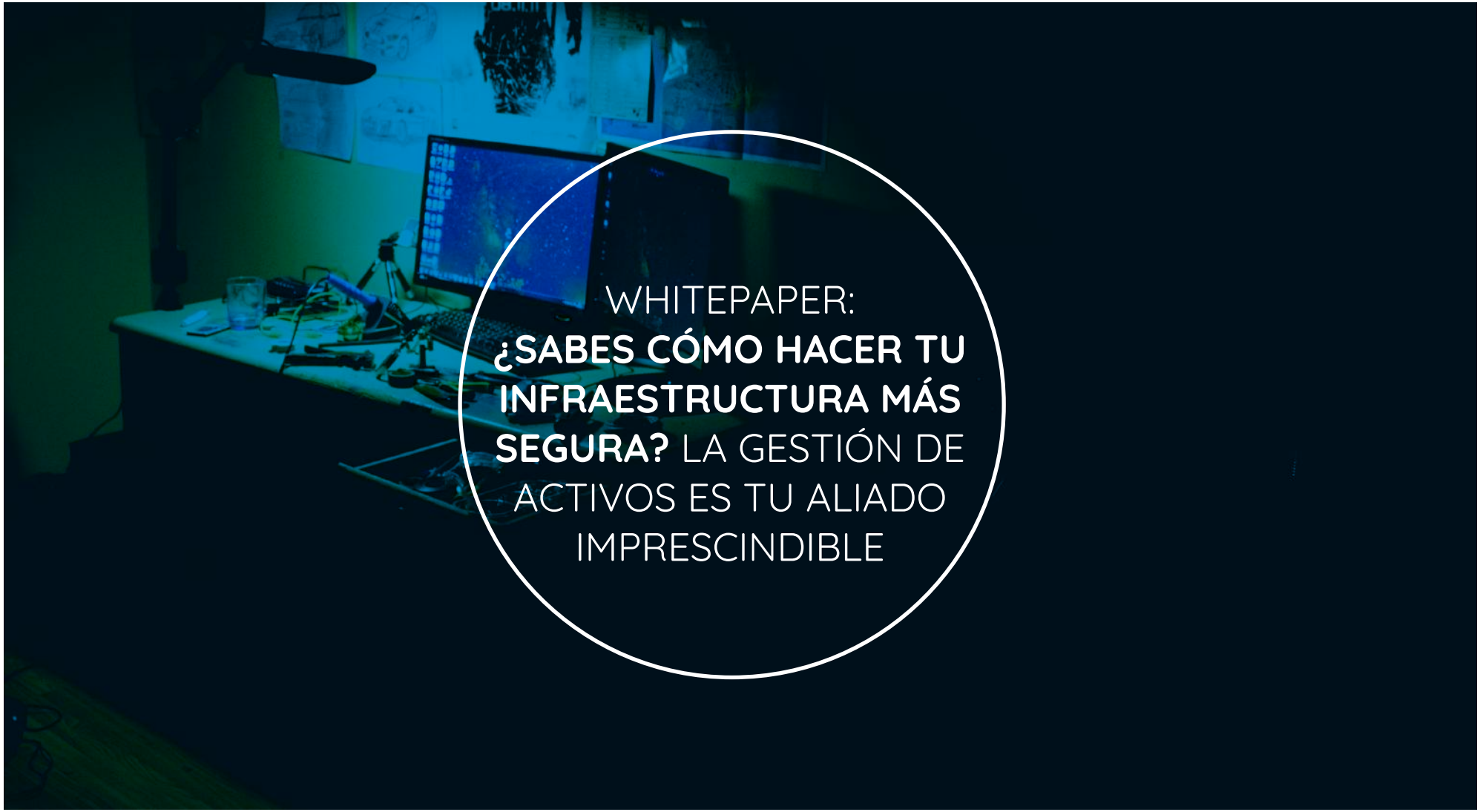
proactivanet

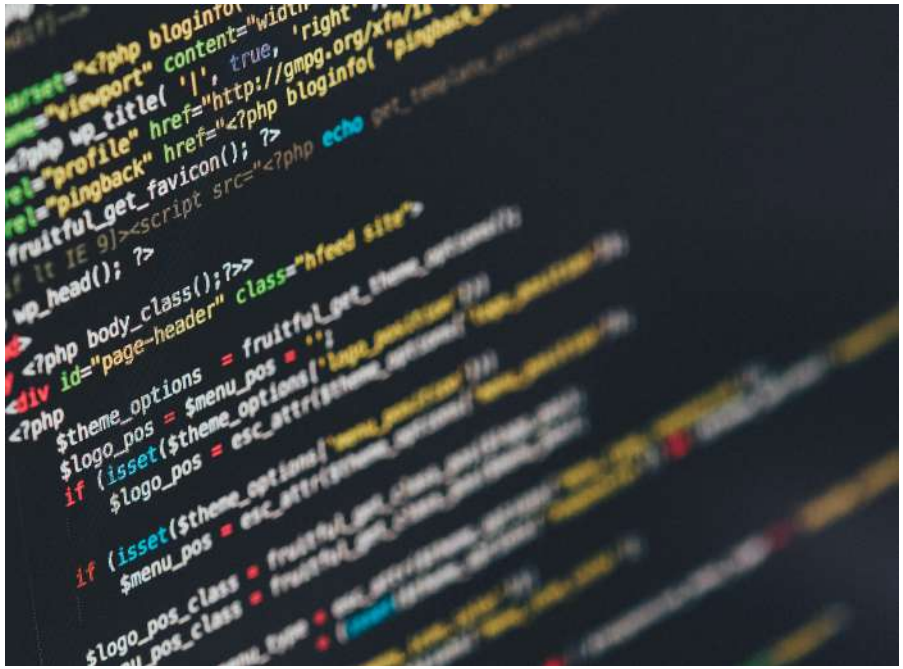


WHITEPAPER:

¿SABES CÓMO HACER TU INFRAESTRUCTURA MÁS SEGURA? LA GESTIÓN DE ACTIVOS ES TU ALIADO IMPRESCINDIBLE

proactivanet.com

La seguridad está entre las mayores preocupaciones que actualmente tienen en la cabeza los CIOs (y, obviamente, CISOs). La pandemia ha generado y sigue generando una situación en la que el teletrabajo (WAH, *Work At Home*) se ha multiplicado exponencialmente, exprimiendo al máximo la capacidad de nuestras organizaciones, y por supuesto, también de nuestras infraestructuras. Es como una gran prueba de estrés para las capacidades de todos los departamentos de la organización, pero muy especialmente para las TI, que son las grandes habilitadoras de ese nuevo milagro que es el poder trabajar desde la comodidad de nuestras casas.



Nuestra casa: entorno hostil para la TI corporativa

Las redes corporativas han salido de su zona de confort de la noche a la mañana, estirando los cables de red hasta el salón de nuestras casas, con la comodidad para el trabajador, pero también los riesgos para la seguridad que ello representa. Nuestras casas pueden ser lugares plácidos y seguros donde vivir, pero no lo son tanto para las TI corporativas. PCs no controlados, consolas de videojuegos conectadas a internet, móviles y tabletas, todo tipo de dispositivos IoT (cámaras de seguridad, aspiradoras, robots de cocina,...) representan un caldo de cultivo estupendo para facilitar un ciberataque a la organización utilizando nuestras casas como trampolín.

