ROADMAP DE MEDIDAS DE SEGURIDAD PARA LA EMPRESA

No cabe ninguna duda de que la securización de la infraestructura IT de nuestra organización es una exigencia de cara a asegurar la continuidad de la misma. Ninguna organización que desee seguir desarrollando su actividad en el futuro puede obviar el establecimiento de medidas de protección de su infraestructura IT.

En los últimos años, son constantes las noticias en las que se evidencia el peligro que puede suponer para cualquier organización ser víctima de un ataque informático: pérdidas económicas, daños en la imagen, filtración de información confidencial,... El 80% de las organizaciones a nivel mundial consideran la ciberseguridad como uno de los principales riesgos para sus empresas. Más del 40% de estas organizaciones han sufrido ciberataques en el último año, lo que supone un coste medio por incidente de 67.000 dólares para la empresa y no todas logran recuperarse.

No solo se trata de proteger el perímetro de red de la compañía, sino que también debemos preocuparnos de la protección de los endpoints y servidores, la identidad, las aplicaciones y los datos, entre otros.

Dada esta cantidad de factores, y teniendo en cuenta que la seguridad debe ser una constante en el despliegue y mantenimiento de infraestructuras IT, no un proceso aislado en el tiempo, puede resultar complicado determinar cuál es el punto de inicio por el que deben comenzarse las acciones de mejora del estado de ciberseguridad de la organización, si bien de manera general podemos establecer unas fases de madurez con acciones concretas en cada una de ellas que nos permiten establecer objetivos y obtener resultados de manera cercana:

FASE 1. INICIAL

En esta primera fase o fase inicial, nuestra compañía necesita evidenciar en qué punto se encuentra en cuanto a ciberseguridad, es decir, cuál es su nivel de exposición a riesgos de seguridad. Además, en esta fase se desplegarán también medidas para mejorar la protección, así como para asegurar el cumplimiento normativo.

AUDITORÍA DE SEGURIDAD

Dentro de las posibles auditorías de seguridad, podemos **destacar las 3 siguientes**, necesarias en cualquier organización independientemente de su tamaño o sector:

AUDITORÍA DE VULNERABILIDADES

Realizando este tipo de análisis sobre nuestros servidores o incluso endpoints, obtendremos un informe en el que se reflejará cuan vulnerables son ante ataques de seguridad.

A partir de este informe, podremos iniciar las acciones de securización tomando el reporte como guía que nos indique la prioridad con la que realizarlas.

AUDITORÍA DE TRÁFICO DE RED

Esta auditoría nos permitirá detectar qué tipo de comunicaciones se están estableciendo en nuestra red: qué servicios externos están siendo utilizados por empleados de la compañía (Dropbox, Google Drive, redes sociales...), con que servidores se establecen las comunicaciones (servidores de correo no autorizados, comunicaciones ocultas a través de proxy o VPNs), o incluso qué tráfico externo está accediendo a nuestra red.

AUDITORÍA DE SITIO WEB

La web de una compañía es su cara visible para millones de potenciales visitantes.

Por ello es importante auditarla de cara a obtener posibles vulnerabilidades que puedan poner en riesgo su integridad, y por tanto comprometan nuestra imagen de empresa.

