2018 IN CYBERSECURITY

THE EXPERTS TALK

panda

pandasecurity.com

ÍNDICE

INTRODUCCIÓN

Una de las principales necesidades que tenemos los seres humanos es la seguridad.

Desde que nacemos necesitamos “seguridad” en los distintos aspectos de nuestra vida, convirtiéndose en un atributo que nos acompaña y forma parte de nuestra propia naturaleza.

Una seguridad que hacemos extensible a todos los ámbitos en nuestro día a día, incluida la protección de los sistemas tecnológicos que utilizamos.

A lo largo de los 28 años de historia de Panda Security, hemos podido analizar la evolución del mundo de la seguridad informática, siendo testigos y partícipes de los avances que han cambiado el mundo.

El continuo avance de las tecnologías ha propiciado que los agentes responsables de las amenazas hayan incrementado la sofisticación de sus ataques y sus herramientas.

El ciberespacio es cada vez más hostil, y obliga a las organizaciones a disponer de los medios técnicos más novedosos para poder hacer frente a los ataques y a sus posibles impactos, así como adoptar políticas de seguridad proactiva para mitigarlos.

Porque el mundo que conocíamos ha evolucionado, hoy hablamos de la ciberseguridad como un concepto que se extiende no sólo para proteger nuestra información almacenada en los sistemas informáticos, sino también dirigida a proteger la infraestructura tecnológica que la soporta y nos hace funcionar como sociedad.

Lo mejor de trabajar en el campo de la seguridad informática es conocer a grandes profesionales del sector con los que compartir inquietudes, experiencias y puntos de vista, como los recogidos en esta selección llamada “2018 in Cybersecurity, The experts Talk”.

Marta Zapata

Responsable de Comunicación
Panda Security

Zane Lackey

NO DEBERÍAS INVERTIR EN SEGURIDAD SOLO POR CUMPLIMIENTO

El concepto de responsable de ciberseguridad se encuentra en un proceso de transición de su antigua función de guardián y protector hacia un nuevo rol como facilitador de seguridad para toda la empresa.

Nos lo cuenta Zane Lackey, uno de los White Hat hackers más importantes a nivel mundial y autor de libros como Mobile Application Security o Hacking Exposed: Web 2.0

En la actualidad, Lackey es el cofundador y CSO de Signal Sciences, una plataforma de protección de aplicaciones web, y también forma parte del Advisory Board del Internet Bug Bounty Program y del Open Technology Fund.

A pesar de que se crean nuevas infraestructuras, servicios y aplicaciones, cosas tan sencillas como los fallos en la seguridad de los endpoints o la ausencia de sistemas de autenticación de dos factores continúan siendo la causa de los ataques globales que llegan a los telediarios.

Arrancamos la entrevista rememorando su labor como White Hat hacker:

Descubre Más

Panda Security:

¿Cómo se detecta una vulnerabilidad y se expone la amenaza para evitar un ataque?

Volviendo a mis días de pentesting, las estrategias más comunes consistían en detectar las asunciones que se hacían en el diseño del sistema y luego descubrir de qué manera podrían ser vulneradas. Posteriormente, adopté esa perspectiva pensando en cómo empoderar al equipo de desarrollo o al de DevOps para que pudieran saber durante el proceso de producción cómo sus servicios estaban siendo atacados.

Es una de las lecciones más importantes que he aprendido de mi etapa de consultor de seguridad white hat y que aplico como CISO que busca construir una empresa segura: ¿Cómo puedo darle al equipo de ingeniería la mayor visibilidad posible para que pueda entender lo que pasa en producción?

PS: **¿Cómo ayudan programas como el Internet Bug Bounty a resolver las vulnerabilidades descubiertas? ¿Cuál es el siguiente paso?**

Confío plenamente en el valor de los programas de bug bounty. Complementan muy bien el pentesting y creo que esta fórmula puede servirle a muchos de los programas de seguridad existentes. Lo más valioso de esta combinación es que el programa de bug bounty puede enfocarse en asuntos muy amplios, dejando el pentest simplemente para áreas específicas, y así alcanzar la mayor cobertura de seguridad posible.

En la búsqueda de soluciones, es importante trabajar con los investigadores y profesionales para que la comunicación funcione, para que la información llegue al equipo de servicios o de aplicaciones y todos puedan formar parte del proceso. Para que una vez detectado el problema, el equipo de producto defina la solución y los plazos que se manejarán. Aconsejo que ambas partes sean lo más transparentes posible.

PS: **Recientemente, el Servicio Nacional de Salud británico (NHS) ha contratado a White Hat hackers para identificar ciberamenazas. ¿Crees que los hackers éticos son indispensables en las organizaciones actuales para evitar brechas y fortalecer la seguridad?**

Cada organización tiene que pensar en cómo podrían atacar sus sistemas. Los White Hat hackers, los tests de penetración, los bug bounties, son solo una parte del todo, pero una parte realmente importante.

No quieras invertir en seguridad solo por cumplimiento o para tachar la lista de las defensas que utilizas.

“CONFÍO PLENAMENTE EN EL VALOR DE LOS PROGRAMAS DE BUG BOUNTY”

Reto a los profesionales de seguridad a pensar en cómo un atacante puede entrar en su organización y a poner en práctica el resultado en las estrategias defensivas. Entonces, todos esos métodos de poner a prueba tus sistemas aportan un círculo de retroalimentación muy importante para mostrar dónde enfocar las defensas. Es decir, "al atacar tus sistemas, aquí es donde han ido".

Creo firmemente en el balance entre ataque y defensa; usar una para guiar la otra y no únicamente trabajar con una de las dos de forma aislada.

PS: **¿La evolución hacia DevOps y la nube es una amenaza o una ayuda en materia de seguridad?**

Adoptar DevOps y la nube puede ayudar a proteger tu empresa. En cualquier metodología de desarrollo, vas a tener vulnerabilidades. Por tanto, la metodología que te permita reaccionar con mayor rapidez es la que hará tu empresa más segura. La transición hacia Agile, cloud y DevOps implica que puedas reaccionar rápidamente.

PS: **¿Qué podemos aprender de brechas de seguridad como la de Equifax que ocurren gracias a vulnerabilidades de aplicaciones web?**

Dos lecciones. La primera, que el 99% de las veces los ataques suceden por cosas comunes y sencillas: sistemas que no fueron parcheados, contraseñas débiles, malware en un endpoint... Invitaría a las empresas a no enfocarse solo en las amenazas complejas, como en exploits de zero day.

La segunda sería comprender que el riesgo de seguridad ha pasado de la red hacia la capa de aplicaciones y los endpoints. Gran parte de los equipos de seguridad siguen centrándose en la infraestructura de red, pero el riesgo está en las aplicaciones y los endpoints.

PS: **¿Cree que las empresas estarán preparadas para el GDPR? ¿Cómo pueden proteger los datos?**

Seguridad y cumplimiento son dos conceptos totalmente distintos, aunque a veces se superponen. Las empresas deben pensar en cómo defender su información y no solo dedicarse a cumplir la legislación, como el . Cómo defienden sus endpoints, sus aplicaciones web, sus APIs. Para ello, deben generar visibilidad de los procesos, poner controles efectivos para el malware, aplicar autentificación de dos factores en tantos servicios como puedan, cobertura y protección en las capas de aplicaciones web.

"EL 99% DE LAS VECES LOS ATAQUES SUCEDEN POR COSAS COMUNES Y SENCILLAS"

PS: **En términos de seguridad de aplicaciones web, ¿prefieres asegurarlas desde adentro, durante la programación, o emplear medidas de seguridad posteriores?**

Hay que hacer ambas. Para defender aplicaciones, hay que pensar qué podemos hacer para eliminar la mayor cantidad de bugs posibles durante el ciclo de desarrollo, pero a la vez es necesario reconocer que siempre habrá bugs y vulnerabilidades. Además, debemos asegurar el propio código durante la programación y no simplemente buscar bugs antes de lanzarlo y, una vez la app está en internet, olvidarnos. Creo que este ha sido un error importante del SDLC (Systems Development Life Cycle) en los últimos 10 años, eliminar los bugs antes de la fase de producción y luego no dar visibilidad o defensa al código una vez en producción.

