netskope

White Paper

Mejores prácticas de confianza cero

RESUMEN

Mucha gente cree que la transformación digital es solo una moda. Se trata de una perturbación económica que impacta en el ritmo de innovación y desarrollo organizacional. Las empresas quieren seguir siendo importantes, introducir productos y servicios en el mercado más rápidamente, ser ágiles y poder reinventarse cuando surja la oportunidad adecuada.

El inmenso crecimiento de la computación en la nube y el auge de los dispositivos móviles ha provocado que los usuarios necesiten acceder continuamente a la información desde cualquier lugar, dispositivo y momento.

Una mentalidad heredada es un obstáculo para las actividades comerciales actuales. Las empresas se dirigen al mercado con nuevos modelos comerciales, ya que mantienen un gran número de relaciones con terceros, lo que finalmente crea una visión diferente sobre cómo debemos hacer planes para el futuro. Hoy en día, la confianza es observadora, contextual y adaptable, no es solo blanca o negra (bloquear o permitir) como ocurría en el pasado. Ninguna entidad puede dar por hecho una confianza implícita, y los componentes que se utilizan para establecer la confianza deben evaluarse en todo momento. A fin de cuentas, de esto trata la confianza cero. Un enfoque más sistemático y seguro para acceder a la información.

El ecosistema de la tecnología heredada actual se está difuminando, por lo que adoptar nuevos planteamientos es fundamental. La transformación digital no puede llevarse a cabo de la noche a la mañana o por sí sola. Se necesita seguridad y la transformación de TI como instrumento de apoyo. Es preciso reflexionar sobre la forma en que proporcionamos un acceso seguro a la información a través de la transparencia porque es lo único que hace que nuestros usuarios estén contentos con un profundo sentimiento de lealtad.

Cuando los conceptos de confianza cero se aplican de forma adecuada pueden ofrecer exactamente eso.

El inmenso crecimiento de la computación en la nube y el auge de los dispositivos móviles ha provocado que los usuarios necesiten acceder continuamente a la información desde cualquier lugar, dispositivo y momento.

INTRODUCCIÓN

A través del crecimiento exponencial de la computación en la nube las empresas no solo han podido consolidar sus patrones de alojamiento y reinventar la forma en que se dirigen al mercado, sino que dicho crecimiento también ha supuesto una velocidad de ejecución que a los equipos de TI tradicionales les costaba lograr con tecnologías heredadas. Aunque podríamos resumir el pasado como «una arquitectura de red basada en el perímetro», actualmente somos mucho más abiertos y diversos.

Sin embargo, la nube es «un instrumento para facilitar los negocios» y amplió el entorno de amenazas en formas que casi hemos olvidado. Esta tendencia de «desarrollo de la nube» cambió la forma en que evaluamos la confianza en el contexto del riesgo empresarial. Hoy en día, la confianza es observadora, contextual y adaptable, no es solo blanca o negra (bloquear o permitir) como ocurría en el pasado. Ninguna entidad puede dar por hecho una confianza implícita, y los componentes que se utilizan para establecer la confianza deben evaluarse en todo momento. A fin de cuentas, de esto trata la confianza cero. Un enfoque más sistemático y seguro para acceder a la información.

Aunque numerosas organizaciones impulsan sus resultados mediante enfoques estandarizados en endpoints, los dirigentes empresariales están empezando a valorar los deseos de los usuarios finales como nunca antes. Por tanto, cada vez es más difícil de gestionar el aspecto operativo de estos dispositivos, ya que hay más tipos de dispositivos a los que dar soporte. Otras empresas se están alejando del mantenimiento y el uso de endpoints; en lugar de permitir a los usuarios llevar cualquier tipo de endpoint al entorno empresarial, se centran en resolver la seguridad de la información.

En definitiva, las empresas quieren que sus usuarios sean innovadores, productivos y seguros, y estén protegidos, independientemente del tipo de dispositivo que utilicen, de la hora a la que trabajen o desde dónde lo hagan. Para ello es necesario tener en cuenta la apertura arquitectónica y empresarial. La confianza cero se centra en:

- Acceso seguro a los recursos con independencia de la ubicación de la red, el usuario o el dispositivo
- Hacer cumplir estrictos controles de acceso e inspeccionar, supervisar y registrar el tráfico de la red en todo momento

La confianza cero evalúa de forma continua todos los aspectos del comportamiento de la entidad durante una conexión de red y proporciona controles de acceso adaptables que se basan en parámetros designados y niveles de riesgo empresarial aceptables.

