Controles y Métricas Asociadas en el Contexto de la Ciberdefensa

Pablo G. Sack, Jorge Etherovic, Jorge S. Ierache
Facultad de Informática Ciencias de la Comunicación y Técnicas Especiales
Universidad de Morón
Cabildo 134 Morón, 5627 2000 int 189
sackpablo@gmail.com, jierache@unimoro.edu.ar

RESUMEN

El presente artículo presenta la línea de investigación aplicada en el contexto de la Ciberdefensa. Se presenta el modelo de un Framework basado en el análisis del estado del arte en materia de controles de seguridad y métricas para asistir a la gestión y diagnóstico de seguridad en el contexto de la Ciberdefensa. Finalmente se comentan los resultados iniciales

.

Palabras clave: Ciberespacio; Ciberguerra; Ciberdefensa; Seguridad Informática; Métricas; Control de Seguridad

CONTEXTO

El proyecto se inserta en la línea de investigación “Seguridad” de la Facultad de Informática Ciencias de la Comunicación y Técnicas Especiales de la Universidad de Morón, el proyecto se encuentra radicado en el instituto ISIER-UM., y se desarrolla bajo el marco del PID 01-001-16 financiado por UM

1. INTRODUCCIÓN

La constante evolución humana ha llevado a la generación de un nuevo espacio artificial que resulta transversal a los espacios naturales (terrestre, marítimo, aéreo, espacial) en los que la humanidad se desarrolla naturalmente. El nuevo ambiente o espacio denominado ciberespacio está plenamente integrado en las actividades humanas, no reconoce fronteras físicas ni estados naciones, permite la evolución de las operaciones en términos de interoperabilidad de los sistemas en los distintos ambientes naturales. Desde este nuevo espacio artificial se presenta un campo de batalla, presente en la puerta de cada computadora infectada por un software malicioso (malware) puede ser un elemento de ataque a gran escala a un país/agencia o empresa sin que su dueño esté enterado. Internet no es un lugar seguro, ya que hay personas que buscan delinquir en la red ya sea por diversión, por dinero, por motivos políticos, etc.

Ciberespacio

La palabra ciberespacio surge de la conjunción de la palabra “cibernao” -proveniente del griego que significa “pilotear una nave” y es utilizado comúnmente en el ámbito de las redes -, y espacio dando así la idea de estar piloteando o navegando sobre un mundo virtual. En la actualidad el ciberespacio se le da un significado más amplio al que se lo aglomera en la conjunción de toda la información disponible (digitalmente) junto con el intercambio de la información y las comunidades electrónicas que surgen en base al uso de esa información [1]. El Ciberespacio en el contexto del campo de batalla ha ido creciendo y convirtiéndose en algo más difícil de definir y defender [2]. En una visión particular de ciberespacio por parte de los autores propone como definición

del ciberespacio: al ámbito artificial transversal a los ambientes naturales (terrestre, marítimo, aéreo y espacial) que conforma el espacio virtual de interacción en el que se desarrollan actividades propias de humanos y máquinas relacionadas con la creación, procesamiento, publicación, almacenamiento, modificación y explotación de datos, información y conocimiento digitales, en un contexto distribuido (computación en nube) a través de redes interdependientes e interconectadas globales, públicas, privadas, híbridas, software y firmware de máquinas, cuyo carácter distintivo está dado por el empleo de las tecnologías de información y comunicaciones.

Ciberguerra

La ciberguerra es definida por Richard Clarke como las acciones realizadas por un estado Nación que penetra computadoras o redes de otras naciones con el propósito de causar daño o ruptura de las mismas. Estados Unidos (DoD) Cyber warfare (CyW) — Cualquier acto destinado a obligar a un oponente para cumplir nuestra voluntad nacional, ejecutado contra el software de control de procesos dentro del sistema de un oponente. [3]

Ciberdefensa

La Ciberdefensa es definida por La OTAN como: El desarrollo de la capacidad de prevenir, detectar, defenderse y recuperarse de los ataques cibernéticos [4]. Defensa implica [5] la capacidad de colocarse en el camino de penetración, identificar tal intento, y frustrar a través de la interrupción y suspensión de la tareas. Para este propósito, los sistemas informáticos se utilizan bloquear vías de acceso; limitación de permisos; verificación de identidad; proporcionar cifrado y habilitar la copia de seguridad y recuperación de desastres. Para Estados Unidos (Comprehensive National Cybersecurity Initiative (CNCI)): La defensa de todo el espectro de amenazas mediante la mejora de las capacidades de contrainteligencia de EEUU y el incremento de la seguridad de las cadenas claves de suministro de información [6].

