CIBERSEGURIDAD en las plantas de producción, ¿por qué es esencial?

La ciberseguridad en las plantas es uno de los aspectos que más preocupa ante el desarrollo de la cuarta revolución industrial, conocida como Industria 4.0, ya que puede afectar seriamente desde la productividad, la destrucción de la fábrica e instalaciones, hasta el impacto ambiental y daños a la reputación corporativa. Por ello, cuidar los riesgos es un gran reto digital. • **Esther Vázquez (*)**

El 70% de las empresas han sufrido ciberataques a través de dispositivos IoT, según un estudio de Extreme Networks (enero 2020). Este mismo estudio señala que "los profesionales del sector bancario son los más preocupados (un 89% dice manifiesta tener plena confianza en la seguridad de red), seguidos de los del sector sanitario (88%), y de servicios profesionales (86%)".

En otro informe publicado en 2019 por Verizon se indica que el uso indebido de credenciales y las malas prácticas internas fueron el principal patrón de incidentes de seguridad durante el 2019.

El desarrollo y uso extensivo de las Tecnologías de la Información y las Comunicaciones (TIC), las cuales se refieren a conceptos como tecnologías digitales, IoT, conectividad, industria 4.0, Internet, ha supuesto una revolución indiscutible, pero también ha traído nuevas amenazas: los ciberataques.

Son tantas las vulnerabilidades a las que nos vemos expuestos y tantos los medios por los que nos pueden atacar que se podría hablar de que ha nacido una nueva forma de hacer la guerra en la que las reglas han cambiado de manera radical.

Ya se escucha que los ciberataques son la primera amenaza mundial incluso por delante del cambio climático. Cuando hablamos de ciberseguridad hablamos de proteger las estructuras digitales (hardware, software, datos) de ataques digitales y accesos no autorizados, por lo tanto, la ciberseguridad comprende todas aquellas tecnologías y medidas que se implementen para tal fin.

Las primeras empresas que se han visto más afectados fueron las grandes compañías que operaban en los sectores financiero, energía y salud. Hoy, dichos sectores ya llevan muchos años de experiencia y ya han aprendido a protegerse mejor. Es por ello que los ciberdelincuentes han cambiado su estrategia y ahora en su punto de mira está el sector alimentario.

(*) Directora de EV Consultoría Alimentaria. Interim Manager en Empresas Alimentarias. España.

¿Quiere decir que el sector alimentario fue inmune a los ciberataques hasta ahora? La respuesta es no. El número de ciberataques en el sector alimentario han ido creciendo al menos en los últimos 13 años, pero hasta el momento sus consecuencias no se habían considerado de alta gravedad, razón por la que quizá no se hayan derivado muchas noticias al respecto.

Sin embargo, todos los datos referidos a números de ciberataques, se deben tomar con cautela, ya que no todos se publican o registran y, en otros casos, la empresa afectada intentará impedir que esta incidencia se difunda, pues sería confesar que su empresa es vulnerable, lo cual crearía desconfianza entre sus clientes a los ciberataques.

¿Por qué poner atención en el sector alimentario?

Los ciberdelincuentes han visto en la industria alimentaria una presa fácil porque no se ha preocupado por este tema y porque utiliza software y equipos anticuados que son relativamente fáciles de hackear. Esto significa que este sector tiene vulnerabilidad para ser hackeada.

Un informe emitido por el Instituto de Defensa y Protección Alimentaria de la universidad de Minnesota en el año 2019, concluyó que la industria de alimentos está en alto riesgo de recibir ciberataques.

Respecto de dicha conclusión, es importante señalar que no sólo la industria alimentaria tiene alto riesgo de recibir ciberataques, sino todos los eslabones de la cadena alimentaria (transporte marítimo, sector primario, puntos de venta), pues todos están utilizando, de un modo u otro, tecnologías digitales.

Consecuencias de sufrir un ciberataque

En ocasiones, los ciberdelincuentes lo que buscan es simplemente un beneficio económico:

1. Lo que pueden lograr a través de programas dañinos del tipo ransonware que básicamente se adueñan de la información de la empresa y piden un rescate para devolver la información a la empresa. El caso más conocido fue el ransonware llamado WannaCry que afectó a nivel mundial a grandes empresas internacionales y al servicio de salud británico.

2. El beneficio económico también lo pueden obtener accediendo a las cuentas bancarias de sus presas. En otros casos, el ciberdelincuente busca que la empresa tenga pérdidas económicas enlenteciendo la cadena de producción, actuando sobre la configuración de los equipos causando productos defectuosos o, bien, robando una fórmula o receta secreta.

3. Otros ciberdelincuentes buscarán dañar la reputación de la empresa. Por ejemplo, en la empresa alimentaria un ataque puede ir dirigido a contaminar el producto o a producir un producto que no cumple las garantías sanitarias y hacer que esto pase desapercibido para el empresario.

Para los operadores de empresa alimentaria todo eso significa un mayor esfuerzo para garantizar la seguridad de los alimentos. No cabe duda que los esfuerzos realizados por el sector alimentario para poner en el mercado productos seguros y con la información adecuada para salvaguardar la salud de los consumidores ha aumentado.

