LOS CERTs COMO HERRAMIENTA DE APOYO A LA CIBERDEFENSA EN LAS FUERZAS ARMADAS

Juan Carlos Polo González
Academia de Guerra del Ejército ecuatoriano

Resumen

El presente trabajo busca establecer una orientación en el manejo de la seguridad informática y su relación directa con la ciberdefensa, a través del desarrollo de una estrategia que facilite la detección, prevención, mitigación y eliminación de ataques informáticos, los mismos que son considerados como principales amenazas de una organización. Para esto, se analiza las diferentes formas en las que puede aparecer y desarrollarse un delito informático y el ámbito en el que se desenvuelve las normas ISO 27000, las mismas que pueden ser administradas en forma eficiente con la implementación de un centro de respuesta inmediata de seguridad informática, propuesta que ya es visualizada en este caso por parte del Comando Conjunto de las Fuerzas Armadas ecuatorianas para controlar esta amenaza.

En la actualidad, el problema radica principalmente en la falta de capacidad de respuesta que tienen las organizaciones contra eventuales ataques informáticos, los mismos que vulneran los protocolos de seguridad y las estrategias de prevención y control. Países europeos considerados a la vanguardia en este campo, ya han considerado entre sus prioridades la preparación de estas políticas.

Una estrategia para solucionar estos eventos es la incorporación de un centro de respuesta a incidentes informáticos inmediatos (COMPUTER EMERGENCY RESPONSE TEAM, CERT), el mismo que debe tener la capacidad de evaluar, coordinar y promover el desarrollo de servicios de prevención ante amenazas informáticas, las mismas que pueden presentarse en toda la infraestructura de una organización. Tomando como premisa fundamental que el personal que trabaje en esta organización debe contar con la capacitación y el entrenamiento especializado y que sus actividades deben orientarse a reaccionar en forma inmediata ante un evento de estas características.

Palabras clave: Ciberseguridad, ciberdefensa, Certs, seguridad informática, doctrina de seguridad

Desarrollo

El hombre nace como un individuo solo, pero su naturaleza de supervivencia lo encamina a agruparse, conformar un grupo para defenderse de los riesgos y peligros que se encuentran en su entorno. Así nacen las organizaciones estatales que permiten a base de un tributo, asegurar la estabilidad emocional y física de sus miembros. Con el advenimiento y desarrollo tan avanzado de la tecnología y los medios electrónicos se puede determinar que no todas las amenazas, en este caso informáticas, son físicas. El uso de la violencia no siempre termina en ataques físicos o en un conflicto. Hoy en día las guerras son asimétricas con acciones en varios campos como el político, económico, psicológico, electromagnético o cibernético.

En este caso puntual, el Estado como ente regulador, es el responsable de la seguridad nacional y para ello dispone de organismos e instituciones estatales, las mismas que deben enfocar sus misiones para asegurar, dominar y controlar sus campos de acción. Este carácter multidimensional debe alinearse con una doctrina de seguridad, doctrina que debe ser flexible en

sus organizaciones y que se adapte a los nuevos fenómenos que surgen como posibles factores de riesgo, amenazas y oportunidades.

Para ir a la par del entorno geopolítico regional, es necesario mejorar los procesos de seguridad informática organizacional. En la actualidad, con los nuevos escenarios planteados, se debe considerar que los ataques no solo provienen de otro Estado, sino de las nuevas amenazas tales como: narcotráfico, crimen organizado, terrorismo, ataques de piratas informáticos, grupos humanos opuestos a un determinado régimen, los desastres naturales, entre otros. Específicamente en las Tecnologías de Información y Comunicaciones, TICs., las amenazas principales son el espionaje, ataques dirigidos, ransomware, la ingeniería social, los crackers, el ciberterrorismo, entre otros.

Bajo este concepto se debe considerar a los ataques informáticos con una amenaza, no solo a los organismos estatales de seguridad sino a todas las organizaciones públicas y privadas en general, organismos que deben manejarse bajo un marco doctrinario que abarque la ciberdefensa y ciberseguridad. Para ello, se debe diferenciar estos dos conceptos que van de la mano y que engloban características similares, pero que no son iguales, y es necesario que todos los actores involucrados en estos sectores de la sociedad asuman la importancia estratégica del ciberespacio, así como de su uso seguro y responsable. En la actualidad, los organismos estatales de seguridad, algunos organismos públicos y algunas organizaciones privadas están llevando campañas de concienciación, especialmente dirigidas a estudiantes.

