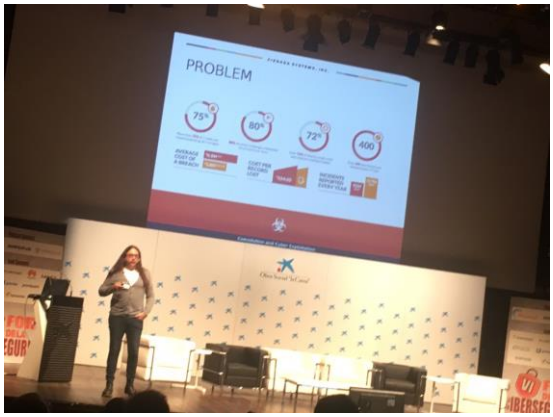
El VI Foro de la Ciberseguridad de ISMS Forum alerta: en cada minuto se viven ya 400 nuevos ciberataques.

JOSÉ M. VERA
Miércoles 27 de septiembre de 2017, 13:17h http://www.onemagazine.es/vi-foro-ciberseguridad-isms-forum-spain-que-se-ha-dicho-inteligencia-artificial

Más ataques, más sistemas proactivos y más estudio del atacante antes de que se produzca. Estas son las necesidades que se han planteado en el foro ejecutivo de ciberseguridad que celebra en otoño el ISMS Forum Spain en el que también se ha alertado de conectarlo todo sin la seguridad básica necesaria.

El **secretario de Estado de Agenda Digital, José María Lassalle** ha inagurado el VI Foro de la Ciberseguridad del ISMS Forum Spain explicando el reto de la mujer en el mundo de la ciberseguridad y el buen trabajo que está realizando el Instituto Nacional de Ciberseguridad, Incibe. El foro, con cerca de 300 ejecutivos de ciberseguridad, ha sido presentado porDaniel Largacha, director del centro de estudios en ciberseguridad de ISMS Forum, ha explicado la importancia de la ciberseguridad, ya que la seguridad ha empeorado en las últimas décadas por la digitalización de la sociedad -sin tener un plan B, en caso de crisis-, por la hiperconectividad derivada de la reorganización. Ello supone que un pequeño problema que ocurre en una región de Asia, como fue el WannaCry, amenazó en 24 horas a todo el mundo. Y por último la interdependencia. No vale salvarse uno, sino que lo que le afectaba al de enfrente te afectaba a ti. Porque ya no se puede prestar un servicio sin contar con el otro.

Por eso la importancia de este foro para abordar los retos de la actual tecnología para proteger las empresas, cómo debería usarse la inteligencia artificial a la seguridad de la información y, también, para plantear nuevos retos para mejorar la defensa de las empresas antes posibles retos.



Anthony Bucci: "En 2017 hay 400 nuevos ciberataques por minuto"

El experto en inteligencia artificial, que comenzó trabajando en una de las primeras instalaciones no militares que trabajaron con inteligencia artidicial, la Case Western Reserve University, ha explicado que en su trabajo, como ceo de Legit Patentes, continúa trabajando en el día a dia

con algoritmos e inteligencia artificial para tomar decisiones. “Así que no soy un gran experto en ciberseguridad sino en la computación evolucionaria y la IA y cómo se puede aplicar a la ciberseguridad”, ha comenzado explicado.

Bucci ha destacado que actualmente el coste de la ciberseguridad es de 400.000 millones de dólares al año. “Lo preocupante es que el 75% de los ataques no son detectados a tiempo, el 72% de las empresas, que son pymes, son atacadas de forma consistente y no salen en el telediario a pesar de las pérdidas que le supone. Para el 2017 nos enfrentamos a 400 nuevas amenazas por minuto.

"El problema es que hay una gran asimetría entre el atacante y los defensores. Si es una vulnerabilidad conocida para hacerla frente cuesta poco, pero en los importantes se calcula que se invierte el trabajo de hasta seis meses para recuperar la normalidad. El problema es que actualmente todo es reactivo. SE hacen cosas tras detectar el ataque. Se diseña un antivirus… tras detectar el virus. Y para los que quieren anticiparse con heurística, con el estudio del comportamiento humano, también hay que haber conocido un patrón human. Así que se trabaja con lo que ya ha sucedido".

Así ha mostrado una simulación en la que se puede ver cómo se reacciona ante un ataque y curiosamente se comprueba que en pocas horas las defensas dejan de servir ante un ataque y las alertas dejan de actuar, por lo que los criminales pueden entrar en la red y hacer lo que quisieran. "Esto pasaría si no se cambiara y evolucionaran los sistemas de seguridad".

"Los criminales y los defensores vamos realizando una carrera en la que se cambian las técnicas de ataque y se adaptan las defensas. Es como el código genético de dos organismos que evolucionan según las mutaciones del otro. Hay conceptos simplistas como el predador y la presa. Si la presa desarrolla el camuflaje el depredador lo hará con sus técnicas de detección porque sino no comerá y se extinguirá. En el mundo académico se estudia como aplicar algoritmos a la coevolución para defender de las ‘mutaciones’ que se producen en los sistemas y

técnicas de ataque. Sí es importante tener en cuenta que hay sistemas, como los llamados Cienaga, la compañía para la que trabajo, que ya utlizan estas tecnologías de algoritmos inteligentes para proteger las empresas".