Hay que empezar a proveer de herramientas al equipo de desarrolladores para que ellos mismos puedan ver cómo están siendo atacadas sus aplicaciones y, por tanto, reaccionar. Los equipos de desarrolladores y DevOps necesitan ser autosuficientes en ciberseguridad. Solo así pueden seguir el ritmo de cambios constantes de las aplicaciones. ■

“DEBEMOS ASEGURAR EL PROPIO CÓDIGO DURANTE LA PROGRAMACIÓN Y NO SIMPLEMENTE BUSCAR BUGS ANTES DE LANZARLO”

Soledad Antelada

EN ESTADOS UNIDOS, LA CIBERSEGURIDAD ES UNA PRIORIDAD NACIONAL

La experta en el sector, ingeniera de sistemas en el departamento de Ciberseguridad del Lawrence Berkeley National Laboratory, opina que la ciberseguridad "salió del underground, de estar formado por un grupo técnico muy pequeño, a entrar en el inconsciente colectivo y pasar a ser un movimiento global".

Soledad Antelada, una de las latinas más influyentes en el mundo tecnológico, tiene una tarea clave: garantizar la seguridad de un sistema en el que trabajan miles de personas.

El Berkeley Lab es un prestigioso centro de investigación científica, en el que han desarrollado su trabajo 12 premios Nobel, gestionado por la Universidad de California, que forma parte del gobierno de los Estados Unidos.

Por su parte, el departamento de ciberseguridad se encarga de proteger al laboratorio y a toda la red de instituciones dependientes del Departamento Nacional de Energía. La experta en ciberseguridad nos cuenta cuáles son las claves de seguridad para proteger este tipo de organismos.

Descubre Más

El pentesting para adelantarse a los cibercriminales

Soledad trabaja directamente como un agente externo, es decir, finge ser un atacante que penetra en la red para llegar a algún equipo o saltar de una red a otra. "Siempre como un intruso", señala. Para ello, utiliza herramientas de escaneo y de explotación, o desarrolla sus propias herramientas. Entre ellas, sus favoritas son Python, SSH Brute Force para ataques por fuerza bruta, Nessus para escaneo de sistemas, y Burp y Netsparker para escaneo de aplicaciones web. Para exploit, "mucho escaneo manual o metasploit y SQL injection".

Antelada nos recalca la importancia que tiene el penetration testing en el Berkeley Lab: "Este tipo de herramienta tiene prioridad para nosotros. Nos queremos enterar primero que nadie y llegar a las vulnerabilidades antes de que las descubran los atacantes para poder solucionarlo rápidamente". También nos cuenta que desde el Departamento de Energía realizan auditorías de ciberseguridad para evaluar la seguridad del laboratorio. Según Soledad, "durante el período de auditorías, evalúan la vulnerabilidad general del laboratorio. Si no encuentran nada es que estamos haciendo bien nuestro trabajo".

"La mejor virtud en la labor del pentester es la paciencia", añade. "Es necesaria mucha prueba y error para descubrir en tu horario de trabajo lo que intentan hacer los malos 24/7. Y encima, luego, tener que arreglarlo".

Consejos para profesionales de seguridad en un mundo conectado

La visión de Soledad sobre el sector es que "más que en equipos, hay que invertir en personas altamente cualificadas". Al apostar por los expertos y reforzar los departamentos de ciberseguridad, tanto empresas como instituciones pueden adelantarse a los sucesos y no esperar a que los ataques tengan lugar para defenderse. En Estados Unidos, señala Antelada, se le da al sector la importancia más alta: "Independientemente del gobierno de turno, la ciberseguridad es una prioridad para la nación".

Para Soledad, también es prioritaria la educación que se le da a los empleados. Según ella, esto será aún más importante a medida que crezca el denominado Internet de las Cosas. Como explica, en el caso del Berkeley Lab: "Allí tenemos todo tipo de instrumentos conectados a la red, como láseres y microscopios, que también se convierten en vectores de ataque". En el caso de que peligre la seguridad de estos dispositivos, "hay que contactar con los científicos que operan estos instrumentos y guiarlos sobre cómo arreglar la vulnerabilidad".

No se trata únicamente de solucionar el problema, sino de educar y guiar a los usuarios sobre la vulnerabilidad, cómo lo han encontrado y cómo se arregla. Esto, dice Soledad, sirve "para que los empleados adopten la mentalidad adecuada respecto

"LA MEJOR VIRTUD EN LA LABOR DEL PENTESTER ES LA PACIENCIA"

a la ciberseguridad y a partir de este momento puedan estar alerta ante actividades sospechosas".

Asimismo, para proteger a las instituciones, es primordial que exista colaboración entre distintas áreas de la organización. "Debe existir un apoyo real entre los trabajadores de los departamentos. Entre los responsables del almacenamiento y gestión de datos, los administradores de sistemas y los desarrolladores de software... Todos deben estar conectados con el departamento de ciberseguridad porque no pueden trabajar por sí solos, dependen de los dueños o administradores de lo que protegen".

La mujer en el sector de la ciberseguridad

Desde Girls Can Hack, Soledad busca acercar la tecnología y la informática a las mujeres para fomentar su participación en un sector que ha sido tradicionalmente masculino. "Soy la primera y única mujer en el departamento de ciberseguridad del Berkeley Lab", cuenta Antelada, "y aunque todavía los porcentajes de presencia femenina en las empresas son muy bajos, veo un cambio en la mujer que ahora empieza a tener interés por estas áreas del conocimiento".

Para cambiar este panorama, Soledad aconseja a las mujeres que quieran adentrarse en el sector: "Anímate. Es un campo muy dinámico en el que se necesita gente, y gente diversa. Los departamentos de ciberseguridad son monótonos y esto es un error. Los problemas de seguridad son diversos y cuanto más variados sean los departamentos, más fácil y creativa será la resolución de los problemas". ■

"VEO UN CAMBIO EN LA MUJER QUE AHORA EMPIEZA A TENER INTERÉS POR ESTAS ÁREAS DEL CONOCIMIENTO"

Silvia Barrera

EN LA LUCHA CONTRA EL CIBERCRIMEN EL 90% ES PREVENCIÓN Y CONCIENCIACIÓN

Experta en ciberseguridad y escritora, Silvia ha sido jefa del grupo de investigación en redes sociales de la Policía durante 5 años y ha dirigido el grupo de forense digital de la Unidad de Investigación Tecnológica durante 3 años.

Hablamos con ella, ahora que ha dejado su actividad en la Policía, para que nos cuente cómo cree que está cambiando el panorama de la ciberseguridad y cómo las instituciones públicas y las empresas pueden protegerse y combatir el cibercrimen.

Descubre Más

PS:**¿Qué supone para ti empezar esta nueva etapa?**

Un mundo de posibilidades. La Policía me ha aportado una visión, un conocimiento y una experiencia excepcional, incomparable. Ha sido un privilegio. Pero, hasta ahora, como parte de la institución pública policial, mi trabajo siempre ha estado en el plano reactivo: identificar y detener a los "presuntos" malos. Sin embargo, el paradigma de la lucha contra el crimen ha cambiado. Ahora las cifras en materia de cibercrimen no llegan ni al 4% de autores identificados (que no condenados). También sabemos que la gran mayoría de delitos a través de Internet, hasta un 80%, se podrían haber evitado. El cibercrimen es un modelo de negocio muy rentable, con poca exposición para el criminal y muy difícil de combatir. Es inevitable y va en aumento. La forma de luchar en la parte reactiva es necesaria pero poco eficaz (por el propio funcionamiento de la Red) e insuficiente.

Hay que empezar a tomar conciencia de que en la lucha contra el cibercrimen el 90% es prevención, concienciación y controles preventivos y el 10% es reacción (investigación y persecución de los hechos). Debemos actuar con todas las herramientas posibles, técnicas y humanas, para evitar que esto ocurra y, si ocurre, estar preparados para reaccionar. Y aquí es donde entra el concepto de la resiliencia.

PS:**¿Por qué crees que es necesario un evento como Panda Security Summit?**

Para dar visibilidad a la ciberseguridad, tratar conceptos clave y situarla en un lugar prioritario, que es donde debe estar. A nivel corporativo, todas las actividades empresariales se sustentan en datos informáticos y estructura TI. Y a nivel estatal, el crimen tiene siempre una implicación tecnológica, en su modus operandi o para la obtención de las evidencias y pruebas, e incluso la Seguridad Nacional de un Estado puede verse seriamente comprometida.

PS:**¿Qué nivel de concienciación y formación general crees que existe en Europa?**

He formado parte de grupos de trabajo en materia de cibercrimen y ciberseguridad en Europa durante cuatro años y he participado en decenas de reuniones. Ahí es donde se ven realmente las diferencias de recursos y la importancia que le da cada país a la ciberseguridad. Holanda, Alemania o Gran Bretaña, por ejemplo, nos llevan diez años de ventaja a España. Destinan a nivel público muchos más recursos técnicos y humanos en ciberseguridad. Incluso, a nivel legislativo, Alemania tiene su propia regulación.

