José Antonio Álvarez, profesor de la UAL: "El 80% de las empresas están expuestas a un ciberataque"

El docente, experto en ciberseguridad y ciberdefensa, advierte de los riesgos a los que se enfrentan las compañías que no se protegen correctamente



José Antonio Álvarez Bermejo, en su oficina de la Universidad de Almería **Guillermo Fuertes**

Una contraseña repetida, un router sin actualizar o un correo que parece proceder de un proveedor pueden bastar para que una empresa lo pierda todo. En Almería, donde la actividad agroindustrial y logística depende cada vez más de sistemas conectados a internet, **la ciberseguridad ha dejado de ser un asunto reservado a grandes corporaciones**. Juan Antonio Álvarez Bermejo, profesor titular de la Universidad de Almería, cuyos campos de actividad son la ciberseguridad y la ciberdefensa, lo resume con una advertencia que no admite medias tintas: **"No hay una sola empresa que se salve".**

Según el Directorio Central de Empresas (DIRCE) del INE, **en Almería hay 44.199 empresas activas.** Álvarez Bermejo sostiene que, **si se habla de compañías con conexión a internet, la cifra de vulnerables se acerca al cien por cien**. Él prefiere fijarla en ocho de cada diez, el 80 por ciento, para dejar margen a aquellos negocios que aún apenas utilizan tecnología. Pero su mensaje es claro. Una panadería que no está digitalizada puede estar

Más leídas

1. El exmarido almeriense de Ayuso que sale en sus memorias íntimas
2. Tres estudiantes de Almería de 48, 54 y 55 años, entre los mejores expedientes de la FP andaluza
3. Herido un hombre de 32 años tras ser apuñalado en el puerto de Garrucha
4. Encuentran a Valentina, la joven de 16 años desaparecida en Almería, gracias a un usuario de TikTok
5. De Almería a la cima de la abogacía nacional: el brillante reconocimiento al talento de Vera Hernández

automatismos, routers o sistemas de gestión conectados a la red ya forma parte del tablero.

públicas han sido atacadas", explica. "**Yo digo que el 80 por ciento, siendo generoso, porque de todas las empresas que tienen conexión a internet no se salva ni una**". El profesor apoya esa estimación en su experiencia profesional y en plataformas como Censys o Shodan, que permiten rastrear dispositivos expuestos en internet y detectar vulnerabilidades conocidas.

La puerta de entrada está en casa

El problema no se limita a los servidores de una compañía ni a los ordenadores de la oficina. Álvarez Bermejo señala que **muchos ataques comienzan por elementos aparentemente insignificantes**, como un router sin actualizar, una cámara conectada, una báscula de supermercado, un sensor de riego o una pantalla digital instalada en un edificio público.

Cuenta que analizó el firmware de un router doméstico y encontró vulnerabilidades, además de conexiones automáticas hacia servidores en China. Ese mismo modelo, asegura, lo ha visto después instalado en un parking de Almería, controlando placas

"Una cosecha no se recupera con una copia de seguridad"

En el campo, el riesgo adquiere una dimensión especialmente delicada. Los invernaderos utilizan automatismos conectados a internet para abrir y cerrar ventanas, regular condiciones ambientales o controlar riegos. Si esos equipos emplean contraseñas por defecto, del tipo "admin, admin", **un atacante puede acceder a ellos y alterar parámetros críticos**. "Si yo veo que están metiendo una mezcla de pH con nitrato, te la puedo modificar y te hago polvo la cosecha", advierte. Y una cosecha, subraya, no se recupera con una copia de seguridad.

El agro, objetivo estratégico

La preocupación del investigador va más allá de los incidentes individuales. El sector agroalimentario está considerado infraestructura crítica bajo la normativa europea NIS2, porque **una**

económico que tendría un ciberataque contra una gran empresa de la provincia durante la campaña navideña.

