DF SUPLEMENTOS
SANTIAGO- CHILE
JUEVES 11.06.2020

SITUACIÓN DE PEQUEÑAS EMPRESAS DEL PAÍS:

ADVIERTEN POCA MADUREZ EN CIBERSEGURIDAD

Las pequeñas unidades productivas, que mueven la economía del país, son inexpertas y reactivas para protegerse, de acuerdo con los resultados de un estudio presentado ayer por IDC.

POR AIRAM FERNÁNDEZ

El 80% de las empresas más pequeñas del país está en etapas tempranas de adopción de soluciones de seguridad TI. Les falta visión, procesos, administración de riesgos, tecnología y personas preparadas para enfrentar las amenazas, reveló el Estudio sobre la Madurez de la Ciberseguridad en Chile, realizado por IDC, con el patrocinio de Claro, Check Point y en colaboración con la Alianza Chilena de Ciberseguridad (ACC).

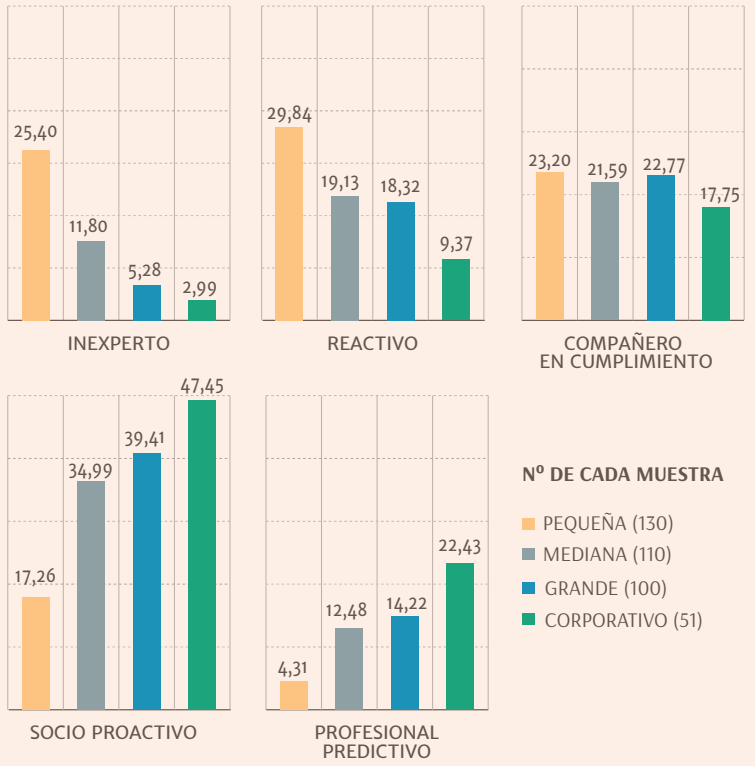
La medición presentada ayer, concluyó que uno de los principales desafíos en todo el ecosistema empresarial del país es madurar la ciberseguridad y "generar una cultura de la información y de los datos", en un contexto de pandemia que ha obligado la aceleración en materia digital y donde sólo en abril, la ACC recibió más de 500 denuncias de estafa y ataques cibernéticos, señaló Natalia Vega, country manager de IDC Chile y Perú.

Para determinar el nivel de madurez de las empresas de Chile, durante agosto y octubre del año pasado IDC entrevistó a 391 ejecutivos encargados de tomar las decisiones en el área, abordando diferentes industrias y ubicaciones. Vega explicó que se consideraron cuatro segmentos de empresas (pequeñas, medianas, grandes y corporaciones), y se siguió el modelo de IDC MaturityScape, que propone cinco niveles: profesional predictivo, donde la ciberseguridad forma parte esencial de la propuesta de valor de TI; socio proactivo, donde priman programas de seguridad "robustos en cumplimiento" y "fácil valoración de costo-eficiencia de las soluciones"; compañero en cumplimiento, con foco en programas y control de seguridad apegados a regulaciones y evaluaciones internas; reactivo, con un staff permanente para requerimientos prioritarios y recursos externos para aspectos de gobernabilidad; e inexperto, donde las medidas básicas de seguridad surgen conforme a las necesidades.

