Seguridad informática: un reto para 2024

Noticias 24hs | 15/12/2023 | 22:08



Concientización y capacitación: quizá este es el punto más importante

Sólo en 2022 las cifras de delitos informáticos en el País Vasco incrementó los registros en un 80%. Algo que, sin duda, es preocupante y que requiere de una serie de medidas añadidas al cuidado que se tiene de manera habitual al navegar por la red y compartir datos.

“Sobre todo, es preocupante cuando se mira desde el foco de la empresa, que necesita garantizar a sus clientes una seguridad en el tratamiento de sus datos. De ahí que cada vez haya que innovar más en la forma de establecer muros que sean difíciles de atravesar por seguridad” explican desde Dosys, empresa soporte informático en San Sebastián especializada en las redes de empresas y particulares.

¿Cuáles son las 10 propuestas para mejorar la seguridad informática?

Autenticación multifactor (MFA): añade una capa adicional de seguridad al requerir más de una

forma de verificación para acceder a una cuenta o sistema. Esto generalmente implica contraseña y un dispositivo para autorizar el acceso.

Seguridad de contenedores y orquestación: Con el auge de las aplicaciones como Kubernetes es importante implementar medidas de seguridad específicas para estos entornos que protejan también los datos.

Uso de Inteligencia Artificial y Machine Learning en seguridad: Las soluciones de seguridad basadas en esta smart technology son cada vez más comunes para identificar patrones de comportamiento malicioso y mejorar la capacidad de respuesta a amenazas en tiempo real.

Seguridad en el desarrollo: implica la colaboración entre equipos de desarrollo y operaciones para garantizar la seguridad desde la fase de diseño.

Ciberseguridad en la nube: Con el aumento de las empresas que adoptan servicios en la nube, es esencial implementar medidas de seguridad específicas para estos entornos.

Detección y respuesta extendida: XDR es una evolución de las soluciones de detección y respuesta que amplía la cobertura a través de múltiples puntos finales y fuentes de datos.

Zero Trust Security: basada en no confiar automáticamente en nada, dentro o fuera de la red, requiere una verificación constante de la identidad antes de permitir el acceso a los recursos.

Seguridad de IoT (Internet de las cosas): A medida que crece la cantidad de dispositivos conectados, es crucial asegurarse de que estos dispositivos tengan medidas de seguridad.

Actualizaciones y parches regulares: Mantener sistemas y software actualizados con los últimos parches de seguridad es fundamental para cerrar vulnerabilidades conocidas.

Concientización y capacitación: quizá este es el punto más importante. La conciencia entre los usuarios y la capacitación en herramientas de seguridad son aspectos críticos para prevenir ataques como el phishing.

Autor: Redacción

https://gironanoticies.com/noticia/224901-seguridad-informatica-un-reto-para-2024.htm