Boletín Informativo / Agosto 2017

UPCLC/FT

Tema: CIBERSEGURIDAD BREVE GUIA PARA AYUDAR A LAS ORGANIZACIONES A PROTEGERSE DEL RANSOMWARE.

25 mayo, 2017/por Gonzalo Vila

A continuación, le damos a conocer una interesante y concisa guía de Roy Zur, socio de ACFCS y presidente de Cybint para ayudar a distintas organizaciones a protegerse del ransomware.

El viernes 12 de mayo de 2017, el mundo entero experimentó uno de los mayores ataques ransomware en la historia. El ataque golpeó a decenas de países en todo el mundo, causando daños a infraestructuras críticas en hospitales públicos y en el transporte público, y a empresas que incluyen instituciones financieras y estudios de abogados.

Desde el año 2016, los ataques cibernéticos a través del ransomware han crecido en forma exponencial, y ahora superan todas las otras formas de malware ubicándose como el peligro número uno para los activos cibernéticos y la infraestructura de la tecnología. El crecimiento de los Bitcoins (métodos de pago digitales que no se pueden rastrear hasta el beneficiario final) ha contribuido enormemente para la creciente popularidad de ransomware entre los hackers.

Para protegerse y proteger a sus clientes de ataques de ransomware es importante saber cómo funciona, y luego tomar las medidas de seguridad adecuadas. La información en este breve artículo busca proveer algunas herramientas para minimizar el riesgo. A continuación, algunas sugerencias para una mayor protección:

1. Conozca su "Cyber Rating" y mejore su "conciencia cibernética". El 95% de todos los incidentes de seguridad implican un error humano, por lo tanto, la primera medida es identificar la principal falla relacionada con un factor humano dentro de la organización. En Cybint, se ofrece una evaluación gratuita para que usted y su organización puedan obtener mejores ideas, información y un panorama más claro:

2. Actualice su sistema en forma regular. Muchas de las actualizaciones en su equipo o smartphone son actualizaciones de seguridad. Esto significa que la compañía (por ejemplo Microsoft® para Windows) identifica la falla de seguridad, y le pide que actualice su sistema para evitar este *breach*. La misma actualización se ha librado a los hackers, que van a buscar los "weakest links" o eslabones más débiles de la cadena. La mayoría de estos vínculos débiles son personas, posiblemente como usted, que no tuvieron el tiempo para actualizar su sistema hasta que fue demasiado tarde.

El Consejo impone sanciones de la UE a través de las decisiones del Consejo, que son adoptadas por los Estados miembros por unanimidad. La UE pone en práctica todas las sanciones impuestas por el Consejo de Seguridad de la **ONU (CSNU).** Además, la UE puede reforzar las sanciones **UNSC** mediante la aplicación de medidas adicionales o la imposición de sanciones autónomas.

3. Evite los sitios web desconocidos. Antes de entrar en un sitio web inexplorado, usted debe comprobar qué tan confiable es. Hay herramientas en línea para ayudarle en esta tarea como https://www.mywot.com/ y listas de sitios web peligrosos.

4. Preste atención a las copias de seguridad. Los hackers saben que el secreto de los ransomware es penetrar a los sistemas de copia de seguridad. Usted debería utilizar varios tipos de copias de seguridad, con una copia de seguridad basada en la nube sincronizando backups (para permitir la recuperación de la versión previa), y copias de seguridad de "offline" (o aisladas) de almacenamiento de datos en lugares inaccesibles a la computadora infectada. Realizar copias de seguridad en lugares como las unidades de almacenamiento externo pueden evitar que la información se vuelva blanco del ransomware, llevando a que la restauración de los datos y la información sea rápida y más fácil.

https://www.delitosfinancieros.org/ciberseguridad-breve-guia-para-ayudar-a-las-organizaciones-a-protegerse-del-ransomware/