Shadow IT detection

20 días

MICROSOFT CLOUD APP SECURITY

KS - Consulting Services

El uso de servicios alojados en la nube se ha ido incrementando toda vez que estos mismos promueven la productividad dentro de las organizaciones. Sin embargo, con el pasar del tiempo, su volumen de uso puede incrementarse inadvertidamente permitiendo que nuevas aplicaciones no autorizadas de dudosa confiabilidad se integren dentro del ambiente en la nube de la organización.

El consumo de aplicaciones "engañosas" compromete la seguridad dentro del entorno en la nube de la organización, permitiendo filtración de información, ataques de desplazamiento lateral, entre otros tipos de amenazas avanzadas. Nuestra propuesta identifica las tareas comunes que los clientes encuentran útiles para implementar en fases, en el transcurso de **30, 60, 90 días, o más**, para robustecer su estrategia de seguridad. Incluso las organizaciones que ya han implementado elementos de Microsoft Cloud App Security pueden recurrir a este ofertamiento para asegurarse de que están sacando el máximo provecho de su inversión.

KS Consulting realiza las siguientes tareas como parte de éste ofertamiento:

Casos de Uso

El alcance final por ejecutar depende de los casos de uso de definir con el cliente, considerando las siguientes capacidades de Microsoft Cloud App Security.

1. Integración de Log collectors para soluciones de firewall third party
2. Control de aplicaciones con acceso condicional
3. Directivas para detección de comportamiento sospechoso
4. Detección y administración de Shadow IT
5. Directivas para gobierno de aplicaciones
6. Bloqueo de descargas de información confidencial
7. Investigación de aplicaciones OAuth en riesgo
8. Investigación de usuarios en riesgo
9. Administración de seguridad para plataformas en la nube

Estrategia de Implementación:

Las mejores prácticas sugieren considerar los siguientes puntos para proteger el ambiente en la nube mediante Cloud App Security:

1. Descubrir y evaluar aplicaciones en la nube.
    a. Habilitar el descubrimiento de Shadow IT mediante Microsoft Defender for Endpoint.

    b. Configurar directivas de App Discovery que identifiquen riesgos y tendencia de aplicaciones.
    c. Administrar las aplicaciones OAuth que son autorizadas por los usuarios
2. Aplicar directivas de gobernanza en la nube.
    a. Etiquetar aplicaciones seguras y no seguras.
3. Limitar la exposición de información que se comparte externamente y reforzar directivas de colaboración.
    a. Conectar MCAS con Office 365.
    b. Conectar MCAS con aplicaciones de colaboración Third Party.
    c. Evaluar la exposición de información a usuarios externos.
    d. Crear directivas que deshabiliten la colaboración con cuentas personales.
4. Descubrir, clasificar, etiquetar y proteger información sensible almacenada en la nube.
    a. Integrar MCAS con Azure Information Protection.
    b. Crear directivas de exposición de información.
5. Establecer directivas de cumplimiento y DLP para la información almacenada en la nube.
    a. Proteger la información confidencial ante la colaboración externa.
6. Proteger y bloquear la descarga de información sensible desde dispositivos no administrados o en riesgo.
    a. Administrar y controlar el acceso a dispositivos de alto riesgo.
7. Proteger las colaboraciones externas estableciendo controles de sesión en tiempo real.
    a. Monitorear sesiones con usuarios externos mediante acceso condicional.
8. Detectar amenazas en la nube, cuentas de usuario comprometidas y ransomware.
    a. Establecer directivas de comportamiento sospechoso, ajustar rangos de IP para conceder acceso.
    b. Detectar actividad realizada desde ubicaciones poco comunes.
    c. Crear directivas para aplicaciones OAuth.
9. Proteger IaaS y aplicaciones personalizadas,
    a. Conectar Azure, AWS y GCP con MCAS
    b. Evaluar assessments de configuración para Azure, AWS y GCP.
    c. Integrar aplicaciones personalizadas al monitoreo de MCAS

La implementación final se realizará de acuerdo a la Definición del Alcance, considerando los Casos de Uso a Implementar.