La tendencia del uso de la tecnología en nuestros días ha evolucionado el medio en el que se desenvuelve la sociedad. Directa o indirectamente, el ser humano necesita y hace uso de estas herramientas en su diario vivir. Cada día son más los incidentes relacionados a la violación de las seguridades informáticas. Todo esto, lleva a una desestabilización, vulnerabilidad y compromiso de la seguridad de una red de computadoras utilizando varios métodos y con distintos objetivos.

En el campo de la ciberseguridad, existen varios acontecimientos que podemos tomar en consideración a nivel internacional y nacional, tales como, el ataque a la página oficial de entidades públicas y privadas como Sony, Honda, Paypal, Fondo Monetario Internacional u otros delitos como: fallos de seguridad a servidores web, intrusión a copias de seguridad en la web, denegación de servicio, robo de datos, publicación dolosa de información estrictamente personal o los actuales ataques a dispositivos móviles. En base a los expertos en seguridad, la mayoría desarrolladores de antivirus, protocolos de seguridad o herramientas que ayudan a la seguridad, estos delitos siguen un mismo patrón de actividad: acceder al sistema explotando una vulnerabilidad y depositar una carga dañina de software maliciosa con un determinado fin.

La ciberdefensa y la ciberseguridad, son dos conceptos íntimamente ligados y abarcan procesos similares que los identifican en su naturaleza. Para comprender de una mejor manera esta relación, primero se debe entender los conceptos de amenaza, ciberespacio, ciberconflicto y ciberataque, para evitar futuras confusiones. La amenaza es la percepción de la capacidad que un potencial adversario posee para infringir un daño o perjuicio, el ciberespacio es el ámbito artificial creado por medios informáticos (RAE), el mismo que no tiene fronteras, el ciberconflicto es la confrontación entre dos partes utilizando la tecnología, y el ciberataque es un ataque desarrollado en el ciberespacio.

Ahora bien, Ciberseguridad es el conjunto de herramientas, procesos, directrices y métodos para proteger a los activos y usuarios de una organización, de un ataque malicioso ejecutado en el ciberespacio. La Ciberseguridad surge como un componente que garantiza el cumplimiento de las propiedades de seguridad de los recursos de una organización (UIT, 2012). La definición de Ciberdefensa comprende la aplicación de todas las acciones y medidas para proteger la

infraestructura de los sistemas de información y comunicaciones frente a los ciberataques y garantizar la Ciberseguridad (NATO, 2013). Una vez que se encuentran claros estos conceptos, es importante evaluar el grado de incidencia que tiene la afectación a la infraestructura crítica respecto a las Tecnologías de Información y Comunicaciones (TICs). Para conocer sus vulnerabilidades y por lo tanto para preparar una estrategia defensiva, tomando en consideración que mientras más la infraestructura critica se acerca al entorno remoto y administración por la vía de redes informáticas a través de redes LAN, MAN o WAN con accesos el internet, más será la vulnerabilidad a un ataque, sin que esto se considere una premisa, porque bien conocido es que también se puede sufrir un ataque al software y hardware, antes de que se conecte a la gran red o a un sistema en explotación.

Uno de los problemas más importantes que se debe plantear, es la implantación de procesos de seguridad informática, amparados en las ISO 27001/27002 (OSI) que son las normas de seguridad de la información desarrolladas por la Organización Internacional para la Estandarización como una guía de buenas prácticas, a fin de precautelar la información que se encuentra considerada como uno de los activos intangibles más importantes de una organización. La información obedece a cuatro principios fundamentales que son: confidencialidad, integridad (no repudio) disponibilidad y autenticidad, todo ello conocido como transabilidad. La seguridad informática puede clasificar su acción en medidas físicas y lógicas, las mismas que permiten evitar un daño producido por un ataque informático caracterizado por el deseo principal de robo de información. Los ataques informáticos pueden ser producto del conocimiento de hackers, cracker u otras dimensiones de piratas informáticos como los ataque de la ingeniería social entre otros, los mismo que pueden atacar a las diferentes capas del ciberespacio: física de infraestructura, lógica de hardware y cognitiva de percepción social (Ventre, 2012).

Existen muchos motivos por los cuales se cometen ataques informáticos, tales como el factor económico, político, protesta, ciberterrorismo. Los delitos informáticos a considerar deben estar enfocados no solo a robo de contraseñas o ingreso a perfiles de redes sociales. Debe ir más allá.