Finalidad y alcance

La finalidad de este documento es proporcionar una visión detallada de los componentes principales y los pasos de implementación de los conceptos pragmáticos de confianza cero.

El alcance de este documento se centra en el acceso a los recursos de la empresa, el análisis del comportamiento y las observaciones.

Destinatarios

Este documento ha sido pensado para una audiencia muy variada que incluye arquitectos de seguridad, sistemas y redes, además de líderes de programas de seguridad, que son responsables de los aspectos técnicos de la creación, utilización y protección de los recursos y activos de la empresa. Aunque tiene un carácter técnico, se espera que los lectores obtengan unos conocimientos básicos sobre seguridad, redes y sistemas de TI.

La confianza cero evalúa de forma continua todos los aspectos del comportamiento de la entidad durante una conexión de red y proporciona controles de acceso adaptables que se basan en parámetros designados y niveles de riesgo empresarial aceptables.

PRINCIPIOS

Los principios son normas y directrices generales que deben ser comprensibles, sólidas, completas, independientes y que no tengan el propósito de establecer lo obvio. Proporcionan información y ofrecen soporte sobre la forma en que una organización se dispone a cumplir su misión, y se han diseñado para perdurar y no sufrir modificaciones. Cada principio debe realizar una declaración que ayude al proceso de toma de decisiones en una empresa.

A continuación, proponemos varios principios de alto nivel que ofrecen orientación al implementar una estrategia de confianza cero que cualquier arquitecto debe estar dispuesto a considerar:

- Todas las personas de una organización deben entender el **CONTEXTO** empresarial.
  - Los activos comerciales (información) deben tener una transcendencia (normalmente procedente del Plan de Continuidad Comercial y el proceso comercial que respalda) y sensibilidad establecidas (normalmente adquirida por la política de clasificación de información de la empresa y los requisitos de integridad necesarios de los datos y el proceso comercial).
- **NO** debe existir confianza implícita entre las entidades.
  - Todas las entidades deben verificarse y evaluarse de forma continua a lo largo de la interacción de la red.
- La confianza no es binaria sino continua.
  - Existen diferentes niveles de confianza según el contexto empresarial y el nivel de riesgo que se considere aceptable.
- El acceso se proporciona **ÚNICAMENTE** al recurso empresarial individual.
  - **NO** hay acceso a la red, sino únicamente acceso a los recursos (aplicaciones, servicios, etc.).
  - Evite las «zonas de confianza» y, en cambio, potencie las sesiones individuales.
- Asuma que todas las redes son iguales
  - Asuma la idea de equiparar intranet e internet.

Supuestos

Es imprescindible entender que se deberán asumir algunas condiciones, tales como que:

- La organización está dispuesta y capacitada para hacer lo que sea necesario.
- La organización cuenta con el apoyo de liderazgo empresarial.
- Existen los recursos necesarios o se asignarán a la organización.
- Hay capacidades tecnológicas disponibles para la organización.

OBTENER CONTEXTO

El uso de principios de confianza cero ofrece una visión completa y estratégica para la creación de un programa de seguridad. Una estrategia debe impulsar la política que se aplica en función de un contexto comercial determinado. Es imprescindible entender que la confianza cero no es una solución temporal ni un producto. La implementación se debe iniciar con un enfoque de grano grueso, y la política pasará a ser más granular a medida que se desarrolla una mayor comprensión de las necesidades del usuario, las necesidades empresariales y el impacto comercial.

La idea tradicional a la hora de aplicar controles mediante el concepto de «Permitir/Bloquear» ya no funcionará y dejará a la organización expuesta a un riesgo considerable. Las organizaciones deben utilizar una perspectiva de riesgos para evaluar cualquier tipo de acceso a los recursos, que depende en gran medida del contexto.