Timeline Operativo

Con base al Alcance Definido, se tomará la Estrategia de Implementación adecuada, y se ejecutará en fases, de acuerdo al siguiente modelo operativo:

- Fase 1: Workshop, Análisis y Diseño.
- Fase 2: Habilitación de Plataformas.
- Fase 3: Configuración de Herramientas.
- Fase 4: Pruebas y Control de Calidad.
- Fase 5: Transferencia de Conocimientos.
- Fase 6: Go-Live.

El tiempo final de implementación se encuentra sujeto a Alcance:

- Básico: 30 días hábiles.
- Intermedio: 60 días hábiles.

- Avanzado: 90 días hábiles, o más.

Herramientas Tecnológicas

- Conditional access app control
- Cloud Discovery
- Log connectors
- App connectors
- Cloud App Security Policies

Mayor Información:

Conditional Access app control

Conditional Access app control emplea una arquitectura de reverse proxy que se integra con el Identity Provider. Esta característica se implementa de manera similar a como se haría con una regla de acceso condicional de Azure AD, estableciendo asignación de usuarios y grupos, selección de aplicaciones integradas, ubicaciones o segmentos de IP para los cuales la regla se aplica. Después de haber definido las condiciones las sesiones de los usuarios serán monitoreadas por Cloud App Security.

Conditional access app control habilita las sesiones y aplicaciones de los usuarios para ser monitoreadas y controladas en tiempo real basándose en directivas de sesión y acceso. Las directivas de sesión y acceso son usadas por Cloud App Security y proveen una mayor visibilidad de las acciones que los usuarios realizan dentro del entorno en la nube de la organización. Con el uso de estas directivas es posible:

- Prevenir filtración de datos externamente: Se pueden bloquear las descargas de documentos confidenciales en dispositivos no administrados.
- Protección en descargas: En lugar de bloquear la descarga de archivos confidenciales, se puede requerir que estos sean etiquetados con Azure Information Protection . Esta acción asegura que esta protegido y su acceso solo esta permitido a los usuarios definidos por la etiqueta.
- Prevenir la carga de documentos sin etiquetado: Antes de que algún tipo de información sensible fuese a ser cargada y compartida con otros usuarios, es importante asegurarse que el documento cuente con la protección necesaria. Es posible establecer controles para bloquear la carga de archivos que no cuenten con un etiquetado apropiado.
- Bloqueo de Malware potencial: Se puede proteger el entorno en la nube de malware restringiendo la carga de archivos sospechosos a la nube corporativa. Cada archivo que se carga puede ser escaneado por Microsoft Threat Intelligence y ser bloqueado instantáneamente.
- Monitorear sesiones de los usuarios con fines de cumplimiento: Los usuarios en riesgo son monitoreados cuando ingresan a sus aplicaciones. Durante esa sesión sus acciones son registradas.

- Bloquear acceso: Permite bloquear el acceso a aplicaciones y usuarios específicos basándose en distintos factores de riesgo.

Cloud Discovery

Cloud Discovery analiza los logs de trafico generados por la organización y los contrasta con el catalogo de aplicaciones de Cloud App Security. Las aplicaciones de este catalogo se encuentran evaluadas y se les asigna un score basándose en más de 80 factores de riesgo.

