BAILANDO CON LOBOS: LA ESTRATEGIA DE CIBERSEGURIDAD EN LA ORGANIZACIÓN

DANCING WITH WOLVES: THE CYBERSECURITY STRATEGY IN THE ORGANIZATION

Autor:

Luis Francisco Blanco Esteban. IaaS365. luisfran.blanco@iaas365.com ORCID 0000-0003-0500-1435

Resumen:

En este artículo se reflexiona sobre el cambio de paradigma que hemos sufrido en apenas los últimos cinco años en el ámbito de la ciberseguridad, de la necesidad de implantar sistemas de gestión, políticas y planes, al mismo tiempo que implantamos las mejores herramientas tecnológicas y equipos de ayuda preventivos y reactivos, pero que con todo y con ello el riesgo cero no existe, los malos ya están aquí, y tarde o temprano nos tocará sufrir un incidente de ciberseguridad, por lo que hay que estar lo mejor preparado posible y no ignorar el riesgo real que existe.

Abstract:

This article reflects about the paradigm shift that we have suffered in just the last five years in the field of cybersecurity, and the need to implement management systems, policies and plans, at the same time that we implement the best technological tools and equipment of preventive and reactive help, but with everything and with it zero risk does not exist, the bad guys are already here, and sooner or later we will have to suffer a cybersecurity incident, so we must be as well prepared as possible and not ignore the actual risk that exists.

Palabras clave:

Riesgo; Geopolítica; SOC

Keywords:
Ransomware; Risk; Geopolitics

¡Que viene el lobo, que viene el lobo! ¿Cuántas veces nos habrán dicho esto en los últimos años con la ciberseguridad? Que si la mayor preocupación de las empresas y los CIO es la seguridad de las TI, que, si el informe de la consultora X dice que las mayores amenazas para el próximo año son las relacionadas con la seguridad informática, bla, bla, bla… pero la realidad es que el estado de madurez de la seguridad en las empresas, instituciones y organismos públicos es defectuoso, por decirlo elegantemente; y el lobo ya está dentro del gallinero.

Venimos de unos tiempos que lo más importante era tener unas rejas en las ventanas, una buena puerta acorazada, un portero de la finca y los más aventajados una alarma conectada a una central de una empresa de seguridad. O lo que es lo mismo, empezamos a poner *firewalls*, a segmentar la red, a utilizar credenciales y perfiles de usuario, a instalar antivirus y a dormir tranquilos.

Pero con el paso de los años nos encontramos aun con empresas sin antivirus, sin cortafuegos, sin planes o estrategias de seguridad de las TIC; y por muy pequeña que sea la organización, por muy poca exposición, riesgo o impacto que crean que tienen, las normas del juego han cambiado, la información ahora es un tesoro, y la conexión a Internet de nuevos dispositivos y servicios, o el potenciación *online* que ha habido en estos años de pandemia, ha multiplicado exponencialmente el riesgo, la exposición y las consecuencias; antes de la pandemia pensábamos solo en las amenazas que podrían afectar a la red corporativa, *on-premise*, en las instalaciones y CPD… El paradigma ha cambiado, y ya no se trata sólo del perímetro y la red interna. Los usuarios remotos están expuestos a otras amenazas que en su “zona de seguridad” no les podía afectar, o al menos, no de la misma manera.

Habitualmente, cuando hablamos de proteger los sistemas y su información nos debemos centrar en las tres dimensiones de la ciberseguridad: primera, la confidencialidad, que

solo entren y vean los que están autorizados; en segundo lugar, la integridad, que no nos manipulen, cambien o rompan nuestra información y, finalmente, la disponibilidad, que podamos acceder y usar la información y los servicios. A estas dimensiones clave se les suele añadir otras dos, que sobre todo nos ayudan a la hora de necesitar auditar y hacer análisis forense, como son la autenticidad del origen de la información y la trazabilidad para registrar las huellas de todos los pasos que se dan dentro de nuestros sistemas.

Con estas cinco dimensiones y un inventariado y catalogación de nuestra información y sistemas, debemos realizar un análisis de riesgo para poder tomar las medidas reales para nuestra necesidad o al menos conocer y asumir los riesgos que no queremos mitigar; realmente las posibles respuestas al riesgo no se asumen, lo que hay que hacer es reducirlas o mitigarlas, aceptarlas o transferirlas. Es necesario recalcar que hay una respuesta muy dada por desgracia que es omitir el riesgo, algo inaceptable por cualquier organización; algo muy parecido a lo que hace un avestruz metiendo la cabeza en un agujero en el suelo sin querer saber nada de lo que pasa a su alrededor, siguiendo los símiles del mundo animal. Es preferible puntuar bajo los niveles de aceptación del riesgo o NAR; por ejemplo, si nuestro nivel de riesgo se mide en una escala de 0 a 10, y tenemos riesgos difíciles de mitigar y fijamos un NAR, lo que esté por debajo de ese NAR, se acepta, pero lo que esté por encima hay que tratarlo. Esto debe ser la base de partida de cualquier organización.

