isms forum spain

CSC Cyber Security Center

VIII Foro de la Ciberseguridad

Organizado por el Cyber Security Centre (CSC) de ISMS Forum

- POLÍTICAS DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS
- MEJORAR LA VISIBILIDAD PARA REDUCIR VULNERABILIDADES
- LA CIBER-RESILIENCIA EN LAS EMPRESAS
- LA PRIMERA LÍNEA ANTE EL CIBERCRIMEN…

POTENCIANDO EL ECOSISTEMA DE LA CIBERSEGURIDAD

Normativa, estrategia y tendencias

FIRMA INVITADA
Roberto Baratta (ABANCA)
La década prodigiosa

ENTREVISTA
Evangelos Ouzounis (ENISA)
Directiva NIS

EDITORIAL
Daniel Largacha (MAPFRE)
Bits de hoy, bugs del mañana

Septiembre 2019
www.ismsforum.es

BARCELONA CYBERSECURITY CONGRESS

PROTECTING & ENABLING BUSINESS

CONGRESS

EXHIBITION AREA

TALENT MARKET

CAPTURE THE FLAG

HANDS ON WORKSHOPS

NETWORKING ACTIVITIES

CYBERSECURITY SOLUTIONS FOR DIGITAL TRANSFORMATION

29 - 31 OCTOBER 2019

GRAN VIA VENUE

Fira Barcelona

Bits de hoy, bugs del mañana

DANIEL LARGACHA

Director del Cyber Security Centre

ISMS FORUM

ismsforum.es

Sobrepasamos ya casi los dos decenios del año 2000. Aunque no se han cumplido muchas de las visiones futuristas del cine (tales como Blade Runer, Gattaca o Regreso al Futuro), lo cierto es que la humanidad, de la mano de las nuevas tecnologías, está encarando un punto de inflexión que seguramente será estudiado en el futuro como un momento que supuso el inicio de una nueva era.

Los cambios que se están introduciendo en la sociedad tienen efectos directos en nuestros comportamientos, costumbres y modo de vida. Algunos de estos cambios son visibles, como los coches autónomos (recientemente alcanzado el nivel 3 por alguna marca), las plataformas de servicios digitales, etc.; y otros no lo son tanto para el ciudadano, como el *cloud,* la automatización de operaciones o el IoT en servicios críticos. Todos implican muchos beneficios para la sociedad, pero también una serie de riesgos para los que debemos estar preparados. Volviendo a las referencias cinematográficas, son muchas las ocasiones en las que se enarbolan las ventajas y beneficios de los avances tecnológicos futuribles, pero pocas en las que se pone de manifiesto el contexto novedoso de riesgo al que éstos se encuentran expuestos. Siendo, precisamente, el momento actual un espacio en el que la realidad y la ficción se encuentran, desafortunadamente no estamos en el mejor de los escenarios. A pesar de los avances que se han hecho a nivel empresarial, gubernamental y legislativo en materia de ciberseguridad, la presente situación requiere, más que nunca, una especial atención en la ciberseguridad. Es importante que la tecnología que se está desarrollando para el futuro, y aquella que se está implantando actualmente, disponga de los elementos necesarios que nos permitan dotar de estabilidad y confianza a la sociedad de hoy y de mañana.

Desde hace ocho años, ISMS Forum, desde el área del CSC (Cyber Security Centre), está trabajando para construir un espacio de colaboración e intercambio entre los actores necesarios (institucionales, empresas y profesionales independientes) para tratar de conseguir el objetivo de impulsar la ciberseguridad en la sociedad. Espero que en este VIII Foro de la ciberseguridad tengamos la oportunidad de avanzar entre todos hacia este hito.«

> **La tecnología debe dotar de estabilidad y confianza a la sociedad de hoy y de mañana**

SUMARIO

BARCELONA CYBERSECURITY CONGRESS

29 - 31 OCTOBER 2019
GRAN VIA VENUE

PROTECTING & ENABLING BUSINESS

Don't miss the chance!
Get your pass with our ISMS discount codes:

VISITOR PASS
FREE
DEEDAC2A

CONGRESS PASS
25% disc
4E11E9E5

barcelonacybersecuritycongress.com

isms forum spain

Fira Barcelona

VI Ciberejercicios Multisectoriales

La ciber-resiliencia de las empresas, a prueba

ISMS Forum Spain, en colaboración con INCIBE, llevará a cabo la sexta edición de los Ciberejercicios Multisectoriales, también denominados como "CiberMS 2019". El objetivo es generar concienciación sobre los riesgos en ciberseguridad y fomentar las buenas prácticas entre las grandes organizaciones participantes, que se fundamentan en la evaluación de la resiliencia, la medición del estado de madurez y la mejora de las capacidades de detección y respuesta en materia de ciberseguridad.

Este año las pruebas girarán en torno al reconocimiento, la intrusión, la explotación/movimiento lateral y la exfiltración, evaluando la capacidad de resiliencia ante posibles ataques a sistemas informáticos e infraestructuras críticas, y mejorar su capacidad de respuesta.

La iniciativa es un proyecto del Cyber Security Centre (CSC), uno de los grupos de trabajo de ISMS Forum, que fomenta el intercambio de conocimientos entre los principales actores y expertos implicados en el sector para impulsar y contribuir a la mejora de la ciberseguridad en España. Además, está abierta la participación para aquellas entidades cliente que quieran ser evaluadas. El plazo para presentar la solicitud termina el próximo 15 de octubre (inclusive) y deberá realizarse a través del correo electrónico **coordinacion@ismsforum.es.**

Buenas Prácticas en Virtualización

Informe CCN-CERT BP/15

Teniendo en cuenta el auge de este tipo de tecnologías, el CCN-CERT ha presentado recientemente un amplio informe titulado Buenas Prácticas en Virtualización, que recoge información de referencia acerca de estas tecnologías y los tipos existentes, poniendo una especial atención a las particularidades específicas que surgen en el ámbito de la ciberseguridad.

Tal y como explica en el informe, este sistema de reparto de recursos se hace hoy prácticamente indispensable en un contexto donde la nube es una tendencia imparable. Aunque el mercado ofrece otras muchas alternativas, a lo largo de este estudio se pone el foco en las herramientas XenServer de Citrix, VMware ESXi de Dell, Oracle VM Server, VirtualBox de Oracle e Hyper-V de Microsoft. De hecho, se dedican apartados específicos a estas soluciones, mostrando el modo adecuado para la creación de la máquina y la asignación de recursos, la protección y cifrado, el aislamiento y configuración de las redes, etc.

Además, se incluye también un decálogo de recomendaciones y buenas prácticas genéricas para todo tipo de hipervisores especialmente pensado para asegurar el máximo nivel de seguridad en este tipo de entornos.

Catálogo de Productos de Seguridad TIC

Guía CCN-STIC-105

Recientemente se ha puesto a disposición del público en general la actualización de la Guía CCN-STIC-105. Este documento, que se puede descargar desde la parte pública del portal del CCN-CERT, recoge el Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC), que sirve de referencia a las Administración Públicas. Esta guía recoge un listado de Productos Aprobados (que se consideran adecuados para el manejo de información clasificada) y Productos Cualificados, aquellos que cumplen los requisitos de seguridad exigidos para el manejo de información sensible en el ENS, en cualquiera de sus categorías (Alta, Media y Básica).

En el primero de estos apartados, los Productos Aprobados, se presentan por categorías y se incluyen todos aquellos que han superado con éxito el proceso de inclusión en el CPSTIC descrito en la guía CCN-STIC 102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada.

En cuanto a los Productos Cualificados, están agrupados en función de si son de control de acceso, explotación de la seguridad, monitorización, protección de las comunicaciones, de la información y soportes o protección de equipos y servicios. Se incluyen todos aquellos que han superado con éxito el proceso de inclusión en el CPSTIC descrito en la guía CCN-STIC 106 Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC.

Además, esta actualización incluye diversos apartados, como el proceso de inclusión de un producto CPSTIC, o la revisión de su validez y su exclusión.

Nace CriptoCert Certified Crypto

Primera certificación técnica profesional española de criptografía

CriptoCert es una compañía española focalizada en la difusión, promoción, educación, capacitación y certificación técnica de profesionales en el campo de la criptografía y protección de la información, y su aplicación en el mundo real, con una orientación tanto ofensiva como defensiva.

Esta iniciativa surge de la mano de tres reconocidos expertos en el campo de la seguridad informática y la criptografía: Jorge Ramió y Alfonso Muñoz (Criptored) y Raúl Siles (DinoSec), todos ellos con una larga trayectoria ampliamente reconocida. Juntos han creado la primera certificación técnica profesional en criptografía y protección de la información, CriptoCert Certified Crypto Analyst, reconocida por el Centro Criptológico Nacional (CCN).

CriptoCert, en colaboración con ISMS Forum, pone a disposición de sus miembros asociados un descuento del 15% sobre el precio oficial de esta innovadora capacitación mediante el código **CRIPTOCERTISMS2019.** Más información ingresando en: www.criptocert.com

Certificación de ciberseguridad

Refuerzo de ENISA en el marco de la UE

En el contexto de la Ley de Ciberseguridad (CSA, *cybersecurity act*), que entró en vigor en junio de 2019, una de las funciones clave reservada para ENISA es la de ayudar en la preparación de los esquemas de certificación de ciberseguridad candidatos. Al hacerlo, ENISA necesita interactuar tanto con los Estados miembros de la UE como con las partes interesadas de la industria, para recopilar opiniones y consejos y así alimentar los esquemas candidatos.

Esta iniciativa tiene como fin el de obtener un marco común de certificación de ciberseguridad en toda la UE, mejorando la capacidad de consumidores y gobiernos para adquirir productos, servicios y procesos de ciberseguridad en el ámbito de las TIC. Además de proporcionar niveles de garantía calificados, se espera alcanzar un grado de ciberseguridad acorde con el perfil de riesgo de la aplicación involucrada. Al mismo tiempo, se busca ayudar a la industria que opera en el mercado interno de la UE, beneficiándose de este marco y produciendo mejores resultados que resistan la competencia global.

Seguridad en las comunicaciones

Cooperación e intercambio de información

A partir del pasado mes de julio 2019, Europa cuenta con más de 414 equipos de respuesta ante incidentes en Europa. Son los denominados CSIRTs, National Computer Security Incident Response Teams. Estos equipos, que trabajan juntos para responder a los ataques cibernéticos, necesitan utilizar canales de comunicación seguros y confiables para compartir información sobre amenazas e incidentes de seguridad, mientras se protege a los ciudadanos y las empresas europeas.

Con una serie de incidentes de ciberseguridad y una superficie de ataque que aumenta cada día, cada vez es más importante poder contar con soluciones de comunicación seguras, completas y escalables, que permitan mejorar la cooperación operativa, así como la preparación y el intercambio de información.

