CIBERSEGURIDAD

defender for office administrado

Servicio basado en la nube que protege ante ataques de phishing, suplantación de identidad y otros tipos de ataques sofisticados de malware a través de links maliciosos que se ofrecen a través del correo electrónico y herramientas de colaboración de Office 365, incluyendo SharePoint Online, OneDrive para la empresa y Microsoft Teams.

CARACTERÍSTICAS

- Protección URL maliciosas

El servicio analiza el contenido del enlace para ver si existe algún tipo de alerta, y si un vínculo no es seguro, se advierte al usuario para que no visite el sitio o directamente se bloquea.

- Protección de Phishing

Funcionalidad que nos protege de ataques de phishing que vienen de personas que a priori conocemos pero en realidad no son ellos quienes nos han enviado el correo (es lo que se denomina ataque basado en suplantación).

- Protección archivos adjuntos maliciosos

Los archivos adjuntos se someten a un análisis de comportamiento de malware en tiempo real que usa técnicas de aprendizaje automático para evaluarlos en busca de actividad sospechosa.

- Informes

Informes de tipo de ataques que están ocurriendo en la organización sobre quién es el objetivo en tu empresa, el malware y spam enviado o recibido en la compañía y la categoría de los ataques.

BENEFICIOS

- Protección nativa para Office 365
- Mejorar la capacidad de protección de las empresas apegado a las mejores practicas de Seguridad
- Esquema de Servicio Administrado
- Mejorar la postura de seguridad

DATOS DUROS

91%
Ciberataques que comienzan con el correo electrónico

20%
Los usuarios de correos electrónicos de phishing hacen clic en 5 minutos

94%
Del malware se distribuye por correo electrónico.

280 days
Tiempo promedio para identificar y contener una violación

$26B
Pérdida atribuida al Business email compromise (BEC) desde 2016

48%
Casi la mitad de los archivos maliciosos son documentos de Office

1Verizon 2019 Data Breach Investigations Report | 2IBM Cost of a Data Breach Report 2020 | 3US Federal Bureau of Investigation, April 2019 | 4Microsoft

Microsoft

alestra