoque orientado a los servicios no cesa de aumentar. Consecuentemente, el enfoque actual, centrado en proteger la infraestructura, será incluso menos eficaz a la hora de proteger las aplicaciones individuales. Por este motivo, es urgente cambiar a un método centrado en las aplicaciones, ya que los problemas no harán más que empeorar.

Incluso en los entornos tradicionales de aplicaciones existentes el uso de este método centrado en las aplicaciones puede solucionar problemas importantes derivados de la seguridad y ayudar a prepararse mejor para el futuro.

Con la informática de cloud y móvil, ahora es posible

Gracias a los avances en la informática de cloud (privada y pública) y móvil, las organizaciones cuentan con las funciones necesarias para centrarse en la protección de las aplicaciones individuales, sentando las bases para lograr una seguridad más efectiva.

Uso de funciones centradas en las aplicaciones

En particular, la informática de cloud y móvil ofrece las siguientes posibilidades:

Función I: utilizar la automatización de infraestructuras para reconocer una aplicación individual y establecer un valor de referencia para la misma.

- Identificar los componentes que integran la aplicación.
  - Obtener visibilidad de las aplicaciones.
- Saber cómo debe operar una aplicación y cómo lo hace en tiempo de ejecución.
  - Saber quién necesita acceder a qué recursos, y la forma en que estos interactúan.

- Utilizar esta información de referencia para proteger la aplicación.
  - Remitirse a esta información para configurar las herramientas de seguridad.

Función II: compartimentar los componentes del sistema en aplicaciones individuales

- Agrupar todos los componentes del sistema que constituyan una aplicación individual.
- Asociar todos estos componentes del sistema y delimitar el grupo resultante con un límite lógico.
- Utilizar el límite para etiquetar la aplicación de forma única.

Función III: colocar elementos de defensa en torno a cada aplicación individual

- Determinar lo que debe estar dentro o fuera del límite que protege la aplicación.
- Establecer los comportamientos que se pueden ejecutar dentro de ese límite.
- Ajustar las herramientas de seguridad al límite de la aplicación.
- Configurar las herramientas de seguridad de acuerdo con la información del valor de referencia y utilizando las etiquetas que proporciona el límite.
- Hacer un seguimiento de la aplicación y adaptar el nivel de protección a medida que cambie.

Vea el diagrama 3 a continuación para comprobar cómo se utilizan estas funciones con el fin de proteger las aplicaciones modernas con eficacia. Para obtener más información sobre las funciones y su utilidad para las organizaciones, vea el apéndice 2.

