PROYECTO FINAL DE INGENIERÍA

Intensivo, 04/2015

EL CAMINO EVOLUTIVO DE APLICAR LOS CONCEPTOS Y CONOCIMIENTOS DE CIENCIAS NATURALES EN LA GENERACIÓN DE MECANISMOS DE PROTECCIÓN CONTRA LA CRECIENTES AMENAZAS CIBERNÉTICAS

Bernardi, Antonio Luis Ángel – LU66428

Ingeniería en Informática

Tutor:
Blanco, Luis Arturo, Universidad Tecnológica Nacional

Agosto 10, 2015

UNIVERSIDAD ARGENTINA DE LA EMPRESA

FACULTAD DE INGENIERÍA Y CIENCIAS EXACTAS

Tabla de Contenidos

Reconocimiento

A mi querida esposa, Maia, quien me animó en el camino y siempre creyó en mí.

Abstract

The use of the knowledge and understanding of natural sciences, in particular the human body, applied to computer security is an appealing concept for two reasons. Firstly, the human immune system provides the human body with a high level of protection from invading pathogens, in a robust, self-organised and distributed manner. Secondly, current techniques used in computer security are not able to cope with the dynamic and increasingly complex cyber threat landscape of computer systems. It is hoped that biologically inspired approaches in this area, including, but not limited, to the use of immune-based systems will be able to meet this challenge. Here I reviewed the research advances in several other related fields of studies. Hopefully, I will present ideas to further design and develop improved protection systems. I will provide an introduction and analysis of the key developments within these fields, in addition to making suggestions for future research.

Objetivo

El objetivo de esta tesis es desarrollar la idea de la necesidad de diseñar, adoptar y desarrollar un marco metódico y las técnicas para un mecanismo defensivo más eficaz, eficiente, adaptable y sostenibles basados en los avances logrados en las ciencias naturales aplicadas a la prevención, detección temprana, respuesta, recuperación y contramedidas contra los ataques cibernéticos.

Cobertura y alcance

La tesis se basa en diferentes fases:

En primer lugar, un análisis del problema en relación con el delito cibernético y el espionaje cibernético;
En segundo lugar, representar el entorno normativo y regulatorio, las metodologías y estándares, las estrategias actuales, políticas, procedimientos, herramientas y soluciones actualmente en marcha para luchar contra esta amenaza;

En tercer lugar, identificar las brechas y por qué los atacantes cibernéticos están ganando la batalla;
Por último, volver a desarrollar la idea de combinar el conocimiento y los avances obtenidos

en otras ciencias, como la microbiología, inmunología, la ciencia cognitiva y la biología evolutiva para apoyar la comprensión de cómo los seres vivos y en particular como el cuerpo humano han evolucionado para ser adaptable a combatir las amenazas contra los virus, bacterias, etc., y los elementos que ponen en riesgo el bienestar y en definitiva la vida.

Esta es una idea que ya ha sido citado por más de dos décadas desde el descubrimiento de los primeros programas maliciosos denominados virus y la posterior elaboración y adopción de software anti-virus ampliamente utilizado hoy en día.

No obstante, esto requiere un nuevo análisis, específicamente en la comprensión de cómo ha progresado el conocimiento del cuerpo humano y en otra ciencias naturales. Esto tiene como objetivo provocar una discusión y posible sentar las bases de las futuras nuevas ideas, marcos metodológicos y herramientas mejoradas que apoyarán en esta batalla que se está perdiendo.

Definiciones

Según Wikipedia:

Cibernética: Cyber-se deriva de "cibernética", que viene de la palabra griega que significa κυβερνητικός *experto en la dirección o de gobierno*. Por lo general es un prefijo añadido a una amplia gama de palabras existentes para describir nuevos, en Internet o temas relacionados con la informática de los conceptos existentes, a menudo los productos y servicios electrónicos que ya tienen una contraparte no electrónica.

Microbiología: Es el estudio de los organismos microscópicos, los que son unicelulares (única célula), multicelular (colonia de células), o acelular (que carece de células).

Inmunología: Es una rama de la ciencia biomédica que cubre el estudio de todos los aspectos del sistema inmune en todos los organismos. Tiene que ver con el funcionamiento fisiológico del sistema inmunológico en los estados de la salud y las enfermedades y mal funcionamiento del sistema inmune en los trastornos inmunológicos (enfermedades autoinmunes, hipersensibilidades, deficiencia inmune, rechazo de trasplantes).

En el mundo académico, la inmunología computacional es un campo de la ciencia que abarca genómica de alto rendimiento y la bioinformática enfoques de la inmunología. El principal objetivo del campo es convertir los datos inmunológicos en problemas de cálculo, resolver estos problemas utilizando métodos matemáticos y computacionales y luego convertir estos resultados en interpretaciones inmunológicamente significativas.

Heurística: En informática, la inteligencia artificial, y la optimización matemática, heurística es una técnica diseñada para resolver un problema más rápidamente cuando los métodos clásicos son demasiado lentos, o para encontrar una solución aproximada cuando los métodos clásicos no encuentran ninguna solución exacta. Esto se logra mediante la optimización, la integridad, exactitud o precisión para la velocidad. En cierto modo, se puede considerar un acceso directo a una solución sin resolver totalmente un problema.

La ciencia cognitiva: es el estudio científico interdisciplinario de la mente y sus procesos. Examina lo que la cognición es, qué hace y cómo funciona. Incluye la investigación sobre la inteligencia y el comportamiento, sobre todo centrándose en cómo se representa la información, procesa y transforma (en las facultades tales como la percepción, el lenguaje, la

memoria, la atención, el razonamiento y la emoción) dentro de los sistemas nerviosos (humanos u otros animales) y máquinas (por ejemplo, ordenadores). La ciencia cognitiva consiste en múltiples disciplinas de investigación, incluyendo la psicología, la inteligencia artificial, la filosofía, la neurociencia, la lingüística y la antropología. Se extiende por muchos niveles de análisis, de aprendizaje y de adopción de mecanismos de bajo nivel a la lógica de alto nivel y la planificación; de los circuitos neuronales de la organización del cerebro modular. El concepto fundamental de la ciencia cognitiva es que "el pensamiento se puede entender mejor en términos de estructuras de representación en la mente y procedimientos computacionales que operan en esas estructuras."

La biología evolutiva es un sub-campo de la biología se ocupa del estudio de los procesos evolutivos que produjeron la diversidad de la vida en la Tierra.

Exclusiones y aclaraciones

Esta tesis no elaborará una descripción detallada de las ciencias mencionadas en la sección Alcance como las referencias a éstos se basan puramente en las referencias a la comprensión obtenida a lo largo de la investigación para esta tesis. Referencias adicionales se han recogido a través de conversaciones informales con expertos en seguridad cibernética en fórums, conferencias y reuniones.

Intentare detallar la mayor cantidad de esas referencias y, cuando sea posible, las personas de referencia como reconocimiento y agradecimiento por su contribución. Esto no debe ser considerado como consentimiento expreso; las ideas o conocimientos referenciados pertenecen a los respectivos autores.

Introducción:

La batalla contra las amenazas cibernéticas se está perdiendo. Informes diarios en los medios nos hace lentamente estar menos sorprendidos. Asumiendo que seremos atacados es desafortunadamente una expectativa y una cuestión de tiempo. La preocupación se está desplazando desde **si** vamos a recibir una llamada de nuestro banco de esas sospechosas transacciones miles de kilómetros de distancia, hacia **cuándo** esto ocurrirá y cuando recibiremos la nueva tarjeta de débito. Del mismo modo los individuos, hasta el más obsesionado con la privacidad, se están acostumbrando a la idea de que las agencias gubernamentales están espiándonos diariamente con argumentos simples como el de la protección pública y la seguridad nacional.

Cuanto mayor sea el avance de la tecnología, los humanos estarán cada vez más cómodos con aceptar y vivir con esas amenazas y riesgos a cambio de los beneficios de estar siempre conectados. Por otra parte, no sólo estamos conectados, con varios dispositivos, (PCs, laptops, tabletas, teléfonos inteligentes, etc.) también nuestras posesiones están conectados (televisores inteligentes, centros multimedia domésticos, refrigeradores, sistemas de alarma, CCTVs, sensores hogareños, cámaras IP, etc.). Esto significa que los vectores de la exposición se multiplican exponencialmente.

A esto se debe agregar la realidad de que el atacante, que fue históricamente un único típico hacker de sótano, y ahora es tal vez la menor de las preocupaciones. La principal atención es que este es un mecanismo cada vez más usado por el crimen organizado. Robo de datos personales para el robo de identidades, para solicitar crédito ilícito, clonación de tarjetas, etc.

Pero esto no es todo, tenemos otros jugadores mucho más poderosos e ingeniosos, los gobiernos. Desde el espionaje tradicional ha movido en el mundo cibernético ahora los nuevos espías son más propensos a ser personas en oficinas en frente de las computadoras que reemplazaron al tradicional espía de la Guerra Fría.

El miedo al terrorismo también ha abierto nuevas vías para que los gobiernos de aprovechar los dispositivos personales y filtrar y analizar prácticamente todos los medios de comunicación electrónicos. A pesar de las leyes europeas de privacidad que van en contra de

las actividades espionaje de la NSA[1] de los Estados Unidos y el CGHQ [2]del Reino Unido que Snowden de la CIA y Assange de WikiLeaks nos develaron la realidad es que también los europeos están divididos respecto al tema. Desde los ataques contra el sistema de transporte del Reino Unido en 2005, hasta los más recientes Charlie Hebdo y Bataclan en Paris a principios y fines del 2015, los Euro-diputados están poniendo el debate una vez más en la mesa para flexibilizar la ley para permitir acceso a la información para que puedan ayudar a prevenir o interrumpir nuevos ataques contra la seguridad pública.

Esto es todo lo que lleva a un paisaje cada vez más complejo de amenazas y vectores de ataque expuestos que no se puede ganar... o ¿si se puede?

[1] National Security Agency
[2] Government Communications Headquarters

Situación Actual

La primera parte, como se ha dicho, tendrá como objetivo describir a qué retos nos enfrentamos ahora y también cómo se originó la idea de esta tesis. Esto fue, básicamente, parte de la investigación que llevé a finales del año 2014 en lo que se refiere a la las amenazas cibernéticas y a la alta tasa éxito de ataques que sigue en aumento y lo poco que se hace para cambiar nuestros modos de pensar y el comportamiento para empezar a tratar de cambiar la dirección sobre como lidiamos esta problemática que no va a desaparecer sino crecer.

El resumen de los resultados de dicha investigación los presenté en la segunda Conferencia Anual de Gestión de Riesgos de Tecnología de la Información, en Londres, Reino Unido el 2 y 3 de febrero de 2015.

Los puntos destacados fueron los siguientes:

- Hay inconsistencia en las predicciones sobre los riesgos emergentes. Los ángulos y vectores de ataques se multiplican y los empresas especializadas en seguridad[3], que su principal propósito es ser los mejores asesores acerca del tema, no son consistentes. Según los reportes de investigación de seguridad publicados en el 2014 por estas empresas muestra, hay 31 riesgos y amenazas a sólo 3 de esos riesgos se han destacado como importantes por lo menos 3 informes clave.

  Esto indica que, como industria, tenemos todavía mucho que hacer y mejorar en un tema que nunca ha sido más importante. En particular, la seguridad de tecnología de la información (TI), riesgos de TI y las disciplinas de auditoría de TI debe mejorar su posición estratégica para fomentar la conciencia continua para poder asesorar correctamente la alta Gerencia y el Consejo de Administración para apoyar una priorización adecuada sobre las inversiones en tecnología y seguridad informática.

  Una realidad que también es importante destacar que en la parte posterior de la crisis financiera mundial que comenzó a fines del 2008, no sólo los grandes bancos globales han sufrido enormes pérdidas y muchos se vieron obligados a ser rescatados para evitar declarar bancarrota sino también grandes multinacionales de todos los sectores

[3] Symantec, Kaspersky, McAfee, Trendmicro, Websense y HP entre otras.

fueron afectados por la falta de crédito y por lo tanto lo que empezó como una crisis bancaria se convirtió en una crisis mundial que afectó a casi todo el mundo.

Esto se menciona porque una de las consecuencias más relevantes de esta crisis fue que el gasto y los presupuestos se redujeron significamente y llevó a que empresas que implementaban tecnología de última generación se limitaran a mantener su infraestructura mínima a costo de inversión casi nulo. El impacto obviamente llevo a que en un periodo de tiempo relativamente corto la tecnología de hardware y software se convirtieran en obsoletos con lo que conlleva a un mayor nivel de exposición de riesgo de TI. Esta falta de recursos para mantener el ambiente de TI actualizado reduce el nivel mínimo de protección y genera mayores riesgos cibernéticos.

- El segundo aspecto cubierto fue un vistazo a los "enemigos". Como se mencionó brevemente en la introducción, los atacantes cibernéticos no son sólo los hackers tradicionales motivados por el argumento "porque pueden", esto es claramente ahora dirigido por agencias del gobierno, ejércitos, grupos paramilitares, células terroristas, crimen organizado y activistas o 'hacktivistas'. Cada uno de ellos tienen un objetivo diferente o propósito y objetivo y algunos están extremadamente bien financiados; por lo tanto, es otra de las razones por que las organizaciones que actualmente se financian insuficientemente no podrán contra la variedad y diversidad de métodos de ataques y atacantes. Sobre el tema de la financiación, McAfee[4] publicó un informe que estima que hasta junio de 2014 hubo un costo impacto estimado de más de medio billón de dólares estadounidenses relacionado a defender y responder a ataques informáticos.