Cloud Discovery provee 2 tipos diferentes de reporte:

- Snapshot reports: Provee el analisis de un set de logs de tráfico cargados manualmente desde firewalls y proxies.
- Continuous reports: Analiza todos los logs que se generan por desde la red organizacional. Estos reportes otorgan una mejor visibilidad sobre lo que ocurre dentro del entorno en la nube de la organización e identifica automáticamente comportamientos sospechosos mediante el uso de Machine learning o por las directivas personalizadas definidas dentro de MCAS

Cloud App Security soporta los siguientes firewalls y proxies para su integración:

- Barracuda - Web App Firewall (W3C)
- Blue Coat Proxy SG - Access log (W3C)
- Check Point
- Cisco ASA with FirePOWER
- Cisco ASA Firewall (For Cisco ASA firewalls, it's necessary to set the information level to 6)
- Cisco Cloud Web Security
- Cisco FWSM
- Cisco IronPort WSA
- Cisco Meraki – URLs log
- Clavister NGFW (Syslog)
- ContentKeeper
- Corrata
- Digital Arts i-FILTER
- Forcepoint
- Fortinet Fortigate
- iboss Secure Cloud Gateway
- Juniper SRX
- Juniper SSG
- McAfee Secure Web Gateway
- Menlo Security (CEF)
- Microsoft Forefront Threat Management Gateway (W3C)
- Palo Alto series Firewall
- Sonicwall (formerly Dell)
- Sophos SG
- Sophos XG
- Sophos Cyberoam
- Squid (Common)
- Squid (Native)
- Stormshield
- Websense - Web Security Solutions - Investigative detail report (CSV)
- Websense - Web Security Solutions - Internet activity log (CEF)
- Zscaler

App Connectors

Los app conectors se integran con las APIs de los servicios para proveer una mayor visibilidad y control dentro de Cloud App Security.

Dependiendo de la aplicación conectada, la conexión con su API habilita los siguientes ítems:

- Información de la cuenta: Información del perfil, status (suspendida, activa, deshabilitada), grupos y privilegios.
- Audit Trail: Visibilidad dentro de las actividades de usuarios, actividad administrativa, actividad de inicio de sesión.
- Permisos de aplicaciones: Visibilidad de los tokens expedidos y sus permisos.
- Gobernanza de la información: Capacidad para colocar documentos en cuarentena.
- Gobernanza en permisos de aplicación: Capacidad para remover tokens.

App connectors de Cloud App Security cuentan con soporte para las siguientes plataformas:

- Azure
- AWS
- Box
- Dropbox
- Github
- GCP
- G Suite
- Office 365
- Okta
- Salesforce
- Service Now
- Webex
- Workday

Cloud App Security policies

Las directivas permiten definir el comportamiento de los usuarios dentro de las aplicaciones integradas a MCAS. Mediante las directivas es posible detectar actividad sospechosa dentro del ambiente en la nube. Existen diferentes tipos de directivas que correlaciona la información que se requiere reunir acerca del ambiente en la nube y las medidas correctivas a ejecutar.

Dentro de la sección de directivas en el portal de MCAS se pueden encontrar distintos tipos de plantillas de directivas, estas pueden ser distinguidas mediante un

icono en particular La disponibilidad de estas directivas depende de la fuente de información que se encuentre habilitada en MCAS.

- Directiva de acceso: controla y monitorea en tiempo real los intentos de inicio de sesión que realizan los usuarios a las aplicaciones en la nube integradas a MCAS.
- Directiva de actividad: permite monitorear actividades específicas realizadas por los usuarios o dar seguimiento a comportamientos sospechosos sobre un determinado tipo de actividad.
- Detección de anomalías: habilita alertas cuando detecta actividad sospechosa en el ambiente en la nube, basado en el factor de riesgo que se configura para disparar las alertas.
- Directiva de descubrimiento de aplicaciones: emite una alerta que notifica cuando una nueva aplicación es detectada dentro de la organización.
- Detección de anomalías en el Cloud Discovery: analiza los logs que se cargan para el descubrimiento de aplicaciones en busca de eventos inusuales.
- Directiva de archivos: permite escanear las aplicaciones integradas a MCAS en busca de archivos y datos, con la finalidad de aplicar acciones de gobernabilidad.
- Directiva de sesión: provee control y monitoreo en tiempo real sobre la actividad del usuario dentro de las aplicaciones integradas a CAS.