En el caso de las pequeñas empresas -aquellas con facturación anual superior a 2.400 UF-, se trata de un "proceso inicial", señaló Natalia Vega, con "emprendimientos que aún se encuentran en una posición inexperta. Una dificultad que tienen es cómo definir su vulnerabilidad y para ello es importante contar tanto con una visión interna como externa, entre otros aspectos, tales como evaluar los riesgos asociados con la confidencialidad, integridad y disponibilidad a nivel de unidad de negocio y aplicación e implementar requisitos de seguridad de datos para monitoreo y encriptación", explicó Vega sobre la forma en que las pequeñas pueden incorporarse al camino para madurar sus niveles en este terreno.

Etapas y estado de madurez de la seguridad de TI en Chile

SITUACIÓN SEGÚN TAMAÑO DE EMPRESA



Otros hallazgos

Respecto a las empresas medianas, el estudio reveló que aplican métricas en programas de seguridad para tomar decisiones y que sólo un cuarto de ellas integra a sus socios comerciales en dichos programas. Muy distinto es el panorama de las grandes, que tienen una "estrategia madura", impulsadas por el cumplimiento de requerimientos de industria, locales e internacionales.

A todos los ejecutivos se les preguntó, entre otras cosas, cómo consideran que la ciberseguridad de su empresa puede compararse con la de sus pares. "El 54 % dijo estar a la par, indicando un nivel de 'compañero obediente'. Sin embargo, el 28% declaró estar en una etapa 'reactiva' o inferior", sostuvo Vega. Sólo el 33% logró ubicarse en un enfoque predictivo y, a juicio de la ejecutiva, es necesario elevar esa cifra.

Una de las dificultades que tienen las pequeñas empresas en esta materia, es cómo definen su vulnerabilidad, según el análisis que hacen en IDC.

Pese a que los resultados se presentan como una radiografía prepandemia, son útiles para que las empresas puedan ajustar sus estrategias de cara al futuro. "Sabemos que las organizaciones tienen foco en ciberseguridad desde hace tiempo. Sin embargo, la construcción de este escenario preparado y fortalecido todavía no está del todo claro", sostuvo Vega, añadiendo que, en general, la inversión "aún es baja".

Para avanzar, hizo hincapié en "desarrollar estrategias integrales que consideren aspectos tecnológicos, sus procesos, staff, definición de riesgo de vulnerabilidad y visión de futuro" de cada compañía. Además, es crucial entender que el desarrollo de esas estrategias debe enfocarse como un ciclo permanente, con iniciativas lideradas por los dueños de las empresas, que no se limiten sólo a soluciones tecnológicas, y donde predecir sea lo primordial, mucho más que prevenir.

En ese sentido, por ejemplo, y "sabiendo que se están introduciendo a un nuevo nivel de riesgo de fraude" en medio de una emergencia sanitaria, "es de esperarse un aumento en la inversión", dijo Vega.

ALTA GERENCIAL JUEGA ROL CLAVE EN DECISIONES PARA UN BUEN RESGUARDO

Expertos aclaran que es vital concientizar a toda la jerarquía de la organización respecto a la importancia de la ciberseguridad, junto con establecer un plan maestro, indexado a un presupuesto.

POR AIRAM FERNÁNDEZ

El rol que debe asumir la alta gerencia y los directorios en los temas de ciberseguridad es crucial. En eso coinciden cuatro altos ejecutivos del área de tecnología consultados por Diario Financiero, respecto a cómo y hasta qué punto deben involucrarse en la toma de decisiones en esta área, que, en muchos casos, se deja sólo a criterio de los departamentos TI.

Para César Pallavicini, gerente general de Pallavicini Consultores y presidente de la Comunidad de Profesionales de Riesgo Operacional, la gestión de seguridad digital debe incluir políticas y normas que involucren a los tres poderes de todas las compañías: accionistas, directorio y alta administración. No es opcional, precisa el ejecutivo: "Las normas internacionales ISO exigen que la alta administración y directorio aprueben formalmente las políticas de riesgo operacional y ciberseguridad. Normalmente, cuando el comité de riesgo operacional o Seguridad de la Información, según esté estructurado en cada organización, aprueba las políticas, éstas deben subir al directorio para su aprobación, quedando en acta de directorio para dejar la evidencia formalizada", detalla.