Controles de Seguridad

En el contexto de la Ciberdefensa para su estudio se propone armar una base sólida y progresiva de controles de seguridad tomando como esqueleto y estructura el documento "The Critical Security Controls for Effective Cyber Defense" [7]: este documento está divido en veinte controles críticos de seguridad que contienen a su vez un grupo de subcontroles. Dichos subcontroles se categorizan con el fin de implementar controles de manera progresiva y escalonada de la siguiente forma: a) Logros Rápidos: Gran reducción de riesgo, poca inversión financiera y técnica; b) Medidas de Visibilidad y Atribución: Mejoran el proceso, la arquitectura y las capacidades técnicas para monitorear sus redes y sistemas informáticos; c)Mejora de la Configuración de Seguridad de la Información: Estos subcontroles ofrecen reducir el número y magnitud de las vulnerabilidades de seguridad y mejorar las operaciones de los sistemas informáticos en red; d) Subcontroles Avanzados: procedimientos que proveen máxima seguridad pero son difíciles de implementar, por ser más caros o requiere de personal altamente capacitado.

Complementar la base de controles de seguridad con lo planteado en "Strategies to Mitigate Targeted Cyber Intrusions" [8]: El documento está dividido en tres partes y realizado por el Departamento de Defensa de Australia y se compone de la

siguiente manera: a) Mitigation Strategies 2014: contiene una breve introducción y un poster con el resumen de las treinta y cinco estrategias para mitigar ciberataques; b) Mitigation Strategies 2014 Details: Describe cada una de las treinta y cinco estrategias para mitigar ciberataques y sus controles recomendados; c)Information Security Manual 2014 Control: Describe los controles mencionados en el documento anterior.Complementar la base con el documento de "Security and Privacy Controls for Federal Information Systems and Organizations (800-53 Rev.4)" [9] que forma parte de un "ciclo de vida de la seguridad".Por último se toma como punto de partida y de referencia el documento "Framework for Improving Critical Infrastructure Cybersecurity" de National. [10]. El mismo está compuesto de tres partes principales. a) Núcleo: Está compuesto por un conjunto de actividades de ciberseguridad, resultados deseados y referencias. Se compone de cinco funciones concurrentes y continuas: Identificar, Proteger, Detectar, Responder y Recuperar. A su vez, cada una de estas funciones principales se dividirá en Categorias, Subcategorias y Referencias informativas. b) Niveles de Implementación: Proporciona un contexto sobre cómo una organización ve los riesgos de ciberseguridad y los procesos para gestionar ese riesgo. Se compone de cuatro niveles: Parcial, Riesgo Informado, Repetible y Adaptativo. c) Perfiles: Representa los resultados en base a las necesidades del negocio que una organización ha seleccionado de las categorías y subcategorías del marco de trabajo.

Métricas

Se seleccionaron los siguientes documentos que contienen un gran número de métricas que se aplicarán en la elaboración del marco de trabajo, siendo los mismos: The CIS Security Metrics [11], "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report " [12],"Cyber Resiliency Metrics V 1.0 Rev.1" [13] y "Measurement, Identification and Calculation of Cyber Defense Metrics" [14].

2. LINEAS DE INVESTIGACIÓN Y DESARROLLO

Las líneas de investigación se corresponden con las normas y métricas en el marco de la ciberdefensa, se explora el desarrollo de frameworks aplicados al diagnostico de una unidad. En el marco de las futuras líneas se considera la incorporación de sistemas basados en conocimientos para asistir al diagnostico en materia de ciberdefensa

.

3. RESULTADOS OBTENIDOS/ESPERADOS

Modelo de Framework

Sobre la base de controles y el marco de trabajo presentados en la sección anterior, se elaboro el Modelo de Framework [15], [16] que facilita la implementación de controles de manera progresiva y realiza un seguimiento de avance a través de las métricas en cada uno de los controles, ofreciendo documentos de consulta por cada control involucrado y links sugeridos. Para esto utilizamos la división de los controles de seguridad propuestos en Framework for Improving Critical Infrastructure Cybersecurity [10]. Dicho documento plantea una división de los controles de seguridad propuestos en cinco fases. Estas fases aglutinarán controles de seguridad que cumplan con el objetivo de cada fase. Las fases serán: **Identificar** (recursos permitidos de la empresa como Hardware, Software, PCs,

etc,); **Proteger**: (configuraciones de Hardware y software, usuarios, contraseñas, cifrados, etc.); **Detectar**: vulnerabilidades, códigos maliciosos, desactualizaciones, accesos no autorizados, etc.; **Responder**: Aislamiento de dispositivos, administración de Logs, eliminación de dispositivos, etc.; **Recuperar**: tiempo, daño, restauración, generación de backups, etc.

Iteraciones dentro del marco de trabajo

Adicionalmente a la división de los controles de seguridad en cada una de las fases, el marco de trabajo constará de cuatro iteraciones que cruzarán todas las fases del mismo. Estas iteraciones tendrán como objetivo lo descripto en la categorización de los subcontroles comentados en la sección anterior del documento The Critical Security Controls for Effective Cyber Defense [7], logrando así la conformación de una grilla que permitirá ubicar los controles de acuerdo a la fase (Identificar, Proteger, Detectar, Responder, Recuperar) e iteración. Las cuatro iteraciones se clasifican como: **a) Logros Rápidos** (primera iteración)**; b) Medidas de Visibilidad y Atribución** (segunda iteración); **Mejora de la Configuración de Seguridad de la Información** (tercera iteración); **d) Subcontroles Avanzados** (cuarta iteración).

