TANIUM

La guía definitiva para la ciberhigiene

La ciberhigiene consiste en planificar de forma proactiva la estrategia de seguridad para evitar los ciberataques.

El modo de trabajo mixto de la fuerza laboral ha ampliado la superficie de los ataques, y el cibercrimen se está volviendo más sofisticado. Esto es evidente con echar un vistazo a las últimas noticias, que cuentan historias de redes de gobiernos, organismos públicos y empresas privadas presas del ransomware.

Y las amenazas son cada vez más audaces.

Es fundamental que las organizaciones sean conscientes de su postura ante el riesgo, y que cuenten con herramientas que proporcionen la visibilidad y el control de terminales necesarios para detectar y poner remedio a las amenazas. Pero las herramientas por sí solas son sólo la mitad de la ecuación. Los responsables de TI saben que para obtener los mejores resultados y mantener y proteger las redes empresariales se requiere alinear las herramientas adecuadas con las prácticas de higiene recomendadas.

La higiene de las TI, o ciberhigiene, es fundamental para la seguridad y la gestión de los sistemas empresariales. Mejorar la ciberhigiene requiere crear un proceso para identificar continuamente activos, riesgos y vulnerabilidades en un entorno dado, y solucionarlos rápidamente a la escala correspondiente. Centrarse en la ciberhigiene puede ayudar a prevenir muchas de las violaciones, las interrupciones y los problemas asociados que enfrentan las empresas víctimas.

A medida que los entornos crecen, aumenta la complejidad, la variedad de los dispositivos y las cargas de trabajo. Las organizaciones deben gestionarlo todo, desde computadoras portátiles y máquinas virtuales (VM) hasta contenedores, a través de amplias redes distribuidas que abarcan múltiples oficinas e incluso continentes. Bajo estas exigencias, la ciberhigiene a menudo se ve afectada.

En este eBook explicaremos los componentes de la ciberhigiene y cómo varias herramientas contribuyen o frustran los esfuerzos para mejorarla.

Saber lo que se tiene

Para preservar y mejorar la ciberhigiene es preciso saber qué activos se tienen. ¿Hay 50 000, 100 000 o 500 000 computadoras y servidores en su organización? ¿Dónde están? ¿Qué son? ¿Qué tienen instalado? ¿Qué servicios proporcionan?

Es para responder a estas preguntas que se utilizan la detección y el inventario de activos. Son la base de la ciberhigiene.

En este capítulo analizaremos por qué esa base es tan importante.

No se puede gestionar lo que no se sabe que se tiene

Se necesitan tres niveles de conocimiento para gestionar sus terminales:

- Qué activos tiene y dónde están
- Qué software se está ejecutando en ellos y tienen o no licencia
- Cómo interaccionan las máquinas de su red entre sí y cuál es su propósito

Todas las empresas, independientemente de su alcance, necesitan esa información, que además, en las TI modernas, cambia constantemente. Los activos de red van y vienen, especialmente con los criterios de 'traiga su propio dispositivo' (Bring Your Own Device, BYOD), una política cada vez más utilizada y en crecimiento en muchas organizaciones.

Algunos activos pueden aparecer en la red sólo ocasionalmente. Y con más empresas animando a sus empleados a trabajar desde casa (WFH), la complejidad aumenta.

Las desventajas operativas de no saber

Parafraseando a Don Henley, un músico estadounidense y antiguo miembro de la banda The Eagles, 'cuando conduce con los ojos cerrados seguramente acabará chocando con algo'.

Una de las primeras cosas con las que probablemente 'chocará' es una vulnerabilidad de seguridad. Si no puede gestionar un activo, no podrá protegerlo. Y no puede gestionarlo si no sabe que lo tiene. Puede haber vectores de ataque que desconozca totalmente, como una vulnerabilidad sin parches.