La calidad del contexto se obtiene de diferentes componentes que deben tenerse en cuenta durante cualquier interrogación de sesión, antes de la conexión con su destino final. Estos componentes son:

- Datos
- Identidad
- Endpoint
- Aplicación (recurso)
- Red
- Visibilidad y análisis
- Automatización y orquestación

Evaluación continua

La evaluación continua de estos componentes proporciona el resultado contextual utilizado para calcular la aceptación de riesgos. De esta forma, impulsa el conjunto de control que influye en la adaptación dinámica de políticas antes o durante el acceso a los recursos.

Datos

La empresa está en constante evolución, pero el ciclo de vida de los datos sigue siendo el mismo. Los datos son el alma de cualquier empresa y así se deben tratar.

Aunque numerosas organizaciones evitan o tienen dificultades para hacer la clasificación típica de sus datos, es fundamental alinearse con el primer principio de confianza cero, «Comprender el contexto empresarial», y completar los siguientes pasos:

- Comprender los datos
  - Detección (la empresa debe comprender dónde se encuentran los datos)
  - Clasificación (la empresa debe establecer su valor relativo y seguidamente analizarlo, contextualizarlo y organizarlo como tal)

- Mapa de confidencialidad (procedente de la sensibilidad), integridad (procedente de la sensibilidad) y disponibilidad (procedente de los procesos esenciales para la empresa)
    - Si esto no se conoce o no se ha establecido, asigne estas categorías (confidencialidad, integridad y disponibilidad) a una calificación predeterminada. Gracias a estos detalles es posible aplicar una política inicial, que posteriormente se puede perfeccionar con el tiempo.
- Identificar a los propietarios y responsables de los datos.

- Proteger los datos
    - Inspección (inspeccionar todos los datos; por ejemplo, descifrado de SSL)
    - Gobernanza (establecer normas y directrices)
    - Control (aplicar conjuntos de control técnico)

Identidad

En una organización hay un gran número de usuarios, pero todos son diferentes. Todos necesitan contar con un nivel de acceso a los recursos específico, por lo que los controles asociados deben aplicarse de forma adecuada. Es indispensable cumplir la gestión completa del ciclo de vida de la identidad, comenzando con el proceso de alta a través de la gestión y la gobernanza hasta el proceso de baja, cuando ya no se necesita dicha identidad. El proceso de baja es un paso en el que muchas organizaciones fracasan debido a que no disponen de un proceso adecuado.

La prevención de la violación y la corrupción de los datos son resultados primarios que se obtienen de buenos programas de gestión de acceso y gobernanza de identidad. Si los usuarios adecuados cuentan con el acceso adecuado a los datos exactos en los momentos exactos, se reduce el riesgo de violación y corrupción de los datos que impacta en las actividades comerciales de una empresa y en los clientes. Los programas de gestión de acceso y gobernanza de identidad deben abordar lo siguiente:

- Gestión de acceso
    - Mapeo de perfil de usuario
    - Alta, baja y transferencias
- Evaluación de credenciales
    - Autorización de autenticación
    - Inicio de sesión único y autenticación de múltiples factores
    - Acceso privilegiado
- Gobernanza
    - Gobernanza de acceso
    - Proceso de solicitud y aprobación
    - Procesos de conciliación y error

Endpoint

Los tiempos han evolucionado desde que las organizaciones «únicamente» demandaban dispositivos administrados por la empresa. Actualmente, los usuarios necesitan multitud de dispositivos para hacer su trabajo, por lo que numerosas organizaciones han comenzado a incorporar programas de «trae tu propio dispositivo» (en inglés Bring Your Own Device, BYOD). Un buen inventario de dispositivos es fundamental para un conjunto de dispositivos administrado, ya que es necesario identificarlos, distinguirlos y protegerlos todos mediante la implementación de controles basados en políticas. Sin embargo, las empresas deben proporcionar un acceso seguro a los recursos a dispositivos ajenos a la empresa.

Introducir dispositivos no confiables o no administrados. Cada vez más, las empresas deben permitir el acceso de otros dispositivos, lo que se traduce en el acceso desde endpoints no confiables, además de programas BYOD mencionados anteriormente.

