FRENTE A LAS AMENAZAS DE SEGURIDAD CIBERNÉTICA

"Al ser un nuevo dominio en defensa y seguridad, las Fuerzas Armadas y de Seguridad de América Latina han estado aprendiendo a enfrentar nuevas amenazas y desarrollar capacidades. Uno de los principales desafíos es obtener las soluciones integradas adecuadas de la industria, que deben incluir capacitación y la capacidad de trabajar de manera sistémica dentro de las estructuras existentes de las fuerzas".

Por Santiago Rivas.

Esta publicación, proveniente de la revista argentina Pucará/Defensa, ha sido autorizada por el Autor.

Las amenazas cibernéticas están creciendo en todo el mundo y América Latina no es la excepción, habiendo sufrido una amplia gama de ataques que afectaron a instituciones civiles y estatales, incluidas las Fuerzas Armadas de algunos países, siendo el reciente caso del Ejército chileno un exponente de eso.

El dominio cibernético plantea una amenaza híbrida, que combina cada vez más los ataques cibernéticos patrocinados por el estado con el cibercrimen con fines de lucro, lo que podría afectar tanto a la infraestructura física como a la cibernética. En los últimos años, los ataques dirigidos a sistemas de hardware y software que monitorean y controlan activos físicos, equipos y procesos se han vuelto cada vez más frecuentes y están siendo habilitados por la creciente convergencia de los mundos de TI (Tecnología de la Información), OT (Tecnología Operativa) e IoT (Internet de las Cosas), que conectan cada vez más los mundos digital y físico.

Para enfrentarlos, las principales preocupaciones de los gobiernos y, especialmente, de las Fuerzas Armadas y de Seguridad, no es solo contar con las mejores plataformas, sino también que sean sencillas de usar y que el personal pueda ser entrenado adecuadamente.

Dado que la mayoría de los ataques ocurren debido a errores humanos de la parte atacada, principalmente debido a la falta de conciencia por parte de las personas de las instituciones objetivo, su capacitación es fundamental, para que puedan ser conscientes de las amenazas y actuar en consecuencia para no abrir el acceso a los piratas informáticos.

Centro de Operaciones de Seguridad Global Leonardo en Chieti, Italia.

Para conocer más sobre las soluciones actualmente en el mercado, hablamos con Angelo Giovinazzo, Head of Cyber & Security International Business Development de Leonardo, una empresa que actualmente ofrece una amplia gama de soluciones y capacidades, incluyendo un entorno de formación basado en la simulación realista de escenarios (gemelos digitales) para preparar al personal y mejorar los procesos. Leonardo proporciona servicios y soluciones para identificar, prevenir, detectar y responder a los ataques cibernéticos aprovechando un enfoque completo de la seguridad cibernética de acuerdo con el marco del National Institute of Standards and Technology (NIST) y una visión sistémica de la seguridad que integra la protección física y digital.

Un gran problema en la región es que, debido a los bajos salarios de las Fuerzas Armadas, las personas que preparan para la ciberdefensa, una vez que obtienen un alto nivel de conocimiento, se van al

sector privado, en promedio después de aproximadamente dos años trabajando para las fuerzas. Por lo tanto, las fuerzas tienen que seguir entrenando a las personas todo el tiempo y necesitan hacerlo rápido y fácilmente.

"*Estamos de acuerdo en el escenario que estás describiendo*", comenzó explicando Angelo, y describió que, por ejemplo, "*Chile ha sido un país blanco de muchos ataques: hace cinco años, los hackers atacaron el Banco de Chile, el segundo banco más grande del país, y sufrieron graves pérdidas financieras, algunos otros bancos en Chile han sido atacados y más recientemente también el Ejército y Carabineros sufrieron un ataque y muchos datos han sido robados. La misma situación se puede detectar en Colombia para el dominio bancario y también en Brasil, que es definitivamente el país que más ataques cibernéticos ha tenido, registrando más del 28% de los ataques de phishing en América Latina.*

Existe una situación similar en toda la región latinoamericana. Hay una brecha en términos de inversiones y conciencia de los riesgos cibernéticos que debe llenarse. Por esta razón, para los hackers de América Latina, y especialmente los sectores bancario y gubernamental, son una prioridad como objetivo".