La ingeniería social es sin duda uno de los grandes vectores de ataque (ya lo era, y con la crisis del COVID-19 se ha disparado aún más), pero no menospreciemos las vulnerabilidades propias de la infraestructura corporativa al sacarla del lugar seguro que era la red interna, y llevarla al entorno potencialmente hostil de la red doméstica.

> **“El 60% de los PCs domésticos están infectados con algún tipo de malware”**

Fuente: Estudio sobre la ciberseguridad y confianza del ciudadano en la Red (abril 2020). ONTSI.

“El 50% de las WIFIs domésticas no cuentan con ningún tipo de contraseña”

Fuente: 2020 User Risk Report. Proofpoint.

Solo un ejemplo nada descabellado: supongamos un equipo corporativo con Windows 7 (aún los hay a miles), conectado a la red corporativa mediante VPN a través de una red doméstica, en donde otro equipo (quizá sin antivirus ni firewall) se descarga “cosas” de internet desde páginas y redes P2P de más que dudosa seguridad. La probabilidad de que ese equipo doméstico acabe infectado es elevadísima. Pero ese equipo está “en la IP de al lado” a la de nuestro equipo corporativo, que hay que recordar tiene un sistema operativo que ya está fuera del ciclo de vida de Microsoft, y que por lo tanto, no recibe parches de seguridad. Además, ese equipo corporativo, ¿cómo tendrá de actualizado el antivirus? ¿Y el firewall estará activo? ¿Y el escritorio remoto lo tendrá desactivado o seguirá activado desde que se configuró a modo de emergencia durante el anterior confinamiento?