CUMPLIMIENTO NORMATIVO

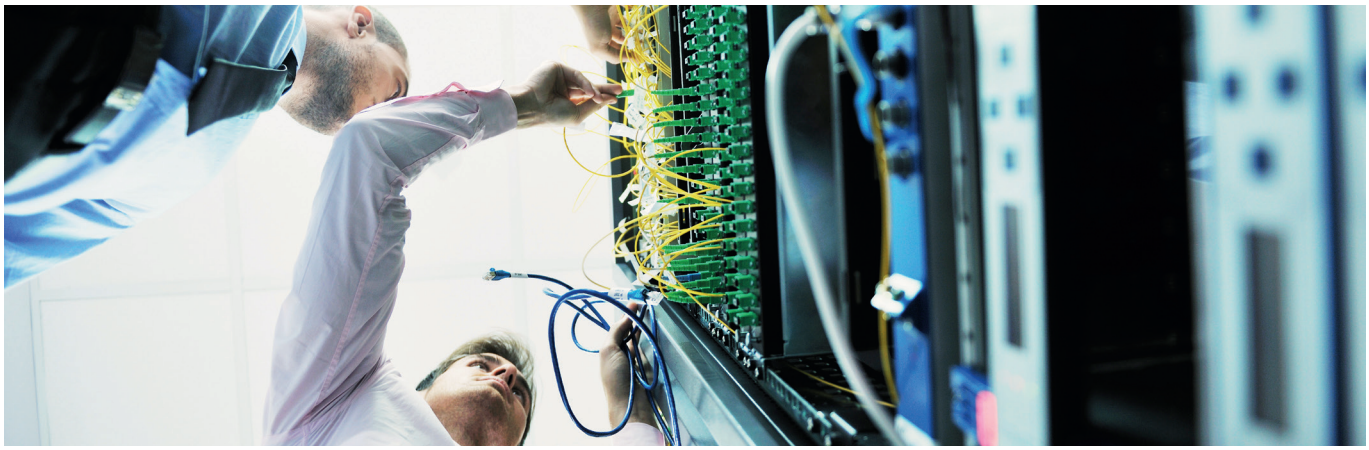
Cuando hablamos de seguridad, no solamente hablamos de acciones puramente técnicas, también deben tenerse en cuenta las cuestiones relativas a normas y estándares que nuestra organización debe seguir para mejorar su seguridad. Todas las organizaciones necesitan cumplir con distintos reglamentos y leyes, concretamente en Europa, todas aquellas empresas, organizaciones, organismos e instituciones que hagan tratamiento de datos catalogados como de carácter personal deben cumplir con el **Reglamento General de Protección de Datos (GDPR).** Por ello, en la fase inicial deben asegurarse que estamos adecuados a GDPR, dadas las importantes consecuencias que puede suponer el no cumplir con este reglamento. Para ello se pueden realizar las siguientes acciones:

- Auditoría previa de estado de adecuación a GDPR.
- Servicios de adecuación a GDPR.
- Sesiones de concienciación a los empleados.
- Mantenimiento periódico.
- Software de gestión de GDPR.

Por otro lado, de cara a las relaciones con organismos oficiales debemos contar con la certificación en el **Esquema Nacional de Seguridad (ENS)**. Se trata de una legislación que viene a regular la seguridad en la utilización de medios electrónicos por parte de Organismos Públicos. Para la implantación de ENS podríamos destacar las siguientes tareas:

- Definición de políticas de seguridad.
- Análisis de riesgos.
- Asesoramiento en la implantación de las medidas de seguridad.
- Servicios de auditoría.
- Mantenimiento periódico.

PROTECCIÓN DE ENDPOINTS Y SERVIDORES



Los equipos endpoints y servidores son utilizados a diario de manera directa o indirecta por los usuarios de nuestras organizaciones. En ellos se almacenan datos de vital importancia para la organización, y su disponibilidad es totalmente necesaria para el normal funcionamiento de la compañía. Por ello, debemos asegurar que no se encuentran comprometidos y disponer de herramientas de respuesta si se ven afectados por algún tipo de compromiso de seguridad. Algunas de las medidas que podemos desplegar en esta fase inicial son:

- **SOLUCIÓN AVANZADA DE PROTECCIÓN DE ENDPOINTS Y SERVIDORES:** nuestros equipos deben estar fortificados con una solución de protección que les permita detectar y detener incidentes de seguridad. Las soluciones antivirus tradicionales ya no son suficientes para detectar algunas de las amenazas más avanzadas, de manera que debemos confiar en soluciones que incluyan aprendizaje automático de manera que no solo dependan de una base de firmas. Además, es de vital importancia contar con una consola central en la que revisar el estado de protección de cada uno de los equipos. **Sophos Intercept X** es una de ellas, se trata de una solución especializada en detección de malware, prevención de exploits y en detener los ataques de ransomware si llegan a producirse. Intercept X incorpora CryptoGuard, una tecnología que permite detectar que se está sufriendo un ataque de ransomware, y al detectarlo lo detiene y revierte los archivos del equipo a su estado original antes del ataque.

