Fuente
América Economía

Fecha
23/Mar/2017

DEFENSA TECNOLÓGICA

El aumento del riesgo de ciberataques en América Latina ha impulsado la demanda de soluciones integrales para abordar el problema. Sectores como el consumo masivo y el financiero son los principales clientes.

POR HUGO FLORES CÓRDOVA, LIMA

Arturo es un empresario peruano que se dedica al comercio mayorista. Hace unos años, abrió un correo electrónico de origen desconocido que le llegó a su *email* del trabajo. El correo estaba vacío. Al día siguiente, cuando abrió nuevamente su *email*, se dio con la sorpresa de que parte

Organización de Estados Americanos y el Banco Interamericano de Desarrollo–, el cibercrimen le cuesta a América Latina alrededor de US$ 90.000 millones anuales. El estudio revela que la mayoría de países de la región no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica.

Según Rengifo, actualmente las empresas de América Latina son afectadas principalmente por ataques a la confidencialidad de la información. "Es cuando sustraen tus datos. Datos que son sensibles y tienen un valor económico", dice. En esa misma línea, Lucas Paus, *security researcher* de ESET Latinoamé-

de los correos en su bandeja de entrada había desaparecido. Según le dijo un técnico en ese entonces, él había sido víctima de un ciberataque. Como Arturo, son muchos los empresarios latinoamericanos que año a año son afectados por este tipo de amenazas. Según una estimación presente en el *Informe Ciberseguridad 2016, ¿Estamos preparados en América Latina y el Caribe?* –elaborado por la

Lo que sucede en el sector privado latinoamericano es un espejo del panorama regional. De acuerdo con Andrés Rengifo, jefe de la Unidad de Crímenes Digitales de Microsoft América Latina, mientras que la transformación digital de las empresas en la región es cada vez más alta, la implementación de medidas de ciberseguridad no se mueve al mismo ritmo.

rica, empresa de soluciones de seguridad informática, detalla que las firmas de la región –según un sondeo desarrollado por ESET– están preocupadas por tres problemáticas puntuales: los *malware* (*software* malicioso que busca dañar un sistema), la explotación de vulnerabilidades de *software* o sistemas y el acceso indebido a la información. "Por otro lado, aparecen preocupaciones específicas que

PROBLEMA GLOBAL. La conectividad ha aumentado los riesgos.

FOTOGRAFÍAS: MICROSOFT DIGITAL CRIME UNIT / REDMOND

EFECTO. El cibercrimen genera importantes pérdidas económicas en la región.

años atrás tenían un menor porcentaje, como el secuestro de información ligado al *ransomware* (*software* malicioso que bloquea las PC desde una ubicación remota y puede llegar a encriptar archivos)", dice el ejecutivo.

Otro cibercrimen que afecta hoy a los empresarios de la región es el *phishing*, y el robo de información de las bases de datos desde adentro de las empresas mediante el uso de *malwares*. "El robo de información es cada vez más sofisticado", manifiesta.

La era móvil ha diversificado los riesgos para empresarios y trabajadores de las empresas. "Podemos ver publicaciones

región. De acuerdo con un informe de la firma, los ataques de *ransomware* no se incrementarán, pero sí se diversificarán sus métodos para afectar a las empresas y usuarios (especialmente a través del *internet of things*). Asimismo, el reporte vaticina que el *hardware* y el *firmware* serán cada vez más blancos de ataques sofisticados. "Los ataques móviles combinarán bloqueos de dispositivos móviles con robo de credenciales, lo que permitirá a los ciberdelincuentes acceder a cuentas de bancos y tarjetas de crédito", indica el reporte.

Respuesta privada

En los últimos años, las empresas han venido invirtiendo en protección de sus servidores mediante *software* para la detección y remoción de amenazas. Sin embargo, hoy la nube es la alternativa que gana más terreno entre las firmas lati-

es decir, la suplantación de identidades mediante un sitio apócrifo. "Este sigue estando a la orden del día y, quizás, extendiéndose ahora más al mundo del *smartphone* por medio de las estafas multimarca de WhatsApp", dice Lucas Paus. A esta lista, según Elías David Gloria, *regional sales manager* de Gemalto, firma especializada en la venta de productos de seguridad digital, se agregan la violación

falsos en redes sociales, *apps* fraudulentas, suplantación de correos electrónicos, suplantación de dominios, entre otros, lo que es una respuesta coherente a la marcada tendencia móvil", dice Ricardo Villadiego, CEO y fundador de Easy Solutions, firma de ciberseguridad especializada en fraude electrónico.

