Homo Sapiens, el eslabón débil de la seguridad de la información

» Claudio Milio
CAETI, Universidad Abierta Interamericana, Argentina
Claudio.milio@uai.edu.ar

Resumen

La información es uno de los activos más importantes que posee una organización y es generada, normalmente, por sistemas automatizados. Dependiendo de quién la deba utilizar, es posible que estos sistemas deban realizar predicciones o decisiones no estructuradas en la que la IA (Inteligencia artificial) ayuda a este proceso. La información tiene la particularidad tener un atributo muy importante que es el tiempo de validez. Hay información que debe ser tratada de manera inmediata, como es el caso de la producida en redes emplazadas en entornos industriales o en la punta de la pirámide de la organización donde es imprescindible su tratamiento para la subsistencia. Esa información debe ser protegida de diferentes amenazas. Y en este punto es cuando los responsables de las organizaciones deben ser conscientes del riesgo potencial de perder información valiosa. Ya no es suficiente pensar si la amenaza se cumple o no, sólo nos tenemos que preguntar cuándo va a suceder. La mejor manera de proteger los datos es gestionar y reducir los riesgos informáticos que pueden afectar a un sistema, tanto en su capacidad de operación como en la posibilidad de generar riesgos en la salud y seguridad pública, a través de la generación de buenas prácticas, la detección temprana de actividades sospechosas a través de la inteligencia artificial y la creación de algoritmos de encriptación compactos que neutralicen las amenazas.

PALABRAS CLAVES: RIESGOS INFORMÁTICOS, SEGURIDAD PÚBLICA, BUENAS PRÁCTICAS, INTELIGENCIA ARTIFICIAL, ENCRIPTACIÓN.

Homo sapiens, the weak link of information security

Abstract

Information is one of the most important assets that an organization has and is normally generated by automated systems. Depending on who should use it, it is possible that these systems have to make predictions or unstructured decisions in which AI (artificial intelligence) helps this process. The information has the particularity to have a very important

attribute that is the validity time. There is information that should be treated immediately as is the case of the one produced in networks located in industrial environments or at the tip of the pyramid of the organization where its treatment for subsistence is essential. That information must be protected from different threats. And at this point is when those responsible for organizations must be aware of the potential risk of losing valuable information. It is no longer enough to think if the threat is met or not, we just have to ask when it will happen. The best way to protect data is to manage and reduce the computer risks that can affect a system, both in its operational capacity and in the possibility of generating risks in public health and safety, through the generation of good practices, the early detection of suspicious activities through artificial intelligence and the creation of compact encryption algorithms that neutralize threats.

KEYWORDS: COMPUTER RISKS, PUBLIC SECURITY, GOOD PRACTICES, ARTIFICIAL INTELLIGENCE, ENCRYPTION.

1. **Introducción**

Los sistemas informáticos que forman parte del universo corporativo, como el control de procesos de negocios, apoyo a toma de decisiones y sistemas específicos de control de procesos industriales, entre otros, pueden tener vulnerabilidades que, encontradas por un tercero interesado en la información o en los procesos que manejan y controlan, son utilizadas para acceder y tomar control del ellos.

A fines de 2019, la empresa Prosegur España publica en Twitter que fue víctima de un ataque del tipo Ramsonware (RIUK) y tuvo que paralizar sus servicios, restringiendo todas las comunicaciones (ABC Software, 2019). El objetivo de este *malware* es encriptar toda la información que se encuentra en la computadora. Una vez ejecutado el *script*, trata de comprometer a los dispositivos que están conectados a la red y luego solicita un rescate en *bitcoins* a cambio del desencriptado. Estos ataques son dirigidos en su mayoría y utilizan herramientas de ingeniería social para engañar al usuario y hacer que lo ejecute.

Según Kaspersky, el interés de este tipo de software ahora gira sobre lo respaldos de seguridad.

(Kaspersky, 2019).

También existen casos de ex empleados que hackearon o robaron información sensible propiedad de sus ex empleadores. (Infobae, 2019).

Ataques a empresas de distinto tipo de industrias como la petrolera (Pemex, mexicana) y la hotelera, (20 cadenas hoteleras de alta gama según Kasperky), entre otras, suceden diariamente. Algunas con resultados de riesgo para la economía de un país o la salud humana.

Todos estos ataques tienen en común la utilización de técnicas para engañar al usuario y así obtener acceso a la información.