Pero empiezan a aparecer otras dimensiones como la reputación, la confianza, la trasparencia, que están cambiando el paradigma en esta democratización y globalización de las TIC que llevamos experimentando es los últimos años, o décadas incluso.

Continuando con lo que dice el manual, la parte teórica nos debe ayudar mucho a abordar la parte práctica, pero no debemos ser conformistas; un Sistema de Gestión de Seguridad de la Información (SGSI) nos permite poner todo en orden y orquestar todas estas necesidades. Como cualquier otro Sistema de Gestión (SG), como el de Calidad o Medio Ambiente, el de la Seguridad de la Información persigue el objetivo de obtener un mejor desempeño, de una manera diligente y ordenada, incluso acercándonos al cumplimiento

de una norma o a la consecución de un certificado como puede ser una ISO/IEC 27001. Y estando pendiente a la evolución del mercado y las tecnologías disruptivas que empiezan a tener su normativa específica u otras normas de buenas prácticas como la ISO 22301 para la continuidad del negocio (SGCN) o la ISO/IEC 27017 para la seguridad *cloud*.

Una organización debe plantearse estas medidas desde estos tres niveles: estratégico, táctico y operativo. Muchas organizaciones, sobre todo por iniciativa de su personal técnico, los frikis de toda la vida, los que inventaron la Internet, la wifi, las bases de datos, los sistemas operativos, etc., llevan a cabo operaciones de seguridad, que les ayudan a proteger su información, desde un flujo *bottom-up*, pero cuesta subir capas. Lo ideal sería tener definida la estrategia de ciberseguridad de la organización, apoyarnos en tareas tácticas y de planificación para alcanzar los objetivos de seguridad marcados y, finalmente, ejecutar las operaciones necesarias que ayuden a alcanzar dichos objetivos, lo que sería un flujo *top-down*.

A toda esta problemática y complejidad intrínseca de la seguridad de las TIC se le suma la complejidad de gobierno y gestión del total de las TIC, incluso el gobierno y la gestión de toda la organización; nos encontramos con organizaciones a las que les cuesta tener una estrategia global y unificada, organizaciones a las que les cuesta gobernar, gobernar es mandar para llevar a una organización a cumplir unos objetivos, les cuesta gestionar, desde el punto de vista de poner los medios para cumplir o dirigirse rectamente a esos objetivos de gobierno.

Las propias estructuras orgánicas o inorgánicas de muchas organizaciones, como bien pueden ser las de las universidades españolas, no favorecen la definición de objetivos estratégicos comunes para la ciberseguridad y su propia gestión con consecución de esos objetivos.

Volviendo al manual, el marco documental de la seguridad TIC nos ayudará a marcar, entre otras cosas, la estrategia de seguridad, a través de la política de seguridad de la organización. Pero no solo de políticas se nutre nuestro marco documental de seguridad,

tendremos que nutrirlo también de procedimientos, que expliquen paso a paso los procesos que se ejecutan para proteger la información de la organización. Incluso guías técnicas, para que los operarios les resulte más fácil llevar a cabo las tareas necesarias.

En definitiva, la seguridad de la información hay que entenderla como un proceso, no como una meta o un *check* para marcar en un informe. El riesgo cero como tal no existe y nunca existirá. Los sistemas de información son cambiantes, la irrupción de nuevas tecnologías o áreas, como el IoT, el Metaverso, la IA, etc., deben someter a la seguridad TIC a un proceso de revisión y mejora continua.

Es fundamental que desde lo más alto de la organización se tenga conciencia de la importancia de la seguridad en los sistemas de información y exista un marco organizacional compuesto por políticas, normas, código de conducta, procesos y procedimientos que sean la referencia en esta materia. Se debe complementar con un marco operacional que defina y detalle cómo conseguir el fin en materia de seguridad.