¿Y qué hay de las implicaciones económicas? ¿Tiene una idea general de dónde está gastando el dinero? Tome por ejemplo las licencias de software de un programa popular como Microsoft 365. Si tiene una licencia para 10 000 copias, ¿usa 20 000 o sólo 5000? ¿Utiliza eficientemente las licencias que paga? O, ¿está fuera de cumplimiento y expuesto a costosas acciones legales?

Además, el cumplimiento no sólo aborda las licencias de software. Tomemos los servicios de salud como caso de uso. Las empresas de servicios de salud deben demostrar su cumplimiento con las disposiciones de la HIPAA y la PCI, que abarcan la información protegida de salud y los datos de tarjetas de crédito. ¿Sabe dónde residen esos datos? Si no lo sabe, no puede demostrar su cumplimiento. No poder demostrar el cumplimiento tiene dos inconvenientes importantes: sanciones normativas y clientes insatisfechos.

¿Qué características son importantes para un conjunto de herramientas para la detección y el inventario de activos?

Las herramientas o la plataforma que utiliza para la detección y el inventario de activos deben poseer:

- Exactitud
- Velocidad
- Escala
- Facilidad de uso

La exactitud, la velocidad y la escala están estrechamente relacionadas. Si tarda dos semanas o un mes en hacer un inventario, para cuando haya terminado, la red habrá cambiado y sin duda acabará por faltar algo.

Cuanto más grande sea la red, más problemas presentará. Por eso la escala es importante. La facilidad de uso entra en juego porque una herramienta difícil de configurar produce errores y la gente no querrá usarla.

Las herramientas más antiguas tienen dificultades con lo que exigen las actuales TI

Las herramientas de detección de activos creadas hace 10 años precedieron a muchas de las que operan los modernos entornos de TI. No pueden funcionar a la velocidad de los cambios que vemos actualmente. Sin embargo, las organizaciones a menudo mantienen las herramientas con las que se sienten cómodas, muchas de las cuales no son fáciles de usar.

De hecho, suelen sentirse orgullosas de dominar las herramientas difíciles de usar. Tal vez escribieron scripts personalizados para que funcionaran de forma más efectiva. Y no sólo eso, se ha desarrollado todo un ecosistema de socios que ayuda a los departamentos de TI a hacer exactamente eso.

Las consecuencias imprevistas y desafortunadas de esa situación son políticas y procesos de TI casi artesanales, no porque sean la mejor forma de abordar un problema, sino porque se ajustan a las capacidades de las herramientas en uso. Las herramientas más arraigadas se convierten en parte de la infraestructura de TI. Pero las mejores políticas de TI deben ser independientes de las herramientas. Una herramienta desarrollada en 1993 o 2010 no puede ofrecer esa flexibilidad.

La detección de terminales es un objetivo en constante cambio

No todas las terminales de una red son computadoras de sobremesa, computadoras portátiles o servidores. Hay impresoras, teléfonos, tabletas y un número cada vez mayor de dispositivos tipo Internet de las Cosas (IoT), tanto industriales como domésticos. La gestión de dispositivos móviles (Mobile Device Management, MDM) es un campo en crecimiento. Con un proveedor de MDM como Microsoft Intune puede hacerse seguimiento de todos los teléfonos de una red.

Pero ¿por qué debería tener que preocuparse de que un dispositivo IoT doméstico ponga en peligro la red corporativa? Este es el motivo:

Un empleado de uno de nuestros clientes trabajaba desde casa. El equipo de seguridad de la empresa estaba recibiendo alertas de que alguien estaba intentando entrar en su portátil. La fuente era un refrigerador con malware que escaneaba la red doméstica e intentaba entrar en el dispositivo, que estaba temporalmente en la red corporativa. Lo mismo podría ocurrir con un interruptor de luz, un termostato o una cámara de seguridad inteligentes.

Esto también es aplicable a las máquinas de una fábrica, muchas de las cuales están dotadas de sensores que se comunican a través de redes inalámbricas con aplicaciones con interfaz web. Esta es tecnología operativa que hace que cada máquina de una fábrica sea un dispositivo de red.