Una organización debe tener en cuenta los endpoints (confiables o no confiables/administrados o no administrados) al establecer su política de acceso de confianza cero. No se trata de la misma política para todo el mundo, por lo que es necesario comprender el contexto del usuario y de la empresa. En ciertas situaciones, los dispositivos no administrados podrán acceder a las aplicaciones (y posteriormente a los datos) de igual forma que los dispositivos administrados. En otros casos, no podrán; puede obtener más información en la sección sobre la clasificación del riesgo.

Aplicación

Con el auge de aplicaciones y servicios en la nube y SaaS, los modelos comerciales y operativos han cambiado. Uno de los aspectos fundamentales de la seguridad es restringir todo lo posible el acceso a los recursos, en este caso, a las aplicaciones. Aquí, la confianza cero es un modelo de seguridad excepcional, ya que los usuarios no necesitan conectarse a las redes, sino que lo hacen a una aplicación determinada o a un servicio mediante sesiones individuales independientes.

Cualquier organización debe tener un concepto muy claro sobre los puntos siguientes en cuanto a los acuerdos de aplicación:

- Tipo de aplicación
- Modelo de alojamiento
- Confidencialidad, integridad y disponibilidad de la aplicación (procedente de los datos a los que accede, almacena o procesa, o del proceso empresarial que respalda)
- Flujos de transacciones: ascendentes y descendentes
- Requisitos de acceso de terceros
- El resultado de una evaluación de riesgos de la aplicación

Red

El perímetro heredado está desapareciendo, la conectividad es universal y la seguridad se ha distribuido. Es crucial comprender los flujos de transacciones y las interacciones entre dos o más puntos. El aislamiento de la red y la microsegmentación a segmentos más localizados son algunas tácticas para reducir el movimiento lateral, pero también permiten controles más granulares sobre el acceso a los recursos.

Los equipos de redes ya comprenden la topología, la entrega de contenido y la calidad del servicio a través del seguimiento y la optimización del rendimiento; sin embargo, la confianza cero introduce cambios más dinámicos dentro de la arquitectura de la red donde es necesario realizar ajustes.

Los endpoints y los usuarios ya no acceden a las redes. Aun así, se pueden conectar directamente a un servicio, aplicación o carga de trabajo individual (esta es la facultad de la confianza cero, ya que ahora podemos reducir de forma importante nuestra superficie de ataque), por lo que es fundamental aplicar los conceptos siguientes:

- Adoptar la postura de seguridad de «denegación por defecto»
- Eludir las «zonas de confianza»
- Aislamiento de sesión
- Microsegmentación

Visibilidad y análisis

Obtener una mayor visibilidad de las transacciones entre los componentes mencionados anteriormente con detalles contextuales y la capacidad de correlacionarlos y analizarlos es totalmente imprescindible. Por lo tanto, podemos comprender mejor la interacción, la calidad y el rendimiento de un ecosistema creado, lo que nos permite mejorar y realizar nuevas políticas refinadas y, por consiguiente, la adopción de controles. Las capacidades se deben alinear con resultados y propósitos determinados, como ayudar con la velocidad de detección y respuesta a las amenazas donde el equipo de relaciones con inversores es el mayor consumidor, centrándose en la búsqueda de amenazas, la investigación forense, las actividades de cumplimiento, etc.

Los programas maduros de confianza cero deberían poder:

- Examinar todo el tráfico (inspección profunda de paquetes, más allá de la telemetría de red)
- Correlacionar datos entre múltiples fuentes con gestión de información y eventos de seguridad (SIEM)
- Identificar comportamientos anómalos con el análisis de comportamientos del entorno del usuario (UEBA)
- Proporcionar una visión global del entorno

Automatización y orquestación

En la actualidad, uno de los retos que afrontan numerosas organizaciones es la disponibilidad de recursos de calidad. La seguridad es uno de los verticales más afectados, donde la desventaja en términos de capacidad ocupa su lugar. Los individuos no pueden proporcionar suficiente velocidad y escala para solucionar dichas complejidades dentro del ecosistema. La creciente complejidad exige el uso de la automatización.