Marcelo Díaz, CEO de Makros, dice que la primera línea de mando es "tanto o más relevante que las finanzas o la operación en una empresa". Por eso, los altos directivos deberían dar el mismo nivel de importancia a este tema. Y lo ejemplifica con los blancos que suelen buscar los cibercriminales: "El 43% de los ataques ocasionados el año pasado estuvo dirigido a la información relevante de la organización y los clientes, más que a la capacidad de operar de la empresa".

Un punto que también toca Adolfo Tassara, CEO de Anida Latam. "Hay casos conocidos en la banca local, pero también otros icónicos en el mundo, donde el impacto financiero ha cobrado la cabeza de altos directivos por no haber actuado con la debida diligencia en estos temas", recuerda.

Pese a esta realidad, no es usual que los directorios estén conformados por expertos en este tema. Pero es algo inminente. Al menos así lo considera Pallavicini, acotando que "en el corto plazo, así como tienen abogados, ingenieros comerciales, auditores de tributaria y otros especialistas, podrían incorporar un experto en ciberseguridad".

Cómo actuar

Ante este escenario, los ejecutivos mencionan una serie de buenas prácticas que podrían aplicar aquellas compañías que no han avanzado lo suficiente.

"Para la mayoría de las empresas es recomendable adoptar lineamientos de normas ISO 27001 e ISO 27032 de ciberseguridad. También es clave considerar la Política Nacional de Ciberseguridad, formar un comité compuesto por la alta gerencia, formalizar y educar en las políticas y tener claro el rol del Oficial de Seguridad de la Información", dice Pallavicini.

Concientizar a toda la jerarquía de la organización es lo primero que menciona Iván Toro, gerente general de ITQ Latam, porque "la idea es ser proactivo y no reactivo". Tanto él como Pallavicini subrayan la necesidad de disponer de un "plan director" de ciberseguridad que debe estar indexado a un presupuesto de inversión y gasto.

Toro añade un plan de contingencia para posibles incidentes de seguridad, realizar auditorías de seguridad a los "activos expuestos", mitigar las vulnerabilidades que puedan suponer un riesgo y no perder de vista que el conocimiento, la capacitación de los encargados y la constante actualización en materia de nuevas tecnologías y tendencias en el área también son elementos cruciales. ■

SALUD SE SUMA A LA LISTA DE BLANCOS MÁS VULNERABLES DE SUFRIR ATAQUES CIBERNÉTICOS

Gobierno, banca y el sector financiero son las áreas que se ven impactadas por cibercrímenes con más frecuencia. Pero también se han sumado las instituciones de salud.

POR CONSTANZA GARÍN

Beneficios económicos y robos de información confidencial -en algunos casos, por temas de seguridad nacional y defensa- son las principales razones por las que los ciberdelincuentes atacan a diferentes instituciones, explica el director de la Alianza Chilena de Ciberseguridad (ACC), Marco Zúñiga.

Históricamente, los sectores que más se han visto afectados por estos ataques en el país son el financiero, la banca, el gobierno y, recientemente, el e-commerce, ya que manejan valores y administran datos, dos características atractivas para sustraer información y obtener dinero.

Además, según Claudio Elorza, Senior Security Network Engineer de Adexus CCIE 40112, son áreas que han elevado el número de servicios transaccionales online, que no están protegidos frente a "ataques volumétricos". Y acá, "el factor humano es el más vulnerable, principalmente por la poca experiencia y conciencia sobre la seguridad de la información, lo que se traduce en una mayor probabilidad de ataques de *phishing*, fugas y accesos no autorizados", enfatiza Elorza.

En ese sentido, para evitar fraudes en las organizaciones es necesario integrar tres pilares de la ciberseguridad: procesos, personas y tecnología.