Ninguna herramienta de detección de activos es capaz de identificar todos los tipos de dispositivos, por lo que la herramienta o plataforma que vaya a utilizar debe integrarse y funcionar bien con aplicaciones compatibles que puedan reconocer dispositivos como teléfonos, tabletas, impresoras, etc.

La detección de terminales es la base de las redes de confianza cero (Zero Trust Network, ZTN)

Cuando todo es un dispositivo de red, todo representa una posible vulnerabilidad de seguridad. Por lo tanto, se necesitan políticas y procedimientos que dividan las terminales en tres categorías: gestionadas, no gestionadas y no gestionables. La detección de terminales es el primer paso crucial en la tendencia hacia la confianza cero, que es una arquitectura de seguridad que supone que no se puede confiar en ningún dispositivo o usuario sin verificación.

La detección de terminales es donde empieza la ciberhigiene y la seguridad. Tiene que empezar por ahí.

Cierre puertas y ventanas

Los responsables de las amenazas son cada vez mejores para encontrar enlaces débiles, explotar vulnerabilidades y configuraciones erróneas antes de que los equipos de seguridad y operaciones de TI estén al tanto de ellas.

El cumplimiento normativo también está aumentando la presión en las organizaciones, ya que les es difícil gestionar las consecuencias económicas y de reputación de las infracciones.

En el centro de cualquier buena estrategia de gestión de riesgos cibernéticos se encuentra la gestión y la configuración de las vulnerabilidades.

1. Priorizar

El crecimiento exponencial de las terminales empresariales hace prácticamente imposible solucionar todos los problemas de inmediato. Por eso es importante establecer prioridades. En primer lugar hay que determinar la importancia de los activos de TI: computadoras portátiles, servidores, máquinas virtuales, contenedores u otro tipo de terminales. Esta labor puede dividirse entre las fases de detección y evaluación del ciclo de vida.

Utilice los resultados de la evaluación para priorizar acciones basadas en la importancia de cada activo y los problemas de vulnerabilidad que les afectan. La visibilidad y la supervisión continuas deben ser aquí palabras clave.

2. Centrarse en la corrección

La corrección oportuna de las vulnerabilidades es esencial, ya que los atacantes actúan rápidamente y mejoran continuamente sus ataques para aprovechar las brechas de seguridad. Aunque muchos equipos de seguridad realizan análisis frecuentes y son conscientes en buen grado de los puntos débiles de las infraestructuras, solucionarlo es otro asunto. Soltar el problema sobre las personas no es la respuesta. Incluso los grandes equipos de TI pueden verse repentinamente agobiados por la gran cantidad de problemas y terminales que necesitan intervención.

La automatización hace que el ciclo de vida discurra de forma fluida. Para los equipos preocupados por los parches automatizados que pueden dañar sistemas críticos, los procesos de evaluación secundarios pueden integrarse en flujos de trabajo automatizados. Estos comprueban qué tan probable es que los parches sean relativamente benignos o que representen un riesgo.

3. Haga seguimiento de su cadencia de corrección a lo largo del tiempo

Entender la velocidad y el éxito de las correcciones revela la efectividad de sus esfuerzos en la gestión de vulnerabilidades. En la fase de verificación, no sólo necesita validar si se han realizado los cambios necesarios, sino también evaluar las métricas de su rendimiento.

Puede ver la rapidez con la que identifica problemas, con la que su equipo los aborda, si se cumplen los acuerdos de nivel de servicio (Service-Level Agreement, SLA) y cómo compara su rendimiento con el de sus colegas. Los datos recientes y exactos ayudan a que esta etapa del ciclo de vida sea más completa e impulsan una cultura de mejora continua.

4. Automatizar en cualquier lugar que sea posible

En un mundo ideal se trataría de automatizar todo el ciclo de vida de la gestión de vulnerabilidades. Esto reduciría los errores manuales y el riesgo cibernético, aceleraría los tiempos de reparación y permitiría que el personal trabajara en otras tareas. Pero todavía hay elementos que algunas organizaciones pueden desear, o que se les exija realizar, revisar, aprobar, auditar y validar directamente.

