LA IMPORTANCIA DE CAPACITAR A SUS EMPLEADOS SOBRE LOS RIESGOS DE UN CIBERATAQUE

MARIANO CORBINO[2]

INTRODUCCIÓN

La tecnología se desarrolla de maneras sorprendentes, al día de hoy nuestras relaciones, horarios de trabajo, citas de importancia, reuniones de trabajo y decisiones empresariales o personales no solo hacen uso de herramientas tecnológicas, sino que muchas veces se apoyan en ellas, todo esta online o permitimos acceso a nuestra información, y esto abre la puerta a los crackers que, a diferencia de los hackers, tienen como uno de sus objetivos destruir.

El acceso sencillo a una gran cantidad de información confidencial significa que cada vez más organizaciones se encuentran en una situación de vulnerabilidad a diversos riesgos cibernéticos, que abarcan un abanico desde la sustracción de datos y *ransomware* hasta el espionaje corporativo.

DESARROLLO

El riesgo de ciberseguridad es la probabilidad de exposición, pérdida de activos críticos e información confidencial, o daño a la reputación como resultado de un ciberataque o violación dentro de la red de una empresa, organización o institución.

El riesgo de ciberseguridad generalmente se define por tres componentes:

- Amenaza (Ataques que puede sufrir la empresa)
- Vulnerabilidad (Debilidad, falla o error)
- Consecuencia. (Daños económicos, perdida de información)

Al referirnos al riesgo cibernético usualmente nos referimos a cualquier tipo de riesgo como ser:

- Interrupción o daño a la reputación de una organización como resultado de la falla de sus sistemas de tecnología de la información
- Pérdida financiera.

El riesgo cibernético podría materializarse en una variedad de formas, tales como:

- Violaciones intencionales a la seguridad para acceder a los sistemas de información.
- Violaciones de seguridad no intencionales o accidentales.
- Riesgos operativos de información de la tecnología, debido a factores como por ejemplo la mala integridad del sistema.

Si los riesgos cibernéticos son administrados erróneamente pueden dejar expuesto una variedad de delitos cibernéticos, con resultados que van desde la interrupción de los datos hasta la ruina económica.

[2] Magister Relaciones Internacionales (UBA). Director y Fundador Mente Inter-Nazionle. Miembro del Departamento del área de Seguridad y Defensa en IRI, UNLP. Secretario del Observatorio en PLA & Compliance en IRI UNLP.

En muchos casos, las empresas también sufrirán un problema reputacional a la vez que intentan recuperar los activos perdidos y/o al menos evitar más robos.

Se debe tener en cuenta que casi la mayoría de las empresas enfrentaron, o enfrentaran un ataque que ponga al descubierto su vulnerabilidad respecto del cibernético, lo primero que debe hacerse es intentar comprender no solo el nivel de riesgo, sino de dónde podrían proceder esas amenazas, para que de esa manera se pueda actuar con rapidez y sobre todo con eficacia ante aquellas.

Algunos puntos a tener en cuanta, sobre algunos, existen muchos más, que pueden aumentar el riesgo cibernético.

- Acceso a edificios públicos (sin el uso de una tarjeta de identificación).
- Utilizar las computadoras de la empresa para ingresar a sus cuentas bancarias.
- Responsables de realizar pagos desde las cuentas de la empresa (asociado con el *Business E-mail Compromise, BEC*).
- Empleados que utilizan cualquier tipo de dispositivo electrónico que fueron facilitados por la empresa en sus hogares o en viajes, sin tener una adecuada protección en sus conexiones hogareñas a internet o al utilizarlos en bares, espacios de *coworking*, aeropuertos, etc. o utilizar por parte de los empleados su propia computadora, Tablet o celular para realizar trabajos dentro del lugar de trabajo
- No revisar las políticas de seguridad cibernética de su empresa asiduamente, incluidas indefectiblemente el no contemplar la actualización regular las contraseñas.

CONCLUSIÓN:

Siendo evidente que lamentablemente el riesgo cibernético se incrementa a medida que el delito cibernético crece y se perfecciona, es necesario para una empresa contar con un sistema de medidas de precaución.

Si bien gestionar los riesgos es primordial, nunca es una garantía del ciento por ciento, es por esto que muchas empresas cuentan hoy en día con un seguro de riesgo cibernético.

Por otro lado, es muy importante que las empresas otorguen todas las herramientas (capacitar) posibles a sus empleados para intentar reducir el riesgo sobre posibles ataques, y es aún más importante que las empresas entiendan que muy lejos de representar un gasto debe ser considerado como una inversión que, a futuro, evitará o al menos reducirá considerablemente algunos de los inconvenientes comentados en el cuerpo principal de este escrito.

Algunos ejemplos para concientizar a sus empleados sobre esta temática podrían ser:

- Cursos con expertos sobre ciberataques, para reconocer las diferentes amenazas cibernéticas y sus diversas finalidades.
- Mostrar en números reales lo que puede significar un ataque cibernético para la empresa.
- Las perdidas no solo de dinero, sino de información y clientes.

Por otro lado, es muy importante, delimitar quienes pueden acceder a los archivos de la empresa, una solución muy utilizada es administrar esos accesos a diferentes usuarios donde solamente aquellos empleados autorizados puedan hacerlo.

Aun sabiendo que no lo protegerá de todos los ataques, siempre es aconsejable tener las últimas versiones del software actualizado, lo que permitirá estar cubierto de mejor manera e intentar evitar de esa forma estar expuesto.

Se debe capacitar a sus empleados sobre las distintas políticas y procedimientos en caso de sufrir un ataque de estas características y es recomendable mantener la información cifrada y realizar copias de seguridad, lo que brindará la posibilidad de recuperar lo necesario para seguir funcionando con cierta normalidad.