Informe de asesoramiento basado en la arquitectura de referencia de ciberseguridad de Microsoft para la empresa Veiligheidsregio Twente

Alumno: Francisco Ramos Cascales

Tutor: Juan Carlos Sánchez Aarnoutse

Grado en Ingeniería Telemática

Septiembre 2020

Índice

1. Resumen

El presente documento es un resumen del trabajo realizado como Trabajo Fin de Grado (TFG en adelante) durante mi estancia Erasmus en la universidad de Saxion (Países Bajos). Adjunto a este documento se podrá encontrar el documento original redactado en inglés que se presentó a modo de memoria del trabajo a los profesores responsables en la universidad de destino, así como a la empresa solicitante del proyecto.

En primer lugar, es conveniente contextualizar la naturaleza de este proyecto, que está condicionado, por un lado, a la oferta y la concepción de proyectos que tiene dicha universidad, y por otro, a la situación sanitaria excepcional derivada de la COVID-19, que surgió durante la elaboración de este trabajo.

La universidad de Saxion tiene un interesante programa Internacional dedicado tanto a estudiantes Erasmus, como a estudiantes del propio país que quieran participar en él. El propósito de este programa es crear grupos de trabajo que se deben hacer cargo de realizar un proyecto para una empresa real. A cada grupo de trabajo se le ofrece una formación inicial, pero posteriormente los integrantes son los responsables de continuar su propia formación para poder satisfacer los objetivos establecidos por la empresa-cliente. Es responsabilidad del grupo gestionar las tareas para cumplir con los objetivos exigidos por la empresa, asignando responsabilidades a los integrantes para cada una de las tareas.

Una vez finalizado el trabajo, cada grupo debe presentar un informe tanto a los directores del trabajo como a la propia empresa en sí, así como realizar una presentación oral del trabajo. De hecho, es necesario mencionar que una pieza clave en este tipo de proyectos es tener como destinatario final una empresa real, con todas las implicaciones que conlleva en cada una de las fases. En primer lugar, las exigencias del proyecto las marca la empresa, y deben ser cubiertas. En segundo lugar, la obtención de información para la elaboración de este trabajo debe realizarse consultando la documentación que tiene la empresa al respecto, o en su defecto, realizando entrevistas y auditorías, lo cual no es sencillo, dado que normalmente no hay tiempo que perder. Por último, las expectativas de una empresa siempre son altas: no quieren un trabajo que no les sirva para nada, para eso no malgastan su tiempo. Buscan un trabajo profesional que les ayude realmente a mejorar su empresa.

Además de todo lo comentado sobre el hándicap de trabajar bajo pedido de una empresa real, debo añadir que esta estancia Erasmus ha tenido lugar entre los meses de febrero y junio de 2020, fechas que han coincidido con la primera ola y expansión de la COVID-19 por lo que ha afectado en algunos aspectos del proyecto, impidiéndonos en todo momento el acceso a la plataforma en la que posteriormente se implementaron los resultados.

Volviendo de nuevo al contexto académico, a mi grupo de trabajo, conformado por otros cuatro integrantes más (Lars Perik, Dylon Saaied, Thomas Nijenhuis, Wesley Bolk), se nos asignó como proyecto realizar una investigación sobre las distintas tecnologías de ciberseguridad de Microsoft, para, con dicha información, entregar posteriormente a nuestro cliente (la empresa Veiligheidsregio Twente) un informe de asesoramiento. Dicho informe se llevó a cabo basándonos en la arquitectura de tecnologías Microsoft mostrada en la figura 1.

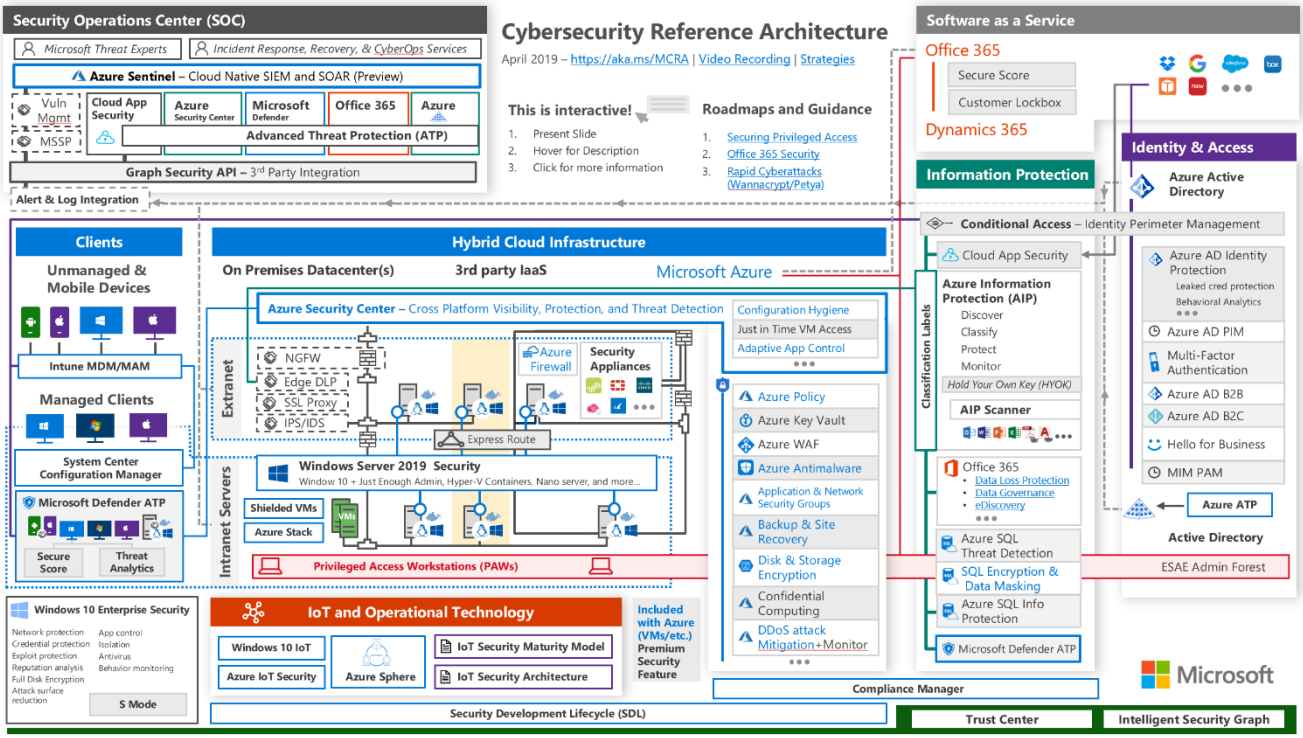

Figura 1. Arquitectura de referencia de ciberseguridad de Microsoft

El enfoque general ha sido el de buscar información en Internet y mediante cuestionarios que se entregando al cliente. Debido a que no fue posible entrar en el entorno real de la empresa para hacer una investigación más exhaustiva y por nuestra cuenta, tuvimos que organizar talleres (los denominábamos workshops) con el cliente, para los que fuimos preparando preguntas y listas de verificación para que de esa forma el cliente pudiera mostrarnos lo que tenían y lo que les íbamos pidiendo que nos mostraran a modo de ayuda en nuestra investigación. Este fue un factor importante para conocer la situación actual y quizás probar algunas opciones. En resumen, la mayor parte de la investigación se realizó en fuentes de Microsoft y la investigación de la situación actual de la empresa se realizó mediante entrevistas y talleres con el cliente.

Para realizar el informe de asesoramiento nos basamos en la arquitectura mostrada en la figura 1, se realizaron videoconferencias con el cliente para ir obteniendo detalles de los distintos elementos que ya tenían desplegados, así como los que querían tener operativos, para los cuales necesitaban nuestra ayuda.

Además, la investigación se llevó a cabo, por un lado, mediante la documentación que Microsoft incorpora en su página web sobre sus distintas tecnologías, donde se pueden ver en profundidad los distintos componentes; y por otro lado, a través de videoconferencias guardadas en la web de Microsoft donde explican sus productos y la forma en la que los utilizan.

A partir de ahora, al hacer referencia a la empresa Veiligheidsregio Twente la llamaremos 'VRT'.

En el resto de este documento se aportan más detalles sobre este TFG, no obstante, a modo de conclusión para esta sección que pretende ofrecer un resumen general del trabajo, se podría decir que mediante este trabajo (compuesto por una fase de investigación más otra posterior de realización del informe de asesoramiento que fue entregado a VRT), conseguimos que mejoraran diversos aspectos de su seguridad empresarial, incrementando la confidencialidad,

facilitando el tratamiento de los datos mediante el uso de etiquetas y agrupaciones para los distintos documentos, entre otras vertientes relativas al manejo de los datos empresariales que también fueron mejoradas mediante la entrega y puesta en práctica de nuestros informes.

Más adelante, concretamente en la sección 3.1.1, se expondrán los distintos apartados de los que me he encargado de forma individual y que por tanto no corresponden a ninguno de mis compañeros.

2. Palabras clave

Desde ahora en adelante, la mayoría de las veces en las que se usen las siguientes palabras clave, se utilizarán las siglas correspondientes a los nombres en inglés, debido al lenguaje del entorno en el que estuvimos trabajando, aunque parte de ella también en holandés y a que algunas de las imágenes que fueron recopiladas incluyen también los siguientes términos en inglés.

Azure Active Directory (Azure AD)

Azure Information Protection (AIP)

Privileged access management (PAM)

Identity & access management (IAM)

Multi-Factor Authentication (MFA)

Active Directory Federation Services (ADFS)

Azure Rights Management (Azure RMS)

Conditional Access (CA)

Security Information and Event Management (SIEM)

Account, global, domain local, permission (AGDLP)

Local Active Directory

Baseline Informatiebeveiliging Overheid (BIO): El Gobierno de seguridad de la información de referencia (BIO) es el marco de estándares básicos para la seguridad de la información en todos los niveles de gobierno en los Países BajosSharePoint

Office365

Monitorización

Etiquetado unificado

3. Alcance del proyecto y división del trabajo

En un principio realizamos una videoconferencia con el cliente en la cual se nos mostró mucha información y se nos comentaron muchas tareas que se esperaban de nosotros, de entre las cuales las primeras semanas tuvimos que ir estudiando y valorando, para así hacer el reparto de trabajo y ver qué cosas podíamos abordar y qué cosas no con el tiempo que teníamos, por lo tanto este apartado recoge todo lo que se propuso por parte del cliente desde un primer momento y se divide en sub apartados en los que se indica finalmente qué apartados quedaron tanto dentro como fuera del alcance de nuestro proyecto.

3.1 Apartados dentro del proyecto

A continuación se exponen distintos apartados que se han tratado en el proyecto:

-Asesoramiento sobre la implementación de componentes especificados (no realización técnica real)

-Asesoramiento sobre la monitorización de componentes especificados

-Se diseñará al menos un componente de la infraestructura de Azure de VRT

- [Azure AD] Privileged access management

- [Azure AD] Identity & access management

- [Azure AD] Servicios conectados (IAM, Beaufort, SharePoint, Office365)

- [Azure AD] Asesoramiento en estructura AD (implementación)

- [AIP] Asesoramiento en clasificaciones de datos

- [AIP] Asesoramiento en implementación general

3.1.1 Apartados realizados exclusivamente por mí

En un principio tuvimos que hacer una división de trabajo sobre los distintos apartados que fuimos elaborando en cuanto a nuestro informe de investigación, por lo que las primeras semanas realizamos una investigación exhaustiva sobre los apartados que se pidieron por parte del cliente y elaboramos un informe en el que recopilamos todos los componentes e información recogida para posteriormente realizar una correcta división del trabajo y realizar este proyecto de manera más efectiva, enfocándonos cada uno de nosotros a distintos temas.

