INFONET

8 Infotips de CiberSeguridad para tu empresa

El eslabón más débil de la cadena de la seguridad siempre es el humano: busca atajos, se le puede engañar y en ocasiones no actúa con toda la precaución que debería.

¿ESTAMOS SEGUROS?

"El único sistema verdaderamente seguro es aquél que está apagado, encerrado en un bloque de hormigón y sellado en una habitación con guardias armados...
E incluso así tengo mis dudas"
Gene Spafford

Desde el origen de los tiempos hasta hace muy poco el ser humano encontraba el peligro, la inseguridad y la exposición en todo aquello que desconocía, que le rodeaba, que le era ajeno o que simplemente no formaba parte de su entorno de confianza; poco a poco esto se fue traduciendo en lo que hoy conocemos como amenazas externas, todo aquello que de una u otra forma amenaza lo que nos rodea o sencillamente no podemos controlar.

Los esfuerzos empresariales en seguridad fueron evolucionando para intentar blindarse frente a ello y las técnicas o mecanismos que se usaron se enfocaron en la seguridad física de las empresas, iniciándose una "carrera" en ser más seguros frente a amenazas externas. Casi a la par apareció lo que conocemos como amenazas internas, fallos de seguridad desde el interior de las propias empresas asociado a empleados que, de forma intencionada o no, generaban fugaz de información, robos, extorsiones y un sinfín de modalidades que acentuaron aún más la necesidad de dotar al tejido empresarial de mecanismo para intentar prevenir esto.

La industria en seguridad evolucionó e innovó a la par de los peligros generando una demanda de recursos y un nivel de modernización casi vital para cualquier compañía... Hasta hace relativamente poco, cuando las amenazas internas y externas cobraron un nuevo sentido con la llegada de la informática y el internet, generándose un nuevo concepto: la ciberseguridad.

Es por ello que a continuación expondremos 8 tips básicos que deberías tener en cuenta para hacer de tu empresa un lugar más seguro a las amenazas más actuales:

Infonet
¿te ayudamos?

1 CULTURA DE SEGURIDADY FORMACIÓN

Los verdaderos protagonistas en la seguridad de tu empresa son los empleados, ellos son los pilares fundamentales en muchos aspectos dentro de tu compañía y también uno de los principales causantes de fuga de información de forma consciente e inconsciente. Ellos manipulan y operan con los datos y por tanto generar buenos hábitos de seguridad a este nivel implicará reforzar la seguridad de tu negocio.

"Una cadena es tan fuerte como su eslabón más débil"... Este dicho popular viene a resumir toda la problemática de seguridad que puede tener una empresa. Por mucho que se invierta en dispositivos y soluciones para proteger los sistemas, si alguna falla, el resto cae como piezas de dominó y la seguridad completa se ve comprometida. Generando una cultura de seguridad e invirtiendo en la formación sobre seguridad a los usuarios se puede cambiar esta situación. Concienciarnos de que "El usuario es el eslabón más importante de la cadena de seguridad". La tecnología nunca es suficiente si no se sabe usar.

Las empresas para mantener un adecuado nivel de seguridad deben:

- Realizar acciones de formación continua y cualificada en seguridad para empleados
- Establecer políticas, normativas y procedimientos de seguridad
- Supervisar que se cumplen las buenas prácticas en seguridad
- Realizar acciones de sensibilización y conciencia en seguridad para empleados

"Una cadena es tan fuerte como su eslabón más débil"

Un ejemplo de buena cultura de seguridad que puede parecer evidente, pero es extremadamente común, es confirmar la identidad de todo aquel que solicite información dentro de la empresa; es aconsejable que tanto recepcionistas, empleados de un call-center o soporte técnico, personal de recursos humanos y cualquier otro activo humano que tenga interacción con personas del exterior y que de alguna forma tienen que facilitar datos de la empresa se aseguren de que lo que transmiten este llegando a la persona adecuada.

La ingeniería social y la suplantación de identidad es más usual de lo que se piensa y por ello es importante que la cultura de seguridad y la formación que realices en tus empleados ayude a identificar estas tácticas

2 CONTRASEÑAS EN UN LUGAR SEGURO

Solemos guardar con mucho cuidado nuestras contraseñas personales, las protegemos como el bien mas preciado, imaginemos entonces el cuidado que debemos tener con las claves de nuestra empresa.

Antes que nada, debemos seguir las recomendaciones que se suelen darse a la hora de crear una contraseña segura. No repetir la misma contraseña en varios sitios, intentar no hacerla con datos personales o valores que se puedan deducir del usuario y procurar que tenga números, símbolos y letras en mayúscula y minúscula.