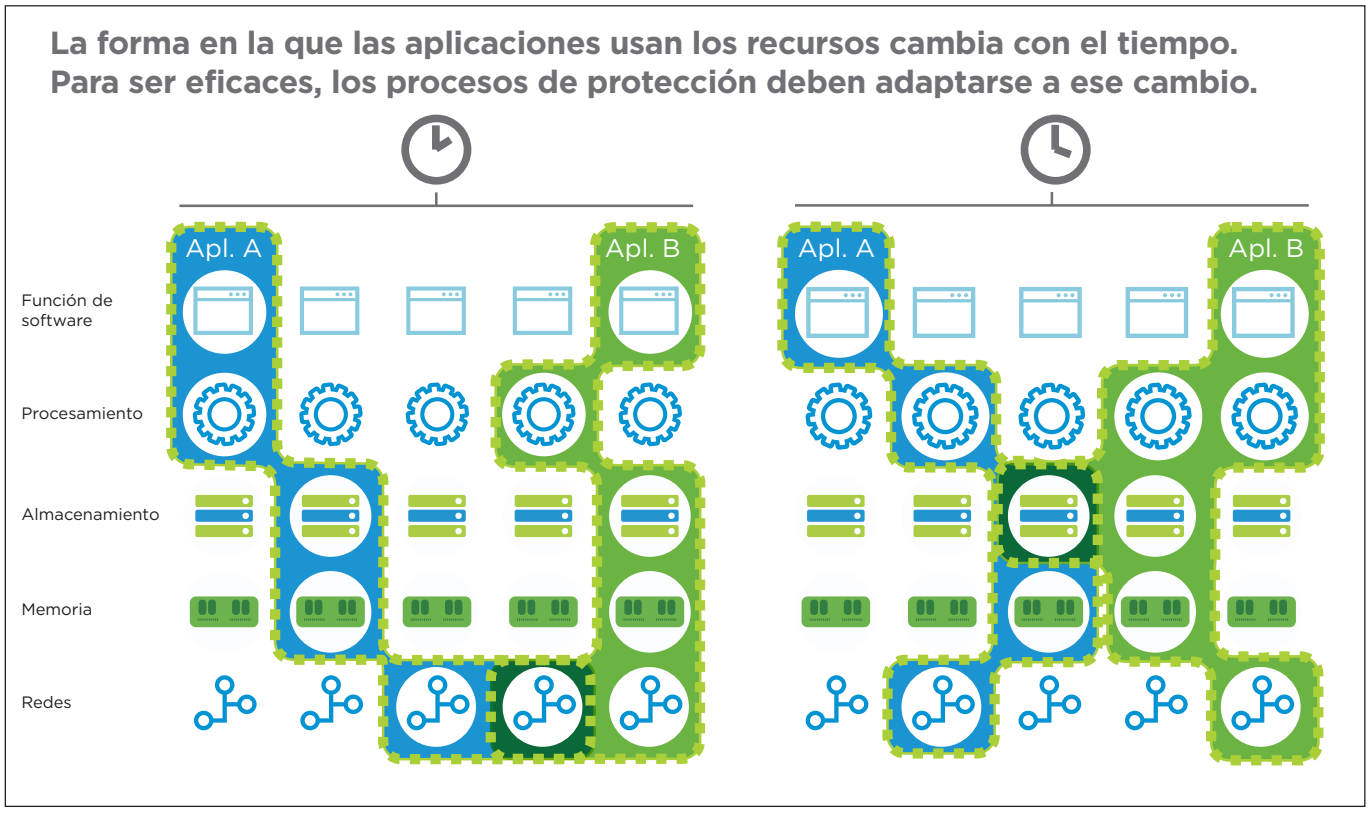

Diagrama 3: una aplicación moderna es un sistema distribuido y dinámico. Utiliza un depósito de recursos compartidos y su uso varía con el paso del tiempo. Para proteger una aplicación de forma eficaz, se deben identificar todos los componentes de software y hardware que conforman la aplicación, agrupar estos elementos, establecer un límite en torno a ellos y etiquetarlos como «Aplicación X» para posteriormente establecer defensas en ese límite. El límite y las defensas deben evolucionar al ritmo de la aplicación.

Implementación eficaz de los principios fundamentales

En un enfoque centrado en las aplicaciones, los principios fundamentales se pueden implementar con efectividad. La seguridad pasa a ser mucho más sencilla y fácil de automatizar:

Principio	Enfoque centrado en las aplicaciones	Implementación más efectiva
La base: la formación	Se debe implantar un proceso de formación **centrada en las aplicaciones** que sea obligatorio para todos: desde profesionales de TI y responsables empresariales, hasta empleados y trabajadores externos.	La formación será más pertinente y se adaptará a las aplicaciones con las que trabajan los profesionales de TI o los usuarios.
1. Informática con privilegios mínimos	Los componentes del sistema y los usuarios solo deben tener acceso a las funciones mínimas necesarias para llevar a cabo su cometido **en cada aplicación** y nada más (control de aplicaciones).	Así, será más difícil para los atacantes obtener acceso, desencadenar comportamientos malintencionados o controlar las interacciones (tanto entre sistemas, como entre usuarios y sistemas).
2. Microsegmentación	Se debe dividir la totalidad del entorno de TI en pequeñas porciones **estableciendo límites en torno a las aplicaciones individuales** para que resulte más sencillo protegerlas y se pueda limitar el daño si una parte estuviera en peligro.	Se dificultará considerablemente el movimiento dentro del entorno de TI. Si los atacantes finalmente consiguen acceder a una de las partes, quedarán confinados a una zona muy pequeña (es decir, una única aplicación) y les resultará difícil llegar a otras.
3. Cifrado	En cuanto a los procesos empresariales esenciales, deben cifrarse todos los datos cuando los almacenen o transmitan **los componentes de una aplicación individual**. Si se produjera una vulneración de datos, los archivos esenciales robados solo contendrían datos ilegibles.	Los datos esenciales estarán cercados por un «límite» lógico que solo podrán atravesar los componentes de las aplicaciones que sean aptos para hacerlo, independientemente del sitio desde el que se ejecuten estas aplicaciones.
4. Autenticación multifactor	La identidad de los usuarios y los componentes del sistema debe comprobarse mediante varios factores (no únicamente contraseñas) y de forma proporcional a los riesgos que entraña la función o el acceso que se haya solicitado **para cada aplicación.**	Aplicar un nivel de autenticación multifactor (MFA) adecuado al nivel de riesgo de cada solicitud será más factible, ya que se gestiona por cada aplicación. Los atacantes tendrán más difícil actuar, ya que no podrán robar ni adivinar contraseñas.
5. Aplicación de parches	Los sistemas están siempre actualizados y sometidos a un mantenimiento continuo **según el conocimiento de cada aplicación individual.** Los sistemas esenciales que no están actualizados representan un riesgo importante para la seguridad.	Resultará mucho más sencillo aplicar parches de forma sistemática porque se sabrá cuáles son los componentes de la aplicación afectados y las posibles consecuencias en los sistemas. Será mucho más complicado que los atacantes se aprovechen de los sistemas vulnerables.

Se empieza por clasificar las aplicaciones

Con un enfoque centrado en las aplicaciones, el equipo de seguridad puede centrar toda su atención en los recursos más importantes, es decir, en las aplicaciones esenciales, en lugar de dispersar la inversión por toda la infraestructura. Las organizaciones empiezan por clasificar las aplicaciones para determinar su importancia y prioridad, de forma que puedan centrar sus iniciativas en las más esenciales. No nos debemos olvidar, sin embargo, que todas las aplicaciones necesitan cierta protección.