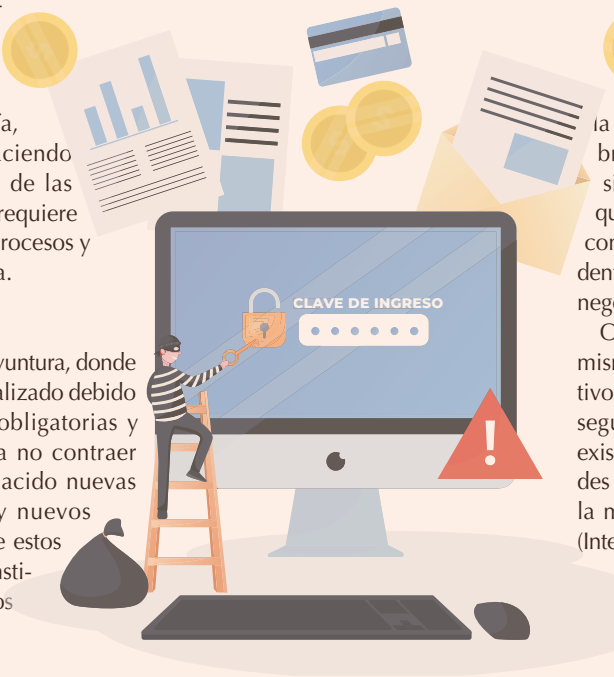
El gerente general de Pallavicini Consultores, César Pallavicini, detalla que las compañías de a poco han tomado conciencia sobre el tema y han comenzado a invertir en la creación de departamentos que se dediquen al monitorio y al manejo de herramientas como "HoxHunt, PerimeterX, WhiteSource, Cloud Management Suite, Firewall de Safeblocks, software de encriptación, monitoreo, Ethical Hacking o Pentest".

Marco Zúñiga, de la Alianza Chilena de Ciberseguridad, añade que hoy, además de que se está invirtiendo en tecnología, también se está haciendo en la capacitación de las personas, "pero se requiere profundizar en los procesos y gobernanza", afirma.

Nuevos focos

En medio de la coyuntura, donde casi todo se ha virtualizado debido a las cuarentenas obligatorias y los resguardos para no contraer el Covid-19, han nacido nuevas formas de atacar y nuevos sectores víctimas de estos hechos, como las instituciones de salud y los hospitales.

Según Cecilia Pastorino, Security Researcher de ESET Latinoamérica, estos fraudes son más frecuentes en países europeos donde "parecen no detenerse" en medio del contexto provocado por el coronavirus, y proyecta que que tanto Chile como el resto de la región, podrían convertirse en un nuevo foco de ciberataques durante la pandemia.



¿Por qué los cibercriminales atacan este sector? La ejecutiva de ESET explica que "se ha vuelto un blanco perfecto" para los ataques *ransomware,* ya que "la interrupción en la continuidad de los servicios que brindan puede tener un impacto significativo para la comunidad, lo que genera la necesidad de resolver con urgencia cualquier tipo de incidente. Y esto es un punto a favor en la negociación para un cibercriminal".

Otros aspectos que vuelven a este mismo sector como un blanco atractivo, son la falta de capacitación en seguridad de los profesionales, "la existencia de múltiples vulnerabilidades por el uso de software obsoleto, la multiplicidad de dispositivos IoT (Internet de las Cosas) que se utilizan y la sensibilidad de la información que manejan", subraya la ejecutiva. ■

GRUPO DF
DF CAPITAL ED
Directora: Marily Lüders • **Subdirectora:** Teresa Espinoza • **Editora de Desarrollo de Proyectos:** Carmen Mieres • **Subeditora:** Claudia Marín • **Periodistas:** Airam Fernández, Constanza Garín **Director de Arte DF:** Rodrigo Aguayo • **Diseño:** Marcia Aguilar • **Dirección:** Edificio Fundadores, Badajoz 45, pisos 10 y 11, Las Condes • **Teléfono:** 2339 1000 **e-mail:** buzondf@df.cl Impreso por COPESA IMPRESORES S.A., que sólo actúa como impresor.

Cuando los datos críticos para el negocio están protegidos y disponibles, las empresas pueden extraer su verdadero valor.

Obtenga protección de próxima generación para datos de misión crítica con Dell EMC Data Protection

- Mantenga a salvo sus datos y adminístrelos con un dispositivo de almacenamiento rápido, seguro y altamente eficiente.
- Obtenga la protección de datos líder en la industria para cargas de trabajo en múltiples nubes.
- Reduzca el riesgo y aproveche el valor de los datos mientras cumple con los SLA y aumenta el ROI.

#1
en protección de datos, disposivos y software

100 %
de cobertura a través de protección de datos continua

¡Save the date!

