Acronis

Libro electrónico de Alex Fields, ITProMentor.com
Encargado por Acronis

Cómo evitar ciberataques en entornos de Microsoft 365:

Introducción a los servicios de ciberseguridad especiales

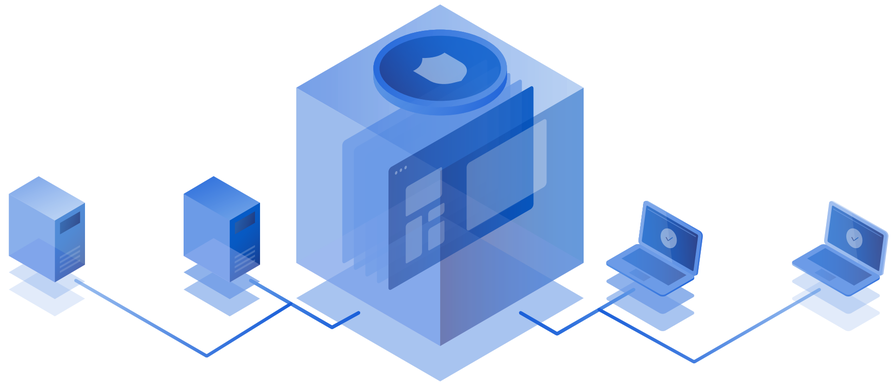
La importancia de proteger los entornos de Microsoft 365

La mayoría de las empresas de hoy, ya sean de mayor o menor envergadura, están adoptando, si no lo han hecho ya, plataformas de software como servicio (SaaS) basadas en la nube como Microsoft 365. Como cualquier otro software, estos sistemas basados en la nube requieren cierto grado de conocimiento técnico para su correcta configuración y protección frente a diversas amenazas y riesgos. El software de productividad listo para su uso se ha diseñado para poder usarse de la manera más sencilla posible, con el mínimo de dificultades.

Sin embargo, el panorama de amenazas surgidas en los últimos años ha obligado a algunos proveedores de servicios basados en la nube a revaluar sus configuraciones “predeterminadas”. Un ejemplo claro es el de Microsoft, que ha tomado medidas para mejorar el estado de seguridad predeterminado de los inquilinos en Microsoft 365. Por ejemplo, la autenticación heredada (denominada, "autenticación básica"), susceptible de sufrir ataques de difusión de contraseña entre otros, quedará en desuso próximamente este mismo año.

Microsoft también ha comenzado a habilitar lo que se conoce como "valores de seguridad predeterminados" para los inquilinos nuevos, que obligan a los usuarios a registrarse para una autenticación multifactor (lo que puede evitar el 99 % de los ataques basados en la identidad). Aunque los inquilinos antiguos también tienen acceso a esta característica, es necesario activarla manualmente.

A pesar de que los valores de seguridad predeterminados constituyen una gran mejora de la configuración básica de los inquilinos nuevos de Microsoft 365, existen muchas otras opciones para los proveedores de servicios gestionados (MSP) de abordar los riesgos e implementar iniciativas de ciberseguridad en la nube para sus clientes de pequeñas y medianas empresas (pymes). De hecho, es muy posible que la mayoría de los clientes desee adaptar sus directivas de seguridad con la ayuda de profesionales competentes. Además, las características avanzadas, como el acceso condicional, resultan más rápidas y mucho menos costosas de configurar en la nube que la mayoría de las soluciones de seguridad tradicionales que se desplegaban antes en las instalaciones locales.



¿Llegarán a ser suficientes nuestras inversiones en algún momento?

Uno de mis clientes, molesto tras la reciente comunicación de una vulnerabilidad importante de Exchange (en las instalaciones locales), me preguntaba si nuestra inversión en ciberseguridad vale de algo a fin de cuentas en un panorama con ciberdelincuentes patrocinados por Estados y otros adversarios de nivel avanzado que superan continuamente los límites, más allá de nuestro alcance. ¿Cómo se supone que vamos a seguirles el ritmo? *"Es como si nos ahogáramos, o al menos como si estuviéramos siempre luchando por mantener la cabeza a flote".*

Es comprensible. En los últimos meses, se han producido varios incidentes graves que han tenido una gran repercusión y una difusión suficiente para afectar incluso a nuestros clientes del sector de las pymes. Hasta ahora, 2021 ha sido otro año estresante en términos de ciberseguridad. Sin embargo, sigue siendo importante luchar por una buena causa y podemos tomar muchas medidas para mantener la cabeza a flote. En esta era de la modernidad, no hay otra opción. La forma de conseguirlo es adoptar los principios del modelo de confianza cero (Zero Trust).

Tres principios del modelo de confianza cero (Zero Trust)

Si ha visto referencias a este enfoque de la confianza cero (Zero Trust) en materiales de marketing de diversos productos de ciberseguridad, puede que aún tenga algunas dudas al respecto. Lo primero que hay que dejar claro es que el modelo de confianza cero (Zero Trust) no es algo que se pueda comprar directamente ni que se encuentre en un lugar físico concreto. Va más allá de ser el último eslogan del sector. Más bien, se trata de una concepción o actitud fundamental en cuanto a la seguridad. Microsoft aplica tres principios básicos para describir su enfoque de confianza cero (Zero Trust):

Verificación explícita
Se trata de validar tantos atributos como sea posible a la hora de conceder o denegar solicitudes de acceso. La tecnología clave de Microsoft que se aplica en este caso es el acceso condicional de Azure AD. Mediante el acceso condicional, se puede verificar de manera explícita la identidad, el endpoint y la ubicación de un usuario, así como otros indicadores de riesgos, para determinar si la solicitud es legítima o ilegítima.

Mínimo de privilegios
El principio del mínimo de privilegios establece que solo se debe conceder el nivel de acceso necesario para llevar a cabo las tareas obligatorias del trabajo, y no más. Esta norma debe aplicarse sin limitaciones y de forma global. Por ejemplo, debe restringir el acceso administrativo para sus servicios en la nube, así como para su infraestructura local, e incluso sus endpoints, como las estaciones de trabajo de Windows 10.

Asunción de las vulneraciones
En algún momento, sus sistemas de defensa fallarán y la confianza se verá comprometida. Debe prepararse adecuadamente para esto, que es inevitable. Ello implica disponer de las personas, las herramientas y los procesos necesarios para ponerlos en marcha y que actúen en caso de que se confirme una vulneración de la seguridad. Asimismo, significa que es necesario detectar de manera activa o "cazar" indicadores de compromiso en su entorno.

La confianza cero (Zero Trust) consiste literalmente en alejarse del concepto de confianza

Uno podría plantearse lo siguiente: *"¿Qué ocurre con estos recientes ataques de cadena de suministro de alto nivel que, fundamentalmente, se aprovechan de la confianza? ¿Están encontrando los atacantes formas de sortear el modelo de confianza Zero Trust?"* Es una buena pregunta. Cuando un atacante vulnera la seguridad de su proveedor (en quien confía) o toma el control de su dominio (que es la base de la confianza en su propio entorno), ¿se vienen abajo estos principios? **La respuesta es no**. De hecho, se hacen incluso más necesarios.