Academia de Seguridad Cibernética.

Esta situación de falta de conciencia es la razón por la cual una de las principales preocupaciones en la región es cómo preparar a la gente para ser consciente de las amenazas.

Angelo explica que es por eso que ofrecen la capacitación en conciencia cibernética sobre los riesgos como una prioridad.

"*Muchos países, también en Europa del Este, están invirtiendo mucho para desarrollar campañas masivas de capacitación en conciencia cibernética para capacitar a los empleados también con cursos de capacitación muy básicos, no solo cursos específicos o de alto nivel.*

Me refiero a cursos de capacitación solo para desarrollar una conciencia cibernética sobre los riesgos en los que podría incurrir el empleado o la institución", explica Angelo y dice que esta es la razón principal por la que Leonardo decidió invertir en la Academia de Ciberseguridad y Seguridad.

"*La Academia no solo se basa en capacitar a las personas para enfrentar el ciberataque. También es para que el resto de la organización sea consciente de cómo lidiar con eso*", explica Angelo y agrega que el objetivo de la Academia también es desarrollar la capacidad local en el país, involucrando, por ejemplo, una universidad.

"*Hicimos esto en Medio Oriente hace solo unos meses, recibimos a 20 capacitadores de una universidad local, el concepto es desarrollar una asociación con la universidad en el país. Capacitar a los capacitadores y que luego puedan desarrollar capacitación en el país.*

En primer lugar, hemos transferido la capacidad de desarrollar cursos de formación específicos en el país. Y en segundo lugar, el país puede tener los beneficios de tal capacidad local teniendo campañas masivas de capacitación de personas. Esto es muy útil para grandes organizaciones como ministerios", explica Angelo.

La plataforma Cyber Range de Leonardo para pruebas y entrenamiento cibernéticos.

Simulación.

"*El entrenamiento es la primera parte de la historia*", dice Angelo y explica que, una vez que las personas están entrenadas, es necesario probar su capacidad de reacción contra un ataque real. "*Piensa en una infraestructura muy compleja, una gran red de TI o una compañía de petróleo y gas que no solo tiene una red de TI, sino también alguna tecnología OT involucrada. Si deseas probar la capacidad de reaccionar contra amenazas cibernéticas reales, no puedes usar la infraestructura real. Entonces, desarrollamos una plataforma llamada Cyber Range, que crea un 'gemelo digital' de la infraestructura real.*

Utilizando gemelos digitales de redes, sistemas y aplicaciones a proteger, así como amenazas y herramientas tanto para ataque como para defensa, tanto individuos como grupos podrán poner en práctica las habilidades adquiridas durante el entrenamiento para defender la infraestructura.

Diseñado con los principios de la gamificación (utilizando mecanismos similares a los de los juegos, con la asignación de objetivos y recompensas por cada logro), el Cyber Range aprovecha tanto la virtualización como la interoperabilidad para simular escenarios operativos inmersivos. Tienes un equipo rojo, compuesto por 'hackers éticos', expertos de Leonardo que atacan la plataforma virtual, y los aprendices, los equipos azules, tienen que defender la plataforma. De esta manera, puedes medir la capacidad de tus oficiales para contrarrestar una amenaza real.

Esto es algo que en Latinoamérica buscan muchos clientes, les interesan las plataformas como Cyber Range para crear Academias locales, para capacitar a sus propios oficiales, porque esta es la única forma en que puedes medir tu capacidad para contrarrestar amenazas reales. De lo contrario, es solo una capacidad teórica, pero no es suficiente en el dominio cibernético". Este tipo de capacitación es considerada esencial por las organizaciones de ciberseguridad y ciberdefensa en América Latina, para poner a prueba sus capacidades y aprender a lidiar con las amenazas en escenarios reales.

