HDC

Últimamente no estoy recibiendo muchos mails pero sí algunas preguntas en el curso en general, por lo que me parece excelente:) No quiero aburrirlos con lo que estoy dando, lamento si los lleno un poco de introducciones pero necesito llenar todos los huecos de la base antes de seguir construyendo hacia arriba:D

En el anterior tutorial vimos qué herramientas podíamos usar a la hora de la defensa lógica. Pero esto no es lo único que existe. Imaginen que protegemos todo nuestro sistema lógicamente pero **una persona puede entrar al establecimiento, sacar el disco duro de la pc y llevárselo en la mano para luego tener todo el tiempo del mundo para analizar los datos que lo contienen**. Aquí hay algo que falla ¿Verdad?

Entonces necesitamos securizar el **espacio físico**. Sobre esto tenemos no sólo intrusiones a espacios restringidos, sino también acceso físico al sistema o a los componentes de él.

Pero no siempre es así. A los peligros físicos los **podemos clasificar** en:

-Desastres naturales como incendios, inundaciones y terremotos.

-Amenazas humanas como disturbios o sabotajes internos.

Los primeros son tan importantes como los segundos. Los desastres que podemos encontrar son:

1. **Incendios**: sobre todo hay que tener en cuenta que la electricidad cumple un factor importante en esto porque al jugar con altas potencias, un cortocircuito no muy grande puede ocasionarlo. Entonces para protegernos, necesitamos aislar bien los cables entre sí y que tengan una buena salida a tierra (luego entenderán toda la física del por qué), y no utilizar cosas inflamables esperando que una simple chispa pueda incendiar todo. También contemos con alarmas de humo, y reglas como no colocar el establecimiento al lado de lugares inflamables o peligrosos ni permitir que se fume. Agregar extintores y controlar la humedad entre el 18 y el 65% como para terminar.
2. **Inundaciones**: Éste es complicado, porque además de ser natural también puede ser ocasionado por consecuencia de querer apagar un incendio. Podemos instalar un detector de inundación -aunque no sé que tan efectivo puede ser-, hacer algún sistema de drenaje no muy complicado y obviamente utilizar un techo impermeable. Intentar que no sea posible que entre agua desde otro lugar.
3. **Terremotos**, tifones y huracanes: Estos desastres naturales son fuertes y cada lugar contará con las precauciones necesarias para aplicarlo ya que no sólo está en peligro una habitacion con computadoras, sino también todo el edificio en general.
4. **Instalaciones eléctricas**: Hay que cuidar esta parte. Usamos mucha energía y necesitamos controlarla de manera eficiente. Primero sobre picos y ruidos -utilizar estabilizadores, térmicas y disyuntor-, luego proteger los cables con un buen aislamiento, bien definidas las conexiones y de manera protegida. Agregar pisos aislados y pasar los cables por debajo de ellos, utilizar un sistema de aires acondicionados e intentar de que las emisiones electromagnéticas no dañen al personal. Ante cortes de luz se puede usar UPS (que es algo así como una batería gigante).

Pero claro que no son los más usuales, y como siempre, el **humano** es uno de los factores más peligrosos. Veamos con qué tipo de amenazas contamos:

1. **Sabotajes internos:** Uno de los más peligrosos, ya que el personal interno puede llegar a tener grandes cantidades de información sobre la seguridad, horarios, personal. También entra en juego los privilegios de ingreso.
2. **Robo:** Error en el acceso físico y en el sistema de vigilancia. Sobre todo si el material es irrecuperable.
3. **Fraude, estafa:** Problemas con el personal, mal capacitados. Sobre todo a veces con información de más.

Creo que estos 3 englobarían al total de problemas. Pero, ¿**Cómo** podemos **prevenirlos**?

1. **Permiso de acceso**: No sólo al edificio entero, sino también a las partes sensibles. Esto lo podemos hacer mediante avisos, puertas bloqueadas con contraseña, tarjetas o biometría. No

dejar lugares sin puertas o sin llaves. Fragmentar bien los sectores

2. **Utilizar candados, cerraduras y otras variantes** para puertas, elementos como CPU's y pequeños componentes.
3. **Cifrar** los datos por si roban el material físico.
4. Si es un elemento portatil, utilizar software para **conocer** la **ubicación** del mismo.
5. **Alarmas y vigilancia.** Tanto de movimiento, de presencia, como cámaras, personal de vigilancia, micrófonos y logs de todo lo sucedido.

Antes de terminar este corto tutorial, tengo que aclarar que ningún sistema va a ser cien por ciento seguro y encima jugamos con el **presupuesto** y los **recursos** que nos dan. Entonces, a no volverse locos. Simplemente hagan lo que tengan que hacer sabiamente.

Pero todavía no terminamos. Hay algo muy importante que llamamos **ingeniería social**. Ésto es utilizar **técnicas sociales** para sacar **información sensible** o realizar actos que uno quiera. Por ejemplo, llamar diciendo que soy de alguna compañía de servicio de internet y que necesito ciertos datos como una contraseña o los dispositivos en la red. Para que no suceda esto, el **personal** debe estar bien **capacitado**. Se le debe hacer entender los peligros que existen en el exterior y de qué manera se puede pasar información sensible. De otra manera se tomarán **represalias**. También hay que **documentar** todos los procedimientos posibles. Se debe lograr que cualquier situación se pueda resolver utilizando algún procedimiento prehecho. Esto lo veremos con más profundidad luego, pero es importantísimo conocer que **toda tu información está en riesgo si una simple persona no puede resguardarla de manera adecuada.**

A parte, hay que **limitar** el **acceso** de la información a la menor cantidad de personas posibles.

Ahora sí finalizamos. Ésto es una simple introducción. Vamos a tener que profundizar los temas para conocer más de cada uno. Sobre todo hablando de la ingeniería social.

Gracias por leer:D espero que sigan el curso. **Próximamente se viene el labo.**

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:

1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