El desarrollo de los virus informáticos son cada vez más complejos, códigos de software maligno para realizar procesos como vaciar cuentas bancarias, el reciente ataque utilizando el ransomware dirigido contra copias de seguridad en la nube o explotar alguna vulnerabilidad en la infraestructura informática, narcotráfico, tráfico de armas, sistema de apuestas ilegales, stack pivoting y return and jump, nuevas técnicas de evasión de mecanismos de cuarentena sandboxing, envio masivo de correo no deseado spam, suplantación de los reminentes de mensajes con la técnica sppofing, uso de troyanos, uso de archivos Bot del Irc para el control remoto de sistemas y sustracción de información, ataque de fuerza bruta, de interposición man in the middle, ataques de waterring hole, botnet, secuestro de dominio, sidejacking o secuestro de sesiones, sniffer, sniffing, ciberbullying o grooming. Todos estos ataques se encuentran camuflados en software que circula en la red, ataques criminales que, desde el mundo virtual, están encaminados a destruir la infraestructura financiera y hasta económica de un país.

Un ejemplo de ello es el ataque mediático de ANONYMUS, el ataque de LULZSEC, o el ataque Dragonfly, una amenaza avanzada dirigida especialmente contra sistemas de control industrial en el sector energético en Europa, el robo de información personal en Orange – Francia, en el cual el incidente de seguridad permitió acceder a información de un millón trescientos mil clientes en el que se incluía nombres, apellidos, direcciones de correo electrónico, números de teléfono móviles y fijos, así como fechas de nacimiento. Los atacantes tienen un gran nivel de control y un amplio rango de recursos, además tienen la ventaja de decidir la naturaleza de la amenaza, como y cuando se va a realizar el ataque, empleando un sinnúmero de herramientas

disponibles en la red, las mismas que incluyen servicios legítimos. Independientemente del origen y naturaleza de la amenaza, la Ciberdefensa de una nación debe construirse sobre un conjunto de capacidades que le permitan alcanzar un estado de riesgo conocido y controlado.

Todos estos ataques sufridos en varios campos, ponen en alerta y revelan la necesidad de contar con protocolos de seguridad a fin de evitar estos actos ilegales. Una de las suposiciones más peligrosas que puede tener una organización, es que tienen conocimiento de cómo un atacante puede llegar a afectar la red. Por otro lado, se debe tomar en cuenta que la brecha digital se ha disminuido en los últimos años, tomando en consideración que la política estatal es brindar a la población servicios de internet más robustos y a un mayor número de individuos. La empresa privada ofrece mejores planes de acceso a internet: El 90% del tráfico internacional en Ecuador se realiza mediante dos cables de fibra óptica; en ambos casos, Ecuador solicitó "la entrega de una determinada capacidad internacional con acceso a la Internet, para uso de desarrollo social y educativo en la estación terminal de cable submarino" a ser administrada por el Fondo de Desarrollo de las Telecomunicaciones (FODETEL). Este recurso llega al 67% de los cantones del territorio nacional. El número de hogares conectados a Internet de banda ancha en 2013 es 891.000 (7.7%), el porcentaje conectado a la Internet de alta velocidad es 0.89%" (DELGADO, 2014). Según el Censo poblacional del 2010 el 33% de pequeños, el 46% de adolescentes y el 41% de jóvenes afirma tener un computadora, el 14% de los niños entre 6 y 9 años se declara internauta, mayores a 10 y menores de 18 años se declara usuario de internet (INEN, 2010).

La serie ISO 27000 aglomera todas las normativas en materia de seguridad de la información. Lo más importante de esta familia son las normas ISO 27001 e ISO 27002. La última de estas, antes conocida como ISO 17799 (modificó su nombre en el año 2007), y basada en la norma británica BS 7799, es un código de buenas prácticas para la realización de un Sistema de Gestión de Seguridad de la Información (SGSI). Está dividida en once dominios (por ejemplo, Seguridad física y del entorno o Control de accesos), y en cada uno de ellos se destacan cuáles son las mejores prácticas o los controles recomendados para dar seguridad en la organización. Esta norma no es certificable, para ello, está la norma ISO 27001, que es la que las organizaciones deben certificar. La misma contiene los requisitos que debe cumplir una organización, para estar acorde a las buenas prácticas enlistadas en las otras normas de la familia (especialmente la 27002).

