SERVICIOS

Gestión de Protección Integral en EndPoint:

El servicio está diseñado para gestionar la seguridad de las plataformas endpoint de las organizaciones en la protección de los datos y dispositivos tanto corporativos como personales.

Proceso

Inicialmente, recopilará información sobre los usuarios, los requisitos de seguridad de la organización y definirá los procesos, las reglas o políticas que se requieren.

Los resultados de la evaluación serán luego revisados por un Consultor Certificado de Azure, quien hará sugerencias basadas en:

- Gestión de amenazas e incidentes
- Mantener un ambiente de trabajo seguro.
- Gestión segura de documentos y aplicaciones.
- Necesidad de autenticación híbrida.

Administración del Servicio

Basados en una comprensión clara de las metas y objetivos comerciales del Cliente para evaluar el alcance y la dirección del trabajo con precisión.

Se gestionará:

Los endpoints: aprovisionamiento e inscripción

Seguridad unificada con controles Zero-Trust. Acceso seguro a los recursos corporativos mediante evaluaciones continuas y políticas basadas en el uso que controlan las aplicaciones de acceso condicional con tecnología de Azure Active Directory (Azure AD) y la integración nativa Microsoft Endpoint Manager.

Protección de datos laborales: Garantiza el cumplimiento del dispositivo y la aplicación para controlar el flujo de datos fuera de las aplicaciones móviles de confianza a través de las directivas de administración de aplicaciones móviles (MAM) y administración de dispositivos móviles (MDM).

Licenciamiento mínimo necesario:

M365 E3 + E5 Security Add-on
M365 E5.
M365 F3 + F5 Security
M365 F3 + F5 Security+Compliance

Evaluación de Identidades en Azure:

La evaluación está planteada para ayudar a los clientes a planificar formas de implementar Azure Identity y Access Management con el objeto de incrementar las defensas contra intentos de accesos no permitidos protegiendo identidades con propuestas de opciones de autenticación sin impacto en la operación y/o productividad

Proceso

Un consultor certificado en Azure recopilará información mediante la revisión del ambiente tecnológico actual y a través reuniones con el personal técnico de IT

Posteriormente se analizarán los resultados de la evaluación y ofrecerá asesoría en:

- Protección de datos confidenciales/sensibles
- Integración con Active Directory (On-Prem, Azure AD, aplicaciones de negocio, aplicaciones cloud, identidades externas)

Entregables

Basados en una comprensión clara de las metas y objetivos comerciales del Cliente para evaluar el alcance y la dirección del trabajo con precisión.

- Informe sobre las prácticas actuales de gestión de identidades y accesos.
- Informe sobre la integración de Identidades con las aplicaciones
- Reporte de análisis de brecha y mejores prácticas
- Tecnologías de Seguridad Azure (MFA, SSO, PIM, PAM, AAD)

Licenciamiento mínimo necesario:

M365 E5.
M365 E3 + E5 security Add-on.
M365 F1 + F5 Security
M365 F1 + F5 Security+Compliance
M365 F3 + F5 Security
M365 F3 + F5 Security+Compliance
Office365 E1 + Enterpirse Mobility + Security (tanto en las versiones E3 ó E5) .
Office365 E3 + Enterpirse Mobility + Security (tanto en las versiones E3 ó E5)
Office365 E5 + Enterpirse Mobility + Security (tanto en las versiones E3 ó E5) .

Gestión de monitoreo, auditoría, esquema de alertas en accesos a buzones de correo y Spam/Malware en Exchange 365

Monitoreo y auditoría activa de los buzones de correo en Exchange 365 que permita identificar, corregir y reducir en forma rápida los accesos a los buzones de los usuarios con cuentas privilegiadas, cualquier anomalía o fallas en la configuración que conlleven a problemas de seguridad y de perdida de información personal, laboral y/o sensible.

Un buzón de correo de Exchange Online puede recibir mensajes de spam con contenido malintencionado en cualquier momento, razón por la cual debe estar atento a todas las amenazas enviadas por correo que ingresen a los buzones de correo de su empleados.

El servicio se propone para facilitar la gestión y entregar información, alertas, reportes y alternativas de mitigación, con el objetivo de reducir cualquier anomalía por cuentas privilegiadas y el uso de estas como así también la protección de ingresos de correo malintencionados.