- **HARDENING DE SERVIDORES:** las acciones de hardening o fortificación de servidores están orientadas a reducir su exposición a incidentes de seguridad, mediante el establecimiento de configuraciones y políticas que reduzcan los posibles agujeros de seguridad que puedan existir en ellos.

- **SECURIZACIÓN DEL ENTORNO DE DOMINIO:** Microsoft Active Directory es uno de los servicios de directorio más extendidos a nivel global. La aplicación de políticas de seguridad adecuadas de manera centralizada puede ayudar a reducir considerablemente la exposición los equipos del dominio a amenazas de seguridad. Además, al tratarse del punto central de identidad, autenticación y autorización de nuestros usuarios, deben aplicarse sobre nuestros dominios medidas de fortificación.

SEGURIDAD APLICADA A OFFICE 365

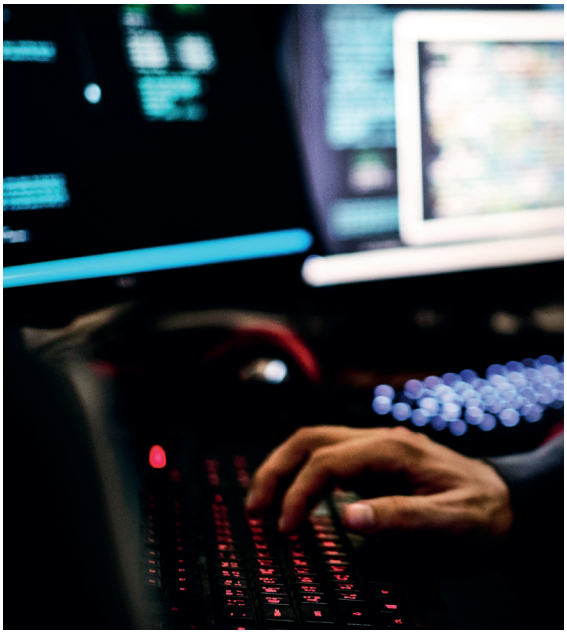
Office 365 es la plataforma de productividad en cloud que incluye servicios y aplicaciones que nos permiten trabajar de manera productiva, colaborativa y descentralizada; además incluye herramientas de análisis e inteligencia que nos permiten la supervisión de datos en tiempo real y posibilitan su análisis.

Para Office 365, la seguridad es un pilar fundamental de su solución, de manera que incluye medidas de seguridad por defecto, si bien también permite establecer líneas adicionales de securización del tenant. En primer lugar, debe realizarse un análisis del estado de seguridad del tenant, para a continuación establecer una serie de medidas que incrementen la protección del mismo.

FORTIFICA TU RED

Toda compañía, independientemente de su tamaño, debe disponer de una solución firewall que, además de las tradicionales funciones de control del tráfico de entrada y de salida de la red, permita:

- Detectar el tráfico por aplicaciones concretas y establecer reglas basadas en aplicación.
- Filtrado web para detección de amenazas en la navegación HTTP y HTTPs.
- Contar con el soporte de base de datos del fabricante, que permita disponer de información actualizada sobre reputación de IPs o sitios con las que se establezca comunicación.
- Incluyan detección de intrusiones.
- Establecer VPNs que permitan el acceso a los recursos de la organización externamente, evitando la exposición pública de los recursos de nuestra empresa.



Las distintas soluciones firewall de **Fortinet** incorporan estas y otras características adicionales, protegiendo el perímetro de red y detectando compromisos en el tráfico de nuestra organización.

FORMACIÓN Y CONCIENCIACIÓN DE USUARIOS

Una de las frases más recurrentes cuando se tratan temas de seguridad informática es "La fortaleza de una cadena es igual a la fortaleza de su eslabón más débil", con esto planteamos que, a pesar de que podamos contar con medidas técnicas avanzadas para la protección de la información, si los usuarios de la organización no están formados en buenas prácticas de seguridad y en cómo hacer un tratamiento adecuado de la información, estaremos ampliamente expuestos a sufrir incidentes de seguridad. Para conseguir que nuestros usuarios realicen un correcto manejo de la información, existen las siguientes posibilidades:

- Realización de formaciones dinámicas presenciales de concienciación para los usuarios.
- Inscripción a plataformas online en las que los usuarios aprenderán las distintas amenazas de seguridad existentes y como protegerse ante ellas.
- Realización de campañas de phising dirigidas para evaluar el grado de concienciación de los usuarios ante las distintas amenazas provenientes de correo electrónico.

