Amenazas globales exigen respuestas globales

Manuel Canalejas, miembro de la Comisión Técnica de la Fundación ESYS y Director de Consultoría de Prosegur

En una ocasión, un periodista preguntó a Billy el Niño por qué atracaba bancos. Su respuesta fue rotunda: “Porque allí es donde está el dinero”. Sin embargo hoy, la respuesta no sería la misma. El mundo ha cambiado. En la época de Billy, todos los objetos relevantes, como el dinero, tenían el soporte físico del papel. Eran cosas y, por tanto, estaban en alguna parte.

Hoy la realidad ha cambiado y cada vez hay menos cosas que requieran el soporte papel. Ese dinero, contratos y otro tipo de documentos han tomado un soporte digital. Ya no ocupan únicamente un lugar físico, como un banco, sino que también se pueden almacenar de forma digital en bases de datos. El dinero, por tanto, además de físico, se ha vuelto intangible. Y por eso, el Billy el Niño de hoy en día ya no sería un atracador de bancos, sino un ciberdelincuente. Ya no tendría que ir al banco, como lugar físico, para llevarse los billetes, sino que le bastaría con hackear un ordenador desde casa y apropiarse del dinero en formato digital.

Hoy todo el mundo es consciente de la enorme velocidad a la que están evolucionando los entornos digitales. Otra cosa es si, en el mundo de la empresa, estamos reaccionando con la suficiente agilidad a estos cambios. Es evidente que los ladrones aprovecharán cualquier punto débil para traspasar el perímetro de seguridad de una empresa o institución. Da igual que éste sea físico o digital. Y, sin embargo, todavía hoy seguimos haciendo distinciones entre uno y otro. Una cosa son las vallas, muros y alambres físicos que protegen una casa, y otra es el conjunto de software y dispositivos digitales que protegen esa misma casa. Pero, en el fondo, esta distinción es meramente teórica, pues a la hora de la verdad, tanto una como otra tienen la misma función: mantener segura la vivienda.

Podemos poner un muro muy grueso rodeando nuestro hogar, una puerta blindada y una cerradura a prueba de bombas, pero si olvidamos cerrar el muro en la parte trasera, quedará un resquicio por el que una persona puede colarse y llegar hasta el dormitorio. Lo que nos encontramos de manera más frecuente hoy en día es que ese punto débil es habitualmente la seguridad lógica. Las amenazas cibernéticas entran por ese hueco que, normalmente, hemos dejado sin vigilar.

Por eso, hace falta que la Seguridad Física y la Ciberseguridad se coordinen. Ambas deben estar al mismo nivel. Es necesario entender todos los riesgos a los que nos enfrentamos, tanto físicos como informáticos, estimar su probabilidad e identificar el tipo de protección que necesitamos en cada caso. Lo importante es entender a qué nos enfrentamos y detectar nuestras debilidades. Una vez lo hayamos hecho, y ese hueco detrás de la casa haya sido localizado, los especialistas pueden implantar las medidas de protección adecuadas.

Sin este punto de vista global, que aúna Seguridad Física y Ciberseguridad, estaremos protegiéndonos a medias. Pondremos muros muy gruesos, pero olvidaremos cerrarlos.

Y lo normal es que acabemos sobreprotegidos en algunos aspectos y vulnerables en otros. Al final, nuestra casa o empresa tendrá brechas. No estaremos seguros.

Los ladrones pueden atacarnos desde dos frentes: el físico o el informático. Provenga de donde provenga el ataque, a la hora de defendernos, seremos más eficaces si observamos estos ataques desde un único punto de vista. Me explico: si contemplamos la Seguridad Física y la Ciberseguridad como dos responsabilidades separadas, que no se tocan, estaremos cometiendo un error. Deberíamos fusionar estas dos realidades, entender que, en el fondo, confluyen en lo mismo. Pueden ser responsables diferentes, pero con objetivos comunes. Esta manera de entender la Seguridad se llama integración. Se trata, entonces, de integrar nuestra visión de la Seguridad Física y la Ciberseguridad.

Así, por ejemplo, las alertas de la Seguridad Física deberían iniciar procesos de Ciberseguridad, y viceversa. Una vez hecho esto, el siguiente paso es coordinar una Seguridad con la otra y medirlas conjuntamente.

Por último, y volviendo a Billy el Niño, cabe recordar que, aunque la prevalencia del dinero físico sigue siendo enorme, no es menos cierto que el dinero se está digitalizando a pasos agigantados. Está haciendo las maletas y mudándose al mundo cibernético, donde encontramos a un Billy el Niño listo para asaltarnos con su ordenador. En el mundo digital hay muchas maneras de aprovecharse ilegítimamente de los demás. Hacen falta soluciones organizadas para evitar que esto suceda. Y para poder desarrollar una actividad económica sin vulnerabilidades. Se trata de conseguir un intercambio económico en red que sea seguro. Al igual que nuestros bancos y comercios están protegidos con alarmas y vigilantes de seguridad, en la red necesitamos lo mismo. Éste es un paso más en la integración de Seguridad Física y Ciberseguridad: conseguir una comercialización segura en el mundo digital.

En conclusión, debemos caminar hacia la integración entre Seguridad Física y Ciberseguridad. Son dos caras de la misma moneda. Si falta alguna de las dos, nuestra Seguridad tendrá una brecha. Hoy esta integración apenas existe y el camino es largo, complicado y no sigue una ruta clara. Por eso muchos se desaniman. Y sin embargo, merece la pena seguir adelante. Empecemos por estos puntos aquí mencionados y, poco a poco, arrojaremos más luz. Daremos un paso más. Iremos haciendo el camino. Y así será como alcanzaremos ese destino final de la integración.