Caso de estudio

Mi firma de colaboradores presta servicios de consultoría desde el año 2012, recientemente, hemos tenido un crecimiento bastante considerable a nivel de organización como de clientes. Lo que ha causado que mi firma sea más reconocida y este en contacto con clientes importantes y delicados. Con esta transformación digital, nos hemos tenido que adaptar a cambios hacia lo digital por lo que invertir en el tema de seguridad en estos momentos es un factor muy importante para nosotros.
Mi infraestructura actual comprende 5000 usuarios distribuidos en las principales ciudades de Estados Unidos y Colombia, mi campo de acción, aunque comenzó siendo de TI, se ha movido en temas de inversiones, asuntos legales y actividades de consultoría para clientes corporativos los cuales mi firma representa. Pearson Speacter se ha ganado una reputación con los últimos años y tenemos todos los días problemas en poder cubrir nuestra confidencialidad documental de manera digital.

Respuesta: *Para el caso de los problemas con la seguridad documental de la empresa se recomienda implementar* ***Azure Information Protection*** *que permite etiquetar y clasificar la información de acuerdo al nivel de seguridad y confidencialidad que tengan los documentos. Como en este caso en particular se maneja información sensible (asuntos legales), se recomienda etiquetar la información.*

Así mismo hemos sido víctimas de intentos de Hack durante muchos años, dada la importancia de nuestros clientes. Tenemos máquinas de Tipo Windows 7 y Windows 10, y manejamos información de tipo sensible dirigida a Juzgados, Cortes. Requerimos una herramienta que monitoree las identidades de mi AD local, para tener administrado los recursos de mi directorio activo.

Respuesta*: Para este caso se recomienda el uso de* ***Azure Active Directory*** *porque esta solución nos permite administrar las identidades y acceso a los recursos de la empresa. Además, se sugiere al cliente que en caso de tener un directorio activo local realizar la migración a cuentas de office 365 en la nube.*

Necesitamos una solución integral que abarque no solo proteger mi información, sino la información que me confían mis clientes, sin importar el lugar del mundo donde se pueda generar. Recibimos clientes con mercados en todo el mundo y la información debe viajar fácilmente in importar el idioma ni el destino de esta.

Respuesta*: Para este caso se recomienda el uso de la herramienta* ***Microsoft defender for identity*** *porque mediante los controladores de dominio se puede obtener información de las actividades que realizan los usurios del directorio local.*

Adicionalmente, para flexibilidad de mis empleados se les permite el uso de sus dispositivos móviles, pero con los años hemos notado que este puede ser un foco de filtración de información confidencial, por lo que requiere alguna solución de administración de dispositivos móviles donde yo pueda tener potestad sobre la información de mi empresa.

Respuesta: *Se recomienda el uso de* ***Microssoft intune*** *porque es una solución orientada a la administración y vigilancia de dispositivos móviles dentro de una organización. Con esta solución se puede acceder a los recursos de la empresa siempre y cuando el dispositivo se haya registrado previamente en la plataforma de intune, con esta solución porque puedo controlar el acceso a las aplicaciones, asignar políticas de seguridad de acuerdo a roles y observar el estado del dispositivo*.

También es muy importante que mis usuarios a nivel de correo electrónico cuenten con una solución para evitar ataques por medio de mails maliciosos.

Respuesta*: Para este caso se recomienda el uso de* ***Defender office 365*** *porque esta solución permite configurar reglas de flujo y salidas de correo, con office 365 es posible analizar enlaces web sospechosos, archivos adjuntos, archivos de SharePoint, OneDrive, proteccion ante ataques de phishing, entro otros*.

Debido a tantos tipos de ataques que se han presentado y de las cuales he visto noticias, es necesario crear algún tipo de regla que me permita que solo se pueda acceder a los recursos de la nube de mi organización solo de direcciones IP de Colombia y USA de resto es necesario que se bloquee dicho acceso.