Uno de los principales malos hábitos de los trabajadores es apuntar la clave en un post -it pegado a la pantalla o debajo del teclado; esto supone claramente un pequeño pero a la vez enorme problema de seguridad empresarial que puede comprometer enormemente la seguridad de la empresa.

Aunque las contraseñas complejas son a menudo consideradas elementos básicos para la seguridad, solo 29% de las organizaciones sienten que ayudan a reducir los riesgos de seguridad. Esto se debe a que las mecanismos que usan los empleados para salvaguardarlas no son los mejores, siendo ellos mismos la principal amenaza interna para las empresas si ser conscientes de ello.

Pero vigilar las contraseñas de la empresa no es solo un trabajo preventivo, también debe haber una gestión posterior que las supervise correctamente. Principalmente se recomienda que las contraseñas se cambien periódicamente o al menos cuando haya sospecha de que han sido comprometidas. NUNCA debemos enviarlas por correo o por mensajería (SMS, Whatsapp, Trello, Line...), incluso cuando se proporciona en un soporte físico, se deberá eliminar adecuadamente cuando nos aseguremos que su destinatario ya la conoce.

“Las compañías deberían vigilar si sus contraseñas son cegadoramente obvias”

Para ir finalizando, es altamente recomendable también no emplear contraseñas corporativas en ordenadores en los que desconozcamos el nivel de seguridad al que están sometidos ya que estos equipos podrían tener instalado programas que capturen contraseñas o pulsaciones por teclado.

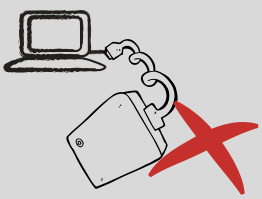
En conclusión, es crucial ser conscientes de que cuanto mas valiosos o vulnerable es un sistema informático, las contraseñas y políticas de gestión que le protegen deben ser aún mas estrictas.

3 EL HARDWARE NO ES PARA SIEMPRE

Hoy en día los sistemas informáticos y los repositorios de datos de las empresas han cambiado a la filosofía "Cloud"; guardas información empresarial con listas de clientes, actividades económicas, datos de recursos humanos, información sensible de ser sustraída, etc... en discos duros de ordenadores en la empresa no suele ser una buena idea.

Los equipos físicos se rompen y en general sufren la inclemencia del propio uso, constantemente expuestos a fallos o lo que es peor, ataques internos o externos que supongan la pérdida de datos valiosos. Lo mismo podemos decir de los dispositivos portátiles y teléfonos corporativos, expuestos a los mismos riesgos y añadiendo la posibilidad de que puedan perderse o ser robados.

Es por ello que se recomienda que la información no se almacene en los propios equipos de lo trabajadores si no en los servidores de la compañía o preferiblemente en servicios en la Nube.



Los "secuestros" de información sobre infraestructuras empresariales están cada vez mas a la orden del día y suponen una clara preocupación para ingenieros y responsables de sistemas. Los ataques por ramsonware, un tipo de malware que toma el control del ordenador de su víctima encriptando la información y pidiendo un rescate a cambio en forma de dinero/bitcoins, esta afectando hasta a un 40% de las empresas según la empresa de seguridad MalwareBytes. Se trata de una amenaza global con un elevado impacto sobre las actividades económicas de las empresas con un aumento de ocurrencia de un 259% en los últimos meses.

"Imagina que secuestran toda tu empresa y no puedes hacer nada..."

Si de todos modos debemos mantener información en el disco duro de los equipos de trabajo, es elemental que se realicen copias de seguridad frecuentemente y en infraestructuras que no puedan ser fácilmente comprometidas por ataques de este tipo,

Un buen servicio cloud empresarial, una correcta política de copia seguridad y un proveedor de servicios tecnológico cualificado puede ser la diferencia entre tener tu empresa segura o perderlo todo,

4 UNA COPIA DE SEGURIDAD NO SE PUEDE PERDER

Parece lógico pero es mas frecuente de lo que podemos imaginar, si realizamos copias de seguridad en dispositivos de almacenamiento externo como pendrives o discos duros portátiles es fundamental que no se transporte en el mismo sitio que la información que respaldan. Parece un consejo de sentido común pero si el respaldo de tu información es un USB que llevas en una mochila donde esta el portátil con la información original y pierdes dicha mochila, no habrás conseguido nada. Lo habrás perdido todo.

Si de todos modos debemos mantener información en el disco duro de los equipos de trabajo, es elemental que se realicen copias de seguridad frecuentemente y en infraestructuras que no puedan ser fácilmente comprometidas por ataques de este tipo,

Lo mas importante para cualquier empresa e continuar trabajando, que todo funcione con normalidad. Es complicado no tener algún incidente y que ademas ese incidente no solo pongan en riesgo los datos si no también la economía y reputación.