Publicado por ENISA, European Union Agency for Cybersecurity, este documento sirve como punto de partida para que las comunidades de respuesta a incidentes realicen su propia evaluación y vean cómo las diversas herramientas de comunicación pueden adaptarse a diferentes tamaños y necesidades. Aunque el documento sigue una metodología para evaluar las soluciones más conocidas, explícitamente no proporciona resultados que puedan reutilizarse, sí puede servir como punto de partida para que otras comunidades puedan llevar a cabo su propia evaluación y vean cómo estas herramientas pueden adaptarse a diferentes tamaños y necesidades.

European Union Agency for Cybersecurity (ENISA)

Secure Group Communications For Incident Response And Operational Communities.

ENTREVISTA

La GDPR es una verdadera historia de éxito europea

Evangelos Ouzounis
Head of Unit – Secure Infrastructures and Services, ENISA

Evangelos Ouzounis cuenta con una amplia experiencia en la Comisión Europea. De forma previa a su entrada en ENISA, trabajó en la *DG Information Society and Media (DG INFSO)* en torno a la estrategia y políticas de I+D para garantizar la seguridad de las infraestructuras y servicios de Europa. Además, fue también cofundador del *Electronic Commerce Centre of Competence (ECCO)* en el *Fraunhofer Institute for Open Communication Systems* en Berlin. En la actualidad es el responsable de implementar el plan de acción CIIP y contribuir al desarrollo de la plataforma NIS.

¿Cuál es el papel de ENISA con respecto a la ciberseguridad en Europa?

La agencia tiene ya unos catorce años. Su objetivo principal es ayudar, tanto a los gobiernos como a miembros del sector privado, a estar más preparados, desarrollar estrategias de ciberseguridad, hacer ejercicios y simulaciones y a implementar mejores prácticas tanto a nivel técnico como no técnico.

De este modo nuestra agencia actúa antes de los incidentes de ciberseguridad, y también después de que se produzcan, para ayudar a sacar conclusiones de lo ocurrido y prepararse para el futuro. Pero no actuamos durante esos incidentes. Ayudamos a la comisión y a los estados miembros a implementar la legislación europea en cuestiones de ciberseguridad, como por ejemplo la directiva NIS y otras.

Por otro lado, nos dedicamos también a desarrollar mejoras prácticas en muchas áreas importantes, como por ejemplo la Estrategia Nacional de Ciberseguridad. Para ello trabajamos en las áreas de IoT y también en lo relativo a cloud.

Esta es una gran parte de nuestro trabajo: identificar problemas y áreas, así como generar mejores prácticas y recomendaciones para decirles a los miembros qué hacer. Además, también debemos servir de inspiración para dar pasos futuros.

Por último, tenemos también una tercera área, en la que trabajamos con los stakeholders en cuestiones más prácticas. Voy a dar dos ejemplos:

Uno es Cyber Europe, un gran ejercicio paneuropeo que realizamos cada dos años con los estados miembros. Es un gran proyecto que tiene mucho reconocimiento.

El otro ejemplo son las formaciones que impartimos. Realizamos muchos cursos, principalmente para instituciones del sector público, en los que les ayudamos a mejorar en aspectos concretos.

Nuestro papel no es el de actuar como expertos, sino el de ser facilitadores del proceso. Identificamos a los stakeholders y los reunimos. Desarrollamos comunidades y trabajamos con ellos para identificar problemas, y luego, con estos problemas como base, desarrollamos mejores prácticas muy centradas en resolver esos retos en concreto. Y, lógicamente, aprovechamos este conocimiento y el expertise ganado para comunicárselo a todos los demás stakeholders.

¿Cuáles son las actividades habituales de ENISA?

A grandes rasgos, nos basamos en un programa anual

de trabajos, que se desarrolla en consenso con los países miembros y normalmente nos centramos en la ejecución de este programa. Hace poco recibimos un nuevo mandato que describe algunas acciones adicionales y ahora mismo estamos esperando que la nueva Comisión Europea nos de ideas y direcciones adicionales. Estos son los tres pilares que definen nuestro día a día.
Tenemos un presupuesto de operaciones, que es el que utilizamos para realizar los proyectos, contratar a terceros, etc. Naturalmente, cuando hay peticiones o nuevas prioridades por parte de los estados miembros, respondemos de la mejor forma posible, en base al presupuesto y los recursos humanos disponibles.

¿Cuál es la preocupación actual de los estados miembros?
Pues, hace unos meses, tanto la comisión como los estados miembros nos pidieron que les ayudáramos con 5G. Querían conocer la situación actual y contar con más información acerca de las herramientas necesarias. Aunque esto no estaba previsto en nuestro programa inicial de trabajo, consideramos que es una gran prioridad. De este modo, hemos cambiado el programa y hemos asignado recursos internos hacia este tema, a fin de ayudar a los gobiernos.

¿Cuál es el estado de preparación de los países y las empresas para resistir un ciberataque?
Este es un área que está en evolución constante. Continuamente se están produciendo nuevas amenazas y vulnerabilidades. Pero a lo largo de los últimos cinco a diez años, los estados miembros han tomado conciencia de la importancia de esta área. Y lo mismo ha ocurrido en el sector privado. Hablando de sectores, hay algunos que son más maduros que otros, por ejemplo, el sector financiero está entre los más avanzados.
Por otro lado, en cuanto a los países, hay algunos que dependen más de sus infraestructuras digitales, como puede ser cloud, redes o similares. Eso significa que, naturalmente, hay intereses y necesidades distintas, así como prioridades diferentes. Tomemos Grecia y España, por ejemplo, en los que el turismo es extremadamente importante. Habrá otros países europeos que no tengan esa prioridad.

> **Nuestro papel no es el de actuar como expertos, sino el de ser facilitadores del proceso**

¿Cómo ha impactado la GDPR el área de la ciberseguridad?
La GDPR es una verdadera historia de éxito europea. Europa demostró un claro liderazgo en este tema y produjo una legislación realmente importante que define toda una serie de elementos importantes. También ayuda a los usuarios a hacer valer sus derechos y define los procedimientos que han de seguir las compañías a la

CIBERSEGURIDAD Y ELECCIONES

Muchos países están preocupados por las interferencias que se pueden producir en las elecciones, pero esto es algo que ENISA no trata normalmente. Según nos cuenta Evangelos Ouzounis, en el pasado ayudaron a los países analizando el problema y han dado algunas soluciones. De hecho, existe un documento público online, publicado por Estonia, en el que participaron otros países.

Es cierto que, tanto la Unión Europea como los estados miembros estaban un poco preocupados antes de las elecciones europeas, pero todo salió bien y no hubo problemas. De todas formas, la mayoría de los países no tiene sistemas de votación electrónica, sino que usan medios tradicionales. Aun así, naturalmente hay muchos ordenadores y sistemas electrónicos involucrados en el recuento, pero no dependemos de las máquinas per se.

hora de tratar los datos personales de los usuarios.

La relevancia de esta legislación ha hecho eco en otros continentes, como por ejemplo los Estados Unidos, en los que están considerando iniciativas similares. Pero también ha servido como inspiración para muchos otros países. Sin duda, es algo de lo que Europa puede estar orgullosa.

¿Con GDPR solo se mejora la privacidad o también la seguridad?

Es evidente que la GDPR ha mejorado sustancialmente la privacidad, porque ahora hay procedimientos mucho más claros y mejor definidos sobre cómo manejar los datos personales. Pero la privacidad y la seguridad están muy relacionados. Debido a que las empresas, ahora, gestionan mejor la información de sus usuarios, clientes y empleados, esto también ha afectado a la seguridad de sus operaciones hasta cierto punto.

> “Nuestro trabajo es identificar problemas y áreas, así como generar mejores prácticas y recomendaciones

Háblenos un poco de la Directiva NIS

Esta es otra pieza legislativa muy significativa, seguramente una de las más importantes de la Unión Europea con respecto a la ciberseguridad. Es un esfuerzo muy

> “La directiva NIS busca conseguir unas condiciones más o menos igualadas en todos los países

ambicioso para conseguir unas condiciones más o menos igualadas en todos los países, de modo que tengan unas características básicas. Por ejemplo, una autoridad competente para todas las cuestiones relacionadas con NIS. También se les pide a los miembros que desarrollen una estrategia nacional de ciberseguridad, y define a muchos sectores que deben ser considerados como críticos, solicitando a los países miembros que identifiquen a los operadores de ese país, que estén activos en esos sectores.

Es un conjunto interesante de ideas innovadoras que entraron en vigor hace casi tres años y, realmente, ha supuesto un reto para los estados miembros a la hora de implementarlas. Pero he de decir que los países han respondido muy bien y ahora tenemos un muy buen entendimiento en torno a lo que supone. De hecho, la implementación avanza a buen ritmo y sin problemas.

La directiva NIS ayuda a los estados miembros a estar equipados y preparados para responder ante incidentes a gran escala. Por esto motivo se ha creado el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, Computer Security Incident Response Team), así como una autoridad nacional competente en la materia.

Las distintas autoridades nacionales están diseñadas para poder cooperar de forma eficaz, intercambiando información relativa a posibles riesgos de seguridad. Como ya he apuntado antes, la idea es proteger los sectores estratégicos de un país que dependan de forma importante de las TIC como, por ejemplo, el energético, el de transporte, el financiero o el de salud.

Las empresas más importantes de estos sectores (que se denominan “operadores de servicios esenciales”), deben aplicar las medidas de protección previstas en la directiva e informar a los gobiernos nacionales si se produce un incidente de seguridad que se pueda considerar como grave.

¿Cómo ve la ciberseguridad dentro de cinco años?

Bueno, tanto nuestras sociedades como nuestras economías van a depender cada vez más de la TI y de las TIC. Veremos nuevos modelos de negocio y redes de comunicación más rápidas, un ejemplo claro es 5G. Asimismo, es muy probable que convivamos con los coches conectados y con muchos más dispositivos in-

teligentes, especialmente en el área de IoT (smart meter, etc.).
Todas estas nuevas innovaciones obviamente están conectadas, hablan entre sí e intercambian información. Al tratarse de hardware y software son, por definición, vulnerables. Así que creo que habrá más crisis o incidentes, ya sean maliciosos o no. Y eso nos va a mantenernos muy ocupados. Pero, a la vez, estamos mejorando en la respuesta a todas estas cuestiones, de modo que estaremos más preparados.