  Además, el aspecto normativo que los organismos reguladores comenzaron a establecer globalmente se generó porque cada vez están recibiendo más presión política y están más preocupados de que algunos Consejos de Administración no están siendo suficientemente conscientes de la gravedad de la situación.

  Por eso algunos entes reguladores optan por ser más intrusivos y más directivos hacia definir controles específicos de seguridad informática. Un ejemplo es la Autoridad Monetaria de Singapur que requiere el cifrado de base de datos de información de los

[4] McAfee Net Losses: Estimating the Global Cost of Cybercrime – June 2014 - http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf

clientes a pesar de algunas de estas bases de datos es interna y no expuestos directamente en la zona desmilitarizada (DMZ).

Un comentario final de este punto se centró en la creciente diversidad de los efectos que pueden ser los ataques que afectan a las organizaciones, no sólo financiera, sino también daños a la reputación, que afecta a la ventaja competitiva y la marca. Todo lo que resulta en la degradación efectiva de los clientes y la percepción pública.

- La tercera sección comenzó a describir los pasos hacia la defensa. Está dirigido para describir lo básico: quién, qué, cuándo, cómo y por qué.
  El "quién" indica claramente que dentro de las organizaciones ya no es un problema de TI. Esto debe ser patrocinado por los más altos directivos de la organización o entidad. En los servicios financieros, el director general y el Consejo de Administración como patrocinadores principales y líderes en la dirección estratégica para establecer un plan para los riesgos cibernéticos. Esto es clave como uno que se mantenga en la parte superior de sus agendas y sea un ejercicio continuo, no algo esporádico. La mayoría de las organizaciones globales están recibiendo el mensaje. Desde el despido del CEO y CIO después del ataque cibernético al cadena de tiendas Target de EE.UU en diciembre de 2013, esto provocó la atención de casi todos los CEO en una escala global o el más reciente caso de Ashley Madison.

  El "quién" elaboró en el aspecto sobre la necesidad de aumentar la transparencia de la información y compartirla con socios estratégicos, clientes, empleados, reguladores, etc., en un esfuerzo multi-industria para unir fuerzas en la guerra contra las amenazas cibernéticas.

- El siguiente aspecto considera el "qué", que empieza a destacar la necesidad de olvidar los supuestos de que la tecnología que fue segura ayer e incorrectamente asumir que seguirá segura mañana. Esto intenta describir el problema de que algunas organizaciones han demorado el reemplazo de la tecnología más antigua que se mantiene casi totalmente obsoletas y altamente vulnerable como puntos ciegos a los ataques.
  Una arquitectura flexible y adaptable, más moderna y basada en la seguridad por diseño, debe ser la base de la tecnología del futuro.

Esta sección también introdujo el primer pensamiento acerca de que la innovación no solo se refiere evitar intentar "reinventar la rueda", sino inculca a observar las interacciones humanas y de la naturaleza para aprender acerca de cómo los organismos se adaptan rápidamente a la hostilidad de los entornos en los que viven. La capacidad y agilidad de adaptación es de suma importancia para las organizaciones de hoy para la supervivencia en este entorno cibernético hostil.

Por último, fue añadido el concepto de aprendizaje automático aplicable a esta adaptación necesaria y la consideración de los avances de la seguridad de los datos masivos (o mejor conocido en inglés como Big Data Security) que aplican los conceptos de variedad-velocidad-volumen de información de seguridad para permitir la detección temprana y reacciones más rápidas contra los ataques.

- El punto de "cómo" presentó varios aspectos como adoptar una solución y un marco estratégico para defenderse. Este fue, pero no limitado a, centrar los esfuerzos en la identificación y priorización de datos críticos y hace que esos datos sean los más difícil de alcanzar. Construir y mantener mecanismos de protección centrados en los datos críticos más allá de la seguridad de la red tradicional. Los aspectos de una fuerte encriptación, gestión de derechos digitales, autenticación de múltiples factores, mientras que éstos no son nuevos, no se aplican generalmente para los datos no expuestos externamente, pero ahora son los controles que se deberían re-considerar. El aspecto en relación con el riesgo de atacante interno es demasiado grande como para ser ignorado. Esto también está relacionado a los conceptos de defensa en profundidad (conocido en inglés como defense-in-depth) y también defensa multicapa (conocida en inglés como layered security).

  La mejor analogía vino a mí después de una discusión con una colega en la preparación para la conferencia del febrero pasado. Cuando le estaba explicando el enfoque en la priorización de los datos clave y críticos como la premisa para el despliegue de cualquier solución. Mencionó el punto de la forma en que el cuerpo humano ha evolucionado para proteger el cerebro con un casco de hueso duro como el cráneo y el corazón con la caja torácica. Estos dos órganos son los más importantes y si éstos son atacados o en peligro las posibilidades de supervivencia son prácticamente nulas, donde otros órganos están menos protegidos porque en el caso de un ataque los efectos pueden ser malos, pero no son tan directamente fatales.

Esto también introdujo el tema de la arquitectura empresarial dentro de las organizaciones, una disciplina que está ganando más y más respeto y arquitectos corporativos de seguridad son actores clave en el diseño de las soluciones de TI de próxima generación. Seguridad por diseño como algunos de los marcos metodológicos de arquitectura más nuevos están describiendo.

El siguiente aspecto de este tema elaborado en la evidente necesidad de llevar el negocio a las discusiones cibernéticas ya que, en última instancia, sus sistemas aplicativos de negocio y los datos son uno de los factores clave de éxito para ellos. Esta actividad 'construir puentes' es, básicamente, hacer que se ellos se involucren y comprometan en tomar conciencia y se comprometan a asumir responsabilidades sobre el problema que estamos enfrentando.

Otro tema en este punto es el problema ya se ha mencionado en la introducción, la falta de financiación y la falta de consistente atención en los múltiples canales y vectores de atacantes para irrumpir en los sistemas puede no todas se resuelva de una vez. El eslabón más débil no es uno, sino multiples y todos se pueden utilizar en partes iguales por los distintos tipos de atacantes para obtener acceso y hasta puede ocurrir al mismo tiempo. A continuación, vuelvo a hacer hincapié en el vector más obvio y éxito de los ataques, nosotros los usuarios. La ingeniería social y ataques de '*spear phishing'* (ataques diseñados para uno o varios usuarios específicamente) son cada vez más efectivos y populares. Así que la educación y el entrenamiento específico sobre estos riesgos a todos los miembros de la organización son cada vez más importante como un mecanismo defensivo clave. No se trata sólo de traer más tecnología y servidores de seguridad para la organización, sino que abarca los canales clave en las que los atacantes explotar, los eslabones más débiles... los seres humanos.

El último punto se refiere a un viejo refrán conocido: "no necesitamos ganar la carrera contra el oso en el bosque, siempre y cuando no seamos los más lentos será suficiente". Ahora tenemos tantos tipos y cantidad de 'osos' que ya no es suficiente salvarse una vez sino que hay que seguir corriendo contra los 'osos' (atacantes) y como enseñanza lo que funcionó ayer puede no ser suficiente mañana, y tal vez ni siquiera hoy.

- El siguiente aspecto cubrió el "cuando"; esto tiene dos premisas simples. Si no hemos comenzado ya, puede ser ya sea demasiado tarde. El segundo punto es sobre el cambio de enfoque de prevención y protección a:
    - CONTENCIÓN - ¿Con qué rapidez podemos "tirar del enchufe" y contener la situación y detener la fuga de información?
    - COMUNICACIÓN - Al igual que en un escenario de recuperación de desastres, las personas adecuadas interna y externas deben ser conscientes de sus responsabilidades y estar comprometidos para asegurar las decisiones y la acciones de una manera pronta y adecuada.
    - TRANSPARENCIA – Como ya fue expresado, ya no es una cuestión de 'si' voy a ser atacado, sino que el problema es 'cuando' se descubrirá que el ataque ya se efectuó y cuánto tiempo se necesita para que usted notifique a sus clientes y socios estratégicos. Incluso a veces a sus entes reguladores.
    - REACTIVIDAD - Al igual que en la etapa de Contención, operar en modo pánico reacción menos deseable. Reaccionar en orden y control no va a suceder por casualidad. Estar preparado y entrenarse para ello. Otra vez estar preparado para 'cuando' ocurra el ataque, no asumir que eso no va a pasar. Mejor preparación significa que es más probable que se podrá manejar mejor la situación.
    - PROACTIVIDAD - también vinculado con el punto anterior; no esperar para aprender de los errores propios solamente, hay que ser proactivo y aprender continuamente de la industria de la seguridad, integrar los controles que otros implementaron post ataques, aprender las técnicas de evasión más recientes utilizados por los piratas informáticos hábiles para irrumpir en los sistemas informáticos. Es probable que estos continúen con las mismas técnicas hasta que ya no les sean viables. ¿Por qué crear una nueva manera de acceder a un sistema cuando el modo conocido sigue siendo válido? Una vez más, el camino de menor resistencia y menor esfuerzo es una opción obvia. Ellos también son seres humanos después de todo. Por lo menos por ahora.
- El siguiente punto presentado cubre la acción final, el "por qué". Necesitamos actuar ahora porque a nadie le gustaría la idea de convertirse en una especie extintas que no pudo adaptarse. Las organizaciones se enfrentan al mismo reto en aumento de la

demanda de los clientes acerca de la apertura de múltiples canales para obtener los servicios, estos múltiples canales ahora llamado omni-canales. Los cuales una vez abiertos conllevan nuevos riesgos y nuevos vectores que estarán disponibles para los atacantes.

La presentación recordó un ejemplo acerca de los depredadores que una vez dominaron la Tierra, pero como la Tierra cambió y no pudieron adaptarse entonces dejaron de dominar y se extinguieron. Dudo que ninguna organización le gustaría ser comparada con estos dominantes seres pre-históricos y ser los fósiles de futuros libros sobre empresas fallidas que no pudieron adaptarse y desaparecieron.

- El aspecto final simplemente mostró el diagrama de una célula blanca, y los paralelismos que podemos encontrar en el cuerpo humano y su sistema de defensa para luchar contra el ambiente hostil en que vivimos. Esta fue la base de la idea de que vamos a tratar de elaborar. Una vez que la investigación comenzó el tema se expandió para identificar otras ciencias potenciales relacionados con el estudio de la naturaleza, los animales y la anatomía humana, la ciencia cognitiva, etc. Una vez más, el objetivo es sentar las bases y provocar una mayor inversión de tiempo y la investigación para aprender de nuestro alrededor para estar en una mejor posición para hacer frente a uno de los mayores retos para el futuro del mundo cibernético.

La presentación completa en ingles puede ser consultada en Appendix A.

ANALISIS DE LOS AVANCES EN LOS CAMPOS DE LAS CIENCIAS NATURALES Y APLICACIONES

La siguiente sección tratará de elaborar un breve análisis de las ciencias mencionadas y lo que podríamos considerar para generar una base de desarrollo de nuevas ideas que se aplicarían a la seguridad cibernética.

Microbiología:

Es el estudio de los organismos microscópicos, incluyendo a los unicelulares (unicelulares), los multicelulares (colonias de células), y los acelulares (que carece de células).

Esta sección cubre el análisis de cómo los micro-organismos interactúan con macro-organismos, como nosotros, para la reproducción y la supervivencia. Como los humanos han evolucionado para ser más resistentes, los micro-organismos han evolucionado por igual y en muchos casos son cada vez más resistentes a los métodos más antiguos para ayudar a los seres humanos para prevenir (vacunas) y de combatir (antibióticos) bacterias.

Un trabajo de investigación publicado[5] sobre cómo las estructuras macromoleculares atraviesan la capa de peptidoglicano, a pesar de no hacer una referencia directa a la seguridad cibernética, describe el rol de la capa de peptidoglicano para prevenir la lisis[6] celular que ayuda a mantener la forma celular y resistir las altas presiones internas de turgencia. Su integridad se mantiene cuidadosamente por la remodelación controlada durante el crecimiento y la división.

El diagrama en el reporte (fig.1) mostró cómo se coloca esta capa entre la capa interna y externa de una célula y que desempeña un papel clave para permitir la movilidad celular y secreciones (o tráfico) y esta capa intermedia (DMZ) es capaz de manejar eficientemente los canales de ensamblaje de entrada y salida para permitir que tales requerimientos celulares.

[5] Maintaining network security: how macromolecular structures cross the peptidoglycan layer - Edie M. Scheurwater & Lori L. Burrows Department of Biochemistry and Biomedical Sciences, Michael G. DeGroote Institute for Infectious Disease Research, Health Sciences Centre, McMaster University, Hamilton, ON, Canada – March 2011

[6] Lisis: Destrucción de una célula por rotura de la membrana celular.

La idea de que estoy tratando de representar apunta a una referencia o aprendizaje de este artículo sobre la necesidad de establecer un mecanismo entre las capas externas e internas (firewalls) para limitar aún más el tráfico que ocurren dentro de la zona de desmilitarizada. A pesar de algunos esfuerzos de configuración para incorporar herramientas de monitoreo de redes tales como los sistemas de detección y prevención de intrusiones (IDS e IPS respectivamente) estos no están realmente filtrando el tráfico efectivamente. En la mayoría de los casos se limitan a escuchar y alertar de cierto tipo de actividad pre-determinada y definida a través de reglas específicas de comportamiento, tal vez algunos sistemas más avanzados están ayudando a identificar un comportamiento inusual aplicando técnicas avanzadas de correlación de datos en tiempo real, pero no al mismo nivel de lo que la capa de peptidoglicano lo logra.

