Guia Contra Ataques Ransomware

Christopher M. Frenz & Christian L. Diaz

Table Of Contents

Resumen Ejecutivo

Al abrir cualquier periódico o sitio web de noticias, el titular que se está convirtiendo cada vez más común es “base de datos de hospital secuestrada". Mientras que los hospitales y otras organizaciones a menudo se preparan con procedimientos contra cualquier eventualidad o incidente, que les permiten continuar con sus funciones a través de papeleo, al enfrentar cortes de energía y otras calamidades, sigue siendo un escenario de desastre encontrarse con toda su organización de infraestructura de información totalmente suspendida, porque alguien hizo clic en un enlace malicioso ó abrió un archivo adjunto de un correo electrónico cuestionable. Por otra parte, muchas organizaciones tienen un número significativo de sistemas casi obsoletos, que hacen de la seguridad un desafío, y a pesar de que cuentan con disposiciones de seguridad muy básicas, a menudo no tienen una cultura corporativa que esté fuertemente centrada en la seguridad de la información. Debido a esto muchas organizaciones luchan con gran esfuerzo al enfrentar ataques de tipo ***Ransomware***. Este documento está destinado a servir como una completa defensa en profundidad basada en una lista de verificación, y sirve como guía para evitar que ataques de ***Ransomware*** penetren en su organización, y al mismo tiempo a garantizar que procedimientos adecuados estén en su lugar para enfrentar brotes legítimos de ***Ransomware*** en su entorno. Dada la prevalencia de los sistemas operativos Windows como objetivo de ataques ***Ransomware***, la guía está orientada hacia dicho entorno, pero está diseñada para ser agnóstica al sistema operativo en uso. Tenga en cuenta que la lista está diseñada para ser completa y, como tal, no todos los controles pueden ser aplicables a todos los entornos.

Protecciones de Perímetro

Esta es su primera línea de defensa, pues poder detener una amenaza antes de que tenga acceso a cualquiera de sus sistemas, o a sus empleados, es siempre ideal.

Firewall

Mientras que una aplicación de ***Firewall*** en el perímetro es una práctica común para la mayoría de las organizaciones, es importante verificar que esté configurada para el filtrado de egreso, así como el filtrado de ingreso. El filtrado de entrada controla qué comunicaciones se permiten entrar a la red de la organización, mientras que el filtrado de salida controla qué comunicaciones se les permite abandonar la red de la organización. Tanto los controles de acceso de entrada como de salida deben basarse en un modelo de privilegios mínimos. Los sistemas que no necesitan acceso a fuentes externas de información u otros sistemas, deben tener prohibida la comunicación con entidades externas. Es mucho menos probable que un sistema sin acceso a entidades externas, se convierta en un punto de entrada para un ataque de ***malware***, si es comparado a un sistema conectado al Internet. Al mismo tiempo, en el caso de que se produzca una infección de tipo ***Ransomware***, dicho sistema no será capaz de llamar a casa, si el filtro adecuado de salida está en su lugar. También se debe activar el sistema ***Logging*** de registro en la aplicación ***Firewall***, ya que los intentos repetidos de acceso relacionados con direcciones de IP maliciosas pueden servir como indicador de un problema.

Servidor Proxy / Filtro Web

Como se mencionó previamente, desconectar sistemas del Internet es una gran defensa de ser factible, pero en realidad es probable que bloquear el Internet totalmente en sus sistemas no sea posible, y podría ser un obstáculo para las operaciones de su negocio. Sistemas conectados al Internet deben ser configurados para pasar por un Servidor Proxy que permita filtrar el contenido de la Web, con reglas de ***Firewall*** que garanticen que el acceso a la Web por medio de dicho servidor, sea el único medio de salida para conexiones http y https. Aunque el enfoque de una "***Lista de Admisión***" (***whitelisting***) para el acceso a la Web es el ideal, organizaciones deben utilizar como mínimo un dispositivo de filtrado para bloquear el acceso a los sitios web maliciosos más sobresalientes, como de ***spam*** / ***phishing***, de evasión de Proxy, pornografía, y otras categorías de sitios web considerados innecesarios para las operaciones normales del negocio. También se recomienda, cuando sea factible, que cualquier sitio web que no ha sido clasificado por el proveedor de Internet, sea bloqueado, ya que existe una mayor probabilidad que el sitio sea malicioso en naturaleza, a que el sitio web sea nada mas un negocio nuevo y válido. Si bien puede ser políticamente poco popular dentro de muchas organizaciones, también se recomienda bloquear el acceso a correo electrónico personal, sitios de intercambio de archivos, redes sociales, mensajería instantánea y redes publicitarias. De ser necesario, se pueden agregar exenciones especiales para sitios de intercambio de archivos, redes sociales, etc,.

