Daniel Andrés Birchner, 30-9-2023

PANORAMA ACTUAL DE LA CIBERSEGURIDAD EN AMÉRICA LATINA: AMENAZAS Y POSIBILIDADES

En los últimos años, el ritmo de ataques cibernéticos contra la infraestructura de gobierno en países latinoamericanos ha ido en aumento. Con alarmantes tasas de crecimiento anual, esta modalidad pone en evidencia las profundas deficiencias (y por otro lado, los logros) de la ciber seguridad en América Latina. Entre las deficiencias, podemos encontrar una progresiva aunque aún ineficaz matriz de ciber-diplomacia, como también la falta de conciencia sobre las vulnerabilidades y la poca inversión y capacitación que de ello resulta. Sin embargo, a partir de 2012 comenzaron a tenerse en cuenta los posibles peligros que trae aparejada la creciente digitalización de la administración pública, así como la delimitación teórico y práctica de su campo de acción y su relación con la defensa. Existen varios estudios que abordan la cuestión de la ciberseguridad en América Latina, sin embargo, los enfoques muchas veces son profundamente técnicos y carecen de una perspectiva holística que permita tener un panorama general de la situación. En este artículo analizaremos brevemente la situación general actual de la ciberseguridad en América Latina, teniendo en cuenta sus antecedentes y las consideraciones teóricas necesarias.

Panorama general de ataques en la región

De acuerdo a las estadísticas de Fortinet[1], los ciberataques en América Latina y el Caribe aumentaron 600% (un 10% de los ciberataques en todo el planeta) en 2022, contando 360 mil millones de intentos de ciberataques. En primer lugar se posiciona México (187 mil millones de ataques), seguido por Brasil (103 mil millones), Colombia (20 mil millones) y finalmente Perú (15 mil millones). Los destinarios más comunes suelen ser las empresas privadas (dado el aumento del trabajo remoto a partir de 2020), seguido por instituciones estatales (distribución de servicios, recursos y en menor medida instituciones militares). De acuerdo a TIVIT, compañía multinacional líder en técnica con presencia en diez países de la región, los móviles son la ganancia financiera (33%), seguido de la denegación de

[1] Fortinet / FortiGuard Labs (2023) – Annual Report 2022. Available: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

servicios (31%) y el robo de datos (22%)[2]. En cuanto a las modalidades más comunes, se encuentran el phishing (suplantación de identidad), los ataques de *man in the middle* y ataques DDoS (denegación de servicio).

La Ciberdiplomacia en la región

Por Ciberdiplomacia se entiende la cooperación internacional en el ámbito cibernético, desde distintas perspectivas y referente a variados espacios y ámbitos de acción. En la ciberdiplomacia se estudian los aspectos de seguridad y la protección, como también la incorporación de tecnologías de información (IT) en comunicación y economía.[3]

En América Latina, la Organización de Estados Americanos (OEA) representa, desde su creación en 1948, el más alto nivel de integración regional. A fines de 1990, la organización americana ya contaba con un innovador Grupo de Trabajo de Delitos Informáticos, y en 2004, lanzó su Estrategia de Seguridad Cibernética[4]. Esta propuesta tenía como antecedente inmediato la anterior declaración del Comité Interamericano contra el Terrorismo (CICTE), que más temprano ese mismo año había declarado esfuerzos conjuntos para combatir el terrorismo cibernético, cualquier sea su origen y/o motivación. El CICTE es el encargado, en términos prácticos, de poner en marcha las coordinaciones emanadas de la OEA en este sentido. En este marco, en 2016 el CICTE lanzó el Programa de Seguridad Cibernética, consistente en el intercambio de inteligencia, especialistas, información u alertas relacionadas a la seguridad cibernética entre los países miembros.

Paralelamente, en América Latina existe desde 2016 el Observatorio de la Ciberseguridad en América Latina y el Caribe, un desarrollo conjunto de la OEA y el Banco Interamericano de Desarrollo. Esta institución permite la medición y verificación del estado de desarrollo de medidas seguridad cibernética en los países constitutivos, brindando orientación y estándares comunes de evolución y definiendo criterios comunes de avance (Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones). A nivel regional, las instituciones y marcos normativos son el Grupo Agenda Digital

[2] TIVIT (2021) - *¿Cuáles son los ciberataques más frecuentes en América Latina?* Disponible en: https://latam.tivit.com/prensa/cuales-son-los-ciberataques-mas-frecuentes-en-america-latina

[3] VEGA, J, (2023) – *Ciberdiplomacia en América Latina: niveles, enfoques y velocidades.* Disponible en: https://www.realinstitutoelcano.org/analisis/ciberdiplomacia-en-america-latina-niveles-enfoques-y-velocidades/

[4] AG/RES. 2004 Estrategia de Seguridad Cibernética.

(MERCOSUR y Alianza del Pacífico, 2017) y la Estrategia Regional Digital (Sistema de Integración Centroamericana, 2015), entre otras.