De alguna manera, esta capa celular representa la necesidad de avanzar en la seguridad de capa intermedia y probablemente resultará en la reducción de la confianza proporcionada por la capa media (DMZ), como lo representado por un estudio de la consultora Forrester sobre las redes de confianza nula[7]. Tambien en más tráfico restringido que sólo permita un tipo pre-definido de actividad; esto significa, que sólo abra un canal o conexión cuando las interacciones con las capas externas e internas lo requirieran. Esto puede conducir a la contención de los ataques que puedan penetrar la capa externa y que intentan moverse hacia los lados para poder elevar privilegios y controlar otros canales de acceso para penetrar la capa interna. Estos ataques intentaran considerarse un miembro de confianza. El atacante no puede tener la libertad para explorar la red o para llegar aún más en las redes internas donde los datos claves pueden residir.

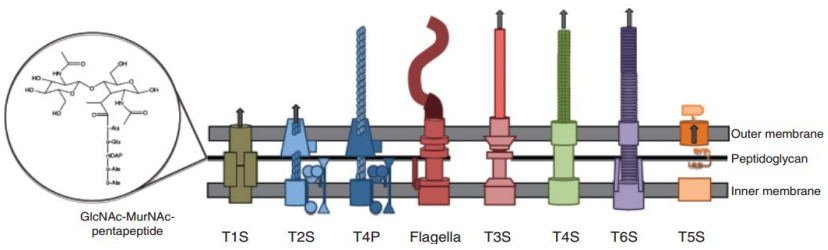


Fig.1

El conocimiento obtenido gracias a los estudios en este campo deben quizás ser la inspiración de una mejor seguridad del perímetro de la red. Como en este caso, organizaciones como las

[7] "Three technical innovations that will ignite Zero Trust [Networks] – Forrester report by John Kindervag and Andre Kindness – May 2015

células tienen que tener las interacciones de muchas maneras diferente y canales a la función diferentes necesidades, como también ocurre con los diferentes "canales" demostrada en el cuadro anterior (figura 1) donde cada uno tipo de interacción (T1S, T2S, etc.) tienen su función única, pero todos ellos siguen el mismo proceso de filtrado y siguen el mismo marco que se interactúa con el exterior. Contrariamente al caso de muchos negocios que usan múltiples canales para interactuar con sus clientes y socios usando marcos de referencia únicos que no son consistentes. El desarrollo de dichas soluciones únicas para cada canal crea discrepancias e ineficiencias que pueden conducir a la exposición a riesgos innecesarios para a la organización.

En conclusión, un marco de desarrollo consolidado para guiar y gobernar el despliegue de nuevos canales debe estar presente para asegurar que cada nuevo canal permita proteger los datos con los mejores mecanismos posibles y eficaces para proteger la integridad de su núcleo.

En conclusión, en cuanto a la microbiología, la lección a tener en cuenta reside en observar cómo las células han evolucionado para estar altamente interconectadas y a la vez hacerlo eficientemente dentro de un entorno hostil y agresivo.

Inmunología:

En mi opinión, la investigación relacionada a los conceptos de inmunología aplicada a la seguridad informática es el más avanzada en comparación a las demás ciencias aquí referenciadas.
La referencia más obvia comenzó con el muy conocido nombre que fue asignado al código malicioso: “virus” o “virus informático”. Desde el descubrimiento de los primeros “virus” a principios de los años 80 y la posterior explosión del Internet en los años 90, hicieron que la distribución de virus informático fuera más rápida y más amplia, entonces fue obvio que las primeras defensas fueran llamadas “anti-virus”.

Muchas compañías de seguridad de software fueron construidos en estas bases como los casos de McAfee (1987), F-Prot (1989), Norton (Symantec, 1990) y Kaspersky (1997).

Sin embargo, la intención de esta sección no es elaborar sobre este tema virus y anti-virus que es bien conocida y un control mínimo básico que ya está arraigado a la mayoría de los usuarios del Internet.

El objetivo principal es desarrollar sobre uno de las primeros documentos de la investigación que he encontré cuando se estaba investigando para la presentación en la Conferencia de Riesgos de TI para principios de este año. El documento al que yo me refiero es "Datos sensibles en un mundo intercomunicado - Representaciones negativos de Datos" (en Ingles “Sensitive Data in a Wired World - Negative Representations of Data”), de Stephanie Forrest, de la Universidad de Nuevo México, 2000.

Hay todo un campo de la ciencia que se basa en esta área conocida como la inmunología computacional. Esto, según Wikipedia, es *un campo de la ciencia que abarca genómica de alto rendimiento y la bioinformática enfoques de la inmunología. El principal objetivo del campo es convertir los datos inmunológicos en problemas de cálculo, resolver estos problemas utilizando métodos matemáticos y computacionales y luego convertir estos resultados en interpretaciones inmunológicamente significativas.*

Volviendo al reporte de Forrester, hay 4 aspectos clave del diseño en todos los seres vivos que basa su análisis en:

- Supervivencia y adaptabilidad evolutiva
- Autonomía
- Robustez, adaptación y auto-reparación
- Diversidad

Ella promovió la aplicación de propiedades del sistema inmune a las propiedades computacionales de:

- Detección de intrusiones
- Respuesta Automatizada
- Filtrado de información colaborativa

Una vez más, este tema por sí mismo es también una ciencia campo bastante grande y complejo que no tengo la intención de expandir o contradecir. Sin embargo, veo un aspecto que se menciona pero no esta tan obviamente representaba.

El punto clave que quería destacar de esto son los aspectos que se elaboran como propiedades de los seres vivos. En particular a la capacidad evolutiva (en ingles “evolvability”) de los seres vivos para adaptarse a entornos cambiantes. Este es claramente el fundamento de los estudios del cuerpo humano en su lucha contra los microorganismos como virus, bacteria, parásitos, etc.. Estos también comparten las mismas propiedades de capacidad evolutiva que les permite sobrevivir incluso en el más hostil de los ambientes. Es por esto que la lucha nunca terminará.

En el sentido de la aplicación a la seguridad informática, el tema presenta dos retos: el primero es que los marcos establecidos para el diseño de sistemas informáticos no están ni siquiera cerca de guiar a los ingenieros de software para desarrollar nuevas aplicaciones y sistemas a seguir los mismos 4 principios de la seres vivos. En general, los sistemas no se construyen a la “auto-evolución” o “auto-reparación”, no pueden ser “autónomos”, pero si podrán ser construidos para ser “diversos” como algunos de ellos están construidos para ser portátiles y multi-plataformas. Hoy en día, el problema se acaba empeorando en este frente como los nuevos sistemas de más crecimiento y demanda se basan en aplicaciones móviles. Muy fáciles de construir, con los ciclos de desarrollo ágiles que proporcionan respuesta

rápida en iteraciones para permitir nuevas características y capacidades que se desplegarán en días en comparación con semanas o meses que solían tomar las aplicaciones tradicionales. ¿Qué pasa con la seguridad entonces? Por ejemplos que hemos visto recientemente, seguridad por diseño no es la norma, sino la excepción.

Así crece la necesidad de moverse y enfocar la atención a las herramientas disponible para proteger tales ecosistema de aplicaciones que controlan la información. Si nos referimos a las herramientas como antivirus, firewalls, detección de intrusos y protección, seguramente estos conceptos se aplican a este. En mi opinión, lamentablemente no es el caso.

En el caso obvio de los anti-virus ya fueron construidos sobre el concepto y supuestos de que hasta que se descargue la actualización específica (o 'signature hash' en ingles), entonces no podríamos detectar un virus. Incluso la intención de que comenzaron a observarse en la década de 2000, que la incorporación de la heurística[8]. Estos esfuerzos, en principio tiene mucho sentido, fueron pobremente implementados resultando en una gran cantidad de falsos positivos e incluso archivos auténticos válidos movidos a cuarentena haciendo que el sistema operativo falle como consecuencia de esto. Esto llevo a que la mayoría de las organizaciones comenzaran a desactivar esta función y dejar el escaneo para ejecutar la detección basada en firmas solamente. Obviamente, la limitación es que todo lo demás no lo ha detectado permanecería sin ser detectados hasta que se capture el código malicioso, la firma se identifique, la firma añada a la base de datos y que está disponible para el programa agente del anti-virus lo pueda bajar de la base de datos central. Esto en muchos casos no está sucediendo en tiempo real y los 'exploits' de día cero puede estar explotados o aprovechado por atacantes por semanas o meses.

No tengo la intención de continuar elaborando sobre de las deficiencias y limitaciones de las soluciones anti-virus ya que esto puede no vale más discusión como los líderes en este campo no han demostrado esfuerzos significativos para proporcionar una mejor solución.

[8] Muchos programas antivirus utilizan reglas heurísticas para detectar virus y otras formas de malware. Exploración heurística busca de código y/o patrones de comportamiento indicativos de una clase o familia de virus, con diferentes conjuntos de reglas para diferentes virus. Si se observa un proceso de archivo o ejecutar para contener patrones de código a juego y / o que se realiza ese conjunto de actividades, entonces el escáner infiere que el archivo está infectado. La parte más avanzada de exploración heurística basada en el comportamiento es que se puede trabajar en contra de virus polimórficos altamente aleatorios, que la cadena simple escaneo de sólo enfoques no puede detectar de forma fiable. Análisis heurístico tiene el potencial de detectar muchos virus futuras sin necesidad de que el virus se puede detectar en alguna parte, presentada al desarrollador escáner de virus, analizada, y una actualización de detección para el escáner suministra a los usuarios del escáner.

Volviendo al trabajo de Forrest, hay una compilación más elaborada sobre tema que ella introduce y la comparación con las demás ciencias por un grupo de investigadores en el Reino Unido[9], que utilizó sus referencias de selección negativa para las aplicaciones específicas para el desarrollo de sistemas de detección de intrusiones. En este trabajo se presentan el tema más simplificadamente que lo hace más fácil de interpretar. Podría resumir los puntos más relevantes para este estudio de la siguiente manera:

- El algoritmo de selección negativa trata de imitar el sistema inmune humano (SIH) aplicando el método de detección de anomalías.
- Esto significa que el SIH está diseñado para ser capaz de detectar y distinguir de las células legítimas (propias), células dañinas ya previamente identificadas como dañinas (basada en firma única) y también las que no se conocen (no propias).
- La aplicación de estos tres elementos (propio, no propios y basado en firmas únicas) permite que los algoritmos combinados puedan resultar en una reducción significativa de los falsos positivos y aumentan la detección de conductas inusuales y no autorizadas.

Es muy interesante leer el trabajo de investigación que desarrolló este tema específicamente para el diseño de soluciones para de la detección de intrusos y seguridad informática de Steven Andrew Hofmeyr[10]. Aunque sólo se hace referencia al análisis de la selección negativa como la clave para el desarrollo de soluciones de seguridad esto está estrechamente relacionado con el otro trabajo del equipo de investigadores del Reino Unido previamente mencionado. Este reporte proporciona un enfoque más holístico hacia otros algoritmos y los compara para una vista combinada y equilibrada de los otros aspectos del SIH respecto a la protección del cuerpo humano.

En conclusión, este tipo de trabajos tendría que mantener la inversión y financiación para mejorar aún más la comprensión de la forma en que el cuerpo humano reacciona a los organismos externos y los combate de manera eficiente.

[9] Immune System Approaches to Intrusion Detection - A Review by Jungwon Kim, Peter J. Bentley , Uwe Aickelin, Julie Greensmith, Gianni Tedesco and Jamie Twycross – January 2007
[10] An Immunological Model of Distributed Detection and Its Application to Computer Security, Steven Andrew Hofmeyr, University of New Mexico, May 1999

Creo firmemente que los mayores esfuerzos estarán altamente dependientes de cómo las anomalías del SIH pueden afectar a la comprensión de la selección negativa, específicamente me refiero a los cambios genéticos que desencadenan en ciertos individuos para desarrollar enfermedades autoinmunes que pueden, en algunos casos, llevar hasta la muerte. No voy a profundizar en esta área de enfermedades autoinmunes como yo todavía no veo el claro progreso hacia revertir los factores desencadenantes que impulsan estos cambio genéticos para generarse en el primer lugar. De acuerdo con las discusiones que tuve con un especialista de enfermedades dermatológicas autoinmunes el año pasado, menciono en su trabajo de investigación que estadísticamente el desencadenante por las enfermedades autoinmunes que se manifiestan son causadas por origen genético 75% y el resto por factores ambientales. Por lo tanto, la necesidad de ver más progresos en el campo de la investigación genética y sus anomalías son fundamentales para continuar progresando en el campo de la seguridad informática aplicada. Eso probablemente tenga que combinar ambos campos de la ciencia para conseguir una versión revisada y reducir significativamente la probabilidad de falsos positivos.

Ciencia Cognitiva:

Sobre este tema me gustaría ampliar un poco más que en las otras ciencias.

De acuerdo con la definición anterior, hay ciertos retos que aún se tienen que develar sobre la comprensión de la mente humana. Estos pueden desencadenar incluso el pensamiento más profundo sobre cómo funciona. Posteriormente podríamos aprender más rápido y hasta podríamos intentar imitarla y copiarla mejor en la eventual creación de una real inteligencia artificial.

Una de las características del desafío es representar de forma racional el libre albedrio. Esta capacidad humana que nos diferencia del reino animal. También será siempre un debate sobre enfrentar las eventuales elecciones de máquinas inteligentes sobre si los humanos seguirán mereciendo ser los "amos" de este planeta.

De todos modos, ese debate puede merecer y colección completa de libros.

