NUESTRA DEPENDENCIA DIGITAL

NOTI 354 – septiembre de 2024

Los llamados "Cisnes Negros" son eventos inimaginados, prácticamente improbables que, al ocurrir, generan un gran impacto en las operaciones de una empresa, en un sector, en la economía o en nuestra forma de vida.

Componentes:

- Debe ser algo atípico.
- Su impacto debe ser extremo o severo.
- Luego de su ocurrencia, debe convertirse en un hecho explicable y predecible.

Imagen tomada de: https://info-veritas.com/explicativos-

El pasado 19 de julio será recordado como el día en el que aeropuertos, trenes, bolsas de valores y hasta importantes bancos a nivel global dejaron de funcionar a raíz de una actualización de un software de seguridad informática que afectó a los sistemas basados en Windows.

Estas fallas, si bien no se debieron a un incidente de seguridad informática, nos recuerdan la fragilidad a la que estamos expuestos como sociedad y como empresas en marcha, todo esto ante la dependencia tan marcada a la tecnología. Es común que en la actualidad si no tenemos acceso a internet en nuestro lugar de trabajo o en nuestra casa, quedamos inutilizados y aislados del mundo exterior; y en el evento que mencionamos inicialmente, sin acceso a nuestros computadores, el mundo se paraliza.

Es por esto por lo que resulta interesante lo ocurrido con esta empresa de seguridad, que se convierte en llamado de atención para todos los que dependemos de la tecnología para funcionar. Se hace evidente la necesidad de contar con una adecuada gestión de los riesgos y en especial, aquella gestión que tienen que ver con la continuidad del negocio. Hasta los eventos más raros e impensados, aquellos que se denominan "cisnes negros" pueden llevar a una disrupción completa de nuestro negocio y conviene hacernos la pregunta de rigor, ¿Está mi empresa preparada para funcionar ante una eventual caída de los sistemas? ¿Cómo puedo seguir operando y atendiendo a mis clientes sin tener acceso a los sistemas o al sitio donde se aloja mi información?

Es fundamental la creación de planes de continuidad del negocio para que ante cualquier novedad, nuestra operación, de cara al cliente, se vea lo menos afectada posible.

Imagen tomada de: https://exeditec.com/seguridad-informatica/

Por: Santiago Duque,
Líder Área de Conocimiento y Desarrollo
ASR S.A.S.

Medellín, Colombia
+573103923352 - 3233453366
asr@asr.com.co
http://www.asr.com.co/

Esto no se responde a la ligera, y será un debate que se tendrá que dar al interior de cada empresa, de acuerdo con la criticidad de su oferta de valor. Sin embargo, vale la pena pensar en las mejores prácticas de la seguridad informática, donde la redundancia de sistemas, la no dependencia de un solo programa informático, ni un solo servidor, nos pueden poner en ventaja frente a la competencia. En este caso en particular de los sistemas afectados en Windows, ¿qué hubiera pasado si tuviéramos distribuido nuestro riesgo con algunos ordenadores basados en Linux?

Incluso, ante eventos tan publicitados mundialmente, no faltarán aquellos que quieran lucrarse de alguna manera, intentando vulnerar la seguridad de los afectados. Esto lo pueden llegar a hacer a través de correos electrónicos suplantando a las empresas afectadas o a quien haya provocado la afectación. Se podrían suplantar páginas web indicando pasos falsos a seguir para corregir los errores y de esta manera aprovechar la conmoción del momento para efectuar sus robos de información de la mano del uso de Ransomware.

Indudablemente no podemos prever la infinita cantidad de eventos de riesgo que nos pueden ocurrir tanto físicos como tecnológicos, pero ante este aviso tan reciente, es importante sentarse a diseñar la continuidad de nuestros negocios y la manera como debemos actuar todos ante este tipo de eventos.

asr@asr.com.co