El avance de las herramientas de tecnología, la conectividad entre dispositivos cada vez más presentes y un futuro próximo donde la sociedad estará, de manera irremediable, interrelacionada

a través de la explosión de Internet de la Cosas, debe verse como un serio problema que atenta contra la individualidad del ser humano, pero seguramente también será un riesgo de seguridad al que tendríamos que prestar la atención necesaria para minimizar los riesgos que en apariencia estamos dispuestos a tomar.

El presente artículo trata el aspecto de la seguridad de la información, dejando el supuesto problema de la pérdida de individualidad para otro estudio.

2. **Problemas**

La posibilidad de la ausencia de políticas de seguridad y de procedimientos que orienten a un comportamiento estándar y estratégico para neutralizar o minimizar los riesgos potenciales, desde la seguridad física y lógica hasta la detección y tratamiento de actividades que pueden producirse por un ataque externo o interno es uno de los principales inconvenientes que deben ser abordados en cualquier instalación donde la tecnología informática está presente.

No se deben olvidar las debilidades que pudieran existir en el *hardware* del sistema de información, debido a la incorrecta configuración, y en especial, en el diseño de la red que, por la falta de seguridad entre las comunicaciones de sus componentes, podrían permitir el acceso del sistema desde el interior o desde exterior.

En este artículo no se tratará el impacto que podría producir IOT como riesgo potencial dentro de una red corporativa o industrial.

En la figura 1 se observa una vista básica de una red SCADA donde se expone una arquitectura típica.

En esta ilustración se puede observar que, aunque podemos inferir que los dispositivos de seguridad están bien configurados y el sistema SCADA está protegido, no podemos asegurar que estén exentos de ataques externos e internos. Hay un riesgo y amenaza potencial: la interfaz hombre-sistema.