Entre estos está la pieza inicial de valoración de activos, que puede ser más arte que ciencia, y el análisis de métricas en la fase de verificación. Aun así, siempre vale la pena evaluar periódicamente si se puede automatizar más.

5. Empiece poco a poco para superar las resistencias al cambio

Una de las barreras más grandes para modernizar la gestión de vulnerabilidades es la gente y la cultura. Puede haber miembros del personal que estén firmemente en contra de las soluciones automatizadas tras haber experimentado una interrupción de la producción en el pasado por parches automatizados. Otras personas pueden temer que sus trabajos estén en riesgo si se utilizan máquinas para solucionar problemas en las terminales. Algunos simplemente se quejan de que “no es así como se hacen las cosas aquí”.

El cambio puede ser aterrador, pero también es esencial impulsar la mejora continua. Encárguese primero de la fruta al alcance de la mano. Esto enseña a las partes interesadas reacias el valor de los enfoques automatizados para la gestión de vulnerabilidades y cuánto más productivas podrían ser.

Pruebe cosas inocuas para empezar, como automatizar la detección para evaluar las fases del ciclo de vida. Un análisis automático, activado tras detectarse un nuevo activo, podría acelerar un proceso que antes duraba cinco días a sólo cinco minutos.

En cuanto a la corrección, considere implementar parches automatizados o actualizaciones de software para problemas de gravedad media o baja en entornos no productivos, para demostrar velocidad y eficacia antes de pasar a entornos de producción.

6. Todo empieza con la política

La tecnología es muy importante, pero no olvidemos lo básico, de donde se deriva todo: las políticas, los planes y los acuerdos a nivel de servicio (Service-Level Agreements, SLA). Podría ser algo tan sencillo como: "Vamos a desarrollar un ciclo de vida de la gestión de las vulnerabilidades, que definiremos, y aquí están los SLA para cada periodo de ciclo." Una vez que los SLA están en vigor, puede quedar claro que las herramientas automatizadas son la mejor forma de lograr dichos objetivos.

7. Escanear continuamente para la reducción integral del riesgo

Con demasiada frecuencia, las organizaciones se concentran en cumplir con los requisitos de cumplimiento mínimos, sin ver el panorama general: la gestión eficaz de las vulnerabilidades es buena para la empresa.

Es importante asegurarse de que el escaneo de terminales no se lleve a cabo simplemente para marcar las correspondientes casillas en una hoja de cumplimiento, sino como parte de una estrategia integral de la gestión de riesgos.

Esto significa analizar continuamente para identificar, priorizar y abordar los problemas a medida que aparecen, en lugar de hacerlo justo antes de una auditoría. Recuerde cubrir todo el entorno de TI, no sólo los activos fijos, sino también el código personalizado en desarrollo.

CAPÍTULO 3

Responder más rápidamente

No responder a un incidente de ciberseguridad oportunamente, ya sea una violación de datos, un evento de ransomware u otro tipo de ciberataque, puede comprometer enormemente las operaciones rutinarias de una organización, al tiempo que ocasiona pérdida de la confianza pública, erosión del valor de la marca y reducción de gran parte de los ingresos.

En este capítulo presentaremos el marco de trabajo PICERL. Consta de seis pasos que las organizaciones pueden adoptar para mejorar y ajustar sus planes de respuesta a incidentes. PICERL corresponde originalmente a las siglas en inglés de Preparar, Identificar, Contener, Erradicar, Recuperar y Lecciones aprendidas.

Paso 1. Preparar

La preparación garantiza que las personas adecuadas de los equipos adecuados se sientan involucradas, entiendan sus funciones y sepan qué hacer cuando se produce un incidente.

La fase de preparación debe generar un plan que los equipos de respuesta ante incidentes (Incident Response, IR) pueden practicar. Los planes de IR deben ensayarse para poder abordar cualquier debilidad. Los simulacros ayudan a los miembros del equipo a ejecutar bajo la presión de un incidente real.