PS:**¿Qué nivel de preparación crees que existe en las instituciones españolas y europeas?**

En España no tenemos nada que envidiar a otros países. De hecho, en materia de lucha contra el cibercrimen somos muy eficientes. No es una cuestión de falta de competencia sino de escasez

"EL CIBERCRIMEN ES UN MODELO DE NEGOCIO MUY RENTABLE, CON POCA EXPOSICIÓN PARA EL CRIMINAL Y DIFÍCIL DE COMBATIR"

de recursos, técnicos y humanos, y el cibercrimen y el mundo digital necesitan una inversión potente.

En un intercambio policial que hice con la Policía Federal Alemana, para la investigación de un caso que afectaba a los bancos alemanes, hacían grupos conjuntos entre funcionarios policiales, fiscalía y sector privado y trabajaban exclusivamente en ese caso hasta que se esclarecía o las posibilidades de investigación terminaban. En España, los investigadores llevan decenas de casos a la vez y aunque se establecen contactos, no se trabaja en grupo de esa manera.

PS:**¿Cuál crees que es el mayor problema de las empresas y las instituciones a día de hoy para no ser seguras?**

El factor humano y después, el técnico. En materia técnica, es evitable mediante una correcta evaluación de riesgos y el empleo de controles internos y externos. No pensemos solo en el empleado, las instituciones y las empresas deben integrar y alinear la ciberseguridad como un objetivo estratégico más de la corporación y asumir los costes necesarios en lo relativo a la seguridad de la información. Se avecinan tiempos duros en materia de riesgos para la seguridad y protección de datos, y los castigos y sanciones que se derivan de ellos pueden suponer costes muy elevados, sobre todo a nivel reputacional. Tenemos los casos recientes de Facebook y Tesla.

PS:**¿Qué retos crees que afrontarán las instituciones y las empresas en materia de seguridad durante los próximos años?**

El cambio de mentalidad del consumidor. Hay que tratar de ser lo más preventivo posible, actuar en cada una de las fases para evitar un mayor coste del cibercrimen al consumidor. Sería una falacia decirle al usuario/cliente que nunca va a ser víctima de un ataque. Lo será. Por ello, hay que estar preparados.

Cuanto más se preocupe por su ciberseguridad, más seguro estará de daños personales, empresariales, reputacionales... La ciberseguridad nunca tiene un coste mayor que el daño que podemos sufrir. La Red ofrece un campo infinito de utilidades y funcionalidades que nos pueden facilitar la vida pero también arruinarla.

“ SE AVECINAN TIEMPOS DUROS EN MATERIA DE RIESGOS PARA LA SEGURIDAD Y PROTECCIÓN DE DATOS”

PS:**¿Qué significa para ti que una empresa o una institución sean resilientes desde el punto de vista de la ciberseguridad?**

La resiliencia es el mejor factor para comprobar la fortaleza de una empresa o institución. Pone a prueba cómo gestionamos nuestras comunicaciones, datos, seguridad e infraestructura TI. Cómo nos repongamos de un posible ataque es también un factor para comprobar nuestra preparación y en qué se puede mejorar. Al final, pone de manifiesto quiénes se adaptan de forma exitosa a los cambios y demandas tecnológicas. Y de cara al cliente externo, el cómo cuides ese aspecto interno en tu organización le hará ver también cómo cuidas la información de tus clientes. Te juegas la reputación y su confianza.

PS: **Bajo tu punto de vista, ¿qué valor de la resiliencia es el más importante para tener una compañía o una institución seguras?**

Todos. Desde el plano preventivo, evitando la gran mayoría de ataques e incidentes, a la detección y la respuesta. Aunque no existe la seguridad 100%, como sabemos, podemos evitar caer casi en ese 99% de ataques evitables. ¿Cómo? Teniendo en cuenta todos los valores de la resiliencia. Tenemos que concienciarnos de que la ciberseguridad es como cuidar nuestra propia seguridad y salud personal. Puede que no saquemos rédito objetivable de ello pero garantiza una larga vida, llena de satisfacciones y éxitos. Esto es la resiliencia. ■

“ PODEMOS EVITAR CAER CASI EN ESE 99% DE ATAQUES EVITABLES TENIENDO EN CUENTA TODOS LOS VALORES DE LA RESILIENCIA”

Pedro Uría

EL RETO FUTURO DE LA CIBERSEGURIDAD NO ESTÁ EN EL MALWARE

Hemos hablado con Pedro, director de nuestro laboratorio PandaLabs, para que nos explique cómo mantener a las organizaciones seguras, protegidas y resilientes cuando el malware ya no es un problema.

Descubre Más

PS:**¿Cuál es el mayor reto al que se enfrentan actualmente las instituciones y empresas en el campo de la seguridad informática?**

El mayor reto está en concienciarles de que la seguridad de sus activos informáticos es crítica y que están en constante riesgo de ser atacadas. Según el INCIBE, España batió su récord de ciberataques en 2017 con más de 120.000 incidentes, un 140% más en tan solo dos años. La previsión es un aumento de esta cifra en 2018 con ataques más complejos.

PS:**¿Qué podemos aprender de brechas de seguridad como la de Equifax, debidas a vulnerabilidades?**

Que ninguna organización está a salvo de los ciberdelincuentes. La utilización de vulnerabilidades para acceder a los sistemas de una compañía es una técnica muy empleada. Este caso es la mayor exfiltración de datos de información personal que se conozca; los hackers robaron los datos de 147,9 millones de estadounidenses.

Las vulnerabilidades de día 0 se comercializan en la Deep Web y son un vector de ataque silencioso y de mucho éxito para las organizaciones criminales. Como ejemplo, Microsoft acaba de sacar un parche de urgencia para una vulnerabilidad crítica de este tipo en su antivirus Windows Defender en Win10. Como vemos, ni siquiera organizaciones como Microsoft en temas críticos, como es su AV, están a salvo.

PS: **Los ataques malwareless y sin fichero son tendencias de ataque, ¿cómo pueden las empresas y Estados luchar contra estos ataques?**

El reto que nos plantea el futuro de la ciberseguridad no está en el malware, está en los hackers. Son cibercriminales expertos con gran preparación y medios, capaces de comprometer un sistema de una organización sin ser detectados al no utilizar ningún malware ni fichero que pueda delatarlos.

Para luchar contra ellos las empresas deben proteger todos y cada uno de sus sistemas informáticos con una solución de ciberseguridad avanzada capaz de monitorizar en tiempo real y de forma constante lo que ocurre en cada máquina. Además, debe poder asegurar que las acciones son lícitas, aunque sean realizadas con aplicaciones legítimas o sin malware.

PS:**¿Cómo podemos ser resilientes ante los intentos del malware para evadir el análisis de la solución de seguridad?**

Para conseguir la ciber-resiliencia es necesario proteger todos y cada uno de los activos de la empresa con una solución de seguridad avanzada capaz de detectar y prevenir y remediar ataques. A su vez, es necesario que esa solución monitorice y xcontrole en tiempo real y sobre la propia máquina física todo proceso y usuario y las acciones que estos realizan. Se requiere de una monitorización, supervisión y atestación de todos los procesos y acciones realizado por un servicio específico de expertos, como el equipo de PandaLabs.

“LAS EMPRESAS DEBEN PROTEGER TODOS Y CADA UNO DE SUS SISTEMAS INFORMÁTICOS CON UNA SOLUCIÓN DE CIBERSEGURIDAD AVANZADA”

Asimismo, es importante educar a los directivos, trabajadores y externos para que no sean engañados y se conviertan en el vector de entrada.

PS: **Hablamos de mantener las organizaciones seguras, protegidas y resilientes cuando el malware ya no es un problema. ¿Hemos alcanzado ya ese nivel de protección o sigue siendo el malware el principal problema de las empresas?**

Depende en gran medida del grado de madurez de la empresa en cuanto a la importancia que se dé a la ciberseguridad y la solución de protección avanzada elegida para proteger su infraestructura.

Para Panda Security, el malware ya no es un problema gracias a la gran visibilidad que disponemos en nuestra solución avanzada Panda Adaptive Defense y el modelo de clasificación del 100% de los procesos que se ejecutan en los endpoints que seguimos. Gracias a ello somos capaces de adelantarnos a los ataques y proteger los sistemas de las empresas que confían en nosotros.

Asimismo, el servicio de Threat Hunting, que se ofrece desde la plataforma Panda Adaptive Defense, está centrado en descubrir nuevos ataques, como el mencionado malwareless.