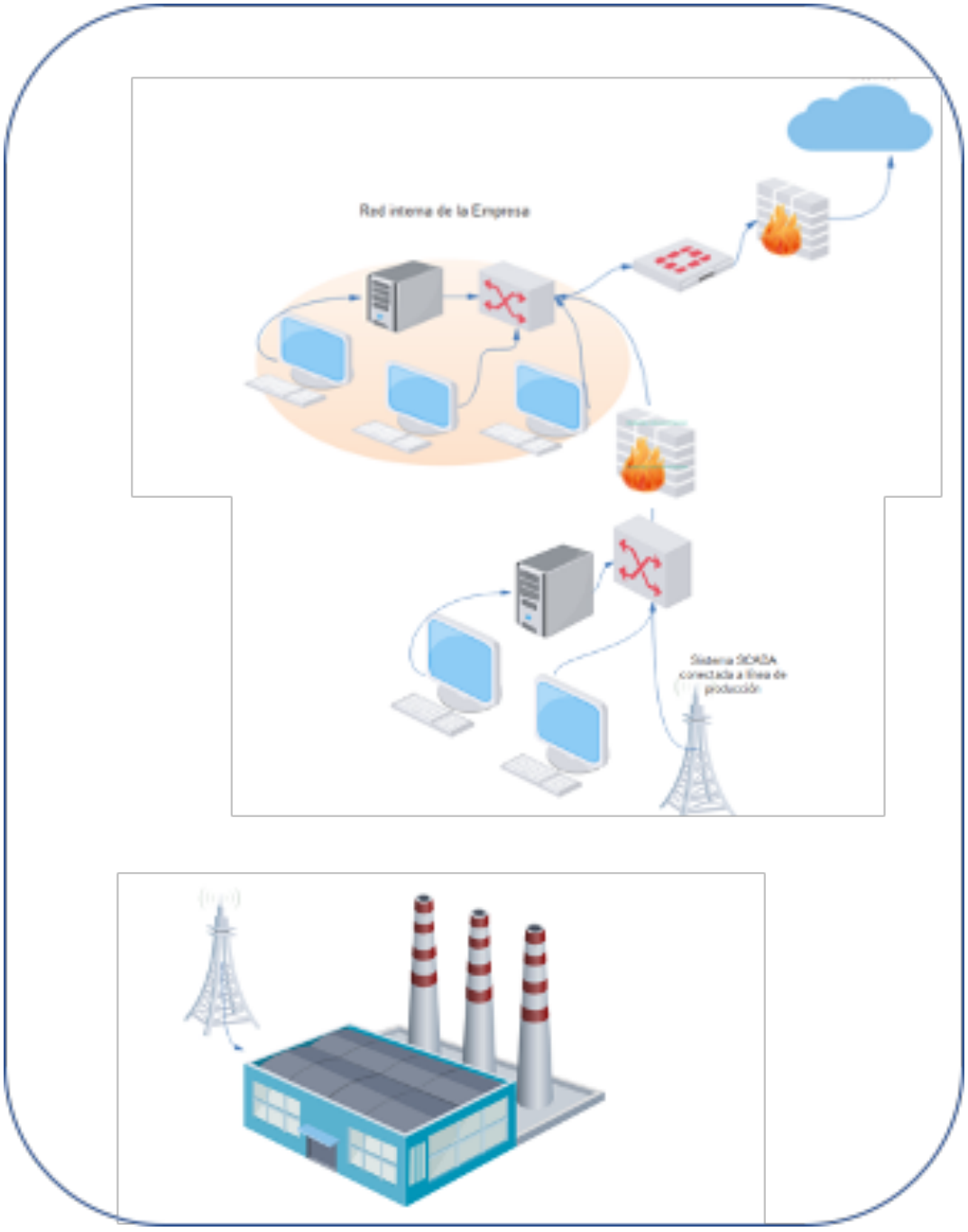

Figura 1. Esquema de una red corporativa con control SCADA.

El ser humano, por impericia o como objetivo real, puede generar y o modificar reglas de acceso, efectuar un ataque de envenenamiento ARP, modificar la programación de los PLC[1] alojados en la zona de producción que pertenecen a la red industrial, preparar la red para un acceso que no debería ser permitido y así comprometer seriamente todo el sistema de la Organización, incluido el sistema SCADA, causando daños físicos, económicos y riesgo para la salud humana.

1 PLC: Controladores programables

La evaluación de riesgos y la elaboración de un plan de mitigación es raramente llevada a cabo, profundizando el probable daño que puede ser ocasionado ante una potencial amenaza.

3. Soluciones

Este trabajo tiene como objetivo establecer mejores prácticas a través de la implementación de normas y procedimientos acompañados por la capacitación de las personas responsables, que puedan resultar en la construcción de un ambiente seguro.

Para lograr el desarrollo de este trabajo, se utilizará el *framework*[2] creado por el Instituto Nacional de Normas y tecnologías (NIST)[3] que depende del Departamento de Comercio de los Estados Unidos. El objetivo de este ambiente de trabajo es recopilar distintas normas referidas a la seguridad de información tales como NIST e ISO[4]. En base a este trabajo se deben generar las políticas básicas y estándar que debe tener un ambiente de riesgo como el que se está definiendo.

No existe la organización sin riesgo

Como ninguna organización puede establecer que no tiene riesgos ante distintos eventos internos y/o externos, se debe analizar la injerencia que puede tener cada riesgo para poder establecer los controles necesarios para mitigarlos.

Buenas prácticas para minimizar el riesgo potencial de ataques

Dentro del marco de la información que nos brinda el *framework* de NIST, se ha elegido la norma ISO/IEC 27001:2013 en su anexo 5; y la norma ISO/IEC 27002, que establece las buenas prácticas para llevar a cabo una política de seguridad.

Para los sistemas SCADA, dentro de las redes industriales, se utilizará como guía la norma NIST SP 800-82 Rev. 2, que brinda una ayuda sobre cómo puede asegurase los sistemas de control industrial, (SCADA, DCS, PLC). (NIST, 2015).

La norma ISO/IEC 27002 contiene un catálogo de amenazas que los sistemas de información deben tener en cuenta. Se enumerará alguna de ellas en la siguiente figura:

2 Framework - Entorno de trabajo: conceptos, prácticas y criterios para enfocar un tipo de problemática
3 NIST: Agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.
4 ISO: Organización Internacional de Normalización

Las relacionadas a imprevistos como desastres naturales y ambientales.	Manipulación de información
Interrupción de la fuente de alimentación	Accesos no autorizado a los sistemas de TI o a aplicaciones o sistemas
Interrupción de las redes de comunicación	Destrucción de dispositivos o soportes de almacenamiento
Espionaje	Fallo de dispositivos o sistemas
Pérdida o Robo de dispositivos, soportes de almacenamiento y documentos	Vulnerabilidades o errores del software
Mala planificación o falta de adaptación	Violación de leyes o regulaciones
Divulgación de información sensible	Uso no autorizado o administración de dispositivos y sistemas
Manipulación de hardware o software	Abuso de Autorizaciones
Terrorismo	Software malicioso
Coerción, extorsión o corrupción	Ataques DoS o denegación de servicio
Robo de identidad	Ingeniería Social
Pérdida de datos	

Figura 2 Amenazas que deben tenerse en cuenta

Cada una de estas amenazas deben ser evaluadas y tratadas teniendo como objetivo minimizar la ocurrencia y el impacto en caso de producirse.