¿Cómo evolucionará el papel de ENISA?
ENISA definitivamente ha sido reconocida como una agencia importante a nivel europeo y ahora tenemos un mandato permanente, lo que quiere decir que vamos a continuar trabajando de forma indefinida.
Hemos recibido más recursos y ahora también disponemos de un mandato para certificaciones, que es un área muy importante. Otro campo en el que vamos a incrementar nuestros esfuerzos es en la cooperación internacional, por ejemplo, con otras agencias fuera de la Unión Europea.
Resumiendo, creo que los países miembros van a seguir confiando en ENISA, y también se van a seguir ampliando nuestras responsabilidades. «

> **Habrá más crisis o incidentes, maliciosos o no, pero estamos mejorando en la respuesta a todas estas cuestiones**

Evangelos Ouzounis participa en este VIII Foro de la Ciberseguridad a través de una ponencia titulada Enhancing The Security Of Eu"S Critical Information Infrastructures - The Nis Directive.

Ataques contra el sector financiero

Informe State of the internet / Security

Recientemente hemos publicado una nueva edición del informe *State of the internet / Security,* en esta ocasión enfocado a las empresas de servicios financieros. Ya se trate de *phishing,* abuso de credenciales, DDoS u otro tipo de herramienta, el dinero es el objetivo de la gran mayoría de los ataques. Todo el ecosistema se basa en eso. Es muy importante prestar atención a estos ataques porque las tácticas, herramientas y procedimientos se ampliarán a otros objetivos si muestran signos de éxito.

La cantidad de dispositivos que requieren conectividad El sector de los servicios financieros siempre ha sido un blanco prioritario para los ciberdelincuentes. De hecho, las herramientas empleadas para atacar a este tipo de empresas forman parte de un amplio ecosistema delictivo. En el informe *State of the internet / Security* ofrecemos una visión global de los ataques perpetrados contra bancos, cooperativas de crédito, empresas comerciales y otras organizaciones que conforman el sector financiero. Estos son algunos de los ataques detectado por el equipo de investigación de Akamai en este tipo de organizaciones.

» ATAQUES DE REFLEXIÓN SYN-ACK

En marzo de 2019, varias organizaciones de servicios financieros comenzaron a ver ataques DDoS utilizando paquetes TCP SYN-ACK para inundar sus centros de datos. Este no es algo común debido a su impacto limitado en el objetivo.

Una mayor investigación sobre estas iniciativas, la cantidad y el tipo de los objetivos afectados, y los efectos secundarios derivados de este tráfico, derivo en una interesante conclusión: uno de los posibles objetivos podría ser dañar la reputación de las herramientas y de los fabricantes, al hacer que las organizaciones de servicios financieros sean identificadas falsamente como malos actores.

Si examinamos un poco más de cerca dos factores que diferencian estos ataques concretos de las inundaciones SYN-ACK anteriores ¿Eran los bancos el objetivo o tenían estos ataques una intención completamente diversa?

» *CREDENTIAL STUFFING*

Se trata de un ataque muy común. Consiste en la inyección automatizada de nombres de usuario y contraseñas, obtenidos mediante filtraciones, en sistemas de autenticación como los formularios de inicio de sesión.

Los atacantes, a menudo, utilizan aplicaciones *all-in-one* (AIO) para automatizar el *credential stuffing* a escala, lo que facilita considerablemente la preparación y puesta en marcha de estos ataques.

En este informe, Akamai analizó 18 meses de datos relativos al *credential stuffing,* desde noviembre de 2017 hasta abril de 2019. Observamos 57.970.472.311 intentos de inicio de sesión maliciosos, de los cuales un total de 3.547.533.230 se produjo contra organizaciones de servicios financieros. A escala mundial, Estados Unidos fue el primer país de procedencia de los intentos de inicio de sesión maliciosos en el sector financiero, seguido de China, Malasia, Brasil y Alemania.

PHISHING

Los ataques de *phishing* es otro de los segmentos importante en cuanto a los dirigidos a entidades financieras. Entre el 2 de diciembre de 2018 y el 4 de mayo de 2019, Akamai detectó 197.524 dominios de *phishing.* De ellos, el 66% tenía como objetivo a consumidores, mientras que las empresas fueron el blanco del 34%. En los dominios de *phishing* que tenían como objetivo a los consumidores, las organizaciones financieras eran el blanco principal.

Por otra parte, Akamai registró 4.460.367.847 ataques web en todos los sectores durante el mismo periodo (18 meses). Algo más del 9 % (411.409.583 de los ataques) afectó al sector de servicios financieros. No obstante, este sector representa el 14 % de los objetivos únicos durante este período. A pesar de que el volumen general de los ataques web está creciendo, el número de aquellos que están dirigidos al sector de los servicios financieros permanece relativamente estable.

TIPO DE ATAQUES

La mayoría (94%) de los ataques que observamos durante este período se llevó a cabo mediante uno de estos cuatro métodos: inyecciones SQL (SQLi), inclusión de archivos locales (LFI), secuencias de comandos en sitios cruzados (XSS) o inyecciones OGNL mediante Java. De hecho, de este último, suponen más de ocho millones de intentos durante estos 18 meses. Este gran volumen nos recuerda que los ataques contra Apache Struts siguen siendo una opción muy popular entre los ciberdelincuentes que tiene al sector financiero entre sus objetivos prioritarios.

En cuanto a los de tipo DDoS, se efectúan a menudo como maniobras de distracción para lanzar ataques de *credential stuffing* o para aprovechar alguna vulnerabilidad. En este periodo de recopilación de datos, Akamai observó más de 800 de estos ataques contra el sector de servicios financieros (más del 40 % de los objetivos únicos). Las inundaciones SYN, RESET y TFTP, así como las de fragmentos TCP, representaron los tipos de ataques DDoS más frecuentes.

Por último, destacar también que los mecanismos de autenticación suelen ser objetivo de estos ataques, lo que significa que los autores normalmente actúan contra API o aplicaciones de inicio de sesión. En este punto es importante destacar que las instituciones financieras utilizan el protocolo abierto de intercambio financiero (OFX) para gestionar los datos por sí mismas, o bien para enviarlos a aplicaciones de terceros. A pesar de que la versión 2.2 se ha convertido en el estándar de facto, muchas entidades todavía procesan los datos con versiones antiguas y menos seguras, algo que hay que corregir.

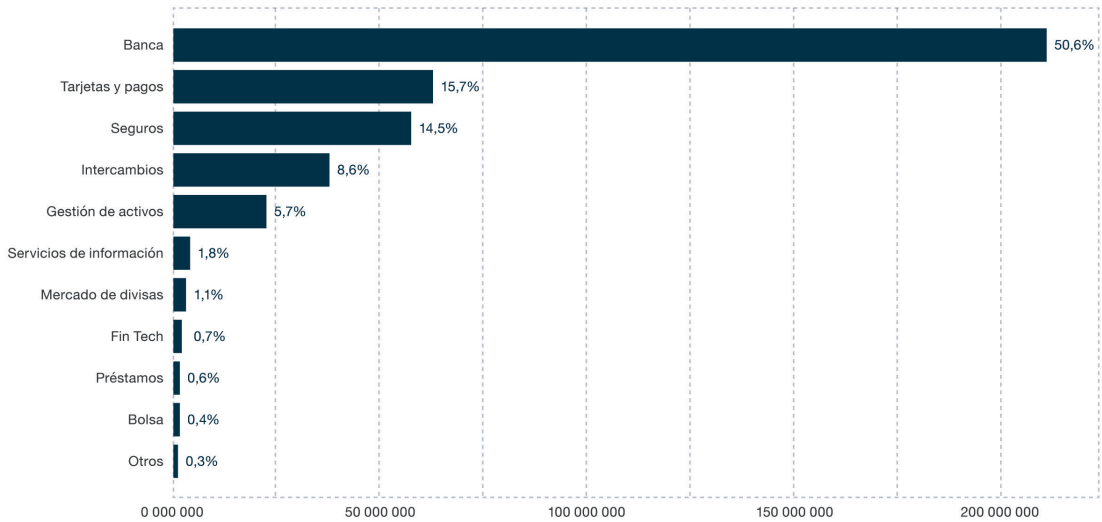
MARTIN MCKEAY

Editorial Editor

AKAMAI

akamai.com

Número de ataques contra servicios financieros



Visibilidad para mejorar el control

Insider Threat Management

La aplicación de técnicas como la inteligencia artificial y *machine learning* otorgan a la fase de visibilidad un valor adicional durante el perfilado, ya que permiten proporcionar mucha más información acerca de todos estos dispositivos de la que se recogía con las soluciones tradicionales, y de una forma mucho más precisa. Además, las capacidades nativas de la nube permiten compartir la inteligencia adquirida localmente, mejorando la visibilidad de manera global.

La cantidad de dispositivos que requieren conectividad a la red sigue creciendo exponencialmente con el paso del tiempo. De hecho, este nivel de evolución viene a coincidir perfectamente con las predicciones realizadas por Gartner a principios de este año. Este analista indicaba que, para el próximo año 2020, se esperan tener en torno a 20.000 millones de dispositivos IoT conectados. Teniendo en cuenta estas cifras, la protección de todos estos dispositivos será clave para poder garantizar la seguridad en un buen número de escenarios, además de proteger también la evolución del negocio cuando se utilicen todos estos nuevos equipos en las empresas.

» ISLAS DE DISPOSITIVOS

Una práctica habitual que se ha venido desarrollando durante los últimos años en las empresas ha consistido en ir conectado a la red estos dispositivos de forma indiscriminada, siguiendo las necesidades personales de cada departamento, haciendo caso omiso a los procesos internos ya definidos.

Un ejemplo habitual suelen ser sensores de temperatura y luminosidad, que se utilizan para racionalizar el consumo y conseguir ajustarse a los requisitos ambientales de forma óptima. Estos sensores, a menudo, son adquiridos a través de canales habituales, aunque únicamente se han analizado las funcionalidades que ofrecen.

El pero, y las incertidumbres, aparecen cuando se llega al paso de la seguridad. Muy posiblemente se traten de sensores basados en elementos de bajo coste, como un *gateway* de comunicación WiFi o Ethernet con sistemas centrales de gestión. Es ahí donde pueden residir los primeros problemas que deben considerarse y analizarse.

LA CLAVE ESTÁ EN LA IDENTIFICACIÓN

Para poder proteger la red debemos saber inicialmente a qué nos enfrentamos y es ahí donde la identificación de todo elemento que está integrado en la red corporativa cobra una especial importancia.

La identificación de los dispositivos que están conectados debe llevarse a cabo en la fase de autenticación en la red. De esta forma, las soluciones de tipo NAC *(network access control)* serán las que nos permitan, en una primera fase, aplicar políticas de seguridad basadas en el contexto proveniente de la fase de visibilidad. Es lo que se denomina *context aware security.*

Durante este proceso, las soluciones deben contar con mecanismos proactivos y automáticos para llevar a cabo dicho análisis de la red para, de esta forma, descubrir todos los elementos que estén conectados, ya sean en conexiones cableadas, inalámbricas (WiFi, gateways IoT, etc.) o incluso a través de terminadores VPN.