La automatización y la orquestación ofrecen una posibilidad sin precedentes para proporcionar un programa de seguridad más eficiente y eficaz. Se trata del proceso adecuado en el momento adecuado. Gracias a la automatización, las organizaciones pueden acelerar la identificación y resolución de amenazas específicas con un nivel de precisión con el que las personas no pueden competir.

Calificación del riesgo y definición de la política de acceso

El establecimiento del acceso a los recursos, como aplicaciones, servicios o datos, se gestiona mediante la aplicación de controles que se definen mediante políticas. Con estas políticas se implementan las reglas de acceso que se establecen por el deseo de riesgo de la organización. La definición de la política y, en consecuencia, qué controles se aplican, se debería determinar por un conjunto de criterios que evalúe cada uno de los componentes comentados con anterioridad.

Las organizaciones pueden adoptar dos enfoques:

- Para cada atributo, evaluar los posibles escenarios de implementación y definir una regla que permita (o restrinja) un nivel de acceso, y aplicarlos de forma acumulativa.
- Establecer un modelo de riesgo que aplique una ponderación a los escenarios de implementación de todos los atributos y defina políticas de acceso en función del conjunto de la clasificación.

Por ejemplo, para el primer enfoque, en el caso de dispositivos no administrados, la organización puede establecer que los dispositivos no administrados solo puedan acceder a aplicaciones que procesan, almacenan o acceden a datos que tienen una clasificación de confidencialidad y una calificación de integridad bajas. Además, el contexto del usuario se puede incluir en esta decisión relativa a la política; por ejemplo, un usuario interno que procede de un dispositivo no administrado puede acceder a aplicaciones que procesan, almacenan o acceden a datos que tienen una clasificación de confidencialidad e integridad más alta. Sin embargo, no pueden acceder a las aplicaciones o datos más importantes.

Cada permutación puede impulsar una definición de política diferente, por lo que se aplica un conjunto de control diferente.

A continuación se citan algunas permutaciones de muestra se citan, pero la organización debe documentarlas y evaluarlas por sí mismas para que se ajusten a la forma en que trabaja la organización y se alineen con sus estándares y prácticas existentes:

- **Usuario:** Interno permanente, contratista interno, tercero
- **Clasificación de la información confidencial:** Estrictamente confidencial, confidencial, privada, pública
- **Clasificación de la integridad de los datos:** Muy alta, alta, media, baja
- **Clasificación de la disponibilidad de los datos:** Alta disponibilidad, 0-4 horas, 4-24 horas, más de 24 horas
- **Endpoint:** Administrado, no administrado
- **Aplicación:** Crítica, importante, menor

En cuanto al concepto de evaluación continua, durante una sesión de usuario, estos componentes deben evaluarse y verificarse en todo momento. Si se observa algún cambio, se deben adoptar medidas. Tal vez finalizar la sesión, forzar la reautenticación o realizar una configuración de autenticación.

Por ejemplo, ahora parece que la sesión se origina en un dispositivo no administrado, cuando antes se pensaba que era un dispositivo administrado. También es posible que el usuario ahora esté tratando de acceder a datos más confidenciales que los que se evaluaron en un principio.

CONCLUSIÓN

La mayoría de las arquitecturas de seguridad actuales se desarrollaron para un ecosistema tecnológico que ya no es relevante. Se necesita una nueva perspectiva para lograr nuevas formas de operar e impulsar su empresa. La arquitectura de seguridad debe centrarse en comprender de forma clara el riesgo empresarial, su contexto y aplicar controles adaptables para afrontar un nuevo conjunto de desafíos, además de permitir que los usuarios y las empresas progresen rápidamente.

Es fundamental lograr un equilibrio adecuado entre seguridad, privacidad y experiencia del usuario.

Netskope, líder mundial en ciberseguridad, está redefiniendo la seguridad de la nube, los datos y la red para ayudar a las organizaciones a utilizar los principios de confianza cero para proteger sus datos. La solución Intelligent Security Service Edge (SSE) de Netskope es rápida y fácil de usar, y protege a las personas, los dispositivos y los datos en cualquier lugar. Para conocer la forma en que Netskope ayuda a los clientes a prepararse para cualquier cosa, visite netskope.com.