La seguridad por capas es un concepto de la ciberdefensa que consiste básicamente en analizar los distintos vectores de entrada o vulnerabilidades, y elegir medidas adecuadas para que, en caso de que una de las capas caiga, existan medidas de defensa en capas sucesivas que puedan garantizar la protección de los datos.

No hay un modelo estándar de las capas en una teoría de capas, por lo que las divisiones entre las diversas empresas pueden no ser iguales, pero podemos proveer uno aquí para simplificar.

* Factor Humano: Se refiere a las vulnerabilidades que presentan los distintos operadores de los sistemas. Cualquiera puede caer ante una estafa o un phishing. No es solo el staff interno de la empresa, sino también los vendedores y la gente con algún grado de acceso.
* Perímetro físico: Se refiere al perímetro físico de las instalaciones de la empresa y a cómo restringir el acceso a personas no autorizadas.
* Perímetro lógico: Se refiere a los confines de la red, donde se encuentran los dispositivos que marcan el acceso a nuestra red, como los cortafuegos, routers, etc., y sus políticas de acceso.
* Red: Se refiere a la red interna de nuestra empresa. Aquí es donde todos los ordenadores y otros dispositivos IoT están interconectados, y suele estar segmentada mediante el uso de distintas herramientas como VPN, DMZ, y VLANs.
* Dispositivos: Se refiere a los dispositivos físicos que hay en la red y a su protección, dado que al tener puertos USB o diferentes medios de entrada abiertos, es fácil inyectar un pendrive malicioso o algo similar.
* Aplicaciones/Software: Es la capa donde se encuentran todas las aplicaciones utilizadas por la empresa, e incluso aquellas que no. Hay que proteger las aplicaciones, sus versiones y accesos.
* Datos: Finalmente, la última capa son los datos, que suelen ser el objetivo de los cibercriminales.

Modelo de seguridad por capas aplicado a una empresa

Aplicaremos el modelo de seguridad por capas a una empresa que no tiene en este momento implementada ninguna medida de seguridad. Empecemos por ver dónde aplican cada una de las capas:

50 empleados divididos en los departamentos de Ventas, Marketing y Recursos Humanos. -> Capa de factor humano. En esta capa, lo que debemos pretender es que los empleados de la empresa sean conscientes de las amenazas con las que se pueden encontrar en internet. Las estrategias de phishing o similares que pueden llegar a sus casillas, o las tácticas de ingeniería social. Aumentando la conciencia y alerta de los empleados ( y proveedores o gente con acceso), podemos asegurarnos de que no caigan ante estas estafas y revelen contraseñas al resto.

**Un ordenador con sus componentes y periféricos necesarios para cada empleado:** Parte de los dispositivos. Todos los ordenadores deben estar seguros y en la medida de lo posible, no ser extraíbles de sus estaciones de trabajo. Además, idealmente, estarían en la oficina, la cual tendría un acceso restringido, ya sea con un identificador, con un badge, o con guardias de seguridad.

Cada ordenador, además, ha de tener sus pantallas bloqueadas cuando no se está usando, pero esto también podría considerarse como una práctica a enseñarle a los empleados.

Una red empresarial LAN para toda la empresa: Para conectarse a la red, esta debería requerir de autenticación. Una red LAN es más segura que una via Wi-Fi, pero lo ideal sería también que esta red estuviera segmentada de manera lógica (creando VLANs) para que cada sector de la empresa esté separado y no se pueda acceder a la red de otro departamento.

Un firewall configurado por defecto: Esto es parte del perímetro lógico de la empresa. Un firewall configurado por defecto es fácil de sortear. Lo ideal sería adquirir un firewall Next Generation, que descargue y actualice sus protocolos de protección de acuerdo a las bases de datos más recientes, para poder defenderse de todas las amenazas emergentes.

El almacenamiento de la información en la nube con las herramientas de gestión necesarios, contratado a un proveedor: Esto es parte de la capa de aplicaciones. Primero que nada, se debe asegurar de que el almacenamiento en la nube comparte las mismas medidas de seguridad que el almacenamiento físico. Además, asegurarse de que el proveedor de servicios en la nube toma todas las medidas de seguridad y cumple con los estándares antes de contratarlo.

Además, debemos restringir el acceso a las aplicaciones en la nube mediante contraseñas robustas y un factor de autenticación doble, como mínimo.

La empresa dispone de página web para realizar la venta de productos de forma online: Debemos asegurarnos de que la página ha sido construida basándose en las buenas prácticas de seguridad para la codificación, como ser testeada ante inyecciones SQL. Además, como la página web forma parte de la zona desmilitarizada, debemos estar seguros de que no hay forma de entrar a los servidores internos desde ella, para que un adversario pueda usarla como punto de entrada.