Básicamente mi parte personal del proyecto ha consistido, en primer lugar, en realizar un *product breakdown structure* (PBS), y un *work breakdown structure* (WBS) puesto que me designaron como el encargado de plasmar de forma general los resultados que el cliente quería por nuestra parte y también de realizar un mapa en el que se vieran los procedimientos que podíamos seguir para alcanzar nuestros objetivos en base al tiempo que teníamos.

En segundo lugar, me encargué de realizar una investigación exhaustiva en fuentes de internet, como páginas de Microsoft, documentos de gitHub y artículos publicados en algunos periódicos, entre otros, sobre los apartados que se indican más adelante en este mismo capítulo.

Por último, en base al informe de investigación que realicé recopilando todo lo relacionado sobre los temas, me encargué de redactar un informe de asesoramiento que se resume en los apartados posteriores de este documento, a los cuales me dediqué de manera individual, y que son los siguientes:

6.1.1 Consejos para Azure AD

6.1.1.1 Azure AD en general

6.1.1.1.1 Prácticas ya existentes

6.1.1.1.2 Prácticas a implementar

6.1.1.3 Acceso condicional

6.1.1.3.1 Prácticas ya existentes

6.1.1.3.2 Prácticas a implementar

6.1.2 Consejos para AIP

6.1.2.1 Protección de datos

6.1.2.1.1 Mejores prácticas

6.1.2.1.2 Ajustes de protección recomendados

6.1.2.1.3 Escenarios comunes e instrucciones relacionadas

6.1.3 Consejos para la SIEM

6.2 Evaluación (del cliente y de los resultados del proyecto)

8 Apéndice

Además de los roles anteriormente dichos, tuve que realizar un itinerario de los avances que íbamos realizando, así como un calendario con distintas entregas que iba programando según obteníamos información para ir así a las entrevistas con el cliente lo más preparados posibles y que nos fueran realmente útiles para seguir con nuestra investigación. Para esto propuse varias listas de verificación (checklists) con preguntas que nos iban surgiendo a lo largo del proyecto y con dudas también para ver con ellos en vivo dentro de su entorno, para que el cliente nos fuera mostrando lo que le íbamos pidiendo y que ya llevábamos preparado.

3.2 Apartados descartados del proyecto

Los siguientes temas fueron propuestos por parte del cliente, pero tras un estudio de todos los temas a tratar, finalmente se acordó con el cliente enfocar el trabajo en los apartados anteriores. El motivo principal para esta decisión fue el tiempo (habría sido imposible abordar todos esos puntos en el tiempo asignado para el trabajo), pero asociado a este motivo estuvo nuestra decisión personal de buscar un mayor grado de conocimiento en los apartados elegidos. Los temas descartados fueron los siguientes:

- Configuración técnica real de los componentes especificados y monitorización opcional.
- Implementación de los componentes especificados en la infraestructura actual (ya implementada).
- [Azure AD] Diseño de AD con grupos reales, OU's, etc.
- [Azure AD] Migración de local AD a Azure AD.
- [AIP] Implementación detallada real de etiquetas según los tipos de documentos.

4. Introducción

VRT ya contaba con muchas de las mejores prácticas para Active Directory, pero aun así, tenían mucho aspectos que mejorar en cuanto a sus configuraciones de seguridad. Lo que ya existía en su entorno, entre otras cosas, era el uso de un solo dominio, una estructura de unidad organizativa al igual que una estructura de organización y el uso del autoservicio para restablecer las contraseñas, entre otros aspectos.

A continuación se enumeran algunas prácticas importantes que aún no se habían implementado, junto con una breve explicación que la empresa nos proporcionó sobre los motivos por los que aun no tenía implementadas las siguientes medidas:

- Separar las cuentas de usuario de las cuentas de administrador.
    - Esta medida aún no se realizaba en Azure Active Directory, pero sí en el AD local. Esto debe cambiarse en la migración a Azure AD.
- Monitorización de eventos de AD.
    - Actualmente VRT ya monitoriza mucha información, pero esto aún no está configurado correctamente y necesitan monitorizar más componentes de los que están siendo registrados. Este documento contiene consejos sobre los distintos elementos que podrían monitorizarse.
- El uso de las herramientas del sistema se registra y se mantiene disponible durante 6 meses.
    - Éste es un elemento de BIO, no está claro si VRT está haciendo esto actualmente, por lo que deberían investigarlo y configurarlo para que permanezca durante 6 meses.

En cuanto a *Azure Information Protection (AIP)*, VRT aún no tenía nada implementado porque todavía no estaban protegiendo prácticamente ningún tipo de información. Es posible que nunca utilicen Azure Information Protection, ya que esta funcionalidad se migrará a Office365 Security & Compliance y pasará a llamarse Etiquetado Unificado. Es mejor comenzar a implementar el Etiquetado Unificado de inmediato en lugar de AIP para que no sea necesaria una migración eventual ni resulte una pérdida de tiempo por parte de la empresa.

Con Azure Information Protection es posible proteger documentos basados en etiquetas. Estas etiquetas también pueden tener un período de retención y el acceso puede basarse en las etiquetas. De esta forma los documentos están protegidos. Estas etiquetas deben ser tan detalladas como el tipo de documento para que se pueda aplicar una retención precisa al documento. Por ahora, las clasificaciones son amplias, como información médica, finanzas e información de IT. Dentro de esas categorías se encuentran diferentes tipos de documentos con sus propios requisitos de retención. Para especificar las etiquetas para este tipo de documentos se debe hacer una estrategia y las etiquetas deben basarse en un análisis de riesgo (según el BIO).

También es posible escanear correos electrónicos y detectar cuándo se envía un correo electrónico con datos confidenciales fuera de VRT. Para ello se pueden crear reglas que lo detecten y tomen las medidas correspondientes (bloquear, notificar, etc.). Alguna información que se debe verificar en las reglas es cuando hay más de tres números BSN en un correo electrónico o adjunto, direcciones IP y documentos etiquetados en consecuencia (adjuntos de correo electrónico).

Finalmente se investigaron de forma profunda los siguientes términos de Azure:

En cuanto a **Azure Active Directory**:

1. ¿Qué dice la BIO sobre el acceso y la administración de identidad?

2. ¿Qué dice la BIO sobre la administración de acceso privilegiado?

3. ¿Cuál es la situación actual? ¿Contexto? Globalmente

4. ¿Qué es Azure AD?

    a. ¿Qué se puede hacer con él?

    b. Opciones disponibles, como grupos y unidades organizativas,

5. ¿Diferencias entre AD y Azure AD?

6. ¿Cuáles son las mejores prácticas de Azure AD en general?

7. ¿Con qué aplicaciones está conectada la AAD de VRT? (los más importantes como SharePoint)

8. ¿Qué es PAM (también se relaciona con Azure AD)?

    a. ¿Cómo puede PAM beneficiar a VRT?

9. ¿Qué es la administración de acceso e identidad (también se relaciona con Azure AD)? ¿La gestión de identidades beneficia a VRT?

10. ¿Cómo implementar el acceso condicional dentro de Azure AD?

En cuanto a **Azure Information Protection:**

1. ¿Qué es Azure Information Protection?

2. ¿Qué dice la BIO sobre este tema?

3. ¿Cuáles son las mejores prácticas de AIP?

4. ¿Qué clasificaciones de datos deben ser usados?

5. ¿Qué configuraciones de seguridad se necesitan para las diferentes clasificaciones de datos?

Al final del proyecto se llevó a cabo una evaluación con el cliente para averiguar si los resultados del proyecto son los que pidió. En resumen, el cliente está contento con los resultados y dijo que es realmente útil. Lo único que faltaba era un resumen de la gestión con una lista de prácticas aún no implementadas para que pudiera tener una visión general de lo que debe hacerse.

5. Objetivos y metodología de trabajo

En este apartado se indican las metas a alcanzar y los resultados a los que la empresa quería que llegásemos. Por tanto, esta parte se divide en dos sub apartados, objetivos y metodología de trabajo que he seguido personalmente.

5.1 Objetivos

El objetivo de este proyecto es el de realizar un informe de asesoramiento para la empresa VRT basado en las distintas tecnologías existentes de Microsoft en cuanto a ciberseguridad.

Desde un principio, tanto el cliente como nosotros teníamos claro que el proyecto no debía expandirse demasiado, puesto que los componentes de seguridad dentro de la empresa eran muchos. Por lo tanto, el principal objetivo de este proyecto fue el de investigar y acordar varios componentes de seguridad sobre los que posteriormente centraríamos tanto nuestra investigación como nuestro informe de asesoramiento.

Todos los objetivos que se marcaron desde un principio con el cliente fueron, en primer lugar, ayudarles a desplegar una infraestructura SIEM que les ayudara a tener todos los datos de su empresa monitorizados y centralizados, en segundo lugar, revisar ciertos componentes que ya tenían monitorizados pero no con buenas prácticas ni tenían aun bien ordenados los datos. Y por último, nuestro principal objetivo ,desde un primer momento, fue el de investigar cómo empezar a monitorizar datos de dos elementos que tuvieran presentes en la empresa pero que aún no estuvieran controlando.

5.2 Metodología de trabajo

Las primeras cuatro semanas del proyecto fueron un poco confusas para el equipo, porque realmente no sabíamos lo que el cliente quería del proyecto. Entendimos que teníamos que investigar cómo funcionaba un SIEM de Azure y, en función de eso, crearíamos un asesoramiento para que ellos posteriormente pudieran desplegar un SIEM en su propio entorno y así tener controlado todo de forma más eficiente.

Debido a que el cliente no pudo brindarnos acceso al entorno, todo esto fue causado por la cuarentena del virus y que hubiera supuesto diversos problemas de seguridad, no pudimos crear una PoC (proof of concept) como en un principio pensábamos hacer.

También quedó muy claro que no podíamos crear un diseño para todo el SIEM ya que no sabíamos qué componentes de Azure debían monitorizarse. Esto tampoco estaba claro para el cliente. No sabíamos qué componentes estaban en la licencia de Azure. En su lugar, optamos por dar un consejo sobre dos segmentos de su entorno y cómo podrían mejorar su seguridad con las mejores prácticas que posteriormente fuimos recopilando, basándonos principalmente en documentos que pueden encontrarse en la web de Microsoft y ciertos repositorios de GitHub en los que también se detallan diversos procedimientos y buenas prácticas para algunas tecnologías de Microsoft.