Solo en 2017, la compañía Intel Security proyecta varias ciberamenazas para la

noamericanas. "El año pasado gran parte del presupuesto global en ciberseguridad fue destinado al fortalecimiento de los componentes virtualizados en la nube o conectados a ella de alguna manera, propensión que esperamos continúe este año", dice Lucas Paus, de ESET Latinoamérica. Justamente, para Elías David Gloria, de Gemalto, las infraestructuras en la nube son altamente coste-eficientes y muy

elásticas, pues se adaptan a la demanda de infraestructura de cada empresa. "Eso las hace muy atractivas", dice.

Ante las ciberamenazas, explica Dmitry Bestuzhev, director de Investigación y análisis para Kaspersky Lab en América Latina, las empresas también han optado por contratar soluciones más integrales. Acá destacan los servicios de *threat intelligence*, los cuales son reportes que, a través del análisis y la organización de la información, ayudan a prevenir y contrarrestar posibles ataques. "Este es un servicio mucho más completo. Con estos reportes una persona sin el conocimiento técnico puede entender estos ataques. Pero también hay una parte técnica, que de forma detallada explica a las empresas cómo encontrar el ataque en su red o fuera de ella cuando estén intentando afectarla", dice.

Primeros en la lista

Las empresas en la región que más demandan soluciones de ciberseguridad son, en buena medida, las grandes, ya que su músculo financiero les permite hacerlo y, a veces, su tamaño las obliga. Si se analiza por rubros, es el financiero el que más solicita este tipo de seguridad en la región. "Los bancos están siempre más

97% de los ataques
son prevenibles si es que se protege la información en los lugares donde se crea, se accede y se guarda, según Oracle.

US$ 575.000 millones
pierde el mundo al año por el cibercrimen, estima el BID.

89% de los ciberataques
a empresas en México tienen motivaciones financieras o de espionaje, estima la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información de ese país.

En ese sentido, Dmitry Bestuzhev sostiene que el ciberespionaje industrial es una amenaza, por lo que muchas firmas invierten en la protección de su investigación y avances. "Los negocios que invierten en esto son el químico, petroquímico, aerocomercial, el de cosméticos, entre otros", dice Bestuzhev. A estos se le suman otros sectores como el comercio electrónico y las telecomunicaciones.

Según Edgar Vásquez, gerente de cuentas estratégicas en Intel Security México, la demanda de servicios, proce-

hackeados. Eso puede pasarle a los dispositivos de los directores o a los gerentes de las compañías. Pero, además, porque la digitalización permite que los ataques sean a través de cualquier dispositivo que se pueda conectar", dice José Luis Najarro.

Para que la demanda crezca, según Edgar Vásquez, es muy importante que las naciones de América Latina y el Caribe consideren a la ciberseguridad un asunto de seguridad nacional. "La ciberseguridad va acompañada de políticas

propensos a ataques, toda vez que mueven dinero y ese siempre será el *target* más pretendido" dice Elías David Gloria.

Pero la demanda ha ido diversificándose en estos años. José Luis Najarro, director de *management consulting* de KPMG Perú, señala que salud es otro rubro que demanda mucho este tipo de servicios. "Las clínicas invierten en este tema porque manejan información sensible de los pacientes. También hay demanda por parte de empresas del sector de consumo masivo. Estas están expuestas a que las hackeen y les roben sus fórmulas", dice.

dimientos y productos de ciberseguridad crece actualmente en la región también entre empresas medianas y pequeñas. Otro cambio importante en lo referente a ciberseguridad, según Andrés Rengifo, es que el tema ya no es una preocupación exclusiva del área técnica, sino, en varios casos, ya lo es de la alta gerencia de las empresas.

Todo indica que la demanda por ciberseguridad seguiría avanzando a pasos grandes en la región. "La presencia de la ciberseguridad en las agendas de las empresas va a aumentar, ya que ahora tenemos *smartphones* y estos pueden ser

públicas, productos y procedimientos que puedan contrarrestar ataques externos e internos", señala. Para el ejecutivo, gran parte del problema pasa por la educación. "Tú vas a una empresa y puedes mostrar la mejor tecnología. Pero el problema es que en muchas ocasiones el cliente no está educado, y eso le impide manejar la tecnología y exigir un buen servicio", dice.

Queda claro que dinamizar la educación entre los empresarios, pero también entre los colaboradores de las empresas, será vital para reducir los riesgos a los que se expone una firma.