¿QUÉ ES CIBERSEGURIDAD Y DE QUÉ FASES CONSTA?

¿QUÉ ES CIBERSEGURIDAD Y DE QUÉ FASES CONSTA?

Desde hace unos años, la palabra ciberseguridad se ha vuelto un estándar entre las empresas, puesto que la informática es ya una herramienta habitual en los negocios y para mantener los sistemas a salvo hacen faltas medidas de seguridad que nos ayuden a evitar vernos expuestos a grandes riesgos. Cuando nos planteamos qué es ciberseguridad, hay que decir que se conoce como la seguridad de la tecnología de la información, puesto que engloba un gran número de técnicas y métodos para proteger nuestro sistema, así como otros dispositivos o las redes. Gracias a las herramientas que tenemos disponibles en relación a la ciberseguridad, nuestro sistema estará mejor protegido de los ataques informáticos, hackeos o cualquier robo de datos o identidad. Por todo ello, es importante que para dotar a nuestro sistema con las mejores medidas, tengamos en cuenta cómo va evolucionando este concepto y siempre estemos actualizados para conocer a la perfección las nuevas herramientas que van apareciendo para evitar estas amenazas.

La ciberseguridad es tan importante que sólo el gobierno de los Estados Unidos invierte de forma anual alrededor de 13.000 millones de dólares en ella. Las autoridades estadounidenses también tienen claro que los ataques informáticos se renuevan constantemente y es por ello que siempre hay que estar alerta y no bajar la guardia en ningún momento.

¿CUÁLES SON LAS AMENAZAS MÁS COMUNES?

A pesar de que los ataques informáticos están a la orden del día y se van renovando de forma continuada, podemos decir que existen varias amenazas que son comunes y habituales dentro de este sector. Nos estamos refiriendo a la ciberguerra, el ciberterrorismo y el cibercrimen. ¿En qué consiste cada una de estas amenazas?

- Ciberguerra: Se trata de un ataque cuya finalidad por norma general es política. En este contexto, los ciberdelincuentes intentan recopilar el mayor número de información posible y datos relevantes que puedan comprometer, en un futuro, a un partido político o un gobierno. Se han dado casos sonados de partidos políticos cuya estructura se ha tambaleado debido a una de estas acciones.

- Ciberterrorismo: Es otra forma de amenaza común, pero en esta ocasión aunque también se intenta recopilar el máximo de información, la finalidad es diferente, puesto que el objetivo es crear un ambiente de terror entre los ciudadanos. Uno de los grandes miedos de la sociedad actual es perder la estabilidad debido a ello.

- Cibercrimen: El cibercrimen es una de las amenazas más comunes y la que más se suele producir en todo tipo de países. A través de ella, los hackers acceden a sistemas informáticos protegidos e intentan obtener ganancias financieras.

También se realiza a nivel de usuario, tomando el control de dispositivos concretos y solicitando cantidades económicas a cambio de su liberación entre otras posibilidades.

FASES DE LA CIBERSEGURIDAD

Protegerse ante los peligros de la era actual implica llevar a cabo procesos de ciberseguridad que se sustenten sobre su efectividad y para hacerlo, hay que conocer las fases en las que aplicarlos. Podemos dividir el proceso en tres fases concretas que suelen ser temario habitual del máster en seguridad empresarial: prevención, localización y reacción.

- **Prevención:** El primer paso siempre es la prevención, lo que reducirá en gran medida el margen de riesgo. Por ello, hay que actuar de forma temprana e informarnos de todo lo que puede ocurrirle a nuestro sistema. Determinar las posibles amenazas y cuáles serán las medidas de prevención y reacción en caso de vernos afectados por una de ellas, nos permitirá estar más preparados. Es primordial que los empleados del negocio tengan unos conocimientos básicos sobre ciberseguridad. Deben conocer las distintas herramientas que se utilizan y cómo garantizar su máximo nivel de seguridad para que no cometan errores que puedan abrir el camino a la entrada de los hackers.

- **Localización:** Después de prevenir, en el caso de haber sufrido algún tipo de problema, habrá que localizar dónde radica el problema. Para ello la mejor herramienta es disponer de un antivirus potente que nos ayude a detectar el ataque en tiempo real y concentrarnos en él de inmediato. Localizar el ataque o la infección no es tan fácil como pueda parecer, dado que los hackers son conscientes del uso de los antivirus y lo que hacen es trabajar de manera que sus ataques puedan pasar desapercibidos. En algunos casos, desde el momento en el que se produce el golpe hasta que la empresa lo detecta, pueden pasar más de 100 días. Para intentar reducir en la medida de lo posible este problema, hay que concentrarse en dos aspectos: gestionar las vulnerabilidades de nuestro sistema y por otro llevar a cabo una monitorización de forma continuada.

- **Reacción**: Una vez que hemos localizado la amenaza, tendremos que dar una respuesta técnica sobre la misma y para ello lo ideal es seguir cinco pasos. Comenzaremos desconectando los equipos de la red y seguidamente instalaremos un antivirus que pueda satisfacer las necesidades o actualizaremos el que ya teníamos.
Después, llevaremos a cabo un análisis sobre el sistema y haremos cambios en todas las contraseñas. Para terminar, será crucial realizar una limpieza a fondo del sistema para comprobar que ya no existe ningún tipo de peligro. En el caso de que nos hayan robado datos o información confidencial, también deberemos proceder de la manera pertinente para comunicarlo a los usuarios afectados y elevar lo ocurrido a una situación de delito informático.

Fuente: https://obsbusiness.school/int/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta

2 DIGITS GROWTH PLATFORM

ACCELERALIA