Las últimas semanas se hizo más claro y fuimos progresando bien de cara a la fecha límite del proyecto. En general, hubiera sido mejor tener acceso a sus sistemas o estar en las instalaciones para poder crear una PoC funcional, también hubiera sido más fácil para nosotros el desenvolvernos con el entorno para así avanzar de manera más rápida y efectiva y no tener que

estar haciendo talleres con el cliente cada semana, de las cuales sólo solíamos disponer de una o dos horas a la semana.

Esto también habría ayudado en la cooperación dentro del equipo, ya que finalmente todo se hizo de forma online y sin mucha libertad dentro de los sistemas, nos tuvimos que ceñir a lo que ellos nos mostraban. Cabe destacar que ni ellos mismos muchas veces tenían idea de las configuraciones que se hicieron dentro de su entorno y que en ocasiones tenían que llamar a los ingenieros que programaron y configuraron los distintos parámetros de seguridad de cada uno de los componentes existentes dentro de la empresa VRT.

6. Resultados y evaluación

Este es el informe de asesoramiento, que se compone principalmente de consejos (best practices) sobre Azure Active Directory (Azure AD) y Azure Information Protection (AIP). También contiene algunos consejos para el despliegue de una infraestructura SIEM que es el objetivo final de VRT, además de una evaluación final de los resultados por parte del cliente.

Este documento contiene los siguientes sub apartados, que se irán explicando con mayor profundidad:

- Consejos para Azure Active Directory
- Consejos para Azure Information Protection
- Consejos para SIEM
- Evaluación

Este documento tiene el fin de ser utilizado por VRT en la implementación de los componentes especificados y puede usarse en colaboración con un consultor de Microsoft.

Esto último es altamente aconsejable puesto que aquí reflejamos lo que el cliente quería realmente en un principio, pero el consultor puede aportar ideas más profundas, dado su grado de conocimiento en estas tecnologías, que puedan hacer cambiar de opinión a la empresa en cuanto a alguna implementación y/o configuración de alguno de los componentes que se describen más adelante.

6.1 Resultados

Este apartado se dividirá en dos sub apartados correspondientes con los resultados obtenidos mediante nuestra investigación sobre Azure AD y AIP para finalmente elaborar el informe de asesoramiento basado en estos componentes los cuales se detallan con mayor profundidad en los siguientes apartados, dedicados básicamente a introducir conceptos y a revisar las prácticas ya existentes para cada componente y buenas prácticas que deberían aun ponerse en marcha.

6.1.1 Consejos para Azure AD

Para crear consejos para la implementación de Azure Active Directory, realizamos una investigación con un enfoque en mostrar las mejores prácticas de seguridad. Hicimos una lista de verificación y revisamos la situación actual del cliente con él. Muchas de estas mejores prácticas ya se están utilizando y estos consejos se centraron en las prácticas que no se están llevando a cabo. La gestión de acceso privilegiado también fue un tema de investigación, pero se extiende a los otros temas del asesoramiento y, por lo tanto, no tiene un capítulo propio.

6.1.1.1 Azure AD en general

Este capítulo trata distintos consejos sobre cómo implementar Active Directory en Azure. Esto se basa en la situación actual de la empresa VRT.

6.1.1.1.1 Prácticas ya existentes

Las siguientes mejores / buenas prácticas de la lista de verificación ya están implementadas. Hay que tener en cuenta que esto cuenta principalmente para el AD local y aún debe hacerse para Azure AD.

- Utilice AGDLP para diseñar grupos (usuarios miembros del grupo global del dominio, grupo local del dominio como permisos para los recursos)
    - Ya implantado en VRT pero en el AD local
- Use un solo dominio

    - Ya en Azure AD
- Deshabilite la cuenta de administrador local o asegúrelos (MFA)
    - En uso en ordenadores/laptops
- Haga que los usuarios usen palabras para las contraseñas con un mínimo de 8 caracteres y que la complejidad sea muy buena
    - Política para esto ya aprobada pero aún no implementada
- Use nombres de grupo descriptivos (sea más fácil saber para qué se usan)
    - Ya en AD local
- Utilice DNS para bloquear dominios maliciosos
    - Ya se está haciendo para bloquear los dominios de correo
- El acceso a los recursos externos debe asegurarse con 2FA
    - Ya implementado para Azure AD
- Utilice las últimas funciones de seguridad de Azure y ADFS (contraseñas prohibidas, bloqueo de IP, MFA)
    - Esto se está haciendo activamente para mejorar la seguridad.
- Política y plan de incidentes y respuesta, procedimientos para incidentes, procedimientos para comunicarse con partes externas
    - Política implementada (violaciones de datos)
- Usar inicio de sesión único
    - Ya implementado para todos los componentes conectados de Azure
- Utilice el autoservicio para los usuarios que deseen restablecer su contraseña
    - Ya en práctica a través de un portal de usuarios

También existen múltiples mejores prácticas que VRT no ha implementado. Estas se tratarán en los siguientes apartados. (Microsoft, https://docs.microsoft.com, 2020)

6.1.1.1.2 Prácticas a implementar

Evalúe periódicamente las cuentas de administrador (privilegiadas) y limpie el grupo de administradores de dominio, mantenga un registro de ello

Esto es importante porque solo debe haber tantas cuentas de administrador (privilegiadas) como sea necesario para reducir el riesgo de compromiso. Esto debe comprobarse periódicamente y registrarse para mantener un control. Según BIO, esto debería suceder en cada cuartil (también para usuarios normales con privilegios más altos). El registro creado ofrece una descripción general de todas las cuentas privilegiadas y facilita la auditoría y el control. También aclara por qué un determinado usuario tiene una cuenta de administrador en el grupo de administradores de dominio o por qué tiene una cuenta privilegiada. Entonces, lo que aún queda por hacer es planificar una verificación de los usuarios privilegiados y el grupo de administradores en cada cuartil y mantener un registro de todos estos usuarios para mantener un control sobre ello.

Cuentas de usuario y administrador separadas para el personal de IT

Esto se debe a que, si una cuenta de usuario se ve comprometida, un pirata informático no tiene una cuenta de usuario privilegiada. Para privilegios más altos se debe usar una cuenta de administrador separada. Actualmente, VRT aplica esto en el AD local pero no en Azure AD. En la situación actual de Azure AD se está utilizando una cuenta de usuario como cuenta de administrador, y debe estar separada como en el AD local.

Habilite la auditoría de equipos (política de grupo) en el dominio para análisis de seguridad

Esto se debe a que puede analizar el registro del ordenador en caso de compromiso y para su uso en un SIEM. Actualmente, los ordenadores portátiles no están en el dominio de Azure AD, pero deberían estarlo y, según VRT, eventualmente lo estarán (todavía en el proceso de cambio a portátiles). Además, la auditoría local debe habilitarse a través de una política de grupo para todos los portátiles / ordenadores.

Monitorizar eventos de AD para detectar señales de compromiso (monitorización de seguridad) | Utilice Azure Identity Protection para la supervisión de Azure AD

Actualmente no se está realizando en VRT. Esto se hace mejor a través de un SIEM donde toda la información estaría disponible en un lugar centralizado. Esto se realiza para detectar compromisos en AD de forma rápida para que se pueda actuar a tiempo. En Azure AD, esta supervisión ya está implementada (activada), puede ver cada inicio de sesión desde cada aplicación / dispositivo. Esto debe monitorizarse activamente y para toda la monitorización en un lugar central, se puede utilizar Azure Sentinel. Debe revisarse al menos una vez a la semana. Busque / revise las siguientes cosas:

- Cambios en grupos privilegiados como el grupo de administradores de dominio y administradores empresariales
- Intentos de contraseña incorrecta
- Cuentas bloqueadas
- Un inicio de sesión exitoso después de múltiples contraseñas incorrectas
- Intentos de inicio de sesión de una cuenta anónima
- Inicios de sesión exitosos en la red del sistema y / o usuario INVITADO (cuenta de ordenador local)
- Registro de eventos de borrado (un pirata informático puede hacer esto para intentar cubrir sus huellas)
- Bloqueos de cuentas
- Software antivirus desactivado (solo para ordenadores)
- Todas las actividades realizadas por cuentas privilegiadas
- Eventos de inicio / cierre de sesión
- El uso de cuentas de administrador local (solo para ordenadores)

Limpiar cuentas antiguas de usuarios y ordenadores de AD

Debe haber un procedimiento para limpiar las cuentas antiguas de usuarios y ordenadores de AD. Esto debería ser parte de una auditoría regular (como una anual). Esto se realiza para mantener organizado su entorno de AD y contendrá menos objetivos para los piratas informáticos (en el caso de las cuentas de usuario). Cada cuenta debe estar conectada a un usuario o servicio, y también es necesaria para que ese servicio funcione. De lo contrario, la cuenta no tiene uso y debe eliminarse.

Supervise los servicios DNS y DHCP para detectar amenazas de la seguridad

La supervisión de DHCP cuando se usa Azure AD puede no ser relevante porque la realizará la red local de los usuarios. El DNS aún debe supervisarse si se usa este DNS de Azure AD. Esto puede ayudar con el análisis de seguridad de la red, ya que registra las solicitudes que un pirata informático podría haber realizado desde dentro de una red. Además, esta monitorización debe estar disponible en un SIEM como un lugar central para la información relacionada con la seguridad.

El DNS de Azure AD debe usarse como servidor DNS para todos los equipos de VRT. Azure AD DNS registrará todas las búsquedas de DNS y esto se puede usar para detectar dominios maliciosos y bloquearlos. Para aprovechar esto al máximo, la información debe estar disponible en una ubicación central con el resto de los datos de seguridad (en un SIEM). Los datos se pueden visualizar de una manera más significativa / práctica. De esta forma, una verificación de seguridad no llevará mucho tiempo y es menos probable que se olviden las verificaciones de componentes específicos (como DNS).

Utilice Office365 Secure Score para comprobar si está configurado correctamente (implementación en relación con la seguridad)

Esto se puede usar para verificar si Office365 está configurado de acuerdo con las mejores prácticas de Microsoft. Obtiene una puntuación basada en la configuración de las funciones de seguridad y la realización de tareas relacionadas con la seguridad. La puntuación es una determinada cantidad de puntos por acción de mejora. También puede basarse en un artículo parcialmente configurado. La puntuación segura no sólo se usa para Office365, sino también para Azure AD, Microsoft Defender ATP, Azure ATP y Cloud App Security. Es altamente aconsejable usar esto para Azure AD.

Derechos de acceso a documentos con grupos (grupos / roles con privilegios)

Todos los derechos / privilegios de acceso deben otorgarse a través de grupos (grupos locales de dominio) y deben documentarse. Esto significa escribir los derechos otorgados, el grupo y por qué necesitan estos derechos. Esto debería usarse para evaluar y limpiar los derechos de acceso en general.

Utilice un punto de referencia de endurecimiento y compruébelo regularmente

Un punto de referencia de refuerzo le indica todos los pasos técnicos que debe seguir para mejorar la seguridad en el entorno más seguro. Esto será de gran ayuda para proteger técnicamente el entorno de Azure AD. Este punto de referencia debe volver a comprobarse cuando se actualice y será una buena práctica comprobarlo anualmente.