Para que un gran número de personas realicen una capacitación básica o simplemente adopten la conciencia sobre la seguridad cibernética, pueden usar la plataforma de capacitación cibernética, que se puede proporcionar en línea. "*Tenemos diferentes alternativas dependiendo del requisito, es totalmente diferente si tienes que capacitar a 40,000 empleados, o quieres capacitar a 100 personas. También el nivel de experiencia que tienen es importante y, por supuesto, el dominio con el que trata la organización. Si estamos hablando de defensa, tenemos cierta experiencia y podemos proponer ciertos cursos de capacitación, si estás hablando del Ministro de Seguridad Pública, es otra historia. Por lo tanto, teniendo esto en cuenta, necesitamos desarrollar un programa de capacitación específico y personalizado*".

En este sentido, Angelo pone un ejemplo de campañas masivas, para capacitar a las personas de una organización para enfrentar una de las formas

más sencillas de atacarla, como es el phishing, que consiste en enviar comunicaciones fraudulentas que parecen provenir de una fuente legítima y acreditada para robar dinero, obtener acceso a datos sensibles e información de inicio de sesión, o para instalar malware en el dispositivo de la víctima. "*Normalmente, cuando realizamos una campaña de ciberconciencia muy masiva, la idea es, en primer lugar, realizar phishing simulado, lo llamamos una campaña de 'White phishing', para medir la robustez de las personas para reaccionar ante correos electrónicos sospechosos, por ejemplo. Así que desarrollamos una campaña de White phishing y medimos el número de personas que no reconocen que esto es phishing. Después de eso, realizamos cursos de capacitación de manera masiva y luego puedes volver a hacer White phishing, solo para medir la diferencia en términos de cómo las personas ahora están listas para contrarrestar la reacción*".

Angelo también agregó que más del 85 por ciento de los ataques exitosos dependen de errores humanos, "*esta es la razón principal por la que nuestros clientes están invirtiendo en capacitación cibernética. De lo contrario, incluso si tiene una plataforma de seguridad cibernética muy robusta y certificada, si el operador no puede reaccionar contra una simple campaña de phishing, pierde*".

La sede de Leonardo Cyber & Security Academy.

Protección sistémica.

Si bien la ciberdefensa está directamente relacionada con ataques físicos a infraestructuras o personas, la compañía desarrolló la plataforma X-2030, con una visión sistémica de seguridad que integra la protección física y digital. Al hacerlo, la compañía puede ayudar a los clientes de defensa a proteger su infraestructura crítica, como bases militares, puertos y aeropuertos, asegurando la resiliencia. El X-2030 es una solución avanzada de software C5I (Comando, Control, Comunicación, Computación, Cibernética e Inteligencia) que integra aplicaciones existentes y tecnología avanzada de sensores, recopilando y analizando grandes cantidades de datos de todos los dominios (tierra, mar, aire, espacio, ciberespacio). La plataforma puede extraer información relevante y proporcionar alertas a los operadores, lo que permite una toma de decisiones rápida y de alta calidad, y hablamos con Angelo sobre ello y cómo se opera. "*Este es un concepto nuevo, nuestra plataforma es una de las pocas capaces de realizar la fusión de datos integrando información proveniente de sensores físicos, bases de datos y el mundo de código abierto. Normalmente tienes unos pocos operadores para monitorear una gran cantidad de cámaras en las grandes ciudades, si también incluyes las cámaras privadas, tienes millones de cámaras monitoreando eventos. Luego consideras otros sensores, como sensores de incendio, por ejemplo. Necesitamos un algoritmo específico que pueda detectar lo que está sucediendo. Nuestra solución llamada Ganimede, que está integrada en la plataforma X-2030, puede analizar automáticamente la transmisión de video de las cámaras, detectando una situación anormal, por ejemplo, una matrícula en una lista negra, o personas peleando,*

