Ataques contra Servicios en la nube

Hoy día, el 98% de las organizaciones globales utilizan servicios basados en nube. No olvidemos que la responsabilidad del uso y seguridad son compartidas tanto por el proveedor como por la empresa contratante del servicio. Es importante resaltar que el salto a la nube viene de la mano de la adopción de nuevas herramientas de seguridad.

Integración de IA y ML

El Machine learning (ML) es una rama de la inteligencia artificial (IA). El machine learning tiene un alcance y un enfoque limitados en comparación con la IA. La IA incluye varias estrategias y tecnologías que están mas allá del alcance del Machine Learning.

Secuestro de Datos en continuo crecimiento

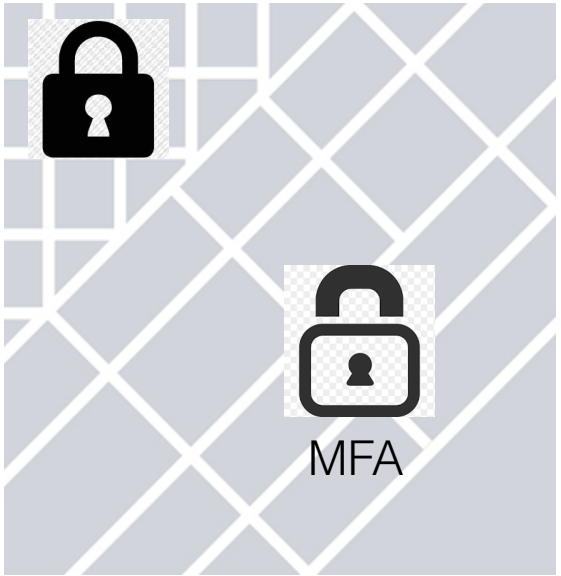
Se necesita una vigilancia permanente para observar no sólo el movimiento de la data, sino también el comportamiento inusual y las interacciones que puedan ser cuestionables en una plataforma o sistema informático. El Ransomware es un negocio en auge por estos días.

Aumento de los dispositivos IoT

Se estima que este mercado crezca a una tasa anual del 23% para alcanzar los USD 336.64 mil millones para 2028. La utilización de estos implica ajustar nuestras políticas de seguridad para controlarlos, tal como algunos marcos de referencia lo están sugiriendo ya.

Autenticación Multi-factor

Hoy en día es indispensable que cuando se accede a una cuenta o aplicación, sea personal o corporativa, los usuarios deban pasar por una verificación de identidad adicional; por ejemplo, tienen que escanear su huella digital o especificar un código que reciben en su teléfono.

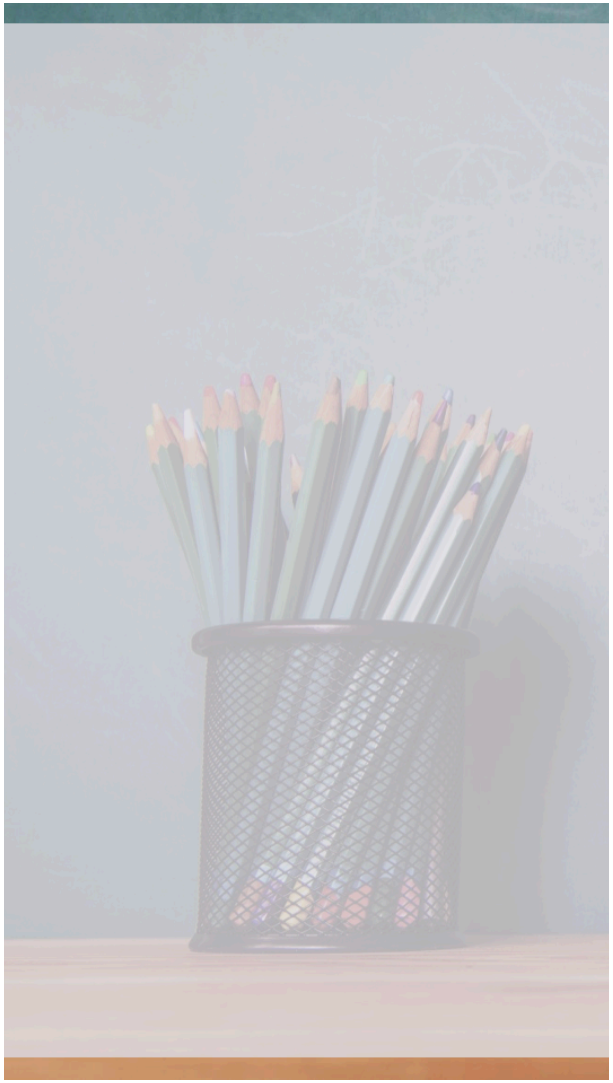


Tendencias Clave en Ciberseguridad 2024

Tecmanario®

Zero Trust

Con Zero Trust el acceso es limitado, solo se conceden autorizaciones de forma selectiva y únicamente para aquellos recursos que sean necesarios por parte de los usuarios. Este tipo de seguridad se caracteriza por la continua autenticación, y es que para acceder será necesario identificarse de manera continua.