La norma ISO/IEC 27002 junto con la norma ISO/IEC 31000[5], ayudan a identificar factores externos e internos que afecten a la seguridad de la información.

Para fortalecer la seguridad se deberá establecer una política de seguridad y el manual de seguridad y los procedimientos que contemplen cuáles son las necesidades y expectativas, además de cuál es el alcance de la política de seguridad, establecer los roles y responsabilidades para cada área y tarea.

También deben establecerse los criterios de cómo se identificarán y evaluarán los riesgos, asegurar la existencia de recursos económicos y humanos necesarios, y la competencia de las personas para las tareas asignadas.

5 Norma que refiere a la gestión de riesgos

La comunicación

Un punto importante pero que rara vez es contemplado con seriedad, es la concientización, la comunicación y la documentación.

Si las personas no entienden la importancia de una política de seguridad o desconocen los riesgos, resultará imposible mitigar los mismos. Esta es principal razón para realizar una capacitación para lograr una inducción acerca de la problemática y se establecerá un mecanismo de comunicación para que las personas involucradas estén informadas sobre la actualidad en lo que, a riesgos, mejoras y cualquier otra actividad pueda ser realizada.

Un enfoque específico sobre la seguridad en las redes industriales

Los ataques realizados en entornos de redes industriales no escapan a lo que hasta ahora se ha expuesto en este artículo. Los mismos problemas aplican a este ambiente, fundamentalmente los referidos a la relación de las personas con los sistemas, falta de capacitación, descuidos, errores, espionaje, etc.

Pero un aspecto fundamental es la prevención de accesos no autorizados, de forma local y/o remota.

En el génesis de la producción industrial, los controles eran manuales, no existía ningún riesgo de ingreso remoto o autorizado y no existía ninguna red que transmitiera información.

Los únicos riesgos potenciales eran los generados por las personas.

Con el correr de los años y la aparición de los microprocesadores, las líneas de fabricación o armado fueron modificando su estructura hasta convertirse lo que actualmente llamamos redes industriales, (figura 1).

Aspectos para tener en cuenta

Además de lo dicho en este artículo, se debe establecer una segmentación entre la red corporativa y la red industrial que contiene los microprocesadores (PLCs,), el sistema SCADA y todo otro dispositivo físico que pueda intervenir en la red.

También es importante:

- Aislar el sistema SCADA protegiéndolo de posibles ataques locales o remotos.
- Instalar dispositivos IDS (sistema de detección de intrusión) y dispositivos software de inspección de paquetes en puntos clave de ente el SCADA y los procesadores que le transmiten información, permitiendo el análisis de la información que es transmitida por los protocolos Modbus[6] (Modbus, 2019) y TCP/IP, DNP3[7] (DNP, 2019) entre otros.
- Establecer reglas de accesos en dispositivos firewall diseñados para este ambiente.
- Instalar y mantener actualizado software de detección de *backdoors*, troyanos y *malware*.
- Establecer un cifrado seguro en la comunicación de datos.

6 Protocolo industrial creado en 1979 para entornos industriales para comunicar distintos dispositivos.
7 Estándar de comunicación para el control y supervisión de procesos industriales

Lamentablemente no existe comercialmente un algoritmo de encriptación que asegure una transmisión desde los sensores hasta el sistema SCADA. El proyecto de investigación de ciberdefensa de infraestructuras industriales[8], está trabajando en esta problemática.

Enfoque de prueba de la eficacia de la seguridad

Además de las auditorías que deben efectuarse según la planificación realizada, es importante realizar pruebas de penetración al sistema de información corporativo y a las redes de entornos industriales para establecer la fortaleza y encontrar las debilidades o vulnerabilidades para que puedan ser eliminadas o neutralizadas. Esta prueba es realizada por personal experto en Hacking Ético.

