Guía de ciberseguridad para pequeñas empresas

YO NAVEGO SEGURO

Contenido

Introducción 3

Primero: cómo te pueden atacar 4

· Malware 4

· Phishing 4

· Ransomware 5

· Suplantación de identidad 5

· Fugas de información 5

Inventario de la información 6

· ¿Qué tipo de información tengo en mi negocio? 6

· ¿Cómo es manejada y protegida esa data? 6

· ¿Quién tiene acceso a esa data y bajo que circunstancias?..... 6

Análisis de riesgos 6

Política de privacidad 8

Llegó el momento, ¿cómo elaborar un plan de ciberseguridad?..... 9

10 Recomendaciones de buenas prácticas de seguridad 10

Introducción

Esta guía ha sido desarrollada para ayudar a las pequeñas y medianas empresas a que se protejan de los incidentes de ciberseguridad más comunes. Sufrir un ataque como este para una pequeña empresa puede resultar devastador. Afortunadamente, la seguridad cibernética no tiene por qué ser difícil. Hay medidas sencillas que si se entienden e implementan de manera correcta pueden evitar o reducir significativamente el impacto de los ataques más comunes.

Desde la Asociación de Bancos Múltiples de la República Dominicana, ABA, entendemos la importancia de estar protegidos y también comprendemos que las pequeñas empresas no tienen mucho tiempo para entender las complejidades de Internet o el establecimiento de respuestas complicadas a los riesgos potenciales.

Pero también sabemos que la seguridad cibernética es uno de los pilares de estas empresas y hacen posible que las mismas crezcan, permitiéndoles innovar y encontrar nuevas formas de crear valor para sus clientes. Es por eso que te presentamos la presente guía, con las pautas básicas para crear hábitos seguros en tu empresa.

Primero: cómo te pueden atacar

Para tener buenos hábitos de ciberseguridad en tu empresa debes conocer cuáles son los ataques más comunes que pueden comprometer la seguridad cibernética de tu negocio. Estos son:

· **MALWARE:** El Centro Australiano de Seguridad Cibernética (ACSC) define el malware como un software o programa malicioso diseñado para provocar cambios o acciones no solicitados por el usuario de ese dispositivo (computadora/móvil). ¿Cómo cuales? Por ejemplo, entrar en tus bases de datos o en tus archivos confidenciales. Es lo que normalmente escucharás como virus o troyano.

· **PHISHING:** Es la forma más común de lo que se conoce como ingenieria social. Según el mismo ACSC, el phishing se basa en correos electrónicos fraudulentos de organizaciones que tú "crees" conocer. Estas imitan el lenguaje, la marca y los logotipos para que parezcan "reales" antes de estafarte para que hagas clic en un enlace o archivo adjunto. Con él, te engañan pidiéndote que proporciones o confirmes tu información, como contraseñas y/o números de tarjetas de crédito o pagar una cuenta falsa. Pueden enviar un archivo adjunto, diseñado para parecer genuino, con malware adentro. Existen dos tipos: Spear Phising y Session Hijack (el nombre no es tan importante, sí lo que hacen).

- Spear Phising: Es una estafa por correo electrónico o comunicaciones electrónicas dirigida a una persona, organización o empresa específica. Aunque a menudo tienen la intención de robar datos con fines maliciosos, los ciberdelincuentes también pueden intentar instalar malware en la computadora de un usuario objetivo. Así es como funciona: llega un correo electrónico, aparentemente de una fuente confiable, pero en cambio lleva al destinatario desconocido a un sitio web falso lleno de malware. Estos correos electrónicos suelen utilizar tácticas inteligentes (actualiza tus datos, has ganado un premio, cuidado vamos a cerrar tu cuenta…) para llamar la atención de las víctimas.

- Session Hijack o Secuestro de Sesión: Su función es lograr el acceso no autorizado a la información o servicios en un sistema. Normalmente esto ocurre cuando un atacante roba o secuestra las cookies de sesión, que son los archivos que se crean cuando navegas por internet. En caso de secuestrar las cookies pueden suplantar la identidad del usuario e iniciar sesión en su nombre. Un ejemplo son las cookies HTTP, que pueden ser robadas y que sirven para mantener la sesión iniciada.

· **RANSOMWARE:** El Instituto Nacional de Ciberseguridad de España (INCIBE) define el ransomware como un tipo de malware o software malicioso que afecta a la información contenida en los diferentes dispositivos, impidiendo su acceso, generalmente cifrado y solicitando un rescate económico a los afectados.

· **SUPLANTACIÓN DE IDENTIDAD:** En este tipo de incidente INCIBE plantea que el ciberdelincuente suplanta la identidad de un proveedor de la empresa, y utilizando técnicas de ingeniería social consigue que la víctima realice una transferencia bancaria al ciberdelincuente pensando que se trata del proveedor legítimo.