Mejora de la efectividad de las herramientas de seguridad actuales

El enfoque centrado en las aplicaciones permite que las organizaciones saquen el máximo partido a las herramientas de control de la seguridad:

- Reducir los errores de configuración de las herramientas de seguridad:
  - Los conjuntos de reglas se han simplificado: a cada aplicación individual se le aplican reglas específicas para ella.
- Configurar las herramientas de seguridad para coordinarlas:
  - Todas las herramientas de seguridad, como cortafuegos, antivirus, sistemas de prevención de intrusiones y sistemas de detección de amenazas, utilizan la misma etiqueta (límite de la aplicación) para identificar el recurso que protegen.
- Interpretar las alertas más fácil y rápidamente y actuar en consecuencia:
  - Las alertas que generan las herramientas de seguridad identifican la aplicación y ofrecen información sobre su prioridad y posibles procedimientos a seguir.
- Usar las herramientas de seguridad de forma más automatizada:
  - Las características de las herramientas de seguridad se pueden coordinar y las actividades de protección, supervisión y respuesta se pueden organizar en torno a las aplicaciones individuales.
- Reducir el coste de las operaciones de seguridad:
  - Se generarán menos alertas y se invertirá menos tiempo en las tareas de investigación.

Integración de la seguridad en la arquitectura

Por lo general, la seguridad es un añadido «a posteriori». Los equipos que se dedican a las aplicaciones se encargan de desarrollarlas, los equipos de infraestructuras crean infraestructuras relativamente genéricas capaces de gestionar todas las aplicaciones y, por último, el equipo de seguridad se encarga de proteger todo esto. Las herramientas de seguridad se implementan, pero no se integran en la estructura de las aplicaciones.

El enfoque centrado en las aplicaciones requerirá un cambio a nivel de arquitectura. No se conseguirá con solo adquirir un dispositivo de seguridad concreto o actualizando el software.

Habrá que adoptar las propiedades únicas que proporcionan las aplicaciones y la infraestructura modernas, y utilizarlas en beneficio de la seguridad (vea el apéndice 3 para obtener más información).

Las tecnologías de cloud y movilidad ofrecen una arquitectura de superposición que se puede utilizar para integrar la seguridad no solo en las aplicaciones nuevas, sino también en las que ya existen. Para ver sugerencias prácticas sobre la implementación en el centro de datos y en un entorno informático de usuario final, consulte los apéndices 4 y 5.

Conclusión

Tan solo con dos medidas básicas (aplicar los principios fundamentales de la ciberintegridad y centrarse en la protección de aplicaciones), las empresas podrían mejorar la eficacia de la seguridad de la información. La informática de cloud y movilidad lo hace posible y brinda una forma de integrar la seguridad en la arquitectura. Este modelo actualizado ayuda a garantizar que los programas de seguridad de la información sean más eficaces en el presente y que, además, estén preparados para el futuro a medida que evolucionen los entornos de TI.

EMPEZAR

Más información sobre cómo puede ayudar a su organización a iniciar la transición hacia una infraestructura de aplicaciones segura >

Síganos:

Apéndice 1: Correspondencia de los principios fundamentales con el CSF del NIST

Los principios fundamentales de la ciberintegridad se basan en normas muy consolidadas. Por ejemplo, todos ellos se corresponden con diversas funciones del marco de trabajo de ciberseguridad (CSF) del NIST (vea más adelante). Estos principios son solo una parte de lo que cubren el CSF del NIST y otros marcos de trabajo. Sin embargo, son los principios clave que harán posible la adopción de un enfoque de seguridad más sencillo y automatizado.

Principios fundamentales	Categorías secundarias del CSF del NIST
La base: la formación	PR.AT: El personal y los partners de la organización reciben formación sobre ciberseguridad y sobre cómo desarrollar sus tareas y responsabilidades relacionadas con la seguridad de la información con arreglo a las correspondientes políticas, procedimientos y acuerdos.
1. Informática con privilegios mínimos	PR.AC-4: Los permisos y las autorizaciones de acceso se gestionan aplicando los principios de privilegios mínimos y de separación de tareas. PR.PT-3: El principio de funcionalidad mínima se incorpora configurando los sistemas para que proporcionen únicamente las prestaciones esenciales. PR.IP-1: Se crea una configuración de referencia para los sistemas de control de las tecnologías de la información y de los procesos industriales, y se lleva a cabo su mantenimiento, incorporando los principios de seguridad adecuados (por ejemplo, el concepto de funcionalidad mínima). DE.AE-1: Se establece y gestiona un valor de referencia para las operaciones de la red y los flujos de datos previstos de usuarios y sistemas.
2. Microsegmentación	PR.AC-5: Se protege la integridad de la red segregándola donde sea apropiado.
3. Cifrado	PR.DS-1: Se protegen los datos en reposo. PR.DS-2: Se protegen los datos en tránsito.
4. Autenticación multifactor	PR.AC: El acceso a los recursos físicos y lógicos, así como a las instalaciones asociadas, está limitado a los usuarios, los procesos y los dispositivos autorizados; además, el acceso se gestiona con arreglo a una evaluación de riesgo de acceso no autorizado a las actividades y transacciones autorizadas. PR.AC-1: Se crean, gestionan, comprueban, revocan y auditan las identidades y las credenciales de los dispositivos, usuarios y procesos autorizados. PR.AC-6: Las identidades se verifican y se vinculan a las credenciales, y se utilizan en las interacciones cuando corresponde.
5. Aplicación de parches	PR.IP-3: Se han establecido procesos de control de cambios en la configuración. PR.IP-7: Se mejoran de forma continua los procesos de protección. PR.IP-12: Se desarrolla e implementa un plan de gestión de las vulnerabilidades. ID.RA-1: Se identifican y documentan las vulnerabilidades de los recursos. DE.CM-8: Se efectúan análisis de vulnerabilidades.

