19/11/2025

El phishing, la amenaza más crítica para la ciberseguridad industrial

Correos fraudulentos e ingeniería social lideran los ataques en sistemas industriales automatizados



En la era de Industry 4.0, la transformación digital ha interconectado fábricas, plantas de energía y cadenas logísticas a una escala inédita; sin embargo, esa misma vinculación —que impulsa productividad y trazabilidad— también amplifica las superficies de ataque. El phishing, en particular, se ha consolidado como la amenaza más crítica para la ciberseguridad industrial, al explotar el factor humano: empleados que abren un correo, descargan un archivo o hacen clic en un enlace malicioso.

El informe Kaspersky ICS-CERT Q2 2025 revela que el 6.49% de las computadoras industriales en el mundo fue blanco de scripts y páginas de phishing, y el 3.06% recibió amenazas directamente a través de clientes de correo electrónico, una proporción creciente por tercer trimestre consecutivo.

Aunque la tasa global de ataques en sistemas industriales descendió ligeramente a 20.5%, el reporte advierte que el vector humano sigue siendo la puerta de entrada más común; en América Latina, el 68% de las empresas reconocen el phishing y la ingeniería social como sus principales amenazas, superando al ransomware (54%) y las brechas de datos (38%).

“El usuario final continúa siendo el punto más vulnerable del sistema”, enfatiza el estudio Cybersecurity of Industrial Systems, publicado en 2024 en la revista Electronics: “Sin una cultura sólida de ciberseguridad industrial, los programas de protección pierden eficacia, pues basta un solo clic para comprometer toda la red operativa”.

América Latina: nuevo epicentro del riesgo cibernético industrial

La región latinoamericana emerge como una de las más vulnerables del mundo industrial. Según Kaspersky, América Latina registró el mayor incremento trimestral de amenazas por correo electrónico y una de las tasas más altas de infección por scripts maliciosos (9.18%), superando a regiones tradicionalmente más atacadas como Europa del Sur o el Medio Oriente.

Esta tendencia se asocia a una falsa sensación de seguridad: el 65% de las empresas considera estar preparada para enfrentar ciberataques, pero solo el 17% revisa sus estrategias de manera continua y más de un tercio invierte menos de lo necesario en protección.

Los costos por incidente también son crecientes; de acuerdo con cálculos regionales del sector, una brecha de seguridad industrial

tiene un costo promedio de 3.8 millones de dólares, cifra que puede multiplicarse cuando la interrupción impacta líneas de producción o compromete datos críticos de energía, alimentos o transporte.

El problema, explican los especialistas, no es solo tecnológico, sino organizacional: la integración entre entornos OT (Operational Technology) y TI (Tecnologías de la Información) —necesaria para automatizar y supervisar operaciones— expone a las empresas a vectores cruzados que antes eran independientes. Un correo de phishing en la red administrativa puede convertirse en un punto de acceso a los sistemas SCADA o PLC de una planta.

Del correo a la planta: anatomía de un ataque

El phishing funciona como vector de infección inicial, que luego desencadena la entrega de malware de siguiente etapa. Kaspersky detectó más de 10,400 familias distintas de software malicioso en ICS durante el segundo trimestre de 2025, confirmando un proceso de ataque cada vez más estructurado:

1. **Contacto inicial:** un correo con un documento MS Office o PDF malicioso contiene macros o enlaces que redirigen al usuario a una página de phishing.
2. **Ejecución:** al habilitar contenido o introducir credenciales, el sistema descarga componentes que abren la puerta a otros programas.
3. **Despliegue:** se instala spyware (troyanos espía, keyloggers o backdoors) para obtener información, moverse lateralmente dentro de la red y preparar el terreno para otros ataques.
4. **Exfiltración o sabotaje:** finalmente, se activa ransomware, mineros o herramientas de espionaje industrial.

Durante 2025, el spyware continuó siendo el malware de siguiente etapa más frecuente, presente en campañas dirigidas a la industria manufacturera, energética y de transporte, su detección en un equipo ICS indica que el ataque inicial —normalmente vía phishing— tuvo éxito.

Sectores industriales bajo presión

De acuerdo con los datos de Electronics, la manufactura (24%), finanzas (18.9%) y energía (10.7%) concentran la mayoría de los ciberataques industriales a nivel mundial. Estas industrias presentan dos rasgos comunes:

1. Dependencia de infraestructura interconectada, que amplía la superficie de exposición.
2. Presencia de sistemas heredados (legacy) sin parches de seguridad o segmentación adecuada.

En el entorno industrial, un ataque de phishing puede derivar en la interrupción de procesos de producción, pérdida de trazabilidad o fallas de control en sistemas críticos, con impactos que van más allá de lo económico: desde daños ambientales hasta riesgos a la seguridad humana.

Un ejemplo reciente citado en el informe de Kaspersky muestra que incluso sectores de biometría y automatización de datos —antes considerados de bajo riesgo— encabezaron la lista de industrias más atacadas en 2025, reflejando la expansión transversal del problema.

Resiliencia industrial: del software a la cultura organizacional

El reto de la ciberseguridad industrial no se limita a instalar antivirus o firewalls; requiere un enfoque sistémico basado en tres pilares:

1). Cultura y capacitación. El elemento humano es tanto la causa como la solución, la capacitación periódica, los simulacros de phishing y la sensibilización sobre políticas de acceso son esenciales para reducir errores. Las empresas más resilientes son aquellas que convierten la seguridad en parte de su cultura operativa, no en un protocolo aislado.

2). Protección multicapa. El estándar ISA/IEC 62443, citado tanto por Kaspersky como por Electronics, propone una arquitectura de defensa que abarca control de accesos, cifrado de datos, segmentación de red, autenticación de dos factores y monitoreo continuo.

“Asegurar los sistemas industriales implica proteger los datos en tres contextos: almacenamiento, procesamiento y transmisión”, explica Electronics. “La seguridad debe integrarse desde el diseño del sistema, no añadirse después”.

3). Tecnología avanzada. La incorporación de inteligencia artificial (IA) y machine learning (ML) permite detectar patrones irregulares y comportamientos anómalos en tiempo real. Según Electronics, la IA no solo mejora la detección, sino también la respuesta automatizada a incidentes, aislando sistemas afectados en segundos y minimizando el daño operativo.

Hacia una estrategia industrial de ciber resiliencia

En los sistemas de automatización, donde convergen humanos, máquinas y datos, un solo error de comportamiento puede desencadenar pérdidas millonarias y comprometer la estabilidad de toda la cadena productiva.

Para fortalecer la resiliencia, los especialistas recomiendan:

- Revisar periódicamente los planes de seguridad y realizar auditorías de riesgo.
- Establecer protocolos de respuesta a incidentes y copias de respaldo fuera de línea.
- Limitar el acceso a internet desde entornos OT, como señala Kaspersky, dado que la exposición innecesaria incrementa la probabilidad de infección por phishing.
- Integrar la ciberseguridad en la estrategia de sostenibilidad industrial, entendiendo que proteger los sistemas también protege a las personas, los activos y el entorno.

La digitalización industrial ha borrado las fronteras entre producción y ciberespacio; en ese escenario, el phishing actúa como un catalizador del riesgo sistémico: una amenaza que inicia con un correo y puede terminar paralizando una planta o filtrando secretos industriales.

Fuente: https://thelogisticsworld.com/

LINK DE LA NOTICIA