"El objetivo de las copias de seguridad es garantizar la continuidad del negocio"

Antes o después algo ocurrirá, es estadístico e inevitable, no importa el tamaño o los medios que se empleen para evitarlo, lo importante es contar con todos los medios posibles para minimizar la pérdida de datos. Disponer de copias de seguridad es importante por estas razones:

- Las copias te permitirán recuperar la información
- Un buen sistema de copias de seguridad te permite una rápida recuperación del sistema.
- Emplear sistemas cloud o supervisados por empresas con experiencia es vital.

Los servicios de Backup de los que dispone Infonet no sólo recuperan la información de los usuarios que se pueda perder por un fallo informático, sino que además, pueden restaurar de forma rápida todo su sistema

5 ALTERNATIVA DE SERVICIOS CLOUD

Si la empresa no cuenta con una infraestructura de almacenamiento interno en condiciones, segura y debidamente supervisada, lo recomendable es optar por un servicio en la nube, bien sea para guardar allí la información directamente, como para emplearlo como sistema de respaldo y copias de seguridad.

Como regla general las empresas que se encargan de prestar servicios cloud cuentan con una serie de medidas que les permiten estar mas preparados que una empresa pequeña o mediana frente a ataques informáticos. Los mecanismos que los proveedores de servicios cloud usan para la protección ante ciberataques añaden una capa de seguridad a tu organización que sería imposible tener en una empresa que no destina una considerable inversión en seguridad de sus sistemas.

La utilización o no de servicios cloud puede reflejarse directamente incluso en dos pilares principales de cualquier compañia moderna actual. SEGURIDAD Y PRODUCTIVIDAD. Una nube dota a la empresa de una capa mas de seguridad y permite a los usuarios disponer de información en cualquier parte,

"Tiene la principal ventaja de ser omnipresente, casi como una figura divina"

Únicamente hace falta un dispositivo con conexión a Internet para acceder a todos tus datos, estés donde estés. Además, es un servicio creado para los usuarios de a pie, de modo que no hace falta ser especialista en tecnología para comenzar a utilizar esta interesante herramienta.

VENTAJAS DE LA NUBE E INFONETCLOUD:

- Control: Protege, controla y monitoriza toda la información de tu empresa. Podrás mantener la información en tus propios servidores o en servidores seguros
- Productividad: aumente la productividad de la empresa posibilitando el acceso y trabajo desde cualquier plataforma y localización.
- Seguridad y personalización: mantén a salvo tu información.

6 UN BUEN ANTIVIRUS...

Antes de usar un equipo o móvil que vaya a conectarse a la red, lo primero que se debe hacer es instalar un adecuado sistema de seguridad. Si esta medida es importante en los entornos domésticos, en el corporativo se vuelve crucial, nuestra empresa tiene que estar segura. Una solución de seguridad como un antivirus o un sistema de firewalls FORTINET para empresas, protege los equipos y los datos de la organización en multitud de circunstancias, incluso cuando los empleados cometen un error o alguna imprudencia. Conciencia a tu plantilla al respecto.

Como regla general las compañias que se encargan de prestar servicios en la nube tienen una serie de medidas que les permiten estar mas preparados que una empresa pequeña o mediana frente a ataques externos informáticos. Los mecanismos que los proveedores de servicios cloud usan para la protección ante ciberataques añaden una capa de seguridad a tu organización que sería imposible tener en una empresa que no destina una considerable inversión en seguridad de sus sistemas.

"Los antivirus son esenciales para el desarrollo de negocios modernos"

Los antivirus son de gran ayuda para las empresas a la hora de protegerse. Sin embargo, debido a la masiva diversificación y evolución de los virus informáticos -gusanos, troyanos, spyware, backdoors-, que actualmente suelen propagarse por los medios de comunicación como el correo electrónico o las redes sociales, tenemos que conocerlos y saber cómo funcionan para entrenarnos en protegernos de ellos. Desde Infonet contamos con antivirus capaces de defender tu negocio en función de tus necesidades, puedes consultarnos el que mejor se adapta a tu empresa. En todo caso, contar con estas herramientas profesionales (de pago) es vital para asegurar un mínimo de protección realmente eficaz.

Un buen ejemplo de aplicación son las políticas de seguridad del antivirus que deben de configurarse correctamente y que deben contemplar una explicación del funcionamiento del virus, el alcance y los daños que ocasiona, cómo llega a los ordenadores, y qué medidas deben llevarse a cabo para evitar infectarse. Esta capacitación debe ser continua y tiene que ser uno de los grandes compromisos de todas las empresa para con los empleados, ya que es la única forma en la que se pueden proteger verdaderamente todos los datos importantes.