NOTA: Los siguientes apéndices proporcionan una información que puede resultar relevante para profesionales y personas que estén al cargo de implementar un enfoque nuevo de seguridad que esté centrado en las aplicaciones dentro de una organización.

Apéndice 2: Información detallada sobre las funciones centradas en las aplicaciones

Los apartados siguientes ofrecen una explicación más detallada y técnica de las funciones centradas en las aplicaciones que se presentaron anteriormente en la página 10 del documento.

¿ES REALMENTE PRÁCTICO?

Mientras que en el pasado resultaba difícil conseguir visibilidad de la aplicación y saber cómo funcionaba, con las nuevas tecnologías, esto resulta más sencillo.

Para las aplicaciones de gran tamaño, existen ahora tecnologías que supervisan el tráfico de la red para ayudar a entender los componentes de la aplicación y la forma en que interactúan.

Para las arquitecturas de aplicaciones más recientes, las técnicas DevOps automatizan el proceso de compilación y supervisan todos los componentes empleados en la creación de aplicaciones desde el principio.

Función I: Reconocer una aplicación y establecer un valor de referencia para la misma

Con esta función, las organizaciones podrán comprender mejor sus aplicaciones esenciales desde el punto de vista de la seguridad. Esto abarca desde determinar sus componentes, identificando los servicios (es decir, las funciones de software) que se deben ejecutar en cada servidor, a conocer los recursos que se utilizan, pasando por cómo deben interactuar estos componentes, entre otros.

Un factor clave es entender el comportamiento esperado de las aplicaciones como, por ejemplo:

- ¿Qué debe estar ejecutándose?
- ¿Qué interacciones están permitidas?
- ¿Cómo deben comunicarse los componentes?

Dado que las aplicaciones son dinámicas, es preciso que las organizaciones puedan llevar un seguimiento de las mismas cuando cambian, cuando los desarrolladores las actualizan y cuando se están ejecutando, por ejemplo, sabiendo cuántas instancias están en ejecución.

¿Qué pueden hacer las organizaciones con esta función?

- Proteger las aplicaciones con eficacia conociendo los valores de referencia.
  - Comprender la aplicación y saber cómo protegerla.
  - Utilizar una fuente de información fidedigna sobre la aplicación para configurar toda su cartera de controles de seguridad.
    - Los equipos de garantía y auditoría de los controles también pueden utilizar esta referencia para evaluar los controles.
- Mejorar los privilegios de forma que sean estrictos pero funcionalmente viables (sin interrumpir procesos).
  - Disponer de la información oportuna para determinar las funciones e interacciones mínimas necesarias para los elementos que constituyen la aplicación, de forma que se cree un entorno de privilegios mínimos para la propia aplicación.
  - Disponer de la información oportuna para determinar el mínimo necesario de comunicación que deben tener los componentes del sistema ya sea hacia, desde o en el interior de las aplicaciones individuales.
    - Esto podría reducir drásticamente la superficie de ataque.
- Conseguir que las alertas sean más procesables.
  - Las alertas de las herramientas de seguridad identificarán la aplicación y, en función de la información suministrada, el equipo de seguridad podrá determinar el trabajo necesario, cómo establecer las prioridades y cuáles son las opciones para corregir los problemas.
- Reducir el ruido y las alertas falsas.
  - Si los sistemas están estrechamente controlados, se reducen mucho las probabilidades de que se produzcan accesos, funciones o interacciones no autorizados. El número de alertas será inferior.
  - Al haber menos alertas, las señales serán mucho más claras porque habrá menos ruido y falsas alarmas.

POSIBILITA EL MODELO DEVOPS

Las aplicaciones más nuevas utilizan los métodos y tecnologías DevOps para compilar, probar e implementar aplicaciones rápida y frecuentemente.

Las organizaciones podrán abandonar los métodos manuales de revisión y pruebas de seguridad, que conllevan plazos de entrega muy prolongados y no funcionan con procesos de desarrollo y aplicaciones ágiles.

SEGMENTACIÓN EFECTIVA

El modelo tradicional de segmentación de redes se basa en atributos como el tipo de servidor (por ejemplo, servidores web o servidores de base de datos). Este enfoque no puede impedir eficazmente la expansión lateral de una aplicación a otra, ya que el funcionamiento de las aplicaciones no se limita a un único segmento de servidores, sino que abarca múltiples segmentos. Los atacantes pueden pasar de un segmento a otro. Para proteger con eficacia una aplicación, hay que establecer un límite en torno a ella y disponer de un punto de control de la red desde el que se pueda controlar y supervisar todo el tráfico entrante y saliente de cualquier porción de esta aplicación.