En esta fase de descubrimiento encontraremos dispositivos muy habituales, como pueden ser los ordenadores de los propios empleados con sistemas operativos más frecuentes (Windows, MacOS, Linux), así como otros elementos comunes en este tipo de espacios como pueden ser impresoras, teléfonos, *tablets,* etc.

Es importante destacar que en este proceso de identificación de dispositivos conectados debemos conocer la mayor información posible, tanto del equipo como del contexto que lo rodea: *switch* y puerto de conexión, sistema operativo, versión, análisis de puertos abiertos, usuario logado en el sistema, aplicaciones instaladas, etc.

Esta información será muy útil, y totalmente imprescindible, a la hora de ejecutar una fase de protección totalmente efectiva. Esto es lo que nos permitirá personalizar el modelo de seguridad, pudiendo aplicar políticas específicas en función del dispositivo conectado, su ubicación dentro de la organización e, incluso, en función del usuario que lo esté utilizando en cada momento.

COSAS CONECTADAS

¿Pero, qué pasa con el sensor de temperatura que hemos utilizado en el ejemplo anterior? Todos estos dispositivos que entran en el rango de lo que se conoce por IoT pueden contener una serie de elementos de conectividad genéricos y las firmas tradicionales pueden llegar a no ser suficientes.

En estos casos se debe contar con una solución que permita identificar a todos estos dispositivos en función del comportamiento que tienen. En base al tipo de dispositivo que hayamos identificado en cada caso —bien haciendo uso de técnicas tradicionales basadas en atributos estáticos o utilizando atributos dinámicos provenientes de su comportamiento— estas soluciones permiten establecer una fase de control donde podremos construir una serie de reglas que controlen determinados parámetros, como pueden ser el origen, destino y protocolos, así como otra información de valor: la frecuencia de la comunicación, o las aplicaciones y servicios que se puedan utilizar.

ATRIBUTOS DINÁMICOS

Además, utilizar técnicas de *machine learning* e inteligencia artificial en esta fase de visibilidad nos puede ayudar a obtener información de contexto muy interesante. Es la conocida como atributos dinámicos. A través de ellos será posible obtener una identificación completa, y mucho más precisa, de los dispositivos identificados.

En el caso del sensor de temperatura que usa un *gateway* de comunicación WiFi, por ejemplo, puede estar basado en un elemento genérico del mercado que pueda tener un sistema operativo como puede ser Linux. En este caso, el sistema permitirá analizar que este dispositivo se conecta a un sistema de gestión central y proporciona métricas usando una serie de puertos y protocolos específicos. De esta forma, se puede crear así una firma dinámica concreta para este comportamiento. Por tanto, la política de seguridad será especifica para él, usando dichos datos y no solo las firmas estáticas que se utilizaban de forma habitual hasta ahora.

> Es especialmente importante la identificación de todo elemento conectado a la red corporativa

Se puede dar el caso de que se conecte a la red un nuevo dispositivo IoT, como puede ser una cámara de *video vigilancia,* pero que usa el mismo *gateway* y cuya firma es la misma, también basada en atributos estáticos. Lógicamente, este elemento tiene una dedicación totalmente distinta a la anterior y utiliza atributos dinámicos que se podrán identificar mediante su comportamiento. Este dispositivo cursa un tráfico con protocolos de *streamimg,* por lo que se perfilará como Cámara CCTV y se aplicará una política de seguridad específica para este tipo de dispositivos.

> Los atributos dinámicos permiten obtener una identificación completa, y mucho más precisa, de los dispositivos identificados

RAFAEL DEL CERRO FLORES

Cyber Security Systems Engineer Southern Europe

ARUBA

arubanetworks.com

Seguridad en el ámbito de *cloud*

Obligaciones y responsabilidad compartida

La adopción de la nube ofrece muchas ventajas, pero también presenta nuevos retos de seguridad. Cuando una empresa pone su TI en manos de un tercero, le cede parte de estas responsabilidades, lo que puede dar lugar a conceptos erróneos sobre el papel que desempeñan los usuarios en la seguridad de sus aplicaciones. En consecuencia, los proveedores *cloud* utilizan un modelo de responsabilidad compartida para aclarar las obligaciones de cada parte.

Los proveedores *cloud* hacen lo posible para garantizar que proporcionan una plataforma segura para el desarrollo y alojamiento de aplicaciones, pero los clientes siguen teniendo la obligación de asegurar sus propias implementaciones. Un modelo de responsabilidad de seguridad compartida es un marco para ayudar a los clientes a comprender sus obligaciones al utilizar sus servicios. Algunos controles son responsabilidad exclusiva del proveedor, mientras que otros lo son del cliente. La responsabilidad de muchos controles depende del tipo de servicio de nube (IaaS, PaaS o SaaS), a mayor control se delegue en el cliente mayor grado de responsabilidad sobre la seguridad. Tanto AWS como Microsoft y Google proporcionan algún modelo de responsabilidad compartida en el que el cliente es responsable de la protección de sus cargas de trabajo.

Según Gartner, las cargas de trabajo de los servidores en *datacenters* híbridos requieren una estrategia de protección diferente a la de los dispositivos orientados al usuario final. Esto se debe a la naturaleza de las aplicaciones en la nube y a la incompatibilidad de los agentes de ejecución diseñados para servidores locales. Los controles de protección de la carga de trabajo recomendados por Gartner no se proporcionan en los modelos de seguridad compartida de estos proveedores. El diseño real de la aplicación de estos controles es responsabilidad de la empresa.

Estas son algunas de las estrategias de seguridad que se pueden utilizar para reducir el riesgo:

- **Aislamiento de recursos.** Separar los recursos en secciones individualmente comprobables y asegurables ayuda a reducir los vectores de ataque y las vulnerabilidades.

- **Aislamiento de redes y aplicaciones.** La utilización de listas de control de acceso a la red (NACL) y los grupos de seguridad (GS) permiten un control granular de activos y reducen la superficie de ataque. Los flujos de datos entre componentes siempre deben grabarse y analizarse para detectar actividades sospechosas, incluidas las conexiones no autorizadas entre aplicaciones, como los ataques *man-in-the-middle* o las anomalías de red (DDOS, virus, explotación de vulnerabilidades).
- **Seguridad de Contenedores.** Los contenedores reducen los vectores de ataque al exponer sólo el servicio requerido. Los orquestadores —como Kubernetes, Mesos o Docker Swarm— proporcionan los medios para aislar aún más las cargas de trabajo a través de permisos, permiten una alta disponibilidad a través de la programación y distribuyen eficazmente la carga entre los *masters.* Hay ofertas nativas en nube nativa que aprovechan el mismo modelo de código abierto de Kubernetes, y son capaces de abstraer de la gestión de la infraestructura. La elección de estos modelos requiere un cierto bloqueo del proveedor de la nube pero, a cambio, reduce la sobrecarga de gestión y los posibles errores de configuración.
- **Microsegmentación.** Con la microsegmentación, cada aplicación se convierte en un componente interdependiente. Las aplicaciones de microservicio encajan perfectamente en redes y contenedores segmentados. La utilización de ambos diseños asegura que el modelo pueda ser flexible con la carga y el cambio de entorno, por ejemplo, durante un aumento repentino o un desastre. Además, reduce la exposición. Si un solo servicio está comprometido, un atacante tiene vectores muy limitados para invadir la arquitectura total, lo que permite una resolución más rápida.
- **Cifrado de datos.** Los tres proveedores líderes de la nube soportan el cifrado del lado del servidor y del cliente. En la encriptación del lado del servidor, el proveedor cifra los datos de un cliente en su nombre después de recibirlos, mientras que en la encriptación del lado del cliente es éste el que cifra sus datos antes de transferirlos a su servicio en la nube. Azure, GCP y AWS proporcionan la capacidad de cifrar volúmenes de datos en los servidores, mientras que el uso de cifrado en tránsito requiere el diseño de la integración de certificados en servicios que utilizan protocolos seguros, como TLS o SSL.
- **Actualizaciones y parches regulares.** En IaaS, el cliente asume toda la responsabilidad de mantener actualizado cada SO del *host.* Sin embargo, pueden reducir su carga de seguridad utilizando los servicios totalmente gestionados de su proveedor. Por ejemplo, podría aprovechar las opciones de *database as a service* (DBaaS) para alojar sus bases de datos relacionales. Las empresas que utilizan hosts de servidores deben aprovechar la gestión de parches AWS cuando sea posible.
- **Herramientas DevOps.** Los principales proveedores ofrecen sus propios servicios internos, como AWS CloudFormation, Azure ARM Templates y Google Cloud Deployment Manager. Si las aplicaciones se alojan en un entorno híbrido, es importante buscar soluciones de código abierto y de terceros que funcionen tanto en la nube pública como en la infraestructura local. Además, el uso de cualquiera de estas tres herramientas probablemente implique bloqueo con el proveedor de la nube. No son propicios para la gestión multi-nube o, si es necesario, para la migración.
- **Monitorización de la carga de trabajo.** Una variedad de diferentes herramientas de monitorización está disponible para el cliente a medida que asumen su papel en un modelo de responsabilidad compartida: las soluciones de monitoreo y gestión de inventario, servicios de control de aplicaciones y de costes o plataformas de protección de cargas de trabajo en la nube (CWPP) .
- **Defensas tradicionales.** Estas herramientas siguen teniendo un papel que jugar, pero el diferente entorno de aplicación que supone la nube implica que deben implementarse de una nueva forma. Esto puede requerir la creación de *scripts* o la automatización para mantener una visibilidad completa sobre una compleja serie de elementos móviles.

AVISHAG DANIELY

Director of Product Management

GUARDICORE

guardicore.com

> **Se requieren nuevas herramientas, capaces de monitorizar entornos segmentados y el tráfico de red entre ellos**

CONCLUSIÓN

El nuevo paisaje de nube de microservicios distribuidos e infraestructura dinámica ha desplazado el énfasis de la prevención de intrusiones desde el perímetro exterior hacia las cargas de trabajo individuales. Esto requiere nuevas herramientas de seguridad, capaces de monitorizar entornos segmentados y el tráfico de red entre ellos. Al mismo tiempo, las cargas de trabajo de TI son cada vez más móviles, lo que permite elegir dónde alojar las aplicaciones en función del rendimiento, el coste y los requisitos de cumplimiento. Como resultado, se necesitan herramientas con capacidades híbridas y multi-nube para garantizar una visibilidad completa en todos los entornos.

Pero para utilizar las herramientas de seguridad de forma eficaz, los clientes también necesitan entender sus responsabilidades compartidas en la nube. Este conocimiento podría marcar la diferencia entre un entorno informático seguro y las consecuencias potencialmente devastadoras de un ataque malicioso.