7 PRECAUCIÓN CON CORREOS Y PROGRAMAS DESCONOCIDOS

Debemos de confiar solo en lo que conocemos. Es habitual que las empresas restrinjan la capacidad de sus trabajadores para instalar NUEVOS PROGRAMAS en sus ordenadores mediante los permisos del sistema operativo implantados por los departamento de sistemas. No obstante, si tienen credenciales suficientes para ejecutar nuevo software en sus máquinas, debes pedirles que eviten descargar de páginas que no conozcan o resulten sospechosas. De hecho, ni siquiera deberían navegar por ellas. El navegador también es una puerta de acceso para los cibercriminales en muchas ocasiones.

Atención con las REDES SOCIALES
El riesgo más reciente y, por lo tanto, uno de los más desconocidos o menos valorados. La actividad de los trabajadores de una empresa en plataformas como Facebook o Twitter puede ser perjudicial para la compañía en ciertos casos, más allá del descenso en la productividad que pueda o no conllevar. Hace poco advertíamos, por ejemplo, de la alarmante cantidad de selfies tomados en infraestructuras críticas que pueden encontrarse en redes sociales como Instagram.

El CORREO ELECTRÓNICO es de las principales herramientas que utilizan los cibercriminales para colarse en las empresas y robar o secuestrar datos sigue siendo el correo electrónico. Si tus trabajadores tienen un correo corporativo, lo primero que deben procurar es no utilizarla para fines personales ni proporcionarla en sitios de acceso público. De lo contrario, podría acabar en una lista de envío de spam y recibir correos que, además de molestos, pueden resultar peligrosos y afectar a toda la empresa.

"La principal brecha de seguridad empresarial son los propios empleados"

En general, el mejor consejo que le puedes dar a tus trabajadores respecto al email es que jamás respondan al correo que proviene de un remitente sospechoso o desconocido, ni mucho menos abran o descarguen sus adjuntos. Podrían esconder malware capaz no solo de afectar a su ordenador sino, en algunos casos, a toda la red de la compañía. En cuanto a aplicaciones mal intencionadas, lo que se debe siempre recomendar es: nunca instalar nada si se desconoce el origen. Deben ser los administradores del sistema los que evalúen e instalen software dentro de la infraestructura informática de la empresa. Por último, usar las redes sociales con precaución y conciencia. la seguridad de la empresa puede depender de ello.

8 ESTRATEGIA EN CIBERSEGURIDAD Y UN ECOSISTEMA TIC PARA TU NEGOCIO

El objetivo de externalizar los servicios TIC de una empresa es obtener un departamento especializado dotado de las capacidades de un gran departamento, con sus recursos, despliegue, tecnologías y medios, conocimiento... pero sin los costes asociados que ello supondría en caso de tenerlo en plantilla

Invertir en la tecnología adecuada para tu negocio es el único punto de partida para ser competitivo en la actualidad, y de la misma forma, invertir en la Seguridad tecnológica de tu empresa es un positivo esencial que no debemos dejar de lado para NO sufrir las consecuencias de las brechas de Seguridad asociadas al mundo tecnológico, las cuales, son fulminantes.

Reflexionemos... casi la totalidad de las empresas sufrirá alguna clase de ataque informático, y ¿quién se va a encargar de proteger la tuya? ¿has creado ya tu ecosistema TIC con capacidad de evolucionar?

Adelantarse a los problemas es la mejor manera de evitarlos. Cualquier empresa, con independencia de su tamaño, debe tener en cuenta una estrategia en Ciberseguridad y un Ecosistema TIC capaz de integrarse, escalar y mejorar ante los cambios tecnológicos, como clave de su éxito. Para ello, es prioritario rodearse de un buen equipo que asuma estas labores, que puede ser propio (en plantilla) o externalizado.

- Reducir notablemente costes y gastos operacionales.
- Disponibiliad inmediata de personal altamente cualificado
- Tecnologías, recursos y medios de alto nivel a tu disposición mejorando la capacidad competitiva de la empresa

"En Infonet somos especialistas en resolver tus problemas"

Rodearte un gran equipo de técnicos informáticos especializados es, sin duda, la mejor medida de Ciberseguridad. Te ahorra tiempo, costes y muchos problemas. La adaptación tecnológica es una tarea constante, no puntual ¡escoge bien!

Infonet ofrece servicios y soluciones TIC de calidad, especializados en soporte informático de alto nivel, ciberseguridad y transformación digital

Infonet ¿te ayudamos?

FUENTES CONSULTADAS:

pandasecurity.com
mcaffe.com
incibe.es
infonet.es

infonet@infonet.es **infonet.es** (+34) 981 57 74 10