Ese es el fondo de la cuestión. La idea de confianza cero consiste literalmente en **ir más allá** del concepto de confianza. Por eso hablamos de verificación **explícita**, de conceder solo el **acceso justo y necesario** y de ser siempre conscientes de que se pueden producir violaciones de la seguridad (y que se ha de tener la capacidad para responder).

Así pues, la situación está clara. La verdadera cuestión es la siguiente: *"¿Cómo de lejos está dispuesto a llegar?"*

Solorigate (Nobelium)

Apliquemos el contexto anterior a un ataque reciente del mundo real, que saca partido de las relaciones de confianza. Para quienes no conozcan aún el incidente de Solorigate, se trata de un importante ataque de ciberseguridad que se detectó a finales de 2020 y principios de 2021, y que afectó a un gran número de empresas y organismos oficiales de Estados Unidos. El ataque lo perpetró un ciberdelincuente extremadamente sofisticado que Microsoft denominó más tarde Nobelium; es muy posible que este grupo cuente con el patrocinio de Estados.[1]

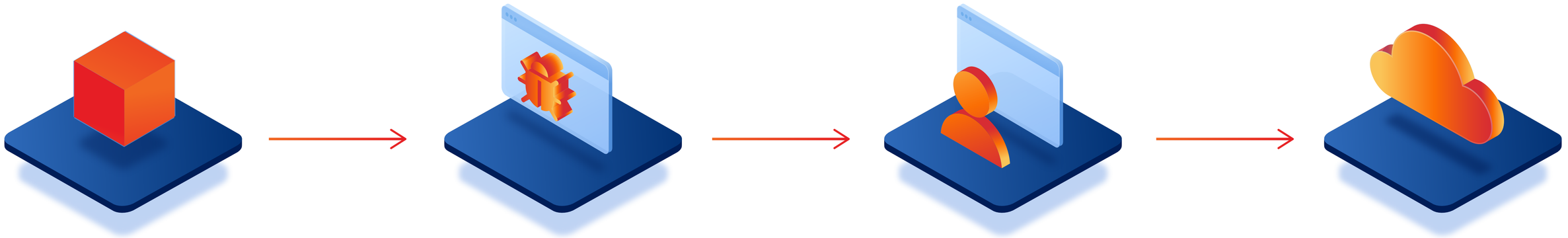
Solorigate fue un ataque de cadena de suministro ejecutado contra SolarWinds, una empresa de software que ofrece un producto denominado Orion, una suite de herramientas de gestión de tecnologías de la información (TI). De esta forma, se pretendía conseguir acceso con privilegios prácticamente automático a las redes y la infraestructura corporativas. La idea era infectar un paquete de software de confianza que se utilice en el trabajo de TI diario y, a partir de ahí, propagarse a otros objetivos dentro de la organización.

La idea era infectar un paquete de software de confianza que se utilice en el trabajo de TI diario y, a partir de ahí, propagarse a otros objetivos dentro de la organización.

SolarWinds Orion se ha implementado en numerosas instituciones públicas y privadas, varias de ellas pertenecientes a la Administración de Estados Unidos (el principal objetivo de este ataque). Es igualmente importante comprender también lo que, según Microsoft, era el objetivo final de Nobelium: filtrar datos del correo electrónico de estos organismos públicos (el proveedor de correo electrónico en muchos de estos casos es el servicio de Office 365 Exchange Online de Microsoft).

Ahora bien, si el objetivo son las cuentas de correo electrónico alojadas en un proveedor externo de servicios en la nube, como Microsoft, ¿qué sentido tiene empezar por atacar una cadena de suministro para infiltrarse en redes internas? ¿Por qué no atacar directamente al proveedor? En primer lugar, tenga en cuenta que el servicio en la nube de Microsoft es un objetivo más abstracto, donde cada cliente tiene su propio límite de seguridad o "inquilino" dentro de la nube de Microsoft. Las empresas que se conectan a este servicio público tienen relaciones de confianza establecidas para gestionar sus propios inquilinos.

De manera general, la cadena de ataque se desarrolló en las siguientes fases:



Compromiso de la cadena de suministro

Los ciberdelincuentes atacan la plataforma SolarWind Orion para inyectar código malicioso en un archivo DLL legítimo.

Acceso inicial y primer servidor de mando y control

El archivo DLL que se ha visto comprometido se carga al iniciarse la aplicación, y el código de puerta trasera se conecta al servidor de mando y control (C2).

Ataques manuales (hands-on-keyboard) in situ

Robo de credenciales, escalada de privilegios y desplazamiento lateral para:
1. Robar claves de firmas de SAML
2. Obtener privilegios administrativos

Ataques manuales hands-on-keyboard en la nube

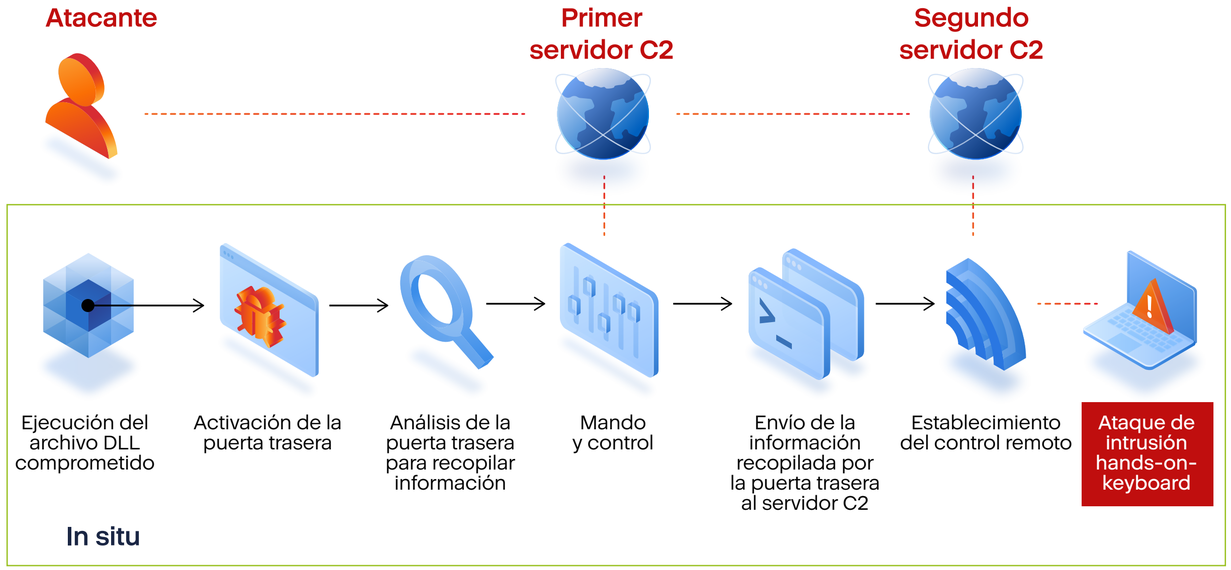
Los atacantes utilizan privilegios administrativos o claves robadas para establecer persistencia en los recursos de la nube y filtrar mensajes de correo electrónico.