No podemos controlar la seguridad de las redes domésticas de los usuarios TI corporativos (aunque no estaría mal al menos ejecutar alguna labor de concienciación). Pero lo que sí podemos (y debemos) hacer, es poner todo lo que esté en nuestra mano para que los equipos corporativos, que se conectan cada día a esas redes potencialmente inseguras, sí sean lo más seguros posible.

Los primeros pasos son mucho más sencillos de lo que parece

Los primeros pasos para tratar de hacer de nuestra red un lugar un poco más seguro pueden asustarnos un poco (de hecho, ¡¡lo hacen!!). El alcance de la ciberseguridad es enorme, y cada día crece más (si las redes crecen, y cada vez hay más dispositivos de más tipos conectados a esas redes, es obvio que el ámbito de la ciberseguridad seguirá creciendo de manera acorde).

Pero lo más importante para empezar, es no tener miedo, y entender que nadie nació aprendido, ni que tampoco hay que comerse la tarta de un solo bocado. Siguiendo los principios de ITIL 4, nada mejor que “*start where you are*” y “*progress iteratively with feedback*” pero siempre “*keep it simple and practical*”. O lo que es lo mismo, analizar la situación actual, e ir avanzando poco a poco, de manera sencilla e iterativa, sin complicarnos demasiado (al menos al comienzo).

Con esa misma idea de avanzar de manera iterativa, práctica y sencilla, el *Center for Internet Security* (CIS), plantea un conjunto de 20 controles que nos ayudarán, de manera gradual, a conseguir mayor seguridad para nuestras infraestructuras. Esos controles se agrupan en tres niveles de madurez:

proactivanet

CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

> **Start by taking care of the basics: build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges and a quick patching process.**

Zurich Insurance Group
Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures
Switzerland

Fuente. CIs (Center for Internet Security)

Lo que no se conoce no se puede hacer más seguro.

Lo ideal es ir avanzando y terminar implementando todos (o casi todos) los controles. Pero como en todo, hay que empezar por orden, y no tiene sentido comenzar la casa por el tejado. Así que empezando por el principio, ¿cuáles son los primeros controles que plantea implementar el CIS?

1. INVENTARIAR Y CONTROLAR LOS ACTIVOS HARDWARE

Main Points:

- Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
- Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.

2. INVENTARIAR Y CONTROLAR LOS ACTIVOS DE SOFTWARE

Main Points:

- Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.

Fuente. CIs (Center for Internet Security)

DIMENSIONAR LA MAGNITUD DE LA TRAGEDIA

Con los dos primeros controles del CIS no estamos haciendo otra que "dimensionar la magnitud de la tragedia" (o al menos parte de ella). Con esos dos controles no se están cubriendo todos los aspectos a considerar bajo el paraguas de la ciberseguridad, pero sí un muy elevado porcentaje de ellos. Y como todo, es un punto de partida con el que empezar a ponerse en movimiento. A partir de esos controles, según vayamos ganando madurez, iremos profundizando mucho más en aquellos aspectos que más nos preocupen, y en donde más riesgos hayamos identificado.

Y es que conocer qué tenemos, dónde, cómo, quién lo usa, en qué estado está,... ayudará a establecer una hoja de ruta hacia una mayor seguridad de la infraestructura. ¿Por dónde empezar si no sabes lo que tienes? ¿Dónde tenemos más dificultades si desconocemos cuál es realmente nuestro parque?

Lo que no se conoce no se puede hacer más seguro. Así que está claro, el primer paso (o los dos primeros según el CIS), es contar con un inventario (muy) detallado de todo nuestro hardware y software.

GESTIÓN DE ACTIVOS TI:
MUCHO MÁS QUE SOLO UN INVENTARIO, UN ALIADO IMPRESCINDIBLE PARA LA SEGURIDAD

Pero aunque la Gestión de Activos Hardware y Software sea el punto de partida para seguir implementando controles de seguridad, ese "simple" inventario ya debería generar información detallada sobre la situación actual, e incluso plantear las primeras líneas de actuación imprescindibles.