Volviendo a la aplicación más realista de la actual comprensión de la conducta humana; el ejemplo perfecto, en mi opinión, es aplicable al los trabajos de redes de análisis de comportamiento y al reconocimiento de patrones. En principio, estos dos conceptos se basan en la aplicación relativamente “sencilla” de cómo los seres humanos pueden reconocer rápidamente una situación, un rostro, un lugar, etc.

El primer aspecto de análisis de comportamiento se basa simplemente en los estudios de cómo los humanos han sido intrínsecamente grabados en las actividades diarias como "esclavos de rutinas". Estas son aprendidas desde desarrollo temprano del cerebro, estas son las reglas de convivencia en sociedad. Estas obviamente varían de acuerdo a las épocas, culturas y regiones. Desde que los humanos han comenzado a vivir en comunidades o grupos, el desarrollo de rutinas o patrones están presentes. El primer ejemplo obvio es el lenguaje y el habla. Un conjunto de sonidos acordados teniendo en cuenta que articula y expresa en una secuencia predefinida puede ser interpretada por un individuo que fue enseñado los mismos sonidos desde su desarrollo temprano.

En la investigación sobre el Análisis Experimental del Comportamiento[11], y sobre Las dificultades de normalización de tareas en un Grupo Experimental Objetivo de seguimiento[12], hay una clara distinción entre los humanos y los no humanos en cuanto al algoritmo utilizado para representar el comportamiento repetido que los seres humanos tienden a desarrollar un nivel más alto de la varianza. En su opinión, esto se puede explicar por la sencilla razón de la elección humana. El impulso instintivo de los animales es más anticipable y se puede predecir con mayor precisión. Esto incluso toma en cuenta la edad y las experiencias que cada animal puede haber tenido que reducir aún más la variación de la conducta.

El algoritmo para una medida comúnmente utilizada de elección, la sensibilidad al refuerzo de la ley de la igualación generalizada (GML; Baum, 1974), ha sido el comportamiento humano y no humano:

$$\boldsymbol{log\left(\frac{B1}{B2}\right) = a log\left(\frac{R1}{R2}\right) + log c}$$

… donde *Bi* se refiere al número de respuestas a *i* alternativa, *Ri* y al número de refuerzos obtenidos en Alternativa *i*. Usando una regresión lineal, los parámetros *a* y logaritmo de *c* son estimados. El parámetro *a* es la sensibilidad al refuerzo y mide el cambio en las proporciones de respuesta resultantes de un cambio en las proporciones reforzador. El logaritmo de *c* es el sesgo inherente, y mide cualquier preferencia proporcional constante por una alternativa sobre la otra.

La razón por la que quería citar este análisis y el experimento se basa en el caso de que hay fuerzas, más allá de la fácil comprensión que nos limita a que reaccionemos rápidamente a acciones inusuales y no experimentadas. El aprendizaje eventualmente desarrollar una reacción más cercana y la acción al grupo de personas que ya han aprendido. Los aspectos claves para aprender de esto es que sabemos algo acerca de cómo los seres humanos se comportan, esto se relaciona con el funcionamiento del cerebro. La reacción del cerebro por defecto a un evento es el primero en identificar si esa situación o acontecimiento se ha producido ya, si es así, a continuación identifica si el resultado fue positivo, entonces traerá el

[11] Research in the Experimental Analysis of Behavior (Herrnstein, 1961, 1970; Davison & McCarthy, 1988)

[12] Standardizing task difficulty in an experimental target-tracking task: a comparison of five types of computer input devices. By Christian U. Krägeloh, Daniel Shepherd, Alvin E. Zapanta, & Jason Landon
Auckland University of Technology, 2013

conjunto de acciones para activar las mismas acciones para intentar obtener el mismo resultado positivo. Si no, entonces el cerebro intentará recordar eventos menos similares y conducir los comportamientos para interactuar con el evento enfrentado. Esto entonces conducir hacia el nuevo aprendizaje.

La aplicación de este conocimiento a la finalidad de este trabajo reside el reconocimiento de nuestra previsibilidad humana a las reacciones a la conducta repetida y la posibilidad de convertir este comportamiento predecible en nuestro favor. Esto significa intentar aplicar la información conocida de ciertos nuevos comportamientos para distinguirlo de los comportamientos pre-aprendidos y esperados y lograr establecer el camino más eficaz para desarrollar capacidades de alertas tempranas.

Esto está estrechamente vinculado al siguiente aspecto que me gustaría elaborar dentro de la ciencia cognitiva y que es el de reconocimiento de patrones.

En esta segunda área se han efectuado muchos más avances y aplicaciones. Los más conocidos están relacionados con el reconocimiento de la voz, la retina, las huellas digitales, el rostro y hasta de gestos. Estos pueden ser capturados digitalmente (o analógicamente) y simplemente compararlos con información almacenada como un mecanismo de autenticación multi-biométrica.

En los casos de reconocimiento de patrones la investigación es mucho más adelantada que otros campos y probablemente va a continuar avanzando a un paso acelerado hacia una mejor precisión para sus aplicativos. Esto eventualmente llevará a una dependencia más alta para los mecanismos de autenticación como la sustitución total de los controles obsoletos o menos fiables. Uno de los mejores ejemplos recientes es la adopción masiva del pago biométrico por la detección de huella digital móvil… más conocido como Apple Pay.

Simplemente por la consistencia de la información de la investigación citando algunas de las futuras aplicaciones de patrón reconocimientos pueden ser referidos a la obra presentada por la Publicación de Cartas de Reconocimiento de Patrones (Conocida en inglés como: *Pattern Recognition Letters Journal*). Hay varios esfuerzos paralelos con respecto al análisis de datos. En particular, noté algunos de los artículos que se refieren al análisis de imágenes cerebrales e imágenes de resonancia magnética cerebral para reconocer y detectar patrones de imágenes

precozmente a posibles tumores que análisis a simple vista era imposibles de detectar. Estos permiten iniciar un diagnóstico temprano incrementando la probabilidad de tratamiento efectivo y potencial recuperación.

Sin embargo, la aplicación que en particular quería referirme es muy utilizado en aplicaciones comerciales recientes y ya han demostrado ser muy útiles. El problema es que requiere un alto nivel de personalización y carece de las capacidades de auto-aprendizaje que son clave para un modelo eficaz, que en este caso puede estar vinculado a un ataque cibernético.

En conclusión, hay varios aspectos del cerebro humano que han intentado interpretar y comprender y luego a reproducirse (matemáticamente). En este caso presentamos brevemente dos aspectos, los comportamientos y patrones que están vinculados y relacionados. Todavía no sabemos mucho acerca de cómo los seres humanos rápidamente son capaces de identificar los aspectos o características de un conjunto de gestos o características más distinguidas y determinar y una vez identificado desencadenar la liberación de un gran conjunto de datos (memorias) relacionado con que las personas, las situaciones, lugares u objetos. Todo esto dentro de la combinación de 5 entradas sensoriales (vista, olfato, tacto, olfato, audición); excluyendo arbitrariamente miles de los conjuntos de sub-datos que vienen a través de nuestro centro de procesamiento central (cerebro) en paralelo y con la capacidad de almacenarlos parcialmente y aun así recuperarlos con la ayuda de las herramientas y técnicas adecuadas. Ni siquiera voy a mencionar el potencial de desencadenar los recuerdos a través de la hipnosis o también de las técnicas de visualización (método conocido como Ioci[13]).

En el caso específico de la seguridad cibernética, en mi opinión y en base a lo expresado anteriormente, estipulo que los atacantes son más propensos a seguir patrones similares de comportamiento tanto y en cuanto estos patrones de comportamiento (técnicas de ataques) que hayan sido y continúen siendo métodos eficaces y eficientes para penetrar una red informática. Simplemente, ¿por qué iban a tratar de descubrir una nueva manera de irrumpir una red informática cuando el método ya utilizado todavía funciona y sigue sin ser detectado? Es por eso que si entendemos que podemos simplificar estos comportamientos a un conjunto de comandos o acciones dadas entonces podemos tener una manera única para alertarnos

[13] Ioci Method: Es un método de mejora de la memoria que utiliza la visualización para organizar y recordar información. Esta técnica se utiliza, entre otras cosas, para recuperar caras, dígitos y listas de palabras.

cuando puede haber un ataque. Las técnicas de reconocimiento de patrones pueden ser la base para esto ya que los avances en este campo han demostrado que ya algunos equipos que están combinando las técnicas de reconocimiento y que analizan la información en tiempo real imitando la forma en que el cerebro humano lo hace.

Para representar a mi proceso de pensamiento propongo un ejemplo de lo que estoy tratando de representar, voy a tratar de resumir el descubrimiento y el ataque de lo que un ser humano puede estar haciendo para identificar gran cantidad de datos e investigar un atacante potencial y distinguirlo de actividad autorizada.

Referirse al Apéndice 2 para una descripción paso a paso del ejemplo de una investigación ejemplo y lo que podría implementarse basado en las herramientas de reporte y monitoreo ya existentes.

El ejemplo refueza la comparación que debemos tener en cuenta para la creación de soluciones sostenibles, de fuentes múltiples que se requieren de medios idealmente independientes (como los 5 sentidos humanos); esto tiene que suceder en tiempo real, no al día siguiente, y los patrones predefinidos (memoria) deben establecerse para detectar temprano lo más probable lo que serán los componentes, comportamientos y patrones de un ataque en proceso. Como consecuencia poder iniciar las medidas de defensa requeridas cuasi-instantáneamente.

Biología evolutiva:

En lo que respecta a este campo de la ciencia sólo me referiré brevemente a esta area como el conductor para determinar la necesidad de, una vez más, repensar la forma en que construimos y defendemos sistemas y aplicaciones informáticas.

Conceptualmente, voy a citar brevemente a Charles Darwin y su libro "*Sobre el origen de las especies por medio de la selección natural"*, para explicar mi punto de que hasta que la construcción de ágil, evolutiva y adaptable del desarrollo de software sea plenamente establecida para la seguridad informática, los niveles de eficacia y eficiencia serán reducidos y, eventualmente serán sistemas obsoletos.

No estoy infiriendo que los atacantes son la "especie" que por la selección natural va a sobrevivir. Mi mención de este campo es que los conceptos evolutivos de adaptación aplican a los nuevos, versátiles, rápidos, ingeniosos, inteligentes y audaces atacantes. Como lo mencionado en la introducción, los atacantes ya no son individuos solitarios, la diversidad de los atacantes nos hace pensar que ya no hay suposiciones válidas y que un enfoque único y simplista no es suficiente.

El desinterés histórico a nivel de la Gerencia sobre estas preocupaciones será crucial a la "selección natural" de la organizaciones que simplemente no serán capaces de hacer frente a la mayor tasa de éxito que los atacantes están recibiendo. Pero es importante destacar que eso es lo que sabemos por las capacidades existentes de detectar distintos tipo de ataques. Sin embargo, estoy seguro de que no sabemos acerca de muchos otros métodos y tácticas que están en uso este mismo momento sin haber sido descubiertas.

Como tal la necesidad conceptual de considerar una mirada más cercana al aspecto de cómo la vida han evolucionado en la Tierra para transmitir el mensaje con claridad. Si las organizaciones no evolucionan y se adaptan al entorno siempre cambiante entonces van a extinguirse.

Elaboré brevemente este ejemplo en mi presentación en el Apéndice 1 al final de la misma cuando me refería a los ejemplos de los antiguos gigantes que dominaron los miles de años de la Tierra.

Especies fueron incapaces de evolucionar. Cité el caso de los mamuts lanudos. Originalmente, estos se creían que habían sido extinguidos por causa de los seres humanos que los cazaban. Sin embargo, un estudio más reciente[14] sugirió que el mamut lanudo se extinguió principalmente por su inhabilidad de adaptarse al cambio climático.

Cité el caso de la gigante cadena de tiendas estadounidense Target y el ataque cibernetico en noviembre de 2013. El caso llamó la atención de la prensa ya que los datos de pago de más de 110 millones de clientes fueron comprometidos. La sorpresa no es eso, es que como resultado de este incidente no sólo el Gerente de Sistemas (CIO), sino también el director general (CEO) perdieron sus puestos de trabajo. Podría no haber sido el primero, pero sin duda establece un gran precedente y llevo a que numerosas Juntas de Directores y Gerencias comenzaran a prestar más atención a las amenazas cibernéticas.

Con el tiempo, esto se puede convertir en una norma y no van a ser grandes noticias, sin embargo a pesar de los aumentos de presupuesto en seguridad cibernética, hay una evidente falta de compromiso y colaboración en y entre todos los sectores. Todavía no están totalmente concientizadas que pueden aproximarse a un punto de inflexión y comenzar a decir: "Yo no quiero extinguirme".

[14] Holarctic genetic structure and range dynamics in the woolly mammoth, by Eleftheria Palkopoulou, Love Dalén, Adrian M. Lister, Sergey Vartanyan, Mikhail Sablin, Andrei Sher, Veronica Nyström Edmark, Mikael D. Brandström, Mietje Germonpré, Ian Barnes, Jessica A. Thomas, September 2013, Royal Society publishing

CONCLUSION

Se hizo evidente para mí en los últimos 18 años trabajando en los campos de la tecnología de riesgos, seguridad informática y auditoría que las organizaciones aún no están preparadas o bien equipados para apoyar de manera efectiva contra la lucha a las amenazas cibernéticas. Las experiencias de trabajo en varios países, varias industrias, en organizaciones pequeñas y multinacionales, las cuestiones de seguridad cibernética tienden a ser las mismas. Departamentos de seguridad de la información no tienen los conocimientos especializados, los recursos y el tiempo para hacer frente a los riesgos existentes y emergentes para luchar eficazmente contra las amenazas cibernéticas.