No contamos con todos los detalles de la vulneración inicial de la cadena de suministro, pero en lo referente al análisis que ofrecemos aquí, no juega un papel determinante. Todo lo que ocurre después de esa primera fase tiene lugar en su entorno, por lo que tiene la posibilidad de interrumpir el ataque únicamente después de que el ataque a la cadena de suministro haya tenido lugar.

[1] **Nota:** para obtener más información sobre el ataque de Solorigate/Nobelium, consulte el centro de recursos de Nobelium de Microsoft, así como la alerta AA21-008A de la Agencia de Ciberseguridad y Seguridad en las Infraestructuras (CISA) de Estados Unidos.

Acceso inicial y primer servidor de mando y control

Estas tres últimas fases ofrecen excelentes lecciones para cualquiera que intente evitar que ataques como estos les puedan afectar. Comencemos analizando la primera fase: acceso inicial y primer servidor de mando y control.



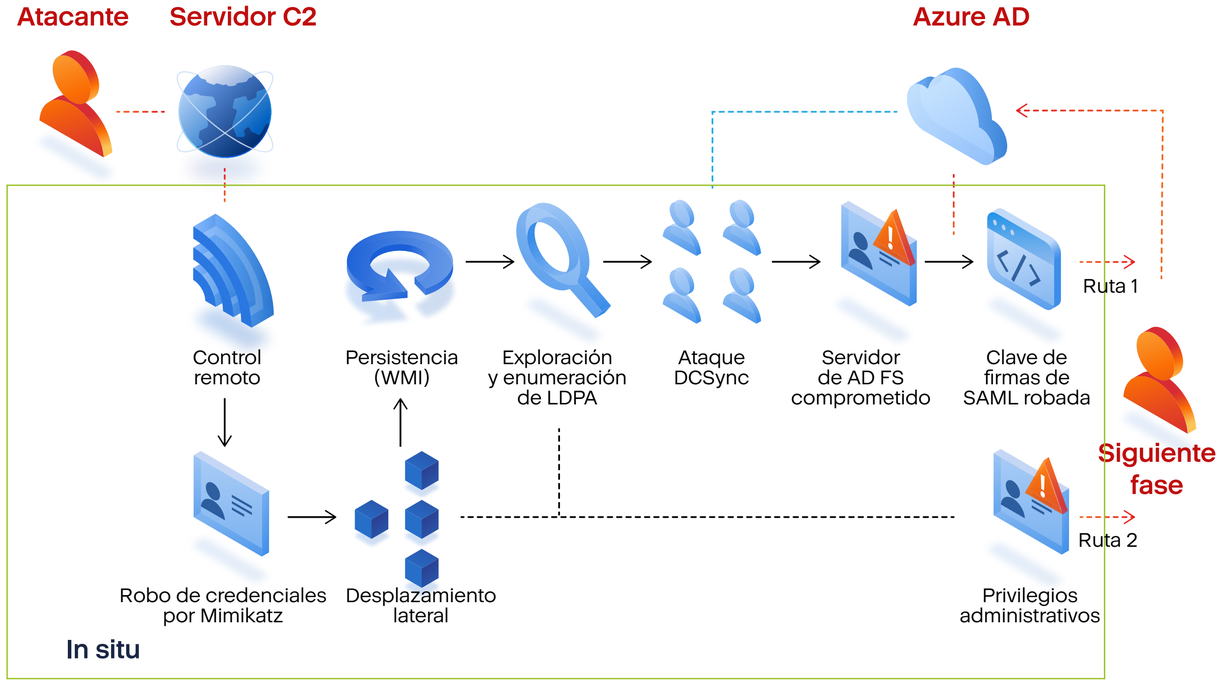
En esta fase, los ciberdelincuentes seleccionan cuidadosamente qué organizaciones atacar: no todas las puertas traseras activadas derivaron finalmente en ataques posteriores de intrusión hands-on-keyboard. Así pues, el contacto de mando y control inicial se estableció simplemente para recopilar información sobre los dispositivos afectados para que el grupo de ciberdelincuentes pudiera determinar si preferían continuar con el ataque en cada caso.

El segundo servidor de mando y control sirve para suministrar acceso remoto a los atacantes, de manera que puedan escalar sus actividades a la siguiente fase. Otro aspecto interesante de esta fase del ataque es que los servidores de mando y control iniciales generan dominios únicos para cada dispositivo afectado. Esta es otra señal del nivel de sofisticación de este ataque y, por supuesto, también complica mucho la detección.

Ataques manuales (hands-on-keyboard) in situ

La siguiente fase del ataque tenía un objetivo principal: obtener acceso a la nube (donde se almacenan los datos). Esto es posible a través de dos rutas distintas:

- **Ruta 1:** encontrar y atacar el servidor de AD FS (si existe)
- **Ruta 2:** encontrar una cuenta de administrador que tenga acceso a la nube con privilegios



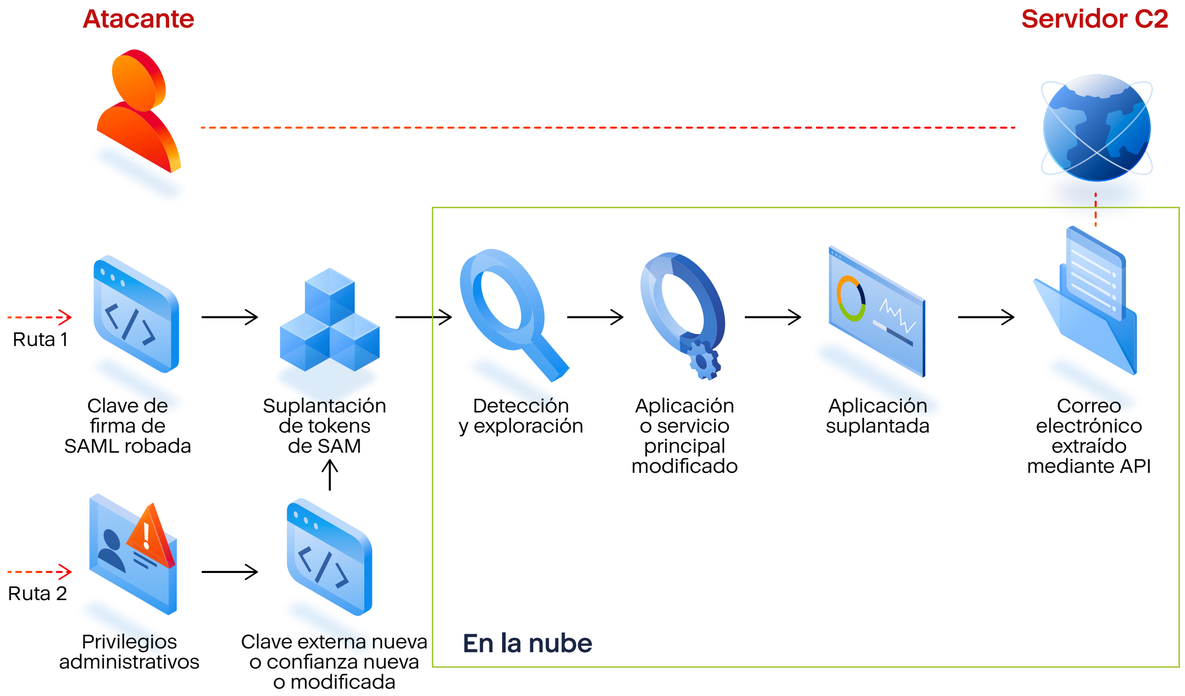
En ambos casos, muchas de las técnicas que se emplearon en esta fase nos resultan familiares: robo de credenciales a través de Mimikatz, desplazamiento lateral y exploración, establecimiento de persistencia, etc. Dado que el acceso inicial se produjo a través de software de gestión de TI comprometido, obtener privilegios de administración del dominio resultaba bastante trivial en este caso. Aunque la mayoría de los ciberdelincuentes considerarían este paso una gran victoria, en el caso de Nobelium no era para tanto. Lo que consiguieron sí que fue extraordinario.