Prohibición de la descarga de archivos ejecutables (por ejemplo: .exe, .scr, etc) en los dispositivos de la red también debe ser puesto en su lugar. Muchos servidores proxy / artefactos de filtrado Web también tienen la capacidad de examinar el contenido Web entrante con un mecanismo de Antivirus. Si dicha medida es respaldada, se recomienda que se mantenga en pleno funcionamiento, y de ser posible, implementar un mecanismo de Antivirus diferente al que se utiliza internamente para aumentar la probabilidad de que exista una versión del Virus en el diccionario de ambos Antivirus para descubrir cualquier amenaza, aunque sea nueva. Los filtros de contenido Web deben actualizarse periódicamente para garantizar que las categorías de sitios maliciosos y otros sitios Web estén siempre actualizados.

Además de los detalles mencionados anteriormente, se aconseja que el tráfico Web a los siguientes Dominios de Nivel Superior (TLD) se bloquee completamente como los resultados de Spamhaus (***https://www.spamhaus.org/statistics/tlds/***) y de BlueCoat (***http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/most-suspicious-tlds-revealed-by-blue-coat-systems/***) sugieren que la mayoría de sitios que tienen su Host en estos Dominios de Nivel Superior (TLD) son sospechosos en naturaleza:

Dominios de Nivel Superior (TLD)
.accountant
.biz
.click
.country

Dominios de Nivel Superior (TLD)
.cricket
.download
.gdn
.gq
.kim
.link
.party
.review
.science
.stream
.tk
.top
.trade
.win
.work
.zip

Filtro de SPAM

Como una defensa perimetral sugerimos filtros de ***SPAM*** que filtren el correo electrónico antes de que penetren su servidor de correo corporativo o si se utiliza correo electrónico externo, asegurarse de que el filtro de ***SPAM*** disponible por su proveedor esté activado. Es mucho mejor bloquear ***SPAM*** popular en el área de perímetro, así como correo que contiene enlaces maliciosos, y correo que contiene archivos adjuntos que puedan ser perjudiciales, en lugar de permitir que otras capas internas de la red de defensa se encarguen. También se recomienda bloquear cualquier mensaje que contenga archivos adjuntos ejecutables como archivos .exe o .vbs. Para las instituciones que no tienen presencia internacional, también puede ser aconsejable bloquear todos los correos electrónicos procedentes de lugares fuera de Norteamérica y hacer una "***Lista de Admisión***" de las excepciones necesarias.
Al igual que aplicaciones software de filtrado Web, los filtros ***SPAM*** siempre deben mantenerse actualizados para asegurarse de que tienen las listas de bloqueo más recientes y que sus mecanismos de Antivirus tienen las últimas actualizaciones de diccionarios para analizar los archivos adjuntos. Cuando sea factible, el motor Antivirus utilizado en el filtro ***SPAM*** debe ser diferente al motor Antivirus utilizado en los dispositivos de uso donde se accede al correo electrónico.

Defensas de la Red

Defensas que pueden desplegarse en el área de ***LAN***, con el fin de ayudar a detectar y mitigar ataques de malware.

DNS Sinkhole

Si bien la conectividad a sitios maliciosos debe ser idealmente bloqueada en el perímetro, se puede agregar una capa adicional de defensa contra el establecimiento de conexiones a sitios maliciosos mediante la creación de un "***DNS Sinkhole***" que evitará conexiones a determinados dominios dando información falsa cuando una solicitud de DNS esté dirigida hacia uno de los dominios en el "***DNS Sinkhole***". Al igual que con las defensas de perímetro, siempre se debe evitar que cualquier sistema o persona tenga acceso a contenido malintencionado, ya que es mucho mejor que mitigarlo una vez que haya sido descargado o accedido por un dispositivo en la red. Idealmente, su lista de dominios en el "***DNS Sinkhole***" debe provenir de una fuente diferente a la utilizada en su filtro Web para asegurar una cobertura más completa de dominios maliciosos. Se puede encontrar una tutoría sobre la creación de "**DNS Sinkholes**" en los servidores DNS de Windows en esta dirección Web: https://cyber-defense.sans.org/blog/2010/08/31/windows-dns-server-blackhole-blacklist

Segmentación de la Red

La segmentación de la red a través de ***VLANs*** y ***ACLs*** que controlan el tráfico entre ***VLANs*** no podrá evitar que un ataque de ***Ransomware*** tenga acceso a sus sistemas, pero sí será de mucha ayuda si una infección de ***malware*** es capaz de obtener un punto de apoyo dentro de su organización. La segmentación de la red puede ayudar a asegurar que una infección de ***malware***, u otro problema de seguridad, permanezca aislado sólo en el segmento de red en que ha sido infectado algún dispositivo electrónico, y así no se extienda por toda la organización. Es particularmente importante para las organizaciones que mantienen sistemas de legado que ya no pueden recibir actualizaciones de seguridad.