No nos engañemos, aquí no aplica lo de la mujer del César en su sentido habitual, aquí no solo hay que parecerlo (con el cumplimiento de la norma) sobre todo hay que serlo. Aquí, me gustaría pedir el ejercicio de enumerar los 5 últimos ataques famosos que han sido reportados y contrastar cuantas de esas organizaciones disponían del manual, los certificados, y toda esa parte documental o procedimental, pero aun así han sido atacadas, la respuesta es… todas.

Una vez que hemos conseguido garantizar, como mejor se pueda, la seguridad siguiendo estos marcos, las mejores medidas y herramientas que nos podamos permitir, tengamos las mejores estrategias, planes, certificaciones, etc. ¿Ya podemos dormir tranquilos? ¿Si viene el lobo, sabiendo que va a venir, no se comerá las gallinas? Pues pinta mal la cosa.

Como vamos viendo, el lobo ya está dentro del corral, los ciberataques o ciberdelincuentes cada día son más complejos y creativos, y los objetivos que se buscan son más globales y suculentos económicamente. Aquí es donde entra en juego los *Advanced Persistent Threats*, normalmente conocidas como APT.

Las “Amenazas Persistentes Avanzadas” son un tipo de ciberataques a gran escala dirigido a organizaciones de cierta relevancia con la finalidad del robo de datos o espionaje . Es un ataque que se cocina lentamente en el tiempo, con una inversión de recursos económicos y personales importantes, que garanticen el éxito del ataque.

Entre los grupos de ciberdelincuentes APT más famosos nos sonará Lazarus Group, originario de Corea del Norte, creado sobre 2009, siendo sus principales objetivos organizaciones de Corea del Sur y de EEUU, usando *ransomware* como WannaCry o MimiKatz como principal arma; uno de los ataques con más repercusión de este grupo fue el ataque contra Sony en 2014 en represalia por producir una película que pintaba a su líder, Kim Jong-un, de una manera que no era de su agrado.

Otro grupo famoso es el Equation Group, esta vez de origen norteamericano y relacionado con la NSA, y con objetivos en organismos de Irán, Siria y Afganistán principalmente, siendo su arma preferida los *zero-days exploits*. Podríamos decir que existe un grupo por cada zona geopolítica con intereses muy relacionados con gobiernos y financiados por agencias de inteligencia y militares en gran medida.

Lo normal es que estos ataques de estos grupos APT se inicien por vulnerabilidades ya conocidas que aún no han sido parcheadas, pero hay otras entradas como son las campañas de *phishing* o *backdoors* de tipo troyanos. Pero también existen las contramedidas que nos salvan, como son la concienciación de nuestras plantillas, nuestras capas perimetrales, la monitorización y detección, o los servicios de inteligencia contra estas amenazas que empiezan a ofrecer algunas empresas o los *Security Operations Center* (SOC), siendo conscientes que la última medida es tener un buen plan de respuesta a incidentes.

Incluso el virus o *malware* más básico puede ocasionar daños considerables a las organizaciones, incluso hacerla desaparecer, tener grandes pérdidas en bolsa o recibir grandes demandas o multas.

Según últimos datos, países del primer mundo, con altos recursos y accesos a la tecnología son los que más han reportado ataques del *ransomware* en el último año, entre ellos, en tercera posición, España. Además de la propia amenaza o ataque sufrido, se pone en duda la reputación y la confianza de estos países a la hora de hacer y recibir negocios.

Dentro de estos ataques reportados, el porcentaje más alto corresponde a organizaciones gubernamentales o administraciones públicas; podemos hacer memoria en los dos últimos años de los ataques más sonados sufridos en España, vendrán a nuestra memoria universidades, oficinas de empleo, ayuntamientos, hospitales, etc. El denominador común de estos organismos, además de la repercusión, es el elevado impacto en el número de usuarios afectados, algo que favorece la extorsión y aumenta la probabilidad de pagar los rescates. Además, este tipo de organizaciones, por las complejidades y naturalezas que ya hemos mencionado, suelen estar menos preparadas que las de sectores privados, pero que tampoco están exentas de ataques.

Con todo esto que se nos viene encima o que ya tenemos ¿Puedes tú solo? ¿Tienes suficientes recursos humanos y económicos? ¿Y conocimientos? Vemos que la inversión y el gasto en TIC va subiendo año tras año, siendo los sectores más expuestos o con mayor riesgo los que más aumentan estas partidas, en especial las destinadas a seguridad y cumplimiento; pero también vemos que si bien no hay forma eficaz de ganar la guerra a los ciberdelincuentes, sí que hay esperanza en buscar aliados, empresas especializadas con grandes profesionales con experiencia, actualizados, trabajando en red y con herramientas cada vez más potentes.