> **La Gestión de Activos TI evidenciará más de un "*must-have para ayer*", sin necesidad de realizar grandes consultorías y escaneos específicos.**

¿Cuáles son, entre otras muchas, estas 10 grandes aportaciones que un sistema de Gestión de Activos TI ofrece de manera inmediata para ayudar a mejorar la seguridad de la infraestructura?

1. INVENTARIO COMPLETO AL 110%
2. SISTEMAS OPERATIVOS FUERA DEL CICLO DE VIDA
3. SISTEMAS OPERATIVOS "MODERNOS", PERO SIN PARCHEAR
4. EQUIPOS SIN FIREWALL O ANTIVIRUS
5. EQUIPOS CON SOFTWARE OBSOLETO
6. BASES DE DATOS ANTIGUAS
7. EQUIPOS CON SERVICIOS "SENSIBLES"
8. DISPOSITIVOS DE RED CON FIRMWARE SIN ACTUALIZAR
9. DISPOSITIVOS MÓVILES CORPORATIVOS Y BYOD CONECTADOS A LA RED
10. USUARIOS ACTIVOS E HISTÓRICO DE ACCESOS

1

INVENTARIO COMPLETO AL 110%

Ya lo hemos dicho, lo que no se conoce no se puede hacer más seguro, y la experiencia nos dice que el porcentaje de infraestructura desconocida no es en absoluto despreciable. Y es precisamente en esa parte "oculta" de la red en donde pueden surgir muchos más problemas de lo previsto. La infraestructura conocida es eso, más o menos conocida; igual dará alguna sorpresa desagradable, pero no será (o no debería) ser algo demasiado gordo. Ahora bien, lo que no se conoce, ¿cómo estará? ¿quién lo estará usando y para qué? (y eso sin entrar en otros aspectos como gestión de costes, nivel de compliance,...).

No evidenciar la parte oculta de la red tirará al traste todos los esfuerzos para hacerla más segura, porque todas las mejoras que se hagan, quedarán sin aplicar en la zona desconocida (y en seguridad, solo una pequeña brecha ya es suficiente para que todo salte por los aires).

Contar con una herramienta de Discovery & ITAM hará que lo desconocido se vuelva conocido, ya que con sus escáneres detectará cualquier equipo conectado a la red, sin importar la dispersión de estos, garantizando que siempre se cuente con un inventario completo y actualizado.

¿Qué le aportará la herramienta ITAM?

- Discovery automático de todos los escenarios tecnológicos.
- Actualización automática de la información de Hardware & Software.
- Informes sobre los equipos cuya información está pendiente de completar.
- Alertas sobre nuevos equipos detectados en la red.

Partiendo de la base establecida en el punto anterior, será necesario ir desgranando poco a poco la información que el 110% del inventario está ofreciendo. Pero no te preocupes por la cantidad de información que ahora tienes, en los siguientes puntos intentaremos analizar los que consideramos más básicos e importantes a tener controlados (y que la plataforma de ITAM entregará -o debería- de manera automática).

2

SISTEMAS OPERATIVOS FUERA DEL CICLO DE VIDA

La herramienta de ITAM debería generar un listado completo de los sistemas operativos que hay distribuidos en el parque, agrupados por familias para una mayor facilidad de búsqueda, pero sin perder el detalle de las versiones concretas de cada uno.

> **Recuerda: "*start where are we are*" y "*progress iteratively with feedback*".**

Con esta información de base, la herramienta ITAM contará con una colección de métricas y dashboard a través de los cuales se podrá revisar qué sistemas operativos ya están fuera del ciclo de vida del fabricante. De esta manera, **la herramienta ITAM identificará de manera automática los equipos que no tendrán disponibles ninguna actualización de seguridad.**

Una vez identificadas las máquinas con estos sistemas operativos obsoletos, se podrá establecer un plan de acción escalonado para la actualización de todos ellos.

¿Qué le aportará la herramienta ITAM?

- Detección automática del Sistema Operativo y su versión, agrupados por familias.
- Listados de equipos de cada familia de Sistemas Operativos.
- Métricas de equipos con Sistemas Operativos obsoletos.
- Listados de equipos fuera del ciclo de vida del Sistema Operativo.