Para otras empresas el malware sigue siendo un gran problema. Cada día hay más malware, es mayor el número de incidentes y la tendencia para el 2018 va a ser un incremento en ataques y en la complejidad de los mismos. ■

“PARA PANDA SECURITY, EL MALWARE YA NO ES UN PROBLEMA”

José Sancho

EMPRESAS QUE GASTAN MUCHÍSIMO EN SEGURIDAD PUEDEN TENER UN NIVEL BAJO DE PROTECCIÓN

Queremos contribuir a arrojar luz sobre un panorama intrínsecamente muy complejo por su multidimensionalidad y que se estructura en tres elementos.

El llamado mundo virtual, el ciberespacio, es el lugar donde se desarrollan prácticamente todas nuestras actividades profesionales y muchas de las personales, y también el lugar donde se producen los ataques.

La principal cuestión es ¿por qué nos atacan en el ciberespacio? La motivación primaria es simple y llanamente económica. La fuente de dinero primordial en este contexto es la información que guardamos, los datos.

¿Y por qué atacar en este entorno? El mundo virtual está basado en software y el software es vulnerable; los ciberataques son rápidos y a bajo coste relativo, comparado con un ataque en el mundo físico.

Descubre Más

A esto se une el hecho de que las leyes existentes contra el crimen no son efectivas cuando se trata de ciberdelitos. Estas leyes están evolucionando despacio y persiste el problema de la atribución del delito, ya que si no se puede identificar al responsable, si no ha dejado pruebas, no hay delito; como bien sabemos, en el ciberespacio es relativamente sencillo que una red criminal bien preparada no deje ningún rastro.

El segundo elemento a tener en consideración son las empresas. Cada vez es mayor el porcentaje de empresas cuya principal actividad consiste en proporcionar servicios, lo que se traduce en una cantidad ingente de bits de información, un botín muy suculento para los ciberdelincuentes.

Por último, los estados serán un elemento crucial en el futuro próximo a la hora de hablar de seguridad. No es casualidad que Estados Unidos, China o Rusia tengan empresas tecnológicas que cubran todas las capas de nuestra actividad digital, ya que estas constituyen la espina dorsal de la economía actual. En este panorama, Europa parte en desventaja. Asimismo, hemos visto que existe una guerra nueva, y cómo esta ciberguerra es probablemente la única que tiene capacidad de transferir riqueza de un estado a otro. Los estados son actores principales en esta guerra: tienen motivos, medios y ocasión.

Resulta evidente que en los próximos meses esta evolución en el cibercrimen será más rápida y más virulenta: las ofensivas van a ir a más porque las personas detrás de los ataques aprenden cada vez a mayor velocidad y las herramientas disponibles también se sofistican. Todos los actores involucrados en la seguridad de una forma o de otra tenemos que tener presente que las medidas preventivas que hemos tomado hasta ahora, basadas en detectar el ataque lo más rápido posible, no son infalibles y tardan demasiado en un entorno que se mueve mucho más rápido que ellas.

El triángulo de la ciberseguridad

En Panda tenemos una visión holística de la ciberseguridad avanzada, que hemos plasmado en un triángulo en el que nos movemos para poder garantizar la seguridad:

Las personas
Los programas
Los datos

La superficie de ataque ha crecido exponencialmente. La transformación digital implica cada vez más software y más datos, y dado que los puntos de vulnerabilidad son infinitos, es imposible una protección total por medio de producto. Se exige un complemento de personas que validen y examinen lo que los productos no son capaces de detectar o arbitrar cuando dos productos ofrecen diagnósticos diferentes.

“EN LOS PRÓXIMOS MESES ESTA EVOLUCIÓN EN EL CIBERCRIMEN SERÁ MÁS RÁPIDA Y MÁS VIRULENTA”

Así, la seguridad para nosotros consiste en recoger todos los datos relevantes de comportamiento de un programa, activado por una persona. Esta visión choca frontalmente con la perspectiva más tradicional de colocar barreras para evitar los ciberataques; lo cierto es que a día de hoy absolutamente todas las barreras son permeables porque el software es vulnerable.

Existe una falta de correspondencia entre la inversión en defensa, y la probabilidad de ataque y de impacto de ese ataque. Así vemos como empresas que gastan muchísimo en seguridad, pueden tener un nivel bajo de protección. Y es porque las inversiones no están realmente enfocadas a la defensa de los contenedores de los activos valiosos que hay que proteger, los endpoint. ■

“EXISTE UNA FALTA DE CORRESPONDENCIA ENTRE LA INVERSIÓN EN DEFENSA, Y LA PROBABILIDAD DE ATAQUE Y DE IMPACTO DE ESE ATAQUE”

Javier Candau

LA COOPERACIÓN ENTRE EL ÁMBITO PRIVADO Y EL PÚBLICO ES FUNDAMENTAL CONTRA LAS AMENAZAS CIBERNÉTICAS

El jefe del Centro Criptológico Nacional (CCN-CERT), Javier Candau, que aportará su visión sobre el reto de la ciberseguridad en España.

Todas las dimensiones de seguridad son importantes para una compañía, según Candau, pero la confidencialidad de ciertos asuntos y procesos cobra especial relevancia.

La gerencia, afirma, debe comprender que el negocio está soportado en sus sistemas y en la información generada, por lo que esta es una decisión estratégica, como lo son las vigilancias y las auditorías. Como máximo responsable del CCN-CERT, Javier Candau sabe cuáles son las claves de un Estado a la hora de combatir la ciberguerra. Entre ellas, se encuentra la implantación de mejoras en líneas como las capacidades de detección, considerando a la ciberseguridad como un servicio horizontal; el intercambio entre el sector público y el privado; la respuesta, que tiene que ser ágil y 24/7 en todos los puntos de la red corporativa; y la disuasión.

Descubre Más

Hasta la fecha, sectores como el aeronáutico, el público en general, la defensa o la energía han sido los principales objetivos de ataques complejos. Para hacer frente a este tipo de incidentes, el CCN-CERT está buscando avances en la sensibilización de las autoridades del Estado y la gerencia de las empresas, y en la capacidad de detección de ataques complejos con herramientas detectoras de anomalías como CARMEN, que se deben integrar con las herramientas de correlación de logs de los organismos y, fundamentalmente, con las herramientas de endpoint.

Además, Javier Candau apunta que se trabaja para mejorar las estructuras de ciberseguridad de los organismos, buscando que algunos servicios se proporcionen como horizontales y que el personal técnico detectado tenga la cualificación suficiente a través de programas de formación y el aporte de información técnica sobre tecnologías y sus configuraciones.

Colaboración con el sector privado y los retos de 2018

Las grandes empresas son aliados del Estado para poder hacer frente a los ciberataques, pero para ello, primero hay que generar en ellas la confianza suficiente, explica Candau, y posteriormente, se les debe aportar un valor diferencial que complemente y refuerce los servicios de seguridad que les proporciona el sector privado. Con ello, el jefe del CCN-CERT espera que las empresas compartan en algún momento información sobre los ataques que sufren y sus inquietudes en ciberseguridad.

El reto fundamental de la ciberseguridad estatal en el presente año es proporcionar servicios horizontales mucho más proactivos, con la implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado (AGE). Además, Javier Candau detalla que el Centro trabaja en la mejora de las plataformas de intercambio, las capacidades de detección, las capacidades de auditoría, y las plataformas y contenidos formativos.

Dentro del planteamiento del CCN-CERT para combatir el cibercrimen contra el Estado, la atribución del origen del atacante pasa a ser el estadio final de la resolución de un incidente, según aclara Candau, ya que este no es determinante. En este sentido, y siguiendo la normativa vigente, el organismo estatal se mueve en términos de peligrosidad/impacto y de velocidad de respuesta.

Javier Candau admite que el cibercrimen ha alcanzado complejidades muy diferentes. Estas van desde las redes de botnet, que generalmente son fáciles de detectar y desinfectar, a ataques de crimen organizado que buscan el beneficio económico directo o el robo de información, pasando por ransomware complejo de difícil análisis criptológico.

