Ética en la ciberseguridad

La ética de la seguridad es una guía para tomar las decisiones adecuadas como profesional de la seguridad. Como otro ejemplo, si usted, como analista, tiene la capacidad de acceder a los datos de nómina y puede darse un aumento solo porque tiene acceso a hacerlo, ¿significa que debería hacerlo? La respuesta es no. Nunca debe abusar del acceso que se le ha otorgado y que se le ha confiado.

los principios éticos que pueden plantear dudas a medida que busca soluciones para mitigar los riesgos. Estas son la confidencialidad, la protección de la privacidad y las leyes.

La confidencialidad. Anteriormente hablamos de la confidencialidad como parte de la tríada CID. Ahora analicemos cómo se puede aplicar la confidencialidad a la ética. Como profesional de Seguridad, encontrará información privada o privada, como la PII. Es su deber ético mantener esa información confidencial y segura. Por ejemplo, es posible que desee ayudar a un compañero de trabajo proporcionándole acceso al sistema de la computadora fuera de los canales debidamente documentados. Sin embargo, esta violación ética puede tener consecuencias graves, como amonestaciones, la pérdida de su reputación profesional y repercusiones legales tanto para usted como para su amigo.

El segundo principio ético para tener en cuenta es la protección de la privacidad. Protección de la privacidad significa proteger la información personal del uso no autorizado. Por ejemplo, imagine que recibe un correo electrónico personal fuera del horario laboral de su gerente solicitando el número de teléfono fijo de un colega. Su gerente le explica que no puede acceder a la base de datos de empleados en este momento, pero que debe tratar un asunto urgente con esa persona. Como analista de seguridad, su función es seguir las políticas y procedimientos de su empresa, que, en este ejemplo, establecen que la información de los empleados se almacena en una base de datos segura y nunca se debe acceder a ella ni compartirla en ningún otro formato. Por lo tanto, acceder y compartir la información personal del empleado no sería ético. En situaciones como esta, puede resultar difícil saber qué hacer. Por lo tanto, la mejor respuesta es cumplir con las políticas y procedimientos establecidos por su organización.

Un tercer principio ético importante que debemos discutir es la ley. Las leyes son reglas reconocidas por una comunidad y aplicadas por una entidad gubernamental. Por ejemplo, piense en un miembro del personal de un hospital que ha recibido capacitación para manejar la PII y el SPII para garantizar el cumplimiento. El miembro del personal tiene archivos con datos confidenciales que nunca deben dejarse sin supervisión, pero el miembro del personal llega tarde a una reunión. En lugar de guardar los archivos en un área designada, los archivos se dejan en el escritorio del miembro del personal, sin supervisión. Cuando el empleado regresa, faltan los archivos. El miembro del personal acaba de infringir varias normas de cumplimiento y sus acciones fueron poco éticas e ilegales, ya que su negligencia probablemente haya provocado la pérdida de datos privados de pacientes y hospitales.