Como valor extra, algunas herramientas ITAM no solo ofrecen la información anterior, si no que además obtienen todo el detalle necesario para analizar si el Hardware de un equipo puede ser actualizado a una nueva versión del sistema operativo (analizando no solo los recursos "teóricos" de la máquina, sino también analizando el desempeño real según los patrones de uso de los usuarios). Sin duda, información adicional que evitará un gran esfuerzo a la hora de planificar la migración, garantizando su éxito y reduciendo los riesgos.

3

SISTEMAS OPERATIVOS "MODERNOS", PERO SIN PARCHEAR

En este caso ya hay algo ganado con respecto al punto anterior: tenemos un listado de equipos que, aunque están sin parchear, están cubiertos por las actualizaciones de seguridad del fabricante, ya que su sistema operativo aún no ha terminado el ciclo de vida.

A partir de aquí, la herramienta ITAM identificará los ordenadores y/o servidores que no se encuentren totalmente actualizados, y permitirá agruparlos de acuerdo a su naturaleza para comenzar un despliegue ordenado de los parches pendientes.

Con la información de los equipos que no están actualizados, los parches que le falta a cada uno de ellos, y la información de la criticidad de dicho parche (todo detectado automáticamente por la herramienta de ITAM), tan solo falta establecer la política de actualización adecuada para que la plataforma empiece a desplegar los parches de manera automatizada.

Este paso representa un paso de gigante, ya que **estaremos más cerca de tener el parque totalmente actualizado, siendo la herramienta ITAM la que ha asumido todo el esfuerzo del despliegue.**

¿Qué le aportará la herramienta ITAM?

- Identificación y descarga de los parches pendientes de desplegar en el parque.
- Identificación de qué parche se debe aplicar a qué equipo.
- Agrupación lógica de equipos para una actualización más ordenada y sin afectar servidores en producción si es necesario.
- Despliegue automático de los parches pendientes para cada equipo.
- Métricas actualizadas del estado de actualización de parches en el parque.

4

EQUIPOS SIN FIREWALL O ANTIVIRUS

Una de las primeras líneas de defensa de los PCs y servidores de nuestra organización es el antivirus y el firewall local. Cuando los equipos están en la red corporativa, además de esta línea de defensa se podrán tener otras (firewalls perimetrales, servidores proxy, escáner de vulnerabilidades,...). Sin embargo, cuando un equipo sale de la oficina para teletrabajar, se encuentra "solo ante el peligro", y estas primeras líneas de defensa se vuelven imprescindibles.

La herramienta de ITAM será capaz de identificar, de entre todos los equipos inventariados, **cuáles son los que no tienen instalado un antivirus y/o un firewall**, además de saber si están actualizados y activos.

Con esa información, accesible a través de un Dashboard, se podrá analizar de manera muy sencilla con el objetivo de tomar decisiones rápidas que nos permitan acercarnos a una red más segura (y dormir así un poco más tranquilos por la noche).

¿Qué le aportará la herramienta ITAM?

- Identificación de los equipos sin firewall o con firewall desactivado.
- Identificación de equipos sin antivirus o con el antivirus desactualizado.
- Métricas que nos indiquen el estado del parque informático.

5

EQUIPOS CON SOFTWARE OBSOLETO

De la misma manera que un sistema operativo debe estar correctamente actualizado, el resto del software instalado en los equipos, también debe estarlo.

Una buena herramienta ITAM cuenta con un minucioso y exhaustivo inventario del software instalado en los equipos del parque, de manera que se pueda hacer un control de las versiones desplegadas en cada uno de los equipos.

De esta manera, **la herramienta ITAM identificará el software que está obsoleto**, dejando en evidencia los riesgos a los que estamos expuestos, pudiendo identificar además los equipos del parque que son vulnerables.

Finalmente, para poder solucionarlo, la herramienta de ITAM permitirá agrupar estos equipos más vulnerables, y así poder **distribuir automáticamente la versión más reciente del software** obsoleto.

¿Qué le aportará la herramienta ITAM?

- Inventario completo del software del parque informático.
- Tipificación y clasificación automática del software.
- Organización del software en base a su versión.
- Asociación de las versiones del software con los equipos que lo tienen instalado.
- Distribución automática de software.
- Alertas de software no permitido.

6

BASES DE DATOS ANTIGUAS

Extrapolando el control de versiones del software obsoleto instalado en los equipos cliente, y aplicando el mismo razonamiento a los servidores, encontramos el caso concreto de los Sistemas Gestores de Bases de Datos (SGBDs). Estos son especialmente importantes, ya que si los SGBDs no están perfectamente actualizados, el riesgo de fuga de información aumenta exponencialmente (datos de usuarios, datos de clientes, datos económicos,...).