Razones para proteger la seguridad informática

Para quienes llevan más de 20 años trabajando en el sector alimentario sabrán que en un principio los peligros típicos asociados a los alimentos se abordaban con el uso de procesos industriales validados y con la implantación de prácticas de higiene. Más tarde llegó la problemática de las alergias alimentarias con lo que hubo que implantar medidas para gestionar correctamente los alérgenos en todo el proceso de elaboración de alimentos.

Por el camino fueron apareciendo nuevos peligros o contaminantes que podían ser vehiculizados por los alimentos Luego fue cobrando relevancia el tema del fraude alimentario, por lo cual las empresas se ven obligadas a tomar medidas si no quieren ver dañada su reputación.

Tras el ataque de terrorismo de las Torres Gemelas en New York en 2011, los operadores de empresa alimentaria americanas ya están obligados a elaborar un plan Food Defense que ayude a evitar cualquier adulteración intencionada del alimento con el propósito de casuar un problema de salud terrorismo alimentario).

Al inicio las medidas típicas del plan Food Defense iban encaminadas a evitar el acceso a personal ajeno de la empresa, asegurar la no manipulación de las materias primas durante el transporte, a evitar acciones de sabotaje por parte de empleados descontentos, a usar sistemas de videocámaras, aislamiento de la fábrica y formación de los empleados.

Actualmente, en plena revolución industrial del Internet of Thing (IoT) y de la conectividad, las empresas se ven obligadas a implantar medidas de ciberseguridad si no quieren sufrir las consecuencias de los ataques cibernéticos.

En la mente de los empresarios que no le han dado la suficiente importancia a esta amenaza, puede estar la idea de que su empresa (por tamaño, facturación, etcétera) no puede ser de interés para un hacker. Es un error pensar así. Un hacker está buscando dinero, información valiosa, datos o incluso manchar la reputación de la empresa, por lo que si estos aspectos son importantes para el empresario también lo serán para un hacker.

Eso nos lleva a la siguiente pregunta: ¿quiénes están detrás de estos ciberataques? Pueden ser organizaciones criminales, alguien de la competencia, personas de la misma empresa contratadas por dichas organizaciones criminales, empleados descontentos, hackers amateurs, etcétera.

Las vulnerabilidades más frecuentes que se encuentran en las empresas son:
1. No haber hecho un inventario de todo los equipos hardware y software conectados a una red.
2. No haber hecho un análisis de riesgos.
3. Falta de aislamiento de activos críticos.
4. Mecanismos de autentificación débiles.
5. Prácticas poco seguras para proteger contraseñas.
6. Utilizar sistemas operativos o soluciones tecnológicas sin actualizar o poco fiables.
7. Falta de personal cualificado.
8. Falta de concientización y formación de todos los trabajadores de la empresa, desde el director hasta el trabajador de base.

Por ello, no cabe duda de la importancia de implantar un plan de ciberseguridad en la empresa o, bien, incluir medidas de ciberseguridad dentro del plan Food Defense en aquellas empresas que lo tengan implantado.

3 aspectos para centrar la ciberseguridad

Todo plan de ciberseguridad debería operar al menos en tres frentes:
1. TECNOLÓGICO: Incluye el diseño del sistema de redes, la configuración del software, protocolos de encriptación, protocolos frente a suplantación de identidad, y mecanismos de detección y monitorización, actualizaciones de sistemas operativos, etcétera.

2. GESTIÓN: Incluye la elaboración de políticas, procedimientos, revisión de contratos, realización de auditorías, simulacros de emergencia, etcétera.

3. PERSONAS: Incluye formación en cómo evitar que entre un ciber ataque en la empresa o que ellos mismos, sin intención, puedan facilitar el acceso al hacker.

Pero, ¿cuál de esos aspectos destaca más, pero se le suele dar menos importancia? A las PERSONAS. Los ciberdelincuentes han puesto el foco en las personas que trabajan en las organizaciones independientemente del puesto que ocupen. Utilizan lo que ahora se denomina ingeniería social. Dichos ataques se basan en la buena fe de las personas y/o en el desconocimiento de ellas para que realicen acciones que puedan interesar al ciberdelincuente.

La vía principal de llevar acabo estos ataques es a través del correo electrónico. A través de éste los hackers pueden actuar de diversas maneras, ya sea sugiriendo descargar un archivo malicioso, conteniendo enlaces a páginas falsas, suplantando la identidad del remitente o intentando hacerse con contraseñas o credenciales.

Debido a la pandemia actual y de alarma sanitaria derivada del coronavirus SARS-CoV-2, es necesario pensar y extender todo un plan de ciberseguridad a las personas que están haciendo teletrabajo o home office. Sus redes y equipos deben garantizar la protección de información sensible de la empresa.

Para un mayor entendimiento de lo que pueden llegar a hacer los ciberdelincuentes en las empresas y a las personas en su vida normal, se recomienda ver la película “El Intruso”, protagonizada por Pierce Brosnan. ▮