- Olvidarse de perseguir amenazas continuamente.
  - Las amenazas cambian constantemente. Este enfoque no consiste en tener que adelantarse siempre a las nuevas amenazas.
- Estrechar la colaboración entre los equipos de seguridad y los de las aplicaciones (vea la columna izquierda).
- Implementar gradualmente: empezar por comprender un conjunto pequeño de aplicaciones esenciales.
  - Comenzar con las aplicaciones esenciales para la empresa que tengan grupos más pequeños de componentes con funciones muy específicas (por ejemplo: «Este servidor web forma parte de la Aplicación X, y este proceso será el único que se comunique con Y»).

Función II: compartimentar los componentes del sistema en aplicaciones individuales

Las organizaciones pueden utilizar la información de referencia que se ha descrito anteriormente para determinar qué componentes del sistema constituyen una aplicación individual, compartimentarlos y establecer un límite lógico en torno a ellos. El límite constituye un método para definir y etiquetar de forma exclusiva una única aplicación. Asimismo, restringe los ataques a una única aplicación, en caso de que alguna se encuentre en peligro.

¿Qué pueden hacer las organizaciones con esta función?

- Configurar una única puerta de enlace para aplicar políticas a las aplicaciones con efectividad.
- Mejorar la protección de las aplicaciones frente a las amenazas en la red.
  - La segmentación basada en la infraestructura, por ejemplo, según el tipo de servidor, no es eficaz (vea la columna izquierda).
- Identificar y etiquetar de forma exclusiva las aplicaciones (vea la columna izquierda).
- Desarrollar políticas exclusivas para cada aplicación.
  - Si las aplicaciones se definen y etiquetan de forma exclusiva, es posible aplicarles políticas.
- Limitar la expansión lateral de una aplicación a otra.
  - Si un atacante accede a una aplicación, le resultará complicado pasar a otra.
- Aplicar controles específicos para cada aplicación en su límite.
  - Las aplicaciones más esenciales pueden someterse a una mayor protección e inspección. Aunque un sistema más débil del entorno esté en peligro, el atacante no podrá expandirse lateralmente a un sistema más esencial.

IDENTIFICADOR ÚNICO

Los controles tradicionales de los procesos de seguridad siguen utilizando la misma etiqueta estática para toda la pila, desde la aplicación hasta el hardware, pasando por el sistema operativo. Pero esto no es así para las aplicaciones modernas, ya que no residen en servidores estáticos. Los identificadores de VLAN tampoco tienen una solución para esto, ya que aíslan varias aplicaciones y no proporcionan un identificador único para cada una de ellas. Para que los controles de seguridad sean efectivos, tiene que haber un identificador único que se utilizará al aplicar políticas a cada aplicación individual.

Función III: colocar elementos de defensa en torno a cada aplicación individual

Gracias a la etiqueta única que ofrecen los límites establecidos en las aplicaciones, las organizaciones pueden configurar controles de seguridad que se aplicarán individualmente a cada aplicación. Por ejemplo, se puede configurar un cortafuegos para que proteja una única aplicación utilizando la etiqueta de su límite. Por otra parte, las organizaciones pueden utilizar información de referencia para configurar los controles de seguridad. Por ejemplo, con la información de referencia, la organización podrá establecer un sistema de prevención de intrusiones y desarrollar un conjunto de reglas para la aplicación particular que esté protegiendo.

¿Qué pueden hacer las organizaciones con esta función?

- Optimizar la ubicación de los puntos de aplicación de políticas:
  - Las políticas se aplican en el límite de cada aplicación.
- Simplificar las políticas de protección de las aplicaciones:
  - Ya no resulta necesario que las organizaciones lidien con las políticas extremadamente complejas de los enfoques actuales que, por ejemplo, utilizan un solo cortafuegos para proteger miles de aplicaciones (vea el diagrama 4 más abajo).
- Reducir la complejidad de la gestión de las claves de cifrado:
  - Resulta mucho más sencillo distribuir claves para el cifrado y descifrado de los componentes del sistema de una aplicación individual que de muchas aplicaciones.
- Aplicar políticas de autenticación multifactor correlacionando de forma sencilla los usuarios de aplicaciones y los componentes del sistema que obtienen acceso a ciertos recursos, así como los factores necesarios.
- Evitar los errores de configuración de los controles de seguridad:
  - Los controles se configuran para proteger una aplicación.
- Incrementar la protección de las aplicaciones individuales añadiendo más controles al límite.
- Disponer de controles de seguridad que funcionen como un sistema:
  - Todos los controles se pueden sincronizar en una aplicación utilizando el límite de la aplicación para etiquetarla.
- Permitir que los controles estén en sintonía con la dinámica de las aplicaciones:
  - Los controles pueden ejercer su protección en los límites cuando las aplicaciones se desplazan.

