Una nueva oleada de ransomware pone de manifiesto la necesidad de entrenar capacidades en la gestión de crisis cibernéticas.

29 junio 2017 http://tecnologia.elderecho.com/tecnologia/ciberseguridad/ransomware-ciberseguridad_0_1106250037.html

El CCN-CERT e INCIBE alertan de una nueva campaña de ransomware, una variante de la familia Petya cuyo funcionamiento es similar a WannaCry, y que ya afecta a empresas a escala nacional e internacional.

Recientes incidentes masivos de ciberseguridad como WannaCry o Notpetya han comprometido en los últimos meses la seguridad de grandes compañías a escala global, generando periodos de inactividad, daños en la reputación e imagen empresarial, y poniendo en riesgo todo tipo de información, incluyendo datos de carácter sensible.

El último incidente, Notpetya, tal y como informa el Equipo del CCN-CERT, se trata de una campaña de ransomware que afecta a sistemas Windows y que cifra el sistema operativo o disco y se propaga por el resto de sistemas conectados a esa misma red. Al igual que sucedía con WannaCry, la nueva campaña solicita un rescate en Bitcoin por valor de 300 dólares; sin embargo, Notpetya puede llegar a afectar al Registro de Arranque Principal y bloquear el acceso completo al equipo, como señala Panda Security en uno de los primeros informes publicados en el sector.

La reacción de organismos y empresas proveedoras en el ámbito de la seguridad de la información no se ha hecho esperar, y en pocas horas se ha producido un aluvión de alertas y consejos para mantener a salvo a las empresas de esta nueva ciberamenaza. Entre los consejos más recurrentes, se encuentran la actualización del sistema operativo, navegadores y soluciones de seguridad, habilitar cortafuegos, aplicar parches publicados por Microsoft y evitar abrir archivos adjuntos provenientes de remitentes desconocidos.

Asimismo, cabe destacar la rápida coordinación del sector privado junto a la Administración Pública y a las Fuerzas y Cuerpos de Seguridad del Estado, para la formación de grupos de trabajo con el objetivo de compartir información detallada, protocolos y procedimientos para prevenir y hacer frente a los ciber-incidentes.

Desde la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, se han puesto en marcha iniciativas focalizadas en la prevención, concienciación a todos los niveles y capacitación como forma de mejorar la preparación de las empresas en la gestión de ciber-incidentes.

Cyber Crisis Management

El proyecto Gestión de Crisis Cibernéticas de ISMS Forum ha supuesto el primer ejercicio en colaboración con organizaciones públicas y privadas con la finalidad de fomentar buenas prácticas en materia de ciberseguridad y gestión de crisis dirigido al sector privado en

España, aportando una interesante contribución para la puesta en común de una óptima gestión de incidentes de seguridad.

El objetivo principal del ejercicio ha sido la evaluación de la resiliencia de 15 grandes compañías participantes ante posibles crisis de componente cibernética y, por tanto, la medición del estado de madurez y la mejora de las capacidades de las organizaciones para resolver la situación de crisis, a la vez que el fomento de la concienciación sobre los riesgos existentes a todos los niveles.

El proyecto se ha desarrollado bajo la dirección y coordinación de ISMS Forum en colaboración con un comité académico formado por 7 entidades, 15 grandes compañías participantes y con el apoyo de entidades públicas como el Departamento de Seguridad Nacional (DSN), el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) y en Instituto Nacional de Ciberseguridad (INCIBE).

Plataforma de Compartición de Indicadores de Compromiso (IoCs) La Plataforma de Compartición de Indicadores de Compromiso (IoCs) puesta en marcha por ISMS Forum en colaboración con S21sec, pretende dar solución a la necesidad de intercambio de indicadores de compromiso entre distintas organizaciones mediante canales seguros e independientes entre sí, evitando la habitual falta de comunicación como debilidad que permite que una amenaza pueda ir afectando empresa tras empresa, de forma masiva, con el consiguiente beneficio para los atacantes.

La plataforma opera bajo los estándares los estándares OpenIOC y STIX/Cybox y permite que cada organización adherida pueda aportar los IoCs que considere convenientes y establecer, para cada uno de ellos, su estrategia de distribución hacia el resto de participantes, analizándolo y almacenándolo en un entorno centralizado que será el que de acceso a esa información anonimizada mediante el uso de perfiles de usuarios y grupos de acceso para cada organización.

La colaboración entre las entidades es un factor clave que va a cambiar la balanza frente a las actuales amenazas, ya que hasta la fecha el aislamiento entre entidades y la falta de colaboración ha sido un factor que ha sido aprovechado por los atacantes para que las consecuencias de sus acciones se extiendan.

(Fuente: ISMS Forum)