Publicada en octubre 2005, hoy es la certificación en seguridad más popular y es aplicada por empresas de todo tipo en todo el mundo. Por último, la ISO 27001 también extiende, respecto a la importancia de "concientizar a los usuarios acerca de los peligros del software no autorizado o malicioso […] En particular, es esencial que se tomen precauciones para detectar y prevenir virus informáticos en computadoras personales" (BORTNIK, 2010).

Del mismo modo, y en relación con la defensa, las Fuerzas Armadas dependen de las Tecnologías de Información y Comunicaciones para comunicarse, ejercer el mando y control de las operaciones, obtener y distribuir información e inteligencia, realizar labores de vigilancia, reconocimiento o adquisición de objetivos o coordinar los fuegos. Todas estas tareas, como parte de la misión fundamental de la institución armada que es la defensa de la soberanía y la integridad territorial. En cada una de estas actividades, las TICs actúan como elemento multiplicador de la fuerza y optimizan la concepción, planificación y ejecución de las operaciones, pudiendo condicionar el desarrollo y resultado de una contienda. Por lo tanto, la posesión de una infraestructura tecnológica robusta, segura y resiliente, la sistematización de las dimensiones que componen el ciberespacio y su integración en la planificación operativa o la capacidad para actuar en este dominio, son algunos de los asuntos que más atención están recibiendo desde las Fuerzas Armadas (THIBER).

En el ámbito de operaciones militares, se debe tomar en cuenta los ataques informáticos especialmente en el componente del campo de batalla de mando y control y considerarlos como una amenaza a la libertad de acción. La pérdida de ella, en la conducción de las operaciones militares, es considerada como negativa para la operación. El Ministerio de Defensa Nacional indicó que considera al espacio cibernético como "vital" para la seguridad del Estado y sus ciudadanos, por lo que anunció el desarrollo de capacidades operativas pertinentes y políticas específicas (NACIONAL, 2014), es por ello que desde el año 2014, con el anuncio de la creación de un Comando de Ciberdefensa por parte del Ministerio de Defensa Nacional, a través del Comando Conjunto de las Fuerzas Armadas. Entidad que se dedicaría principalmente a la protección de infraestructura crítica para las operaciones del Estado. Con una inversión de 8 millones de dólares, se desea liderar el concepto de Ciberseguridad en esta institución militar y llegar a ser una organización a la vanguardia de la seguridad informática en Ecuador, ya que un ataque a la infraestructura informática en Fuerzas Armadas puede causar un impacto bastante fuerte en la seguridad integral del país o la intervención remota y maliciosa en la infraestructura de servicios básicos de un país como el caso de luz eléctrica o agua potable.

Existe varias estrategias de ciberseguridad y/o ciberdefensa, para determinar las tendencias y características más relevantes en base a: detección de activación maliciosa, detección mitigación y terminación de ataques, análisis dinámico de riesgos, ataque y daños, recuperación de ciberataque, toma de decisiones a tiempo, gestión de la información de Ciberdefensa o técnicas como pruebas de penetración, medidas de sensibilización y educación (España, 2012).

Planificar, desarrollar y establecer un centro de respuesta a incidentes informáticos, es otra respuesta que está tomada en cuenta por los países más desarrollados y que cuentan con los recursos necesarios. Estos centros conocidos como CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incedent Response Team) por sus siglas en Ingles. Esta iniciativa ya ha sido tomada por países vecinos, en la región trece países cuentan con Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT).

Los ataques informáticos en los últimos tiempos, han demostrado que todavía no se tiene una infraestructura adecuada para prevenirlos, y se evidencia la incapacidad de las organizaciones para enfrentar este tipo de amenazas, lo que ha obligado a considerar la importancia de la ciberdefensa en el entorno público y privado. Inicialmente, un CERT puede ser destinado para proporcionar servicio de respuesta inmediata a incidentes a nivel de la infraestructura informática critica clasificada en: software, hardware, base de datos, sistemas, redes internet, y posteriormente elaborar proyectos de investigación, innovación y transferencia tecnológica relacionados a temas de respuesta a incidentes y delitos informáticos.

Entre los procesos agregados de valor de un CERT se puede considerar: detección o identificación de la amenaza, bloquearla, monitorearla, reportarla, guardar registros y evidencias de la amenaza, responderla, pedir información a los organismos o actores involucrados, hacer uso de la infraestructura, comunicación transversal y horizontal con otros centros de apoyo.