El responsable del CCN-CERT también señala que los objetivos fijados son suficientes para proteger las infraestructuras críticas del país ante ciberataques, pero estos sistemas no plantean el reto de la protección de las redes operacionales. Candau reconoce que ya no es una opción que estas no estén interconectadas, porque el negocio necesita esa información, así que aboga por políticas de seguridad coherentes y vigilancia exhaustiva tanto de las interconexiones como del tráfico y las anomalías en los protocolos industriales. Por ello, se tiene que aplicar la seguridad en todos los planos: físico, ciber y humano. ■

“EL CIBERCRIMEN HA ALCANZADO COMPLEJIDADES MUY DIFERENTES”

Nicola Esposito

LA CLAVE PARA LA RESILIENCIA ES UNA ESTRATEGIA MADURA Y UN BUEN PARTNER

Esposito, director del CyberSOC EMEA Center de Deloitte y Socio en Deloitte Advisory, nos ayudará a entender cómo Deloitte, desde su área de Cyber Risk, ayuda a las organizaciones a fortalecer su programa de gestión del riesgo y seguridad.

Descubre Más

PS:**¿Cuáles son las amenazas avanzadas más importantes a las que se enfrentan las empresas hoy?**

Las amenazas avanzadas combinan múltiples métodos de targeting, herramientas y técnicas. En la actualidad, el malware es una de las amenazas más importantes debido a su capacidad para extenderse rápidamente por toda una organización e incluso alrededor del mundo.

PS: **¿Qué valor de la resiliencia dirías que es el más importante para la seguridad de una compañía?**

No hay un solo valor. Todos ellos (prevención, detección, contención, respuesta y mejora continua) deben ser tenidos en cuenta para adoptar un enfoque serio sobre seguridad de la información. De acuerdo con este enfoque, y para ofrecer a sus clientes una solución end-to-end, Deloitte ha desarrollado su Common Store Front basado en las cuatro áreas de Estrategia, Seguridad, Vigilancia y Resiliencia.

PS:**¿Cómo puede contribuir a la mejora de la infraestructura de ciberseguridad de las empresas la creación de un ecosistema de seguridad integrado y conectado?**

La creación de este ecosistema puede ayudar a que cada compañía sea más segura y forme parte de una cadena de seguridad. Esta es una de las razones por las que Deloitte promueve una red de Threat Intelligence, para poder compartir indicadores de compromiso (IoCs) e incrementar las capacidades de detección de sus clientes. Este tipo de redes permiten que estos IoCs sean comunicados casi en tiempo real, para así reducir el tiempo de exposición al malware asociado.

PS:**¿Cuáles son los riesgos a los que se enfrenta una empresa no resiliente?**

Las empresas no resilientes probablemente no tienen en cuenta la seriedad de los riesgos de ciberseguridad. Este es el mayor reto. Una vez que la dirección de la empresa lo reconoce, necesita un partner de confianza para construir un programa de seguridad robusto. Aquí está el segundo reto: encontrar un partner que sea capaz de guiarles en un camino que podría ser complicado.

PS:**¿Cuáles son las claves para crear empresas resilientes?**

La clave para la resiliencia es una estrategia madura y un buen partner. Con una estrategia madura podemos afrontar los riesgos de manera adecuada, empezando por los riesgos de negocio y no enfocándolos directamente desde el punto de vista tecnológico. Una estrategia que debe incluir los valores mencionados anteriormente: seguridad, vigilancia y resiliencia. También son claves los partners que tengan visión global, que comprendan el alcance de las amenazas actuales, y capacidades end-to-end para comprender los riesgos de negocio, asesorar al cliente al respecto, e implementar y operar las tecnologías para hacer de su negocio uno resiliente.

“LA CLAVE PARA LA RESILIENCIA ES UNA ESTRATEGIA MADURA Y UN BUEN PARTNER”

PS:**¿Cuál es el riesgo de ignorar la resiliencia?**

El mayor riesgo es la alta probabilidad de ser impactado por un ciberataque y la imposibilidad de recuperarse después de él. Aparte de todo lo que supone que los sistemas críticos estén comprometidos, también existe el peligro de que se vea afectada la reputación de la marca, que en algunos casos puede tardar años en recuperarse. También existe el riesgo asociado al cumplimiento de las regulaciones, que está unido a los controles de seguridad que se implementan en cada compañía.

PS:**¿A qué parte de la ciberresiliencia crees que deberíamos prestarle más atención?**

La parte más olvidada de la resiliencia, o que igual no es considerada adecuadamente, es la detección. Principalmente porque la detección significa tener visibilidad, y para obtenerla hay que comprender dónde y cómo prestar atención a todas las otras secciones que conforman la ciberresiliencia. En Panda sabemos que la detección y respuesta ante los ataques es primordial para mantener la ciberseguridad empresarial. Por ello, herramientas como Panda Adaptive Defense garantizan la protección de estos aspectos que en ocasiones podrían ser pasados por alto. ■

“LA DETECCIÓN SIGNIFICA TENER VISIBILIDAD”

Mónica Valle

WANNACRY MARCÓ UN ANTES Y UN DESPUÉS PARA LAS EMPRESAS ESPAÑOLAS

Es periodista, experta en temas de ciberseguridad desde hace años y, además, ahora está de estreno. Mónica Valle acaba de lanzar 'Ciberseguridad, consejos para tener vidas digitales más seguras', un libro dedicado al internauta medio, pero lleva años en contacto con varias de las empresas de ciberseguridad más importantes del mundo.

Con este bagaje, Valle tiene sobrada experiencia para dibujar un estado de la situación de las empresas españolas en lo que a ciberseguridad se refiere. Un estado en el que, en su opinión, "Wannacry marcó un antes y un después en concienciación. Las empresas grandes ya están concienciadas porque llevan mucho tiempo haciéndolo, y ya lo ven más como una inversión que como un gasto".

En estos casos, "el problema llega con las pequeñas y medianas empresas, ya que para ellas sí que supone el gasto de un presupuesto que no siempre es fácil encontrar. Son las que más han tenido que ponerse al día, y más aún con la aprobación del GDPR, que a muchas les ha pillado con el pie cambiado".

Descubre Más

Las tareas pendientes en ciberseguridad

Para ella, “todavía queda mucho por hacer” en materia de ciberseguridad empresarial. Y es que “muchas veces se actúa de forma reactiva: no haces nada hasta que le pasa a otra empresa. Pero eso en ciberseguridad es un error, porque hay que ser preventivo y proactivo y poner las medidas antes de que te pase algo. En ataques de ransomware, por ejemplo, cuando te atacan el daño ya está hecho, va a ser muy difícil recuperar nada, las empresas deben ser conscientes de esto”.

“Es muy importante saber reaccionar”, asegura, “porque en función de eso puedes minimizar los daños. Las empresas que aún no son conscientes de la importancia de la ciberseguridad a nivel de prevención tampoco son conscientes de la importancia a nivel de reacción y de conseguir que el daño sea el menor posible”.

Y es que “los que te quieren atacar tienen muchísimas opciones y lo pueden hacer desde muchos flancos, y no es fácil prevenir eso. Todos los expertos lo dicen: todas las empresas han sido o serán atacadas. Por eso hay que centrarse tanto en prevenir como en saber reaccionar”.

Por otro lado, hay un factor que hace todavía más importante la protección de la ciberseguridad en una compañía: “Ahora no solo tienen que proteger su información, sino también demostrar que cumplen unas normas básicas de ciberseguridad. Además, si se incumple la ley, ahora las sanciones son muy elevadas”.

Cualquier empresa puede ser atacada

Sin embargo, “hay empresas que piensan que no son ‘importantes’ como para ser atacadas, pero, ¿acaso tu información no es importante para ti? Sin esa información no eres nadie, y no serías la primera empresa que ha tenido que cerrar por perder esta información. Seas del tamaño que seas, cualquier información que tengas es muy importante, como poco, para ti”.

Además “también hay que tener en cuenta el daño reputacional que te puede ocasionar un ataque. La ciberseguridad se basa en la confianza de tus clientes, tus proveedores, etc., así que el reputacional es otro de los mayores riesgos para cualquier tipo de empresa.”

“HAY QUE SER PREVENTIVO Y PROACTIVO Y PONER LAS MEDIDAS ANTES DE QUE TE PASE ALGO”

La clave: formación de los empleados

Cuando hablamos de ciberseguridad, siempre surge una pregunta: las empresas que recurren a ella lo hacen por propia convicción... ¿o porque están asustadas y temen lo que pueda pasar? ¿Hasta qué punto se conjuga la concienciación con la preocupación por las consecuencias de un ciberataque?

Mónica Valle lo tiene claro: "Muchas, en parte, están asustadas. Como no existe cultura de ciberseguridad, muchas se asustan porque no saben de estos temas, pero cuando se informan, forman a sus empleados y se ponen las pilas dejan de estar asustadas".

Y esa es, en su opinión, una de las claves esenciales: "Es vital formar a los empleados.Si un empleado sabe que no debe hacer clic en determinados enlaces por email,muchas veces se podrá evitar que se produzca un ciberataque o que sus consecuencias sean demasiado graves".

