PERIÓDICO	PÁGINA	FECHA	SECCIÓN
EL UNIVERSAL	16	04/05/2024	OPINIÓN

SALVADOR GUERRERO CHIPRÉS

Ciberprotección a debate

Empresas, gobiernos y personas lo saben: nadie está exento de un ataque cibernético. La preocupación está en saber cuándo va a suceder y cómo prepararse para afrontarlo.

Las operaciones diarias de la mayoría de las empresas y todos los gobiernos dependen de la tecnología. Oportunidades y vulnerabilidades viajan juntas.

Una nota publicada el martes en la sección *Cartera*, por Antonio Hernández, sitúa la magnitud del tema: según el *Cyberthreat Defense Report 2024*, el 97 por ciento de las compañías privadas ha sido atacada ciberméticamente.

Las posibilidades de sufrir un ciberataque son crecientes y las estrategias criminales más especializadas. Conocer la dinámica ciberdelincuencial y definir medidas de prevención es una tarea entre personas interesadas en el tema, expertos, organismos ciudadanos, empresariales y autoridades.

Conforme abandonemos el escepticismo y consideremos la posibilidad de ser víctimas en algún momento fortaleceremos la oportunidad de una cautelosa y no necesariamente cara seguridad cibernética.

Actualización de antivirus, de software, un firewall adecuado, copias de seguridad, protección del hardware, asegurar la red Wi-fi, resguardo especial de información o una cultura de seguridad en la empresa son recomendaciones esenciales.

Antes de continuar, trata recordar ¿cuándo fue la última vez que actualizaste el antivirus de tus dispositivos?, ¿desde cuándo no cambias tus contraseñas?, ¿cuáles son los protocolos de acceso a

PERIÓDICO	PÁGINA	FECHA	SECCIÓN
EL UNIVERSAL	16	04/05/2024	OPINIÓN

Poco nos detenemos a revisar la ciberseguridad personal, mientras los legisladores nos quedaron a deber en la materia.

los sistemas empresariales?

El estereotipo del hacker capaz de vulnerar o traspasar los filtros de una empresa para sustraer información valiosa o vaciar cuentas del banco, es casi siempre el mismo: hombre joven, de lentes y bajo perfil y una gran habilidad, aunque no necesariamente inteligencia si asumimos que vivir el bien es más inteligente que vivir la depredación del otro.

Los agresores, además de los ciberdelincuentes profesionales, son los propios empleados y proveedores nacionales e internacionales. Conforme cambian y se amplían las formas de conexión digital, en esa misma proporción crece el riesgo.

Ponemos a debate la efectividad de políticas de seguridad pública como la implementada en CDMX por Claudia Sheinbaum —puntera hacia la presidencia, continuada por Martí Batres y muy probablemente también por Clara Brugada como lo anticipan las encuestas. Sin embargo, poco nos detenemos a revisar la ciberseguridad personal y los legisladores quedaron a deber en la materia al no actualizar el marco normativo.

Los expertos reconocen al ransomware, programa para secuestrar información de las compañías, y al phishing, creado para apropiarse de datos personales, como las dos formas más comunes de ataque a las compañías. Según *The Global Risk Report 2024*, la inseguridad cibernética es uno de los cinco mayores peligros para los próximos dos años.

Frente a esa realidad, todo esfuerzo de ciberprotección es bienvenido. ●

Presidente del Consejo Ciudadano de la Ciudad de México @guerrerochipres