FORTINET | vnicom

Configure estrategias, procesos y tecnología de endpoint para enfrentar el ransomware

Contenido

Resumen ejecutivo

El panorama de amenazas continúa evolucionando con ataques más sofisticados y técnicas evasivas. El ransomware es una de las formas más escalofriantes del cibercrimen que enfrentan las organizaciones en la actualidad y que no desaparecerá. FortiGuard Labs informa que hubo un aumento de siete veces en la actividad de ransomware en diciembre en comparación con julio de 2020.[1] Una encuesta global de ransomware también mostró que el 67 % de las organizaciones fueron el objetivo del ransomware y casi la mitad indicó que fue atacado más de una vez.[2]

El ransomware puede acceder a un sistema de varias formas, por lo general, con un simple clic o incluso sin un clic en absoluto. Debido a que el ransomware es tan frecuente, las organizaciones deben estar preparadas. Estas deben tener estrategias implementadas para estar preparadas antes, durante y después de un ataque de ransomware. Muchas empresas maduras ya tienen planes de respuesta a incidentes, que se deben utilizar. No obstante, para reducir el riesgo y el alcance de los incidentes potenciales, también se deben hacer muchas cosas con anticipación para reducir el riesgo de un incidente y saber qué hacer en medio de un ataque.

La continua evolución del Ransomware como un servicio (RaaS), el énfasis en la "caza mayor" (grandes rescates por grandes objetivos) y la amenaza de divulgar datos comprometidos si no se cumplía con las demandas crearon un mercado de crecimiento masivo del que los cibercriminales obtuvieron grandes beneficios.[3]

Introducción

Los ataques de ransomware están aumentando y tienden a ser extremadamente meticulosos. Los atacantes se están tomando el tiempo para hacer un reconocimiento para dirigirse a víctimas específicas y podrían estar al acecho en el entorno durante semanas, trazándolo y eludiendo los controles de seguridad. Cuanto más tiempo acechan los atacantes, más daño pueden hacer. Este tiempo les da la oportunidad no solo de eliminar la carga útil del ransomware, sino también de descubrir formas de exfiltrar sus datos y luego mantener esa información secuestrada. Las organizaciones necesitan estrategias integrales de prevención, detección, respuesta y corrección para que los sistemas críticos se puedan restaurar lo más rápido posible.

Estrategia previa al incidente

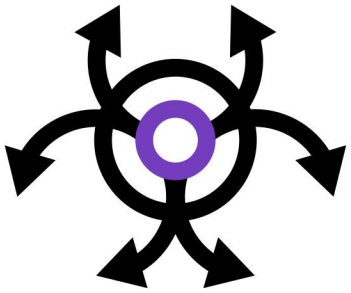
Las organizaciones a menudo tienen que hacer cambios fundamentales en la frecuencia, ubicación y seguridad de sus copias de seguridad de datos. Cuando se combina con el compromiso de la cadena de suministro digital y una fuerza laboral que trabaja a distancia en la red, hay un riesgo real de que los ataques puedan provenir de cualquier lugar. Las soluciones de seguridad basadas en la nube, como el borde del servicio de acceso seguro (SASE), para proteger los dispositivos fuera de la red; seguridad avanzada de endpoint, incluyendo soluciones de detección y respuesta de endpoint (EDR) que pueden interrumpir el malware en medio de un ataque; y el acceso de confianza cero y las estrategias de segmentación de la red que restringen el acceso a las aplicaciones y los recursos con base en la política y el contexto, deben considerarse para minimizar el riesgo y reducir el impacto de un ataque exitoso de ransomware. Por último, el elemento humano sigue siendo tan importante como la tecnología. Es importante proporcionar continuamente a los empleados actualizaciones sobre las nuevas metodologías de ataque de ingeniería social para que sepan lo que deben y no deben hacer.

Dicho esto, debido a que los endpoints son el destino final del ransomware, se debe enfocar en una seguridad sólida de endpoints. Este proceso comienza con la reducción de la superficie de ataque de cada endpoint mediante el cierre puertos y dispositivos periféricos innecesarios, el control de las aplicaciones instaladas en el sistema, la protección de las vulnerabilidades para que no sean aprovechadas y el mantenimiento esta configuración segura. A partir de esto, es fundamental utilizar un análisis estático sólido que combine la inteligencia frente a amenazas con el aprendizaje automático. El análisis se debe efectuar en todo código que se agrega a los dispositivos y complementar con una inspección dinámica basada en el comportamiento de toda la actividad en tiempo de ejecución para detectar amenazas. Es fundamental tener la capacidad de actuar en tiempo real y contener los ataques en progreso sin esperar una clasificación y respuesta a la alerta manual.

