CIBERRIESGOS

UNA NUEVA AMENAZA PARA SU EMPRESA.

ERRORES COMUNES, SOLUCIONES PROFESIONALES.

Partner Tecnològic

10 Errores de seguridad en las Pymes

1- Considerar que la información de su empresa o sus sistemas no interesan a nadie.

2- Creer que la seguridad sólo compete a los informáticos y descuidar aspectos tan importantes como los legales y organizativos.

3- Pensar que un antivirus y un firewall son suficientes.

4- Considerar que la seguridad es un producto y no un proceso y no realizar mantenimiento de sistemas, conocimientos etc... diario sin tener en cuenta nuevos requerimientos legales.

5- Pensar que la confidencialidad es algo de espías y grandes multinacionales.

6- No contemplar la seguridad en los contratos corporativos, sin tener en cuenta cláusulas de confidencialidad o requerimientos legales marcados por LOPD.

7- Desconocimiento de la Ley Orgánica de Protección de Datos (LOPD).

8- Mirar sólo hacia fuera. La mayor parte de los problemas de seguridad provienen de dentro de las propias organizaciones. En algunos casos, por usuarios malintencionados pero en muchos otros casos, por simple desconocimiento, por ejemplo: uso de USB infectado, abrir un adjunto o pinchar en un enlace que le llega en un correo o simplemente tirar a la papelera información confidencial

9- Ofrecer servicios a través de Internet sin tener en cuenta su seguridad.

10- Descuidar la gestión de la red y los sistemas. Muchas empresas todavía descuidan el mantenimiento de la seguridad de sus servidores y redes, lo que conduce a dispositivos de red vulnerables, puntos WiFi que permiten acceder a la red corporativa, bases de datos de uso interno accesibles a Internet o servidores sin actualizar desde hace años.

Estar protegido ante un ataque ciber no es sólo un tema de seguridad, va más allá, afecta a la competitividad de tu negocio.

Los ataques ciber están incrementando de forma exponencial y se dan en todos los sectores de actividad. Sufrir un ataque puede suponer pérdida de datos, paralización de actividad, desconfianza de tus clientes, inestabilidad en la gestión del día a día, entre otros efectos. Todo ello perjudicaría seriamente la competitividad de tu empresa.

Y es que la tecnología puede detectar y bloquear este tipo de ataques pero la tecnología siempre tiene que ir acompañada de un equipo sensibilizado y que sepa cómo actuar ante cualquier mínima sospecha de ataque así como de soluciones de protección que el mercado ofrece.

Te indicamos, de forma sencilla, lo que no puedes olvidar para que en tu empresa todo esté en orden

- Análisis de riesgo

  Conocer cuánto de sensibilizado estás con el ciberriesgo es el primer paso para poder mejorar. Lo que no se conoce o no se mide, no se puede mejorar.

  Determinar que cantidad de datos manejas y de qué tipo son. No todos los datos valen lo mismo, por lo que el esfuerzo de protección y la inversión que se haga variará según el caso.

  Identificar los sistemas y los datos de interés que pueden ser atacados y dañados, en básico para estimar el coste de recuperación de la información y del restablecimiento de la situación.

  Establecer prioridades en la protección y recuperación de datos es clave.

- Plan de seguridad para tu empresa

  Será el resultado de la fase anterior y debe contemplar mecanismos detección, de defensa y de reconducción de la situación. Debe ser pieza clave a compartir en la organización; la base para el trabajo de concienciación y capacitación de los empleados.

  Mantener la competitividad de tu empresa merece que en el plan estratégico se identifique una partida para hacer frente a una brecha de seguridad. Sé realista y revisa que información has de cuidar más. No dejes al azar la protección de los datos con los que trabajas, uno de los principales activos de tu empresa.

Revisa las principales consecuencias legales que tendrás que afrontar en caso de ataque, las responsabilidades que te pueden ser exigidas.

- Equipo adecuado

  Es una parte crítica e imprescindible para evitar un ataque o para minimizarlo, en caso de estar afectado por una brecha de seguridad. Por ello es importante que identifiques las capacidades técnicas del equipo y establezcas un comando de seguridad.

