ARQUITECTURAS DE SEGURIDAD BÁSICAS EN REDES WI-FI

Por qué usamos el término Arquitecturas de Seguridad Básicas en plural y no en singular?? Esto se debe a que debido a la heterogeneidad y particularidad de los organismos, tanto desde el punto de vista organizacional, como económico, se plasman diferentes alternativas para mitigar los problemas asociados a redes wi-fi inseguras.

El problema de la seguridad en redes Wi-Fi

Actualmente la seguridad se ha convertido en uno de los principales problemas de los sistemas de acceso inalámbrico. Varios elementos han contribuido a ello:

- Utilización de un medio de transmisión compartido sin control por parte de los organismos.
- Dispositivos con capacidad de acceso a dicho medio.
- Rápida implantación de esta tecnología en la sociedad.
- Novedad de la tecnología empleada
- Políticas que priman su expansión y dejan de lado aspectos relacionados a su seguridad.

Wi-Fi sin proteger

Las consecuencias más comunes de ataques a redes Wi-Fi son:

- Consumo de ancho de banda
- Acceso no autorizado a equipos
- Responsabilidades legales

Consumo de ancho de banda: Resulta sorprendentemente sencillo conseguir una conexión a una de las muchas redes inalámbricas desprotegidas, y sólo un poco más difícil a alguna de las protegidas con algún tipo de medida mínima. Como consecuencia de este tipo de acceso no autorizado, el ancho de banda de las correspondientes redes WIFI se ve claramente mermado, más aún si éstas son utilizadas como medio de acceso a conexiones de tipo ADSL, cable módem, etc.

Acceso no autorizado a equipos: En general, las protecciones frente a equipos externos a la red local suelen ser más fuertes que aquellas que se aplican frente a equipos que pertenecen a la misma red local. De ahí, que en el momento que un equipo no autorizado se conecta a la red inalámbrica, los equipos que se encuentran conectados a dicha red y los que se encuentran en la misma LAN, suelen ser muy vulnerables. Las consecuencias de un acceso no autorizado a un equipo, puede provocar: el robo o destrucción de datos almacenados en dicho equipo, el robo de claves y contraseñas de acceso a cuentas bancarias, certificados personales, etc.

Responsabilidades legales: Como se ha comentado anteriormente, la intrusión en la red inalámbrica suele hacer mucho más vulnerables a los equipos de esa misma LAN, lo que facilita el acceso no autorizado. A partir de aquí, un equipo atacado puede servir como equipo atacante de sistemas remotos, esto podría dar lugar a responsabilidades legales si se considera que el propietario de la red WIFI o la persona que la ha instalado, lo ha hecho de manera descontrolada y sin tener en cuenta ningún tipo de medida de seguridad preventiva.

Límites difusos

El medio de transmisión WIFI es un medio compartido en el cual cualquier dispositivo que se encuentre en el alcance de la señal puede escuchar o interferir en el mensaje de la comunicación.

Además, en el caso de la tecnología WIFI el coste de los elementos hardware necesarios para poder captar o interferir en las comunicaciones es realmente bajo, y cualquiera puede tener acceso a ellos.

Todo esto ha hecho que el ámbito de la red local se haya deslocalizado respecto al recinto donde da servicio y que las medidas de seguridad encaminadas al control de acceso a recintos, salas, edificios, hogares resulten ineficientes de cara a proteger la red local.

El problema de gestión del espacio de cobertura de la red WIFI se ve agravado en ocasiones con la instalación de puntos de acceso no autorizados, es decir, sin el control de la organización. Estos puntos no controlados son potenciales entradas a la LAN de la organización, y habitualmente no están configurados con las medidas de seguridad mínimas, ya que normalmente se instalan como una solución rápida, fácil y barata a un problema de conectividad sin tener en cuenta las medidas de seguridad mínimas a adoptar.

Gobernanza de Seguridad de la Información

La gobernanza como concepto aislado representa “el proceso de toma de decisiones y el proceso por el que las decisiones son implementadas”.
Al hablar de gobernanza corporativa se hace referencia al compromiso de la dirección ejecutiva de una compañía y consiste en “un conjunto de políticas y controles internos por los cuales se dirigen y gestionan las organizaciones, sin importar su tamaño”.

Del mismo modo, la **gobernanza de seguridad de la información** describe el proceso por el cual se aborda la seguridad de la información desde un nivel ejecutivo en la organización.
La seguridad de la información debe ser una prioridad de la dirección ejecutiva; por lo tanto debe comenzar como una responsabilidad de gobierno corporativo. Esto establece la necesidad de integrar la seguridad de la información en la dirección corporativa a través del desarrollo de un marco de gobierno de la seguridad de la información.

La gobernanza de seguridad de la información es parte de la gobernanza corporativa. Por otra parte, es un componente general que afecta directamente a todas las etapas del proceso de gestión de política de seguridad de la información, insistiendo en que no es solamente un proceso interno de la organización, sino que también puede incluir la participación de entes externos.

Políticas de Seguridad de la Información

Una buena **política de seguridad de la información** debe ser trabajada consensuadamente, para constituir una base sólida en las organizaciones, ya que “sin políticas de seguridad formales, la seguridad es arbitraria, sujeta a los caprichos de algunos”.

Los resultados de la evaluación y análisis de riesgos deben conducir a la elaboración de la política de seguridad, que consiste en un **documento que indica el compromiso y apoyo de la alta dirección**, así como la definición del papel que debe jugar en la consecución de la misión y visión de la organización. En esencia se documenta para explicar la necesidad de seguridad de la información.

CONCLUSIONES

1. Desde la DGTIC como órgano rector en materia de TI en el ámbito de la Administración Pública Provincial del Poder Ejecutivo (Decreto N° 1187/2018), proponemos el desafío de conformar un marco de **gobernanza de las TI** (Sector Público, Sector Privado y Universitario).

2. Dicho marco gobernanza de las TI deberá incluir a la **gobernanza de la seguridad de la información**, tal cual lo plasma el Modelo de Políticas de Seguridad de la Información de la Provincia del Chaco (Decreto N° 2743/2018).

3. Una de las PSI que impulsa la DGTIC, es la de fijar roles y responsabilidades en el uso de redes wi-fi de los organismos.