PEDRO VIÑUALES

VP Global Presales

CYTOMIC

cytomicmodel.com

Políticas Zero trust

Usuarios, máquinas y procesos

A finales de 2018, el analista Gartner indicaba que más del 50% de los fabricantes de dispositivos IoT no podrán enfrentarse eficazmente a las amenazas procedentes de una práctica de autenticación débil. Además, según señala PandaLabs, a lo largo de este año 2019 se han incrementado los ataques sin *malware.* Este tipo de ataques son más difíciles de detectar y responden a nuevas y más avanzadas tácticas utilizadas por los ciberdelincuentes actuales, que realizan ofensivas dirigidas con *malware* propietario, utilizan aplicaciones legítimas y *goodware.*

En este escenario, el empeño primordial debería ser la detección de comportamientos sospechosos que puedan desarrollarse en usuarios, máquinas y procesos. De hecho, según Panda Labs, el principal reto para el 55% de las empresas es precisamente la detección de estas amenazas avanzadas.

> La preocupación no debe centrarse en los fallos según su origen, sino en función de su objetivo

POLÍTICAS DE ZERO TRUST

Para hacerles frente de un modo eficaz, las empresas deben renovar sus estrategias de seguridad y poner sobre la mesa cuestiones como quién se conecta a la red, por qué puede acceder, desde cuándo y hasta cuándo, de qué modo accede a ella y, lo más importante, qué información puede ver. Es decir, se trata de utilizar técnicas más completas, implantando políticas de tipo *Zero Trust* en las que nada debe ejecutarse si no se confía en ello. En este tipo de políticas, la preocupación no debe centrarse en los fallos según su origen, sino en función de su objetivo.

Sin embargo, según señala el analista Forrester, la mayoría de las organizaciones no están realmente implementando el marco Zero Trust de manera efectiva. Esto se debe, en parte, a que no comprenden por completo la tecnología y los cambios organizativos necesarios para ponerlo en práctica.

Zero Trust recurre a tecnologías tales como la autenticación multifactorial, IAM, orquestación, análisis, cifrado, puntuación y permisos del sistema de archivos. Pero también exige políticas de gobernabilidad tales como dar a los usuarios la menor cantidad de acceso que necesiten para realizar una tarea específica .

Además, una adecuada estrategia *Zero Trust* requiere abarcar al menos tres de los elementos claves para la ciberseguridad en la compañía: la red, los datos, los recursos humanos, la carga de trabajo, la automatización y la visibilidad y el análisis, así como una API potente que permita la integración.

EXTERNOS E INTERNOS

Una vez la empresa ha adoptado este modelo, se encuentra en una situación mucho más beneficiosa, ya que permite a las organizaciones hacer frente tanto a ataques externos como internos, consiguiendo un mejor control sobre la seguridad.

El *Zero Trust* es el único enfoque válido para frenar las nuevas amenazas en el ámbito de la ciberseguridad. Monitorizar toda la actividad, exponer cualquier comportamiento que pueda parecer sospechoso, centrarse en la información a la que van dirigidos los ataques, antes incluso de que ocurran… Todo esto forma parte de la anticipación y la producción de inteligencia, que es lo que va a permitir a las empresas hacer frente a los nuevos *modus operandi* de los que hablábamos al inicio.

Algo que hay que tener en cuenta es que, dentro de esa anticipación, un reto muy importante es detectar las amenazas procedentes del usuario, que en numerosas ocasiones pertenece a la propia organización.

Esto implica que los análisis de seguridad se deben trabajar en diferentes niveles. Por un lado, en los casos de atacantes internos o incluso de personas de la propia organización que puedan suponer una amenaza, son necesarias técnicas de *deep learning* y análisis de seguridad sofisticados.

Por otra parte, en los casos de amenazas conocidas o desconocidas, pero que se identifican de forma ágil, se pueden utilizar modelos estadísticos y *machine learning* más sencillo, con un nivel medio o bajo de sofisticación del análisis.

> Un reto muy importante dentro de esa anticipación es descubrir amenazas procedentes del usuario

La seguridad de las redes del mañana

Cinco requisitos básicos

JOSÉ LUIS LAGUNA

Systems Engineer Manager

FORTINET

fortinet.com

Uno de los resultados más perturbadores del actual proceso de transformación digital ha sido la rápida aparición del *edge* o borde. La red basada en *edge* está reemplazando al perímetro tradicional, permitiendo a las organizaciones expandir sus redes de forma más dinámica, crear conexiones WAN dinámicas, adoptar estrategias de movilidad e IoT y habilitar el procesamiento distribuido. También está introduciendo una amplia gama de nuevos desafíos de seguridad que no se pueden abordar con las soluciones o estrategias actuales.

Cada vez que un *endpoint,* un dispositivo IoT, un contenedor, una delegación o cualquier otra configuración se conectan a su entorno central para entregar o recopilar datos, procesar información o ejecutar una carga de trabajo, estamos creando un borde. Cualquier dispositivo con una dirección IP alcanzable es un dispositivo *edge.* Pueden ser de consumo como teléfonos, relojes y automóviles; implementados en una delegación como *routers,* dispositivos de acceso integrado (IAD) o multiplexores; soluciones SD-WAN o incluso contenedores *cloud*.

» ASEGURANDO EL EDGE

Ya existen más dispositivos IP habilitados que humanos, y muchos de ellos pueden admitir múltiples conexiones. Esto significa que hay miles de bordes en uso en un momento dado, con miles de millones de potenciales dispositivos *edge* a la vuelta de la esquina. Y cada uno de ellos necesita protección.

Aunque la seguridad de una organización es tan buena como su enlace más débil, un dispositivo personal en una red de delegaciones que se conecta a la Internet pública puede no requerir el mismo grado de escrutinio que una videoconferencia en la que se discute sobre propiedad intelectual. Hay que lograr un equilibrio entre la protección de datos críticos y la administración de recursos limitados, como el ancho de banda.

Los requisitos para asegurar que cada nueva conexión perimetral reciba la seguridad que requiere son:

- **Conexiones seguras.** El cifrado es esencial para los dispositivos que se conectan a las redes públicas. Las comunicaciones complejas y los requisitos de colaboración requieren el desarrollo y mantenimiento de una VPN integrada. Además, algunas transacciones pueden requerir un cifrado más allá de IPSec y SSL.
- **Control de acceso.** Todos los dispositivos se tienen que identificar en el momento de la conexión, y deben aplicarse las políticas adecuadas, también a lo largo de la ruta de datos.
- **Redes segmentadas.** Los dispositivos autorizados deben asignarse a un segmento de red específico donde se puede monitorizar en detalle y evitar el acceso a recursos no autorizados. Los dispositivos o aplicaciones que tengan un comportamiento anómalo pueden ponerse inmediatamente en cuarentena.
- **Inspección habilitada.** Las herramientas de seguridad deben inspeccionar los datos cifrados a velocidad de red y los eventos de seguridad detectados necesitan activar una respuesta consistente en toda la red distribuida.
- **Gestión centralizada.** Compartir y correlacionar la inteligencia de amenazas, identificar los comportamientos anómalos y orquestar una respuesta coherente a través de un sistema de gestión central.

El crecimiento del borde está transformando por completo las redes, y el 5G contribuirá a impulsar y acelerar este proceso. Para abordar los nuevos desafíos debemos entender dos cosas:

> **Habilitar las redes del mañana requiere redefinir las soluciones de seguridad implementadas hoy**

- Las soluciones de seguridad heredadas no pueden llevarnos más lejos. La seguridad que se enfoca en una conexión a través de una puerta de enlace en un perímetro, o incluso al inspeccionar el contenido que fluye a través de esa conexión, tiene poca utilidad en un mundo donde las redes, datos, flujos de trabajo y dispositivos están en un estado de continuo cambio.
- Un único enfoque para la seguridad perimetral seguramente fracasará. La protección no solo debe abarcar toda la red distribuida, sino que también se debe ajustar dinámicamente —sin intervención humana— a los cambios continuos de la red.

Habilitar las redes del mañana requiere que las organizaciones vuelvan a redefinir radicalmente las soluciones de seguridad que tienen implementadas hoy.«

CARLOS MUÑOZ

Senior Presales Engineer
Security Advisor

MCAFEE

mcafee.com

Una orquestación más madura

Fases de la operación de seguridad

En los últimos años, el escenario al que tienen que enfrentarse las áreas de seguridad de las empresas ha variado de forma evidente: se ha producido un incremento exponencial en el número de dispositivos y tecnologías utilizadas por las organizaciones, y también de las nuevas técnicas usadas por los atacantes; todo ello en un contexto marcado por la masiva adopción de servicios *cloud.*

En muchas ocasiones, los departamentos encargados de gestionar la operación de seguridad se ven incapaces a la hora de analizar este ingente volumen de información.

Para abordar este problema es necesario analizar las fases fundamentales en el desarrollo de la operación de seguridad —identificación, análisis y respuesta—, intentando incorporar en cada una de ellas las piezas que puedan faltar para mejorar la capacidad de análisis y respuesta de las organizaciones.

> **Actualmente existen soluciones que permiten automatizar el proceso de investigación completo**

FASE DE IDENTIFICACIÓN

La identificación de comportamiento anómalos es la base para el desarrollo de investigaciones posteriores. En esta fase, el SOC (centro de operaciones de seguridad) debe contar con el conjunto de herramientas necesarias para ayudar al analista en la identificación automática de los incidentes, ayudando al analista a poner el foco en aquello que realmente importa.

Una de las técnicas utilizadas en la identificación de amenazas es el uso de reglas de correlación, aunque es importante mantener y actualizar este conjunto de políticas al estado del arte actual. Para ello, es necesario contar con servicios expertos, que se nutran del conocimiento fusionado que aporta la gestión de seguridad en múltiples clientes.

En esta fase se deben en cuenta aspectos como la identificación de anomalías mediante el perfilado de las entidades analizadas (usuarios, direcciones IP, hosts, dominios, etc.) o el uso integrado del SIEM con funcionalidades tipo UEBA.

La incorporación automática de cyber threat feeds permite la creación de procesos de correlación dinámicos, que ayuden a identificar estos indicadores de ataque entre el volumen de eventos recibidos. Además, la utilización de estándares como TAXII o STIX permiten automatizar el consumo de esta información en un formato entendible por la plataforma de orquestación.

FASE DE ANÁLISIS

Una vez identificados los incidentes a los que prestar atención, habrá que comprobar si requiere de una respuesta inmediata, si es necesaria su monitorización o si se trata de una falsa alarma, en cuyo caso el sistema debe ser ajustado para evitar de nuevo su detección.

Los sistemas de orquestación incorporan funcionalidades nativas que ayudan a pivotar sobre el incidente de seguridad, permitiendo su contextualización en un marco de tiempo que permita triangular el incidente con otros posibles eventos recibidos.

Las soluciones EDR, permitirán conocer el grado de impacto de un indicador entre los puestos de trabajo y servidores de la organización, detectando movimientos laterales y malware latente. Se trata de una pieza fundamental en los procesos de investigación.