"Si paran algunas de las mayores empresas de Almería , el impacto en el PIB de la provincia sería brutal", señala. Su análisis, aún pendiente de publicación en una revista internacional de protección de infraestructuras críticas, aborda precisamente la cadena de suministro y las consecuencias de una interrupción en el sector.

No se trata solo de robar dinero. El profesor explica que los ciberdelincuentes persiguen también información valiosa, como bases de datos de semillas, know-how industrial o datos personales. Esa información **puede acabar en mercados de la dark web, donde se comercializan desde filtraciones de contraseñas hasta documentación robada**. "Si robo la base de datos de una empresa de semillas, probablemente lo hago porque sé dónde me la van a comprar", subraya.

Las pymes son especialmente expuestas porque, a menudo, no disponen de sistemas de seguridad avanzados ni de personal especializado. **Uno de los fraudes más habituales es el conocido como Business Email Compromise**. Los atacantes acceden al correo de una empresa, observan facturas y relaciones comerciales y sustituyen los números de cuenta para desviar pagos.

La inteligencia artificial agrava el problema. Antes, los correos fraudulentos solían contener errores evidentes; ahora pueden imitar el estilo de un proveedor, incorporar datos reales de una licitación y dirigirse a una persona concreta. Álvarez advierte de que los portales de transparencia, aunque necesarios, **facilitan información que puede ser utilizada para construir engaños muy verosímiles.**

"Si una constructora está participando en una obra con un ayuntamiento, eso está publicado y se sabe quién contrata con quién", explica. "Entonces **se puede intentar engañar a la administración diciendo que se viene de parte de esa empresa,**

un ataque dirigido, diseñado para que la víctima baje la guardia.

La frontera entre lo personal y lo laboral

Otro factor de riesgo es la difuminación entre la vida privada y la profesional. **Muchos empleados utilizan el mismo teléfono para el trabajo y para sus redes sociales**, y guardan tarjetas bancarias o accesos corporativos en el móvil. Un ataque contra una cuenta personal puede convertirse, así, en una puerta de entrada a la empresa.

El profesor pone un ejemplo. Si alguien suplanta el perfil de Instagram de un empresario y publica insultos contra otro directivo, el daño no es solo técnico. **"No solamente es el ataque real a la empresa, sino también el reputacional"**, dice. En un entorno donde la reputación condiciona contratos, clientes y

de datos.

Álvarez Bermejo no propone soluciones milagrosas, pero sí medidas básicas. Recomienda **no utilizar la misma contraseña en todos los servicios, cambiarlas periódicamente, evitar guardar las claves más sensibles en el navegador** y desconfiar de enlaces recibidos por correo o WhatsApp. También insiste en mantener actualizados routers, cámaras y cualquier dispositivo conectado, ya que el firmware obsoleto suele contener fallos conocidos.

Para los particulares, sugiere utilizar soluciones de seguridad en el móvil, activar la VPN cuando se navegue desde redes públicas y comprobar los códigos QR con herramientas que analicen el destino antes de abrirlos. "El objetivo no es meterte miedo, **el objetivo es que lo utilices con responsabilidad**", concluye.

Jornadas de ciberseguridad

La Universidad de Almería prepara, junto a Policía Nacional, Guardia Civil, Coexphal y Diputación, unas jornadas de ciberseguridad los días 18 y 19 de febrero. El encuentro se centrará en proteger el sector industrial conectado

EN: Ciberseguridad | Seguridad | Internet | Tecnología

© LA VOZ DE ALMERÍA S.L.U. 2026

Descarga la APP: Google Play Apple Store

Aviso legal Política de privacidad Política de cookies Condiciones de los servicios Política de privacidad en RRSS Contacto Publicidad

Reglamento UE 2024/1083 Canal ético Ajustes de cookies Declaración de accesibilidad

8,61/10 WCAG 2.1 AA

CERTIFIED
SG-RSC-ODS
SISTEMA DE GESTIÓN DE LA RSC ALINEADO CON LOS ODS
BUREAU VERITAS