Centralice la administración de identidades (solo una instancia de Azure AD, sin AD local)

Esto ya está aplicándose, pero aún se remarcará debido a la transición en curso de AD local a Azure AD. VRT utiliza un entorno IAM donde se administran todos los usuarios. Los derechos se seguirán realizando a través de AD y las cuentas de administrador también están solo en AD como debería ser, y el AD local debe eliminarse gradualmente para que solo quede Azure AD. (activedirectorypro, 2020) (Microsoft, https://docs.microsoft.com, Julio)

6.1.1.2 Privileged Access Management (PAM)

Con el fin de minimizar la superficie de ataque de los piratas informáticos tenemos la posibilidad de utilizar PAM lo cual es una excelente manera de garantizar las buenas prácticas al acceder a ciertos recursos en una red. PAM consta de soluciones que ayudan a proteger, controlar, administrar y monitorizar el acceso privilegiado a recursos críticos.

6.1.1.2.1 Prácticas ya existentes

Las siguientes prácticas ya están implementadas / parcialmente implementadas:

- No se permite compartir cuentas de administrador
    - Ya es parte de la política
- Minimizar la cantidad de cuentas privilegiadas personales

    - En su lugar, la política es no tener cuentas privilegiadas personales
- Analizar el riesgo de cada usuario privilegiado
    - Sin cuentas de usuario privilegiadas, analizan los riesgos de las cuentas de servicio privilegiadas.

6.1.1.2.2 Prácticas a implementar

Las siguientes prácticas no están implementadas todavía:

- Supervisar y registrar toda la actividad privilegiada
    - No se hace lo suficiente, hay registro, pero no monitorización activa
- Educar a los usuarios sobre buenas prácticas en materia de seguridad
    - Han dado pequeños pasos, han elaborado un plan de comunicación y han diseñado un módulo de aprendizaje electrónico con este fin para cada empleado
- Documentar las políticas y prácticas de gestión de cuentas
    - Igual que el punto anterior
- Proporcione privilegios adicionales según el tiempo, elimine automáticamente los privilegios después de un período de tiempo (también forma parte de la administración de acceso privilegiado (PAM))
    - Tienen umbrales (90 días), cumplen esta regla
- Cuando use cuentas de servicio, ciérrelas, asigne sólo los derechos necesarios que deba tener cada cuenta y no configure las contraseñas habilitando la opción que hace que nunca caduquen (es recomendable cambiarlas frecuentemente)
    - Procedimiento llevándose a cabo

(securityboulevard, 2020)

Supervisar y registrar toda la actividad privilegiada

Monitorizar y registrar cuentas privilegiadas en la red puede ser vital para reconocer cuándo ocurre algo anormal con respecto al acceso a los datos. Monitorizar activamente los inicios de sesión, por ejemplo, puede ser una forma útil de darse cuenta cuando ciertos usuarios están accediendo a recursos a los que de otra manera no deberían acceder. El registro debe consistir en acciones realizadas por cuentas de administrador, administración de bases de datos o cambios en AD (usuarios y similares), deshabilitación de servicios en servidores, etc. Lo más importante es saber cuándo se agrega un usuario a un grupo privilegiado. La supervisión también debe comprobar si hay inicios de sesión incorrectos con una cuenta con muchos privilegios. Al configurar un panel de control y definir un conjunto de reglas que indiquen cuándo ciertos recursos a los que nadie debería acceder (por ejemplo), puede ver y reaccionar fácilmente ante estas situaciones. Otra opción que puede ayudar es habilitar una notificación por correo electrónico para que cuando ocurra algo anormal, la persona responsable sea notificada directamente sobre el evento.

Educar a los usuarios sobre buenas prácticas en materia de seguridad.

Los usuarios son el tipo de vulnerabilidad número uno, por lo tanto, es imperativo que los usuarios sepan cómo operar ciertos programas y tengan un buen conocimiento sobre los riesgos de usar estos programas. Cuando se habla de buenas prácticas, hay algunos ejemplos como: no hacer una reutilización de contraseñas, no establecer contraseñas comunes (welcome1234, etc.) pero también una política de escritorio limpio, no dejar contraseñas en papel escritas y a la vista. Otra buena práctica es bloquear su ordenador mientras no está en la estación de trabajo.

Documentar las políticas y prácticas de gestión de cuentas

Documentar las políticas y prácticas de administración de cuentas es una buena manera de hacer un inventario de las políticas y prácticas que utiliza VRT actualmente. Al documentar estas políticas y prácticas, todos tienen más claro lo que deben hacer y lo que no deben hacer. Esta documentación se puede crear en un documento de Word o en una hoja de Excel. Esto también se puede utilizar como referencia para nuevos empleados.

Proporcione privilegios adicionales según el tiempo, elimine automáticamente los privilegios después de un período de tiempo

Si un determinado usuario tiene que acceder a ciertos recursos que necesitan privilegios elevados, no se le deben otorgar estos privilegios para siempre. Para mayor seguridad, estos privilegios deben asignarse al usuario por un período de tiempo limitado. Por ejemplo, al realizar actualizaciones para un determinado servidor, la cuenta de usuario debe tener privilegios de administrador durante el tiempo que sea necesario para que el administrador opere el sistema. Una vez realizado todo el trabajo en el (los) sistema (s), los privilegios se eliminan nuevamente. Este tipo de privilegio basado en el tiempo protege la red porque ciertos usuarios no tendrán privilegios de administrador cuando no los necesiten.

Cuando use cuentas de servicio, ciérrelas establecer solo los derechos necesarios y no configure la contraseña para que no caduque nunca

A veces, no puede o no quiere usar una cuenta personal para ciertas tareas en un sistema. Para fines de automatización, se utilizan las llamadas cuentas de servicio, estas cuentas no tienen una persona que las utilice. Estas cuentas se ejecutan en sistemas que necesitan realizar tareas automatizadas y, por lo tanto, la mayoría de las veces funcionan las 24 horas del día, los 7 días de la semana, porque estas cuentas no son operadas por un humano y son muy específicas en el tipo de tareas que deben realizar. Puede bloquear fácilmente los permisos que se necesitan para que un programa se ejecute en esa cuenta. Pero debido a que no hay ninguna persona que la use, la contraseña debe cambiarse de vez en cuando (cada mes, por ejemplo) para mantener la cuenta lo suficientemente segura para que pueda volver a usarse. (thycotic, 2020) (microsoft, 2020)

6.1.1.3 Acceso condicional

Al utilizar el acceso condicional, puede tomar decisiones basadas en señales y hacer cumplir las políticas de la organización. Considere el acceso condicional como simples declaraciones if-else: si un usuario desea acceder a un determinado recurso, entonces debe completar una determinada acción para verificarlo. A continuación, se muestran las mejores prácticas que ya se utilizan y las que no se utilizan:

6.1.1.3.1 Prácticas ya existentes

Las siguientes prácticas ya están implementadas / parcialmente implementadas:

- No incluya administradores cuando agregue una nueva política que no esté destinada a ellos para que aún puedan cambiarla
- No use las opciones "bloquear" y "todas las aplicaciones" en una sola política
- Cree una cuenta de usuario dedicada a la administración de políticas y excluida de todas sus políticas
- No confíe en un único control de acceso

6.1.1.3.2 Prácticas a implementar

Las siguientes prácticas no están implementadas (todavía):

- Pruebe nuevas políticas con grupos pequeños antes de aplicarlas a todos los usuarios
- Aplicar políticas de CA a todas las aplicaciones
- Asegúrese de que cada aplicación tenga aplicada al menos una política de acceso condicional
- Minimice la cantidad de políticas de CA (no una por aplicación)
- Analice sus aplicaciones y agrúpelas en aplicaciones que tengan los mismos requisitos de recursos para los mismos usuarios.
- Configurar cuentas de acceso de emergencia
- Habilitar políticas en el modo de solo informe
- Excluya los países de los que nunca esperará un inicio de sesión
- Use controles personalizados para redirigir a los usuarios a un servicio compatible para satisfacer los requisitos de autenticación fuera de Azure AD

(Microsoft, https://docs.microsoft.com, 2020)

Pruebe nuevas políticas con grupos pequeños antes de aplicarlas a todos los usuarios

Para asegurarse de que las nuevas políticas no rompan las políticas existentes y para asegurarse de que las nuevas políticas realmente funcionen, aplíquelas primero a un pequeño número de usuarios. En caso de que algo no esté configurado correctamente, el impacto del cambio será significativamente menor que cuando aplica estas políticas a una gran cantidad de usuarios.

Minimice la cantidad de políticas de CA (no una por aplicación)

La creación de varias políticas lo hace más claro en lugar de poner todas las políticas en una. Esto le da más control sobre el acceso.

Analice sus aplicaciones y agrúpelas en aplicaciones que tengan los mismos requisitos de recursos para los mismos usuarios.

Categorice los grupos que usan los mismos recursos y son usados por los mismos usuarios, de esta manera usted crea una lista más clara de políticas que se aplican a más de una sola aplicación.

Configurar cuentas de acceso de emergencia

Mitigue el impacto del bloqueo accidental del administrador creando dos o más cuentas de acceso de emergencia en su organización. En el caso de que algo salga mal, no se le bloqueará y puede utilizar una de las políticas para recuperar el control sobre las políticas de CA.

Habilitar políticas en el modo de solo informe

Para evaluar el impacto de su política (conocer los usuarios y los nombres afectados por ella). Una vez que guarde la política en el modo de solo informe, puede ver el impacto en los inicios de sesión en tiempo real en los registros de inicio de sesión. (Microsoft, docs.microsoft.com, 2020)

Excluir países de los que nunca esperará un inicio de sesión

No hay ninguna razón para aceptar inicios de sesión desde ubicaciones en las que no hay personas trabajando, por lo que excluir estos países / ubicaciones bloqueará los inicios de sesión desde esos lugares. Se reduce el riesgo de sufrir ataques.

Use controles personalizados para redirigir a los usuarios a un servicio compatible para satisfacer los requisitos de autenticación fuera de Azure AD

Los controles personalizados redirigen a los usuarios a un servicio compatible para satisfacer los requisitos de autenticación fuera de Azure AD. Esto significa que puede utilizar un método de autenticación que no dependa de Azure. (Microsoft, docs.microsoft.com, 2020)

6.1.1.4 Baseline Informatiebeveiliging Overheid (BIO)

Esta parte hace referencia a la BIO con respecto a IAM (Identity & Access Management). IAM es el nombre colectivo de todo lo relacionado con cuentas de usuario (y grupos) y permisos de acceso. Algo que toda organización tiene. El BIO (Baseline Informatiebeveiliging Overheid) es una norma de seguridad que todas las organizaciones gubernamentales (como VRT) deben cumplir. Se puede comparar con la norma ISO / NEN 27001/2. Contiene pautas de seguridad que deben implementarse para garantizar la seguridad de la información. Una parte de estas pautas también se refiere al uso de cuentas y grupos, que están vinculados a Azure Active Directory. En este capítulo se tratan las pautas que se aplican a Azure Active Directory.