Preguntamos a los clientes si su equipo de IR ha participado en un simulacro y ha entendido sus funciones. También preguntamos quién notifica a RR. PP. y a los departamentos jurídico y financiero.

La fase de preparación ayuda a determinar si se dispone de las herramientas adecuadas. Si no es así, ¿se cuenta con fondos para conseguirlas y proporcionar la correspondiente capacitación? Una vez creado un plan y el presupuesto de IR, debe revisarse y aprobarse por la alta dirección.

Paso 2. Identificar

Ante un incidente, la fase de identificación es donde debe empezarse a intentar responder preguntas como:

- ¿Cuándo empezó y cómo ocurrió?, ¿contraseña o activo robado?, ¿correo electrónico de phishing?, ¿código malicioso de un disco portátil?, etc.
- ¿Cuál fue el punto de entrada? ¿Fue una vulnerabilidad sin parchar?
- ¿Quién lo encontró y cómo?
- ¿Cuál es el alcance? ¿Se limita a una o dos personas, a activos, o está extendido?
- ¿Es posible continuar con la actividad? ¿Afectarán los pasos que se tomen alguna de sus líneas de negocio?

Muy a menudo son credenciales las que han comprometido el punto de entrada. Y a partir de ahí, los atacantes pueden aprovechar cualquier oportunidad que encuentren.

Paso 3. Contener

La contención consiste en ejecutar un plan para evitar la propagación del comportamiento no deseado. Una estrategia de contención a corto plazo podría ser tan sencilla como emitir un comando de cuarentena para evitar que un activo, una aplicación o un sistema se comunique con cualquier cosa salvo una herramienta de seguridad.

La contención a largo plazo es una solución que se implementa en toda la empresa, pero que puede no solucionar completamente la causa raíz del incidente. Esta podría ser una táctica para ayudar a la policía o a los organismos reguladores. Conviene tener estrategias de contención a largo plazo conectadas a los sistemas de copias de seguridad y de recuperación de datos.

Los parches y las actualizaciones también forman parte de la contención. ¿Tiene vulnerabilidades no corregidas relacionadas con algún incidente? Si es así, es hora de acelerar el programa de parches para la aplicación o el software del sistema operativo en cuestión.

Este es también un buen momento para revisar qué usuarios tienen acceso como administradores y a qué sistemas. ¿Cuál es la superficie de ataque en relación con Active Directory? ¿Ha habilitado la autenticación multifactor? Todos estos son problemas importantes a tener en cuenta para la contención.

Paso 4. Erradicar

Ahora está intentando eliminar la causa de la violación, tanto la raíz como las ramas. Esto significa, por ejemplo, en el caso del malware, que ha encontrado y eliminado de forma segura cada instancia que ha identificado. Ha reparado y mejorado la protección de los sistemas como y cuando correspondía. Ha reimaginado sistemas cuya protección ya no puede mejorar. Ha actualizado si inteligencia sobre amenazas para asegurarse de que puede identificar artefactos relacionados con la violación en cuestión.

Mientras desarrolla el proceso, puede cambiar el alcance de sus esfuerzos. Tras un ataque de ransomware, por ejemplo, es posible que muchos de sus sistemas necesiten sustituirse y restaurarse desde su última copia de seguridad buena conocida. Y si no detecta todos los artefactos relacionados con el ataque o no ha abordado la vulnerabilidad que se explotó para entrar, podría ser atacado de nuevo.

La clave de la erradicación es la rigurosidad. ¿Lo encontró todo? Sea lo que sea, quiere que "eso" sea la pregunta final. A menudo un socio o tercero con experiencia especializada puede ayudar con la fase de limpieza.

Paso 5. Recuperar

El daño está hecho; ahora es el momento de concentrarse en darle solución. Debe ser muy honesto consigo mismo. ¿Cuándo puede volver a poner en producción los sistemas afectados? ¿Los ha parchado, mejorado la protección y probado? ¿Ha utilizado su equipo rojo (el grupo que desempeña el papel de enemigo) para ejecutar un ataque simulado contra estos sistemas, utilizando las mismas técnicas que los atacantes? Seguramente deseará poder decir: "Abordamos las vulnerabilidades, y aquí está la prueba."