Si el entorno estaba configurado para la federación local con un servidor de Servicios de federación de Active Directory (AD FS), esta era la ruta preferida para conseguir acceso a la nube. Así el atacante podía obtener el control de la confianza de la federación y, a continuación, robar la clave de firma de SAML para poder crear sus propios tokens de SAML y avanzar.

Si el dominio no estaba configurado para la federación (lo que Microsoft denomina un dominio "administrado"), los atacantes tenían que obtener acceso a una cuenta de administrador que tuviese privilegios tanto para las instalaciones locales como para la nube. Por desgracia, esta es una práctica increíblemente común: sincronizar una cuenta de administrador del dominio con la nube y asignar los mismos privilegios de administrador global de la cuenta.

Ataques manuales (hands-on-keyboard) en la nube

En esta fase siguiente, la idea era establecer persistencia en la nube y, finalmente, extraer datos de correo electrónico de Exchange Online. Si el atacante ya había clonado al proveedor de identidades en las instalaciones locales (AD FS), entonces podía emitir sus propios tokens de SAML. Si había comenzado solo con acceso de administrador global, es posible que debiera realizar el paso adicional de crear una nueva relación de confianza con su propia clave externa y, entonces, emitir tokens de SAML a partir de ahí.



Sea como fuere, llegado este punto, ya no era necesario acceder al entorno local y, en algunos casos, incluso se molestaron en volver y eliminar las huellas que habían dejado en las fases anteriores.

Llegados este punto, ya no era necesario acceder al entorno in situ y, en algunos casos, se molestaron en eliminar las huellas que habían dejado en las fases anteriores.

Un atacante menos experimentado habría abordado esta fase de otra manera. Lo más probable es que hubiese accedido al correo electrónico directamente suplantando cuentas o conectándose a los buzones de correo y, después, estableciendo reglas de reenvío. El problema con este enfoque más tradicional es que llama mucho la atención. Deja a su paso una gran cantidad de datos de auditoría y existe un mayor riesgo de que las actividades queden al descubierto antes de que se consigan sus objetivos.

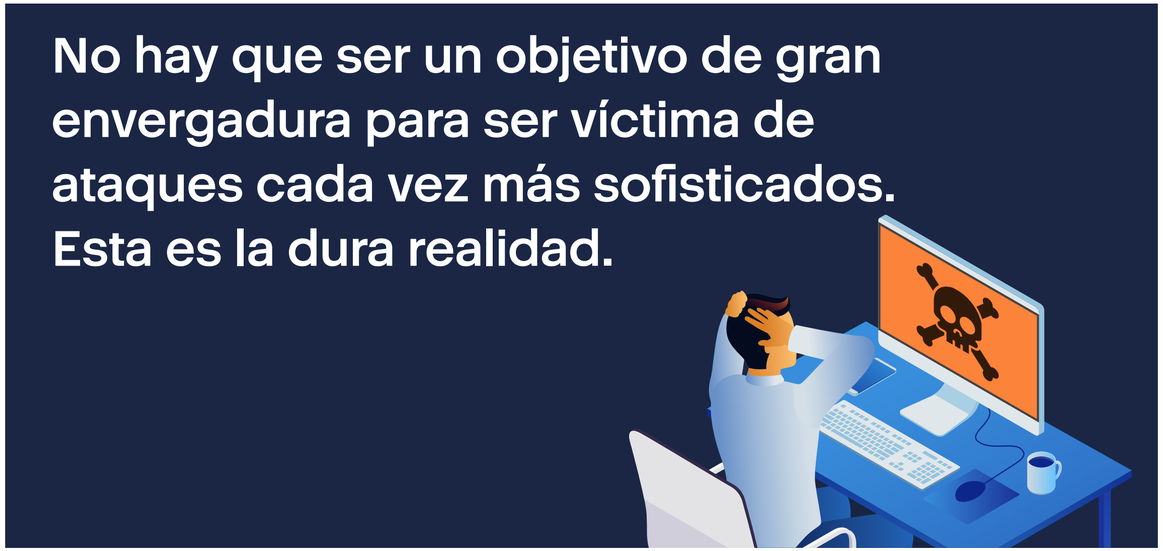
Lo llamativo de este incidente en concreto no es solo que el ciberdelincuente consiguiese llevar a cabo su ataque de cadena de suministro contra la Administración estadounidense y otras entidades indirectas de SolarWinds, sino que consiguiese hacerlo **sin que se le detectase.**

Al buscar aplicaciones existentes que ya estuviesen conectadas a Microsoft 365, Nobelium pudo agregar o modificar permisos en ellas sin ser descubierto, y suplantar entonces las aplicaciones para ejecutar extracciones en masa contra el servicio de Exchange Online. Por ejemplo, supongamos que tiene una copia de seguridad de terceros configurada para su correo electrónico basado en la nube. Eso significa que tiene un objeto de aplicación en Azure AD que ya tiene acceso para leer todos los mensajes de correo electrónico. Si no tuviese dicha aplicación, podría modificarse un objeto de aplicación distinto para agregar los permisos necesarios a fin de leer los mensajes.

En ambos casos, la aplicación se ha manipulado para que el atacante pueda suplantarla a su capricho. Así pues, las solicitudes de datos realizadas por la aplicación parecerían perfectamente legítimas. Básicamente, el atacante de Nobelium fue capaz de blanquear la filtración de ingentes cantidades de datos de correo electrónico. Además, sin llamar la atención.

Puede que esté pensando esto: ***"Bueno, suena muy interesante, pero es muy poco probable que afecte a pequeñas empresas como la mía".*** Pues se equivoca. Además de las grandes corporaciones, algunas pymes también se vieron afectadas por este ataque. Es más, la realidad que vivimos actualmente es que los ciberdelincuentes menos experimentados están observando a los más avanzados y aprendiendo de ellos cada vez más rápido. Ya hay disponibles kits en GitHub que facilitan a otros la reproducción de algunas de estas mismas técnicas.

