Protocolos de seguridad para evitar malware WannaCry

¿Qué es Wannacry?

Es un software malicioso de tipo **Ransomware,** el cual es un programa que "secuestra" los archivos y además tiene la capacidad de replicarse dentro de la red. Se diferencia de un virus en que éste último sólo provoca mal funcionamiento del computador y, en ocasiones, la pérdida de algunos archivos. Sin embargo, no pide recompensa alguna.

Formas de Prevención

- No interactuar con el correo electrónico de spam: al hacer clic en vínculos o abrir archivos adjuntos sospechosos, puede estar abriendo la puerta al ransomware u otro tipo de malware. Simplemente, elimine el spam de inmediato sin abrirlo.

- Evitar descargas y sitios sospechosos: los sitios web que prometen ilegalmente software, música y películas gratuitos suelen utilizarse como anzuelo para atraer a víctimas confiadas.

- Aplicar todos los parches de seguridad que ha liberado Microsoft en el computador con Windows y no postergar su instalación (reinicio del computador), es por seguridad propia, del establecimiento y del propio puesto de trabajo.

- Realizar un respaldo de forma periódica de todos los datos importantes, utilizando herramientas de backup, discos duros externos, pendrives u otros.

- Usar un programa de seguridad confiable, como antimalware y firewall: la protección correcta reconocerá los sitios, las descargas y el spam peligrosos, y le pondrá un freno al ransomware antes de que se pueda instalar. No obstante, mantener actualizada la protección; de lo contrario, esta no podrá reconocer las nuevas amenazas.

- Desconectar el Wi-Fi o quitar el cable de red de inmediato, en caso de ejecutar un archivo sospechoso que puede tratarse de un ransomware, que aún no haya aparecido en la pantalla característica en el computador, quizás se pueda detener la comunicación con el servidor C&C antes de que termine de cifrar los archivos.

Atentamente
Marcelo Vargas Silva
Encargado de soporte técnico
Dpto. de Informática Educativa