El compromiso de la alta dirección, a pesar de haber una mejora significativa, no ha sido el que se necesita para cambiar la dirección de esta desafortunada tendencia.

Los atacantes son cada vez más capaces de aprovechar esta situación y están teniendo una mayor tasa de éxito.

Necesitamos algo radical, aunque no necesariamente nuevo, para poner adelante una base para nuevas estrategias, fuerzas conjuntas, multi-industrias, multi-disciplinaria y colaborando, compartiendo y aprendiendo juntos, no como unidades individuales. Eso fue lo que inspiró el pensamiento detrás de este trabajo. La naturaleza no trabaja sola. Es en los ecosistemas naturales que requiere a todos sus componentes cumplir con su rol para la supervivencia, no para uno o más de sus miembros, para todo el ecosistema.

Entonces, miré más de cerca y noté el mismo patrón en los seres vivos. Todas las partes del cuerpo juegan un papel, y no puede ser simplemente considerarse no importantes.

Entonces comencé a ver que la mayoría de las otras ciencias relacionadas con el estudio de los seres vivos han hecho progresos significativos hacia la comprensión de la función y el propósito de este tipo de cosas. Me di cuenta de que las ciencias ya necesitan para transformar ese conocimiento en los conjuntos de datos y de interpretar y reproducir ese conjunto de datos, los investigadores empiezan a crear algoritmos.

Entonces estos algoritmos, si se entienden y se aplican a los efectos de la seguridad informática servirán como la base para construir un marco de trabajo más sostenible,

sustentable y adaptable de herramientas de seguridad de última generación. Esto asegurará la supervivencia contra la batalla que se están perdiendo contra las amenazas cibernéticas.

Concluyo con un llamamiento a los investigadores y expertos en ciencias para comenzar a traer esas experiencias juntas, y de nuevo, no de manera aislada. Las experiencias y los esfuerzos, si no se comparten a través de otros campos no pueden ser totalmente aprovechados y su beneficio no será maximizado.

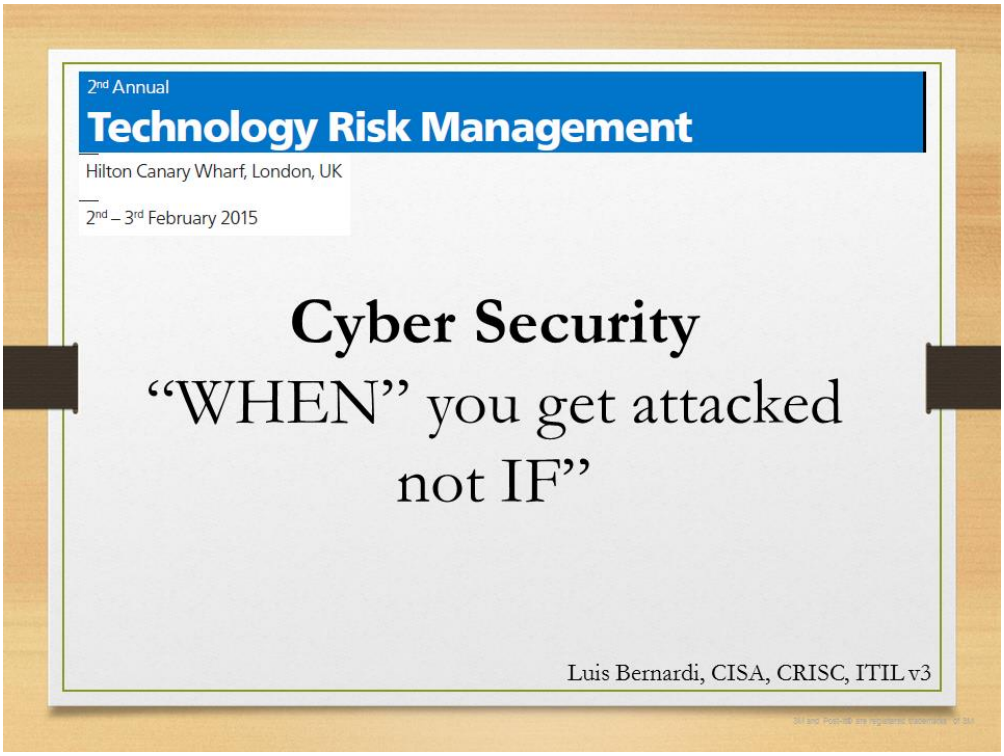
Con todo, la batalla puede ser más justa si las herramientas y los recursos de los dos, atacantes y defensores se distribuyen con más igualdad. Los esfuerzos conjuntos serán más que suma de los recursos individuales. Los esfuerzos y recursos sobrepasaran a los disponible para los atacantes; se verán forzados a invertir más y el costo más alto para ellos los hará posiblemente re-pensar sus objetivos. La guerra está lejos de terminar, pero sin duda hay muchas áreas en las que podemos estar mejor. Creo sinceramente que el aprendizaje conjunto a través de las ciencias y el fomento del intercambio multidisciplinario es el camino.

Unidos somos más.

APPENDIX

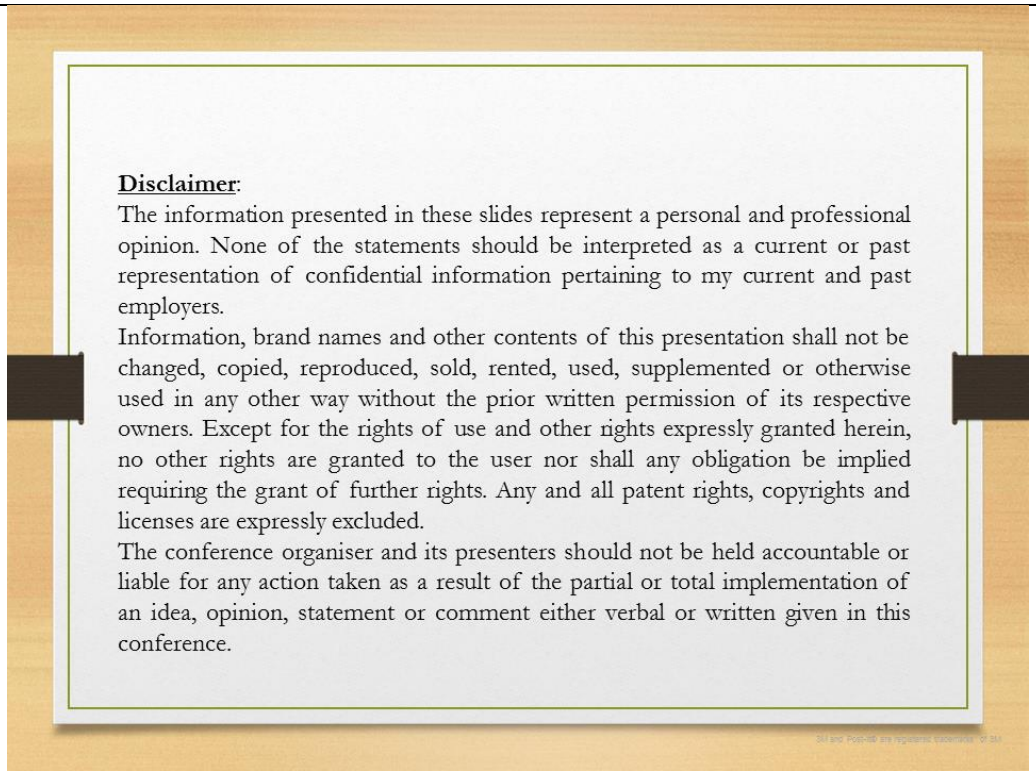
Appendix A

Presentación en el IT Risk Management – Marcus Evans Conference, Londres, Reino Unido en Febrero 2015



Seguridad Cibernetica

"Cuando" sera atacado, no "si"



La información presentada en este documento representa una opinión personal y profesional. Ninguno de los conceptos presentadas deberán será interpretados como una representación de información confidencial de mis presentes y pasados empleadores.

La información, marcas, nombres y otros contenidos de esta presentación no deben ser cambiadas, copiadas, reproducidas, vendidas, alquiladas, usadas, suplantadas o de alguna otra manera sin el previo permiso escrito de sus respectivos dueños intelectuales. Excepto por los derechos de uso y otros derechos expresamente otorgados, ningunos otros derechos serán otorgados tampoco alguna obligación implícita requiriendo el otorgamiento de otros derechos. Todos los derechos de patentes y derechos de marcas y licencias están expresamente excluidos.

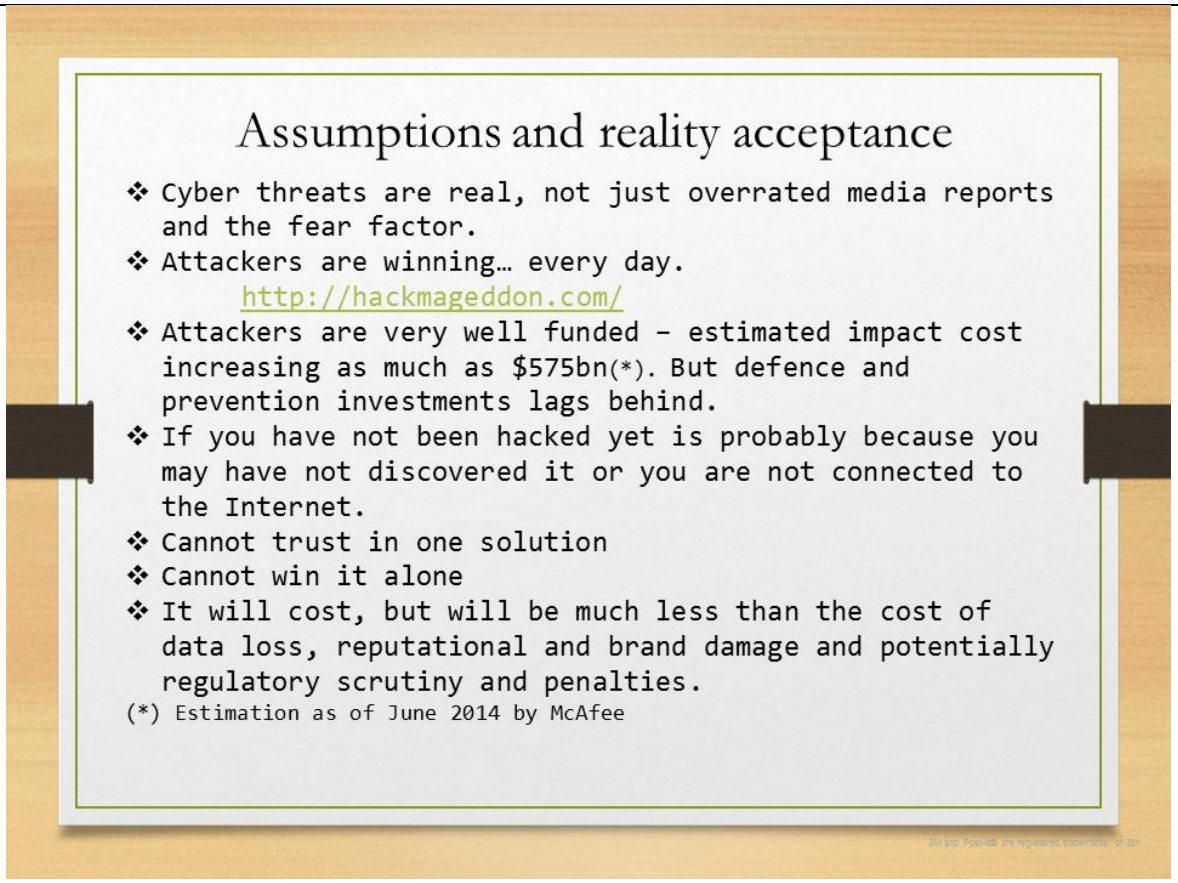
Los organizadores de esta conferencia y sus presentadores no serán responsables o imputables por ninguna acción como resultado de ninguna idea, comentario, opinión parcial o total sea verbal o escrito en esta conferencia.

Las predicciones de amenazas a la seguridad informática

Las predicciones son inconsistentes

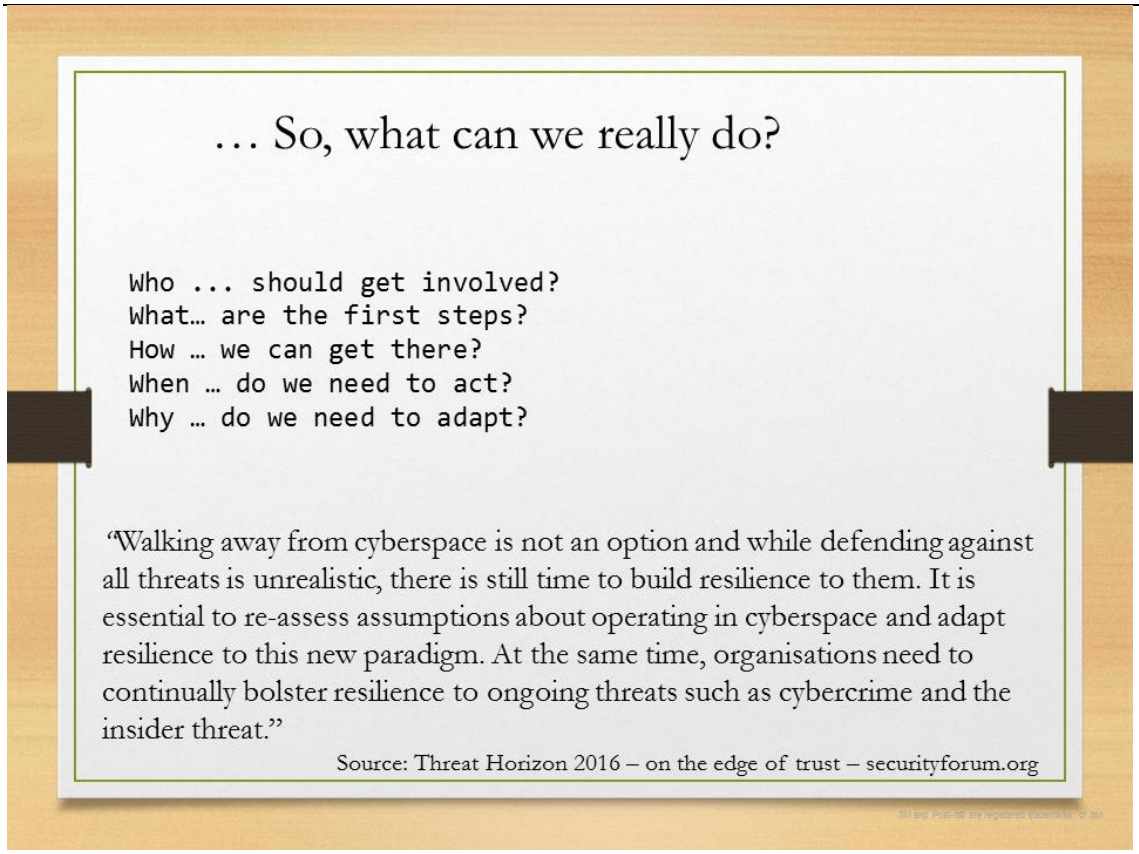
¿Entonces que se puede hacer?