En pocas palabras, no tiene que ser un objetivo de gran envergadura para ser víctima de ataques cada vez más sofisticados. Así es el mundo en el que vivimos, por más que nos pese.



Lecciones aprendidas

¿Qué hemos aprendido del incidente de Solorigate?

Puede resultar tentador darnos por vencidos y zanjar la cuestión con la excusa de que no hay nada que podamos hacer para superar las amenazas dado el panorama actual. Quizás deberíamos limitarnos a pagar un seguro de ciberincidentes y dar por concluido el tema. Sin embargo, discrepo. Sí, puede resultar difícil mantenerse a flote en unas aguas tan turbulentas, ¿pero por qué no evitar ahogarse? Sería un suicidio. Claro, es posible que se ahogue de todos modos, pero no se rinda a las primeras de cambio.

Mi consejo es apostar fuerte por el enfoque de confianza cero (Zero Trust). Analicemos algunas de las posibilidades que tenemos en Microsoft 365. Repasaremos de nuevo los tres principios y elaboraremos una breve lista para dibujar el itinerario típico Zero Trust en la nube de Microsoft. Además, también encuadraré estos elementos en un marco de ciberseguridad común denominado CIS Critical Security Controls.

Verificación explícita

1. Aplicar una autenticación fuerte (MFA)

La autenticación multifactor (MFA) no es una solución infalible, pero continúa siendo la mejor medida para proteger sus identidades en la nube (especialmente sus cuentas de administrador). Contar con otro paso para verificar la identidad de un usuario es esencial para evitar los típicos ataques basados en la identidad, como los de difusión de contraseña (otra técnica que Nobelium empleó cuando no tuvieron la opción de utilizar una puerta trasera). Además, es la mejor defensa contra el phishing y el robo de credenciales. Es cierto que existen otros sistemas de protección del correo electrónico que pueden servir como primera línea de defensa, pero en el contexto de la confianza cero (Zero Trust), tiene que asumir que en algún momento las credenciales de sus usuarios finales se expondrán o se interceptarán. Por eso, la MFA es ya imprescindible. Como me gusta advertirles a mis clientes: *"Si no implementan la MFA, básicamente, están claudicando a verse comprometidos".*

Como ya indiqué anteriormente, tenemos a nuestro alcance varias maneras de combatir esta situación y es posible que los nuevos inquilinos tengan esta opción habilitada de forma predeterminada.

Valores de seguridad predeterminados: esta opción es gratuita y está disponible con todas las suscripciones. Habilite esta característica en Azure AD > Propiedades (desplácese a la parte inferior de la página para acceder a un enlace donde podrá configurar sus valores de seguridad predeterminados).

MFA por usuario: es otra opción gratuita. También puede habilitar o deshabilitar la MFA por usuario. Consulte este artículo para obtener más información. Tendrá que realizar pasos adicionales para bloquear la autenticación heredada si emplea este método.

Acceso condicional: este es el enfoque preferido por la mayoría de las empresas a partir de ahora. En este caso, tiene la posibilidad de personalizar sus directivas de seguridad en mayor medida (a diferencia de los valores de seguridad predeterminados, que no se pueden personalizar). Las directivas de acceso condicional requieren al menos Azure AD Premium P1 (que se incluye con los planes de Microsoft 365 Business Premium o Enterprise).

Si tiene pensado utilizar el acceso condicional (opción recomendada), asegúrese de implementar al menos estas directivas para empezar:

- Bloquear la autenticación heredada
- Exigir autenticación multifactor para administradores
- Exigir autenticación multifactor para la administración de Azure
- Exigir autenticación multifactor para todos los usuarios

Estas cuatro directivas, si se configuran juntas, se asemejan a las funciones habilitadas mediante los valores de seguridad predeterminados.

La implementación de una autenticación fuerte cumple diversos requisitos del marco CIS Critical Security Controls: 4.5 (Exigir autenticación multifactor para cuentas de administrador) y 16.3 (Exigir autenticación multifactor para todos los usuarios).

También disponemos de la autenticación sin contraseña, pero abordaremos esta otra opción más tarde.

En el caso de Solorigate, la MFA no les preocupaba demasiado dado que ya tenían acceso a redes de confianza y podían crear sus propios tokens de SAML a su antojo. Además, cabe mencionar que el ataque de difusión de contraseña desempeñó un papel clave en la estrategia general de Nobelium (recuerde que la difusión de contraseña se mitiga en un 99,9 % desactivando la autenticación básica y activando la MFA), pero era solo una de varias opciones de todas formas. También podían contar con la vulneración de la cadena de suministro y obtener acceso por otros medios, como ya hemos visto en la cadena de ataque.

2. Exigir dispositivos conformes a las normativas

Las directivas de acceso condicional también ponen a nuestro alcance otras opciones de verificación. Por ejemplo, exigir que los dispositivos se marquen como conformes a las normativas. A la hora de implementar directivas basadas en dispositivos, es buena idea también bloquear las plataformas de dispositivos no admitidas, de modo que no haya lagunas en este tipo de verificación. Por sí solo, el cumplimiento normativo de los dispositivos puede ser una medida de seguridad eficaz contra determinados tipos de ataques avanzados (por ejemplo, los ataques de intermediario), pero además existen otras muchas ventajas ocultas en términos de estrategia general.

Exigir el cumplimiento de las normativas en los dispositivos significa que cada dispositivo se deberá inscribir para su administración para que se le pueda conceder acceso a los recursos. Este paso es importante por diversos motivos. En primer lugar, un dispositivo administrado tiene un 71 % menos de probabilidades de verse comprometido en comparación con un dispositivo no administrado, según datos de Microsoft. Esto se debe a que permite implementar controles de dispositivos (por ejemplo, la eliminación del administrador local o la reducción de la superficie expuesta a ataques) que reducen aún más las posibilidades de que un atacante ejecute malware, robe credenciales, realice desplazamientos laterales, etc.

En segundo lugar, gracias al cumplimiento normativo, se obtiene inventario y control sobre los activos de hardware y software de su empresa. Esto le ayuda a cumplir el marco CIS Critical Security Controls 1 (hardware) y 2 (software). Además, una vez que tiene el control de su inventario, puede implementar medidas adicionales que hacen más difícil que los posibles atacantes se afiancen y puedan desplazarse por el entorno (consulte el punto 5 de CSC sobre la configuración segura del hardware y el software).

Eso nos lleva al siguiente principio del modelo de confianza cero (Zero Trust).

Mínimo de privilegios

Existen muchas formas de aplicar el principio del mínimo de privilegios, tanto en las instalaciones locales como en la nube. Empecemos por asumir que los atacantes conseguirán acceso a recursos corporativos internos (como fue el caso de Nobelium). En este caso, la idea es implementar controles que creen un obstáculo natural o "radio de explosión" que contribuya a mitigar el impacto del evento de violación de seguridad inicial, así como a evitar actividades posteriores que puedan derivar en otros compromisos de la nube.

