NIST SP 800-30 Rev. 1

Guía para la evaluación de riesgos

NIST SP 800-30 es una publicación que proporciona orientación sobre la realización de evaluaciones de riesgos. Describe estrategias para identificar, analizar y remediar riesgos. Las organizaciones utilizan NIST SP 800-30 para comprender la probabilidad y la gravedad de los riesgos, lo que les ayuda a tomar decisiones informadas sobre la asignación de recursos, la implementación de controles y la priorización de las medidas de remediación.

Este documento de cuatro páginas es una adaptación de la norma NIST SP 800-30 Rev. 1. El término "Rev. 1" significa que es la primera versión actualizada de esta publicación. El NIST revisa ocasionalmente sus documentos para incorporar nueva información, reflejar cambios en la tecnología y los requisitos regulatorios, o atender comentarios.

Nota:NISTCentro de recursos de seguridad informáticaContiene más información sobre SP 800-30 Rev. 1.

Fuentes de amenaza

La norma NIST SP 800-30 define y categoriza las fuentes de amenazas como entidades o circunstancias que pueden afectar negativamente a los sistemas de información de una organización. Esta información es útil para identificar y evaluar riesgos potenciales. Al consultarla, considere la intención y las capacidades de las fuentes de amenazas internas y externas.

Nota: En la siguiente tabla se enumeran algunas posibles*fuentes de amenaza*que podrían comprometer un servidor de base de datos de acceso público.

Tipo	Ejemplos	Descripción
Human	*Usuario estándar* • Empleado • Cliente *Usuario privilegiado* • Administrador del sistema *Grupo* • *do*competidor • Proveedor • Compañero de negocios • Estado nación *Forastero*	Amenazas derivadas de individuos o grupos que podrían explotar recursos cibernéticos, ya sea intencional o accidentalmente. Por ejemplo, podrían alterar datos de forma que afecte negativamente a la empresa. Alternativamente, podrían robar datos intencionalmente y dañar equipos empresariales.

	• Pirata informático • Hacktivista • Amenaza persistente avanzada (APT)	
Technological	*Hardware* • Salmacenamiento • Tratamiento • Comunicaciones *Software* • *EL*sistema(s) operativo(s) • Redes • software malicioso	Amenazas que se originan por factores no humanos. Por ejemplo, fallas de equipos debido al envejecimiento, el agotamiento de recursos u otras circunstancias.
Environmental	*Entorno operativo* • Controles de temperatura • Controles de humedad • Fuentes de alimentación defectuosas *Peligros naturales* • cortes de energía • Fenómenos meteorológicos extremos	Amenazas derivadas de factores accidentales no humanos. Por ejemplo, fallos de equipos causados por el entorno operativo.

Eventos de amenaza

NIST SP 800-30 define y categorizaeventos de amenazacomo casos reales en los que una fuente de amenaza explota una vulnerabilidad y causa daños o perjuicios a los sistemas de información de una organización. Esta información es útil para comprender mejor los tipos de riesgos a los que se enfrentan los activos. Se pueden identificar controles y contramedidas más eficaces al comprender los posibles eventos de amenaza.

Nota: La siguiente tabla enumera sólo algunas posibles*eventos de amenaza*que podrían comprometer un servidor de base de datos de acceso público.

Ejemplos	**Descripción**
Realizar reconocimiento y vigilancia de la organización.	La fuente de amenazas examina y evalúa las vulnerabilidades de la empresa a lo largo del tiempo utilizando diversas herramientas (por ejemplo, escaneo, observación física).

Obtener información sensible mediante exfiltración	La fuente de amenaza instala software malicioso en los sistemas de la organización para localizar y adquirir información confidencial.
Modificar/eliminar información crítica	La fuente de amenaza altera o elimina datos que son críticos para las operaciones comerciales diarias.
Certificados de falsificación artesanal.	Fuente de amenazacompromisosuna autoridad de certificación para hacer que sus conexiones parezcan legítimas.
Instalar rastreadores de red persistentes y específicos en los sistemas de información de la organización.	La fuente de amenaza instala un software diseñado para recopilar (rastrear) el tráfico de red de forma continua.período de tiempo.
Realizar ataques de denegación de servicio (DoS).	La fuente de amenaza envía solicitudes automatizadas y excesivas para saturar las capacidades operativas del sistema.
Interrumpir operaciones de misión crítica.	La fuente de amenaza compromete la integridad de la información de tal manera que impide a la empresa realizar operaciones críticas.
Ofuscar futuros ataques.	La fuente de amenaza toma acciones para inhibir la eficacia de los sistemas de detección de intrusiones o las capacidades de auditoría de la empresa.
Realizar ataques del tipo "hombre en el medio".	La fuente de amenazas intercepta sesiones entre sistemas internos y externos. Posteriormente, transmite mensajes entre sistemas organizacionales y externos que les hacen creer que se comunican directamente a través de una conexión privada.

Probabilidad de un evento de amenaza

En general, la*probabilidad*La evaluación de un evento de amenaza debe basarse en una combinación de factores. Por ejemplo, la evidencia disponible, la experiencia previa y su criterio experto.

Tenga en cuenta la intención/capacidades de una fuente de amenaza y los eventos de amenaza potenciales al producir una puntuación de probabilidad.

Valores cualitativos	Qcuantitativovalores	Descripción
Alto	3	Es casi seguro que una fuente de amenaza inicie un evento de seguridad. Un evento podría tener efectos múltiples, graves o catastróficos en las operaciones y los activos de la empresa.
Moderado	2	Es probable que una fuente de amenaza inicie un evento de seguridad. Un evento podría reducir significativamente la funcionalidad de las operaciones y los activos de la organización.
Bajo	1	Es muy poco probable que una fuente de amenaza inicie un evento de seguridad. Un evento podría tener efectos mínimos e insignificantes en las operaciones y los activos de la empresa.

Gravedad de un evento de amenaza

En general, la*gravedad*El impacto de una amenaza es una medida de su impacto potencial en las operaciones comerciales. Por ejemplo, ¿el evento causaría la interrupción total de una función comercial? ¿Podría interrumpir temporalmente un proceso comercial y pasar desapercibido?

Considere el impacto comercial de*eventos de amenaza*al producir una puntuación de gravedad.

Valores cualitativos	Valores cuantitativos	Descripción
Alto	3	Es casi seguro que una fuente de amenaza inicie un evento de seguridad. Un evento podría tener efectos múltiples, graves o catastróficos en las operaciones y los activos de la empresa.
Moderado	2	Es probable que una fuente de amenaza inicie un evento de seguridad. Un evento podría reducir significativamente la funcionalidad de las operaciones y los activos de la organización.
Bajo	1	Es muy poco probable que una fuente de amenaza inicie un evento de seguridad. Un evento podría tener efectos mínimos e insignificantes en las operaciones y los activos de la empresa.