¿Como podemos estar preparado para todas las amenazas?



Suposiciones y aceptación de la realidad

- Las amenazas cibernéticas son reales, no solo reportes de la prensa amarilla que apelan al factor miedo.
- Los atacantes están ganando, cada dia… hackmageddon.com
- Los atacantes están muy bien financiados y motivados – se estiman incrementales costos de impacto de USD575.000 millones. La defensa y prevención están aumentando pero a un paso más lento.
- Si ya ha sido aún “hackeado” es probable que no lo haya descubierto o simplemente no esté conectado al Internet.
- No se puede confiar en una única solución.
- No se puede ganar solo.
- Ganar costara, pero será mucho menos costoso que la perdida de datos vitales para su organización, el costo reputacional, el daño de su imagen y marca, y potenciales multas y restricciones impuestas por entes reguladores.



…. Entonces que se puede hacer?

¿Quién… deberá envolverse e involucrarse?

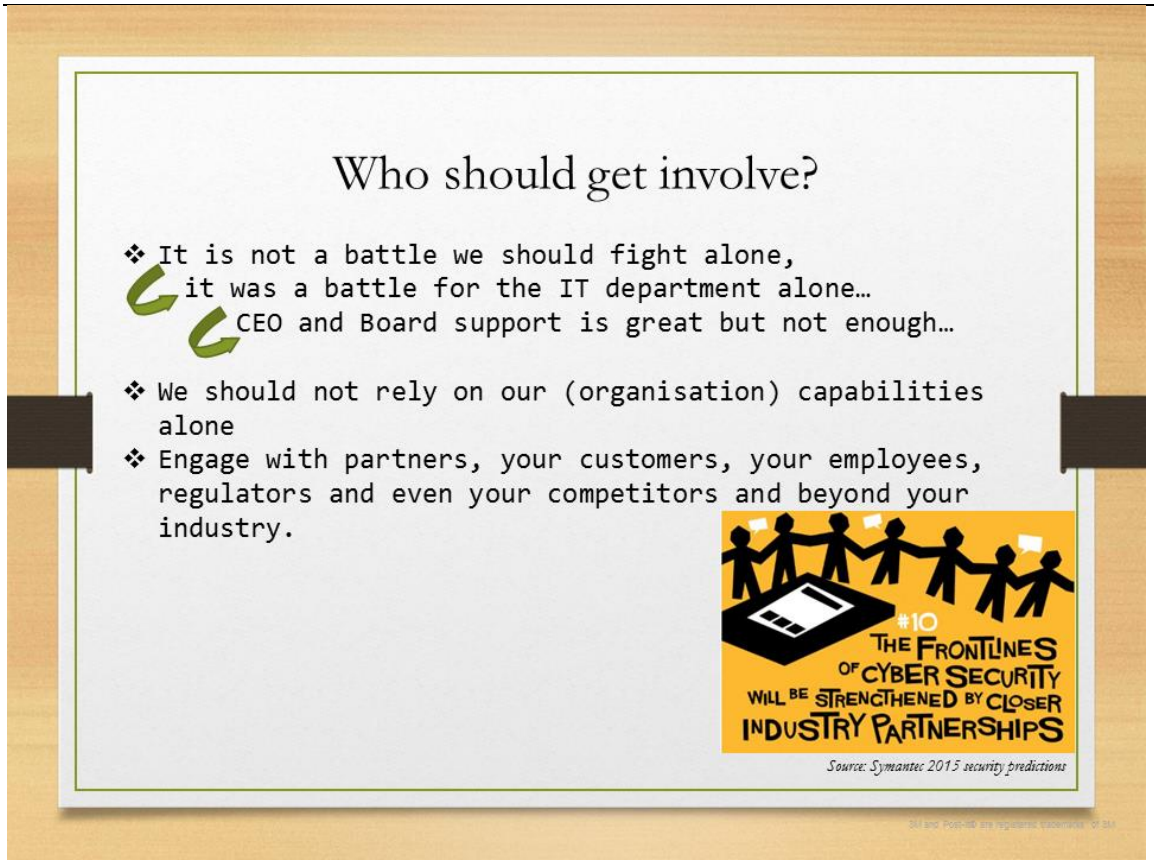
¿Cuáles… serán los primeros pasos?

¿Cómo… se puede llegar al objetivo deseado?

¿Cuándo… se debería actuar?

¿Por qué… debemos adaptarnos?

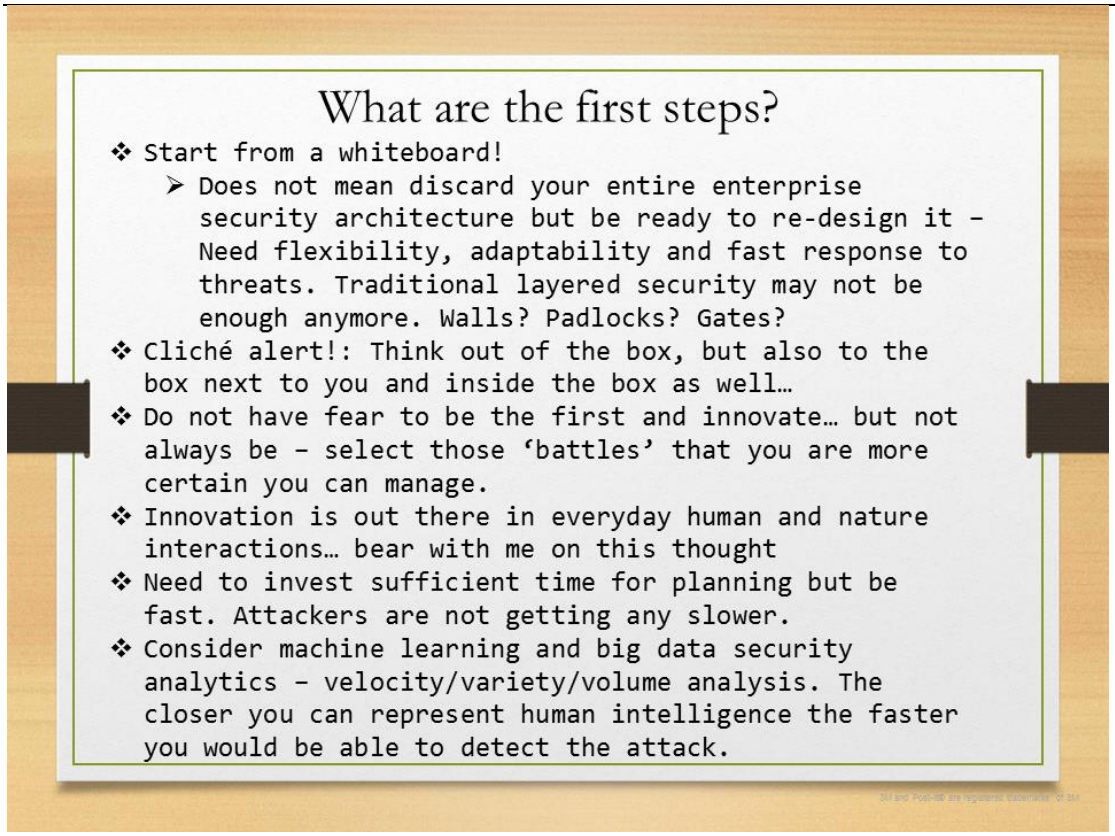
"Escaparse del ciberespacio no es una opción y a la vez de defenderse de todas las amenazas es irrealista, todavía queda tiempo para construir una barrera o resistencia a esas amenazas. Es esencial de re-analizar las suposiciones de operar en el espacio cibernético y adaptase a ser resistente a este nuevo paradigma. Al mismo tiempo, las organizaciones necesitan constantemente adaptarse para mejorar las defensas a las amenazas cambiantes del crimen cibernético y la amenaza interna."



¿Quién deberá involucrase?

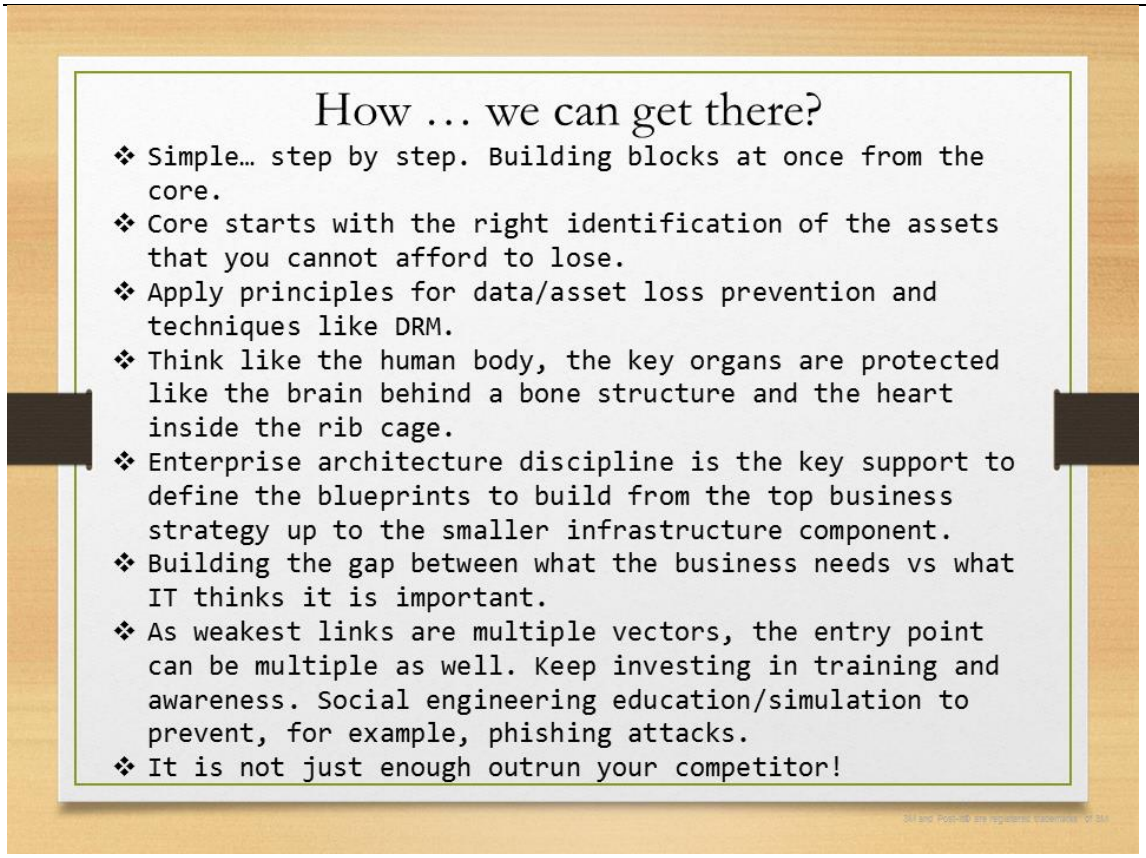
- No es una batalla que se debe pelear solo, era una batalla del departamento de tecnología solamente, donde solo recientemente la alta gerencia está empezando a apoyar, aunque no es suficiente.
- No debemos confiar solamente en las capacidades internas de nuestra organización.
- Debemos conectarnos con socios, clientes, empleados, reguladores, e incluso sus competidores incluyendo organizaciones de otras industrias.

Symantec 2015 predicciones de seguridad #10: “Las fronteras de la seguridad cibernética serán estrechamente establecidas por asociaciones entre industrias.”