3. Adoptar cuentas solo de la nube (al menos los administradores)

Ya mencionamos este punto cuando abordamos la cadena de ataque. Probablemente ya se imagine de qué se trata: debe tener especial cuidado con las cuentas con mayores privilegios. Una práctica recomendada consolidada desde hace mucho tiempo consiste en utilizar cuentas de administrador independientes y específicas, así como minimizar el número de cuentas con privilegios de superusuario asignados, como los administradores de dominio (en entornos locales) y los administradores globales (en la nube). Esto se aborda en el punto 4 del CSC sobre el uso controlado de los privilegios administrativos.

No obstante, conviene dar un paso más, así que también se deberían separar las cuentas administrativas locales y las de la nube. Muchas empresas sincronizan todas sus cuentas y asignan privilegios administrativos globales completos para la nube a administradores de dominio clásicos. No lo haga.

Es una práctica nefasta que se aprovechó en el ataque de Solorigate (y en otros). Un ciberdelincuente que compromete un dominio no debería tener jamás acceso automático a otro.

Muchas empresas sincronizan todas sus cuentas y asignan privilegios administrativos globales completos en la nube a administradores de dominio clásicos. No lo haga.

Es más, por el bien de su entorno, debería plantearse si tiene sentido mantener la infraestructura tradicional en las instalaciones locales. Especialmente en el caso de las pymes, conviene plantearse seriamente la transición a las cuentas solo de la nube. No obstante, incluso si decide que desea mantenerla (quizás por motivos de compatibilidad con una aplicación heredada de la línea de negocio), ¿necesita realmente conectar esa infraestructura de generación anterior a la nube?

Ocurre muy a menudo que el motivo original por el que se optó por implementar tecnologías como Azure AD Connect o AD FS era mantener

las mismas contraseñas en las instalaciones locales y en la nube. Pero, ¿conoce la autenticación sin contraseña de Azure AD? ¿Qué sentido tiene mantener la sincronización de contraseñas si apenas (o nunca) tiene que usar la contraseña en la nube? [2]

Muchas pymes se beneficiarían de simplificar su entorno y eliminar la sobrecarga adicional que supone la sincronización de directorios: Azure AD Connect, AD FS, el último software de Exchange Server híbrido en las instalaciones locales, etc. Estas reliquias se están convirtiendo cada vez más en una carga que, francamente, dados los inconvenientes que suponen, no compensa para la mayoría de pequeñas y medianas empresas. Así pues, trasladar todas sus cuentas a la nube es una excelente idea.

4. Activar las solicitudes de consentimiento del administrador

A menudo se conceden privilegios a aplicaciones de terceros para interaccionar con datos de Microsoft 365, pero podemos controlar cómo se producen estas solicitudes de concesión de permisos. De forma predeterminada, todos los usuarios tienen la capacidad de permitir solicitudes de permisos de aplicaciones externas. Puede limitar o eliminar la capacidad de los usuarios estándar de conceder estas solicitudes en **Azure AD > Aplicaciones empresariales > Consentimiento y permisos.**

Además, también se pueden activar las solicitudes de consentimiento del administrador en **Azure AD > Aplicaciones empresariales > Configuración del usuario.** Esta opción le permite delegar la responsabilidad de añadir y gestionar aplicaciones y permisos a usuarios específicos dentro de su empresa.

Esta característica nos ayuda a cumplir subcontroles del punto 2 del CSC sobre el inventario y el control de recursos de software, así como el punto 4 del CSC sobre el uso controlado de los privilegios administrativos.

5. Realizar regularmente auditorías de aplicaciones y roles de Azure AD con privilegios

Como hemos visto con Solorigate y otros ataques, los adversarios a menudo establecen sus propios permisos de aplicaciones y cuentas. Por lo tanto, es una buena idea realizar periódicamente auditorías en su entorno para comprobar si se puede eliminar alguna cuenta o permiso. Tiene que hacerlo para todas sus cuentas, pero debe prestar especial atención a los roles de Azure AD que tienen acceso con privilegios como los de administrador global, lector global, administrador de usuarios, administrador de Exchange, etc. Las aplicaciones empresariales también se deben someter a auditorías de forma regular. Para obtener ayuda para realizar esta tarea, consulte el módulo de PowerShell de respuesta a incidentes de Azure AD. Esta herramienta incluye algunas funciones prácticas que le permiten generar cuentas con privilegios y permisos de aplicaciones, por ejemplo:

```
$TenantID = Get-AzureADIRTenantId -DomainName <InsertarDominioPrincipal>
Get-AzureADIRPrivilegedRoleAssignment -TenantId $TenantID -CsVOutput
Get-AzureADIRPermission -TenantId $TenantID -CsvOutput
```

[2] **Nota:** técnicamente, el atributo de contraseña de la nube continuaría existiendo, pero Microsoft recomienda no cambiar la contraseña a menos que crea que la cuenta se ha visto comprometida.

Este resultado se debe someter a auditoría con regularidad y compararse con una referencia o muestra óptima conocida del inquilino. Estos elementos están correlacionados con los subcontroles del punto 16 del CSC sobre la supervisión y el control de cuentas, así como del punto 18 sobre seguridad de software de aplicaciones.

¿Hay algo más que podamos hacer en cuanto a conceder el mínimo de privilegios? Claro que sí. Siempre se puede hacer más, pero las opciones citadas estarán accesibles para la mayoría de los entornos gestionados y para las suscripciones más conocidas, como Microsoft 365 Business Premium. Eso nos lleva al último principio del modelo de confianza cero (Zero Trust).

Asunción de las vulneraciones

No podemos asumir que todas las medidas de defensa anteriores nos protegerán de manera infalible. Por desgracia, no bastan. Si bien todas estas medidas complican enormemente la tarea a los posibles atacantes, no impiden que alguien burle su sistema de defensa. ¿Qué se puede hacer entonces? Es necesario que aplique el modo de respuesta a incidentes. Sin embargo, la respuesta a incidentes no comienza únicamente cuando se detecta una vulneración, sino que comienza ya: debe prepararse hoy mismo, porque estar preparado lo es todo en lo que respecta a la respuesta a incidentes.

6. Crear y poner en marcha un plan de respuesta a incidentes formal

Son demasiadas las empresas que no tienen en cuenta la planificación, pero se trata de un servicio realmente valioso que los MSP podrían ofrecer a empresas más pequeñas con presupuestos y recursos limitados: la planificación de la respuesta a incidentes. Los planes de respuesta a incidentes describen quién es responsable de qué actividades, tanto durante como después de una violación de la seguridad u otro evento de ciberseguridad. También puede indicar algunos pasos que el equipo debe realizar en diversas circunstancias. ¿Qué ocurre cuando los datos se pierden o se roban? ¿Qué ocurre si la empresa sufre un ataque de ransomware? ¿Qué ocurre cuando se le bloquea para acceder a su inquilino? Etcétera. Es conveniente documentar e incluso poner en práctica algunos de esos supuestos, ya que le servirá de preparación para afrontarlos de la mejor manera cuando ocurran de verdad. Puede encontrar online numerosas plantillas de directivas para comenzar, como esta de SANS. Además, Microsoft publica algunos manuales de respuesta a incidentes para diversos escenarios comunes, como el phishing y la concesión ilícita de consentimientos de aplicaciones. Estos recursos son un excelente complemento para cualquier plan de respuesta a incidentes de Microsoft 365.

