La seguridad informática de los Sistemas de Automatización Industrial que incluyen infraestructuras críticas contra ataques informáticos es un factor que puede afectar de manera sustancial la disponibilidad y la operativa de sus funciones y la estabilidad del proceso o la continuidad del funcionamiento global del sistema industrial. Un diseño adecuado brinda una protección eficaz y eficiente que permita analizar los riesgos con antelación, determinar la probabilidad de sufrir ataques y su impacto en el proceso industrial.

Ciberseguridad: metodología de Evaluación de Riesgos aplicada a los sistemas industriales

Por ***Facundo Gagliardo, Carlos Samitier y Ariel Lichtig (Artec Ingeniería S.A.)***

Los ataques informáticos a los sistemas críticos de operación industrial tienen un impacto directo en la disponibilidad y la fiabilidad. Sin embargo, este no es el único factor para considerar, ya que la seguridad informática tiene asociado un impacto económico que puede desglosarse en dos componentes: uno tangible, que es la inversión que se realiza para proteger el sistema y, otro estimativo, que es el coste de las pérdidas causadas por los ataques exitosos.

El diseño de este tipo de sistemas requiere tomar las medidas de seguridad que garanticen el cumplimiento de los objetivos de disponibilidad y fiabilidad, incluso en presencia de ataques informáticos y que el costo de las medidas de protección contra ataques será aceptable considerando las limitaciones presupuestarias y la relación con el valor de los activos protegidos.

En consecuencia, es importante garantizar la eficacia de las medidas de protección con el objetivo de rentabilizar la inversión y asegurar la protección adecuada. Esto solo se puede lograr si se realiza un análisis de riesgos que incluya un estudio de la funcionalidad del sistema industrial y de sus vulnerabilidades para establecer las medidas de protección adecuadas.

Este trabajo presenta una metodología de análisis de riesgos basada en las directrices de las normas internacionales de seguridad específicas de los sistemas críticos de operación industrial.

Proceso de análisis

El riesgo de sufrir un ataque informático se expresa como la probabilidad de que una amenaza sea capaz de explotar alguna de nuestras vulnerabilidades con vectores de ataque realizables en el entorno de operación. Los vectores de ataque son el medio que utilizan los atacantes para explotar una vulnerabilidad y realizar un ataque.

Realizar un análisis de riesgos tiene como objetivo identificar los riesgos de nuestro sistema y su probabilidad de ocurrencia para determinar las actuaciones necesarias que garanticen la disponibilidad y la operación correcta del sistema. Esto se consigue al identificar los riesgos que son factibles en el sistema y que tienen un efecto sobre su funcionamiento.

El proceso de análisis parte de la estimación de las amenazas, que realmente implicarán un riesgo solo si existe una vulnerabilidad que pueda ser explotada.

En consecuencia, conocer las vulnerabilidades es el primer paso para un análisis de riesgos, ya que si no existe la vulnerabilidad tampoco existe el riesgo.

Para evaluar cómo las amenazas se materializan en nuestro sistema es importante considerar sus características específicas como se describe a continuación.

Características específicas de los sistemas de automatización industrial

Aunque es ampliamente conocido que la mayoría de los sistemas de automatización industrial son de "Misión Crítica", en ocasiones no se considera sus implicaciones. Es decir, se trata de sistemas que deben ser tolerantes a fallos, lo que implica que la avería de un componente no debe afectar su funcionamiento. Sin embargo, en esta definición no se consideraron los posibles ataques informáticos que introducen nuevos modos de fallo con posibles impactos mayores que las averías. En definitiva, el objetivo de

diseño de estos sistemas debe ser la disponibilidad, esto es, el tiempo total en el que el sistema se encuentra operativo. La indisponibilidad puede ser causada por averías o por ataques informáticos. Esto implica que estos sistemas deben incorporar un cierto nivel de redundancia para tolerar averías y protección frente a ataques informáticos para reducir la probabilidad de que un ataque tenga éxito y, de esta forma, garantizar el objetivo de disponibilidad.

Para incorporar medidas de seguridad que sean efectivas es imprescindible conocer el modo de funcionamiento del sistema que se desea proteger. Una característica relevante es que a pesar de utilizar tecnologías normalizadas, como Ethernet y el protocolo IP, su principio de funcionamiento y arquitectura no están relacionados con las típicas aplicaciones de los sistemas de la información (IT) puesto que es habitual que las funciones de estos sistemas estén implementadas mediante servidores que interaccionan entre sí sin necesidad de un cliente y de automatismos distribuidos basados en mensajes espontáneos en tiempo real.