Actualmente existen soluciones que permiten automatizar los procesos de investigación: recogen información de soluciones EDR, EPP y SIEM, entre otras, y aplican algoritmos de clasificación permitiendo automatizar el proceso de investigación completo.

FASE DE RESPUESTA

El objetivo último es la implementación de respuestas para mitigar el impacto de la amenaza identificada. Si la solución de orquestación soporta los estándares de comunicación, tal y como algunos fabricantes están proponiendo, facilita el desencadenamiento automático de acciones sobre el conjunto de contramedidas existentes. En este sentido, las soluciones SOAR pueden facilitar notablemente la automatización de procesos.

En definitiva, el foco en estas tres fases, junto con la apertura de la organización al consumo de información de seguridad global para evitar que quede aislada del conocimiento aportado por la comunidad, permitirá evolucionar la orquestación de seguridad a niveles de madurez más avanzados.

Visibilidad y control en la nube

Evitar la fuga de datos

SAMUEL BONETE

Country Manager

NETSKOPE

netskope.com

El impacto de los servicios *cloud* en el tráfico web empresarial va en aumento. Tanto es así que, según el último informe publicado por Netskope, en la actualidad representa el 85% de todo el tráfico corporativo.

Para explicar este incremento debemos fijarnos en la realidad actual, aquella marcada por la transformación digital, una evolución tecnológica que está llevando a las empresas a sustituir el uso tradicional de la web por los servicios *cloud.* Ya sea en modo SaaS, IaaS o PaaS, los servicios en la nube siguen aumentando año tras año, hasta situarse hoy en una media de 1.295 por empresa (según el mismo estudio) teniendo en cuenta los distintos beneficios que propone a la hora de optimizar los procesos empresariales.

INFORMACIÓN CORPORATIVA

Hoy en día, las aplicaciones de almacenamiento y colaboración en la nube comprenden la mayoría de los servicios *cloud,* mientras que los de redes sociales orientados al consumidor —como Facebook, Twitter, LinkedIn y YouTube— ocupan también un lugar destacado. Ambas tendencias ponen de manifiesto una misma realidad: las empresas permiten a sus empleados utilizar las redes corporativas con fines personales. De esta forma, en muchas ocasiones, los datos empresariales, tanto de clientes como de empleados, quedan expuestos.

Otra tendencia que está marcando el panorama actual es el número de aplicaciones permitidas por TI. En la actualidad, este tipo de soluciones suponen menos del 4% de las utilizadas en la empresa. El resto, las denominadas *shadow IT,* son manejadas con frecuencia por áreas de negocio y, comúnmente, implican riesgos como la fuga de datos confidenciales.

Sin visibilidad sobre ellas, desde el área de TI se utilizan tácticas de seguridad heredadas, como el bloqueo en el perímetro o en el *endpoint,* lo cual genera fricción y la necesidad de hacer excepciones.

DE LA WEB AL *CLOUD*

A la luz de esta realidad, es imperativo evaluar la existencia de controles adecuados para proteger todo el tráfico. Dado que la mayoría de las herramientas de seguridad se centran en el tráfico web tradicional, este cambio significativo hacia la utilización de la nube está provocando que los equipos de seguridad se queden ciegos, que desconozcan qué ocurre.

En este sentido, y dado que no existe un enfoque único que garantice la seguridad de una empresa según esta adopta nuevas herramientas y tecnologías, una comprensión clara del tráfico y una vigilancia adecuada de lo que ocurre —tanto en el perímetro como fuera de él— son un importante requisito. Asimismo, y por las características propias de la nube, es recomendable optar por la integración de una plataforma de seguridad 100% *cloud,* capaz de mantener los peligros de la nube a raya.

PROTECCIÓN NATIVA

Además de la integración de una tecnología *cloud* nativa, que permita detectar y mitigar las amenazas propias de la nube, también es recomendable seguir una serie de pautas:

- La evaluación periódica y sostenida de la seguridad de los recursos de IaaS.
- La ejecución de análisis DLP del contenido compartido externamente en aplicaciones *cloud* permitidas para impedir la fuga de información.
- Asimismo, los usuarios deben ser advertidos ante los peligros de ejecutar macros no firmadas u otras procedentes de una fuente no fiable, incluso aunque parezcan provenir de un servicio *cloud* legítimo.
- Tampoco deben abrir cualquier archivo (a menos que estén muy seguros de que son inofensivos) independientemente de sus extensiones.
- Además, otra recomendación a tener en cuenta es mantener actualizados los sistemas y el antivirus con las últimas versiones y parches.

Por último, también será crucial en esta carrera por la seguridad la oportuna implementación de una plataforma de protección capaz, entre otras, de encontrar amenazas híbridas y aplicar políticas de uso tanto para los servicios no autorizados como para las instancias no permitidas de servicios *cloud* aceptados.

Netskope Cloud Report

Reports and interactive guides to learn about the most interesting cloud app, activity, and policy trends.

FERNANDO ANAYA

Director regional para España y Portugal

PROOFPOINT

proofpoint.com

Mitigar el "factor humano"

La ciber-resiliencia en las pymes

En el entorno actual, las pymes no son inmunes a sufrir ciberataques, aunque a menudo este tipo de empresas tienden a considerarse como el pez pequeño en comparación con otras organizaciones y esto las lleva a pensar que no merecen la pena como objetivo.

Según un informe global sobre el fraude por correo electrónico elaborado en 2018 por Proofpoint, no existe casi ninguna conexión entre el tamaño de la empresa y la frecuencia con la que esta se ve afectada por estafas vía email. Esto hace que sea igual de probable que las pymes experimenten ataques BEC *(business email compromise)* con la misma frecuencia que empresas más grandes.

> **Los ataques se dirigen cada vez más a las personas, y no únicamente a la infraestructura de TI**

» EL USUARIO FINAL

La capacidad de las empresas para protegerse frente a situaciones adversas comienza por la concienciación de sus empleados. El usuario final es clave para que un ataque de *phishing o ransomware* tenga éxito. La cuestión no es cuánto va a suponer para las pymes formar a su personal sobre ciberamenazas, sino cuál será el precio que tendrán que pagar por ignorar este aspecto de la seguridad.

Normalmente, las pymes suelen contar con menos margen de maniobra frente al impacto financiero que pueda tener una transferencia fraudulenta o errónea, o para disponer de fondos para reparar o recuperarse frente a posibles daños. También es menos probable que tengan acceso a herramientas técnicas avanzadas que las ayuden a prevenir que esos ataques lleguen a sus empleados. Todo esto significa que, en general, los errores de los usuarios tendrán mayor coste y afectarán en mayor medida su sostenibilidad como organizaciones.

Hemos llegado, por tanto, a un punto en que las habilidades en ciberseguridad no son algo que esté simplemente bien que tengan los empleados. Han pasado a ser un imperativo dentro de las empresas.

A veces, los ciberdelincuentes pueden ver a las pymes como un objetivo más débil o vulnerable en comparación con compañías más grandes. Algunas tecnologías de defensa, como antivirus o *firewalls,* resultan fundamentales en cualquier estrategia de ciberseguridad y es de vital importancia garantizar su actualización a medida que los atacantes desarrollan y adoptan nuevas formas de *malware.* Sin embargo, esto solo es una parte de lo que debería ser una defensa óptima en ciberseguridad para una pyme.

En la actualidad, los ataques se dirigen cada vez más a las personas, y no únicamente a la infraestructura de TI, ya que es mucho más sencillo explotar las vulnerabilidades humanas mediante tácticas de ingeniería social simples, pero sofisticadas, en correos electrónicos de *phishing.*

Los ciberdelincuentes han encontrado nuevas maneras de aprovechar el denominado "factor humano", esa confianza y curiosidad que lleva a las personas bien intencionadas a entrar en el juego de los atacantes. Las ciberamenazas pueden ser de diferentes tipos, desde engañar a usuarios para que hagan clic en enlaces maliciosos y consigan así instalar *malware* hasta correos electrónicos que suplantan la identidad de un miembro de confianza de la organización para convencer a los empleados de que envíen fondos o revelen datos confidenciales.

» FORMAR A LOS EMPLEADOS

En definitiva, la ciber-resiliencia para las pymes significa poder prevenir de forma proactiva un incidente de ciberseguridad a través de estrategias que protejan, en primer lugar, a sus empleados, en vez de a su infraestructura TI.

No obstante, a la hora de protegerse de este "factor humano", son muy pocas las pymes que dan valor a la formación de sus empleados para hacerlos más resilientes. Sin un mayor nivel de concienciación en este sentido, siempre habrá alguien en la empresa que haga *clic* donde no debe.

Por eso, la formación debe ir más allá de un simple curso *online* a realizar por los empleados. Hay que conseguir que estos sean cada vez menos susceptibles a las ciberamenazas y que puedan detectar cualquier intento de ingeniería social de modo que los correos electrónicos fraudulentos puedan ser identificados a tiempo, antes de que causen daños significativos.«

Motivos, medios y oportunidad

La nueva ecuación de riesgo

RAMSÉS GALLEGO

Strategist & Evangelist, Office of the CTO

SYMANTEC

symantec.com

Una de las más simples definiciones de riesgo que he encontrado en mi carrera se manifestó en forma de ecuación: para que exista un riesgo debe haber una amenaza que utilice una vulnerabilidad, con una probabilidad de que ello ocurra, y debe haber un impacto (amenaza, vulnerabilidad, probabilidad e impacto). Es decir, debe existir alguien que quiera hacer daño, que nuestros sistemas tengan un agujero (que será explotado por el atacante), que exista una probabilidad de que esa casuística se dé (cuanta mayor exposición y/o agujeros mayor probabilidad) y, por supuesto, debe haber un impacto, un daño, una pérdida (de lo contrario, podríamos hablar de riesgo residual o incluso existente, sin consecuencias reales).

Teniendo en cuenta esta ecuación, y con el objetivo de mitigar ese riesgo, únicamente podemos trabajar en tres de las cuatro variables que la forman. Solo podemos disminuir el factor de exposición al reducir las vulnerabilidades existentes, es decir, al cerrar esos agujeros. Haciendo esto, de manera natural estaremos reduciendo la probabilidad de que un ataque ocurra y eso también es trabajar en la dimensión de empequeñecer el riesgo. Además, protegiendo los activos con las contramedidas adecuadas (conociendo siempre el valor de lo que queremos proteger) estaremos reduciendo el impacto. Magnífico.

Sin embargo, lo que no podemos evitar es que haya agentes que quieran causar el mal, robar información corporativa y/o que, simplemente, quieran provocar situaciones disruptivas para la entidad. No podemos evitar que haya malhechores y debemos contar con ese factor de amenaza.