· **FUGAS DE INFORMACIÓN**: Una fuga de información o fuga de datos se produce cuando se pierde la confidencialidad de la información de la empresa. Puede ocurrir cuando los empleados están conectados a una red insegura. Ahí también se produce lo que se llama ataque de intermediarios, esto es vulnerar las transacciones entre dos partes y robar la data o que una de las partes ya esté comprometida y, de esa manera, afecte a la otra.

Inventario de la información

Es recomendable realizar un inventario de la información que tiene tu negocio y quién posee acceso a la misma, para mantener un registro de ella, colocarla en un lugar seguro y moverla según sea necesario. La Comisión Federal de Comunicaciones de los Estados Unidos explica estos aspectos para que sepamos qué debemos buscar, registrar y tomar en cuenta:

¿Qué tipo de información tengo en mi negocio?

Una empresa típica tendrá todo tipo de datos, algunos de ellos más valiosos y sensibles que otros, pero todos los datos tienen valor para alguien. Tus datos comerciales pueden incluir información de clientes como registros de cuentas, transacciones e información financiera, datos de contacto y dirección, historial y hábitos de compras y preferencias, así como información del empleado, como archivos de nómina, información bancaria de la cuenta de nómina directa, domicilios y números de teléfono, direcciones de correo electrónico personales y del trabajo.

¿Cómo es manejada y protegida esa data?

Se dice que los datos están en mayor riesgo cuando están en movimiento. Si todos los datos relacionados con la empresa residen en una sola computadora que no está conectada a Internet, y nunca salió de esa computadora, probablemente sea muy fácil de proteger. Pero la mayoría de las empresas necesitan que los datos se muevan y se utilicen en toda la empresa. Cada vez que estos se mueven, pueden estar expuestos a diferentes peligros. Como propietario de una pequeña empresa, debes tener un plan y un conjunto de pautas al momento de que los datos sean transferidos o enviados de un dispositivo a otro.

¿Quién tiene acceso a esa data y bajo que circunstancias?

No todos los empleados necesitan acceder a toda la información. Cuando hagas un inventario de tus datos y sepas exactamente qué datos tienes y dónde se guardan, es importante asignar derechos de acceso a esos datos. Esto significa, simplemente, crear una lista de los empleados, socios o contratistas que tengan acceso a datos específicos, y dejar estipulado bajo qué circunstancias y cómo serán gestionados y rastreados esos privilegios de acceso.

Análisis de riesgos

Una vez has realizado un inventario de la información, corresponde hacer un análisis de riesgos. Ya sabes los tipos de ataques que existen, la información con la que cuentas y quien tiene acceso a ella, por lo que toca inferir a qué tipo de ataque está expuesta la misma, como los mencionados anteriormente. Luego, determinar la probabilidad de que ese riesgo ocurra y las consecuencias que podría traer eso a tu empresa.

A continuación, identifica aquellos riesgos que por su nivel de probabilidad, son inaceptables que sucedan. Para esos, debes proponer diferentes iniciativas para la implantación de controles, que tendrán un coste asociado.

Tras identificar los riesgos establece y documenta el nivel de riesgo aceptable: el valor para medir qué riesgos deben ser tratados y los riesgos que son asumibles. ¿Cómo puedes tratar un riesgo? A través de 4 posibles estrategias:

1. Transferir el riesgo a un tercero: por ejemplo, contratando un seguro.
2. Eliminar el riesgo: Eliminando un proceso que ya no es necesario.
3. Asumir el riesgo, siempre justificadamente: el costo de disponer de un centro de respaldo en caso de interrupción de los servicios por un ataque a nivel

de ciberseguridad puede ser costoso. Sin embargo, resulta necesario asumir el riesgo por varias horas a pesar de su impacto económico.

4. Implantar medidas para mitigarlo: tener un sistema de equipos para continuar trabajando en lo que se soluciona la amenaza o algún acuerdo recíproco con otra compañía en caso de que se produzca un ataque.

Política de privacidad

La privacidad es importante para tu negocio y clientes. La confianza (o falta de ella) en tus prácticas comerciales, productos y el manejo seguro de la información exclusiva de tus clientes puede afectar tu rentabilidad. Tu política de privacidad es un compromiso con tus clientes que se utilizará para proteger su información de la manera que ellos esperan y que se adhieran a sus obligaciones. Esta política comienza con una declaración simple y clara que describe la información que recopilas sobre los clientes y lo que haces con ella.

Por eso es importante crear una política de privacidad con cuidado y publicarla claramente en el sitio web. Es importante compartir estas políticas de privacidad, reglas y expectativas con todos los empleados y socios que puedan tener contacto con esa información. Tus empleados deben estar familiarizados con la política de privacidad requerida legalmente y lo que significa para sus rutinas laborales diarias.

Algunos de los datos que deben tener protegidos por su política de privacidad son:

- Información personal de los empleados y socios: nombre, dirección, correo, tarjetas de crédito, cuentas de banco, RNC, seguro médico, seguridad social, licencia, número de casa, etcétera.

