INFINYT

Las mejores prácticas que se pueden tomar para reconstruir la confianza, cuando esta se haya roto

Introducción

Los recientes ataques de alto perfil expusieron cómo una sola violación puede afectar adversamente de una sola vez, a un gran número de agencias de gobierno y de la industria. Una empresa promedio usa 288 aplicaciones1, ademas de varias infraestructuras locales y en la nube. Si incluso un solo proveedor de hardware o software en la cadena de suministro de una organización es hackeado y no existen medidas de seguridad efectivas, existe una alta probabilidad que un ciber ataque tenga éxito. Las consecuencias pueden incluir tiempo de inactividad de la empresa, pérdida de ingresos, y también una ruptura de confianza entre la empresa y su proveedor.

Si realmente se ha roto la confianza, estas son las mejores prácticas que se pueden tomar para reconstruir esa confianza y mantenerse protegido contra futuros ciber ataques:

Tener un inventario y un mapa de dependencia

1

Lo más importante que pueden hacer los profesionales de la seguridad para proteger cualquier entorno es saber qué tienen, dónde está, cómo está configurado y de qué depende. En resumen, es imperativo tener un inventario y un mapa de dependencia para sus sistemas y servicios. Si bien esto no detendrá a un atacante, es necesario que comprenda qué está protegiendo, quién y qué puede acceder a él, y cuando algo sale mal, cuál es el "radio de explosión". No olvidar de dónde los sistemas podrían tener un impacto en los clientes.

Una vez que se hayan identificado los activos más importantes y sensibles, hay que concentrarse en asegurar de estar cómodo con la forma en que estos se mantienen (y el acceso a los mismos), quién tiene acceso a los activos y el mapa completo de dependencias que pueden comprometerlos. Los ejercicios sobre el incumplimiento de objetivos específicos pueden ser bastante esclarecedores. La base de datos MITRE ATT&CK de técnicas adversas proporciona multiples detalles a considerar.

Plan para tener una brecha de seguridad

2

En cualquier entorno de suficiente valor o complejidad, la probabilidad de tener una violación de seguridad aumenta con el tiempo. Esto no significa que no se deban proteger los sistemas. Significa que se debe planear reducir la oportunidad que tiene un atacante de hacer cosas malas una vez que obtenga acceso. Se puede lograr esto si se tienen capacidades rigurosas de detección, respuesta y corrección.

Las prácticas de seguridad maduras incluyen simulacros basados en escenarios que ejercitan los procesos de detección, respuesta y corrección. También incluyen informes formales sobre cuán efectivas son las prácticas actuales y los planes para mejorarlas.

El NIST provee una guia de alto nivel en este proceso en su marco de ciber seguridad. Además el plan, Modernizacion rápida en seguridad de Microsoft está diseñado para pensar en estos problemas y utilizar la tecnología para implementar soluciones sólidas y utilizables en las redes de Windows.

Plan para tener una brecha de seguridad

3

Algunos podrían decir que se debería retrasar la aplicación de parches. Pero esto solo garantiza que cualquier vulnerabilidad de seguridad parcheada pueda ser explotada en un entorno durante un período de tiempo más largo. En su mayor parte, las organizaciones carecen de la capacidad de evaluar la estabilidad de un parche, y mucho menos la seguridad, por lo que ejercitar inmediatamente el músculo de la implementación y la reversión es el camino a seguir en la mayoría de los casos.

Tener cuidado al considerar la idea que hay qu emoverse de inmediato para construir y alojar todo uno mismo. Los negocios se basan en el riesgo y la mayoría de las organizaciones no pueden permitirse contratar el número y la calidad de personas que podrían hacer que esto suceda. Si bien los entornos más sensibles pueden requerir una gran experiencia, hardware o software personalizado y entornos flexibles cuidadosamente construidos, la mayoría de los entornos no lo harán. En su lugar, elegir a los proveedores con cuidado y comprender para qué sistemas deben y no deben usarse esas soluciones.