personas gritando, un disparo. Disponemos de más de 20 algoritmos diferentes, basados en Inteligencia Artificial, monitoreando automáticamente miles de cámaras y proporcionando al operador una alarma en caso de que detectemos este tipo de situaciones. Dependiendo del evento, debido a que X-2030 entiende qué tipo de eventos están ocurriendo, sabemos qué necesitamos. Si se trata de un incendio, en primer lugar, necesitamos detectar dónde se encuentra. Necesitamos entender si hay otras cámaras alrededor del lugar donde se ha detectado el incendio. Si no tenemos cámaras, podemos tratar de encontrar la información en otro lugar. Normalmente, hoy en día hay muchas personas moviéndose con teléfonos móviles y, en caso de un evento, toman una foto o un video del evento y lo publican en Instagram. Podemos usar esto como un sensor, porque X-2030 entiende que hay alguien en Instagram hablando de un incendio en esa calle, y utiliza la información para proporcionar al operador una conciencia situacional completa.

La plataforma realmente ayuda al operador a gestionar el evento, proporcionando también información sobre los recursos que puede utilizar y sugiriendo cómo reaccionar. Con un movimiento muy simple de su dedo en el mapa, el operador puede realizar una llamada grupal porque el sistema localiza todas las fuerzas policiales en el área, los bomberos, ambulancias.

Usted sabe que las fuerzas policiales, ambulancias, bomberos suelen utilizar diferentes tecnologías y estándares de comunicación (la policía que utiliza redes TETRA o P25, las ambulancias usan DMR o redes 5G estándar, por ejemplo): para hablar entre sí necesitan una solución que integre banda estrecha y banda ancha y permita la interoperabilidad, eso es RIM, la solución de red híbrida multiportadora de Leonardo, integrada en la plataforma X-2030", describe Angelo.

Plataforma X-2030.

Contra los ciberataques.

Para prevenir y responder a los ataques cibernéticos, la compañía ofrece servicios administrados a través del Centro de Operaciones de Seguridad (SOC), que es una instalación con operadores dedicados de muy alto nivel, educados en el dominio cibernético, que tienen herramientas para monitorear continuamente la red del cliente, el tráfico, la TI, para detectar de antemano que algo malo está sucediendo. "*Tienes dos posibilidades, podemos implementar algunas contramedidas de nuestro SOC porque, por ejemplo, una empresa compartió información de que el router ABC tiene un problema y lanzaron una nueva versión del software con un parche para ser instalado. En este caso, nuestro SOC implementa automáticamente la actualización a la red del cliente. Por otro lado, nuestro SOC puede monitorear el tráfico en la red para verificar si alguien está tratando de atacar. Y nuestros expertos pueden responder utilizando herramientas específicas dedicadas y su propia capacidad para comprender que algo malo está sucediendo. Este es un servicio específico proporcionado por el SOC*", describe Angelo.

Como muchos clientes quieren tener su propio SOC, Leonardo puede proporcionar el diseño y las tecnologías al cliente, capacitar a sus propios funcionarios y permitirles administrarlo. Fueron adjudicados en 2021 para diseñar y construir el nuevo Centro de Operaciones de Ciberseguridad de la Agencia Espacial Europea (ESA). "*Este es el caso de todos los Ministerios de Defensa, porque quieren tener su propio SOC y no dejarlo en manos de otra persona que monitoree la red. En el caso de instituciones como la ESA, construiremos su SOC, pero será operado bajo la responsabilidad técnica de su Oficina de Seguridad. Depende del cliente, algunos clientes prefieren comprar el servicio, gestionado por nosotros, algunos otros como las fuerzas de defensa o policiales prefieren tener su propio SOC y gestionarlo, porque quieren mantener un control completo sobre los datos sensibles*", explica Angelo. "*También podemos apoyar de forma remota a las personas que gestionan el SOC localmente. Entregamos la plataforma; capacitamos a los oficiales y apoyamos al cliente en la primera fase de las operaciones para permitir que sus operadores sean independientes*", agrega Angelo.

