datto | BUSINESS MANAGEMENT

RMM y gestión de parches:

La primera línea de defensa contra las amenazas informáticas

La ciberseguridad ha sido un tema recurrente entre los profesionales de TI durante bastante tiempo, pero la responsabilidad de un proveedor de servicios gestionados, o MPS, de mantener los entornos protegidos ha aumentado de forma bastante dramática durante la última década a medida que las amenazas se han vuelto más comunes.

Los delincuentes informáticos actuales siguen aprovechando los correos electrónicos con ingeniería social[1] como el principal vector de ataque. Según el informe de Anti-Phishing Work Group[2] T1-2019[3], el número total de sitios de phishing desde el cuarto trimestre del 2018 al primer trimestre del 2019 han aumentado en un 30%. Además del aumento del phishing, el informe del T1-2919 de ProofPoint Quarterly Threat[4] indica que los correos electrónicos con URLs maliciosas superaron a aquellos con correos electrónicos que contenían adjuntos maliciosos en un nivel 5 a 1 y han subido un 180% en comparación con el T1 del 2018. Los usuarios están más cerca que nunca de estar a un solo clic de la amenaza. Un único clic por error en la URL de un correo electrónico que redirija al usuario a un sitio web falso provocará la ejecución de un código para explotar una vulnerabilidad.

Los profesionales de la seguridad están de acuerdo en que una estrategia de seguridad integral es polifacética e incorpora el endurecimiento de los perímetros, la educación del usuario final, la gestión de parches de software y la planificación para la recuperación ante desastres.

También es cada vez más complejo prevenir los ataques de forma proactiva antes de que se produzcan. Las amenazas, como las variedades de ransomware, se adaptan a medida que las medidas de prevención maduran y emergen nuevas tecnologías que hacen que sea difícil para las empresas, sobre todo las más pequeñas con recursos limitados, mantenerse por delante de los delincuentes.Sin embargo, el problema debe ser abordado frontalmente. Como Gartner indica, "el riesgo de la ciberseguridad, si no se trata de forma apropiada, se traduce en un riesgo para la empresa, pérdida de reputación, incumplimientos regulatorios e interrupción general de las operaciones". El coste de la interrupción es demasiado significativo, y a menudo es más alto que el de la prevención cuando se responde a un evento cuando éste se haya producido.

Los proveedores de tecnología hacen lo que pueden para garantizar que las vulnerabilidades se corrigen tan rápido como sea posible, lanzando normalmente una actualización solo horas después de conocer la vulnerabilidad. Un estudio de caso bien documentado es la aparición de WannaCry[5] en el 2017. Microsoft supo de la vulnerabilidad en el sistema operativo Windows el 14 de marzo del 2017, y ese mismo día lanzó un boletín de seguridad MS17-010[6] marcado como CRÍTICO. La aparición global apareció dos meses más tarde, poniendo en peligro 230 000 ordenadores en 150 países en 24 horas. El código malicioso que explotaba la vulnerabilidad solventada por Microsoft estuvo corriendo libremente durante casi un mes antes de producirse el ataque. Cuando las cosas se calmaron, había al menos 300 000 dispositivos que no habían recibido la actualización crítica de Microsoft.

Los ataques de perfil alto, como WannaCry, concienciaron a las empresas y los MSP son a menudo a los que se busca para proporcionar guía estratégica y medidas tácticas para proteger los entornos TI de sus clientes. Para hacer esto de forma adecuada, los MSP deben abordar las implicaciones de seguridad de su cliente cuidadosamente. No hacer esto podría establecer una falsa sensación de seguridad y exponer potencialmente a los clientes a costosas interrupciones.

Primeros pasos con los servicios de gestión de parches

Un MSP tiene la oportunidad de crear una línea de servicios que pueden agruparse o proporcionarse a la carta.

- Los tipos de servicios pueden incluir:
- Evaluaciones y gestión de vulnerabilidades
- Evaluaciones y gestión de parches
- Evaluaciones de configuración segura
- Pruebas de seguridad de la aplicación
- Evaluaciones y gestión del cumplimiento

Según Gartner, el objetivo de un servicio adecuado de gestión de parches es "mitigar los riesgos de los fallos de seguridad o los problemas de rendimiento estandarizando los procesos de gestión de parches en toda la organización". El servicio puede iniciarse definiendo una línea de referencia de cumplimiento en todo el entorno gestionado. Desde ahí, determinar las versiones mínimas de las aplicaciones necesarias para el negocio que deben existir y luego identificar las brechas y la ruta para la corrección. Dedicar un tiempo adecuado a comprender los riesgos asociados con las aplicaciones de otras empresas y cuál es el plan de contingencia si un parche no puede implementarse o lleva a una interrupción.

En muchos casos, el MSP querrá probar sus parches en un entorno de prueba, laboratorio o enuna pequeña población de dispositivos tolerantes al riesgo. Antes de la implementación, los MSP deberían confirmar que sus objetivos tienen copias de seguridad verificadas, especialmente si son dispositivos cruciales para las operaciones, como los servidores. Verificar que todas las personas implicadas comprenden los planes primarios y de contingencia y están listas para responder si la implementación falla. Tras una implementación correcta, volver a evaluar el entorno y confirmar el cumplimiento. Identificar las anomalías no conformes y crear un plan de seguimiento para resolver. La última etapa es informar de los resultados a las partes interesadas.

Crear un servicio alrededor de la gestión de parches requiere una combinación de documentación del proceso del programa y herramientas tecnológicas para ejecutar de forma efectiva. El MSP debería posicionarlo a sus clientes como una disciplina continua e integral, no un proyecto a corto plazo.

Todas las partes interesadas deberían comprender la frecuencia de las actualizaciones, los dispositivos objetivo sujetos a recibir actualizaciones, y cómo definir y medir el cumplimiento.

Aprovechar el poder de una plataforma completamente automatizada y basada en políticas como Datto RMM[7], posicionará a los MSP para implementar sistemáticamente parches para las aplicaciones empresariales típicas tan pronto como están disponibles, ayudando a cerrar la ventana de exposición para las vulnerabilidades conocidas y de día cero. Datto RMM también generará informes fáciles de comprender, aportando una visibilidad clara a los sitios y dispositivos con mayor riesgo. Poder tener una conversación, respaldada por datos, establece aún más al MSP como un socio estratégico que intenta de forma proactiva evitar el tiempo de inactividad y mantener los mejores intereses de los clientes.

datto

Sede central
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
Estados Unidos
partners@datto.com
www.datto.com
888.294.6312

Oficinas globales
EE. UU.: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291

©2020 Datto, Inc. All rights reserved.

1. https://www.datto.com/blog/5-types-of-social-engineering-attacks
2. https://apwg.org/
3. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf
4. https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q119-quarterly-threat-report-0528.pdf
5. https://www.datto.com/blog/why-are-ransomware-attacks-like-wannacry-so-effective
6. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
7. https://www.datto.com/business-management/datto-rmm