6.1.1.4.1 Prácticas ya existentes

VRT ya tiene desplegados la mayoría de estos elementos. Estos elementos se encuentran en la siguiente lista:

- Existe un procedimiento formal para registrar y eliminar cuentas con los derechos de acceso correctos
- No se utilizan cuentas de grupo (cuentas compartidas)
- El acceso a los sistemas de información está autorizado por un funcionario autorizado
- Los derechos se pueden otorgar en función de las funciones de las personas (y están registrados)
- Los propietarios de los recursos de la empresa deben verificar los derechos de acceso de los usuarios con regularidad, al menos una vez al año
- Todos los derechos sobre los recursos se eliminan cuando un usuario finaliza su contrato y deja de trabajar para la organización
- Se utiliza la autenticación de 2 factores al conectarse desde zonas que no son de confianza
- Requisitos de contraseña (mínimo de 8 caracteres, caracteres especiales, etc.)
- Solo el personal autorizado tiene acceso a las herramientas del sistema
- El acceso al código fuente de la aplicación está restringido

6.1.1.4.2 Practicas a implementar

Estos elementos aún deben implementarse para cumplir con la BIO con respecto a la gestión de identidad y acceso.

Con base en un análisis de riesgo se determinará qué funciones obtendrán qué derechos de acceso (separación de derechos de función)

Actualmente, los derechos de acceso se basan en funciones en VRT, pero esto no se realiza mediante un análisis de riesgo. Los riesgos deben identificarse en función del acceso que se

necesita y, a través de esos riesgos, debe determinarse si esas funciones en particular deben tener esos derechos de acceso.

Los derechos de acceso especiales se controlan y restringen + se comprueban en cada cuartil

Para VRT ya se están controlando y restringiendo los derechos de acceso especiales, pero no se verifican en cada cuartil. Esto aún debería agregarse. Esta es una evaluación sobre si las cuentas aún necesitan esos derechos y, si no los necesitan, pueden eliminarse para hacer que el entorno sea más seguro.

Se toman medidas para aislar información con interés específico

Para VRT, esto está en manos de los usuarios, los propietarios de los documentos / información. Esto no es parte de una política. La información importante de las bases de datos debe estar protegida y solo debe ser accesible a través de los medios adecuados (una aplicación específica). Los documentos deben clasificarse y, según esas clasificaciones, deben protegerse. Esto es parte de Azure Information Protection.

Los usuarios solo pueden ver la información necesaria para practicar su función

VRT sabe que esto es necesario, pero aún no lo ha hecho. Primero necesitan la clasificación de datos y esto se hará a través de Azure Information Protection. Es importante que el personal solo pueda ver la información necesaria para hacer su trabajo y no más, esto hace que el entorno sea más seguro ya que hay menos puntos de acceso a la información (cuentas que tienen acceso).

El acceso a la información de proveedores externos se basa en el análisis de riesgos y está registrado

Actualmente, esto no está siendo registrado, pero se basa en un análisis de riesgo. El siguiente paso es mantener un registro sobre qué proveedor tiene acceso a qué información. Esto ya podría conocerse a través del análisis de riesgos y también debe mantenerse registrado y actualizado.

El uso de las herramientas del sistema se registra y se mantiene disponible durante 6 meses

Esto se está registrando, pero es posible que no se guarde durante seis meses según VRT. Esto debe comprobarse y configurarse. Esto ayudará en el análisis de seguridad cuando se infrinja una cuenta privilegiada con acceso a las herramientas del sistema porque luego se puede ver lo que ha hecho la cuenta. Con las herramientas del sistema se entienden cosas como Active Directory y herramientas de administración de computadoras. En una hoja de Excel entregada por VRT sobre tipos de datos y retención, se menciona el período de 6 meses para el registro informático, por lo que ya se conoce. (informatiebeveiligingsdienst, 2020)

6.1.1.5 Implementación

Es mucho implementar todos los elementos que se enumeran anteriormente. Es mejor tener todo en mente (también lo que ya está implementado) al realizar la migración completa a Azure AD desde el AD local. Por supuesto, las buenas prácticas de seguridad que ya existen para el AD local deben copiarse en Azure AD.

Es mejor verificar todos los elementos que aún no están en su lugar y hacer una lista de lo que es fácil de hacer y lo que no. Primero debe hacer los elementos fáciles y luego continuar con los elementos más difíciles. De esa manera, ya puede tener muchas de las prácticas implementadas

de primera mano. Podría ser mejor usar esta lista en una conversación con un consultor de Microsoft, ya que el cliente dijo que se usaría como una lista que se utilizará después para un consultor de Microsoft.

6.1.2 Consejos para AIP

Para crear un asesoramiento para la implementación de Azure Information Protection, realicé una investigación basada en las mejores prácticas relacionadas con la seguridad e investigué escenarios comunes que podrían ocurrir en la empresa. Compuse una lista de verificación y se revisó la situación actual con el cliente. También voy a exponer varios escenarios y explicar cómo mejorar la protección de datos, proporcionar clasificación de datos e información específica que podría ser importante de monitorizar dentro de la empresa.

6.1.2.1 Protección de datos

El servicio de protección de datos usa Azure Rights Management (Azure RMS). Proporciona políticas de encriptación, identidad y autorización. La protección permanece con los documentos y correos electrónicos independientemente de la ubicación, red, servidor o aplicación. Las reglas de acceso se pueden aplicar a documentos y correos electrónicos, como evitar que se impriman y evitar que se reenvíen correos electrónicos, entre otras funciones.

La configuración de protección puede ser parte de la configuración de las etiquetas, por lo que se puede clasificar y proteger documentos o correos electrónicos aplicando una etiqueta. Cuando se crea una etiqueta que incluye la configuración de protección para AIP, se crea una plantilla de administración de derechos (plantilla RMS) y luego se puede usar con aplicaciones y servicios que admitan Azure Rights Management. (Microsoft, docs.microsoft.com, 2020)

6.1.2.1.1 Mejores prácticas

Si se requiriera una integración de correo electrónico adicional, sería mejor migrar desde la medida actual de la empresa tomada a través de una configuración en Office que los encripta, y usar Azure Information Protection con Exchange Online, con el cual puede enviar correos electrónicos protegidos a los usuarios y ellos pueden leerlos en cualquier dispositivo. Dado que ya está integrado con Exchange Online, será más fácil de controlar. (Microsoft, docs.microsoft.com, 2020)

Una vez que las etiquetas específicas se hayan establecido finalmente, para facilitar a los usuarios la selección de etiquetas para una correcta clasificación, es mejor instalar el cliente de etiquetado unificado AIP. Esto instala la barra de protección de la información en las aplicaciones de Office y los usuarios pueden elegir fácilmente la etiqueta correcta de acuerdo con cada documento, haciéndoles mucho más fácil y rápido el trabajo. (Microsoft, docs.microsoft.com, 2020)

6.1.2.1.2 Ajustes de protección recomendados

Al configurar una etiqueta para la configuración de protección, en el panel Protección, seleccione Azure (clave de nube) en lugar de HYOK (AD RMS). Una vez hecho esto, haga clic en el cuadro desplegable y seleccione la plantilla que desea usar para proteger documentos y correos electrónicos con esta etiqueta. Esta solución es mejor ya que no se requiere una infraestructura de servidor (menor coste y más rápido) y facilita compartir recursos con socios y usuarios de otras organizaciones mediante el uso de autenticación basada en la nube. También proporciona un seguimiento de documentos, una revocación y una notificación por correo electrónico de los documentos confidenciales que se comparten, pudiendo así tomar medidas a tiempo en el caso de que sea necesario.

Con respecto a los “Vencimientos del contenido del archivo”, se recomienda configurarlos con la opción “El contenido nunca caduca” (a menos que el contenido tenga un requisito de tiempo específico). Esto se utiliza para definir una fecha o un número de días en el que estarán protegidos los documentos.

Con respecto a “Permitir el acceso sin conexión”, podemos dividir los posibles escenarios en dos diferentes:

Primer escenario: Cantidad de días que el contenido está disponible sin conexión a Internet = **7** para datos comerciales **SENSIBLES** que podrían causar daños a la empresa si se comparten con personas no autorizadas.

Segundo escenario: Número de días que el contenido está disponible sin conexión a Internet = **NUNCA** para datos comerciales **MUY SENSIBLES** que causarían graves daños a la empresa si se compartieran con personas no autorizadas. (github, https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-protection.md, 2020)

6.1.2.1.3 Escenarios comunes e instrucciones relacionadas

Cuando se desee facilitar a los usuarios la protección de sus correos electrónicos que contengan información confidencial, es mejor configurar una etiqueta para que los usuarios protejan fácilmente los correos electrónicos con información que no debe ser compartida con personas no autorizadas. Cuando se desee facilitar a los usuarios la colaboración en un documento protegido, es preferible configurar la colaboración segura de documentos mediante Azure Information Protection.

Para proteger automáticamente los correos electrónicos de los usuarios enviados fuera de la organización, se deben configurar reglas de flujo de correo para las etiquetas de Azure Information Protection. Para clasificar y proteger automáticamente los almacenes de datos locales existentes, es importante implementar el escáner Azure Information Protection, ya que ayuda a descubrir datos confidenciales dentro de los documentos existentes que la empresa aún tiene almacenados localmente y no en la nube.

6.1.2.2 Etiquetado Unificado

A principios de este año, Microsoft anunció que eliminará gradualmente el servicio clásico Azure Information Protection. La eliminación gradual de Azure Information Protection comenzará el 31 de marzo de 2021. Se requerirá la aplicación de Unified Labeling (Etiquetado Unificado) en Office 365. Con el cliente de etiquetado unificado de Azure Information Protection, los administradores pueden proteger los correos electrónicos y documentos de la organización. Con Unified Labeling, VRT tendrá en un lugar centralizado la administración de las etiquetas de confidencialidad que ayudarán a proteger y clasificar los datos confidenciales.

El etiquetado unificado es una solución para que las organizaciones trasladen la política de seguridad de la información a configuraciones técnicas. Esto ayudará a VRT a proteger los datos confidenciales que actualmente tienen en la nube. Los empleados pueden aplicar etiquetas de clasificación y políticas de seguridad en correos electrónicos y documentos. Esto encripta la información confidencial para que sea accesible solo para el personal autorizado, independientemente de dónde se encuentren estos datos.

Con el complemento Azure Information Protection dentro de la suite de Office, los empleados tienen la barra de clasificación a mano para aplicar etiquetas de clasificación en sus documentos.

Las etiquetas de confidencialidad en Office 365 Security and Compliance son ahora las etiquetas de clasificación que permiten una integración más amplia de Microsoft Information Protection. Con este concepto de etiquetado unificado, las opciones de clasificación y protección de datos también son posibles para MacOS, iOS y Android. Las etiquetas de clasificación no solo afectan a los documentos y correos electrónicos, sino también al uso de SharePoint Online y Microsoft Teams. (GITHUB, 2020)

VRT no utiliza ninguno de estos conceptos, por lo que no tendrán que migrar del cliente clásico al cliente de etiquetado unificado. La suscripción a Azure Information Protection se obtuvo después de junio de 2019, por lo que se transferirá a Unified Labeling automáticamente y no se requiere ninguna acción en esa parte por VRT.

6.1.2.2.1 AIP frente al etiquetado unificado (cliente)

Para VRT, el consejo sería comenzar con el etiquetado unificado porque aún no se ha configurado ninguna clasificación o etiquetado. No se recomendaría configurar el cliente clásico porque VRT tendrá que migrar la configuración a Unified Labeling antes de marzo de 2021. Esto significa que se perdería todo el tiempo y la inversión.