Respuesta*: En este caso se recomienda el uso de* ***Azure AD*** *porque mediante el uso de acceso condicional puedo conceder el acceso a aplicaciones o recursos en la nube basados en ciertas condiciones y políticas de seguridad que se establezca.*

También, para mejorar la productividad de mis empleados y bajar un poco la carga de requerimientos hacia el área de TI, requiero algún tipo de solución que me permita que los usuarios gestionen su contraseña de manera independiente. Pero también requiero que la contraseña que se establezca, sea lo suficientemente compleja para que se considere robusta.

Respuesta*: En este caso se recomienda el uso del* ***Self-Service Password Reset o*** *también conocido como restablecimiento de contraseña de autoservicio que ofrece al usuario a la posibilidad de cambiar su contraseña sin la necesidad que intervenga el administrador. Para el caso de definir una contraseña robusta se recomienda el uso de* ***Password Protection*** *o proteccion de contraseña esta funcionalidad permite detectar contraseñas débiles mediante inteligencia artificial y evitar que se seleccione. Es importante mencionar que estas dos soluciones vienen instaladas en el* ***Azure Active Directory***

De igual manera y como se han visto en muchas aplicaciones adicionalmente requiero que mis usuarios tengan un paso mas en su autenticación para validar que efectivamente sean ellos quien se autentican antes mis servicios.

Respuesta: *En este caso se recomienda el uso del método de autenticación Multifactor Authentication (MFA) que permite que un usuario puede acceder a un recurso solo después de cumplir un segundo paso de autenticación que puede ser huella digital, mensaje texto, entre otros. Esta propiedad también puede ser activada dentro de la solución Azure AD*

Finalmente cuento con algunas máquinas virtuales en Azure y algunos otros recursos, pero, necesito que solo un listado de personas específicas que administren estos recursos.

***Respuesta**: Para este caso se recomienda el uso del servicio **Privileged Identity Management (PIM)** porque permite administrar, controlar y monitorear el acceso a recursos importantes de la organización, por la tanto se asigna permisos a una cantidad específica de usuarios para que accedan a la información. Este servicio también se encuentra en Azure AD.*

Hemos sido clientes durante muchos años de Alphabet Services Google Inc., pero estamos dispuestos a recibir asesoramiento de alguna compañía que pueda brindarnos un protocolo de seguridad sólido y creíble no solo al interior de nuestra organización, sino de frente a todos nuestros posibles contendientes, colegas, asociados.

En resumen, para suplir las necesidades de seguridad de la organización se recomienda hacer uso de las siguientes recomendaciones:

- Para administrar y monitorear los recursos del directorio activo local se recomienda Azure Active Directory.
- Para el caso de la administración y gestión de dispositivos móviles se recomienda usar Microsoft intune.
- Para el caso de proteger la información de la empresa como de los clientes de diferentes localidades se recomienda Microsoft defender for identity
- Para el caso de la seguridad de correos electrónicos se recomienda usar Microsoft office 365.
- Para proteger los documentos digitales se debe usar Azure Information Protection.
- Para crear las reglas de seguridad donde solo se permite el acceso a la nube a ciertas direcciones IP se recomienda el uso de Azure AD donde se debe configurar los accesos restringidos.
- Para la gestión de contraseñas de manera independiente por parte de los usurios y asignación de contraseñas seguras se recomienda el uso de Self-Service Password Reset y Password Protection.
- Para el caso de que los usuarios tengan un paso más de autenticación se recomienda usar el método Multifactor Authentication (MFA)
- Para el caso de la administración especifica de una lista de personas a los recursos de la organización se recomienda usar el servicio Privileged Identity Management (PIM*)*

Adicionalmente si el cliente desea se puede le ofrecer la herramienta **Microsoft Cloud App Security** para tener conectada todas las aplicaciones y tener un sistema de seguridad muy completo y centralizado donde se tiene acceso a todo el inventario de actividades que se realiza en la organización.

Microsoft
Intune