Implementar procesos y técnicas que puedan ayudar

4

En cada violación de seguridad, hay que asumir que los adversarios capaces estarán muy bien informados sobre las tecnologías que se utilizan y perseguirán los sistemas que les brinden el mayor acceso a las cosas que son más valiosas para ellos. El objetivo de todo proveedor es detectar cuándo sucede eso y tratar de hacer su trabajo lo más ruidoso posible para que puedan ser detectados y eliminados. Algunos ejemplos de tecnología que pueden ayudar incluyen WebAuthn y SmartCards, módulos de seguridad de hardware (HSM) y rotación de claves, recolección y análisis de registros en tiempo real y detección y respuesta de anomalías en el comportamiento del usuario

Asegurar todas las claves privadas

El diagrama anterior muestra íconos que representan claves en lugares donde se usan comúnmente y, por lo tanto, también corren el riesgo de ser hackeados. En casi todas las violaciones de seguridad, se encontrarán credenciales, claves y secretos violados. El objetivo de las dos primeras tecnologías no es prevenir completamente el abuso de esas claves, sino más bien garantizar que, si se abusa de ellas, ese abuso ocurra solo en o a través de los sistemas a los que están conectadas, en el momento en que están conectadas. Esto brinda la oportunidad de monitorear los secretos más críticos cada vez que se utilizan.

WebAuthn y SmartCards pueden reemplazar las contraseñas de usuario, OTP o SMS, con una sólida criptografía de clave pública / privada vinculada al hardware. Esto significa que un atacante no puede robar esos secretos y, en el caso de WebAuthn, incluso requere que el usuario interactúe físicamente con su autenticador cada vez que se usa la clave. Esto hace más "ruido" y, por lo tanto, brinda más oportunidades para detectar el uso indebido incluso si el sistema al que está conectado el dispositivo está comprometido.

Los HSMs pueden mantener sistemas federados de identidad o crear sistemas que firman claves para que no se eliminen del entorno y, por lo tanto, puedan controlarse de la misma manera.
Ambas tecnologías son fundamentales para su uso no solo para los servicios de Internet, sino también para los sistemas que están "detrás del firewall", ya que siempre es prudente asumir que alguien está detrás del firewall. Esto crea la base de una arquitectura zero trust o beyondcorp que le da menos privilegio a todos los sistemas.

Si bien puede ser un largo camino para que muchos entornos complejos lleguen allí por completo, comenzar con los sistemas más sensibles lo antes posible tiene un retorno de la inversión muy alto.

Logs y Análisis de logs

El cronograma de un ciberataque puede ser largo. Es imprescindible asegurarse de tener los logs correctos, la retención de logs correcta y los procesos correctos para evitar que un atacante borre o modifique logs (incluso cuando obtienen un acceso elevado al entorno). Sin eso, no se podría confirmar un informe de una violación de seguridad, y mucho menos detectar una. Cualquier forma de acceso a Internet para sistemas con acceso privilegiado al entorno debe controlarse estrictamente, incluidas las rutas menos obvias a Internet, como dns tunneling.

El acceso permitido debe ser monitoreado y registrado, y los expertos deben examinar minuciosamente los comportamientos inusuales o nuevos.

Modelado de comportamiento y detección de anomalías

Empleados atentos detectan muchas infracciones importantes. Lograr el equilibrio adecuado de alertas, no solo para el equipo de seguridad, sino también para los empleados, es clave. Demasiado, y serán ignorados; muy poco, y no tendrán la oportunidad de darse cuenta.

Las tecnologías que crean perfiles de comportamiento del usuario o del sistema y alertan al usuario o al administrador de seguridad de un comportamiento inusual han recorrido un largo camino, y su implementación de manera transparente y enfocada puede ayudar a mejorar la detección y la respuesta en toda la organización.

Yubico puede ayudar a reconstruir la confianza cuando esta se haya roto

Si bien no existe una fórmula mágica para prevenir un ciber ataque, existen muchas prácticas y tecnologías bien establecidas que pueden ayudar a garantizar que las organizaciones puedan compartimentar cualquier daño, detectar brechas rápidamente y responder y recuperarse antes de que los adversarios lleguen demasiado lejos.

Yubico ofrece soluciones en ciber seguridad que pueden ayudar a reconstruir la confianza. La YubiKey – una llave de seguridad basada en hardware, resistente a phishing y muy facil de usar – asegura el acceso a los sistemas de TI y servicios en línea. Yubico tambien ofrece el YubiHSM – un módulo de seguridad de hardware (HSM) que cambia las reglas del juego para la protección criptográfica de servidores, aplicaciones y dispositivos informáticos, en un factor de forma nano ultraportátil y a un costo asequible.

YubiKeys y YubiHSMs son fabricados en Estados Unidos y Suecia manteniendo la seguridad y control de calidad a lo largo de todo el proceso de fabricación.

INFINYT

Seguridad Inteligente

+ 52 (81) 2474 5555
info@infinyt.mx
INFINYT.MX