En el entorno laboral, podemos reducir ese nivel de inseguridad del empleado recurriendo a herramientas que permiten atajar un ataque incluso antes de que llegue a producirse. Las soluciones de ciberseguridad avanzada monitorizan los sistemas de la organización en tiempo real, detectando y deteniendo cualquier comportamiento sospechoso que podría resultar dañino. Prevenir el ataque antes de que ocurra ayudará a reducir el estrés que produce en un empleado ser, efectivamente, víctima de un ciberataque.

"LAS SOLUCIONES DE CIBERSEGURIDAD AVANZADA MONITORIZAN LOS SISTEMAS DE LA ORGANIZACIÓN EN TIEMPO REAL"

Xavier Mertens

EL CRYPTOJACKING ES UNO DE LOS ATAQUES MÁS BRILLANTES QUE HE VISTO

La meta del hacker solía ser destruir o robar información, pero hoy lo que intenta es obtener beneficios a cambio de ella. Vemos cómo se profesionalizan los ataques y se crea un negocio a su alrededor:

Hace unos años no era tan fácil comprar ransomware o alquilar un bot para atacar. Xavier Mertens, consultor de ciberseguridad independiente y bloguero reconocido en el sector de la seguridad informática, insiste en la importancia de la seguridad tradicional para hacer frente a estas nuevas amenazas altamente eficaces. La participación de Mertens como voluntario en el SANS Internet Storm Center, el sistema mundial cooperativo de alertas de ciberamenazas, lo convierte en un profesional conocedor de los ataques de vanguardia.

Descubre Más

PS: **¿Cómo pueden los profesionales del sector adaptarse a las nuevas necesidades?**

Las medidas de protección habituales no dejan de tener importancia. Si los empleados pueden adherirse a las medidas clásicas: implementar una segmentación adecuada, contraseñas seguras, configurar los dispositivos correctamente y no exponer información o herramientas importantes en la web, creo que podrían estar protegidos ante cualquier amenaza moderna.

La mayoría de los problemas de seguridad ocurren porque la gente necesita llevar a cabo sus tareas diarias, y no conocen los planteamientos básicos para solucionarlos. Recientemente intenté escanear un documento y, tras haber revisado credenciales y firewall y verificado que la impresora funcionaba correctamente, me di cuenta de que no funcionaba porque tenía configurado el protocolo Server Message Block version 1 (SMBv1), que ya ha sido ampliamente desaprobado. Por tanto, tienes que decidir si lo habilitas o no. Por lo general, los usuarios habilitarán la configuración predeterminada porque no saben cómo cambiarla o no tienen tiempo para hacerlo y necesitan seguir con su día a día. Pero no es tan complicado, como expertos del sector, solucionar estos problemas básicos y proteger la seguridad de herramientas tan comunes en las empresa como las impresoras.

PS: **¿Qué es el Internet Storm Center? ¿Cuál es tu labor como ISC Handler?**

El Internet Storm Center es una organización cuyo propósito es monitorizar Internet y velar por su correcto funcionamiento. Por medio de herramientas automatizadas, recolectamos información para los profesionales del sector, generamos contenido útil a modo de diario de ciberseguridad e intentamos aumentar la sensibilidad ante el problema. Por ejemplo, con el dshield project permitimos que las personas envíen sus registros de firewall para incrementar nuestra base de datos y construir un sistema de análisis en base a la repetición. Fuimos capaces de detectar el botnet Mirai porque tenemos herramientas que demostraban picos de actividad en puertos específicos. Somos “los bomberos del Internet”.

PS: **¿Cómo podemos evitar ataques recientes como los que tienen como finalidad el minado de criptomonedas?**

La protección sigue siendo la misma que para otro tipo de malware, porque el minado de criptomonedas se realiza con un código malicioso que se ejecuta en tu ordenador. Los consejos básicos: una solución de ciberseguridad que te proteja de forma completa y no clicar o descargar archivos desconocidos. Sin embargo, creo que el cryptojacking es uno de los ataques más brillantes que he visto. Los criminales se están pasando del ransomware a la minería porque es mucho menos intrusivo y no necesitas utilizar tantos recursos para evitar ser detectado.

Con el ransomware no sabes si la víctima pagará el rescate porque podría tener una copia de seguridad de sus archivos. En cambio, con la minería de criptomonedas es seguro que recuperarás el dinero invertido, y es mucho menos invasivo. Se puede ejecutar la minería en cualquier tipo de dispositivo, no está restringido a Windows, Mac o Linux como el ransomware, y el sistema de la víctima seguirá funcionando a pesar del ataque.

Uno de mis compañeros en el ISC estudió la potencia de su ordenador mientras minaba criptomonedas. Los ventiladores y el CPU del ordenador estuvieron siempre ocupados y operando al máximo.

“INTERNET STORM CENTER ES UNA ORGANIZACIÓN CUYO PROPÓSITO ES MONITORIZAR INTERNET Y VELAR POR SU CORRECTO FUNCIONAMIENTO”

Imaginemos las consecuencias que podría tener el minado en una empresa con múltiples ordenadores: crece el consumo de electricidad, tiene un impacto importante en el tráfico al centro de datos y puede incluso aumentar la temperatura de la oficina.

PS: **Tienes un certificado GIAC en ingeniería inversa de malware. ¿Crees que las empresas deberían invertir en este tipo de análisis?**

No creo que se deba invertir en reverse engineering a menos que se disponga de mucho presupuesto y mucho tiempo. El propósito de las empresas no es entender el comportamiento del malware; su meta es volver a la actividad lo antes posible. Al analizar archivos maliciosos, lo que buscamos es saber por qué reacciona de esa manera para generar una lista de indicadores (Indicators of Compromise) para compartirlo con investigadores del sector y ofrecer esta inteligencia a los clientes.

PS: **¿Cómo elaboras un plan de respuesta a incidentes eficaz?**

Los planes de respuesta a incidentes son complicados de abordar, especialmente si se trata de compañías que no tienen los recursos o el personal adecuado. En mi opinión, siempre se puede empezar por cosas pequeñas. El primer paso es estar preparados, aumentar la sensibilidad e involucrar a todos los empleados, y esto lo puede hacer cualquier empresa.

PS: **Ya que se acerca la fecha límite, ¿cómo pueden prepararse las empresas para el cumplimiento del GDPR?**

Con el GDPR lo que se pretende es proteger la privacidad de los usuarios. Tomando en cuenta esto, si has implementado una estrategia de seguridad exhaustiva, si sabes dónde se encuentra tu información y cómo está protegida, y si solo recolectaste la información estrictamente necesaria para tu negocio, el GDPR no debería ser un problema para ti. Este reglamento nos devuelve a las raíces, a los consejos básicos: encripta tu información, no almacenes contraseñas en archivos públicos, no expongas bases de datos en internet... Posiblemente el mayor reto será para las empresas pequeñas que no dispongan de un inventario de toda la información que poseen, no solo datos internos sino también lo que comparten con proveedores y usuarios. Estamos viviendo un proceso de revisión de toda la información que poseen las empresas y esperemos que las empresas hayan tomado las medidas para adaptarse al GDPR. ■

Enrique Ávila

LA CIBERSEGURIDAD NO ES NEGOCIABLE, LA PÉRDIDA DE RECURSOS PUEDE SUPONER EL FIN DE TU EMPRESA

Enrique Ávila tiene una posición y un punto de vista privilegiados: es el director del Centro Nacional de Excelencia en Ciberseguridad (CNEC), un organismo referente en materia de ciberseguridad que integra tres capacidades fundamentales: la universidad como centro generador de conocimiento, las empresas como soporte económico y de innovación y las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) como principales usuarios de tecnologías y conocimiento orientado a la lucha contra el cibercrimen. Nuestro protagonista, por tanto, conoce al dedillo la evolución de la ciberdelincuencia en España, así como los esfuerzos de este país al luchar contra ella y la concienciación (o no) de empresas y ciudadanos al respecto.

Descubre Más

Cuando le preguntamos si estamos en un escenario ascendente, es decir, si los ciberataques van a seguir creciendo en 2018 y 2019, no lo duda un solo segundo: "En 2019, en 2020... Salvo catástrofe tecnológica, el cibercrimen cada vez será más rentable, al menos mientras no varíen las actuales circunstancias: la aterritorialidad del ciberespacio, la seudonimización de los actores y la asimetría de recursos para causar un daño u obtener un beneficio ilícito inducen, sin duda, un crecimiento exponencial de este tipo de actividades".

