El administrador de TI que acabó con la Shadow IT

Confrontar las Shadow IT y recuperar los recursos de software

Las Shadow IT se han convertido en un nombre conocido, especialmente en las oficinas, para las empresas modernas actuales. Sin embargo, muchas organizaciones no se dan cuenta de los numerosos riesgos que implica ignorar estas instalaciones tecnológicas clandestinas. Según un estudio, el promedio de empresas grandes utiliza aproximadamente 1220 servicios en la nube independientes, que supone 13 veces más los 91 servicios reconocidos por los departamentos de TI. No solo las IT en la sombra se oponen directamente a los departamentos de TI, también pueden crear vulnerabilidad de seguridad y costes innecesarios. Por lo general, los empleados utilizan las Shadow IT porque piensan que ahorran tiempo y dinero a su empresa y a su departamento de TI. En realidad, el uso de las TI simplemente elude la gestión crítica, la integración y las garantías relacionadas con la seguridad y el soporte que aportan.

Imagínate un mundo en el que las Shadow IT se permitan en toda la empresa y que amenazaran la seguridad, la rentabilidad y la eficiencia de toda la empresa más de lo que nadie hubiera imaginado. Sería el salvaje oeste: tiroteos en las calles, doncellas en peligro y antiguos pianos de salón sonando en segundo plano. Entra Clark, el gestor de TI (y héroe de esta historia), su jefa Cynthia, CIO, y su fiel compañero, Steve, el administrador del sistema. Los tres se sientan silenciosamente juntos. Su departamento ha perdido el control, y nadie sabe con certeza qué tecnologías se utilizan en toda la organización. La tendencia de la consumerización de las TI, que consiste en el uso en la oficina de populares tecnologías de consumo destinadas para el hogar por parte de los empleados, ha facilitado la implementación de tecnologías por parte de los empleados sin el control del departamento de TI.

Este problema no es exclusivo de Clark y su equipo. En una encuesta de Intel Security, el 23 % de los encuestados confesó que sus departamentos gestionaban la seguridad sin la asistencia de TI.

Un día, Clark decidió poner un límite. Estaba cansado de ser controlado por los caprichos de las Shadow IT y de no saber qué tecnología se estaba usando para mantener el negocio en funcionamiento. Así que decidió hacer algo al respecto. Movilizó a su equipo, desarrolló un plan de acción y se precipitó a la batalla contra las Shadow IT.

Como una compañía que depende fuertemente de la aprobación del departamento de TI, queríamos aprender más sobre pensamientos de Clark acerca de las aplicaciones fraudulentas y entender mejor su enfoque sistemático para confrontar las Shadow IT y desarrollar una cultura de gestión de TI más transparente.

LifeSize
Proveedor de software de comunicación y colaboración en la nube

Clark
La encarnación de un heroico gestor de TI para una empresa no muy diferente a la tuya

¿Cómo encontrasteis el problema? ¿Qué hiciste para encontrar a los culpables?

Comenzó con un artículo que leí que decía, "**Siete de cada 10 ejecutivos no saben cuántas aplicaciones de TI en la sombra utilizan en su organización**". Me resultó curioso comprobar si ocurría lo mismo en mi empresa. En numerosas ocasiones, mi equipo ha escuchado hablar de estas diferentes aplicaciones que los departamentos utilizaban en la oficina, pero nadie nos había hablado directamente sobre el tema. Y, mientras que algunas eran benignas, otras eran potencialmente maliciosas, y no podíamos permitirnos ningún riesgo. Empezamos a monitorear de cerca con el fin de identificar nuevas y desconocidas herramientas o aplicaciones en nuestras exploraciones habituales, lo que dio lugar a un análisis de vulnerabilidad de toda la empresa.

Existen programas creados específicamente para detectar nuevas aplicaciones en la red. Los rastreadores de red y las herramientas de escaneo de seguridad pueden proporcionar toda la información sobre flujos de datos nuevos y desconocidos. Por supuesto, el monitoreo no elimina completamente la amenaza de TI en la sombra, pero suministra información. Hacer este análisis no solo nos mostró que nuestros empleados estaban utilizando herramientas que desconocíamos, sino que nos aportó información suficiente para iniciar evaluaciones de riesgos y, en el peor de los casos, investigar soluciones alternativas que se adaptaran mejor a nuestras necesidades.