  Los empleados vinculados a la informática y los que cuentan con perfiles más técnicos cuentan con mayores recursos para reaccionar ante un ataque, pero no es suficiente. La formación del resto de la plantilla y la concienciación en la materia es un pilar básico. Una puerta de entrada de los ataques ciber suelen ser las imprudencias de los propios empleados. No olvides la puesta en marcha de plan de formación, que además puede ser liderado por los perfiles más técnicos y con competencias en la materia.

- Mecanismos de defensa

  El primer mecanismo de defensa consiste es ser consciente de que se puede sufrir las consecuencias de una brecha de seguridad en cualquier momento. El segundo mecanismo consiste en saber que ninguna protección es 100% segura y así te lo contamos. Los hackers se van adaptando a las defensas que se van estableciendo.

  Nuestra mejor recomendación es que estés atento a las tendencias del mercado y sobre todos que cuentes con un partner que se adapte a los cambios y te de la mejor solución profesional en caso de que sufras un ataque.

- Actúa frente a un ataque

  Cuando sufras un ataque ciber -y esto ocurrirá-, lo primero es proteger los activos más sensibles con la puesta en marcha del plan trazado de seguridad.

  Actúa rápido. No lo dejes pasar ya que cuánto antes actúes menores serán los daños que sufras y los que puedas provocar a terceros. El tiempo corre a favor del daño que los hackers provocan.

  Informa a todos los empleados para que actúen con máxima precaución.

Denuncia el caso a la autoridad competente, que cuenta con unidades especializadas en este tipo de delitos. A menudo es un punto que se olvida pero en la medida en que se registren estos ataques, el respaldo de las administraciones será mayor.

Recordemos que el ciberriesgo es un ataque directo a la competitividad y buen funcionamiento de la economía, no se trata de un ataque individual sin más.

PUNTOS BASICOS PARA PREVENIR CIBER ATAQUES.

Análisis de riesgo

• Conocer tu nivel de concienciación con el ciberriesgo es el primer paso para poder mejorar.
• Saber que cantidad de datos manejas y de qué tipo son. No todos valen lo mismo, por lo que la protección y la inversión variará según el caso.
• Identificar los sistemas y los datos de interés que pueden ser atacados y dañados, es básico para estimar el coste de recuperación de la información y del restablecimiento de la situación.
• Establecer prioridades en la protección y recuperación de datos.

Plan de seguridad para tu empresa

• Debe contener mecanismos de detección, de defensa y de reconducción de la situación. Se debe compartir en la organización, para la concienciación de los empleados.
• Contemplar en el plan estratégico una partida para hacer frente a una brecha de seguridad.
• Revisa que información has de cuidar más. No dejes al azar la protección de los datos con los que trabajas.
• Revisa las principales consecuencias legales que tendrás que afrontar en caso de ataque.

Mecanismos de defensa

• Ser consciente de que se puede sufrir las consecuencias de una brecha de seguridad.
• Ninguna protección es 100% segura.
• Estate atento a las tendencias del mercado y cuenta con un partner que se adapte a los cambios y te de la mejor solución profesional.

Actúa frente a un ataque

• Lo primero, es proteger los activos más sensibles con la puesta en marcha del plan trazado de seguridad.
• Actúa rápido.
• Denuncia el caso a la autoridad competente.
• El ciberriesgo es un ataque directo a la competitividad.

Equipo adecuado

• Identifica las capacidades técnicas del equipo y establece un comando de seguridad.
• La formación de toda la plantilla y la concienciación en la materia es básica.
• Una puerta de entrada de los ataques ciber suelen ser las imprudencias de los propios empleados.
• No olvides la puesta en marcha de plan de formación, que además puede ser liderado por los perfiles más técnicos.

Como resumen de todos los puntos anteriores tenemos que ser cuidadosos en los mecanismos de defensa que utilizamos y que se resumen en tres puntos.

Mecanismos de defensa

- Ser consciente de que se puede sufrir las consecuencias de una brecha de seguridad.

- Ninguna protección es 100% segura. Por lo que siempre necesitaras un seguro que garantice tu patrimonio.

- Estate atento a las tendencias del mercado y cuenta con un partner que se adapte a los cambios y te de la mejor solución profesional.

La perfección en soluciones de ciberriesgos

ToBeIT
THAT IS THE SOLUTION

Partner Tecnológico

Usach
Cd´Assegurances

Partner Asegurador