Vulnerabilidades y Potencialidades

Sólo siete de los treinta y dos países relevados[5] en el continente cuentan con un plan de protección de infraestructura crítica, mientras que otros veinte tienen equipos de respuesta a incidente de ciberseguridad. La región latinoamericana es, a nivel mundial, una de las más vulnerables ante ataques cibernéticos[6], y se encuentra en el sexto lugar de aquellas que han priorizado el desarrollo de cibercapacidades, sólo por encima de África y parte de Oceanía[7]. Uno de los posibles criterios para medir la vulnerabilidad podría ser la comparación entre la cantidad de servicios digitalizados y la cantidad de medidas de seguridad disponibles. A mayor cantidad de servicios, pero menor cantidad de medidas, mayor será la vulnerabilidad. Y es que la digitalización de servicios ha sido la tendencia en la región desde mediados de 2015, con grandes volúmenes de información de registro de personas, así como datos sensibles de funcionarios, controles de distribución eléctrica, agua y gas, ordenados y controlados con tecnologías de información (IT). Sumado a ello, el evento inesperado de la pandemia en 2020 aceleró y potenció los mecanismos de e-commerce y las fintech. La principal dificultad radica, en que la conciencia de vulnerabilidad, la legislación y la de inversión en equipos, capacitación e infraestructuras de seguridad, no han crecido proporcionalmente al proceso de digitalización.

La falta de conciencia es resultado de una pobre capacitación en seguridad cibernética. Siendo el 95% de los ataques cibernéticos productos del error humano[8], la falta de educación deviene en una pobre o nula prevención. El phishing es la técnica de ingeniería social número uno en la región, con un 70 % de los ataques llevados a cabo mediante esta metodología. De acuerdo a un estudio de la empresa Kasperky[9], hay 544 ataques de este tipo por minuto en toda la región, y las cifras tienden claramente a aumentar cada año.

Por otro lado, si bien existe un cierto grado de integración regional y lucha conjunta contra los ciberataques, las modalidades y técnicas ofensivas implicadas evolucionan

[5] BID - *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.* Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

[6] Datos del Banco Interamericano de Desarrollo (BID). 2020.

[7] Cibersecurity National Index - E-Governance Academy.

[8] IBM – (2022) Cyber Secirity Intelligence Index Report.

[9] Kaspersky (2023) – *Nueva Epidemia: el phishing se sextuplicó en América Latina con el reinicio de la actividad económica y el apoyo de la IA*. Disponible en: https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

constantemente. Muchas leyes y procedimientos convenidos entre los países nunca fueron debidamente reglamentados, es decir, dotados de una planeación de recursos y una adquisición y disposición de equipos. La continua evolución de la amenaza cibernética requiere una actualización permanente de los marcos jurídicos y legislativos que regulan y dictamina qué es un ciberataque, la relevancia y posibilidad de su trazabilidad y la coordinación y disposición de recursos para su prevención y mitigación. Lamentablemente, en la actualidad otras problemáticas más inmediatas (sociales, económicas y políticas) han dificultado la priorización de este tipo de amenazas.[10]

Finalmente, la escasa conciencia de vulnerabilidad así como la falta de una consolidada cooperación regional, resultan en una flagrante falta de inversión. Invertir en ciberseguridad significa no sólo destinar recursos a la constante capacitación y concientización del personal, sino también a la actualización permanente del hardware necesario.

A modo de conclusión

América Latina es aún un espacio joven en lo que a ciberseguridad se refiere. Si bien existe una leve tendencia regional hacia la cooperación y las amenazas son innegables, existen aún discusiones cotidianas que minan, a nivel interno, la concientización e inversión en ciberseguridad, y a nivel regional, el proceso de integración y cooperación entre los países. Siendo una región históricamente pacífica en cuanto a enfrentamientos internacionales (en comparación a otros continentes), América Latina sigue dando una mayor prioridad a problemáticas urgentes de seguridad interna como el narcotráfico y la trata de personas. Sin embargo, es necesario tener en claro que una creciente digitalización de servicios debe r siempre acompañada de una correspondiente estructura de prevención. La zona ha sufrido, y sufre constantemente, significativos ataques informáticos, pero la escasez de recursos financieros (ya sea por disponibilidad o malversación) implica la priorización de invertir en problemáticas con un mayor peso político y social, como las ya mencionadas. En este contexto, la integración regional representa la mayor potencialidad de la zona, ya que en un continente donde casi todos los países comparten un idioma común, niveles de desarrollo tecnológico similar y vastos antecedentes en lo que respecta a la lucha conjunta de amenazas endémicas, se presentan

[10] VERA, G. (2022) - Ciberdefensa en LATAM: entre le peligro y la indiferencia.

ventajas inigualables para concentrar los esfuerzos contra una problemática común. Eso, claro, requiere primero una conciencia de vulnerabilidad común.