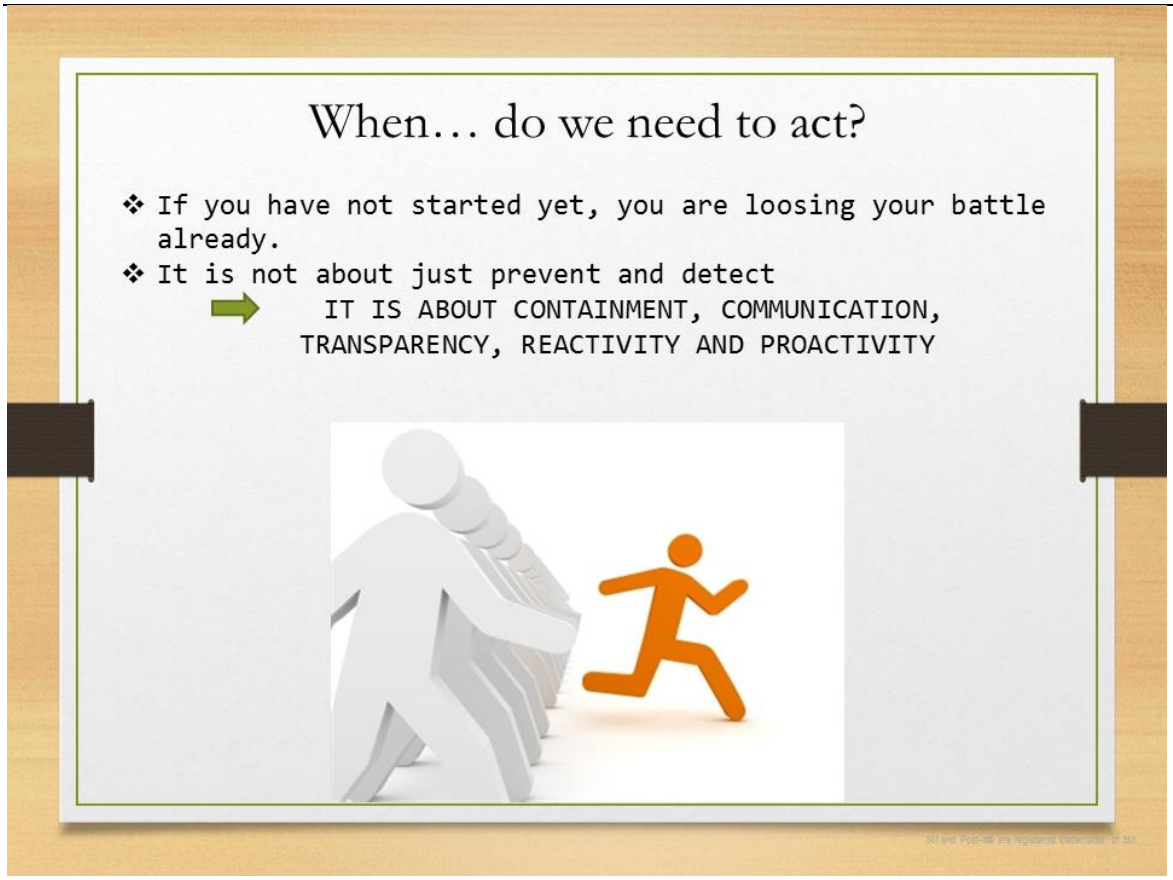
¿Cuáles son los primeros pasos?

- Comenzar desde una página en blanco
    - Esto no significa descartar la entera arquitectura empresarial pero deberemos estar listos a rediseñarla. Se necesita flexibilidad, adaptabilidad y rápida respuesta a las amenazas. La seguridad de capas ya no es suficiente.
- Hay que intentar "ver abajo del agua" o tal vez "sobre el agua" y "encima del agua". Hay que ver en todas direcciones.
- No teman a ser el primero e innovar, pero sea selectivo y no tome la primera idea que le caiga si no está preparado a manejar resultados inesperados.
- La innovación está a nuestro alrededor, en cada humano y naturaleza.
- Necesitamos invertir suficiente tiempo en planear pero debemos hacerlo rápidamente. Los atacantes no están desacelerando.
- Consideremos aprendizaje automatizado y la seguridad basada en análisis de datos masivos considerado las variables de velocidad, variedad y volumen. Cuanto más cercano que podemos representar inteligencia humana, más probable será la detección certera de ataques.



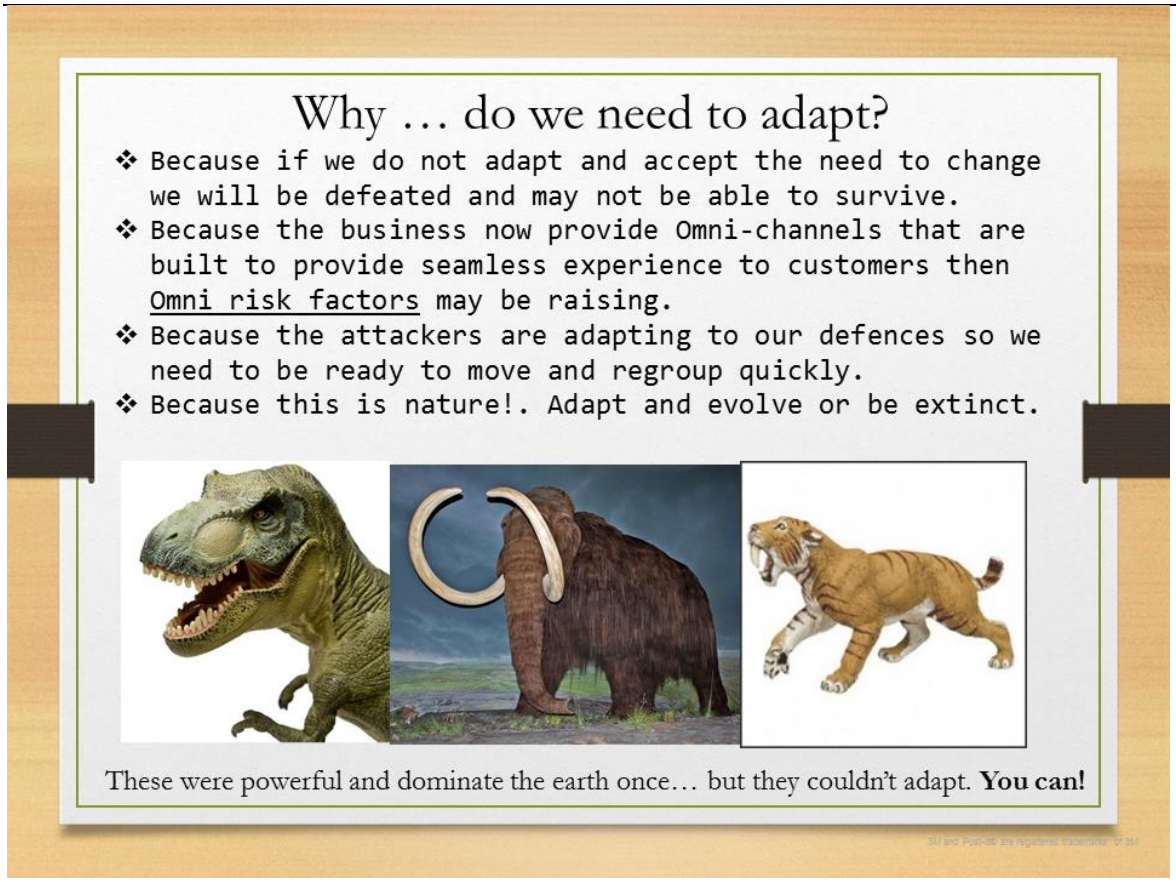
¿Cómo se puede llegar al objetivo?

- Simplemente: paso a paso. Construyendo bloques desde el centro de la organización.
- Comenzar con la identificación de los activos críticos de la organización que no se puede prescindir de ellos.
- Aplicar los principios de prevención de datos y activos críticos como las técnicas de administración de registros digitales por derechos de acceso (“Digital Rights Management” en inglés).
- Tal cual el cuerpo humano protege los órganos claves como el corazón protegido por la caja torácica y cerebro por la estructura ósea del cráneo.
- La arquitectura empresarial como disciplina es la clave para la definición de los planos del negocio. Desde la estrategia global hasta el componente más detallado.
- Construir un puente entre lo que el negocio necesita y los que el departamento de tecnología puede brindar.
- Como los factores vulnerables son multidimensionales, los factores de exposición son también múltiples. Hay que seguir invirtiendo en entrenamiento y capacitación. La educación sobre las técnicas de ingeniería social son vitales para la prevención; por ejemplo, contra los ataques de “phishing” (emails con vínculos a páginas infectadas con códigos oculto para lograr instalación de virus o robo de credenciales de autentificación).
- No es suficiente con ser mejor que la competencia.



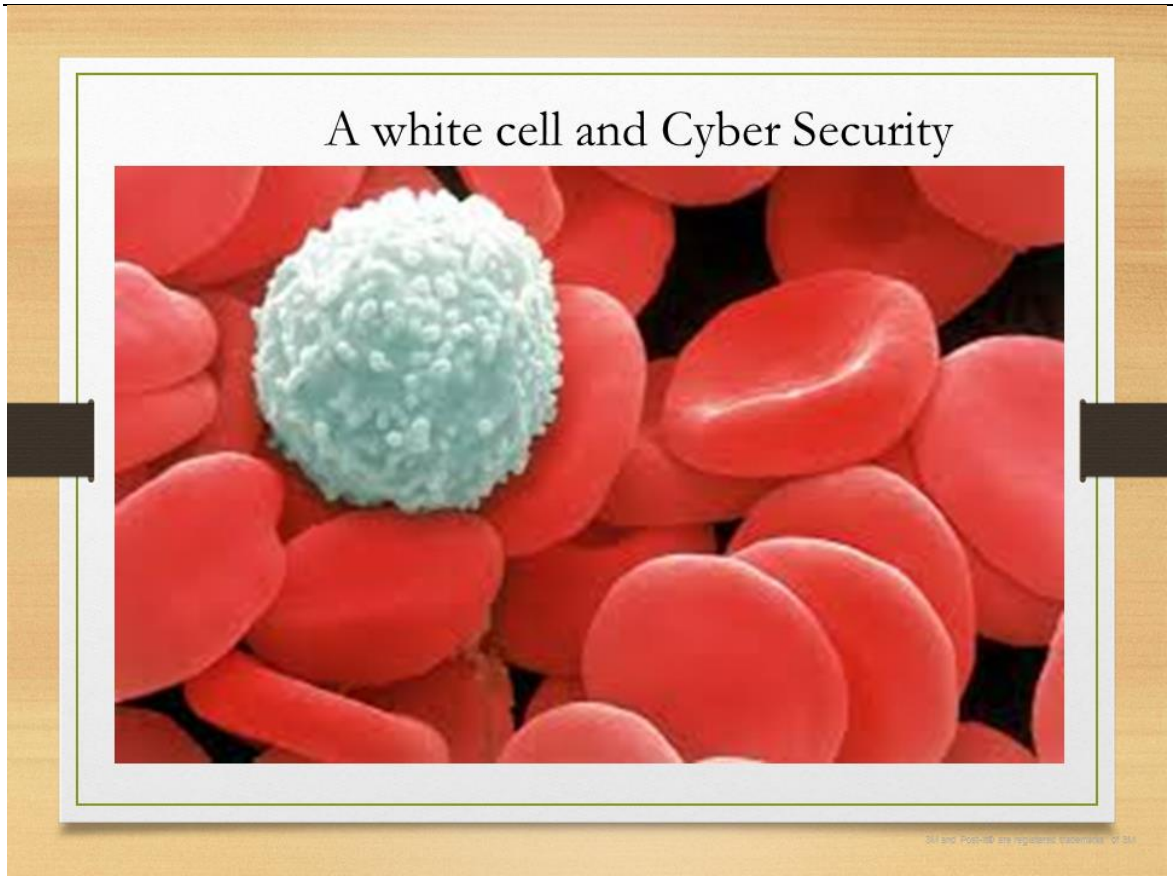
¿Cuándo deberemos actuar?

- Si no ha comenzado ya, entonces está perdiendo la batalla
- No es solo de defenderse y prevenir, es acerca de contener el ataque, comunicar a los actores necesarios y responsabilidades, ser transparentes, ser reactivos y proactivos.



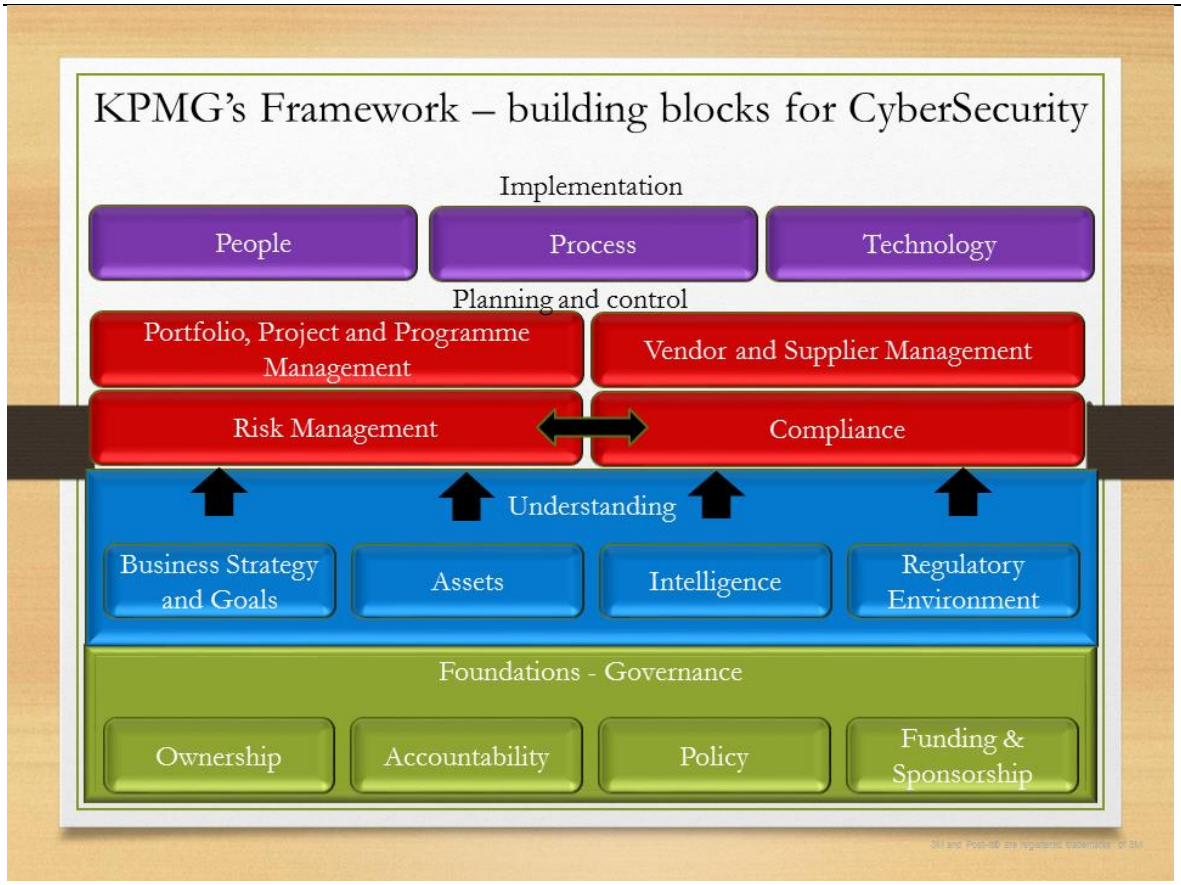
¿Por qué debemos adaptarnos?