Microsoft aconseja utilizar la plataforma de etiquetado unificado cuando su suscripción se obtuvo después de junio de 2009 y aún no se ha implementado nada. En este punto, la mayoría de las organizaciones deberían ejecutar el cliente de etiquetado unificado de forma predeterminada según Microsoft.

6.1.2.2.2 Estrategia de despliegue

En primer lugar, cuando se utilice la plataforma de etiquetado unificada, no será necesario realizar ninguna otra acción porque se configurará automáticamente. Microsoft tiene una configuración de política predeterminada con etiquetas preconfiguradas. Cuando se implemente la plataforma de etiquetado unificada, todas las configuraciones de políticas, etiquetas y funcionalidades adicionales se pueden configurar a través del Centro de administración de Microsoft.

Fase 1 (planificación)

Revise lo siguiente para garantizar un entorno seguro:

- Cómo funcionan las etiquetas de confidencialidad en la aplicación de Office (etiquetado integrado y cliente de etiquetado unificado).
- Para compartir secretos u otra propiedad intelectual, use las sub-etiquetas AIP en una política de alcance para datos altamente regulados que encripta el contenido y restringe el acceso a grupos específicos.
- Implemente políticas de DLP para evitar que los usuarios compartan accidentalmente datos confidenciales.
- Implemente Windows Information Protection para protegerse contra la fuga de datos.
- Implemente Cloud App Security para mapear el entorno de la nube y monitorizar y detectar eventos e incidentes de seguridad.
- Se recomienda revisar el blog del cliente de etiquetado AIP antes de utilizar el cliente de etiquetado unificado.
- Confirme que VRT tiene una suscripción que incluye la funcionalidad y las características.

Refleje lo anterior en la comunicación del usuario final antes de implementar y publicar la política de etiquetado unificado.

El escáner de protección AIP y las etiquetas unificadas de soporte de análisis se administran desde la hoja AIP en el Portal de Azure. Las actividades de auditoría analítica que se generan solo se pueden utilizar con el cliente AIP.

Fase 2: plan para proteger los datos

Actualmente VRT no tiene nada configurado en clasificación, políticas o etiquetas. Por lo tanto, no es necesaria la migración del etiquetado clásico al etiquetado unificado. La migración de servicios no significa migrar de etiquetas clásicas a etiquetado unificado, sino administrar etiquetas y políticas en la hoja de Azure Information Protection. Para activar el etiquetado unificado, el primer paso a seguir es activar el etiquetado unificado en Azure Information Protection Portal.

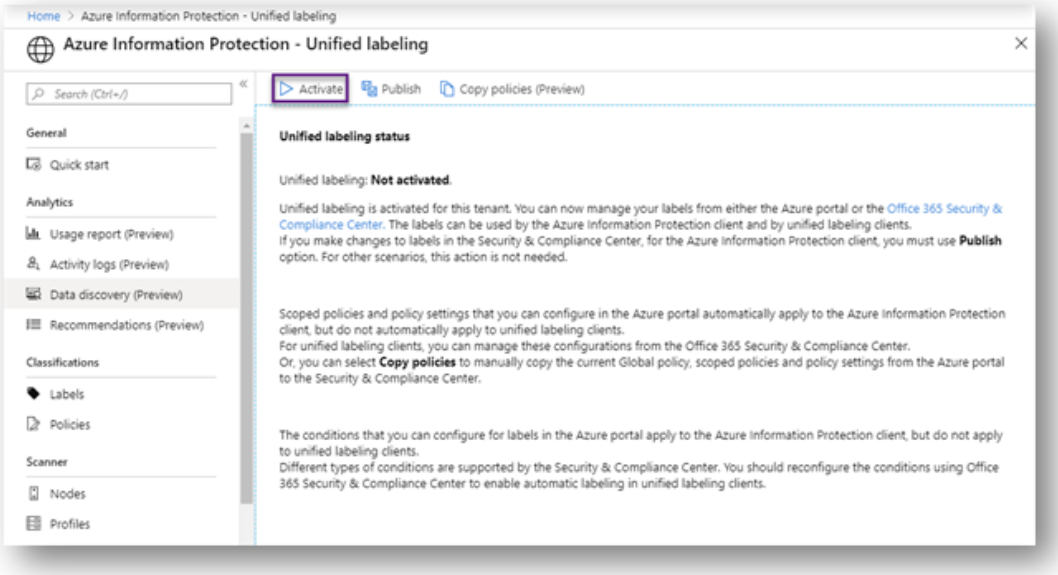

Figura 2: Habilitando el etiquetado unificado (unified labeling)

El primer paso después de habilitar el etiquetado unificado es decidir qué datos clasificar, proteger y monitorizar en Office 356 y otras aplicaciones SaaS.

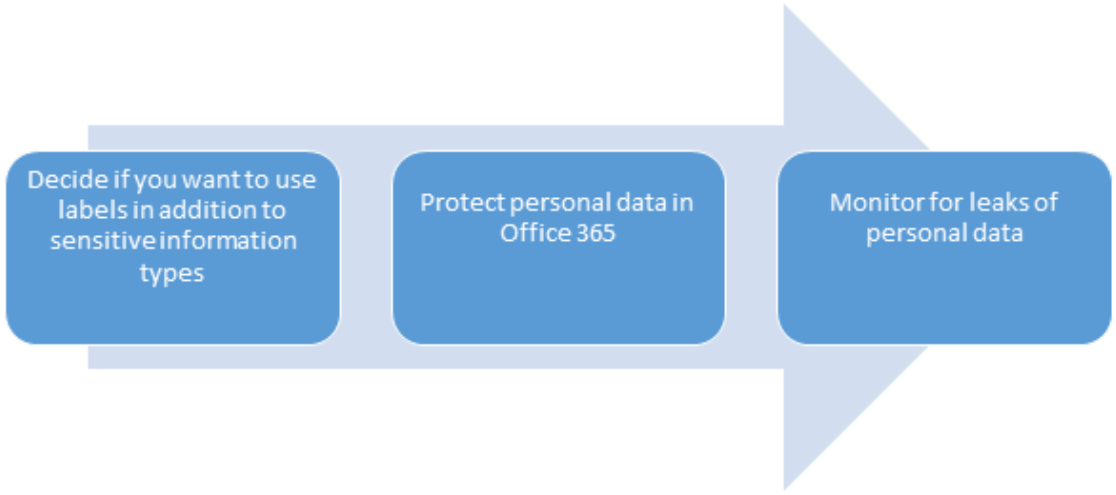

Figura 3: Paso 2. Etiquetado unificado

El segundo paso es opcional, pero para VRT es recomendable encontrar datos personales que deban protegerse. La herramienta de exhibición de documentos electrónicos de búsqueda de contenido en el centro de cumplimiento buscará en buzones de correo de Exchange, carpetas públicas, SharePoint, OneDrive, conversaciones de Skype, equipos y grupos de Yammer.

Figura 4: Búsqueda de contenido

VRT también puede utilizar la guía de inicio rápido del escáner de Microsoft para descubrir información confidencial. La información que encuentra el escáner ayuda con la clasificación y proporciona información sobre qué etiquetas se necesitan y qué archivos necesitan protección.

Debido a que este método no requiere configurar etiquetas o definir la taxonomía de clasificación, ejecutar el escáner es adecuado para VRT porque se encuentran en una etapa muy temprana de implementación. Para los almacenes de datos locales, se debe utilizar el escáner AIP. Para los almacenes de datos en la nube, se debe usar Azure Cloud App Security.

El tercer paso para proteger los datos mediante el etiquetado unificado es desarrollar, personalizar y crear etiquetas que ayuden a proteger los datos;

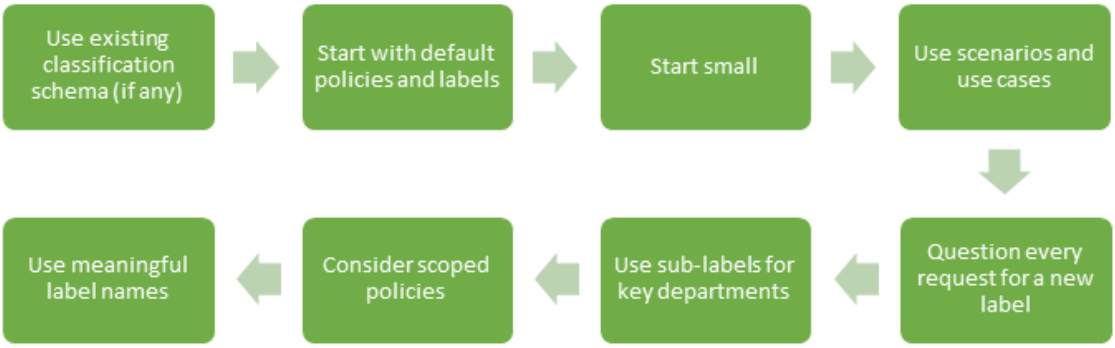

Figura 5: Desarrollo, personalización y creación de etiquetas

Para crear una estrategia de clasificación para VRT, pueden personalizarla para cumplir con los requisitos comerciales. Utilice la política AIP predeterminada para decidir qué etiquetas de clasificación asignar para los datos de VRT. Eche un vistazo al capítulo 2.3 para comenzar con las etiquetas (categorías amplias).

FASE 3: Configurar e implementar clasificación y etiquetado

El último paso es verificar que los usuarios finales obtengan las políticas y etiquetas de etiquetado. Para la mayoría de los usuarios, Azure Information Protection debe implementarse porque cumple con los requisitos comerciales de VRT.

Para estos usuarios, las mismas etiquetas se publicarán en Windows, Mac, iOS y Android. Los administradores pueden gestionar las etiquetas y la configuración de políticas en el centro de gestión.

Los almacenes de datos locales con documentos que tienen información confidencial, los documentos clasificados o protegidos deben escanearse para su etiquetado.

El cliente se puede implementar mediante un ejecutable o un archivo de Windows Installer.

6.1.2.3 Clasificación de datos

Este apartado contiene las clasificaciones de datos. Se trata principalmente de categorías amplias. Clasificaciones de datos (etiquetas).

En AIP es posible definir etiquetas que se pueden conectar a un documento. Para esta etiqueta, se puede definir el acceso (restricciones). Esto sirve para tener el control del acceso a información específica. También agregamos el tipo de datos, si es privado para la organización, es información pública o está restringida a equipos específicos dentro de la organización. Las categorías son las siguientes:

- Información comercial (cosas como planificación)
  - Datos privados
- Finanzas
  - Datos privados
- Gobernanza (políticas)
  - Datos privados
- Datos personales empleados (contratos de trabajo, administración de sueldos, etc.)
  - Datos restringidos
- Empleados de datos médicos
  - Datos restringidos

- Legal (contratos)
    - Datos privados
- Datos de infraestructura de TI (direcciones IP, nombres de computadoras, registro, etc.)
    - Datos privados

Lo anterior se basa en una hoja de Excel que entregó VRT que contiene diferentes tipos de datos y retención. Más adelante se añaden algunas adiciones a esto. Se agrega una etiqueta para información pública. Para este tipo de información no se necesita seguridad. Además, la información también puede ser para un equipo o departamento específico, es posible que no quieran que otros dentro de la organización tengan esta información. Para eso también debe haber etiquetas por equipo / departamento.