Dijimos que Leonardo utiliza algoritmos de inteligencia artificial para el análisis de video, para detectar las situaciones que requieren atención, pero la IA también se puede usar para la inteligencia de amenazas cibernéticas, "*El sistema de inteligencia de amenazas de Leonardo utiliza la infraestructura informática de alto rendimiento de la compañía, analizando automáticamente más de 5 millones de indicadores de compromiso cada año (rastros digitales de incidentes de TI), la gran cantidad de datos de las redes sociales (SOCMINT), y fuentes abiertas (OSINT), incluidos sitios web y medios, bases de datos o informes públicos, imágenes fotográficas o datos satelitales. Recopila la información correcta, realiza una correlación cruzada y presenta al operador la información correcta, lo que le permite administrar el evento*", describe Angelo, ya que una de las cosas más importantes para los operadores en seguridad cibernética es cómo fusionar toda esta información y obtener la alerta para que puedan escalar la respuesta a estas amenazas. Por lo general, los C-SOC manejan demasiados ataques pequeños y necesitan saber cuáles son importantes y cuándo actuar contra ellos. Como ejemplo, desde Leonardo explican que en su Centro de Operaciones de Seguridad en Chieti gestionan 137.000 eventos de seguridad por segundo procedentes de los sistemas de monitorización de las infraestructuras de los clientes gestionados, lo que genera automáticamente más de 1.800 alarmas de seguridad (Delito de Seguridad) y cada año, el SOC Global de Leonardo maneja alrededor de 21.600 incidentes de ciberseguridad. "*Obviamente, utilizamos la automatización en este análisis. Lo importante es una combinación entre tecnología avanzada para realizar análisis y analistas calificados porque uno sin el otro no pueden funcionar*".

Operaciones ofensivas.

A pesar del interés de las Fuerzas Armadas de América Latina en tener capacidades para realizar operaciones ofensivas, Angelo explica que hay dos cuestiones a considerar en este dominio para Leonardo: "*En primer lugar, hay regulación europea que limita la posibilidad de utilizar la capacidad cibernética ofensiva y la segunda es la ética Leonardo para proporcionar al cliente este tipo de herramientas*".

Una ventanilla única.

Una de las ventajas de Leonardo es que sus soluciones de ciberseguridad se basan en un know-how muy fuerte basado en su amplia experiencia desarrollando soluciones de seguridad y comunicaciones profesionales, "*por lo que sabemos exactamente cómo funciona una fuerza policial y cuáles son los requisitos. También tenemos fuertes capacidades para proporcionar la solución para la inteligencia, porque desarrollamos todas las plataformas para que los Carabinieri italianos desarrollen la investigación y hemos desarrollado la plataforma y la capacidad interna para gestionar el cibercrimen. Por lo tanto, nuestro diferenciador podría ser la posibilidad de cubrir no solo una plataforma como la que se puede encontrar en el mercado que proporciona inteligencia o simplemente ciberdefensa, sino una cartera integral que abarca comunicaciones, inteligencia, capacitación y también plataformas, todo integrado en el comando y control*", explica Angelo. Además, como trabajan todo el día brindando servicios a sus clientes, monitoreando sus redes en busca de amenazas, el personal de la empresa se capacita constantemente. El trabajo en los sectores de defensa y seguridad y aeroespacial también implica que sus soluciones deben estar aseguradas por diseño y, como ejemplo, Angelo dice que utilizan el Cyber Range para verificar la resiliencia cibernética de sus plataformas. "*Si quieres comprobar si alguien puede atacar un helicóptero, podemos simular la plataforma del helicóptero, la red de TI del helicóptero y podemos tratar de entender si es fácil o no atacarlo. Por lo tanto, nuestros colegas de la división de helicópteros nos están utilizando como consultores para verificar la resistencia de los helicópteros*", agrega. Esto significa que la compañía puede proporcionar una amplia variedad de herramientas, que están probadas e integradas, con un sistema de capacitación integral y con el apoyo de un equipo de personas con vasta experiencia en el tratamiento de ataques cibernéticos, proporcionando una solución completa para enfrentar todas sus amenazas en el dominio cibernético.

Santiago, 16 de agosto de 2023.