Aumento de amenazas por el uso de información privilegiada

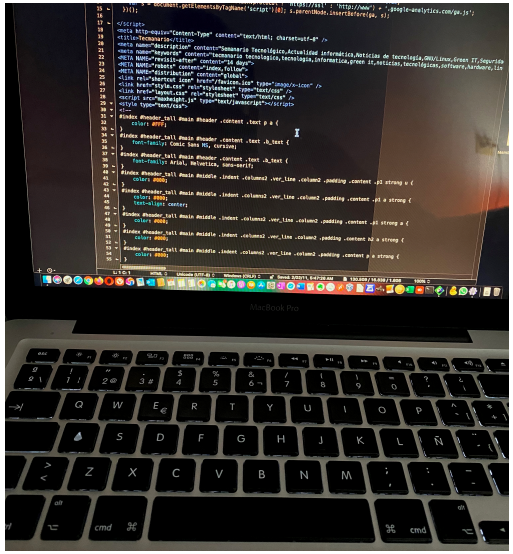
Las violaciones de datos y los incidentes de ciberseguridad causados por información privilegiada no se han tomado en serio. A menudo, son tratados con sigilo porque suponen una vergüenza de cara a los clientes y un problema para las área de recursos humanos según señalan varias investigaciones realizadas. El descubrimiento de estos sigue siendo un dolor de cabeza para las organizaciones, pues a menudo se requirió la notificación inicial por parte de un tercero, lo que significa que los equipos de TI aún no tienen la visibilidad que necesitan sobre las amenazas internas

Explosión de BYOD y dispositivos móviles

Este fenómeno constituye un campo de interés para quienes estudian problemáticas relacionadas a la seguridad de la información en dispositivos móviles. Conlleva a que aparezca un nuevo desafío en materia de investigación en lo que hace a aspectos relacionados con la seguridad y privacidad de la información. Pues, aunque es cómodo para el usuario, también implica riesgos a la seguridad de la organización.

Creciente brecha de habilidades de TI

Existe una marcada distancia entre el conocimiento técnico que un empleador necesita para cumplir sus objetivos empresariales y las capacidades de los empleados de la organización. La profundización del conocimiento ha especializado a tal punto el saber técnico y tecnológico que se hace mas difícil encontrar el perfil adecuado.



Amenazas por falsificación.

Además de afectar al valor de sus productos y servicios, los productos falsificados también pueden provocar pérdidas de ventas y beneficios. El cuidado de la marca corporativa ha llevado a la creación en los últimos años de una área dedicada 100% a vigilar este activo.

Guerra internacional patrocinada por el Estado.

Los ciberataques patrocinados por Estados suponen una gran preocupación para las empresas privadas. En un reciente estudio muchas de las empresas encuestadas esperan que este tipo de ciberataques aumenten aún más en los últimos años y concluyen que esta amenaza solo se ve superada para el sector privado por el crimen organizado.Es importante por ello el aumento de la inversión empresarial en ciberseguridad con el apoyo de los gobiernos nacionales. El 60% de los ejecutivos consultados consideró que su país ofrece un nivel muy bajo de protección.

Ataques al sector salud

Los ciberataques contra el sector Salud no solo tienen consecuencias económicas, sino que pueden afectar al bienestar de las personas. En los dos últimos años este ha sido uno de los 3 sectores mayormente afectados.

Comportamiento organizacional.

Todas aquellas acciones, creencias y comportamientos que se asocian con la seguridad y control de la información dentro de una organización hacen cultura y permiten robustecer la postura de seguridad informática de cara a los desafíos que esta impone.

Amenazas contra vehículos conectados

El 47 % de los ciberataques se realizan contra los sistemas de acceso sin llave. Los servidores en los que los sistemas de conducción conectada almacenan la información reciben el 17 % de los ataques. El 4 % de estos ataques se lleva a cabo contra la unidad de control del motor. Otros: los sistemas de entretenimiento, los puertos USB y las conexiones Bluetooth representan otro 10 % de los casos.

Conciencia de los usuarios.

Es indispensable tener dentro de la planeación estratégica un programa orientado a hacer conciencia, capacitar a los usuarios y prepararlos acerca de las posibles amenazas a la información y cómo evitar situaciones que puedan poner en riesgo los datos de la empresa.