Los equipos utilizados para su implementación son dispositivos inteligentes que incorporan un gran número de funciones con un nivel de criticidad muy diferente. Esto dificulta el análisis de vulnerabilidades y principalmente determinar el efecto de los ataques sobre esas funciones.

Un tercer factor que se debe considerar es el hecho de que las nuevas tecnologías de automatización permiten implementar funciones de forma distribuida, lo cual complica el análisis porque, además de los equipos, intervienen las comunicaciones en la implementación de las funciones del sistema.

Realmente, el problema es proteger las funciones del sistema, es decir, el foco de protección frente a ataques informáticos en lugar de estar en los equipos debería estar en las funciones, ya que las funciones se realizan con diferentes recursos del sistema y, en general, se encuentran distribuidas con lo cual su desempeño depende de varios equipos y de las comunicaciones asociadas.

Análisis de vulnerabilidades

El análisis de vulnerabilidades provee los datos de partida para el diseño del esquema de protección frente a ataques informáticos.

En efecto, los ataques exitosos son los que logran explotar una vulnerabilidad para realizar una acción maliciosa. Estos ataques se evitan con medidas de protección entre los atacantes y los equipos con vulnerabilidades.

Estas medidas de protección deben ser las adecuadas para evitar que los ataques tengan éxito. Por lo tanto, es imprescindible conocer las vulnerabilidades y todos los detalles de cómo pueden ser explotadas para tomar las medidas de protección adecuadas.

Existen varias organizaciones que analizan los equipos y las aplicaciones de mercado para detectar sus vulnerabilidades. Si bien no existe una norma internacional para la medición de las vulnerabilidades, se ha alcanzado un consenso internacional sobre cómo evaluar las vulnerabilidades[1] y es el siguiente:

Las vulnerabilidades se identifican mediante el código CVE (*Common Vulnerability Exposure*). Asociado al código se incluye la descripción de la vulnerabilidad, el vector de ataque utilizado y el nivel de severidad.

El nivel de severidad de una vulnerabilidad se cuantifica mediante el código CVSS (*Common Vulnerability Scoring System*). El coeficiente CVSS es el resultado de una fórmula que indica el nivel de severidad en la escala de 0 a 10.

El cálculo del CVSS considera los siguientes factores:

- Vector de acceso.
- Complejidad del acceso.
- Complejidad de la autentificación.
- Nivel de confidencialidad. Facilidad para obtener información confidencial.
- Integridad. Facilidad para modificar la información.
- Disponibilidad. Facilidad para bloquear alguna funcionalidad atacada.

La detección de una vulnerabilidad y su valoración mediante el coeficiente CVSS facilita la toma de decisiones, debido a que valora la severidad además de aportar información sobre la amenaza asociada, el vector que se puede utilizar y el efecto sobre el elemento atacado.

Conocer los detalles de funcionamiento del vector de ataque es importante, ya que si el vector no es realizable en nuestro sistema, la vulnerabilidad no podrá ser explotada y, por lo tanto, no tendrá un riesgo asociado.

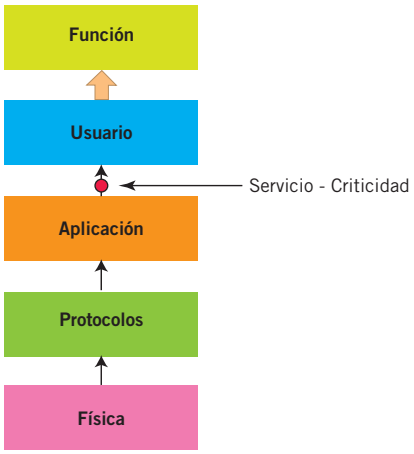

Figura 1. **Modelo de capas.**

En resumen, el riesgo viene dado por la existencia de una amenaza que al utilizar un vector explota una vulnerabilidad de algún componente del sistema y provoca un mal funcionamiento de una o varias de sus funciones.

Riesgo e impacto

Conocer los riesgos es importante, pero también debemos considerar que las medidas de protección deben ser proporcionales al impacto del ataque sobre las funciones del sistema teniendo en cuenta el nivel de criticidad de cada función.

Proteger un sistema de automatización industrial en función del riesgo produce una protección que no es eficiente y, por lo tanto, tiene un coste elevado al que se suma que las medidas de protección innecesarias pueden degradar el desempeño del sistema.