Segmentación de Máquinas Virtuales

Así como la segmentación de red discutida anteriormente es clave para asegurar que el número de sistemas a los que se puede propagar una infección de ***malware*** se minimice, es importante recordar que muchas comunicaciones de máquinas virtuales, tienen lugar a través del plano posterior de un servidor y no transversal a los equipos de red estándar como interruptores (switches). Para infraestructuras altamente virtualizadas, es recomendable implementar tecnologías de segmentación de máquinas virtuales, como ***NSX*** de ***Vmware*** o ***HNV*** de Microsoft, para garantizar que las comunicaciones de máquinas virtuales puedan ser controladas con mecanismos de seguridad de red equivalentes a los de los sistemas físicos.

Sistemas de Detección de Intrusiones de Red (NIDS)

El uso de un IDS de red (***NIDS***), probablemente no será una forma muy efectiva para evitar que ***malware*** tenga acceso a su sistema, ya que la mayoría se orienta más hacia la detección de intentos de explotación que en el ***malware*** mismo, pero un sistema ***NIDS*** puede utilizarse para alertar a posibles ataques, ya que pueden ser utilizados como métodos de alerta, si se están realizando intentos de comunicación a direcciones IP maliciosas como centros de comando y control de ***botnets*** y sitios Web de generación de claves para herramientas de ***Ransomware***. Entre más temprano el personal del área de IT y de Seguridad de la Información sea alertado de la presencia de un ataque de ***malware***, mayor es la posibilidad de detener un incidente con éxito, y ésta es una de las vías de detección que puede emplearse. Dependiendo de la implementación, los sistemas ***NIDS*** también pueden ayudar a identificar un sistema dentro de la organización que intenta infectar otros sistemas.

Protección de Dispositivos Electrónicos en la Red

Protecciones que existen en computadores personales y otros sistemas de interacción para usuarios.

Totalmente Actualizado y con Parches Implementados

Ransomware y otros tipos de ***malware*** a menudo utilizan una variedad de métodos de explotación para ganar un punto de apoyo dentro de sistemas, y si se garantiza que el Sistema Operativo y todas las aplicaciones instaladas en el sistema estén totalmente actualizados y con parches implementados, se minimizará el número de maneras en que los dispositivos electrónicos puedan ser explotados con éxito. En lo que respecta a ***Ransomware***, mantener su servicio de correo electrónico, de navegador y Flash totalmente actualizado es de importancia crítica. Las organizaciones deben contar con procedimientos robustos para garantizar una gestión correcta de parches y revisión de rutina del software.

Ni Aplicaciones Ni Servicios Innecesarios

Si una aplicación no existe en el sistema, no puede ser explotada, por lo que garantizar que la configuración de dispositivos electrónicos, sigan el modelo de privilegios mínimos, es una forma eficaz de reducir la superficie de ataque en dichos dispositivos. Es particularmente recomendable no permitir la ejecución de Java y Flash en equipos que no lo requieran.

Sin Derechos Administrativos

Derechos administrativos sólo deben utilizarse para tareas administrativas, y tareas normales en una computadora nunca deben realizarse desde una cuenta con privilegios administrativos. Esto evitará que muchos tipos de ***malware*** consigan un punto de entrada, ya que cuentas de usuarios regulares pueden no tener los permisos adecuados para "instalar" el ***malware***.

Antivirus (AV)

El Antivirus debe ejecutarse en todos los dispositivos electrónicos de la red, y debe ser configurado para tener acceso a archivos, otros recursos, y a aplicarles el escaneo. El Antivirus debe mantenerse actualizado, y se debe configurar un sistema de alertas para notificar al personal de IT sobre cualquier posible infección. Es importante recordar que los mecanismos de Antivirus se basan principalmente en sus diccionarios, y como tal, sólo puede detectar con eficacia las amenazas conocidas. Antivirus no pueden proporcionar ninguna protección contra un nuevo virus o una nueva variante de ***malware***. Idealmente, este debe ser de un fabricante diferente al que se utiliza en el nivel de defensa del perímetro.

