COMUNICADOS .CO

Miércoles, 27 de septiembre de 2017.

Entidades y empresas pueden prepararse contra los ciberdelitos

Los ciberdelitos se han convertido en un verdadero dolor de cabeza tanto para organizaciones como para usuarios en general. Según el FBI los ataques en promedio de *ramsonware* ascienden a los 20.000 diarios y millón y medio por trimestre a nivel global. En los últimos tres años, solo este delito informático ha dejado daños estimados en USD$2.300 millones.

Colombia también está en la mira, según el Gaula de la Policía Nacional a la fecha se han registrado 12 casos de ataques cibernéticos a empresas establecidas en territorio colombiano provenientes de países europeos y asiáticos. El Coronel Fredy Bautista, Jefe del Centro Cibernético Policial explica que cuando se presenta un evento de cibercrimen generalmente éste proviene de varias jurisdicciones, pues cada uno de los actores que están involucrados en las amenazas pueden estar ubicados en diferentes países del mundo.

COMUNICADOS .CO

Miércoles, 27 de septiembre de 2017.

En el reciente **Foro sobre Ciberseguridad** realizado por la entidad certificadora líder del país, **Certicámara** S.A, y una de las empresas líderes en seguridad en el mundo, **Symantec,** se dieron cita líderes de tecnología y seguridad de la información de empresas privadas y entidades públicas, en Bogotá, Medellín, Bucaramanga y próximamente en Cali, a fin de actualizar a los asistentes sobre el cibercrimen, la importancia de la ciberseguridad y el uso de mecanismos de seguridad que contrarresten estas amenazas, recordando además el **top 4 de las amenazas** cibernéticas: **la contaminación de búsquedas en google** (o pago de campañas publicitarias en nombre de bancos que llevan a sitios falsos), **los perfiles falsos en redes sociales**, **las apps** peligrosas (especialmente en tiendas Android) y **la falsificación de correos corporativos** (como por ejemplo la suplantación de correos provenientes de la DIAN**),** ahora más con el auge de los correos que está enviando esa entidad para efectos de firmar electrónicamente las declaraciones de renta.

Para contrarrestar lo anterior y concientizar a los líderes de las empresas que asistieron al foro, se presentaron los mecanismos tecnológicos, estrategias defensivas, preventivas y correctivas que las empresas, entidades gubernamentales y ciudadanos pueden apropiar para blindar sus sistemas, entornos electrónicos y en general su información personal: uno de los activos más importantes que tienen las personas naturales y jurídicas. **David Kummers**, especialista en seguridad en redes de **Certicámara S.A.,** enfatizó en la importancia de implementar tecnologías con tres propósitos: **Protección, Prevención y Detección**. En el **primero** las organizaciones pueden implementar herramientas como certificados de servidor seguro y cifrado fuerte, WAF (firewall de aplicaciones web); en el **segundo** se debe contar con escaneos de vulnerabilidades y centros de operaciones de ciber-seguridad SOC/NOC, y en el **tercero** se pueden implementar escaneos de malware, sistemas de monitoreo de aplicaciones y herramientas para prevenir ataques de denegación de servicio el cual se ha convertido en el dolor de cabeza de muchos administradores de sistemas.

Kummers explicó que los navegadores web también han venido implementando cambios se seguridad durante este año y uno de los más importantes será publicado en Octubre para la **versión número 62**del famoso navegador **Chrome**, dicho navegador mostrará como "**inseguros**" los portales web que no cuenten con una conexión **https** lo cual impone un importante reto para todas las empresas que tengan una presencia en internet pues deberán implementar certificados de servidor

seguro SSL en sus portales, para evitar suplantaciones de portales y sitios web. De acuerdo con Dean Coclin, directivo de Symantec, las entidades gubernamentales en todo el mundo están migrando a conexiones HTTPS en todos sus portales lo cual garantiza que el acceso a los dominios .gov solo se permitirá por conexiones cifradas y si la página cuenta con la conexión segura.

La realidad es que existen herramientas que blinden a las empresas y usuarios de los delitos informáticos, pero entonces, ¿por qué siguen en aumento las denuncias de ataques cibernéticos? Para Kummers, las organizaciones aún no invierten recursos económicos suficientes en altos estándares de seguridad, o lo que es más preocupante, no lo hacen de una manera eficiente y apropiada conforme sus activos de información, y ven lejos la posibilidad de convertirse en víctimas de algún ataque cibernético. En cuanto a los consumidores y/o usuarios finales se evidencia la falta de prevención y de un uso adecuado de las tecnologías. *Tenemos la cultura de pagar por daños y no por prevención*.

