NIST Publicación especial 1271
https://doi.org/10.6028/NIST.SP.1271es
Agosto 2021

Primeros pasos de NIST Marco de ciberseguridad: Guía de inicio rápido

Amy Mahn[1], Jeffrey Marron[1], Stephen Quinn[2], Daniel Topper[3]

[1] División de Ciberseguridad Aplicada de NIST, Laboratorio de Tecnología de Información
[2] NIST División de Seguridad informática, Laboratorio de Tecnología de Información
[3] Huntington Ingalls Industries

¿Qué es el Marco de ciberseguridad de NIST y cómo lo puede usar mi organización?

El Marco de ciberseguridad de NIST[4] puede ayudar a una organización a comenzar o mejorar su programa de ciberseguridad. Construido de prácticas que se sabe que son efectivas, puede ayudar a las organizaciones a mejorar su postura de ciberseguridad. Promueve la comunicación entre las partes interesadas internas y externas sobre ciberseguridad y en el caso de organizaciones más grandes, ayuda a integrar y alinear mejor los riesgos de ciberseguridad con los procesos más amplios de la gestión de riesgo empresarial según lo descrito en la serie NISTIR 8286[5].

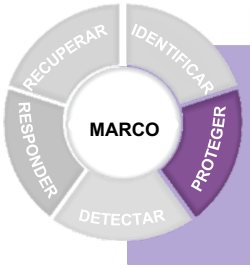
El marco está organizado en cinco funciones clave: identificar, proteger, detectar, responder, recuperar. Estos cinco términos ampliamente conocidos, cuando se consideran conjuntamente, proporcionan una visión integral del ciclo de vida para la gestión del riesgo de ciberseguridad en el tiempo. Las actividades enumeradas debajo de cada función pueden brindar un buen punto de inicio para su organización:

IDENTIFICAR

Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de: sistemas, activos, datos y capacidades.

- **Identificar los procesos y activos críticos empresariales:** ¿cuáles son las actividades empresariales que absolutamente deben continuar para que sea viable? Por ejemplo, esto puede ser mantener un sitio web para obtener pagos, proteger información de clientes/pacientes de manera segura o garantizar que la información que su empresa recolecta permanezca accesible y correcta.
- **Flujos de información de documentos:** no solo es importante comprender qué tipo de información su empresa recolecta y utiliza, sino también comprender dónde están ubicados los datos y cómo se usan, especialmente donde hay contratos y compromisos con socios externos.
- **Mantener el inventario de hardware y software:** es importante tener conocimiento de los computadores y el software en su empresa porque estos con frecuencia son los puntos de entrada de los actores maliciosos. Este inventario puede ser tan simple como una hoja de cálculo.
- **Establecer políticas para la ciberseguridad que incluyan roles y responsabilidades:** estas políticas y procedimientos deben describir claramente sus expectativas sobre cómo las actividades de ciberseguridad protegerán su información y sistemas y cómo apoyan los procesos críticos empresariales. Las políticas de ciberseguridad deben integrarse con otras consideraciones de riesgo empresarial (p. ej., financieras, de su reputación).
- **Identificar amenazas, vulnerabilidades y riesgos a activos:** garantizar que se establezcan y gestionen procesos de gestión de riesgo para garantizar que se identifiquen, evalúen y documenten las amenazas internas y externas en registros de riesgos. Garantizar que las respuestas a riesgos sean identificadas y priorizadas, ejecutadas y los resultados monitoreados.

[4] https://www.nist.gov/cyberframework
[5] https://csrc.nist.gov/publications/detail/nistir/8286/final



PROTEGER

Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios.

- **Gestionar el acceso a activos e información:** crear cuentas únicas para cada empleado y garantizar que los usuarios sólo tengan acceso a la información, los computadores y las aplicaciones que necesitan para sus labores. Autenticar a usuarios (p. ej., contraseñas, técnicas de múltiples factores) antes de que les sea otorgado el acceso a información, computadores y aplicaciones. Gestionar y hacer seguimiento de manera precisa del acceso físico a los dispositivos.

- **Proteger los datos sensibles:** si su empresa almacena o transmite datos sensibles, asegúrese de que estos datos sean protegidos por cifrado tanto cuando sean almacenados en computadores como cuando sean transmitidos a otras partes. Considerar el uso de verificación de integridad para garantizar que solo se hayan hecho cambios aprobados a los datos. Eliminar y/o destruir datos de manera segura cuando ya no sean necesarios o requeridos para fines de cumplimiento.

DETECTAR

Desarrollar e implementar las actividades apropiadas para identificar cuando ocurra un evento de ciberseguridad.

- **Probar y actualizar los procesos de detección:** desarrolle y pruebe procesos y procedimientos para la detección de entidades y acciones no autorizadas en las redes y el entorno físico, incluyendo la actividad del personal. El personal debe estar al tanto de sus roles y responsabilidades para la detección y el reporte relacionado tanto dentro de su organización y hacia las autoridades legales y de gobernanza externas.