Próxima Generación de Antivirus

Estas son soluciones de Antivirus que no necesitan diccionarios por la naturaleza de su mecanismo, y como tales, tienen el potencial de detectar ataques de día cero y nuevas variedades de ***malware***. Antivirus de próxima generación utilizan métodos tales como detección de comportamiento, aprendizaje automático, y ejecución de archivos basados en el ***cloud*** para tratar de identificar intentos de explotación y ***malware***. Algunos paquetes de Antivirus de próxima generación están certificados bajo protocolos de ***PCI-DSS***, y sirven como reemplazos de Antivirus regulares, pero no todos. En muchos casos se pueden utilizar como un posible complemento para Antivirus tradicionales.

Sistemas de Detección / Prevención Basados en Host (HIDS / HIPS)

Estos sistemas pueden ser independientes o integrados en una solución de protección de dispositivos electrónicos ofrecidos por fabricantes de Antivirus. Trabajan para detectar cambios suspicaces en archivos críticos del sistema, posibles desbordamientos de memoria, y otras actividades potencialmente sospechosas en dispositivos electrónicos. Pueden ayudar a proporcionar información desde el inicio de un posible ataque, y algunos tienen una capacidad limitada para mitigar ciertos intentos de explotación.

Filtro de Web

Muchos paquetes de protección de dispositivos electrónicos proporcionan un medio adicional para filtrar contenido de Web sospechoso, y es aconsejable activar dichos filtros, sobre todo si se sigue la recomendada práctica de utilizar fabricantes diferentes tanto para sistemas internos, como para sistemas al frente del perímetro. Esto aumentará la probabilidad de que todo contenido Web de dudosa procedencia, sea bloqueado antes de que un sistema o usuario pueda acceder a él.

Filtros de SPAM

Al igual que con el filtrado de contenido Web, filtrado de ***SPAM*** también es posible a nivel de dispositivos electrónicos, y el tener una solución de filtrado diferente instalada en estos, puede

ayudar a aumentar las probabilidades de que ***SPAM*** y correos electrónicos maliciosos que intentan pasan por alto las defensas en el perímetro, se detecten. Esto es crítico, ya que ciertas variantes de ***Ransomware*** como ***Locky*** se propagan comúnmente a través de los datos adjuntos contenidos en correos electrónicos maliciosos.

Inhabilitar Compatibilidad con Macros

Las macros y otros contenidos ejecutables se pueden incrustar en documentos utilizados en aplicaciones de oficinas, como editores, Office, y en archivos PDF. La probabilidad es que la gran mayoría de usuarios en una organización no tienen ninguna necesidad legítima para el uso de estos contenidos, y por ende, la compatibilidad con dichas características debe desactivarse de forma predeterminada.

Politica de Restricciones en el Uso de Software / AppLocker

Las directivas de "***Pólizas de Grupo para Objetos" (GPO)***, se pueden establecer para prevenir la ejecución de ciertas aplicaciones incluidas en una ***Lista de Bloqueo*** (***blacklist***), y evitar que aplicaciones en dicha lista, se ejecuten en determinadas locaciones, como por ejemplo en el folder AppData en el perfil de un usuario, lo cual es un objetivo común para un malware. Organizaciones pueden desarrollar sus propias políticas, o si prefieren, utilizar políticas diseñadas contra ataques de tipo ***Ransomware***, proveídas por organizaciones como "***Third Tier***". Como alternativa a ***Listas de Bloqueo***, la utilidad ***CryptoPrevent*** también se puede utilizar para implementar políticas de restricción del uso de software en dispositivos electrónicos. Dichas políticas son un buen complemento para el software Antivirus que se tenga en uso, ya que no están basadas en los diccionarios del Antivirus, y pueden evitar que las variantes de ***malware*** más sofisticados, puedan ejecutar correctamente. Asegúrese de desarrollar pruebas de ensayo con estas políticas, para asegurar que no interfieran con aplicaciones legítimas que se utilizan en su infraestructura. Una mejor propuesta a la ***Lista de Bloqueo***, es el enfoque en ***Listas de Admisión (whitelist)*** de aplicaciones, pero este es un proyecto más desafiante y demorado, porque se debe asegurar que las aplicaciones que son legítimas, funcionen correctamente y no sean interrumpidas una vez se ha establecido la ***Lista de Admisión***.

Archivos de Host (Host Files)

Los archivos de Host (***Host Files***) son comprobados antes de que el servicio ***DNS*** resuelva direcciones IP, y según lo mencionado previamente, se pueden utilizar ***DNS Sinkholes*** para evitar que los dominios maliciosos se resuelvan correctamente. Aparte de otros mecanismos de filtrado Web, este enfoque podría proporcionar otra capa de defensa contra un usuario o sistema que potencialmente podría estar conectándose a un sitio Web mal intencionado.