Los ciberdelitos se han convertido en un verdadero dolor de cabeza tanto para organizaciones como para usuarios en general. Según el FBI los ataques en promedio de *ramsonware* ascienden a los 20.000 diarios y millón y medio por trimestre a nivel global. En los últimos tres años, solo este delito informático ha dejado daños estimados en USD$2.300 millones.

Colombia también está en la mira, según el Gaula de la Policía Nacional a la fecha se han registrado 12 casos de ataques cibernéticos a empresas establecidas en territorio colombiano provenientes de países europeos y asiáticos. El Coronel Fredy Bautista, Jefe del Centro Cibernético Policial explica que cuando se presenta un evento de cibercrimen generalmente éste proviene de varias jurisdicciones, pues cada uno de los actores que están involucrados en las amenazas pueden estar ubicados en diferentes países del mundo.

En el reciente **Foro sobre Ciberseguridad** realizado por la entidad certificadora líder del país, **Certicámara** S.A, y una de las empresas líderes en seguridad en el mundo, **Symantec,** se dieron cita líderes de tecnología y seguridad de la información de empresas privadas y entidades públicas, en Bogotá, Medellín, Bucaramanga y próximamente en Cali, a fin de actualizar a los asistentes sobre el cibercrimen, la importancia de la ciberseguridad y el uso de mecanismos de seguridad que contrarresten estas amenazas, recordando además el **top 4 de las**

Miércoles, 27 de septiembre de 2017.

amenazas cibernéticas: **la contaminación de búsquedas en google** (o pago de campañas publicitarias en nombre de bancos que llevan a sitios falsos), **los perfiles falsos en redes sociales**, **las apps** peligrosas (especialmente en tiendas Android) y **la falsificación de correos corporativos** (como por ejemplo la suplantación de correos provenientes de la DIAN**),** ahora más con el auge de los correos que está enviando esa entidad para efectos de firmar electrónicamente las declaraciones de renta.

Para contrarrestar lo anterior y concientizar a los líderes de las empresas que asistieron al foro, se presentaron los mecanismos tecnológicos, estrategias defensivas, preventivas y correctivas que las empresas, entidades gubernamentales y ciudadanos pueden apropiar para blindar sus sistemas, entornos electrónicos y en general su información personal: uno de los activos más importantes que tienen las personas naturales y jurídicas. **David Kummers**, especialista en seguridad en redes de **Certicámara S.A.,** enfatizó en la importancia de implementar tecnologías con tres propósitos: **Protección, Prevención y Detección**. En el **primero** las organizaciones pueden implementar herramientas como certificados de servidor seguro y cifrado fuerte, WAF (firewall de aplicaciones web); en el **segundo** se debe contar con escaneos de vulnerabilidades y centros de operaciones de ciber-seguridad SOC/NOC, y en el **tercero** se pueden implementar escaneos de malware, sistemas de monitoreo de aplicaciones y herramientas para prevenir ataques de denegación de servicio el cual se ha convertido en el dolor de cabeza de muchos administradores de sistemas.

Kummers explicó que los navegadores web también han venido implementando cambios se seguridad durante este año y uno de los más importantes será publicado en Octubre para la **versión número 62**del famoso navegador **Chrome**, dicho navegador mostrará como "**inseguros**" los portales web que no cuenten con una conexión **https** lo cual impone un importante reto para todas las empresas que tengan una presencia en internet pues deberán implementar certificados de servidor seguro SSL en sus portales, para evitar suplantaciones de portales y sitios web. De acuerdo con Dean Coclin, directivo de Symantec, las entidades gubernamentales en todo el mundo están migrando a conexiones HTTPS en todos sus portales lo cual garantiza que el acceso a los dominios .gov solo se permitirá por conexiones cifradas y si la página cuenta con la conexión segura.

COMUNICADOS .CO

Miércoles, 27 de septiembre de 2017.

La realidad es que existen herramientas que blinden a las empresas y usuarios de los delitos informáticos, pero entonces, ¿por qué siguen en aumento las denuncias de ataques cibernéticos? Para Kummers, las organizaciones aún no invierten recursos económicos suficientes en altos estándares de seguridad, o lo que es más preocupante, no lo hacen de una manera eficiente y apropiada conforme sus activos de información, y ven lejos la posibilidad de convertirse en víctimas de algún ataque cibernético. En cuanto a los consumidores y/o usuarios finales se evidencia la falta de prevención y de un uso adecuado de las tecnologías. *Tenemos la cultura de pagar por daños y no por prevención*.