Sin profundizar en estas técnicas, intentaré explicar los pasos para poder lograr un buen pentest.[9]

Prácticamente, las posibilidades que la organización tenga o pueda generarse un entorno de prueba / control de calidad son pocas. En estos casos se deberán evaluar los sistemas y red que están en producción teniendo el cuidado de no comprometer su normal funcionamiento. Si el evaluador pertenece a la organización, normalmente existe un principio de acuerdo sobre en qué cuestiones se trabajará en la prueba. Si el evaluador, experto en hacking ético, es contratado para realizar las pruebas de penetración, normalmente trabajan bajo tres modalidades. Cada una de ellas establecerá el grado de profundidad y de secreto entre las partes.

Exploración de superficie

El evaluador tratará de saber toda la información sobre la organización, sus sistemas, objetivos y funciones, los sistemas de misión crítica, cuáles son los usuarios finales y cómo impactan en la organización. También hará un reconocimiento de la infraestructura, cómo está diseñada la red y cuáles son los mecanismos de seguridad que pudieran tener instalado. Todos estos datos sirven para encontrar vulnerabilidades conocidas de los dispositivos y del software instalado. Con esta información el evaluador puede estudiar el esquema de ataque que utilizará.

Pruebas de ataque

Con la información recolectada, el pentester puede comenzar a intentar vulnerar los sistemas y los dispositivos de infraestructura. El evaluador atacará los puertos abiertos, tratando de entrar a los sistemas. Ejecutará acciones que provoquen denegación de servicios, buscando la paralización del sistema. Utilizará contraseñas por defecto de los dispositivos y ataques de fuerza bruta *online* para poder ingresar a los sistemas probando las fortalezas de las contraseñas utilizadas por los usuarios y verificará que las contraseñas por defecto de los dispositivos y software hayan sido cambiadas. También verificará la capacitación de los usuarios en cuanto a riesgos de seguridad informática.

8 Proyecto de investigación llevado a cabo en la casa de altos estudios CAETI de la universidad abierta interamericana, Argentina.
9 Pentest es una prueba de la fortaleza de la seguridad desplegada en los sistemas de información y sus redes para detectar debilidades en la funcionalidad y riesgos de perder datos o robo de información.

Revista Abierta de Informática Aplicada/vol 4 (2020): 41-50
ISSN 2591-5320

Algunas verificaciones importantes:

- ¿Las credenciales por defectos han sido cambiadas?
- ¿Existen usuarios con roles administrador o invitados no utilizados?
- ¿En el caso de SCADA, los PLC son accedidos desde los dispositivos correctos?
- ¿Los sistemas críticos están aislados? ¿Los sistemas SCADA están separados del resto de la red?
- ¿La organización sigue el plan de seguridad establecido por la dirección?

Informes:

Luego que se haya llevado a cabo la prueba, el pentester generará dos informes con distinto grado de detalle técnico. Un informe ejecutivo para los responsables con detalles generales de las vulnerabilidades encontradas y puntos de mejora y un informe técnico con la misma información, pero con más detallados para que los técnicos puedan asegurar las debilidades documentadas.

Conclusiones

Hasta aquí se ha realizado un análisis superficial sobre los problemas de seguridad en instalaciones de organizaciones y en especial en entornos SCADA, tratando de concientizar que las buenas prácticas son un punto importante en la protección y mitigación de amenazas que seguramente, en algún momento vamos a experimentar.

Bibliografía

» ABC Software (28 de 11 de 2019). *Prosegur sufre un ciberataque y se ve obligada a paralizar sus servicios*. Obtenido de https://www.abc.es/tecnologia/informatica/software/abci-prosegur-sufre-ciberataque-y-obligada-paralizar-servicios-201911271938_noticia.html

» DNP. (2019). *DNP DISTRIBUTED NETWORK PROTOCOL*. Obtenido de https://www.dnp.org/

» infobae. (2 de 10 de 2019). *Infobae.com*. Obtenido de https://www.infobae.com/america/2019/10/02/un-ex-empleado-de-yahoo-hackeo-6000-correos-robo-videos-y-fotos-con-contenido-sexual/

» International Organization for Standardization. (18 de 12 de 2019). *ISO*. Obtenido de https://www.iso.org/home.html

» Kaspersky (2 de 12 de 2019). *Kaspersky.com*. Obtenido de https://latam.kaspersky.com/about/press-releases

» Modbus. (2019). *Modbus organization*. Obtenido de http://www.modbus.org/

» NIST. (2015). *Guide to Industrial Control Systems (ICS) Security*. Obtenido de https://www.nist.gov/publications/guide-industrial-control-systems-ics-security