Inhabilitar Puertos USB

Aunque no es tan común como los vectores de ataque transmitidos por medio de Web o correo electrónico, ha habido variantes del ***Ransomware*** de ***CryptoLocker*** que se ha sabido propagarse

a través de unidades ***USB***. Siempre que sea posible, se debe bloquear el acceso a puertos USB.

Infraestructura de Máquinas Virtuales (VDI)

Si los dispositivos electrónicos en organizaciones se proveen en forma virtual, una opción adicional para la defensa contra ***malware***, es garantizar que todas las máquinas ***VDI*** no sean persistentes, y que los sistemas vuelvan a un estado predefinido después de cada sesión. Esto asegura que cualquier ***malware*** que ha infectado una máquina ***VDI***, se elimine una vez finalizada la sesión del usuario, ya que la reversión del sistema restaurará la máquina "como nueva", a un estado de ***pre-infección***.

Kit de Herramientas para Mejorar la Experiencia de Mitigación (EMET)

EMET es una utilidad gratuita distribuida por Microsoft que ayuda a detectar y prevenir métodos de explotación que buscan aprovecharse de la corrupción de memoria. ***EMET*** es también una buena adición a técnicas como Antivirus, ya que no está basada en sus diccionarios, y como tal, tiene la oportunidad de detener incluso, sofisticados programas ***malware*** y sus intentos de explotación. Asegúrese de probar ***EMET*** exhaustivamente antes de implementarlo para garantizar que no interfiera con ninguna de las aplicaciones legítimas utilizadas en su empresa. Más información sobre ***EMET*** se puede encontrar en: https://technet.microsoft.com/en-us/security/jj653751

Solución de Contraseña de Administrador Local (LAPS)

Aunque los autores no están informados sobre alguna variante de ***Ransomware*** conocida que se propague a otros sistemas utilizando la técnica de ***"Sobrepasando el Hash" (Pass the Hash)***, es una vulnerabilidad explotable muy común, y está presente en muchas infraestructuras de Windows, ya que la contraseña de Administrador Local de cada máquina es común en todos los sistemas. **LAPS** cambia la contraseña de administrador local aleatoriamente en los sistemas y almacena las contraseñas en ***Active Directory (AD)***. Además proporciona controles de acceso que se establecen para controlar quién puede buscar estas contraseñas de Administrador Local almacenadas por el ***AD***. Por lo tanto, LAPS hace más difícil para los agresores y ataques potenciales como por ejemplo de tipo ***worm malware***, poder moverse lateralmente a través de una organización infringida. Más información sobre LAPS se puede encontrar en: https://technet.microsoft.com/en-us/library/security/3062591.aspx

Aislamiento de Aplicaciones (Sandboxing)

El aislamiento de aplicaciones es un método de reclusión de aplicaciones para que sólo tengan acceso a un estricto conjunto de recursos que son estrictamente controlados, como memoria y espacio en el disco. Normalmente, se impide que aplicaciones aisladas puedan ejecutar cambios permanentes en el disco duro. Aplicaciones aisladas, como los navegadores Web y sus respectivos complementos, pueden ayudar a prevenir que ciertas formas de ***Ransomware*** puedan

impactar su sistema, ya que dicho aislamiento tiene un gran potencial, como es evitar que ***Ransomware*** tenga acceso a los archivos en el disco duro o compartimientos de la red.

Servidor NAS

La mayoría de organizaciones tienen unidades de almacenamiento compartidas, alojadas en algún tipo de dispositivo ***NAS (Network Access Server)*** que podría tener consecuencias afectadas por ***Ransomware***. Los mecanismos de protección que se enumeran a continuación se suman a todas las recomendaciones de protección, como actualizaciones y aplicación de parches completas, Antivirus, etc., descritos en la protección de dispositivos electrónicos.

Permisos de Archivo

Un principio común en la seguridad de la información es el de ***Privilegio Mínimo***, por el cual usuarios solo deben tener acceso a lo que se requiere para hacer su trabajo y nada más. Desafortunadamente en lo que respecta a las unidades de almacenamiento compartidas en red, no es infrecuente que muchas organizaciones experimenten fallas en la implementación de estos principios con el pasar del tiempo. El departamento de IT no siempre es informado apropiadamente cuando un empleado es transferido a un nuevo departamento o de alguna otra manera cambia roles dentro de una organización. Esto a menudo se traduce en permisos que se agregan para el nuevo rol, pero los permisos que ya no son necesarios de la antigua función no son removidos. Si bien es una buena práctica general de seguridad eliminar los permisos de acceso innecesarios, dado el aumento de ataques de ***Ransomware***, ahora es el momento pertinente para que toda organización realice auditorías enfocadas en los permisos de acceso a todos los recursos de archivos que son compartidos, y así garantizar que el principio de ***Privilegios Mínimos*** se haga cumplir. Es mucho más difícil para una infección de ***malware*** lograr la encriptación de archivos si el usuario no tiene acceso a dichos archivos en primer lugar. Por lo tanto, mientras que este control no puede prevenir un ataque de ***Ransomware***, puede ayudar grandemente con la mitigación de la cantidad de datos afectada en su organización.