FASE 2. INTERMEDIA

Para comenzar esta fase debemos contar con una visión general del estado de seguridad de nuestra organización, y haber implementado medidas que permitan que permitan un cierto control de cumplimiento de nuestra infraestructura IT. Durante esta fase intermedia, podrían desplegarse las siguientes medidas:

PROTECCIÓN DEL DATO

La información es uno de los activos más importantes para cualquier empresa, que se vea comprometida o incluso sustraída por un tercero puede tener consecuencias fatales para la organización. Por eso es necesario establecer medidas de protección directamente sobre la información, más allá de solo proteger la ubicación de la misma. Con **Azure Information Protection (AIP)** podemos proteger la información independientemente de su ubicación, ya que la seguridad se encuentra localizada en el propio documento, de tal manera que, si un tercero llega a conseguir un documento de nuestra empresa, no podrá abrirlo si no le hemos dado permisos.

AIP nos permite clasificar, etiquetar y proteger la información, quedando custodiada durante su ciclo de vida,pudiendo hacer el seguimiento de quién ha accedido a la información, así como revocar un acceso concedido con anterioridad. AIP se integra además con nuestros servidores de ficheros on premise, permitiendo establecer la protección de forma automática.

Por su parte, las políticas de **DLP** de Office 365 permite detectar fugas de información de la organización, reportando cuando se producen o incluso impidiendo la salida de la información confidencial. Podemos establecer patrones de información consideradas sensibles y en base a ellos crear reglas que definan si se permite o no su salida de la organización.

ESTÁNDARES E ISOS

Con el objetivo de garantizar la confidencialidad, integridad y autenticidad de la información, existen múltiples normas e ISOs que nos marcan las directrices que la organización debe seguir. La implementación de una de estas ISOs facilitará a las empresas las labores de gestión de la seguridad, y además contar con uno de ellos puede suponer un punto diferencial para nuestra empresa de cara a demostrar la calidad de nuestras operaciones frente a clientes y competidores. Algunas ISOs de seguridad destacables son:

- ISO 27001
- ISO 22301
- ISO 27017

PLANES DE CONTINUIDAD DE NEGOCIO

La continuidad de negocio es un punto vital en todas las organizaciones con el objeto de estar preparadas para poder continuar su operativa en el caso de que sufran una catástrofe en sus sistemas de información.

Disponiendo de un plan de continuidad de negocio, así como procedimientos de continuidad y recuperación para cada uno de los activos y servicios, podremos minimizar el impacto de un imprevisto en la organización y poder seguir dando servicio y evitar posibles pérdidas.

PROTECCIÓN Y GESTIÓN CENTRALIZADA DE EQUIPOS Y SERVIDORES

Cuando integramos el parqué de endpoints y servidores de nuestra compañía en una solución de configuración y gestión centralizada como SCCM de Microsoft obtenemos grandes ventajas en la gestión y unificación de los dispositivos. Algunas de las características de esta solución:

- Dispondremos de un inventario de las máquinas de la organización en tiempo real, pudiendo acceder a información avanzada sobre las mismas.
- Establecimiento de líneas bases de configuración.
- Gestionaremos de manera sencilla el despliegue de parches de seguridad y de aplicaciones.
- Podremos realizar plataformados de equipos de manera eficiente.
- Obtención de informes de seguridad.

EXTENDIENDO LA CAPACIDAD DE ANÁLISIS DE NUESTRO FORTINET

FortiAnalyzer es la solución de Fortinet que nos permitirá potencias las capacidades de detección de compromisos de nuestros firewalls Fortinet, ya que recogerá, analizará y correlacionará los eventos de seguridad que se produzcan en los distintos firewalls.

FortiAnalyzer generará alertas cuando detecte incidentes de seguridad, y también podremos obtener reportes de distintos indicadores de seguridad de la red.