Se desarrollo un demostrador del Framework que permitió una evaluación orientada a la primera cuadrícula correspondiente a los controles de seguridad de dos de los documentos previamente seleccionados ([7] y [8]) e incorporando a cada uno de los controles de seguridad dentro del framework propuesto Ejemplo de una interacción se observa en la Fig.1

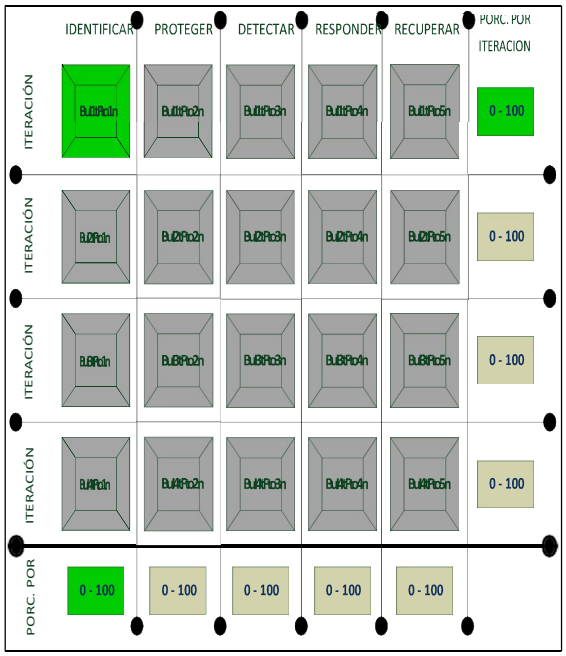

Figura 1.Framework. Iteración 1- Logros Rápidos/ Fase 1 Identificar

4. FORMACIÓN DE RECURSOS HUMANOS

El grupo trajo se conforma de dos investigadores formados un investigador alumno. Se finalizo una tesis de grado en relación a la línea de investigación presentada.

5. BIBLIOGRAFÍA

[1] David A Umphress, T.C. "El Ciberespacio": ¿Un Aire y un espacio Nuevo?, Air&Space Power Journal, august 2007.

[2] Geers, K. A, "Brief Introduction to Cyber Warfare". Common Defense Quarterly, pp16-17, Spring 2010

[3] Alford Jr., Lionel D, CYBER WARFARE: PROTECTING MILITARY SYSTEMS., 2000. (Disponible: https://turnitin.com/viewGale.asp?r=53.8117643938158&svr=06&lang=en_us&oid=25740519&key=427186604ab0a08b8bbb71d05c16f6f4)

[4] C. Czosseck, R. Ottis, K. Ziolkowski, 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON 2012),

C. , pp162, Disponible:https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2012_Proceedings_0.pdf)

[5] Tabansky, L. “Basic Concepts in Cyber Warfare”, Military and Strategic Affairs , vol. 3. N° 1 , pp. 75-92 , May 2011.

[6] The Comprehensive National Cybersecurity Initiative, (Disponible:https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative)

[7] The Critical Security Controls for Effective Cyber Defense. Version 5 (CSC-5) del “Council on CyberSecurity. https://www.sans.org/media/critical-security-controls/CSC-5.pdf

[8] Strategies to Mitigate Targeted Cyber Intrusions” del “Department of Defense – Intelligence and Security of Australian Government.http://www.asd.gov.au/infosec/mitigationstrategies.htm

[9] Security and Privacy Controls for Federal Information Systems and Organizations (800-53 Rev.4) de National Institute of Standards and Technology (NIST).http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[10] Framework for Improving Critical Infrastructure Cybersecurity de National Institute of Standards and Technology (NIST).http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[11] The CIS Security Metrics. The Center for Internet Security, november 2010.(Disponible: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf)

[12] Measurement Frameworks and Metrics for Resilient Networks and Services, Technical report ENISA, february 2011.

[13] Deb Bodeau, Rich Graubart, Len LaPadula, Peter Kertzner, Arnie Rosenthal, Jay Brennan “Cyber Resiliency Metrics V 1.0 Rev.1”., MITRE , april 2012.

[14] Juan E. Sandoval, Suzanne P. Hassell. “Measurement, Identification And Calculation Of Cyber Defense Metrics”, MILCOM, pp. 2174-2179,october 2010.

[15] Sack, P , Ierache, J “Controles de seguridad propuesta inicial de un framework en el contexto de la ciberdefensa” XXI CACIC (Junín, 2015) 11p, ISBN: 978-987-3806-05-6

[16] P. G. Sack and J. S. Ierache, "Initial proposal of a framework in the context of cyberdefense to articulate controls and metrics associated," Computing, Communication and Security (ICCCS), 2015 International Conference on, Pamplemousses, 2015,pp.1-6.doi: 10.1109/CCCS.2015.7374178
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7374178&isnumber=7374113ieee