Estrategia de monitoreo continuo

Un informe reciente de Aberdeen estableció una referencia de la efectividad de seguridad de la protección del endpoint tradicional basada en firmas en un 92.5 % (dejando un riesgo de compromiso del 7.5 %). El informe también estableció el valor incremental de la reducción de la superficie de ataque en un 3.5 %, lo cual aporta una eficacia del 97 %. Calculó que la seguridad de endpoints basada en el comportamiento puede aumentar la efectividad al 99.6 % (es decir solo deja 0.4 % de exposición al riesgo).[4]

Para todas las medidas de prevención, las organizaciones que tienen un centro de operaciones de seguridad (SOC) con cobertura de 8 horas al día, 5 días de la semana o 24 horas al día, los 7 días de la semana, es una buena idea tener un acuerdo de servicio con su proveedor de seguridad de endpoint o socio de servicios de seguridad administrados para recibir apoyo de cobertura y escalamiento fuera del horario de atención. Estos servicios se enfocan en monitorear alertas y amenazas sospechosas, lo que proporciona orientación y los próximos pasos a los encargados de responder a incidentes, que incluyen la búsqueda proactiva de amenazas que incluye la búsqueda de Indicadores de Compromiso, la identificación de programas potenciales vulnerables y no autorizados y la recuperación y análisis de artefactos forenses. Una vez que se analiza el evento, una notificación de incidente explica la amenaza y las recomendaciones para su revisión o pasos de corrección.



El ransomware está involucrado en el 27 por ciento de los incidentes de seguridad de malware.[5]

Estrategia de respuesta

Cuando se descubre un incidente de seguridad, es imperativo responder de inmediato para minimizar el posible daño, incluso si hay contención implementada. Se requieren competencias especializadas, herramientas y procesos repetibles para la mitigación efectiva de las amenazas. Estos se pueden utilizar para evaluar la situación y determinar cómo contener la amenaza y recuperar las operaciones.

Incluso con las herramientas de personal y el proceso implementado, continúa siendo importante una mayor preparación y práctica para facilitar las acciones de respuesta en medio de un ciberincidente emergente. Estas actividades incluyen:

- Un examen de la preparación para la respuesta a incidentes para evaluar la postura de seguridad actual de una organización mediante la revisión de la arquitectura de la red, los controles de seguridad y las funciones y responsabilidades del personal. El objetivo es identificar la tecnología, las personas y los procesos
- La revisión del libro de estrategias de respuesta a incidentes para determinar la suficiencia y las áreas de mejora del proceso paso a paso en caso de un incidente de ciberseguridad importante, como un ataque de ransomware
- Ejercicios de sobremesa de respuesta a incidentes para simular los tipos de incidentes y probar el plan y la ejecución de la respuesta a incidentes reales de la organización con el objetivo de practicar y mejorar los procesos de respuesta

Resumen

Cuando una organización se encuentra en medio de un ataque de ransomware, es demasiado tarde para implementar las estrategias, los procesos y la tecnología para detener el daño. La planificación y preparación antes de que ocurra un ataque es clave. Para ayudar a los equipos de seguridad a mitigar el daño de las amenazas y minimizar el tiempo que lleva responder, las organizaciones deben invertir en soluciones que cubran todas las etapas de la reducción de la superficie de ataque, la prevención y la detección de amenazas, la contención y la respuesta.

[1] "Global Threat Landscape Report: A Semiannual Report", FortiGuard Labs, febrero de 2021.

[2] "The 2021 Ransomware Survey Report", Fortinet, 3 de noviembre de 2021.

[3] "Global Threat Landscape Report: A Semiannual Report", FortiGuard Labs, febrero de 2021.

[4] "Quantifying the Risk Reduction of Evolving Endpoint Security Technologies", Aberdeen Strategy and Research, julio de 2021.

[5] "2020 Data Breach Investigations Report", Verizon, 2020.

FORTINET | ovnicom

http://www.ovni.com/fortinet