Proceso/Tareas

- Auditoría en el Centro de cumplimiento de Microsoft 365.
- Monitoreo de las actividades de los Usuarios y Administradores y Delegados.
- Retenciones del registro de Auditoría.
- Análisis y monitoreo de delegación de buzones, contactos y calendarios.
- Análisis y monitoreo de buzones genéricos y/o compartidos.
- Accesos condicionales de Usuarios privilegiados a la consola de Administración
- Análisis y Monitoreo de usuarios de riesgo
    - Indicadores basados en acceso, en datos, en aplicaciones
    - Mitigación

Administración del Servicio

- Gestión del del entorno de seguridad del servicio de correo en nube (E365).
- Informe global detallado del estado del servicio.
- Gestión de Alertas.
- Informes periódicos de la salud del sistema.
- Detalles sobre mensajes de spam, como remitente, destinatario, otros
- Lista de los principales destinatarios de spam y la cantidad de spam que han recibido durante un período de tiempo especificado.
- Detección de correos electrónicos maliciosos, lista de los nombres de remitentes y destinatarios, la hora de recepción, etc.
- Listado de los principales destinatarios de malware y la cantidad de malware que han recibido durante un período de tiempo específico.
- Recomendación de mejoras

Licenciamiento mínimo necesario:

M365: E5.
M365: E3 + E5 compliance add-on
M365 F1 + F5 Compliance Add-on.
M365 F1 + F5 Security+Compliance
M365 F3 + F5 Compliance Add-on.
M365 F3 + F5 Security+Compliance
Office365:E5.

Migración a Microsoft Intune

Con independencia que ya cuente con una solución (Mobile Iron, Airwatch, MaaS360, entre otros) o (comienzo desde cero), Intune combina MDM/MAM en una sola solución permitiendo que todos los usuarios se beneficien del conjunto más amplio de características que esta herramienta ofrece (*)[i]

Proceso

Se recopilará información (relevamiento inicial) mediante la revisión del ambiente tecnológico actual y a través reuniones con el personal técnico de IT

Revisión de la configuración actual de MDM corporativo

- Análisis de las políticas de seguridad, perfiles de los dispositivos y las reglas de cumplimiento.
- Casos de uso.
- Inventario de dispositivos.
- Propiedad y la cartera de aplicaciones.
- Análisis de los resultados de la evaluación.

Informe de conclusiones y recomendaciones

- Análisis de gap: evaluación de la preparación técnica y la integración de Intune con iOS / Android
- Análisis de dependencias: evaluación de las dependencias faltantes que deben remediarse
- Recomendaciones: opciones de diseño para implementar un entorno que siga las mejores prácticas de Microsoft y los estándares de la industria para casos de uso definidos.

Entregables

- Plan de migración con la secuencia y el cronograma detallado
- Comunicación a usuarios finales
- Guía de Mejores Prácticas

Licenciamiento mínimo necesario:

M365 E3
M365 E5
Office365 F1
Office365 F3
Office365 E1 + add on de Enterpise Mobility + Security (tanto en las versiones E3 ó E5).
Office365 E3 + add on de Enterpise Mobility + Security (tanto en las versiones E3 ó E5)
Office365 E5 + add on de Enterpise Mobility + Security (tanto en las versiones E3 ó E5)

Concientización y Entrenamiento - Simulación de ataque controlado

(MSFT 365 E5 – Defender)

A través de la ejecución de escenarios de ataque realistas en su organización, ayudamos a identificar y encontrar usuarios vulnerables (empleados descuidados o desinformados) con el objetivo que comprendan los comportamientos esperables antes situaciones de exposición con el fin que tomen conciencia de la ciberseguridad educándolos sobre los diferentes riesgos y amenazas a los que están expuestos.

Proceso

Se definirán, en conjunto con el Cliente

- El tipo de campaña y temática
- Template o desarrollo de la pieza (personalización)
- Opciones de segmentación (grupos de Usuario)
- Opciones de entrenamiento
- Simulación (testing)
- Definición de cronograma de ejecución
- Despliegue

Entregables

Reportes de:

- Impacto de la simulación.
- Actividades del usuario.
- Estado de aprendizaje.
- Acciones de mejora.

Licenciamiento mínimo necesario:

M365 E3
M365 E5
Office 365 Plan 2.