CONSEJOS DE SEGURIDAD PARA PYMES

La crisis sanitaria desatada por COVID-19 está poniendo en evidencia la necesidad de implantar el teletrabajo en las Pymes como única medida para continuar su actividad sin desplazarse al lugar de trabajo con los consabidos riesgos que en estos momentos supone.

Ante esta urgente necesidad, muchas empresas están habilitando conexiones remotas sin tener en cuenta unas mínimas garantías de seguridad, proporcionando oportunidades de entrada a sus sistemas de información por los delincuentes cibernéticos. Viene al caso recordar que el cometido de la seguridad de la información es proteger los datos que tiene, maneja y dispone una organización y se fundamenta en tres pilares que son confidencialidad, integridad y disponibilidad.

Es en torno a estos tres pilares que debe desarrollarse la estrategia de seguridad de la información en la organización, no es tiempo de ver qué opción es mejor, si no de afrontar con rapidez la protección de los activos de información y tener presente que lo Bueno no siempre es amigo de lo Mejor. Tiempos futuros vendrán para esas cuestiones.

El objetivo de la confidencialidad es prevenir la divulgación no autorizada de la información y está relacionada con:

- **El uso de contraseñas robustas**
  - No utilizar la misma para todo.
  - Longitud mínima de 8 dígitos utilizando Mayúsculas, minúsculas, números y símbolos.
  - No divulgarla
  - No utilizar en la organización la misma contraseña para más de un usuario
  - Verificar que no hay usuarios residuales dados de alta, ya no trabajan en la compañía, de pruebas, etc., sin contraseña o con contraseñas simples (1234, qwerty, usuario, …)

- **No proporcionar información**
  - Personal, NIF, cuenta bancaria, número de tarjeta bancaria, si no estás seguro de la identidad del destinatario (válido para correos electrónicos, llamadas telefónicas, páginas web, y cualquier otro sistema de comunicación)
  - Si te llama Apple, Microsoft, el Banco o cualquier otro proveedor desconfía, no llaman nunca a nadie si antes no has llamado tú, no proporciones ninguna información.
  - No te conectes a la Banca Online desde una WiFi abierta o compartida que no controles tú. (Bar, Aeropuerto, Free WiFi, …).

T +34 933 012 022
Fontanella 21, 2n 1a. 08010 Barcelona
pich.bnfix.com

- **Practicar hábitos saludables**

  - Cuando estés conectado a la empresa o trabajando con los medios de la empresa se responsable. Un mal uso pondrá en riesgo a toda la organización, abstente de abrir correos o visitar páginas Web fuera del ámbito profesional.
  - Presta atención a los correos electrónicos que recibes, verifica el remitente, si la dirección está bien escrita y conoces a quien lo envía, ante la duda una llamada telefónica para confirmar el envío del correo es la mejor opción.
  - Tomate tu tiempo, al hacer clic en Siguiente, Aceptar o Abrir, no estás en una competición para ver quien abre más correos electrónicos en cinco minutos.
  - No descargues archivos y programas de Internet, o aceptes ventanas emergentes al navegar, son la principal causa de entrada de malware de mando y control y pone en peligro a toda la empresa. Tú piensas que eres muy listo porque tienes tal programa gratis y en realidad eres un pardillo que has mordido el anzuelo proporcionando al ciberdelincuente acceso directo a la organización.
  - Si compras por Internet busca comercios electrónicos en que confíes, estén vinculados a pasarelas de pago electrónico reconocidas (VISA, Mastercard, PayPal, …) y si es demasiado bueno para ser verdad, desconfía, posiblemente sea una estafa.
  - No se gana un concurso en el que no se ha participado, ni eres el visitante 1 Millón de la página Web y has ganado un iPhone, ni nadie te mandará dinero. Cierra la ventana, es una estafa.
  - Utiliza la configuración de privacidad para cualquier dispositivo, aplicación o servicio que utilices.
  - Presta atención a los permisos que solicita la aplicación, contactos, fotos, micrófono, ubicación, … y restringe el acceso si no confías. El SÍ A TODO es una mala práctica.

La integridad busca que la información se mantenga inalterada ante accidentes o intentos maliciosos y que solo los autorizados puedan modificarla y está relacionada con:

- **Defensa por capas**

  - Paquetes de seguridad para los puestos de trabajo y servidores, antivirus, antimalware, firewall local, inspección de procesos, anti-exploits, anti-phising y seguridad en navegación Web, protección frente ataques a la red, protección de correo electrónico, encriptación, control de parches, respuesta y contención, protección frente al ransomware, respuesta automatizada ante amenazas, son herramientas que se deben valorar para una protección integral. El clásico antivirus únicamente protege frente al 30% de los riesgos.
  - Actualización del conjunto de programas que operan en la organización, no solo del sistema operativo Windows de los PC y servidor, también Adobe Reader, Office, Java y un largo etcétera. Las versiones obsoletas sin mantenimiento del fabricante deben de ser sustituidas por versiones vigentes con soporte.