¿Te informaron cuando algunas herramientas requeridas de un departamento

Claro. Brindamos asistencia a muchos teletrabajadores en nuestra compañía, y uno de los retos que rápidamente detectamos es que si no dispones de formas de habilitar a los empleados a trabajar a distancia

no eran compatibles con tu organización de TI?

aprobadas por TI, encontrarán sus propias formas de hacerlo. Es el momento en el que la seguridad corre riesgos debido a la transmisión de documentos insegura, la pérdida o robo de los dispositivos y otros factores. Nos dimos cuenta de que al ser transparentes sobre nuestros requisitos de seguridad y de red y al motivar a nuestros empleados a comunicarse con la TI durante la fase de descubrimiento del nuevo software, pudimos participar en más debates y mejoramos nuestro posicionamiento para la selección final. Es sorprendente ver lo feliz que son las personas al contar con tu ayuda para buscar y elegir soluciones en lugar de dar rodeos y buscar opciones por sí mismos.

¿Cómo conseguiste que tus empleados presentaran información sobre sus Shadow IT? Debió haber sido difícil.

Eso ocurrió al principio. La Shadow IT representa una verdadera amenaza solo para aquellas empresas que no están dispuestas a hacerle frente, así que nosotros decidimos hacerle frente. La tendencia de las organizaciones de TI suele ser amenazar con un período de cárcel a aquellas empresas que utilizan software no aprobado, lo que en mi opinión parecía un poco excesivo. Decidimos adoptar un enfoque más pacífico, así que ofrecimos un refugio seguro para aquellos departamentos que utilizaban la Shadow IT. En lugar de tomar el control de estos programas inmediatamente y cerrarlos, hicimos un análisis, determinamos los riesgos y ofrecimos soluciones comparables donde era necesario para lograr el resultado que buscaban las unidades de negocio. Eso también nos permitió establecer un diálogo sobre los riesgos relacionados con cada programa. Este ejercicio realmente nos puso a todos en la misma sintonía y estableció un clima de confianza y honestidad entre "nosotros" y "ellos".

¿Cómo

Muchas personas me han preguntado lo

mantuviste la coherencia con esta estrategia? El problema de las Shadow IT está solucionado por ahora, pero ¿cómo garantizas que no volverá a ocurrir en tu empresa?

mismo, y la respuesta es bastante simple. Se trata de relaciones. Entablé una relación con cada jefe de departamento, nos reuníamos habitualmente para debatir estrategias tecnológicas y establecimos un debate abierto entre departamentos y la organización de TI. Además, era imprescindible que mi jefa, Cynthia, CIO, mantuviera un estrecho contacto con el resto de la plantilla sobre la transparencia de la tecnología y los riesgos potenciales de la adopción de tecnologías no aprobadas.

Una vez se ha combatido las Shadow IT, ¿qué consejo tienes para los departamentos de TI que empiezan a tratar el tema en sus organizaciones?

Aprovechando las ventajas de crear un diálogo abierto con los compañeros de la empresa: los clientes. Escuchando sus opiniones, aprendiendo más sobre los problemas que intentan resolver y estando dispuesto a aportar información. Una vez recibí una solicitud para revisar una herramienta que otro departamento de la organización ya había aprobado e implementado. En este caso, fue mucho más fácil, e incluso más barato, ajustar nuestro plan para añadir varias licencias más en lugar de haber iniciado un nuevo contrato. El último consejo que comparto es no subestimar el poder de una sencilla interfaz de usuario. Asegúrate de equilibrar tus requisitos de seguridad y de red con la utilidad final de las aplicaciones. Una de las cosas que quiero buscar es una solución que se integre con nuestra SSO. Solo reducirá el número de contraseñas que los empleados necesitan para realizar seguimientos y actualizaciones durante todo el año.

La combinación de prácticas de contraseñas poco seguras con aplicaciones de TI en la sombra puede crear importantes vulnerabilidades de seguridad. Visita nuestro blog "The Best Defense Against IoT DDoS Attacks" (La mejor defensa contra los ataques DDoS a IoT) para proteger la red.

Acerca de Lifesize

Lifesize es un sistema de colaboración aprobado y diseñado especialmente para TI con el fin de proporcionar seguridad, resistencia y fiabilidad en la red. Tenemos más de una década de experiencia en el diseño de cámaras de alta definición y teléfonos de pantalla táctil. Nuestra intuitiva interfaz y el

directorio compartido ofrecen a los usuarios todo lo necesario para colaborar de forma más eficaz a través de aplicaciones aprobadas por TI, de modo que no es necesario el uso de aplicaciones adicionales no autorizadas. Los flujos de comunicación de Lifesize admiten cifrado de TLS (Transport Layer Security) y AES de 128 bits para toda señalización por defecto, y operamos en una red privada de fibra a través de la nube de IBM. Por si fuera poco, nos respalda nuestro galardonado servicio financiado por un acuerdo de nivel de servicio (SLA) con compatibilidad para 24x7x365.

FUENTES

http://blogs.cisco.com/cloud/shadow-it-rampant-pervasive-and-explosive
http://www.csoonline.com/article/3083775/security/shadow-it-mitigating-security-risks.html
http://www.digitalistmag.com/resource-optimization/2016/02/11/2016-state-of-shadow-it-04005674