Combatir las ciberamenazas globales, de grupos organizados y coordinados, con objetivos tan claros y focalizados, no puede depender de ti solo, necesitas ayuda, necesitas esos CERT, CSIRT, SOC, en definitiva, perfiles especializados, dedicados, profesionalizados, actualizados, habituados, especialistas, no valen los administradores de sistemas y redes habituales, o los consultores de seguridad que nos ayudan en otros momentos, es hora de echarse a la trinchera y sacar la bayoneta.

Cada día hay más gobiernos, instituciones, multinacionales y sectoriales que contratan estos servicios, de forma colectiva y mutualizada, compartiendo recursos y aunando esfuerzos, y no solo desde empresas del sector privado se brindan estos servicios, tenemos grandes referencias como el INCIBE, el CCN, Policía Nacional y Guardia Civil, o incluso la propia Europol con el EC3 o la Interpol y la OTAN, que intentan dar una respuesta coordinada ante ataques globales o nacionales, intercambiando información sobre ciberseguridad y actuando de forma rápida y coordinada.

Pero además de estas fuerzas de élite debemos contar con nuestra infantería, nuestros empleados y usuarios, esos que están entre bambalinas en un entorno cada día más digitalizado y que no son conscientes de los riesgos a los que están expuestos y el gran impacto que tienen sus pequeñas acciones. Gran parte de estos ciberataques que afectan a la continuidad del negocio están relacionados con falta de formación y concienciación de estos empleados y usuarios que son engañados o realizan malas prácticas sobre la tecnología con unas consecuencias desproporcionadas en relación con sus actos. Son múltiples y variadas las herramientas, plataformas y técnicas que surgen en el mercado para concienciar a los empleados y usuarios en el buen uso de las tecnologías, desde formación a simulación incluso a escenificación de estas situaciones.

No solo la concienciación de los usuarios es importante, complementariamente es fundamental la capacitación técnica de los empleados, sobre todo de los que participan directamente en operaciones de seguridad, gestión de los *firewalls*, gestión de las copias de seguridad, gestión de permisos e identidades, gestión del control de accesos… Siendo un buen punto de partida para esa capacitación y buenas prácticas las distintas guías de buenas prácticas para la configuración segura de los sistemas que nos ofrece en España el CCN-CERT.

Además de la concienciación, podemos optar por la autorregulación usando códigos de conducta internos en la materia que permitan a estas organizaciones adoptar reglas o estándares específicos que faciliten y supervisen el cumplimiento de normas que ayuden a evitar las peores consecuencias.

Pero como venimos diciendo, lo normal es que suframos un ciberataque de alguno de los tipos que hemos ido explicando, aun habiendo sido diligentes y cumplido todas las recomendaciones y buenas prácticas. En ese momento, necesitaremos esos equipos de respuesta a incidentes como hemos dicho, pero adicionalmente es muy recomendable tener un ciberseguro, producto nuevo en el mercado que cada día está más de moda, por su necesidad, y que cada día es más complicado de adquirir, por los filtros de cumplimiento que ponen las compañías y que cada día tienen un precio más elevado; estos seguros no nos salvarán del ataque, pero dependiendo de las coberturas que contratemos si podrán asumir el coste de los equipos de respuesta a incidentes y amortiguar las previsibles pérdidas económicas sufridas por la parada de la producción y de las posibles reclamaciones, demandas o multas ocasionadas por el ataque.

En conclusión, debemos tener una buena base teórica, equipos y empleados capacitados, concienciados y dimensionados a la necesidad, debemos tener recursos y presupuestos dedicados y generosos, contar con socios e instituciones expertas, profesionalizadas y especializadas, no pensar que nosotros lo sabemos todo, valorar los seguros económicos de respaldo, estar informados y asesorados de lo que se nos viene encima, de cómo cambia el juego, los jugadores y sus reglas; esforzarnos como si todo dependiera de nosotros, pero teniendo la certeza de que habrá otros factores que no dependan de ti, de tu organización, y que la probabilidad de sufrir un ciberataque es cercana a cien .

Llegados a ese momento, de los incidentes de seguridad hay que aprender, las famosas lecciones aprendidas que permitirán a la organización a identificar acciones correctivas u oportunidades de mejora, para reducir la probabilidad de que el incidente se repita o reducir el impacto en caso de que suceda de nuevo. En definitiva, reducción del riesgo (al reducir probabilidad o impacto).

¡Suerte, el lobo ya está aquí, no seas avestruz!