NUEVAS AMENAZAS

Reflexionando sobre ese factor, me vino a la mente otra ecuación (motivos, medios y oportunidad) que podría explicar por qué existen esas amenazas y la razón por la que se experimentan aumentos (así lo recoge el informe anual ISTR de Symantec) del 1.500% en algunos tipos de ataques, como ocurre con *formjacking,* entre otros.

Como ocurre en el mundo físico, un atacante digital precisa de un motivo para hacer daño. Los dos fundamentales son dinero y disrupción social o política. Sin embargo, si no se tienen los medios adecuados, el ataque se quedaría en la fase de diseño... Pero existen medios muy avanzados, con costes que han reducido drásticamente el ARPA (ingreso medio por ataque, *average-revenue-per-attack*) y que, incluso, son prestados por otros grupos compartiendo los beneficios.

Finalmente, en esta nueva aproximación de riesgo, los atacantes necesitan de una ventana de **oportunidad** en su faceta de factor de exposición, de visibilidad de la compañía, de gestión de vulnerabilidades... Internet permite la invisibilidad del atacante o, si se tiene visibilidad, el sistema judicial internacional no siempre facilita la persecución del delito. Así, el aspecto de oportunidad es tan relevante como los otros dos factores.

Si a todo eso le añadimos tácticas, técnicas y procedimientos sofisticados, a veces incluso usando mecanismos que se utilizan para la protección (no olvidemos que el pilar principal de los ataques de *ransomware* es el cifrado de los datos), nos encontramos ante una situación de ¿debilidad? ante los ataques.

> **Solo podemos disminuir el factor de exposición al reducir las vulnerabilidades existentes**

PROTEGER Y DEFENDER

No quisiera finalizar esta reflexión sin abordar un aspecto positivo de todo ello: esos motivos, medios y oportunidad también los tenemos aquellos que queremos proteger y defender. Hoy en día, las compañías conocen los motivos para salvaguardar información —no solo la ley sino el sentido común debe jugar un papel instrumental aquí—, tienen los medios para ello (ofuscación en el uso de la nube, cámaras de aislamiento, navegación segura, cifrado de las comunicaciones, etc.) y, sobretodo, la oportunidad.

Nunca ha habido tanta información ni tecnología para realizar esa protección y defensa de manera efectiva. Nunca se ha tenido tanta inteligencia de amenazas, capturada con millones de puntos de información en puestos de trabajo, en la red, en cabinas de almacenamiento, en el *gateway,* en los dispositivos móviles...

Por todo ello, el riesgo se definirá con las variables **motivos / medios / oportunidad.** Para los malos... y para los buenos.

JOSÉ
DE LA CRUZ

Director
Técnico

TREND MICRO

trendmicro.com

Desglosar las alertas grises

Los servicios de MDR

En ciberseguridad, las cosas que son blanco o negro son definitivas, claras y reconocibles: son maliciosas o benignas. Ahora, el panorama se amplía y evoluciona, acompañado por una variedad de grises. Las amenazas desconocidas activan estas alertas grises en las herramientas de detección y respuesta de los endpoints (EDR) a diario. ¿Merecen un análisis más profundo?

Una alerta gris es creada cuando se encuentra un archivo o un incidente con una característica o comportamiento no revelado. Por ejemplo, una herramienta de detección puede emitir una alerta gris para una determinada aplicación al registrar un comportamiento potencialmente no deseado, como las molestas ventanas emergentes o los anuncios. Pero es posible que esa aplicación tenga alguna utilidad, y se esté dispuesto a lidiar con esos efectos no deseados. En ese caso, el área de seguridad puede optar por no examinar la aplicación. Sin embargo, esos anuncios podrían tener malware e infectar los endpoints. Por eso, el equipo de seguridad debe analizar una alerta gris para determinar su verdadera naturaleza y los pasos a seguir.

> A medida que las amenazas se vuelven más complicadas, es más difícil determinar esas alertas grises

Ahora abundan las amenazas sofisticadas, difíciles de detectar con las soluciones tradicionales. A pesar de ello, la agrupación o la recopilación de información pueden hacer que afloren alertas grises en las herramientas EDR. Además, retrasar el análisis de las alertas grises, o ignorarlas, puede llevar a que las amenazas avanzadas entren en el sistema sin ser detectadas, pudiendo funcionar como droppers o cargadores de otras más insidiosas, como el ransomware, para infiltrarse en un sistema. Las amenazas no detectadas, y las alertas grises no analizadas, aumentan la vulnerabilidad ante riesgos que podrían provocar pérdidas financieras, trastornos operativos y daños de reputación.

MACHINE LEARNING

A medida que las amenazas se vuelven más complicadas, es más difícil determinar esas alertas grises. Por eso resulta muy beneficios contar con una solución de seguridad que utilice tecnología de machine learning, que permita la identificación precisa y el bloqueo de amenazas nuevas o no clasificadas en un conjunto de reglas en evolución. Pero una buena práctica es asociar esta tecnología con otras, para crear una postura de seguridad fuerte y multicapa.

Las soluciones de seguridad avanzadas, como las herramientas EDR que utilizan machine learning, son más eficaces cuando las dirigen profesionales de seguridad capaces de desmitificar y conectar alertas grises a otros eventos de la red. Para proteger completamente un sistema, las alertas grises de varios vectores de ataque (la red, el servidor y el correo electrónico), deben ser correlacionadas y analizadas.

DEMASIADAS ALERTAS GRISES

Cuando el volumen de alertas grises es demasiado alto, los equipos de ciberseguridad pueden verse abrumados. La falta de competencias en esta materia es una preocupación creciente en el ámbito empresarial y no contar con profesionales de alto nivel puede resultar una desventaja.

Pero, aun teniendo personal experimentado, una organización no es inmune a la falta de conocimientos. Un 66% de los encuestados en un estudio afirma que su personal actual experimenta una mayor carga de trabajo debido a la escasez de personal cualificado. En cualquier caso, incluso si tienen gente con conocimientos a bordo, se sobrecargarán con múltiples tareas incluyendo la identificación de qué alerta gris priorizar para su análisis entre el vasto volumen con el que se ven inundados en su día a día.

La detección y respuesta gestionadas (MDR o managed detection and response) ayuda a las organizaciones al proporcionar supervisión de alertas 24x7, capacidades de detección de amenazas y respuesta por parte de profesionales experimentados en ciberseguridad capaces de maximizar las soluciones de seguridad en beneficio de la organización.

Los servicios de MDR ofrecen a las organizaciones una experiencia avanzada y eficiente en inteligencia de amenazas ayudando a reducir el problema de la falta de habilidades como ventaja adicional.

La primera línea ante el cibercrimen

Tecnologías innovadoras para profesionales de la seguridad

JULIÁN DOMÍNGUEZ

Sales Engineer

VARONIS

varonis.com

La seguridad cumple un papel algo paradójico en una organización: a menudo es la primera línea de defensa, pero también es la última oportunidad para mantener alejados a los atacantes.

Es una enorme responsabilidad apuntalar la infraestructura de TI de una empresa y salvaguardar las "joyas de la corona": datos que van desde el código fuente y la propiedad intelectual invaluable, hasta los detalles personales y de pago de los empleados y clientes.

Un paso en falso y su empresa podría ser víctima de un ataque o multada por la AEPD (Agencia Española de Protección de Datos) por incumplimiento del GDPR (Reglamento General de Protección de Datos). No hay presión, ¿verdad?

» TRES TECNOLOGÍAS

Afortunadamente, el futuro de la ciberseguridad ya está aquí. Estas tres tecnologías ayudarán a reforzar las capacidades de las organizaciones y a proteger los datos internos contra las últimas amenazas.

1. Automatización. Según algunas estimaciones, la escasez mundial de profesionales de ciberseguridad ha alcanzado una cifra cercana a los tres millones. Las posiciones permanecen sin cubrir a medida que los atacantes intensifican sus esfuerzos.

Afortunadamente, la automatización está eliminando poco a poco las tareas “mundanas” que inundan el día a día. Con las reglas correctas establecidas, lo que parecía una tarea tediosa e imposible —por ejemplo, eliminar permisos sobreexpuestos para recursos humanos y archivos financieros— se puede realizar en mucho menos tiempo.

Esta es la primera de estas tecnologías recomendadas, use la automatización para liberar a su personal de seguridad capacitado para que pueda centrarse en lo que realmente importa.

2. Aprendizaje automático. Según algunas estimaciones, se crean más de 2.5 quintillones de bytes de datos todos los días. Las empresas deben hacer frente a cada vez más datos y usuarios y, por lo tanto, más amenazas a su información crítica.

Un humano no puede hacerlo todo. El aprendizaje automático es necesario. No es solo una palabra de moda. Esta tecnología ayudará a filtrar el mar de información recopilada por la SIEM *(security information and event management)* para encontrar patrones que podrían indicar que un ataque está en marcha. En lugar de perseguir alertas e intentar identificar la señal del ruido, esta tecnología puede detectar qué eventos son más propensos a ser significativos y si requieren una mayor investigación.

3. Análisis del comportamiento del usuario (UBA). El monitoreo del comportamiento incluye contexto sobre usuarios, dispositivos y datos. Es casi inevitable que un atacante omita las protecciones de punto final y perímetro en algún momento. Se vuelve extremadamente difícil para los malos actores cubrir sus huellas si las compañías monitorizan cómo trabajan sus usuarios y cómo usan los datos.

UBA *(user behavior analytics)* puede facilitar información para saber quién trabaja a horas inusuales y accede a archivos confidenciales. Los algoritmos y reglas de UBA pueden decidir con mayor precisión qué es inusual para un usuario específico y, de esta forma, ayudar a reducir los falsos positivos.

> “El futuro de la ciberseguridad pasa por la automatización, el aprendizaje automático y el análisis del comportamiento

» RETO Y OPORTUNIDAD

Por su puesto, con cada ventaja que aparece se genera también la correspondiente desventaja: los atacantes ya están utilizando algunas de estas nuevas técnicas para penetrar en sistemas vulnerables.

Lo más probable es que algunas compañías ya estén comprometidas y que ya existan una serie de atacantes observando y esperando el momento adecuado para actuar. ¿Estarán usted y su equipo de seguridad listos para la próxima amenaza?«

FIRMA INVITADA

La década prodigiosa

El futuro económico digital

Nos acercamos inexorablemente al final del año y resulta que, además, esto nos coloca también al final de una década que entiendo será conocida en el futuro como los “años 10” o algo así. Con la llegada del nuevo año, que está ahí, a la vuelta de la esquina, entramos en los “años 20” del nuevo siglo. Por lo tanto, será una fecha icónica, incluso catártica, como tantas cosas hoy en día. Época que será más de imágenes y sentimientos que de realidades y hechos.