Este elemento está correlacionado con el punto 19 del CSC sobre la respuesta a incidentes y su gestión.

7. Supervisar los registros de auditoría y generar alertas

Para ayudar a los que intervienen en la respuesta a los incidentes, una de las mejores cosas que puede hacer con antelación es realizar auditorías. Cuando se produce un incidente, necesita datos precisos que los expertos en ciberseguridad puedan revisar, ya que esta información nos revela qué ha pasado, cuándo, y qué cuentas o aplicaciones se han podido ver comprometidas, entre otros datos. No hay nada peor para un equipo de respuesta a incidentes que verse sin datos. Hace que el trabajo sea mucho más difícil, ya que les obliga a solucionar los problemas de visibilidad antes de poder realizar unas tareas de recuperación verdaderamente útiles.

Una de las mejores cosas que puede hacer con antelación es activar las auditorías. No hay nada peor para un equipo de respuesta a incidentes que verse sin datos. Hace que el trabajo sea mucho más difícil.

Como mínimo, tiene que activar la búsqueda en el registro de auditoría unificado, de manera que los eventos se registren de forma centralizada y se puedan buscar. Una vez hecho esto, puede activar también las directivas de alerta integradas que Microsoft proporciona por medio del Centro de seguridad y cumplimiento. De esta manera, los eventos sospechosos dentro del inquilino se reenvían a un buzón de correo supervisado.

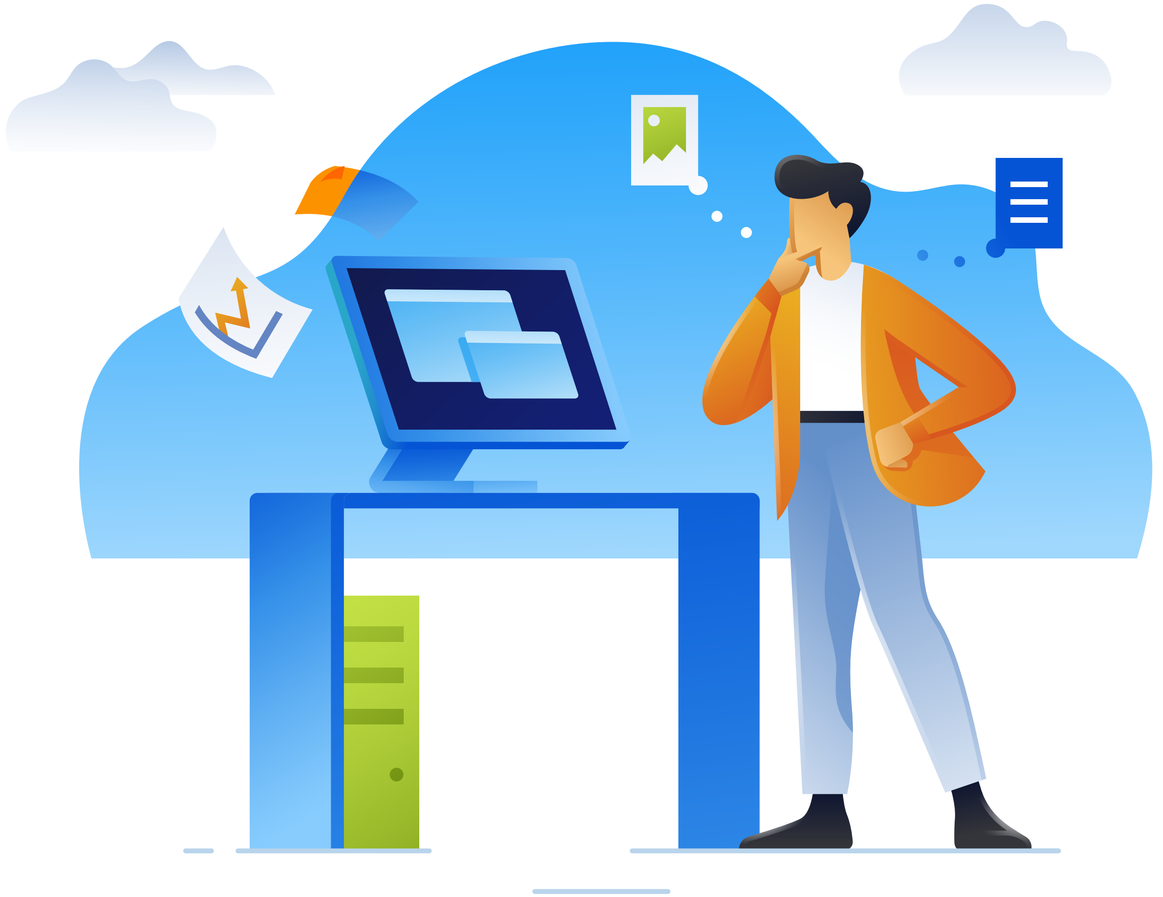
Si desea dar un paso más, platéese una herramienta de administración de eventos e información de seguridad (SIEM) como Azure Sentinel, para que pueda agregar otras fuentes de registros y personalizar su retención de datos de registro. Esto servirá de ayuda no solo durante la respuesta a los incidentes, sino también a la hora de detectar posibles amenazas de seguridad, mediante el análisis o "caza" de indicadores de compromiso (IOC) en los datos de registros. Sentinel es excelente también para los MSP, ya que se puede integrar con Azure Lighthouse para proporcionar administración multiinquilino para sus clientes. Consulte este artículo para obtener más información: Build a scalable security practice with Azure Lighthouse and Azure Sentinel (Cómo crear una práctica de seguridad ampliable con Azure Lighthouse y Azure Sentinel).

No obstante, cabe mencionar de nuevo que Microsoft también publica el módulo de PowerShell de respuesta a incidentes de Azure AD, una opción gratuita que permite a los responsables de la respuesta incidentes recopilar datos de Azure Active Directory, independientemente de si el cliente cuenta con una herramienta de SIEM implementada o no. La cantidad de datos históricos disponibles para esta herramienta depende del nivel de suscripción que tenga para Microsoft 365. Se recomienda contar al menos con Azure AD Premium P1 (disponible en Microsoft 365 Business Premium y versiones superiores), que le proporciona 30 días de datos de auditoría para consultar. Obviamente un sistema de SIEM sería más idóneo, pero debe saber que siempre hay otras herramientas a las que recurrir si otras no están disponibles.

Estos elementos están correlacionados con el punto 6 del CSC sobre mantenimiento, supervisión y análisis de registros de auditoría.

8. Plantearse añadir una solución de copia de seguridad a Microsoft 365

¿Qué ocurre con las copias de seguridad? ¿Realiza Microsoft copias de seguridad en la nube? En realidad, sí, pero las copias de seguridad de Microsoft no son sus copias de seguridad. Microsoft no proporciona a los clientes ningún tipo de acceso de autoservicio a las copias de seguridad que almacena. Algunos apuntan a otras características nativas, como las directivas de retención y la suspensión por litigio, pero estas medidas de protección están indicadas para usarse en asuntos legales y temas de cumplimiento normativo, y no como copias de seguridad. Además, muchos clientes seguirían sin sentirse cómodos al tener, por decirlo así, todos sus huevos en una misma cesta (la de Microsoft).



