DETECCION Y CONTECCION DE MALWARE

La empresa Giotex, no cuenta con ningún equipo firewall, que monitorea el tráfico de red entrante y saliente, y que decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Debido a esto se elaboró un pequeño archivo de PDF, donde se le explica de qué manera pudiera contagiarse el usuario. Al igual se le menciona al usuario que si llegara a tener alguno de estos síntomas favor de notificar al departamento:

-El equipo se vuelve más lento de lo normal.

-El equipo está encriptando archivos de manera que no pueda acceder a ellos y soliciten un pago.

-El navegador web lleva a sitios que no pretende visitar, redireccionado a otros sitios.

-El equipo sin ningún motivo este desactivado, el antivirus que trae el sistema operativo.

-El equipo este enviando y recibiendo paquetes excesivos, sin tener ningún tipo de actividad de navegación.

-Aparecen advertencias en el equipo, a menudo acompañadas de ofertas de compras.

-En caso de no poder enviar correos electrónicos, y se les notifique que por medio de correo que el usuario ha enviado mas de 500 correos por hora.

-El antivirus del equipo se encuentra desactivado.

También se les hace una serie de recomendaciones, que si las sigues muy probablemente nuca se contagie:

-Nunca abras mensajes de desconocidos. Ten cuidado con aquellos mensajes que tengan asuntos llamativos; son los que más probabilidad tienen de contener virus.

-Los más típicos son avisos de un paquete de UPS, DHL u otra compañía de mensajería, una transferencia de PayPal o un error en el envío de mensajes de correo electrónico. Si te llega algo así, desconfía, no abras los ficheros adjuntos a no ser que estés completamente seguro de que es algo que tú has solicitado.

-Nunca descargues programas comerciales o cracks de programas desde Bittorrent, webs de descargas, eMule, etc. Muchos de estos programas están infectados o son realmente malware. Incluso algunos archivos de vídeo que pueden descargarse por estos canales son virus que se hacen pasar por películas, libros o archivos de música.

-Evita acceder a páginas no seguras. Las páginas seguras empiezan por ‘https://’ y muestran el icono de un candado en el navegador.

-Utiliza contraseñas seguras y emplea contraseñas diferentes para los distintos servicios online que utilices.

-NUNCA facilites información confidencial por email. Piensa que tu banco, por ejemplo, nunca te pedirá que le envíes datos personales o información sobre tu cuenta por correo electrónico. En caso de no estar seguro, llama al número de teléfono oficial de tu banco, nunca al número que aparezca en el correo, y pregúntales.

A pasar de no tener equipos sofisticados que analicen el trafico de nuestra red, o ser inteligentes y que detecten los cambios y nos alerten de algún posible ataque, se tiene limitado la navegación, y bloqueado la publicidad con un programa llamado pihole, para poder tener un poco más de seguridad., y de manera interna se están cambiando el tipo de usuario del sistema, para evitar que si en un futuro se llegara a contagiar el usuario no podrá ejecutar acciones debido a que ya no será administrador.