- Firewall corporativo. Conectar la red empresarial confiándolo todo al Router con NAT del proveedor de conectividad a Internet hoy en día es una temeridad. Los ciberdelincuentes realizan ataques de fuerza bruta hasta que encuentran una debilidad y entran en los sistemas de información. En los últimos meses la mayoría de los ataques de infección por ransomware en las organizaciones han llegado por esta vía.
- Promover la utilización de conexiones VPN punto a punto entre los equipos de la empresa y los usuarios en teletrabajo.
- Emplear la firma electrónica para garantizar el origen y la integridad del documento o correo electrónico. Ataques de suplantación de identidad cambian la cuenta bancaria del documento enviado por la del atacante.
- Si no es posible firmar electrónicamente los documentos informar a clientes y proveedores de cuál es la cuenta bancaria de la empresa mediante un certificado de titularidad bancaria y que cualquier cambio sobre la cuenta requiere de un nuevo certificado. Clientes y proveedores a su vez deberían hacer lo mismo.

Políticas, Roles y Recursos

- Definir qué está permitido hacer
- Definir quién puede hacerlo
- Definir qué recursos se ponen a disposición
- Permite mantener el control de los sistemas de información, verificar si los controles operan como se diseñaron y proporciona la adecuada segregación de funciones.

La disponibilidad supone que el sistema de información se mantenga trabajando sin degradación y permanezca accesible para los autorizados y se relaciona con:

Infraestructura tecnológica disponible y deseada

- El caudal de datos contratado con el proveedor de conexión a Internet es adecuado para el trabajo normal, pero insuficiente cunado todos los recursos de la compañía se conectan para el teletrabajo. Seguramente en este momento organizar turnos para la conexión será mejor solución que pretender que el proveedor aumente el caudal.
- Hacer un inventario de la conexión a Internet y los medios de que disponen los empleados, así como su disponibilidad a que puedan ser usados para el teletrabajo. Revisar si los equipos de los empleados cumplen con suficientes garantías la defensa por capas indicada en el apartado anterior.
- Si en este momento faltan portátiles y tablets y sobran PC, tenerlo en cuenta para futuras compras. Dentro de las posibilidades trasladar PC a los empleados que trabajan en casa.
- Si faltan licencias de conexión remota, evaluar si es necesario comprar todas o pueden habilitarse turnos. Es necesario evaluar la capacidad del servidor y de la conexión a Internet antes de comprar licencias, porque estos dos

recursos pueden actuar como factor limitador al desplegar la totalidad de licencias adquiridas.

- **Copias de seguridad y resiliencia**

  - En este momento no importa mucho donde esté la copia de seguridad, si en la nube o en local, en una cinta o disco externo, donde esté, está bien, lo más importante es comprobar a diario que se realizan correctamente y sin errores, que son recuperables, que la imagen del servidor permite recuperarlo rápidamente, que disponemos de más de un conjunto de copia (dependiendo del sistema y de la organización mínimo entre dos y cinco conjuntos de copia), que hay al menos un conjunto de copia fuera de los locales de la empresa y por último y más importante que se copia a diario toda la información crítica de la empresa.
  - Los sistemas críticos no son únicamente los servidores, considerar si los PC de usuarios clave en la organización también deben ser respaldados a diario por la información o configuración que albergan.
  - Las copias de seguridad deben de estar desconectadas físicamente de la red o de los equipos, si el conjunto de copia está en línea la entrada de un ransomware u otro agente malicioso también destruirá la copia de seguridad. Las unidades de copia desconectadas son el último bastión de defensa para restablecer la información de la organización.

- **Planes de recuperación de desastres y planes de continuidad**

  - Buscan reducir el impacto causado por un desastre informático.
  - Es necesario disponer de un listado con nombres y teléfonos de empleados, colaboradores y proveedores críticos para agilizar la activación del Plan.
  - Es necesario disponer de un repositorio externo actualizado con programas y datos de configuración del sistema de información, si el sistema no está funcionando y no disponemos de información llevará tiempo recuperarla.
  - Conocer el tiempo necesario para una recuperación total de copia de seguridad nos permitirá conocer cuando la empresa volverá a estar operativa.
  - El Plan de continuidad detalla el modo en el que la empresa proseguirá con sus operaciones después de un desastre para ello debe:
  - Analizar los procesos críticos o clave del negocio y determinar los costes de un paro en el servicio y a partir de cuánto tiempo la situación compromete la continuidad de la empresa.
  - Evaluar si existe algún modo de proporcionar un servicio de emergencia para los servicios críticos y estudiar cómo se volverá a la normalidad.

Estos breves consejos no recogen la totalidad de aspectos a los que se enfrenta una Pyme al abordar la seguridad de sus sistemas de información y únicamente buscan destacar aquellos que en este delicado momento nos parecen más importantes.

Pueden encontrar más información en el Instituto Nacional de Ciberseguridad, www.incibe.es y recordarles que estamos a su disposición para cualquier cuestión que necesiten.

Joaquim Altafaja
joaquim.altafaja@pich.bnfix.com
CISA, CISM, CGEIT
responsable entornos informáticos

BNFIX PICH
Tax · Legal · Audit