Tanto si cuenta con sistemas de protección como las directivas de retención como si no, si se ve inmerso en una situación comprometida en la que ha perdido datos debido a un ataque de ransomware o de otro tipo, el servicio de soporte técnico de Microsoft solo podría ofrecerle una recuperación que se limitaría a su "máximo esfuerzo razonable". Si una operación de restauración no funciona, no habrá mucho que hacer. Así pues, a la mayoría de las empresas les interesan soluciones de terceros como Acronis Cyber Protect, que protege los datos de todos los sistemas y aplicaciones, incluidos Windows, Microsoft 365, Active Directory y SharePoint, además de ofrecer funciones integradas de cifrado de copias de seguridad, antimalware y antiransomware, MFA, tecnologías de restauración instantánea, y la capacidad de realizar un seguimiento del estado de la protección de datos críticos en toda la organización.

Este elemento se refiere al punto 10 del CSC sobre la función de recuperación de datos.

Conclusión

Los ataques actuales contra Microsoft 365 van más allá de los típicos intentos de phishing y difusión de contraseña que hemos observado en años pasados. Actualmente, estamos siendo testigos de cómo ciberdelincuentes más sofisticados como Nobelium enseñan a otros atacantes a manejarse mejor en estos nuevos entornos que priorizan la nube o los móviles.

Hay que reconocer que hay otras muchas cosas que podemos y debemos hacer para evitar, o al menos minimizar, las probabilidades de que la confianza se ponga en riesgo, ante todo. Es esencial implementar un proceso riguroso de administración de parches y evaluación de vulnerabilidades para mantener sus entornos de Windows y Microsoft 365 actualizados y libres de puertas traseras que se puedan aprovechar. Las soluciones antimalware que se centran en las amenazas emergentes, como los ataques de día cero o los ataques sin archivos, también son cruciales para protegerse frente a las ciberamenazas modernas. La implementación de seguridad del correo electrónico también puede contribuir a reducir los riesgos y a proteger sus buzones de correo electrónico de Microsoft 365 contra el phishing, los intentos de suplantación, el malware, las amenazas persistentes avanzadas (APT) y otros ataques que intentan robar datos sensibles u obtener acceso no autorizado o beneficios financieros.

No obstante, gestionar varias soluciones individuales y formar a su equipo para que sepa utilizarlas podría ser especialmente complicado para las pymes y los MSP. Por eso, muchos proveedores de servicios buscan soluciones integradas sobre las que crear sus servicios, como Acronis Cyber Protect Cloud, ya que reúnen varias funciones en una única plataforma, lo que reduce en gran medida la carga de gestión y el coste total de propiedad.

Aunque estas capas de protección tradicionales continúan siendo una opción óptima y necesaria para cualquier empresa, hay algo inevitable: quienes no adopten un enfoque de confianza cero (Zero Trust) más profundo se quedarán atrás, sujetos a un número cada vez mayor de amenazas. Sencillamente, no es posible garantizar, por ejemplo, que el 100 % de los ataques de phishing o interceptación de credenciales se eviten siempre, y sí, a veces las amenazas proceden de otras fuentes de confianza. No existe una solución infalible en este caso. Es necesario implementar controles de seguridad probados en varias capas para garantizar la mejor y más completa cobertura que pueda.

Aunque la lista que se proporciona aquí no es exhaustiva, observo que la mayoría de las pequeñas y medianas empresas tienen mucho trabajo por hacer en cuanto a los puntos que hemos abordado aquí.

Verificación explícita

Aplicar una autenticación fuerte (MFA)
Exigir dispositivos conformes a las normativas

Mínimo de privilegios

Adoptar cuentas solo de la nube
Activar las solicitudes de consentimiento del administrador
Realizar regularmente auditorías de aplicaciones y roles

Asunción de las vulneraciones

Planificar la respuesta a incidentes
Supervisar los registros de auditoría y generar alertas
Plantearse una solución de copia de seguridad de terceros

Acerca del autor

Alex Fields

Alex, que creció en el seno de una pequeña empresa familiar, comenzó a adoptar las soluciones de TI de Microsoft desde muy joven. En su tiempo libre después de clase, adquirió experiencia en Windows Server, Exchange Server y la migración a Small Business Server.

Tras finalizar sus estudios universitarios, volvió al mundo de las tecnologías de la información, con un proveedor local de servicios gestionados, donde obtuvo experiencia en soluciones basadas en la nube de Microsoft más modernas durante una gran parte de esa década.

Ha recibido el premio Microsoft MVP por sus artículos técnicos y otras contribuciones a la comunidad.

Actualmente, trabaja de manera independiente, y ayuda a los MSP y otros consultores de TI a adoptar tecnologías modernas y crear prácticas de servicios gestionados en la nube. A día de hoy, vive en Minneapolis, en Minnesota (Estados Unidos). Le encanta escribir sobre temas tecnológicos y comparte sus ideas, experiencias, prácticas recomendadas y lecciones aprendidas con la comunidad.

Otras perspectivas de Acronis

Blog de Acronis: ofrece las últimas novedades y análisis del líder mundial en ciberprotección.

Canal de Acronis en YouTube: presenta vídeos de casos de uso, demostraciones, análisis de ciberamenazas y noticias de la empresa.

Centro de recursos de Acronis: reúne documentos técnicos, libros electrónicos, artículos especializados, tutoriales, infografías, etc., sobre ciberprotección.

Eventos de Acronis: aquí se publican eventos, seminarios web, entrevistas, etc., con información para inscribirse.

Acerca de Acronis

Acronis unifica protección de datos y ciberseguridad para ofrecer una ciberprotección integrada y automatizada que resuelve los retos de salvaguarda, accesibilidad, privacidad, autenticidad y seguridad (SAPAS) en el mundo digital moderno. Con modelos de implementación flexibles que se adaptan a las necesidades de los proveedores de servicios y los profesionales de TI, Acronis proporciona una ciberprotección de primera línea para datos, aplicaciones y sistemas, con soluciones de próxima generación antivirus, de copia de seguridad, recuperación ante desastres y protección de endpoints. Gracias a sus galardonadas tecnologías antimalware con inteligencia artificial y de autenticación de datos basada en blockchain, Acronis protege cualquier entorno, en la nube, híbrido o local, por un precio reducido y previsible.

Fundada en Singapur en 2003 y establecida en Suiza en 2008, hoy Acronis emplea a más de 1500 personas en 33 ciudades de 18 países. Sus soluciones cuentan con la confianza de más de 5,5 millones de usuarios particulares y 500 000 empresas, incluidas el 100 % del Fortune 1000, y equipos deportivos profesionales de primer nivel. Los productos de Acronis están disponibles en más de 40 idiomas a través de 50 000 partners y proveedores de servicios de más de 150 países.

Acronis

Encontrará más información en **www.acronis.com**