Copias de Volumen Shadow Copy

Mientras que algunas variantes más nuevas de ***Ransomware*** tienen cierta capacidad de prevenir la restauración de datos desde copias almacenadas en un volumen ***Shadow Copy***, el tener copias instantáneas de datos tomadas en tiempos determinados, puede proporcionar una manera rápida de restaurar dichos datos en muchos casos. Windows admite capturas instantáneas en cualquier momento de datos almacenados, y la posibilidad de retrotraer versiones anteriores de archivos.

Capturas Instantáneas de Máquinas Virtuales

La Virtualización de un servidor de infraestructura es bastante común, pero también es posible proteger el servidor contra ***Ransomware***, mediante la toma de capturas instantáneas, a máquinas virtuales, programadas regularmente que pueden permitir regresar el estado de una máquina

virtual a un punto previo en el tiempo. Esto puede proporcionar una opción de recuperación alternativa en el caso de que un ataque ***Ransomware*** sea realidad.

Inventario de Datos

Tener un inventario de datos que sean clasificados dependiendo de qué tipo de información está almacenada en los archivos compartidos, es muy beneficioso, ya que puede ayudarle a seleccionar sus prioridades de recuperación y remediación. Por otra parte, versiones de ***malware*** que amenazan a víctimas con robar información privada para después promulgarla, también están apareciendo. Tener una idea clara de qué datos fueron cifrados o de otra manera afectados por el ***malware***, ayudará a la organización a evaluar mejor la amenaza del robo de información privada.

SIEM y Administración de Logs

Firewalls, servidores, dispositivos ***IDS***, filtros Web, dispositivos electrónicos, etc. generan todos datos de registro que pueden proporcionar pistas sobre un ataque de ***malware***. Tener una solución ***SIEM*** para supervisar y procesar estos registros, puede ayudar a proporcionar una indicación temprana de un posible brote de ***malware*** y, como tal, puede ayudar a mejorar los tiempos de respuesta. Tener estos datos colectados de forma centralizada, también puede ayudar en el análisis de los mismos, si un análisis de causa raíz necesita ser realizado más tarde.

Copias de Seguridad (Backup)

En el caso de un ataque, el método de recuperación de un ataque de ***Ransomware*** tendrá la presencia de planes apropiados para realizar copias de seguridad y una efectiva recuperación.

Copias de Seguridad y Plan de Recuperación

La organización debe tener un punto de recuperación y un objetivo sobre el tiempo que tomará la recuperación, bien definidos para cada activo, lo que les ayudará a determinar el tipo de tecnología y procedimientos necesarios para realizar copias de seguridad adecuados para su infraestructura en particular. Debe haber políticas y procedimientos claramente documentados para describir los horarios en que se realizarán las copias de seguridad, cómo se supone que los datos deben ser copiados o recuperados, quién es responsable por las copias de seguridad y el proceso de recuperación, etc. También vale la pena que los empleados sean entrenados en esta área.

Capturas Instantáneas de Almacenamiento de Datos

En la mayoría de infraestructuras de gran tamaño, el almacenamiento del servidor suele estar alojado en un ***SAN (Storage Area Network),*** y la mayoría de dispositivos ***SAN*** modernos permiten retener una o más capturas instantáneas de volúmenes de almacenamiento. Las capturas instantáneas de almacenamiento deben configurarse de modo que, si es necesario, un volumen se puede revertir a un estado anterior que se realizó antes del ataque. La frecuencia de las capturas

instantáneas debe determinarse de acuerdo con el punto de recuperación predeterminado y los objetivos de tiempo de recuperación de su organización.