Ávila no es ajeno a uno de los mayores caballos de Troya de este tipo de delitos: la dejadez o la falta de concienciación. Y es que "la percepción del riesgo es, a la vez, baja y poco entendida, por parte tanto de ciudadanos como de empresas". En su opinión, de hecho, "las empresas han de trabajar la resiliencia y la mitigación de los riesgos".

¿Cómo protege una pyme su ciberseguridad?

En cualquier caso, es evidente que muchas pequeñas compañías difícilmente pueden tener acceso a inversiones en su propia ciberseguridad, de modo que "proteger a las pymes, que son generadoras de la mayor parte de los puestos de trabajo de nuestro país, ha de ser una política de Estado", si bien es cierto que "tanto el Gobierno como el propio INCIBE están realizando un esfuerzo titánico para generar un ecosistema de servicios, de redes de contacto, de acciones de concienciación y cursos de formación, orientados a pymes. Ellas también tienen la responsabilidad de conocer y aplicar estos recursos".

Pero, bajando de lo abstracto, ¿cómo puede proteger su ciberseguridad empresarial una compañía pequeña y con recursos muy limitados? Para el director del CNEC "lo deseable sería tener a un experto que sea el interfaz entre la pyme y los proveedores de servicios de ciberseguridad. Y si el coste es inasumible, siempre resultará más económica –y en líneas generales más segura– la provisión de servicios desde infraestructuras centralizadas, sin minorar por ello los riesgos de uso de estas mismas infraestructuras compartidas en las que, no siendo tú el objetivo de un ciberataque, puedes transformarte en una víctima colateral del mismo".

La ciberseguridad no es opcional

En cualquier caso, el contexto también ha cambiado. Hasta hace poco, la protección de la ciberseguridad empresarial dependía (más o menos) de la libertad y la voluntad de cada empresa. Sin embargo, la definitiva entrada en vigor del GDPR, que impone multas de numerosa cuantía para las compañías que no sean diligentes al tratar su ciberseguridad, ha provocado que la actitud de las empresas tenga que cambiar a la fuerza.

"EL CIBERCRIMEN CADA VEZ SERÁ MÁS RENTABLE, AL MENOS MIENTRAS NO VARÍEN LAS ACTUALES CIRCUNSTANCIAS"

Enrique Ávila lo tiene claro: "La ciberseguridad no es negociable. El cumplimiento normativo en materia de ciberseguridad y protección de datos personales también afecta a las empresas y, les guste o no, en nuestra sociedad actual la pérdida de los recursos de TI significará, con una alta probabilidad, el fin de la empresa, ya sea por continuidad de negocio, por pérdida de reputación, por sanción administrativa o incluso penal, con el coste económico y social que ello representa para nuestro país".

En este sentido, por tanto, el director del Centro Nacional de Excelencia en Ciberseguridad apunta en dos direcciones, la obligatoriedad y la concienciación (también de los trabajadores), ya que cualquier empresa "debe y está obligada a invertir en la protección de su infraestructura TI así como en la capacitación de sus empleados en esta materia, de la misma manera que obtiene muchos de sus beneficios gracias a esa misma infraestructura de TI y al uso eficiente que de ella hacen". ■

"LA PÉRDIDA DE LOS RECURSOS DE TI SIGNIFICARÁ, CON UNA ALTA PROBABILIDAD, EL FIN DE LA EMPRESA"

Pablo González

LA SEGURIDAD 100% NO EXISTE

La tecnología ha evolucionado a un ritmo vertiginoso, y con ella, las oportunidades para las empresas y la sociedad. Pablo González Pérez, Technical Manager y Security Researcher en Telefónica, observa que estos avances también han traído consigo nuevos riesgos y amenazas en el sector de la ciberseguridad.

Pablo, con una amplia experiencia en la industria, es Director del Máster Universitario en Seguridad de Tecnologías de la Información y de las Comunicaciones de la Universidad Europea, Microsoft MVP en los años 2017-2018 y 2018-2019, y escritor de libros como “Ethical Hacking: Teoría y práctica para la realización de un pentesting”.

Discover More

PS:**¿Qué tendencias consideras importantes durante los últimos años en el panorama de la ciberseguridad?**

En mi opinión, estas son las tendencias más relevantes:

• Los delincuentes aprovechan las criptomonedas para lograr un beneficio a través de acciones maliciosas. Hace apenas unos pocos años pasaban inadvertidas.

• La aparición del ransomware y el modelo de negocio que hay detrás ha marcado un antes y un después. También la sociedad ha entendido este tipo de amenaza, ya que se ha dado cuenta de los riesgos en Internet.

• Los casos de robos de datos a empresas. Esto es algo que ha crecido y que, por desgracia, seguiremos viendo en un futuro.

• La aparición del nuevo reglamento de datos para la protección de los ciudadanos.

• Ataques a infraestructuras críticas.

• La aplicación de la inteligencia artificial en el campo de la ciberseguridad. Sin duda, irán de la mano en los próximos años.

• El incremento del conocimiento y la concienciación. Es algo que poco a poco ocurre y se va notando, sobre todo en las nuevas generaciones.

PS:**¿Qué diferencias has visto en el tipo de ataques y de amenazas?**

La principal diferencia es el uso de diferentes tecnologías que han ido surgiendo. Un ejemplo sencillo es el caso del phishing, siempre ha estado ahí, pero hoy en día vemos como debido a técnicas de QRLJacking o al uso de Apps OAuth se da un enfoque distinto al engaño y se consigue el acceso a la cuenta, en estos casos sin necesidad de contraseña. Con cada nueva tecnología que aparece van asociados nuevos riesgos o una evolución de estos.

PS:**¿Es posible prevenir brechas de seguridad recientes como la de Facebook, que expuso la información personal de más de 50 millones de usuarios?**

Hay una frase que muchos profesionales del sector han comentado y es que “todo es hackeable”, es decir, toda empresa puede ser víctima de un incidente de seguridad. Es importante que la sociedad y las empresas tengan este hecho en mente y entenderlo. Implantar medidas de prevención con el objetivo de disminuir el riesgo lo máximo posible es algo vital a día de hoy, pero no todo puede ser preventivo, debe existir una alineación de riesgos entre medidas preventivas y reactivas. La seguridad 100% no existe, por lo que se debe seguir trabajando de forma iterativa en la manera en la que las empresas se protegen, sumar medidas preventivas, alinear reactivas y crear una base en la que las personas de la organización queden involucradas en la seguridad de la organización.

“CON CADA NUEVA TECNOLOGÍA QUE APARECE VAN ASOCIADOS NUEVOS RIESGOS O UNA EVOLUCIÓN DE ESTOS”

PS: **El IoT aumentará los vectores de ataque. ¿Cómo podemos proteger un mundo en el que todo está conectado?**

La protección debe ser compartida entre proveedor y consumidor. En mi opinión, la seguridad no debe ser abordada por un solo rol, ya que en la ecuación tenemos, al menos, dos. Si ambas partes asumen su responsabilidad en la protección de la información estaríamos ante una robustez mucho más asumible en lo que a términos de riesgo se refiere. Por un lado, la inclusión de la seguridad desde la captura de requisitos, desde el diseño de los sistemas es algo que aportaría un grado de madurez al proceso muy interesante.

Es algo que afecta al coste directo de fabricación, pero que a la larga favorece a todos y un retorno que se puede cuantificar. Un ciclo de vida de desarrollo seguro aporta madurez al proceso, es un punto mínimo al que debemos acudir. En cada etapa del proceso se pueden añadir elementos como:

- Captura de requisitos de seguridad.
- Modelado de amenazas.
- Análisis de superficie de ataque.
- Análisis estático y dinámico.
- Revisiones de código.
- Pentesting.
- Testing.
- Fortificación con configuraciones seguras.

Lógicamente, los elementos comentados van apareciendo en diferentes fases de este tipo de metodologías y aportan un valor más que interesante a la creación de software y de sistemas. La idea es sencilla, pensar en la seguridad desde el principio. Por otro lado, cuando el consumidor hace uso de los sistemas debe entender los riesgos y amenazas a los que se expone, simplemente por el hecho de utilizar tecnología. Esto es algo que la sociedad va aprendiendo, aunque no a la velocidad que nuevas amenazas y riesgos aparecen en nuestras vidas.