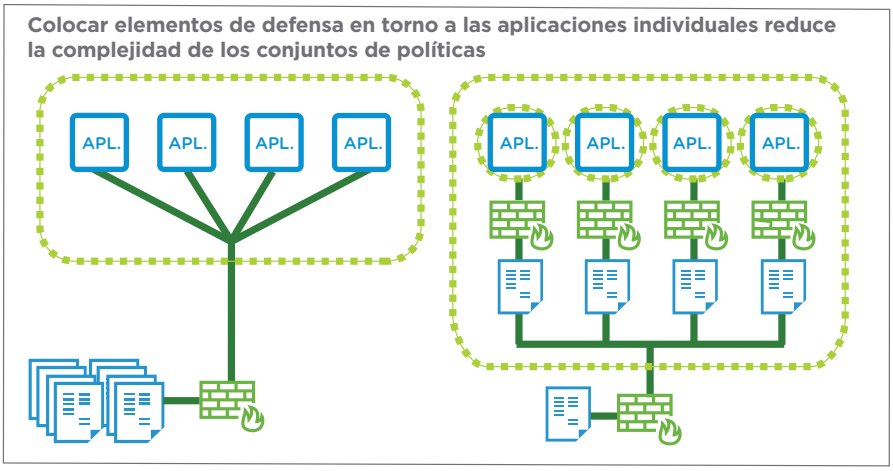

Diagrama 4: Por lo general, con los métodos actuales, los cortafuegos se configuran en el perímetro para aplicar políticas al tráfico entrante y saliente de todos los componentes en los límites de todas las aplicaciones, lo que conlleva la gestión de decenas de miles de reglas de cortafuegos. Los conjuntos de políticas son inmensos y complejos. Si se configura un cortafuegos para cada aplicación, únicamente tendrá que supervisar el tráfico de entrada y salida de los componentes de una sola aplicación, lo que reduce y simplifica drásticamente el conjunto de políticas.

Apéndice 3: Propiedades exclusivas de la informática de cloud y móvil

Las funciones centradas en las aplicaciones (descritas en el apéndice 2) que pueden utilizar ahora las organizaciones para implementar métodos más eficaces para la seguridad de la información son una realidad gracias a los recientes avances en la informática de cloud y móvil.

PROPIEDADES EXCLUSIVAS DE LA INFORMÁTICA DE CLOUD

La estructura básica de la cloud es la virtualización, que proporciona una capa de desvinculación entre la infraestructura física y las aplicaciones.	
Contexto de las aplicaciones	• La capa de virtualización: • Recopila, protege y distribuye información contextual sobre todas las aplicaciones que se están ejecutando en el entorno virtualizado. - Esto es inherente a la función de virtualización porque controla la dinámica de las aplicaciones, como transferir las cargas de trabajo a los recursos disponibles, equilibrar cargas o aumentar o reducir los recursos según necesite la aplicación. - También dispone de un esquema de las cargas de trabajo y de los componentes del sistema en el entorno y conserva este esquema, ya que las cargas de trabajo están en continuo movimiento. • Brinda una única perspectiva desde la que se puede ver: - La conexión entre la aplicación que se ejecuta y el hardware en el que se ejecuta. - La topología de la aplicación. • La disposición de los diversos componentes del sistema que conforman la aplicación en la red. - Cómo se ha aprovisionado la aplicación y cómo funciona en tiempo de ejecución.
Aislamiento	• La capa de virtualización: • Ofrece un dominio de confianza independiente. - Brinda visibilidad del sistema invitado, pero también aislamiento del mismo. • Ofrece un punto de inserción aislado para ubicar controles de seguridad con el fin de proteger el límite de las aplicaciones. - Conserva el límite de la aplicación aunque las cargas de trabajo se desplacen a máquinas físicas diferentes o a vínculos de red.
Inalterabilidad	• Si se utiliza la capa de virtualización, los componentes inalterables se pueden sustituir en cada implementación, en lugar de actualizarlos «in situ». - Se puede generar una imagen común una sola vez por cada implementación, además se puede probar y validar.
Componentes definidos por software	• Con la virtualización, el comportamiento de los componentes del sistema se inicializa, controla, modifica y gestiona mediante programación. • Se trata de un punto de control flexible desde el que se pueden poner máquinas en cuarentena, volver a crear imágenes de máquinas, bloquear tráfico, realizar instantáneas de las máquinas, incorporar mayor visibilidad, etc.