- Porque si no nos adaptamos y aceptamos que debemos cambiar seremos derrotados y seremos incapaces de sobrevivir.
- Porque las organizaciones ahora canales de ventas o acceso al usuario múltiples los que esperan y demandan una experiencia similar de funciones y facilidades por igual. Esto conlleva a un factor de riesgo múltiple. Los controles requieren adaptación a cada plataforma.
- Porque los atacantes o predadores se adaptan muy rápidamente a los mecanismos de defensas muy rápidamente. Entonces necesitamos rápidamente a prepararnos a la próxima ola de ataque que vendrá sin descanso.
- Porque es parte de la naturaleza. Adaptarse y evolucione o será extinto.
- Estas poderosas criaturas alguna vez dominaros sus ambientes pero no pudieron adaptarse y se extinguieron, ustedes pueden!



Una celula blanca y la seguridad informática o cibernética

(Como ejemplo de un mecanismo de defensa distribuida, adaptable y eficiente)



El marco de trabajo de KPMG para la construcción de bloques en la defensa de ataques cibernéticos.

Implementación: Gente, Proceso, Tecnología.

Planeamiento y Control: Gerenciamiento de Proyecto y Programas – Gerenciamiento de proveedores – Gerenciamiento de riesgos – Gerenciamiento de cumplimiento normativo.

Comprensión de: Estrategia del negocio y sus goles, Activos, Inteligencia y ambiente regulador.

Fundación y Control Gerencial: Apropiación de responsabilidad e imputabilidad – Políticas – Financiamiento y Patrocinio.

Appendix B: Ejemplo de la interacción humana en el análisis e interpretación de datos para determinar trafico inusual y potenciales ataques.

Primero, asumimos que la organización cuenta con un equipo dedicado al monitoreo y control del flujo de redes de datos. Al menos la entidad cuenta con las herramientas de captura de datos.

El ejemplo se basa en la popular herramienta de análisis de paquetes de datos (en inglés: sniffer) llamada wireshark. Esta imagen capturada es de la consola de wireshark:

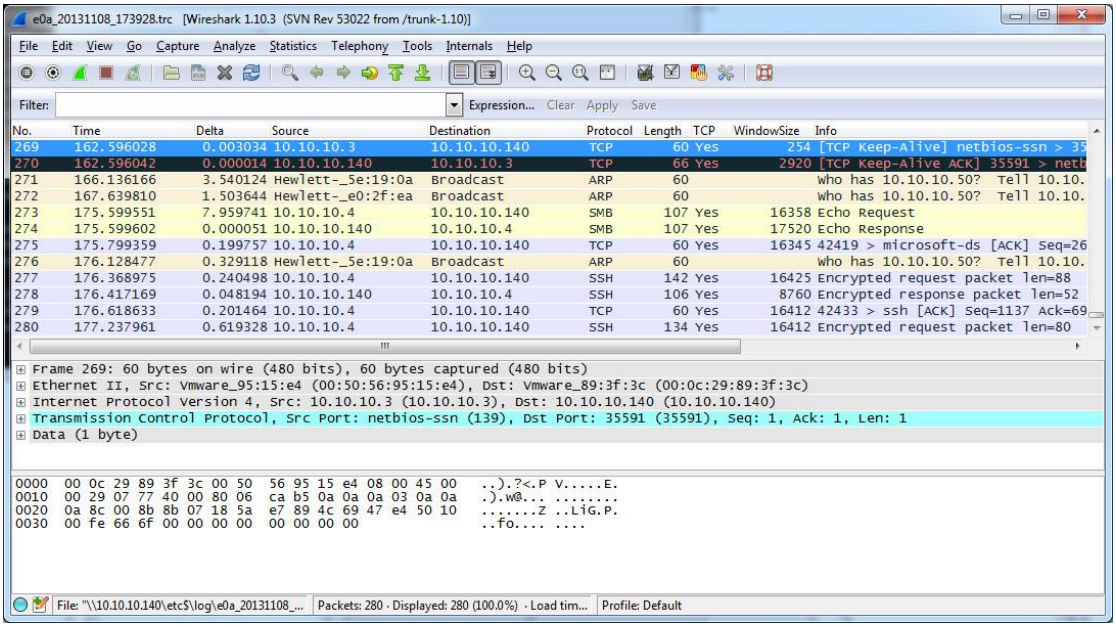


Fig.1 wireshark sniffer

Estos datos son obviamente muy difíciles para un administrador de red para leer y analizar y detectar cualquier actividad inusual por lo que debe haber herramientas en su lugar para leer este tipo de datos para ayudarlo. Esto puede ser útil solamente cuando se cuenta con alguna investigación específica para hacerlo pero, como tal, es poco probable ya que cualquier dato sin contexto no tendría sentido, sobre todo que esto está sucediendo en un volumen que es inmanejable.

Por esta razón se han incorporado herramientas inteligentes de análisis de datos. Un ejemplo muy popular en este campo es el de Splunk que puede automatizar la representación en tiempo real de múltiples fuentes de datos en modo gráfico.

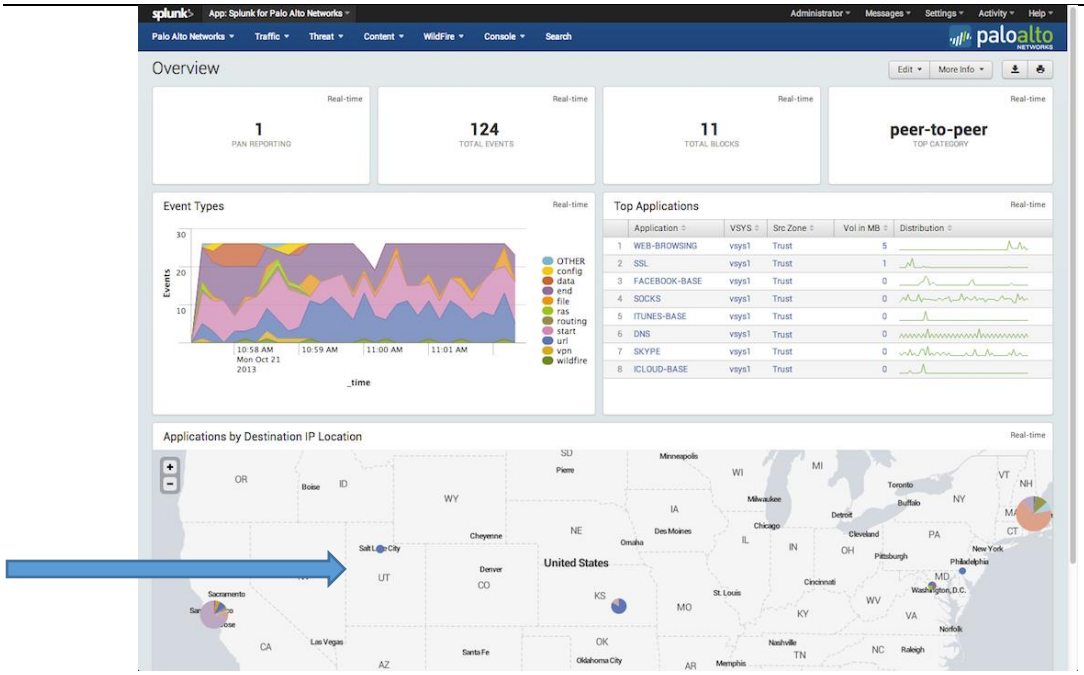


Fig 2. Pantalla de la consola de Splunk para redes de Palo Alto Networks.

En este caso, se puede ver una pantalla que representa a varios datos de múltiples fuentes y puede ayudar a detectar alguna información o pista que requiera investigación.

Por ejemplo, usted es capaz de identificar que algunas actividades puede ser sospechosas debidas a la ubicación geográfica de las conexiones IP de destino. Sin embargo, una variable que usted sabe que la empresa no tiene ninguna operación en Salt Lake City, sin empleados o proveedores. ¿Por qué entonces la pantalla está mostrando alguna pequeña actividad de esa zona? Eso puede provocar, tal vez, un administrador de red o un equipo de seguridad de TI comience a investigar.

De todos modos, esto puede no ser suficiente. En la aplicación del análisis del comportamiento de una herramienta debe ser capaz de proporcionar un patrón preestablecido de comportamiento esperado en base a lo que el tráfico ya estaba clasificado como válido y, por tanto, por excepción clasificar las desviaciones a estos patrones de reducir el tiempo invertido en las investigaciones que dieron como resultado en los falsos positivos.

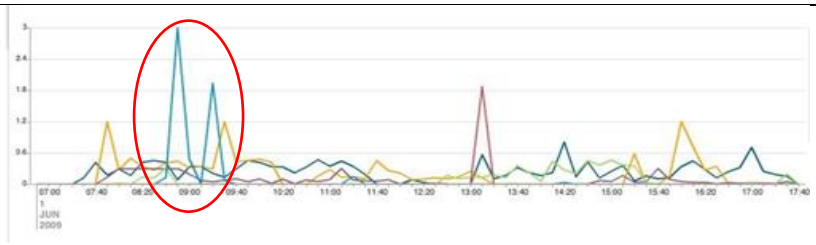


fig. 3 Diagrama con los flujos de datos en Mbp/s por tipo de tráfico.

Más aun, asumiendo que el gráfico anterior (figura 3) es un gráfico que representa los flujos de datos y la línea amarilla es el tráfico esperado por aplicación. Aquí las líneas azules, entre 8:40 y 9:20, están mostrando picos inusuales y deben ser evaluados para entender por qué estos dos picos inesperados están presente. También hay un pico rojo inesperada a las 13:10. Otra advertencia debe ser también investigada. Ahora, en el supuesto de que la organización tiene 1000 de redes y aplicaciones, entonces sería poco realista de que todo este volumen de alerta y advertencia se investiga. Entonces, ¿que lo que hay que hacer…?

Siguiendo este ejemplo, tomemos algunos supuestos adicionales para completar la información obtenida después de la primera reacción de la alerta del pico de 8:40. El equipo de seguridad de TI sacó los registros como por herramienta utilizada en la figura 1 (Wireshark) de manera similar al ejemplo anterior, los datos se han capturado y tiene que empezar a utilizar las capacidades de filtrado para reducir los puertos específicos de destino, los servicios que desencadenó los picos. Aun con los filtros se cuenta con miles de líneas de registros y siguen siendo bastante complejo el seguimiento. El investigador decidió descargar los datos y comprobar que con los propios modelos de análisis de datos. En primer lugar algunos datos clasifican los métodos para reducir el tráfico específico IP de destino o de origen IP y si la distribución del tráfico puede corresponder a poco elevado tráfico, simplemente por el aumento de las operaciones.

El análisis señaló que una gran parte del tráfico eran comandos GET en puertos HTTPS que pueden haber sido todos causados por los usuarios que hacían clic en enlaces en correos electrónicos. Una alerta roja para los ataques de tipo *phishing*. El investigador escaló rápidamente los resultados de acuerdo con el proceso de gestión de incidentes de seguridad informática. Entonces, para su sorpresa, su manager le informó que había pruebas de un *phishing* planificadas que un equipo externo de test de penetración de redes (White Hat ethical hack) que se estaban llevando a cabo como parte de los planes anuales pen-testing. El

proceso tomó el analista de todo el día y los otros dos alertas no fueron investigados por falta de tiempo.

El punto de este ejemplo es la elaboración de las deficiencias de las herramientas y procesos para permitir que las organizaciones no sólo para detectar eventos o comportamientos fuera de lo normal, pero para invertir de manera eficiente sus analistas especializados para investigar las alertas.

Una madura herramienta de análisis de comportamiento ideal debería haber sido capaz de modelar los datos en tiempo real, identificar los picos de forma automática, proveed del registro para el tráfico requerido, y una vez más en tiempo real proporcionará antes de las 9:00 el tráfico y la información relacionada de patrón que se produjo pocos minutos antes. Esto entonces se debe pasar a un analista para confirmar, si es necesario, y para permitir la escalada rápida a pocos minutos más tarde.