

Los ciber riesgos se intensificarán en 2017 con más ciber espionaje y ataques a la integridad de los datos, según el informe “2017 Cybersecurity Predictions” de Stroz Friedberg

El nuevo informe destaca seis predicciones para 2017 que ayudarán a los profesionales de la seguridad y a los directivos a prepararse para las principales ciber amenazas

25 de Enero de 2017 – Stroz Friedberg, compañía de Aon, alerta que en 2017 se intensificarán los ciber ataques, habrá nuevas regulaciones y se experimentará un giro en la forma en la que las empresas enfocan la gestión de los ciber riesgos. Las principales amenazas este año incluyen casos de ciber espionaje a nivel nacional, un incremento en los ataques a la integridad de los datos y un aumento en los ataques con daños a dispositivos relacionados con IoT (Internet of Things).

Con la seguridad cibernética firmemente arraigada como una de las cuestiones más importantes que afectan a la seguridad internacional, la política, la estabilidad económica y la delincuencia transaccional, la comprensión de los riesgos cibernéticos existentes y emergentes es más relevante que nunca. Las predicciones de Stroz Friedberg describen las principales amenazas cibernéticas a las que se enfrentan las empresas y ofrecen recomendaciones sobre cómo las organizaciones pueden aumentar su resistencia frente a estas amenazas.

"En 2016 hemos sido testigos de todo tipo de casos, desde ataques cibernéticos que influyeron en la opinión pública hasta el hackeo de dispositivos IoT o la introducción de nuevas regulaciones de seguridad cibernética. Este año veremos una intensificación de estas amenazas y la aparición de nuevos desafíos, a la vez que se desdibujan las líneas entre las acciones y responsabilidades del Estado, los mercados, las empresas y la sociedad civil ", afirma Ed Stroz, co-presidente y cofundador de Stroz Friedberg. "La avalancha de noticias falsas y los ataques en las elecciones del año pasado son sólo una señal de lo que vendrá, ya que los atacantes encontrarán nuevas maneras de buscar un acceso más rápido y amplio a los datos y de explotar información confidencial".

Las predicciones destacadas en este informe incluyen:

- **Los criminales aprovechan los dispositivos IoT como botnets (redes de robots informáticos o bots) para atacar la infraestructura:** En 2017 Stroz Friedberg prevé que habrá un aumento en los dispositivos IoT comprometidos, aprovechados como botnets y utilizados como puntos de lanzamiento para la propagación de malware, SPAM, ataques DDoS y mantenimiento del anonimato de las actividades maliciosas.
- **El espionaje cibernético y la guerra de información a nivel nacional influyen en las estrategias globales y políticas:** El espionaje cibernético seguirá influyendo en la política global y se extenderá a las próximas elecciones en América Latina y Europa. Rusia, China, Irán y Corea del Norte seguirán siendo regiones objeto de gran preocupación en 2017, a medida que continúen desarrollando grupos de alto conocimiento en crímenes cibernéticos.
- **Los ataques a la integridad de los datos aumentan:** El sabotaje de datos se convertirá en la próxima gran amenaza en 2017. Los criminales buscarán sembrar confusión y duda sobre la exactitud y fiabilidad de la información, perjudicando la toma de decisiones en el sector privado y público.
- **Las tácticas de phishing y de ingeniería social se vuelven más hábiles, orientadas y avanzadas:** A medida que las organizaciones continúan aprovechando las tecnologías emergentes, incluyendo la nube y el IoT, y paralelamente reforzando las defensas perimetrales para elevar el nivel de seguridad de la red, los delincuentes concentrarán su atención en el elemento humano como punto de entrada. En 2017, las tácticas avanzadas de ingeniería social

serán más específicas, astutas y eficaces, explotando el vínculo más débil - los empleados - que las organizaciones siempre encuentran difícil de salvaguardar.

- **Las presiones reguladoras hacen que el Red Teaming sea clave, siendo el desarrollo del talento en ciberseguridad uno de los principales retos:** El aumento de la presión de los reguladores de todo el mundo obligará al desarrollo de las capacidades internas de Red Teaming en 2017. Además, las empresas que no están en el negocio cibernético se enfrentarán a un reto diferente: reclutar, motivar y retener talento cibernético altamente técnico para mantener a sus Red Teams a la vanguardia de la ciberseguridad. Este empuje ocurrirá probablemente primero en los centros financieros como Hong Kong, Singapur, Unión Europea e incluso EE.UU.
- **Los sectores más avanzados apoyan la due diligence sobre ciberseguridad previa a las fusiones y adquisiciones:** La industria de servicios financieros y otros sectores regulados serán los primeros en adoptar la due diligence sobre ciberseguridad como una parte crítica del proceso de due diligence previo a cualquier fusión y adquisición, como lección aprendida de las transacciones de alto perfil que no llegaron a buen fin en 2016 por su exposición a distintas vulnerabilidades cibernéticas.

Acerca de Stroz Friedberg

Stroz Friedberg, compañía de Aon, es una empresa especializada en gestión de riesgos cuyo objetivo es ayudar a los clientes a resolver los complejos retos derivados del entorno digital, interconectado y regulado que prevalece actualmente en el mundo empresarial. Líder global en seguridad informática con los principales expertos en medicina forense digital, respuesta a incidentes e investigación sobre seguridad; investigación; eDiscovery y Due Diligence, Stroz Friedberg trabaja para maximizar el bienestar de la organización, lo que garantiza su sostenibilidad, protección y capacidad de recuperación. Fundada en 2000 y adquirida por Aon en 2016, Stroz Friedberg cuenta con oficinas en nueve ciudades de Estados Unidos, Londres, Zurich, Dubai y Hong Kong, trabajando actualmente con compañías Fortune 100, el 80 por ciento de la AmLaw 100 y los 20 mejores bufetes de abogados del Reino Unido.

Acerca de Aon

Aon plc (NYSE: AON) es una empresa líder en servicios de gestión de riesgos, intermediación de seguros y reaseguros, soluciones de recursos humanos y servicios de outsourcing. Aon cuenta con una sólida estructura internacional integrada por 72.000 empleados en 120 países, lo que le permite ofrecer a sus clientes un valor añadido a través de soluciones innovadoras y efectivas en materia de gestión de riesgos y personas. Visite <http://www.aon.es> para más información sobre nuestras capacidades y sobre la forma en la que Aon desarrolla al máximo las posibilidades de sus clientes.

Sigue a Aon España en las redes sociales:

www.twitter.com/Aon_Espana / www.facebook.com/aon.espana1 / <https://www.linkedin.com/company/aon-spain>

Para más información por favor contacte con:

Aon /Dirección de Comunicación

T: 91 340 50 18

dcomunic@aon.es