PROPIEDADES EXCLUSIVAS DE LA INFORMÁTICA MÓVIL

La informática móvil ofrece prestaciones únicas a través de la funcionalidad nativa del dispositivo, así como de la funcionalidad de los escritorios virtuales y las tecnologías de gestión de dispositivos móviles.	
Contexto de usuarios y dispositivos	• La informática móvil ofrece un completo conjunto de datos sobre los usuarios y los dispositivos para ayudar en la toma de decisiones referentes a la autenticación y el control de los accesos en función del nivel de riesgo, por ejemplo: - Datos de usuarios y dispositivos: • Biométricos: huella dactilar, voz, imagen. • Ubicación geográfica. • Identificador del dispositivo: número de serie, certificado. • Parámetros de la red (wifi, Intranet, etc.) y dirección IP. • Configuración del dispositivo: hardware, sistema operativo, aplicaciones instaladas. • Situación de seguridad: dispositivo gestionado o no gestionado, software de seguridad, dispositivo sometido a «jailbreaking» o «rooting», estado de las actualizaciones de software y aplicación de parches. • Fuera de banda: llamada telefónica, notificación automática. - Decisiones de acceso condicional • Varios dispositivos: se determina si la ubicación geográfica del teléfono móvil y del ordenador portátil es diferente antes de conceder el acceso. • Combinación de datos de usuario y dispositivo: se determina si se trata de un usuario de confianza y un dispositivo gestionado en una red segura antes de conceder el acceso.
Aislamiento	• Los escritorios virtuales ofrecen una conexión aislada a las aplicaciones. - Permite que las organizaciones restrinjan el acceso de los usuarios a un conjunto concreto de aplicaciones (en lugar de poder acceder a todas las aplicaciones de la red). • Los escritorios virtuales también separan el uso de las aplicaciones del uso del dispositivo. - Evita que las aplicaciones y sus datos asociados se encuentren presentes en el propio dispositivo móvil. En su lugar, el dispositivo móvil tan solo visualiza una presentación remota de las aplicaciones.
Inalterabilidad	• Los escritorios virtuales no persistentes son inalterables. - Se pueden crear de forma instantánea a partir de una imagen maestra controlada y, posteriormente, destruirlos para volver a crearlos cada vez que se quieran utilizar. Con la inalterabilidad, resulta muy difícil que los atacantes sean persistentes.
Telemetría	• La supervisión remota, la aplicación de políticas y la corrección de problemas permiten: - Actualizaciones y aplicación de parches continuas - Borrado del dispositivo en caso de robo o pérdida, de error de registro, o si está en itinerancia fuera del alcance de una wifi segura - Puesta en cuarentena o apagado de los dispositivos que no cumplan los requisitos

Apéndice 4: Implementación en el centro de datos

Este apéndice ofrece recomendaciones específicas para la implementación de funciones centradas en las aplicaciones en el centro de datos de una organización.

Función	Sugerencias de implementación
1. Reconocer una aplicación y establecer un valor de referencia para la misma	• Crear sistemas de registro sobre cómo se configuraron las aplicaciones esenciales y la interacción esperada entre los componentes del sistema. - Esto se puede llevar a cabo en colaboración con los equipos de las aplicaciones, atendiendo a los sistemas de aprovisionamiento o a través de la formación y aplicando valores de referencia o sistemas y modelos de automatización. - Sirve como información esencial de registro para identificar y diagnosticar problemas. • Crear una lista blanca para una aplicación (para un sistema de componentes, procesos y la forma en que interactúan o se comunican en una red).
2. Compartimentar los componentes del sistema en aplicaciones individuales	• Aprovechar la estructura virtual para crear un límite lógico en torno a la aplicación o servicio, es decir, microsegmentación. - Aplicar dicho límite con un cortafuegos distribuido, y además con una red aislada de capas 2 y 3 para crear un espacio de direcciones que no sea contiguo. - Todos los componentes de la aplicación se encuentran en un único segmento aislado, con un solo límite de control. • Establecer un único punto de salida. - Los componentes de las aplicaciones dentro de un segmento se pueden comunicar libremente entre sí. - El conjunto de servicios que se comunican a través de ese límite está restringido (DHCP, DNS, AD, etc.). - El límite de la aplicación es un punto definido en el que puede coordinar los controles para inspeccionar el tráfico en esos proveedores de servicios.
3. Colocar elementos de defensa en torno a cada aplicación individual	• Usar la capa de virtualización con el fin de coordinar los controles con la aplicación. - Gracias a las redes definidas por software y los controles de seguridad basados en software, ahora es funcionalmente viable establecer defensas en torno a cada aplicación individual.

Apéndice 5: Implementación para la informática de usuario final

Este apéndice ofrece recomendaciones específicas para la implementación de funciones centradas en las aplicaciones para la informática de usuario final.

Función	Sugerencias de implementación
1. Reconocer una aplicación y establecer un valor de referencia para la misma	• Utilizar escritorios virtuales no persistentes en lugar de aplicaciones persistentes en los terminales como parte del proceso para garantizar que las aplicaciones conservan el funcionamiento esperado. - Con una imagen de escritorio no persistente, el sistema operativo y las aplicaciones mantienen el estado esperado destruyendo la imagen de escritorio cuando se cierra la sesión y volviendo a crear una nueva en el siguiente inicio de sesión. - En caso de que una imagen de escritorio no persistente esté en riesgo, el ataque se eliminará ese mismo día cuando el usuario cierre sesión. Por lo general, los atacantes necesitan un tiempo (de varios días o incluso más) para propagar el ataque desde la máquina inicial a través de la red, por tanto, los escritorios no persistentes pueden obstaculizar la expansión de estos atacantes más allá de su posición inicial. - Impide al atacante mantener una posición en el entorno. Evita que las amenazas persistentes avanzadas (APT) hagan honor a su nombre. • Efectuar comprobaciones de seguridad en tiempo real para determinar con rapidez si un dispositivo incumple las políticas de seguridad y corregir los problemas inmediatamente o deshabilitar su acceso a los recursos corporativos.
2. Compartimentar los componentes del sistema en aplicaciones individuales	• Aislar el proceso integral, es decir, los usuarios conectándose a las aplicaciones. - Conecte la aplicación compartimentada a la infraestructura del usuario final. • Utilizar la tecnología de infraestructura de escritorios virtuales (VDI) para garantizar que los usuarios solo podrán acceder a los sistemas que deben. - Utilizar controles de acceso en la capa de la aplicación. - Por ejemplo, permitir a los trabajadores externos acceder solamente a las aplicaciones que necesitan. • Cuando los trabajadores externos inician sesión en un escritorio virtual, solamente tendrán acceso a un microsegmento (aplicación). • Utilizar la tecnología VDI junto con la microsegmentación para evitar que los atacantes propaguen sus ofensivas por la red. - La plataforma de escritorio virtual puede utilizar la microsegmentación para asegurarse de que si la máquina de un usuario se ve amenazada (por ejemplo, por suplantación de identidad), el atacante solo pueda acceder a un pequeño número de hosts en lugar de a miles. • El atacante solo podrá acceder al conjunto limitado de aplicaciones para las que está autorizado el usuario a través de la VDI. - El uso de la microsegmentación por parte de la VDI hace más sencilla la segregación. • Se basa en la identidad del usuario: una vez que el usuario inicia sesión, se le suministra de forma dinámica su propia visión de la red. • No es necesario realizar tareas complejas de asignación de redes con antelación ni preconfigurar diferentes conjuntos de depósitos de escritorios, cada uno tiene distintas VLAN asociadas.