Copias de Seguridad Fuera de Conexión

Aunque las tecnologías como la replicación en tiempo real entre dispositivos SAN y centros de datos son ideales para propósitos de continuidad de operaciones, no son muy útiles para recuperarse de un ataque de ***Ransomware,*** ya que son versiones cifradas de los archivos las que se replicarán rápidamente en otras ubicaciones. Para restaurar datos provenientes de una copia de seguridad correctamente, después de un ataque de ***Ransomware,*** estos se deben extraer del sistema sin conexión donde están almacenados, y sin haber sido alterados, para garantizar que los datos que se están recuperando no han sido sometidos a encriptación, o se hayan convertido en datos irrecuperables. Aunque no es tan atractivo como muchos sistemas recientes de copias de seguridad basados en discos más nuevos, cassette también puede seguir sirviendo como un medio de copia de seguridad ideal para almacenar múltiples copias instantáneas históricas por unidad de tiempo en su infraestructura. La frecuencia para realizar copias de seguridad, debe determinarse de acuerdo a puntos de recuperación predeterminados, y los objetivos de tiempo de recuperación de su organización.

Pruebas de Copias de Seguridad y Recuperación

Los planes de recuperación de desastres a menudo se dejan olvidados en el camino, hasta que un desastre se hace realidad, lo que puede ser un gran error. Copias de Seguridad y métodos de recuperación deben ser probados exitosamente en un programa de rutina, para asegurar que todos los sistemas funcionen correctamente, y que los miembros del personal estén suficientemente informados para operar dichos sistemas. No desearía descubrir que la copia de seguridad de uno de sus servidores críticos, no estaba siendo correctamente realizada, justamente después de un ataque de ***Ransomware*** u otro desastre. Las pruebas de rutina también mejorarán el tiempo de recuperación en caso de que realmente ocurra un desastre.

Entrenamiento para Concientizar Usuarios

A pesar de contar con muchos mecanismos de protección, la realidad es que todavía es posible que un correo malintencionado o un enlace malicioso penetre, y dicha situación se le presente a un usuario. En este caso, mientras que el Antivirus, las políticas de restricción de software, y otras defensas en dispositivos electrónicos aún pueden servir de protección, la mejor defensa es contar con un usuario bien educado, que sea capaz de reconocer un correo electrónico sospechoso y reportarlo al departamento de IT para lograr una investigación de manera oportuna. Cuanto antes se denuncien tales indicaciones sospechosas, más pronto podrán ser bloqueadas en el perímetro, de inmediato se pueden contactar compañías de Antivirus para actualizar sus diccionarios, y así desplegar defensas para ayudar a detener la propagación de la amenaza en toda la organización.

Malware en Cosas del Internet (IoT - Internet Of Things)

Malware en Cosas del Internet como ***Mirai*** y ***Brickerbot***, han ilustrado el potencial de compromiso sobre dispositivos electrónicos ***IoT,*** al igual que sucede con cualquier otro dispositivo de computación habilitado en la red. Los siguientes controles no son una lista completa de controles de seguridad de ***IoT***, sino una lista de los controles de seguridad que con mayor probabilidad pueden ayudar con la prevención, mitigación y corrección de un ataque de ***Ransomware***. Esta sección solo cubrirá controles que se aplican en dispositivos ***IoT***. Los controles de red, etc., tales como la segmentación de la red, son fundamentales para la seguridad adecuada de dispositivos ***IoT***, pero han sido mencionados en otras secciones.

Evitar Credenciales Predeterminadas

Hasta la fecha, el vector más común de ataque para el comprometer dispositivos ***IoT***, ha sido el uso de Credenciales Predeterminadas por el fabricante, como en el caso de ***Mirai***, donde se utilizó una lista de 62 pares de nombres de usuarios y sus contraseñas, para comprometer cientos de miles de dispositivos electrónicos. En pocas palabras, el cambio de la contraseña predeterminada en su dispositivo ***IoT,*** ayudará a prevenir las numerosas tensiones provocadas por ataques de ***Malware*** actuales que apuntan a dispositivos ***IoT***.

Bloqueos de Cuentas de Acceso

Dada la prevalencia de ***Malware*** contra dispositivos ***IoT*** que utilizan ataques de adivinación de contraseña, la configuración de directivas de bloqueo de cuentas, es imprescindible siempre que sea posible, pues puede ayudar a detener muchas variantes de este tipo de ***Malware***. El acceso debe ser restringido después de 3 o más intentos fallidos.

Copia de Repuesto del Firmware

En caso de que un dispositivo electrónico esté infectado, contar con una copia de repuesto del ***Firmware*** de estos dispositivos, o una forma de restablecer el dispositivo a un estado similar a “como nuevo”, puede ser esencial para devolver el dispositivo a su condición original y a un estado funcional.

Configuración de las Copias de Seguridad

Relacionado con el control anterior, tener todas las configuraciones específicamente personalizadas y todo tipo de ajustes almacenados con copias de seguridad, puede ser crítico para restaurar rápidamente un dispositivo electrónico a un estado funcional.