La recuperación también significa definir cómo el incidente cambiará el alcance de su supervisión. ¿Durante cuánto tiempo supervisará la actividad que causó la violación: 30 días, tres meses, seis meses? ¿Y qué buscará? Las pruebas del equipo rojo ayudarán, al igual que los artefactos recogidos durante la contención.

Tiempo promedio para implementar soluciones

El tiempo promedio de corrección (Mean Time to Repair, MTTR) es el tiempo que se tarda en avanzar por las fases de identificación, contención y erradicación de su plan de IR.

En 2018, el informe de violación de datos de Verizon encontró un MTTR de entre 14 y 30 días para organizaciones de alto rendimiento. Pero hay una fuerte tendencia entre los profesionales de la seguridad para reducir esa cifra a medida que los planes de IR maduran y los equipos mejoran en su práctica.

Paso 6. Lecciones aprendidas

Este paso debe comenzar con una reunión posterior a la acción que incluya a todos los que formaron parte del equipo de respuesta a incidentes: TI, cumplimiento, legal, relaciones públicas, etc.

Aquí es donde tendrá la oportunidad de revisar y documentar lo que ha aprendido sobre la violación.

- ¿Qué parte de su plan de IR funcionó o no funcionó?
- ¿Hubo brechas en las que eran necesarias más personas? ¿Tuvo que ponerse en contacto con un tercero o con un equipo interno que no estuviera en su lista de recursos?
- Dependiendo del incidente, ¿necesita cambiar su forma de operar? ¿Utilizó las herramientas de que disponía de forma efectiva? ¿Se configuraron correctamente?
- ¿Cómo fue la comunicación entre los distintos equipos? ¿Podría mejorarse?
- ¿Hubo algún aspecto que involucrara al empleado en la violación, como un ataque de phishing o un manejo inadecuado de los datos? ¿Se puede abordar esto con capacitación?
- ¿La vulnerabilidad explotó de forma endémica una línea de negocio, o a toda la organización? ¿Podría abordar la vulnerabilidad con una estructura o proceso operativo diferente?

Cuanto más flexible sea el plan de IR, más aprenderá de una violación cuando ocurra. Todo lo que aprenda debe regresarle a la fase de preparación, que siempre se puede afinar y mejorar.

Conclusión

La realidad es que el ransomware y otras ciberamenazas están aquí para quedarse. Las redes más codiciadas y la infraestructura crítica siempre serán un objetivo. La intención de este eBook era proporcionar una comprensión amplia y conceptual de lo que es la ciberhigiene, así como algunas directrices de higiene, prácticas recomendadas y conocimientos a tener en cuenta que ayudarán a preparar a los equipos de TI para defender las terminales que gestionan de forma más eficaz.

Es en el paso de la perspectiva a la acción donde la ciberhigiene suele estropearse. La información se pierde entre las grietas de las herramientas y los equipos fragmentados.

La coordinación efectiva de las implementaciones de parches y software en un entorno requiere que los equipos de operaciones y seguridad de TI trabajen como unidad, sean colaborativos y rindan cuentas. Esto requiere que se implementen sistemas base y se definan claramente los flujos de trabajo compartidos.

Una evaluación de ciberhigiene ofrece visibilidad del estado de su entorno de TI para que pueda entender el estado de sus terminales, identificar brechas críticas y saber cómo mejorar la ciberhigiene para reducir la probabilidad de que su organización aparezca en los próximos titulares de prensa. Tanium puede ayudar en esto.

Trabaje con nuestros expertos para definir una ruta procesable hacia una mejor gestión y seguridad de terminales con una **evaluación de riesgos sin costo alguno.**

Conozca cómo Tanium proporciona datos y análisis de alta fidelidad de terminales que aportan información para la toma de decisiones críticas de TI en tanium.com →