Academia de Ingeniería México

NUEVOS ALERTAMIENTOS CIBERNETICOS

La impresora de tu empresa, la puerta de entrada a hackeos

Según los resultados de una encuesta realizada por parte de especialistas en análisis de seguridad, hacia diferentes tipos de empresas, nos deja ver que las mayores amenazas a la seguridad de la información son externas y corresponden a hackers, crimen organizado y competidores.
Por lo que toca a las amenazas internas se dice que provienen de exempleados y antiguos proveedores, y en este caso el acceso a la información se da a través de sistemas de impresión o fotocopiado, pues no se tiene un control de acceso a la red y se da mayor valor a las afectaciones por falta de tinta y papel.

Los puertos de las impresoras permiten el acceso a los sistemas de seguridad de las organizaciones y por tanto existe la posibilidad de fuga de información confidencial.

Por lo anterior se vuelve un tema elemental el contar con un monitoreo permanente de los empleados y saber cómo interactúan con el sistema de impresión, pudiendo utilizar para la autentificación llaves criptográficas o el uso de tokens en teléfonos.

Campaña de phishing busca comprometer cuentas de Netflix

Fuente: www.hobbyconsolas.com

Se ha emitido una alerta por parte de El Instituto Nacional de Ciberseguridad de España (INCIBE) sobre una nueva campaña de phishing (suplantación) que busca obtener credenciales de la plataforma de videos Netflix. Este ataque se sabe empieza a extenderse a otros países. La campaña utiliza un correo falso con el asunto “verificación de cuenta”, y lo que se busca es que el usuario acceda a la página Web de la plataforma y que vuelva a introducir su nombre de usuario y su contraseña, **para esto se incluye un enlace para llevar a cabo dicha verificación**. Obviamente este enlace no redirige al sitio oficial, sino a una página que suplanta la de la plataforma. En caso de introducir tus claves de acceso, los datos quedarán en manos de los ciberdelincuentes, que los podrán vender a otras personas, para que utilicen tu cuenta sin tu consentimiento.

Uso de tecnologías para trabajar de manera remota aumenta debido a COVID-19

Fuente: www.zdnet.com

En las recientes semanas, debido a la necesidad de aislamiento por la crisis del COVID-19, las organizaciones han estado buscando herramientas para que sus trabajadores laboren de manera remota, esto ha ocasionado que aumente el uso de las redes de internet con la consecuente disminución del performance en el servicio, así como el uso tecnologías RDP (Remote Desktop Protocol) y VPN (Virtual Private Network).

Se ha identificado que el uso de RDP ha tenido un aumento de alrededor del 41%, del mismo modo, la cantidad de servidores que ejecutan protocolos VPN han aumentado un 33%. Si bien, el uso de estas tecnologías implica un beneficio para las organizaciones, ya que sus empleados pueden trabajar desde sus hogares, pero también conlleva un riesgo si no se cuenta con las configuraciones adecuadas y se toman las medidas de seguridad pertinentes.

Casos como la venta 500 mil cuentas del sistema de videoconferencias de ZOOM disponibles en la Dark Web, ejemplifican el tipo de riesgo del que estamos hablando.

Para cualquier pregunta o comentario nos vemos en Twitter en @jfniembro

Y les invito a seguir a Pedro Ferriz de Con en Centralfmonline.com

.