Interfaz de Administración Restringida

Las interfaces de manejo de gestiones de administración deben estar separadas de las interfaces que interactúan con el Internet, siempre que sea posible, y esta interfaz, debe estar situada en un segmento de red completamente aislado. El acceso de Administrador debe estar restringido a la interfaz de administración siempre que sea factible.

Mecanismos de Actualización

Todos los dispositivos electrónicos ***IoT*** deben estar configurados para recibir actualizaciones regularmente, y asegurarse de que dichos dispositivos siempre estén utilizando la versión de ***Firmware*** más reciente que esté disponible.

Manejo de Vulnerabilidades

Todas organización debe implementar un programa integral sobre gestión de vulnerabilidades, diseñado para identificar todos los sistemas de información (dispositivos electrónicos, servidores, IoT, etc.) que no han recibido los parches adecuados, y que no cumplen con las políticas de seguridad definidas por la organización. El programa debe incluir disposiciones para realizar acciones correctivas dentro de un período de tiempo finito, con el objetivo principal de reducir la superficie de ataque en la organización, lo cuál se logrará con el tiempo. Las iniciativas de gestión de la vulnerabilidad deben incluir disposiciones para el monitoreo continuo, para así lograr que toda vulnerabilidad, pueda ser identificada y mitigada a medida que surja.

Respuesta a Incidentes

Aunque esperamos que todas las recomendaciones de defensa mencionadas anteriormente mantengan incidentes al mínimo, las organización debe estar preparada para el hecho real, de que no importa qué tan bien configurados estén los controles de seguridad, un incidente de ***Ransomware*** es siempre una posibilidad.

Planes de Respuesta a Incidentes

Una de las peores prácticas que una organización puede promover, es esperar hasta que ocurra un incidente para empezar a pensar en cómo lidiar con ello. Las organizaciones deben tener un plan completamente establecido que defina cómo reaccionarán ante un incidente, y quién será responsable de qué acciones durante las fases de detección, contención, erradicación y recuperación. También es importante que todo el personal sea educado a conciencia sobre el Plan de Respuesta, y que esté capacitado para responder apropiada y eficazmente. Para organizaciones sin ningún tipo de plan de respuesta a incidentes, un buen recurso de partida es: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Incidentes Simulados

Cuando ocurre un incidente, la mejor manera de mitigar el daño es detectar y contener el incidente lo más rápido posible. La mejor manera de hacer esto es probar rutinariamente su plan de respuesta a incidentes para ver cómo las personas dentro de su organización responden a un incidente simulado. Si bien hay muchos incidentes de simulacro que podrían llevarse a cabo, algunos recomendados como punto de partida incluirían campañas de correos electrónicos con ataques de tipo ***phishing*** contra empleados, y un ataque de ***Malware*** simulado, que se puede realizar con seguridad y confidencia, utilizando una prueba ***EICAR***, la cual es una prueba de respuesta ante los programas Antivirus instalados en equipos.

Recuperación de Datos

Si ocurre un desastre, es mejor poder recuperar sus datos y aplicaciones obteniéndolos de una copia de seguridad que no ha sido afectada por un incidente, que a través de un proceso de descifrado, ya que esto ayudará mejor a asegurar un sistema totalmente limpio en el futuro, aunque se sabe que no siempre es posible. Si usted se convierte en una víctima de ***Ransomware***, y está atrapado sin una copia de seguridad de sus datos, puede valer la pena revisar el sitio Web ***www.nomoreransom.org*** que ofrece la detección de variantes de ***Ransomware*** basado en la descarga de un archivo de ejemplo, y también aloja las claves de descifrado de varios de los ataques conocidos como ***Wildfire***, ***Quimera***, ***Teslacrypt***, ***Sombra***, ***Coinvault***, ***Rannoh*** y ***Raknhi***.

Seguro

Un número cada vez mayor de empresas está transfiriendo algunos de sus riesgos cibernéticos a las compañías de seguros mediante la adopción de políticas contra las violaciones de datos. Algunas compañías de seguros ahora proporcionan políticas o provisiones dentro de sus políticas que tratan particularmente con los ataques de ***Ransomware***. Las empresas de industrias fuertemente atacadas y consideradas como objetivos grandes, tal vez deseen considerar la posibilidad de tomar políticas que cubren tales ataques, o determinar si sus políticas existentes cubrirán los ataques de ***Ransomware***.

Indicadores de Compromiso

Los indicadores de compromiso pueden ser útiles para determinar si un sistema ha sido expuesto o afectado por ***Malware***. Un buen recurso sobre indicadores de compromiso para la mayoría de variantes de ***Ransomware*** se puede encontrar aquí: http://goo.gl/b9R8DE