La herramienta ITAM ayudará con una información primordial, detectando automáticamente los SGBDs instalados en nuestros servidores (¡y clientes!), e incluso llegando a conocer su nivel de actualización, configuraciones de acceso, bases de datos alojadas,...

De esta manera, la herramienta ITAM será capaz de presentar un cuadro de mandos que identifique qué motores de bases de datos están desplegados en los servidores corporativos, incluyendo los alojados en la nube, de manera que se pueda saber a ciencia cierta las versiones de cada uno de ellos.

Este cuadro de mandos (Dashboard), ayudado por la siempre valiosa información de la CMDB, ayudará a programar la migración de versión de los SGBDs que ya están obsoletos y fuera de la cobertura del fabricante.

¿Qué le aportará la herramienta ITAM?

- Detección automática de SGBDs en los equipos, tanto clientes como servidores.
- Obtención completa de la información de cada SGBDs.
- Métricas de SGBDs con versiones obsoletas.

7

EQUIPOS CON SERVICIOS "SENSIBLES"

Tener los servidores (¡y los clientes!) con un sistema operativo "moderno" que esté cubierto por las actualizaciones de seguridad del fabricante, y que tenga aplicadas todas estas actualizaciones de seguridad, es requisito necesario pero no suficiente. Muchos de los equipos se instalan con la configuración "por defecto", y dejan activos servicios sensibles a través de los cuales se abre una (o varias) puertas de entrada para ataques externos.

La herramienta ITAM detectará qué servicios están instalados en cada uno de los equipos y en qué estado están. En muchos casos, servicios como IIS, FTP, TELNET, Samba o SSH son servicios que están configurados para que se inicien automáticamente con el arranque del equipo. La herramienta ITAM dará un listado completo de estos servicios, mostrando en qué equipos están instalados y el modo de arranque configurado.

Uno de los servicios más delicados es el de escritorio remoto (RDS), que nos deja peligrosamente expuestos los equipos a un ataque externo, sin perder de vista la gran cantidad de equipos clientes en la red doméstica.

La herramienta de ITAM ayudará a identificar qué equipos servidores y clientes tienen activo el servicio de escritorio remoto (RDS), y cuál es el puerto de conexión utilizado para ello.

¿Qué le aportará la herramienta ITAM?

- Listado completo de servicios instalados en el parque.
- Información sobre los servicios instalados en cada equipo y su configuración.
- Detección de los datos relevantes del servicio RDS.

8

DISPOSITIVOS DE RED CON FIRMWARE SIN ACTUALIZAR

Es fundamental tener los PCs y servidores con el sistema operativo totalmente actualizado, pero no es menos importante mantener el firmware de los dispositivos de red igualmente actualizado a la última versión.
En muchas ocasiones, la puerta de entrada para un ataque externo no se realiza a través de los PCs o servidores, sino de equipos de red con brechas de seguridad conocidas que no se han solucionado por tener una versión antigua del firmware.

La herramienta de ITAM detecta e inventaría de manera automática todos los dispositivos de red, y es capaz de obtener toda la información SNMP ofrecida por el fabricante. De esta manera, **se podrá obtener automáticamente la información de la versión del firmware** (entre otras cosas) de cada uno de los dispositivos conectados a la red.

¿Qué le aportará la herramienta ITAM?

- Detección automática de cualquier tipo de equipo conectado a la red.
- Obtención del inventario SNMP completo.
- Clasificación de la información SNMP más relevante para cada tipo de dispositivo.
- Alertas sobre nuevos equipos detectados en la red.

9

DISPOSITIVOS MÓVILES CORPORATIVOS Y BYOD CONECTADOS A LA RED

La movilidad es una realidad que ya ha llegado a todas las organizaciones, y el número de dispositivos móviles (smartphones, tablets,...) con acceso a datos corporativos no deja de crecer. Crecimiento, por otro lado, más complejo de controlar que en el caso del equipamiento fijo "tradicional", ya que gran cantidad de estos equipos realmente no son propiedad de la organización, sino que pertenecen al usuario (BYOD, *Bring Your Own Device*).

