Cómo proteger los activos más valiosos de la empresa y crear una cultura de la seguridad

Miguel Ángel García Matatoros, director general de Blue Telecom Consulting (BlueTC).

27 de noviembre 2018

Miguel Ángel García Matatoros, director general de Blue Telecom Consulting, BlueT

Ninguna empresa está exenta de riesgos en la era de la globalización, la digitalización e Internet de las Cosas. La cultura del "siempre conectados", en la que las fronteras de la vida profesional y personal ya no son tan nítidas, solo complica el escenario. Por otra parte, la actividad empresarial se basa en tecnologías tales como Movilidad, IoT, Cloud, Virtualización, Inteligencia Artificial… lo que obliga a dedicar un mayor esfuerzo en la protección de los activos, incluidos los datos de clientes y proveedores, en un escenario, a menudo, complejo y desconocido.

Atacar es Sencillo

Las posibilidades que tienen ahora los hackers son muchas y muy variadas. Ni siquiera hace falta ser un informático experto para llevar a cabo un ataque, que puede llegar a ocurrir por un error en la configuración o protección de un equipo, o por un mal uso del mismo. Ante ese escenario, ya no tiene sentido protegerse solo de posibles ataques sofisticados y dirigidos específicamente a nuestro negocio. Nuestra empresa puede ser víctima colateral en un ataque a otras compañías, sectores o regiones geográficas. Eso **nos obliga a todos a velar no solo por la seguridad de nuestra propia empresa, sino también por evitar que se convierta en el punto débil dentro de un sistema conectado** y que acabe afectando a un tercero.

No se Puede Proteger Todo

En cuanto a los activos a proteger, debemos ser conscientes de que ya no es posible proteger todo y eliminar todos los riesgos. Eso requiere priorizar y empezar por lo más importante. Cada empresa sabe mejor que nadie de qué activos dispone y cuáles son críticos para que sus operaciones se desarrollen con normalidad. Por eso, **es recomendable que cada una defina bien cuáles son los recursos y datos que hay que asegurar** para garantizar la actividad.

La Creación de Una Cultura de Seguridad

Con ese punto de partida, se hace necesario definir una estrategia de protección. Para ello, es imprescindible trabajar de forma transversal con todos los departamentos de la empresa, así como incorporar los sistemas, herramientas y metodologías especializadas y, finalmente, dejarse asesorar por expertos en seguridad. De esa labor deben salir unos protocolos que todos los empleados conozcan, entiendan y sigan. Eso **requiere, por lo tanto, iniciar y mantener iniciativas de formación para toda la plantilla**. Solo de esa forma será posible crear una cultura donde todos contribuyan a mantener un nivel adecuado de seguridad y sean capaces de detectar brechas o incidencias sospechosas. Este plan puede también incluir formación a clientes que utilizan la infraestructura, productos o servicios de la organización.

> Es imprescindible trabajar de forma transversal con todos los departamentos de la empresa

Plan de Contingencia

Por último, debe definirse un plan de contingencia para que la organización esté preparada para actuar en caso de sufrir un ataque. Si se produce una incidencia, el objetivo tiene que ser reestablecer la actividad y volver a la normalidad lo antes posible con el mínimo daño. Ese plan debe ponerse a prueba con ensayos prácticos y experimentar los ajustes necesarios a fin de poder adaptarlo a las cambiantes condiciones del entorno.

Implicaciones Legales y Competitivas

Aunque la responsabilidad de poner en marcha un plan integral de seguridad en la organización reside en la alta dirección, ya no basta con iniciar el proceso y delegar la ejecución y mantenimiento en el departamento relacionado con las tecnologías de la información y las comunicaciones. Cuando hablamos de seguridad, todos debemos sentirnos responsables. Debemos conocer los peligros que pueden afectarnos, ser capaces de identificarlos y de actuar convenientemente cuando tengan lugar. La dirección, por su parte, debe ocuparse de formar a sus empleados, de proporcionar las herramientas necesarias para la protección de la empresa y, muy importante, de comunicar a las autoridades los incidentes que se produzcan, de acuerdo a la legislación vigente en cada momento.

Ya hay muchas organizaciones que van por delante de la legislación y buenas prácticas, manteniendo unos altos niveles de seguridad y sometiéndose a auditorías externas por empresas especializadas en detectar posibles riesgos. Para ellas, esta actividad de control supone una ventaja competitiva, ya que la seguridad no se entiende como una obligación, sino como una forma de fidelización de los clientes, demostrándoles que en ningún otro sitio podrán sentirse más seguros.