- **Hacer respaldos con regularidad:** muchos sistemas operativos tienen capacidades integradas para hacer respaldos; también hay soluciones de software y en la nube disponibles que pueden automatizar el proceso de respaldos. Una buena práctica es mantener un conjunto de datos respaldados fuera de línea con frecuencia para protegerlo contra ransomware.
- **Proteger sus dispositivos:** considerar instalar cortafuegos con base en nodos de la red y otras protecciones como productos de seguridad de punto final. Aplicar configuraciones uniformes a los dispositivos y controlar los cambios a las configuraciones de dispositivos. Desactivar los servicios o las características de dispositivos que no son necesarios para apoyar las funciones de su misión. Garantizar que haya una política y que los dispositivos sean eliminados de manera segura.
- **Gestionar las vulnerabilidades de los dispositivos:** de manera regular, actualizar tanto los sistemas operativos y las aplicaciones que están instalados en sus computadores y otros dispositivos para protegerlos de ataques. En lo posible, activar las actualizaciones automáticas. Considerar el uso de herramientas de software para escanear dispositivos para buscar vulnerabilidades adicionales; remediar vulnerabilidades con altas probabilidades y/o efectos.
- **Capacitar a los usuarios:** capacite y vuelva a capacitar de manera habitual a todos los usuarios para que esté seguro de que están al tanto de las políticas y procedimientos empresariales de ciberseguridad y de sus roles y responsabilidades específicos como una condición de empleo.

- **Conocer los flujos de datos esperados de su empresa:** si usted sabe qué datos y cómo se espera que se usarán en su empresa, tendrá mayor probabilidad de notar cuando algo inesperado ocurra y lo inesperado nunca es bueno cuando se trata de la ciberseguridad. Los flujos de datos inesperados pueden incluir información de clientes que se exporta desde una base de datos interna y que sale de la red. Si ha contratado trabajo en la nube o a un proveedor de servicio administrado, converse con ellos sobre cómo hacen seguimiento de los flujos de datos y reportes, incluyendo eventos inesperados.

- **Mantener y monitorear los archivos de registro:** los archivos de registro (logs) son cruciales para identificar anomalías en sus computadores y aplicaciones empresariales. Estos archivos log registran eventos como cambios a sistemas o cuentas así como la iniciación de canales de comunicación. Considerar el uso de herramientas de software que puedan acumular estos archivos de registro y buscar patrones o anomalías del comportamiento de red esperado.

RESPONDER

Desarrollar e implementar las actividades apropiadas para tomar acción en relación con un evento de ciberseguridad detectado.

- **Asegurarse de que los planes de respuesta sean probados:** es aún más importante probar los planes de respuesta para asegurarse de que cada persona sepa sus responsabilidades al ejecutar el plan. Mientras más preparada esté su organización, la respuesta será probablemente más efectiva. Esto incluye conocer cualesquiera requerimientos de reportes legales o intercambio de información requerido.
- **Asegurarse de que los planes de respuesta sean actualizados:** probar el plan (y la ejecución durante un incidente) inevitablemente revelarán mejoras necesarias. Asegúrese de actualizar los planes de respuesta con las lecciones aprendidas.

RECUPERAR

Desarrollar e implementar las actividades apropiadas para mantener planes para la resiliencia y para reestablecer cualesquiera capacidades o servicios que hayan sido afectados durante un evento de ciberseguridad.

- **Comunicarse con las partes interesadas internas y externas:** parte de la recuperación depende de la efectividad de la comunicación. Sus planes de recuperación necesitan dar cuenta cuidadosamente de qué, cómo y cuándo se compartirá la información con varias partes interesadas para que todas las partes interesadas reciban la información que necesitan pero que ninguna información inapropiada se comparta.
- **Comprender el efecto de los eventos de ciberseguridad:** si se detecta un evento de ciberseguridad, su empresa debe trabajar rápida y exhaustivamente para comprender la amplitud y profundidad del efecto. Busque ayuda. Comunicar información sobre el evento con las partes interesadas apropiadas puede ayudarlo a mantenerse en buenos términos con sus socios, entidades supervisoras y otros (potencialmente incluyendo inversionistas) y mejorar políticas y procedimientos.
- **Coordinar con las partes interesadas internas y externas:** es importante asegurarse de que los planes de respuesta y las actualizaciones incluyan a todos los proveedores de servicio externos y todas las partes interesadas clave. Ellos pueden contribuir a mejoras en la planeación y la ejecución.

- **Asegurarse de que los planes de recuperación sean actualizados:** al igual que con los planes de respuesta, probar la ejecución mejorará la conciencia de los empleados y socios en cuanto a estos planes y resaltará las áreas de mejora. Asegúrese de actualizar los planes de recuperación con las lecciones aprendidas.
- **Gestionar las relaciones públicas y la reputación de la compañía:** uno de los aspectos clave de la recuperación es gestionar la reputación de la empresa. Cuando desarrolle un plan de recuperación, considere como hará la gestión de relaciones públicas para que el intercambio de información sea preciso, completo y oportuno —y no reaccionario.

Document translated courtesy of U.S. Department of State with support from the Digital Connectivity and Cybersecurity Partnership (DCCP). The official English language version of this publication is available free of charge from NIST at https://doi.org/10.6028/NIST.SP.1271.

NIST National Institute of Standards and Technology U.S. Department of Commerce