La plataforma de ITAM permitirá conocer y tener controlados todos los equipos móviles que tienen acceso a la información de la red corporativa, clasificándolos según su propietario (organización o BYOD), la plataforma, localización,... y vinculando el dispositivo al usuario responsable del mismo. Además, **se podrán conocer y establecer políticas de seguridad** (obligatoriedad del pin, bloqueo automático de pantalla,...) **y aplicar medidas en caso de pérdida del dispositivo** (forzar bloqueo y cambio de pin, geolocalización, borrado completo,...).

¿Qué le aportará la herramienta ITAM?

- Listado de dispositivos con acceso a la red corporativa.
- Detalle de la configuración de seguridad de los dispositivos móviles.
- Configuración automática de políticas de seguridad (pin, bloqueo,...).
- Bloqueo y borrado completo de toda la información en caso de robo o pérdida.

10

USUARIOS ACTIVOS E HISTÓRICO DE ACCESOS

Uno de los activos más importantes de las organizaciones es la información y el conocimiento que se genera a partir de ella. El famoso "*know how*" es uno de los tesoros más valiosos para cualquier organización, y por tanto, hay que cuidarlo y protegerlo como uno de los bienes más preciados.

Si a lo anterior se le une que gran parte de las fugas de información y ataques contra los sistemas corporativos tienen su origen en usuarios internos, hace que conocer con todo detalle **qué usuarios y grupos están activos en cada momento (tanto a nivel local como a nivel de dominio) será una información crítica proporcionada con la herramienta ITAM.**

Esa información será "cruzada" con el resto de datos del inventario, de tal manera que se podrá conocer de manera automática e inmediata:

- El histórico de logins de cada usuario en cada equipo del parque.
- Cuentas de correo corporativo configuradas.
- Dispositivos USB conectados a cada equipo.
- Los accesos de los usuarios a servicios que contienen información corporativa sensible, tales como servidores SharePoint o bases de datos Microsoft SQL Server.

Además, los departamentos de TI también tendrán que tener un control exhaustivo de dónde está la información, y sobre todo, saber quién puede acceder a la misma. Para ayudar en esta tarea, **la herramienta ITAM es capaz de identificar qué usuarios o grupos de usuarios tienen acceso a un archivo o carpeta específico y cuáles son los permisos** que se le han concedido.

¿Qué le aportará la herramienta ITAM?

- Inventario automático de usuarios y grupos, tanto de dominio como locales.
- Identificación de usuarios locales con privilegios de administración.
- Histórico de todos los logins de usuario en cualquier equipo del parque.
- Auditoría de conexiones de usuarios y dispositivos a servidores Sharepoint y bases de datos Microsoft SQL Server.
- Auditoría de los permisos sobre carpetas y archivos, tanto en unidades de red como en unidades locales (incluyendo las del sistema).

RIESGOS DE NO CUMPLIR LOS PUNTOS ANTERIORES

Contar con toda la información anterior de manera automática no es ni mucho menos un capricho. Es una necesidad para reducir los riesgos a los que se enfrenta la organización, liberando horas del personal de TI para tomar la mejor decisión en cada momento e implementar acciones de mejora.

> **El tiempo debe invertirse** en analizar la información y tomar las medidas necesarias, **pero no debería malgastarse** nunca en la mera obtención de la información (para eso ya están las máquinas y el software).

A continuación se enumeran sólo algunos de los riesgos a los que las organizaciones se enfrentan cuando no cuentan con la información anterior, o cuando teniéndola al alcance la mano no toman las medidas oportunas:

- **Coste económico y sanciones legales derivados de:**
  - · publicación de información sensible.
  - · falta de licencias SW.
- **Pérdidas económicas, pérdidas de cuota de mercado e impacto reputacional de sufrir un ataque.**
- **Pérdida de disponibilidad de los servicios** debido a ataques internos o externos a través de vulnerabilidad no conocida (o conocida, pero no parcheada).
- **Pérdida de productividad de los usuarios** al utilizar equipos obsoletos y más vulnerables, con la correspondiente pérdida de competitividad en el mercado.
- **Pérdida de tiempo de los técnicos derivados de:**
  - · las tareas para sobreponerse a un potencial ataque.
  - · tareas fácilmente automatizables.
- **Pérdida de *"Know How"*.**

ARGENTINA | BOLIVIA | CHILE | COLOMBIA | ECUADOR | ESPAÑA | MÉXICO | PANAMÁ | PERÚ | URUGUAY

www.proactivanet.com