PROTECCIÓN DE DISPOSITIVOS MÓVILES

En los móviles y tablets de los trabajadores de la organización, se procesa y almacena información perteneciente a la empresa. De cara a asegurar que estos dispositivos no se vean comprometidos, debemos confían en una solución de administración de movilidad empresarial que nos permita:

- Disponer de inventario de hardware y aplicaciones de los dispositivos.
- Ejecutar borrado, bloqueo y otras operaciones de administración remota.
- Aplicar políticas de restricciones de funciones y de aplicaciones.
- Establecer líneas bases de seguridad.
- Proporcionar catálogo de aplicaciones a los usuarios.
- Obtener informes avanzados de los dispositivos.

IBM Maas360 with Watson e **Intune de Microsoft** son 2 soluciones EMM (Enterprise Mobility Management) que nos permitirán llevar a cabo estas funciones, recuperando el control de los dispositivos de movilidad.

FASE 3. MADUREZ

Para comenzar esta fase debemos contar con una visión general del estado de seguridad de nuestra organización, y haber implementado medidas que permitan que permitan un cierto control de cumplimiento de nuestra infraestructura IT. Durante esta fase intermedia, podrían desplegarse las siguientes medidas:

CONSOLA SIEM

Disponer de una consola SIEM nos permitirá detectar compromisos de seguridad en nuestra organización mediante el análisis y correlación de los eventos de seguridad de los dispositivos de la red, así como del tráfico que fluye por ella.

IBM QRadar es la solución SIEM líder en el cuadrante de Gartner durante más de 6 años, la cual nos permitirá disponer de las siguientes capacidades:

- Disponemos de un punto centralizado con los eventos de seguridad de tal manera que se facilita la gestión y se optimiza la detección.

- Nos permite tanto el análisis de eventos de seguridad (logs) de los servidores y dispositivos de red, como análisis de los flujos de tráfico de red, escalando la potencia de detección frente a otras soluciones.

- Soporte nativo de gran cantidad de orígenes de datos.

- Explotación de información ya existente. No necesitamos generar nuevas fuentes de datos, los dispositivos de nuestra red ya contienen la información de seguridad que necesitamos.

- Correlación de las distintas fuentes. IBM QRadar nos permitirá correlacionar los eventos de distintos dispositivos entre sí, así como con los flujos de red, de manera que se amplía sustancialmente la capacidad de detección de APT, entre otras amenazas.

- Uso de información histórica. Además de la información en tiempo real, QRadar nos permite almacenar durante un tiempo definido toda la información recibida, de tal manera que se puede estudiar con posterioridad si es necesaria su investigación.

- Bases de datos de IBM X-Force Exchange: la plataforma de inteligencia de seguridad de IBM permite hacer todavía más potente a QRadar con la obtención de información actualizada de amenazas de seguridad a nivel mundial.

- Personalización de los casos de uso. Además de un elevado número de casos de uso definidos desde el inicio del despliegue, QRadar permite la creación de casos de uso personalizados, ajustándolos a las peculiaridades de nuestra organización.

- App Exchange de IBM X-Force Exchange: existen a nuestra disposición más de cien aplicaciones que posibilitan una mayor integración de QRadar con los dispositivos de red, como, por ejemplo, con fabricantes como Fortinet, Palo Alto o Microsoft.

- Posibilidad de generar alertas y respuestas. Ante la detección de un compromiso de seguridad, QRadar puede generar una alerta e incluso una respuesta para detener la amenaza.

- QRadar incorpora un módulo de análisis de comportamiento de usuarios (UBA) que nos permitirá detectar compromisos en las cuentas de usuario de nuestra organización.

Como se indica al principio de este documento, la seguridad debe ser un factor constante en el despliegue, mantenimiento y uso de las infraestructuras IT de toda organización, no basta con implementar medidas en un momento dado.

Por ello, alcanzar la fase 3 no supone que 'hayamos terminado nuestro trabajo', es necesario realizar un seguimiento constante y preciso de la seguridad de nuestra compañía, así como adaptarlo a las nuevas necesidades y amenazas que surjan.

internet y tecnología

www.efor.es
976 46 76 76
marketing@efor.es