"El futuro sugiere que crecerá el ransomware, dando lugar a una economía subterránea, con empresas que sean capaces de desarrollar sistemas de defensa que permitan detectar patrones en individuos que estén intentando desarrollar este tipo de ataque. También llegarán muchas amenazas nuevas para las que sólo habrá defensa simulando estos posibles nuevos entornos y cómo les haríamos frente con nuestras defensas. Hay que actuar antes del atacante en vez de cuando éste ya ha actuado", ha terminado explicando Bucci.

Álvaro Cordero, de Akamai USA ha explicado cómo trabaja la empresa a través de una plataforma que permite conocer el tráfico mundial y proteger a las empresas que están en ella. Entre otros ataques importantes detectados ha sido importante Mirai, que iba contra infraestructuras. Actualmente ya no se trata de afectar webs, sino las DNS, etc. ¿Cómo defenderse de ellos? Con una gran capacidad de procesado y limpiado del tráfico, con detección y mitigación para reducir las consecuencias del ataque y, también, disponer de un soporte contínuo, ya que la campaña del Mirai duró una semana.

Cordero ha explicado cómo se comienza a detectar los 600 Gbps de ataque que hicieron saltar las alertas de varios sistemas y cómo con las herramientas de Akamai se pudo minimizar y anular el ataque a pesar de

estar siendo realizado por dispositivos de todo tipo, también móviles, y desde 100 países del mundo. El problema para anular este tipo de ataque es que están muy distribuido, con más de 200.000 servidores, y a través de una herramienta podemos configurar nuestra plataforma en poco más de cinco minutos.

También se ha realizado una mesa redonda en la que han participado desde **Raul Pérez, Global Security Architec de Panda, Alberto Ruiz de Sophos, Alberto Cita, de Simantec, José de la Cruz de Trend Micro, Alfonso Mártinez de Forcepoint y Samuel Bonete de Fortinet. Una mesa que ha moderado el nuevo CISO de Bankinter, Gonzalo Asensio.**

En ella se ha comenzado analizando si pensar que hay que defender el perímetro o la red en todo su interior. Se trata de tener unos criterios claros para trabajar en ciberseguridad con el llamado Machine Learning, con máquinas que aprenden en su día a día a defender la empresa de ciberamenazas. “Hay muchos vectores de entradas que no tenemos en cuenta. Pero también pueden ser una fuente de información. Por ejemplo, Fortinet tiene más de 300.000 clientes y nos facilitan información de lo que ocurre, de las amenazas que reciben… recopilados 38 teras de información al año de tráfico de red, archivos maliciosos, peticiones a una IP… Información que completamos con lo que compartimos con otros fabricantes en diferentes asociaciones o sistemas como Virus Total. Se trata de información que tiene tal cantidad de datos que sería imposible utilizarse sin el uso de las máquinas, de la inteligencia artificial”, ha destacado el regional Sales manager de Fortinet, Samuel Bonete.

Sólo la inteligencia artificial permite hacer frente a millones de ciber amenazas

Raul Pérez de Panda Security ha explicado cómo la inteligencia artificial puede solventar los problemas de escalabilidad. “Ahora se paga por soluciones de seguridad pero no evitan la infección. Los malos cada vez escalan más, con malware más complejo, mejor distribuido y más complejo. Así que los sistemas de detección eurística clásicos no valen.

Se generan 1.000 millones de samples al día. Cada vez que me llega un ataque es muy probable que sea nuevo. Somos una compañía que no tiene cientos de personas defendiendo empresas así que en 2001 apostamos por la inteligencia artificial para hacer frente, de forma automática, al malware entre otras técnicas detectando el goodware. El resultado es que hemos conseguido una detección casi del 100% con nuestros actuales sistemas de inteligencia artificial. Pero estos algoritmos necesitan mucho trabajo hasta conseguir lo que hemos logrado y es que las máquinas y el deparmento que llamamos los 'algoritmeros', integrado por profesores de matemáticas, puedan tener un 100% de defensa".

El deep machine learning permite detectar y mitigar ciberataques en tu dispositivo

Alberto Ruiz, presales en Sophos Iberia, ha destacado que "el deep learning es un paso más sobre el machine learning. Este depende del ser humano, ya que somos nosotros el que establecemos los patrones de trabajo. Deep Learning es la nueva puesta de Google, Amazon, etc. enviando muestras de software malicioso y es la propia tecnología la que toma sus decisiones. Ello permite detectar de forma automática el cisne negro en medio del lago de cisnes blanco. Se trata de que el sistema tome conclusiones, incluso distintas de las humanas. El ser humano siempre condiciona el aprendizaje mientras que en Sophos Labs lo que hacemos es introducir en el sistema muestras maliciosas para que el sistema saque sus conclusiones y sea utilizado por los clientes para su defensa. El Deep Machine Learning nos permite realiza la defensa en cada puesto de trabajo, llevar esa protección siempre contigo. Por ejemplo, se pasa entre 500 y 10 Gigas mientras que el Deep Learning unos pocos megas. Ello permite dar respuestas en cualquier pequeño equipo en 20 milisegundos. Se trata de detectar pero también mitigar y eso es lo que consigue y el reto de Deep Machine Learning que hemos desarrollado en Sophos tras la compra de Invicia que era experta en esta tecnología".