- Información pública
    - Datos públicos
- Cada equipo / departamento *
    - Datos restringidos

Se debe monitorizar la información que es privada para la organización o restringida a personal específico. Esto significa el uso de alertas cuando esta información se comparta fuera de VRT.

Debido a que los tipos específicos de información (o documentos) tienen diferentes períodos de retención, es mejor investigar qué tipos de documentos se pueden definir con sus propios períodos de retención. Las categorías anteriores son demasiado amplias para esto. Se puede hacer con la lista de Excel que se proporcionó por VRT. Con base en este tipo de documentos, se pueden hacer etiquetas con sus propios períodos de retención y además es posible restringir el acceso en función de esas etiquetas. De esta manera, ciertos tipos de información se pueden eliminar automáticamente después de la retención y solo pueden ser vistos por personal autorizado.

Las etiquetas que se utilizarán no necesariamente tienen que crearse en AIP y sería mejor crearlas en el Centro de cumplimiento y seguridad de Office365 (etiquetado unificado), ya que el etiquetado AIP migrará a ahí. A partir del 31 de marzo de 2021, AIP dejará de estar disponible.

6.1.2.3.1 Datos específicos que monitorizar

Dentro de Office 365 existe la posibilidad de monitorizar el uso de información específica dentro de Exchange (correo electrónico), Teams (chat), OneDrive y SharePoint. Cuando la información se comparte con la persona equivocada (de acuerdo con las reglas que están configuradas), se activará una notificación (también es posible notificar al usuario) o se bloqueará. Los datos para monitorizar, además de las etiquetas, se muestran a continuación:

- Combinación de caracteres que parecen una contraseña aleatoria o una clave criptográfica
- Documentos debidamente etiquetados
- Direcciones IP
- Códigos pin
- Más de 3 números BSN
- Más de 3 direcciones de correo electrónico (en el cuerpo del correo o en el documento)
- Más de 1 códigos IBAN
- Más de 3 nombres
- Direcciones que no sean de VRT o entidades relacionadas (policía, estaciones de bomberos, etc.)

- Más de 3 números de teléfono
- Más de 3 números de fax
- Direcciones MAC
- Nombres de servidores / equipos
- Ubicaciones de archivos compartidos

Cuando la información solo debe ser accesible para ciertas personas, es mejor bloquear la información por completo y agregar a estas personas como excepciones. En general, es mejor hacer esto en lugar de permitir todo y bloquear personas o dominios específicos. Esto puede basarse en información específica como en la lista anterior o en las etiquetas que se agregan a los documentos.

Tomemos como ejemplo los datos médicos de los bomberos. Esta información, por ejemplo, solo puede estar destinada a dos personas. Esto significa que los correos electrónicos que contienen estos datos también deben bloquearse, excepto para las direcciones de correo electrónico de estas dos personas (o una bandeja de entrada colectiva solo accesible para ellos).

6.1.2.4 AIP y BIO

Este capítulo contiene elementos de Baseline Informatiebeveiliging Overheid (BIO) (Informatiebeveiligingsdienst, 2020) que son aplicables a Azure Information Protection.

Si se mantiene el BIO, debe haber una política de seguridad de la información establecida por la organización. Esto debe ser realizado por la gerencia y debe contener al menos los siguientes puntos:

1. Los principios estratégicos implementados y aplicables y las condiciones previas para la seguridad de la información deben alinearse con la política general de seguridad y la política de provisión de información (5.1.1.1 a)

Cuando se van a implementar nuevas políticas de seguridad de la información, es importante mirar la política de seguridad actual, esto significa que no debe entrar en conflicto: la persona A tiene derechos para distribuir un determinado archivo y, debido a las nuevas implementaciones, la persona B no. Por lo tanto, entra en conflicto y debe tenerse en cuenta.

2. Debe haber una descripción de las funciones de seguridad de la información. Por ejemplo: Tarea, responsabilidades y autorizaciones. (5.1.1.1 b)

Por ejemplo: una persona tiene que (responsabilidad) hacer copias de seguridad de ciertos archivos (tarea) y necesita tener derechos para hacerlo (autoridad).

3. Deben estar presentes las asignaciones de responsabilidad para las cadenas de sistemas de información a los administradores. (5.1.1.1 c)

Esto es para que se sepa (o al menos se escriba) quién es responsable de qué información.

4. Se deben realizar evaluaciones sobre las políticas de seguridad de la información. (5.1.1.1 e)

Esto es para que las personas se actualicen y recuerden para no perder de vista la política de seguridad de la información.

5. Se debe promover la conciencia de seguridad. (5.1.1.1 f)

Esto se puede hacer educando al personal sobre las razones y los problemas que pueden ocurrir si no se manejan adecuadamente. Por ejemplo con presentaciones educativas en PowerPoint.

Dentro de la organización también debe existir un marco de gestión con respecto a la implementación y ejecución de la seguridad de la información. Esto se hace para que la organización pueda iniciar y controlar esta seguridad.

6. Se deben asignar y definir responsabilidades de seguridad de la información (6.1.1)

   6.1 Deben definirse las responsabilidades y tareas de la dirección sobre AIP dentro de la organización. (6.1.1.1)

   6.2 Esto debe definirse con respecto a las regulaciones y leyes. (6.1.1.2)

   6.3 Debe haber un perfil de función del Director de Seguridad de la Información (CISO) (6.1.1.3)

      6.3.1 Hay un CISO designado (6.1.1.4)

7. Las tareas y responsabilidades en conflicto deben separarse para reducir la posibilidad de cambios no autorizados o no deseados o el mal uso de los recursos de la empresa. (6.1.2)

   7.1 Existen medidas contra el acceso no deseado o no autorizado a los activos. (6.1.2.1)

Esto podría dar lugar a conflictos dentro del espacio de trabajo: cuando se trata y se escribe correctamente, esto no debería ocurrir.

8. Debe haber contactos apropiados con agencias gubernamentales (6.1.3)

   8.1 Se detalla quién se pone en contacto con qué agencia gubernamental con respecto a AIP. También debe haber requisitos relevantes cuando se produce este contacto. (6.1.3.1)

   8.2 Este resumen de contactos debe revisarse anualmente. (6.1.3.2)

Debido a que los gobiernos pueden tener control sobre las empresas, no querrás cometer errores aquí. Los problemas se pueden prevenir dirigiendo a personas específicas a tareas específicas que deben seguir las pautas sobre cómo comunicarse con las agencias gubernamentales. Además, los formularios de contacto que se utilizan con regularidad se pueden crear previamente para que solo sea necesario completarlos (plantillas).

Asegurar que la información reciba un nivel adecuado de protección que esté de acuerdo con su importancia para la organización.

9. La información debe clasificarse en relación con los requisitos legales (8.2.1)

   9.1 Esta clasificación ha sido sometida a un análisis de riesgo. Esto se hace para que se sepa qué protección es adecuada (8.2.1.1)

10. Cuando la información está etiquetada, debe hacerse de acuerdo con un conjunto apropiado de procedimientos en cuanto al esquema de clasificación de información establecido por la organización (8.2.2).
11. Debería haber procedimientos para manejar los activos de la organización de acuerdo con el esquema de clasificación de información elaborado por la organización (8.2.3)

6.1.3 Consejos para la SIEM

El objetivo final de VRT es conseguir una infraestructura SIEM en pleno funcionamiento con Azure Sentinel. Para ello, todos los componentes de Azure deben configurarse correctamente primero, incluida la configuración de supervisión adecuada para enviar información a Azure Sentinel. Se inicia a través de Azure Active Directory y Azure Information Protection proporcionando un consejo sobre cómo se debe implementar (buenas prácticas) y qué se debe monitorizar.

A VRT se le proporcionó un conjunto de casos de uso para comenzar con el SIEM. Algunos de los cuales se describen a continuación:

Nr.	Nombre	Descripción del evento y detección
1	Sistema interno haciendo barrido de red en un puerto	Detecta el comportamiento de un barrido de red en un puerto de red
2	Intentos detectados de fuerza bruta por el IDS	Detecta cuando se está realizando un ataque de fuerza bruta
3	Posible fuerza bruta exitosa	Aquí se comprueba si se ha realizado un intento de inicio de sesión exitoso después de varios intentos de inicio de sesión incorrectos.
4	Detección de dominios, direcciones IP o URL maliciosas	Detección cuando un usuario desea acceder a un dominio, dirección IP o URL que se sabe que es malicioso.
5	Inicio de sesión anónimo en red	Detecta cuando alguien intenta iniciar sesión con una cuenta ANÓNIMA
6	Inicio de sesión exitoso con cuentas integradas	Detección cuando se realiza un inicio de sesión exitoso usando cuentas INVITADO o SISTEMA.
7	Registro de eventos borrados	Detecta cuándo se borra el registro de eventos en un sistema Windows.
8	Acceso de grupo privilegiado concedido	Cuando una cuenta recibe altos privilegios.
9	Error de autenticación de cuenta privilegiada	Intentos de inicio de sesión fallidos desde una cuenta con muchos privilegios
10	Éxito de fuerza bruta externa desde un host de origen único	Ataque de fuerza bruta externo exitoso desde un host externo

Tabla 1: Funciones a implementar en la SIEM

Los elementos de la tabla 1 que están marcados en verde ya están en el consejo anterior del presente documento (principalmente en AAD). El resto de elementos no están directamente asociados con AAD o AIP y aún deben desarrollarse medidas para mitigar estas posibles vulnerabilidades. Esto involucra otros componentes / productos (tanto componentes hardware como software) que están fuera del alcance de este proyecto.

De cara a implementar la SIEM, es importante tener en cuenta que se debe empezar paso a paso, un primer consejo sería el de escoger subconjuntos de datos clave y estudiarlos para ver la información que presentan, antes de juntar todos los componentes, es mejor ir poco a poco y clasificar las fuentes según el origen de los datos, pudiendo realizarse esto mediante una división entre datos perimetrales y datos internos (según la zona de la red de donde provengan).

En cuanto a los dispositivos perimetrales, pueden incluir los dispositivos que se encuentran de cara al exterior, como firewalls, dispositivos de detección/prevención de intrusos y proxies entre otros.

Y en cuanto a los dispositivos internos, pueden incluir aquellos por ejemplo que brindan servicios de autenticación, como pueden ser aquellos relacionados con el DHCP, bases de datos, LDAP o virtualizadores.

Otro consejo sería el de tener claro el alcance que se quiere tener al monitorizar los datos, que datos son importantes para VRT de tener bajo control, puede realizarse mediante un análisis de riesgos, por ejemplo. Es bueno además ver de forma gráfica los flujos de datos y analizar patrones de esos flujos para mejorar la capacidad de detección y poder diferenciar flujos de datos anómalos que puedan ser propiciados por algún tipo de ataque.

Conforme la SIEM comience a funcionar es importante tener en cuenta que cada vez existen ataque más complejos por lo que se necesitarían reglas también cada vez más elaboradas, esto implica que se debe trabajar constantemente en la SIEM para lograr detecciones cada vez más sofisticadas, por lo tanto, es necesario incluir personal que esté siempre trabajando en la SIEM y sus reglas. (sadvisor, 2020)

6.2 Evaluación

Evaluación del cliente

Para cumplir con la rúbrica de probar la solución hicimos una evaluación con el cliente (VRT) sobre los resultados (asesoramiento).