El CERT debe estar en condiciones de identificar inconvenientes fundamentales, por ejemplo que las instituciones públicas y privadas no han coordinado sus políticas de manejo de información frente a la impunidad que existe actualmente en los delitos informáticos, a pesar que la normativa ya tiene implementado una serie de recursos legales. Otro de los objetivos de estos centros es el fortalecimiento de las capacidades técnicas y operativas de las instituciones gubernamentales para afrontar las amenazas y ataques cibernéticos, monitoreando la infraestructura critica, minimizando los riesgos vinculados a la información crítica de un Estado, reforzar la protección de los sistemas informáticos de las Fuerzas Armadas y Policía Nacional, reaccionar adecuadamente

ante los ataques cibernéticos que atenten contra la seguridad de una organización. Además, se debe coordinar con la Policía Judicial a fin de realizar programas de prevención, atención, investigación y apoyo a la judicialización de los delitos.

En resumen, un CERT tiene objetivos específicos enmarcados en cuatro grandes áreas que son: la autoridad, el escalamiento, la coordinación y la capacitación, todos ellos afianzan una sociedad de información segura. En base a los estándares internacionales, las mejores prácticas, la administración física y técnica de la seguridad y la personalización se puede establecer dos vías de manejo de la información; primera, la conveniencia que tiene la demanda; y, la segunda, la confianza en la entrega de la misma. Los objetivos que se desprenden son: la coordinación con los organismos estatales para la promoción de políticas, procedimientos, recomendaciones, protocolos y guías de seguridad informática y velar por su implementación, promover el desarrollo de nuevos centros en todos los niveles del Estado, ya sea público o privado, ofrecer servicios de información y prevención de amenazas informáticas y su respectiva respuesta a los incidente, coordinar en la formación de talento humano especializado en el campo de la seguridad que tiene relación con estas tecnologías, apoyar a otros organismos estatales de seguridad integral, fomentar un sistema de gestión del conocimiento, proveer al Estado la inteligencia necesaria para mitigar estos delitos tomando en consideración que el análisis necesario para identificar un atacante puede llevar meses de estudio, con la utilización de recursos informáticos y el respectivo personal capacitado.

Conclusiones

La tecnología avanza con mayor rapidez y con ello las amenazas informáticas a través del cometimiento ilícito de actos cibernéticos, especialmente ligados al manejo de información. Las principales amenazas están relacionadas con el narcotráfico, crimen organizado, fraude al fisco, fraudes económicos, resentimiento político, robo de información organizacional. Todos y cada uno de ellos, aprovechándose de las vulnerabilidades de la infraestructura informática de las organizaciones o de la ingeniería social en la parte humana de este campo, sin contar que los usuarios cada día comprometen más su privacidad, al no tener un adecuado manejo de contraseñas.

Los estados, como vigilantes de la seguridad integral, han adoptado mecanismos y herramientas para protegerse de estos ataques, y entre las principales estrategias es la creación de centros de atención a ataques informáticos con una respuesta inmediata en su accionar a través del uso de las tecnologías de visualización y análisis de datos, manejo de planes de contingencia y el aumento de alianzas corporativas entre la industria de la seguridad y los gobiernos.

En el Ecuador ya se han realizado algunos proyectos pilotos sobre este tema, y es el Ministerio de Defensa, a través del Comando Conjunto, quien quiere liderar el campo de la seguridad informática con la creación de un Comando de Ciberdefensa, el mismo que se encargará de protocolizar todas las actividades encaminadas a asegurar los procesos informáticos relacionados con la Información.

Referencias:

Bortnik, S, (2010). La serie de las normas ISO 27000. Obtenido de Seguridad Corporativa

CICTE-OEA, (2011). CERTS en América Latina

Delgado, J. A, (2014). Gobernanza de Internet en Ecuador: Infraestructura y acceso. Artículo presentadohttp. Quito.

España, M. d, (2012). El ciberespacio, nuevo escenario de confrontación. Imprenta del Ministerio de Defensa.
INEN, (2010). Censo poblacional
NACIONAL, M. D, (2014). Agenda Política de la Defensa. Quito
NATO, (2013). MC0571.
OSI, (s.f.). Organización Internacional de Estandarización.
RAE, R. A, (s.f.). Diccionario de la RAE.
Thiber, T. C, (s.f.). Instituto de Ciencias Forenses y de la Seguridad de la Universidad Autónoma de Madrid.
UIT, (2012).
Ventre, D, (2012).