Sin que sirva de menoscabo de lo que venga, y sin temor a errar mucho el tiro (temor ninguno, ya que lo que impera ahora mismo es el chapuzón y lanzarse a la piscina, que un tuit pasa muy rápido y nadie se acuerda), estos diez años han sido lo que podríamos denominar como "una década prodigiosa" en el mundo de la ciberseguridad.

A principios de este siglo, hace ya casi veinte años, la preocupación era otra: hablábamos del efecto 2000, del boom urbanístico o sobre cómo gestionar una economía que apuntaba a crecimientos por encima de la todopoderosa Alemania. Además, el IBEX 35 —junto con otros indicadores— nos decían que en este país o nación éramos casi ricos y omnipotentes, y que lo de Internet era imparable… Pero aun estábamos viendo qué podríamos hacer con aquello.

Esta década que termina nos coloca en otra situación muy distinta: nos hemos pegado el “batacazo padre”, lo del ladrillo no duró (y eso que ya lo sabíamos) y dolió más de lo previsto, el IBEX —y otros índices tan sagrados como el tipo de interés— resultaron víctimas de la situación y muy poco útiles para el nuevo mundo que viene. Además, resulta que la economía debe ser digital y que lo de Internet no era un juguete, sino la base de todo. Sí, de todo. Vaya añitos estos.

ESTAR PREPARADOS

Resulta que en estas estamos. Los padres y representantes de las patrias varias que nos atañen, léase Comisión y Parlamento Europeos, reaccionaron a tantas obviedades e intentan, mal que bien y a trancas y barrancas, hacernos a todos mejores y más sensatos. Unifican

reguladores en el ámbito europeo, desarrollan normativa a ritmo desbocado y proponen el mundo que viene fijando una suerte, algo obvia, de futuro económico digital para la que los europeos debemos estar preparados. Lógicamente, otros focos de potencia económica (léase EE. UU., China y poco más) están peleando y dando duro en esto. De aquí nos vienen las ínclitas siglas que tanto nos motivan en el ambiente de la ciberseguridad, como GDPR, NIS, PSD2…aliñadas por la versión patria de las mismas ENS, RGPD…

Todo este ambiente se une a la evolución natural de la "cosa" digital, donde el concepto ciber se ha solapado con el de transformación digital, para convertirse en el *leitmotiv* de las compañías, organizaciones y demás colectivos e individuos.

El objetivo es evolucionar para tratar de transformarnos en algo que saque provecho de lo que viene; al menos, que nos permita sobrevivir y que, si podemos, nos ayude a dejar atrás el modo en que gestionábamos a principios de siglo.

> "Esto de lo digital ya no va de la máquina, sino de lo que hacemos con ella. El software manda

» CURVA DE ADOPCIÓN SIDERAL

Convertimos la seguridad informática de toda la vida en ciberseguridad, sobretodo porque mola, pero también —principalmente— porque los que sí se han transformado rápido y con ciclos *agile* bien implantados son los delincuentes y las organizaciones que los amparan, y bien amparados. Y nos están dando por todas partes, tanto que se han convertido en un sector económico de primer orden.

Pasamos de aquello de "hablar el lenguaje de negocio, tener visibilidad y dotarnos de recursos y capacidades", a que todo es ciberseguridad, que es importantísimo y que hay que hacer algo, mucho, aunque no sepamos muy bien el qué y el cómo. Empezamos a vivir ciberataques y cibercrisis en carne propia, no ya en los medios y en las estadísticas. Claro, como humanos que somos, no hay nada como un tropiezo para que tengamos cuidado y, si es importante y duele, pues mejor. Sin pasarse, eso sí.

Nos damos cuenta de que no todo vale. Que el mercado se infla y todo el mundo te vende ciberseguridad, aunque la estrategia del presupuesto y el musculo no nos lleva a ningún lado porque las cosas siguen pasando y seguirán pasando. Que la curva de adopción digital no es exponencial, sino sideral, y que ni siquiera podemos soñar con seguirla en términos de seguridad y resiliencia. Poco a poco nos damos cuenta de que lo importante es lo importante. Eso sí, también está lo urgente.

» EL SOFTWARE MANDA

Convencemos, o por lo menos lo intentamos, a las organizaciones y a los individuos para que presten más atención a lo más relevante, para que estimemos los impactos de los "y si…", y que los entrenemos. Les ponemos nombres, como Plan de Cibercrisis, y los probamos, porque sabemos que van a ocurrir y que nos esperan a la vuelta de la esquina.

Nos damos cuenta de que esto de lo digital ya no va de la máquina, sino de lo que hacemos con ella. Que el software es lo que manda. Que todas las organizaciones son —somos— "empresas de software" y que los individuos somos aquello que el software nos permite ser. Y empezamos a pergeñar cosas como los SecDevOps: triple pirueta invertida, que supone desarrollar constantemente y ponerlo en producción al instante, todo seguro y probado…Ahí es nada.

Como ya no cuela que para todo esto tenemos presupuesto barra libre (como si en algún hubiera sido así, permítame la licencia), tenemos que gestionar y proponer retornos, casos de negocio y equilibrio coste/beneficio. Nada nuevo, pero más duro y que, en el fondo, ayuda a la función. En una organización no hay una función que se sostenga por sí misma sin demostrar lo que aporta y, no nos engañemos, eso se mide en euros o la divisa que ustedes más aprecien.

» INDUSTRIALIZACIÓN

Sí, llegamos al final de esta década. Diez años que nos han llevado tan lejos que no sabemos casi de dónde venimos. Pero me da que los que vienen, los años veinte, van a ver una función más normalizada, menos exótica y, por lo tanto, menos atractiva para los que disfrutaban de ese halo místico y pionero. Esto se ha convertido en una función industrial y corporativa, es más, regulatoria y de gobierno.

Definitivamente, hemos perdido las coderas y la camiseta negra. Ahora toca otra cosa.«

> "Los que sí se han transformado rápido, y con ciclos agile bien implantados, son los delincuentes

ROBERTO BARATTA

Miembro de la Junta Directiva de ISMS Forum

ISMS FORUM

ismsforum.es

IX ENCUENTRO DE CLOUD SECURITY ALLIANCE ESPAÑA

Círculo de Bellas Artes de Madrid (C/ Alcalá 42, Acceso por C/ Marqués de Casa Riera, 2)

17 OCT

www.ismsforum.es

IV FORO DE LA MOVILIDAD E INTERNET DE LAS COSAS

27 NOV

Círculo de Bellas Artes de Madrid (C/ Alcalá 42, Acceso por C/ Marqués de Casa Riera, 2)

www.ismsforum.es

ISMS Forum Spain

ISMS Forum Spain es una asociación sin ánimo de lucro creada en 2007 para promover el desarrollo, conocimiento y cultura de la Seguridad de la Información en España y actuar en beneficio de toda la comunidad implicada en el sector. Se constituye como un foro especializado de debate para que todas las empresas; organismos públicos y privados; investigadores y profesionales colaboren, intercambien experiencias y conozcan los últimos avances y desarrollos en el ámbito de la Seguridad de la Información. Todo ello desde la transparencia, la objetividad y neutralidad.

La Asociación nació respaldada por empresas representativas y organizaciones comprometidas con la Seguridad de la Información. Los socios fundadores proceden de muy diversos ámbitos que van desde la enseñanza superior y la I+D hasta la Consultoría, pasando por los sectores de Banca, Certificación, Seguros, Construcción, Servicios Jurídicos o Telecomunicaciones. En su vocación plural y abierta, la Asociación invita a todos los profesionales, empresas e instituciones involucrados en la gestión de la Seguridad de la Información a asociarse.

Hazte socio de ISMS Forum y disfruta de más eventos como este

- Forma parte de la mayor red activa de organizaciones y expertos comprometidos con la Seguridad de la Información en España, que ya cuenta con más de 230 empresas asociadas y más de 1.200 profesionales asociados.
- Ten acceso gratuito a los actos públicos, foros y jornadas organizados por ISMS Forum Spain, y consigue descuentos para asistir a eventos de terceros.
- Recibe nuestro boletín informativo mensual con toda la información de todas las herramientas divulgativas (informes, proyectos, guías y estudios de referencia) fruto de la labor de sus Grupos de Trabajo, así como las novedades más recientes del sector.

TARIFAS

Grandes corporaciones:
1.100€, con derecho a 24 miembros

Empresas y organizaciones:
550€, con derecho a 8 miembros

Microempresas (menos de 10 trabajadores):
165€, con derecho a 2 miembros

Independientes:
65€

ISMS Forum Spain, la red abierta de conocimiento que conecta empresas, organismos públicos y privados, investigadores y profesionales comprometidos con el desarrollo de la Seguridad de la Información en España.

¿Quieres formar parte?

**El trámite para hacerse socio de ISMS Forum Spain se realiza a través de la web: www.ismsforum.es*

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD

FORMACIÓN

El curso de especialización en ciberseguridad ofrece profundos conocimientos sobre los fundamentos y gobierno de la ciberseguridad, arquitecturas, políticas, estrategia y estándares, análisis y gestión de riesgos, marco normativo, operativa de ciberseguridad, infraestructuras críticas, ciberinteligencia, gestión de incidentes, buenas prácticas y soft skills de la figura del Director de Seguridad de la Información.

CONTENIDO

Dominio 1: Gobierno de seguridad.
Dominio 2: Análisis y gestión de riesgos.
Dominio 3: Cumplimiento legal y normativo.
Dominio 4: Operativa de Ciberseguridad.
Dominio 5: Ciberinteligencia, cooperación y capacidad
Dominio 6: Gestión eficaz de incidentes.
Dominio 7: Infraestructuras críticas.
Dominio 8: CISO Soft Skills
Sesiones prácticas.
Simulacro de examen.

¿A QUIÉN VA DIRIGIDO?

- Profesionales con responsabilidades en el ámbito de la seguridad de la información
- Abogados
- Técnicos de sistemas
- Auditores
- Consultores
- Técnicos de seguridad

PRÓXIMA EDICIÓN

04-19 DE NOVIEMBRE DE 2019
10 SESIONES DE LUNES A JUEVES
HORARIO: 16.00h - 20.00h
MODALIDADES: presencial (12 plazas máx.)
y seguimiento online

Inscripción abierta hasta el 25 de octubre

INFÓRMATE

Escríbenos a formacion@ismsforum.es
www.ismsforum.es
(+34) 915 63 50 62

Una iniciativa de

isms forum spain

CSC Cyber Security Center

PLATINUM PARTNERS

Akamai

aruba
a Hewlett Packard Enterprise company

Guardicore

Infoblox
NEXT LEVEL NETWORKING

GOLD PARTNERS

CROWDSTRIKE

CYTOMIC

FORTINET

kaspersky

McAfee

netskope

paloalto NETWORKS

proofpoint

radware

Symantec

TREND MICRO

VARONIS

isms forum spain

@ISMSForumSpain

ISMS Forum Spain