	• Utilizar la tecnología móvil junto con la microsegmentación para restringir los recursos del centro de datos a los que puede acceder una aplicación o dispositivo móvil. - Cuando un dispositivo va a acceder a los recursos del centro de datos, según la identidad del dispositivo este solo podrá acceder a una porción muy limitada de la red, por ejemplo, una dirección IP o puerto específicos. • Poner fin a la VPN en el límite de la microsegmentación, proporcionando al usuario una conexión autenticada y segura directamente a una aplicación. - Tradicionalmente, la VPN terminaba en el perímetro, de forma que una vez que el usuario se encontraba en su interior, tenía acceso a muchos sitios de la red.
3. Colocar elementos de defensa en torno a cada aplicación individual	• Utilizar la tecnología VDI para aplicar controles de seguridad directamente a las aplicaciones. - Resulta más eficaz aplicar controles de seguridad a las aplicaciones si se centralizan en un centro de datos en lugar de aplicar estos controles a miles de dispositivos. • Aproveche las tecnologías de contenedorización de sistemas operativos y aplicaciones para separar con seguridad las aplicaciones y los datos corporativos de los personales en un caso de uso de dispositivos personales en el trabajo, de forma que se puedan aplicar los controles de seguridad directamente a las aplicaciones corporativas. - Las aplicaciones se distribuyen en entornos de pruebas y de forma cifrada. • Utilizar los datos de los terminales para garantizar que existen suficientes pruebas en relación con la identidad y la confianza para satisfacer el nivel del riesgo de la solicitud de acceso a una aplicación esencial concreta. - Por ejemplo, en el caso de un dispositivo desconocido, el usuario necesita una autenticación de dos factores para acceder a la aplicación. En el caso de un dispositivo de confianza y registrado, al usuario le basta con la autenticación de un solo factor. El dispositivo funciona como un segundo factor. En el caso de una red wifi de confianza (en una oficina corporativa), el usuario puede utilizar la autenticación de un solo factor. La verificación de la red funciona como un segundo factor. • Utilizar la información de geolocalización para tomar decisiones en tiempo real sobre el riesgo de acceder a una única aplicación esencial. - Se consulta la geolocalización del ordenador portátil y el teléfono móvil de un usuario y, si se encuentran en ubicaciones geográficas diferentes, el nivel de riesgo requerirá una serie de pasos adicionales en el proceso de autenticación. Por ejemplo, se puede enviar una notificación automática al teléfono móvil para solicitar una verificación. • Utilizar la identidad federada para que la autenticación sea más segura y que el inicio de sesión de los usuarios resulte más sencillo. - La autenticación federada mediante directorios de terceros evita el desarrollo de prácticas no seguras como: • Sincronización de los directorios. • Múltiples contraseñas que obligan inevitablemente a los usuarios a escribirlas o reutilizar la misma contraseña en todas las aplicaciones. • Utilizar la tecnología móvil para garantizar automáticamente la idoneidad de los dispositivos en términos de seguridad, al margen del sistema operativo que tengan (Windows, OSX, Android, QNX, etc.). - Por ejemplo, sondear los dispositivos para identificar problemas de seguridad, como la falta de parches y, después, corregirlos distribuyendo inmediatamente los parches.

VMware e Intel transforman las redes y la seguridad con la red de cloud virtual, su visión sobre las redes para la era digital. La red de cloud virtual utiliza la tecnología NSX y se ejecuta en la arquitectura de Intel. Proporciona una capa de software omnipresente en la infraestructura del centro de datos, de la cloud, perimetral y de otros tipos de hardware, y ofrece seguridad y conectividad generalizada para las aplicaciones y los datos con independencia de dónde residan.

EMPEZAR

Más información sobre cómo puede ayudar a su organización a iniciar la transición hacia una infraestructura de aplicaciones segura >

Síganos:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.com/es