En consecuencia, el diseño de la seguridad informática debe centrarse en el impacto de los ataques sobre las funciones críticas. La dificultad está en determinar el impacto sobre cada una de las funciones del sistema, debido a su complejidad. La forma de abordar un problema tan complejo es descomponerlo en problemas más simples. Esto se consigue al aplicar los principios de estructuración en capas introducidos en la norma IEC 62351-1[2]. Con esos principios se propone el modelo de capas que se muestra en la figura 1.

En la figura podemos apreciar las diferentes capas que conforman cada función del sistema:

- La capa física incluye los aspectos físicos de los equipos o medios de comunicación utilizados por la función. En esta capa solo se consideran los ataques físicos, como interrumpir la alimentación e interferencias de radiofrecuencia, etc.
- La capa de protocolo incluye los protocolos utilizados para comunicar los diferentes elementos que implementa la función. En consecuencia, en esta capa se consideran los ataques a los protocolos, como "Man-in-the-Middle", denegación de servicio, etc.
- La capa de aplicación se refiere al software que implementa el servicio. Estos servicios se deben proteger para evitar ataques de suplantación de servidores y otros ataques como se describe en la norma IEC 62443.
- La capa de usuario se refiere a la persona o automatismo que al utilizar un servicio implementa una función. Por ejemplo, un operador que ejecuta un mando, el automatismo de regulación de un proceso industrial.

Este modelo refleja lo que sucede en la realidad: un ataque no se dirige y afecta un concepto genérico, sino que afecta un elemento concreto, que a su vez, afecta la función que soporta el sistema.

En este modelo podemos observar como la función hereda las vulnerabilidades de las capas que la implementan. Las vulnerabilidades de cada capa afectan a las capas superiores de diferente forma, de esta manera puede suceder que el efecto de un ataque aumente o disminuya al propagarse hacia las capas superiores. La bondad de un diseño consiste en que los ataques a las capas inferiores queden atenuados por las capas superiores de forma que se reduzca el efecto del ataque sobre la función.

Principios de diseño similares se aplican para implementar funciones tolerantes a fallos, debido a averías o mal funcionamiento de alguno de sus componentes. Estos principios de

diseño deben considerar el efecto de los ataques para ello es imprescindible conocer las vulnerabilidades de cada capa por separado.

Evaluación transversal del impacto

Además de los ataques dirigidos a una vulnerabilidad conocida de alguna de las capas descriptas, existen lo que se conoce como riesgos transversales o de entorno, esto es, riesgos que provienen de elementos comunes a todo el sistema y que pueden afectar de diferente forma a cada una de las capas. Estos riesgos no están relacionados únicamente con los aspectos tecnológicos, sino que también incluyen aspectos relacionados con los recursos humanos y con la organización de la empresa, entre los que se deben incluir los criterios genéricos de diseño y mantenimiento. De hecho, representan factores o componentes genéricos que pueden afectar a la seguridad del Sistema de Operación.

Los principales factores que introducen este tipo de riesgos son los siguientes:

- Políticas de seguridad. La falta de políticas de seguridad, o de políticas aplicadas o difundidas inadecuadamente, pueden representar un factor que facilite algún tipo de ataque e incluso aumente su impacto.
- Procedimientos que afectan la seguridad. Los procedimientos operativos pueden tener un impacto sobre los ataques, bien para prevenirlos o atenuar su efecto o, en el caso de que no existan medidas de seguridad específicas, facilitar ciertos tipos de ataque.
- Cultura de seguridad informática. Una cultura de seguridad informática poco desarrollada provoca que se menosprecien las amenazas, no se tomen las medidas de seguridad adecuadas y, por lo tanto, aumente el efecto de un ataque.
- Capacitación. La capacitación debe incluir los aspectos de seguridad informática intrínsecos a la operación y el mantenimiento del sistema con el objetivo de que las personas que operan y mantienen el sistema apliquen las mejores prácticas para prevenir ataques informáticos.
- Criterios de configuración. La configuración de los equipos que implementan el sistema debe considerar los criterios de seguridad informática para evitar el uso de claves de acceso por defecto o dejar puertas traseras habilitadas, etc.
- Comunicaciones externas. Las comunicaciones entre las diferentes instalaciones, los centros de control y operación y las instalaciones periféricas pueden ser atacados, situación que facilita un ataque posterior a las funciones del sistema. La seguridad informática de estos canales y de la red de área extensa que los implementa (WAN) debe ser tenida en cuenta, ya que puede introducir vulnerabilidades. La aplicación de gestión de las comunicaciones es el elemento más crítico, porque si un atacante gana el control de ese centro, puede modificar la red a su antojo y realizar diferentes tipos de ataques o facilitar ataques externos.