En general, la investigación y los consejos son buenos y realmente útiles. A diferencia de otros proyectos de estudiantes que venían con soluciones complejas que no se implementan fácilmente, los resultados de este proyecto realmente se pueden utilizar. Es práctico y es lo que se nos pidió en un primer momento, antes de la realización del proyecto.

Lo único que faltaba era una lista (resumen) de todo lo que se debía hacer, por lo que aún no se han implementado todas las prácticas. Con esta lista, podrá dirigirse a sus socios y decirles que implementen los elementos de la lista. También hace que sea más fácil informar / convencer a la gerencia de la empresa de que se deben tomar medidas en función de las prácticas, ya que obtienen un resumen que es más fácilmente legible que el informe completo de investigación. La lista lo hace factible. Debido a esto, esta lista se crea y se agrega a este documento como un apéndice. En general, el cliente está satisfecho con los resultados.

Evaluación de resultados del proyecto

Según los resultados, creo que se alcanza el objetivo del proyecto porque este informe ayudará a VRT a implementar Azure AD y AIP de acuerdo con las mejores prácticas y normas de seguridad. También se cumplen todos los requisitos que se establecieron con el cliente en un principio. El asesoramiento se basa en las mejores prácticas para ambos componentes, incluida la supervisión, varios temas dentro de estos componentes también forman parte del asesoramiento como PAM e IAM para Azure AD y etiquetado unificado para Azure Information Protection.

7. Conclusiones

Aquí concluye el informe de asesoramiento. Me gustaría agradecer a René van den Nieuwenhoff por guiarnos en todo momento y también agradecer a Jeroen Brouwer por darnos esta tarea y brindarnos información siempre que la necesitábamos.

Como se señaló en el capítulo de evaluación, creo que se ha alcanzado el objetivo del proyecto y, por lo tanto, se han obtenido buenos resultados. Lo siguiente que debe hacer VRT es implementar Azure AD y AIP según los consejos y, para ello, es mejor usar el resumen correspondiente al apéndice 1 para obtener y mantener una descripción general de lo que se debe hacer.

Este proyecto ha sido de gran utilidad para saber las tecnologías en materia de ciberseguridad que Microsoft posee e implementa en sus sistemas en la actualidad. Sirve para tener una visión amplia de como se integran todas las capacidades de Microsoft con las arquitecturas de seguridad existentes, lo cual resulta muy útil a la hora de unir tecnologías, monitorizar datos provenientes de distintos componentes, desarrollar una SIEM donde se manejen los datos de forma centralizada, entre otros aspectos.

De acuerdo con lo dicho por el cliente cuando finalmente terminó de leer nuestro informe de asesoramiento, la empresa VRT está contenta e iban a ponerlo en práctica nada más entregárselo, eso sí, lo harían con la ayuda del servicio técnico de Microsoft para mayor control de los cambios internos, puesto que manejan datos de alta confidencialidad. Nos avisaron de que seguiríamos en contacto para que nos fueran diciendo sus impresiones a la hora de introducir los cambios en el sistema. Posteriormente nos contaron que todo iba sobre ruedas y que les ha servido de mucho nuestro trabajo, por lo que podemos decir que los resultados obtenidos han sido buenos, y ambas partes están contentas con el proyecto realizado.

Gracias por leer este documento.

8. Apéndice

Estas son las prácticas que aún no se han implementado.

Cabe destacar que, en cuanto a mi trabajo individual, no me he encargado de las partes correspondientes a la BIO ya que mis compañeros tenían mayor facilidad con este tema puesto que muchas de las fuentes eran en Holandés y ya sabían de antemano muchas normas sobre esto.

Azure Active Directory:

- Implementar la política para el uso de frases de contraseña (la política ya se hizo)
- Evaluar periódicamente las cuentas de administrador (privilegiadas) y limpiar el grupo de administradores de dominio, llevar un registro
- Cuentas de usuario y administrador separadas para el personal de TI
- Habilite la auditoría en equipos (política de grupo) en el dominio para análisis de seguridad
- Monitorear eventos de AD para detectar señales de compromiso (monitoreo de seguridad) | Utilice Azure Identity Protection para la supervisión de Azure AD (direcciones IP y usuarios de intentos de inicio de sesión, etc.)
- Limpiar las cuentas antiguas de usuarios y computadoras de AD: procedimiento necesario
- Supervise DNS y DHCP para detectar amenazas a la seguridad
- Utilice Office365 Secure Score para comprobar si está configurado correctamente (implementación en relación con la seguridad)
- Derechos de acceso a documentos con grupos (grupos / roles con privilegios)
- Utilice un punto de referencia de endurecimiento y compruébelo regularmente
- Gestión centralizada de identidad (solo una instancia de Azure AD, sin AD local)
- Supervisar y registrar toda la actividad privilegiada
- Educar a los usuarios sobre buenas prácticas en materia de seguridad.
- Documentar las políticas y prácticas de gestión de cuentas
- Proporcione privilegios adicionales según el tiempo, elimine automáticamente los privilegios después de un período de tiempo
- Cuando use cuentas de servicio, ciérrelas, solo los derechos necesarios y no configure la contraseña para que nunca caduque
- Minimice la cantidad de políticas de CA (no una por aplicación)
- Analice sus aplicaciones y agrúpelas en aplicaciones que tengan los mismos requisitos de recursos para los mismos usuarios.
- Configurar cuentas de acceso de emergencia
- Habilite las políticas de acceso (Azure) en el modo de solo informe (para el registro)
- Excluya los países de los que nunca esperará un inicio de sesión
- Use controles personalizados para redirigir a los usuarios a un servicio compatible para satisfacer los requisitos de autenticación fuera de Azure AD
- En base a un análisis de riesgo se determinarán qué funciones obtendrán qué derechos de acceso (separación de derechos de función) (BIO 9.2.2.2)
- Los derechos de acceso especiales se controlan y restringen + se comprueban en cada cuartil (BIO 9.2.3)
- Se toman medidas para aislar información con interés específico (BIO 9.4.1.1)

- Los usuarios solo pueden ver la información necesaria para practicar su función (BIO 9.4.1.2)
- El acceso a la información de proveedores externos se basa en el análisis de riesgos y está registrado (BIO 9.4.2.2)
- El uso de las herramientas del sistema se registra y se mantiene disponible durante 6 meses (BIO 9.4.4.2)

Azure Information Protection:

- Utilice el etiquetado unificado en lugar de AIP para no tener que migrar antes de marzo de 2021 (tendrá todas las mismas funciones)
- Utilice el cliente de etiquetado unificado AIP (localmente en estaciones de trabajo)
- Etiquetas: use la configuración "El contenido nunca caduca" (a menos que sea necesario para la retención)
- Al configurar etiquetas, use la clave de la nube de Azure en lugar de HYOK para la protección
- Permita el acceso sin conexión basado en datos confidenciales (durante 7 días) y muy confidenciales (nunca)
- Utilice el escáner AIP para buscar información confidencial y etiquetarla en consecuencia
- Para almacenes de datos en la nube, se debe usar Azure Cloud App Security
- Para compartir secretos u otra propiedad intelectual, use subetiquetas AIP en una política de alcance para datos altamente regulados que encripten el contenido y restrinjan el acceso a grupos específicos.
- Implemente políticas de DLP para evitar que los usuarios compartan accidentalmente datos confidenciales
- Implementar la protección de la información de Windows para proteger contra la fuga de datos
- Implemente Cloud App Security para mapear el entorno de la nube, monitorear el uso y detectar eventos e incidentes de seguridad.
- Use reglas para detectar información confidencial en correos electrónicos, OneDrive, SharePoint, etc.que se comparte fuera de VRT (ya está en su lugar)
- Base el acceso a las etiquetas en bloquear a todos y permitir personas específicas como excepciones
- La parte BIO para AIP se agregó más tarde, por lo que se desconocía qué partes de BIO ya estaban presentes en VRT. Esto significa que no se puede poner aquí ninguna referencia con respecto a BIO AIP.

9. Bibliografía

activedirectorypro. (20 de Junio de 2020). *https://activedirectorypro.com*. Obtenido de https://activedirectorypro.com/active-directory-security-best-practices/: https://activedirectorypro.com/active-directory-security-best-practices/

GITHUB. (2 de Junio de 2020). *github*. Obtenido de https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-migrate-labels.md: https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-migrate-labels.md

github. (12 de Junio de 2020). *https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-migrate-labels.md*. Obtenido de https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-migrate-labels.md: https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-migrate-labels.md

github. (12 de Junio de 2020). *https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-protection.md*. Obtenido de https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-protection.md: https://github.com/MicrosoftDocs/Azure-RMSDocs/blob/master/Azure-RMSDocs/configure-policy-protection.md

informatiebeveiligingsdienst. (15 de Mayo de 2020). *https://www.informatiebeveiligingsdienst.nl*. Obtenido de https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/ : https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

Microsoft. (12 de Junio de 2020). *docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting: https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

Microsoft. (15 de Junio de 2020). *docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting: https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

Microsoft. (19 de Junio de 2020). *docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-gb/azure/information-protection/what-is-information-protection: https://docs.microsoft.com/en-gb/azure/information-protection/what-is-information-protection

Microsoft. (19 de Junio de 2020). *docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-gb/azure/information-protection/what-is-information-protection: https://docs.microsoft.com/en-gb/azure/information-protection/what-is-information-protection

Microsoft. (12 de Junio de 2020). *docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-gb/azure/information-protection/configure-client: https://docs.microsoft.com/en-gb/azure/information-protection/configure-client

microsoft. (15 de Julio de 2020). *https://docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services: https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

Microsoft. (20 de Junio de 2020). *https://docs.microsoft.com*. Obtenido de https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/manage/component-updates/executive-summary: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/manage/component-updates/executive-summary

Microsoft. (22 de Junio de 2020). *https://docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

Microsoft. (8 de Junio de 2020). *https://docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/plan-conditional-access: https://docs.microsoft.com/en-gb/azure/active-directory/conditional-access/plan-conditional-access

Microsoft. (25 de 2020 de Julio). *https://docs.microsoft.com*. Obtenido de https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

sadvisor. (27 de Julio de 2020). *sadvisor.com*. Obtenido de https://sadvisor.com/capacitaciones/13743/10-consejos-para-un-siem-exitoso/: https://sadvisor.com/capacitaciones/13743/10-consejos-para-un-siem-exitoso/

securityboulevard. (15 de Junio de 2020). *https://securityboulevard.com*. Obtenido de https://securityboulevard.com/2020/01/new-insights-into-privileged-access-management-pam-best-practices/: https://securityboulevard.com/2020/01/new-insights-into-privileged-access-management-pam-best-practices/

thycotic. (2 de Julio de 2020). *https://thycotic.com*. Obtenido de https://thycotic.com/company/blog/2019/09/24/privileged-access-management-best-practices/: https://thycotic.com/company/blog/2019/09/24/privileged-access-management-best-practices/