- Información de salud (si aplica).

- Información de los clientes: direcciones físicas, direcciones de correo electrónico, historial de navegación, entre otros datos relevantes.

Llegó el momento, ¿cómo elaborar un plan de ciberseguridad?

Has realizado todo el trabajo previo a la redacción de un plan de ciberseguridad. Estás listo para desarrollar las partes que requiere un plan básico de ciberseguridad. Para ello, la empresa multinacional de ciberseguridad Fortinet, nos da las pautas para crear nuestro plan en solo 4 pasos. Estos son:

Paso 1: Conectividad segura: protege los datos a medida que viajan a través de tu red y permite un acceso seguro a la nube. ¿Cómo? Comienza con una seguridad de red. Dígase, un firewall de próxima generación o cortafuegos de próxima generación que le dan a tu negocio la protección, la flexibilidad y la escala fundamentales que necesita para crecer rápidamente y minimizar el riesgo. Los sistemas operativos de Windows y IOS por lo general vienen con un Firewall integrado que controla cómo los programas acceden a Internet.

Paso 2: Proteger aplicaciones en la nube: construye tu oficina conectada a la nube de manera segura. ¿Cómo? Proteger los datos y a los usuarios mientras consumen aplicaciones de software como servicio, en verdad recae en la empresa y no en el proveedor, algo que sorprende a muchos negocios. Un agente de seguridad de acceso a la nube (CASB), un servicio de suscripción, ofrecen una capa de protección dentro de estas aplicaciones para evitar que se filtre información sensible e impedir que el malware entre y se propague.

En este paso resulta importante también contar con seguridad de correo electrónico. El correo electrónico ofrece a los atacantes un medio para utilizar la ingeniería social y la suplantación de identidad para enviar archivos maliciosos y lograr que los usuarios hagan clic en enlaces maliciosos sin saberlo. Puedes reducir en gran medida el riesgo a través de la inspección de archivos adjuntos, el análisis de archivos y la verificación de enlaces maliciosos.

Paso 3: Protección de usuarios: protege a tus usuarios donde estén. Cuando los colaboradores abandonan la oficina, ya no están conectados a su seguridad de red, a menos que utilicen una red privada virtual (VPN) para volver a conectarse. La seguridad de punto final adecuada protege a sus usuarios con una tecnología similar utilizada en el firewall para detectar y bloquear ataques básicos y avanzados. Por lo que es recomendable instalar un VPN para crear una ruta cifrada de retorno a la red de la oficina, lo que brinda seguridad al usuario tal como si estuviera sentado en su escritorio.

Paso 4: Controla los costos: optimiza y simplifixa la seguridad, la gestión y las operaciones en curso. ¿Cómo? Con administración basada en la nube. Esto ofrece la capacidad de iniciar sesión rápida y fácilmente, acceder a información esencial y tomar medidas que pueden salvar un negocio durante un incidente de seguridad. La administración basada en la nube brinda acceso en cualquier lugar donde haya acceso disponible a Internet; y administrar múltiples dispositivos desde un panel simple simplifica aún más las operaciones en curso.

10 RECOMENDACIONES DE BUENAS PRÁCTICAS DE SEGURIDAD

01 Utiliza un administrador de contraseñas o password manager para guardar tus contraseñas.

02 Desarrolla una política con requisito de que tus contraseñas sean fuertes, utilizando frases.

03 Utiliza autenticación en dos o más pasos para tus plataformas digitales.

04 Encripta el Wifi de tu empresa. Básicamente, colocarle una contraseña a tu router y no dejar que sea público. ¿Por qué? Una contraseña que permite que únicamente quien la conozca se puede conectarse al router y acceder a Internet.

05 Oculta información sensible o delicada para que no se encuentre a simple vista. ¿Cómo? Bloqueando físicamente los dispositivos y usar bloqueos de TI (Tecnologías de la Información) disponibles, como biometría y claves de seguridad.

06 Configura la actualización de aplicaciones de manera automática.

07 Instala un VPN si tu empresa está bajo la modalidad de trabajo remoto.

08 Planifica ante la pérdida de información.

09 Todos los dispositivos deben contar con antivirus.

10 Realiza copias de seguridad periódicas de tu información. Una opción interesante es utilizar servicios en la nube para hacer respaldos de información. Existen servicios como SugarSync, Dropbox o G Cloud Backup que permiten al usuario hacer copias de seguridad en la nube de varios dispositivos incluyendo dispositivos móviles.

www.YoNavegoSeguro.com.do

Fuentes: Fortinet/INCIBE/ACSC

ABA

Asociación de Bancos Múltiples
de la República Dominicana Inc.

Contacto:
809-541-5211 | 809-541-5219
comunicaciones@aba.org.do
www.aba.org.do

www.YoNavegoSeguro.com.do