“CUANDO EL CONSUMIDOR HACE USO DE LOS SISTEMAS DEBE ENTENDER LOS RIESGOS Y AMENAZAS A LOS QUE SE EXPONE”

PS:**¿Crees que los ataques se hacen más complejos o los ciberatacantes se profesionalizan?**

En algunos casos los ataques son más complejos, se explotan vulnerabilidades o se aprovechan fallos más complejos, aunque en otros casos no ocurre lo mismo. En ocasiones pensamos que un incidente de seguridad viene de la mano de una serie de técnicas muy complejas y resulta que entraron por un phishing básico a un empleado o porque alguien extrajo los datos internamente, sin un control adecuado de trazabilidad. Por otro lado, los atacantes también se especializan y saben aprovechar las últimas tendencias con el fin de obtener un beneficio. Esto es algo normal, ya que cada vez hay mayor investigación, más cantidad de información accesible y el volumen de datos en el sector de la seguridad crece cada día.

PS:**¿Consideras prioritario el uso de soluciones de ciberseguridad avanzadas para proteger los endpoints, ya que estos se multiplican? ¿Qué papel crees que jugará la inteligencia predictiva en materia de soluciones de ciberseguridad en los próximos meses o años?**

Si entendemos la ciberseguridad como un modelo en el que se debe proteger cada capa y cada zona, de manera similar a lo que indica un modelo de defensa en profundidad en un entorno militar, toda solución correctamente configurada y que ayude a mejorar la seguridad y disminuir la probabilidad de amenaza o su impacto es prioritaria. Sin lugar a la duda, la inteligencia predictiva ayudará a mejorar las soluciones de ciberseguridad. Se convertirá en uno de los pilares de las herramientas de la industria. La importancia de adelantarse a las situaciones y riesgos será fundamental para una mejora continua de la ciberseguridad.

PS: **Tu especialidad es el pentesting: ¿Qué herramientas utilizas para llevar a cabo los análisis correspondientes?**

Hay que disponer de un conjunto de entornos y herramientas con los que uno se debe sentir cómodo. No son importantes los nombres concretos, sino más bien explorar la necesidad a cubrir y lo que te puede aportar una herramienta concreta en cada momento. Por supuesto, en muchos entornos acabas utilizando las mismas herramientas y la destreza manual. Hay que ir viendo las nuevas herramientas que aparecen y que pueden hacer el trabajo más fácil.

PS:**¿Qué importancia tiene el hacker ético en el mundo empresarial actual?**

El hacking ético es una parte fundamental dentro del mundo empresarial actual. La necesidad de las empresas de sentirse seguras en un entorno digital para poder ejercer su actividad de negocio hace que la aportación del hacking ético sea imprescindible para

“LOS ATACANTES TAMBIÉN SE ESPECIALIZAN Y SABEN APROVECHAR LAS ÚLTIMAS TENDENCIAS CON EL FIN DE OBTENER UN BENEFICIO”

poder ayudar a mejorar dicha seguridad y, por lo tanto, la actividad de negocio.

PS: **También eres docente en el sector de la ciberseguridad. ¿Qué grado de importancia tiene la enseñanza en esta industria?**

La concienciación, el conocimiento, la formación son la base de la cultura de seguridad de cualquier empresa o, al menos, así debería serlo. La seguridad es fundamental para que las organizaciones y los usuarios de Internet puedan realizar sus actividades de forma natural y segura. La enseñanza tiene un papel importante en la industria, que puede venir dada de muchas formas: universidades, empresas privadas, libros, blogs, artículos, revistas, incluso por uno solo, el autodidacta. Es más, en muchas ocasiones uno debe ser autodidacta para asimilar diversos conocimientos, ponerlos en práctica en entornos controlados y poder entender mejor las posibles situaciones, riesgos y amenazas.

La formación a empleados también es una de las bases en la creación de una cultura de seguridad en la organización. Es algo vital para la organización y,

“EL HACKING ÉTICO ES UNA PARTE FUNDAMENTAL DENTRO DEL MUNDO EMPRESARIAL ACTUAL”

seguramente, lo más complejo de conseguir. Apuestas como la gamificación, la innovación y los retos pueden ayudar a hacer que los empleados se conviertan en agentes propulsores de la seguridad en las empresas.

PS:**¿Cómo puede una empresa aumentar su ciberresiliencia? ¿Qué medidas de seguridad son ineludibles?**

Existen diferentes formas, pero la primera es querer ser realmente resiliente. En mi opinión hay algunas cosas a tener en cuenta:

• Disponer de un equipo que responda de forma eficaz y eficiente ante un incidente. Que esté formado y pueda analizar las posibles situaciones y tomar decisiones.

• La utilización de técnicas de predicción e inteligencia son vitales hoy en día para las organizaciones.

• La correlación de eventos y casos permitirá obtener una visión global de la situación.

• Disponer de medidas de recuperación que permita a una organización restaurar a un estado anterior en caso de incidente grave.

Además, no se debe olvidar que disponer del conocimiento dentro de la organización es algo vital. ■

“LA CONCIENCIACIÓN, EL CONOCIMIENTO, LA FORMACIÓN SON LA BASE DE LA CULTURA DE SEGURIDAD DE CUALQUIER EMPRESA”

Panda Security Summit PASS

The European **Cybersecurity** Hub

Vivimos en una sociedad digitalizada. Asistimos a una transformación de las relaciones sociales, del tejido empresarial y de las gestiones de los gobiernos.

Para proteger nuestra vida digital, y la de nuestro negocio, la ciberseguridad se convierte en un requisito de nuestra actividad diaria. Y a su vez, su gestión necesita una revisión profunda, con nuevos modelos de seguridad.

Con el objetivo de descubrir las necesidades, mostrar las tendencias y conocer los puntos de vista de las distintas estructuras que forman nuestra sociedad, en Panda Security celebramos nuestra primera cumbre de de ciberseguridad avanzada el pasado mes de mayo. El Panda Security Summit 2018 tuvo a la ciber-resiliencia como eje central y los CISO y CIO de las grandes empresas españolas y europeas como espectadores entre los más de 400 asistentes.

El evento, presentado por Silvia Barrera, sirvió como marco de análisis de las últimas tendencias en ciberseguridad, tanto de ataque como de protección en todas las fases de la cadena de seguridad, y del estado global del sector, desde el punto de vista de analistas, instituciones públicas y empresas privadas.

A lo largo de todas las conferencias y talleres, los participantes pudieron dar forma a los pilares fundamentales para alcanzar el máximo nivel de seguridad en las organizaciones.

La importancia de ser resiliente desde el punto de vista de la seguridad quedó ampliamente reconocida como característica fundamental, además de ser el leitmotiv del último informe publicado por Panda Security, presentado en el #PASS2018.

Asimismo, todos los ponentes ofrecieron ideas y compartieron su experiencia para prevenir los ataques, conseguir volver al estado original tras los incidentes de seguridad y paliar sus efectos con una buena estrategia de respuesta. El esquema común a todas las estrategias analizadas fue prevención, detección, contención y respuesta.

En este Ebook has podido leer alguna de estas reflexiones de primera mano de los participantes del Summit como Javier Candau, jefe del

Centro Criptológico Nacional (CCN-CERT), que se centró en el desafío que representa la ciberseguridad en España.

Ian McShane, Research Director de Gartner, detalló en su conferencia que el reto para 2019 es reforzar la prevención, especialmente en la estrategia de protección de endpoints. "El endpoint necesita algo más que un antivirus, las herramientas específicas de detección y respuesta (EDR) son la clave, ya que ofrecen una trazabilidad imprescindible para analizar y prevenir. Pero estas no van a sustituir a los humanos, todavía necesitamos la figura del analista", explicó.

Nikolaos Tsouroulas, Head of Cybersecurity Product Management en ElevenPaths de Telefónica, explicó que "la tecnología es necesaria, pero primero están las personas. Los profesionales de seguridad son la mejor inversión en este ámbito".

La jornada también contó con la participación de Nicola Esposito, director del CyberSOC EMEA Center de Deloitte, que destacó factores como la aplicación de plataformas de threat intelligence, la creación de controles de detección de amenazas y la monitorización del perímetro con alertas automatizadas, pero siempre con un papel fundamental del factor humano.

Por último, el director del laboratorio PandaLabs, Pedro Uría, ofreció las claves de la seguridad, protección y resiliencia empresariales en este momento en el que el malware ya no es el problema. En su lugar, los hackers son el reto de futuro de la ciberseguridad, ya que utilizan métodos más complejos. Tras más de 28 años en marcha, Panda Security celebró su primera cumbre sobre ciberseguridad. Una cita ineludible para todos los profesionales de la ciberseguridad y que no puedes perderte en su próxima edición: Panda Security Summit 2019. The European Cybsersecurity Hub!

Descubre más

Ver Video

Más Información:

https://www.pandasecurity.com/business/

Email:

communication@pandasecurity.com