	USUARIO	APLICACIÓN	PROTOCOLO	FÍSICA
POLÍTICAS	X+	X-	---	X
PROCEDIMIENTOS	X+	X--	---	X-
CULTURA	X+	---	---	X-
SERVICIOS	X+	X	---	---
CONFIGURACIÓN	X-	X	X	X
COMUNICACIONES	X	X	X	X--
TECNOLOGÍA	---	X	X	X+
ARQUITECTURA	---	X	X-	X-

Tabla 1. **Relaciones transversales.**

- Tecnología. Potenciales fallos en modo común. Hay tecnologías intrínsicamente seguras, como los enlaces de fibra óptica subterráneos mientras que otras son intrínsicamente inseguras como el wifi. La selección de la tecnología introduce vulnerabilidades intrínsecas en la capa física, la capa de protocolo y la de aplicación.
- Arquitectura del sistema. La arquitectura del sistema puede facilitar la propagación de un ataque a una capa superior o puede frenar el impacto.

En la tabla 1 se muestra un ejemplo de las interacciones entre los factores transversales de entorno y las capas. Cada casilla muestra si existe interacción y si esa interacción aumenta o disminuye el impacto de un ataque.

Con la aplicación de estos factores correctivos se puede obtener la matriz impacto-probabilidad (Figura 2).

Cada celda de la matriz de impacto contiene todas las funciones en riesgo. Incluye la siguiente información:

- Identificación de la función.
- Vulnerabilidad asociada que indica su código de identificación CVE.
- Origen y ubicación de la vulnerabilidad.
- Vector utilizado.
- Impacto estimado.

A partir de estas informaciones se pueden tomar las medidas de protección adecuadas a tiempo que obtenemos una evaluación de los aspectos de seguridad informática del entorno, que se debe utilizar para tomar las medidas correctivas que permitan minimizar el efecto de los ataques.

La matriz impacto-probabilidad aporta una información de priorización de las acciones, es decir, clasifica las vulnerabilidades que producen un mayor impacto con una mayor probabilidad y, por lo tanto, son las que requieren una toma de medidas de protección urgente.

		PROBABILIDAD				
		1 REMOTO	2 IMPROBABLE	3 PROBABLE	4 MUY PROBABLE	5 CIERTO
IMPACTO	1 TRIVIAL	1	2	3	4	5
	2 MENOR	2	4	6	8	10
	3 MODERADO	3	6	9	12	15
	4 MAYOR	4	8	12	16	20
	5 CRÍTICO	5	10	15	20	25

Figura 2. **Matriz impacto-probabilidad.**

Conclusiones

La criticidad de los sistemas de automatización industrial, su arquitectura y su funcionamiento requiere la implementación de medidas específicas de protección frente a ataques informáticos que permitan obtener un nivel de protección que garantice la disponibilidad de la operación.

El análisis de vulnerabilidades es un paso fundamental en la implementación de un sistema seguro, ya que proporciona los datos de partida para determinar las medidas de protección necesarias.

La complejidad de los sistemas de automatización industrial requiere una metodología de análisis específica que considere los principios de funcionamiento y las prioridades de la operación. Utilizar la metodología de IT brinda resultados que no tienen la precisión adecuada, como consecuencia no permiten optimizar el sistema ni garantizar el cumplimiento de los objetivos de disponibilidad, además se suma el riego de que pueden afectar al desempeño en tiempo real del sistema.

En este artículo se ha mostrado la importancia de conocer el impacto de los ataques informáticos sobre las funciones del sistema de automatización, ya que es un efecto perceptible y evaluable que afecta el desempeño. La metodología de análisis de impacto basado en el modelo de capas complementado con el análisis del entorno permite obtener resultados que reflejan el impacto de los ataques con mayor precisión y optimizar las medidas de protección frente a ataques informáticos.

Referencias

1. http://cve.mitre.org
2. IEC 62351-1. Communication network and system security-Introduction to security issues.

IEC 61850 series. Telecommunication networks and systems for power utility automation. Edition 2.

ISA/IEC 62443 series. Industrial communication networks- Network and system security.