ANIDA y **Dell Technologies** lo invitan a avanzar en el conocimiento de la protección de datos, el próximo **8 de julio.**
Más detalles próximamente en nuestras redes sociales.

@anidalatam | @Anida Latam

ANIDA

DELL Technologies
PLATINUM PARTNER

Contáctanos a info@anidalatam.com

LUCES Y SOMBRAS DE LA SEGURIDAD INFORMÁTICA

Los expertos coinciden que en un par de años, Chile ha avanzado en el tema pero aún nos queda camino por recorrer.

POR CONSTANZA GARÍN

Hace poco más de dos años, se vivió el primer *hackeo* con robo de dinero que se conoce en el país: US$ 10 millones sustraídos al Banco de Chile. Tras ese episodio, el país ha tenido avances considerables en el tema, considera Hugo Galilea, director de la Alianza Chilena de Ciberseguridad (ACC), con una inversión en ciberseguridad que subió 6,5% en 2018 y 4,8% en 2019. Sin embargo, "aún queda una brecha importante que saldar", advierte.

En ese sentido, Chile se encuentra por debajo respecto a la inversión que hace Latinoamérica en seguridad informática. Según el informe "ESET Security Report 2019", el 55% de las empresas chilenas encuestadas afirmó haber sufrido al menos un incidente de seguridad en 2019 y apenas el 58% implementa herramientas de *backup* (debajo del 64% de la región).

Considerando los avances del país, el gerente general ITQ Latam, Iván Toro, destaca la creación de departamentos especializados en seguridad informática, el desarrollo de planes de concientización sobre ciberseguridad para los empleados y también la inversión en herramientas como Machine Learning, "aplicado a la contratación de servicios de Red Team para simular un ataque dirigido contra sus compañías".

César Pallavicini, gerente general de Pallavicini Consultores, resalta soluciones como Cloud Managment Suite, Firewall de Safeblocks y softwares de encriptación, entre otros. Sin embargo, advierte que estas soluciones se han observado "fundamentalmente" en empresas del sector financiero, seguros, telecomunicaciones y en algunas AFP, pero "no en el resto debido a, fundamentalmente, la falta de conciencia de los accionistas y directivos. Por eso es necesario que los organismos reguladores sean más rigurosos en la supervisión y más drásticos en las sanciones", opina.

En ese sentido, el CEO de VainaTec, Cristián López, considera que hace falta una política concreta que exija a las empresas tener soluciones mínimas de seguridad, que garanticen la capacidad de reaccionar ante una falla total o parcial de servicios.

Con todo, pese al consenso acerca de que aún queda por avanzar en

La inversión en ciberseguridad subió 6,5% en 2018 y 4,8% el año pasado.

ciberseguridad, Ricardo Dorado, director of Growth de Fundación País Digital, cree que es clave la labor que ha tenido el Equipo de Respuesta ante Emergencias Informáticas (CSIRT) a cargo del Ministerio del Interior, así como también "el movimiento de Cyber Security Awareness impulsado por los senadores Felipe Harboe y Kenneth Pugh".

Nuevos riesgos

El teletrabajo masivo que ha impulsado la cuarentena, trajo nuevos riesgos para las empresas, principalmente a través de las plataformas de comunicación a distancia.

"Con el teletrabajo nos enfrentamos a una realidad compleja: los computadores podrían estar menos preparados, ocupando redes más desprotegidas, sin *firewalls*, antivirus, EDR, programas para detectar *phishing* y ausencia de bloqueo de sitios", subraya Hugo Galilea, de la ACC.

Ante ese escenario, el ejecutivo sostiene que es indispensable la capacitación del personal, a fin de enseñar y estar preparados para bloquear estafas o instalación de programas que pongan en peligro la organización.

Coincide Rolando Martínez, gerente comercial de E-Sign, quien añade que en nuestro país existe un déficit de "12 mil profesionales de ciberseguridad", por lo que es necesario la capacitación ya que cada vez "las amenazas son más sofisticadas". ■

ANIDA

ANIDA PRESENTA DELL EMC DATA PROTECTION

Un nuevo nivel en **Protección de Datos**

En el contexto actual, donde la gestión de la información es fundamental para mantener la continuidad de los negocios, proteger los datos es vital para que las empresas sean competitivas. Dell EMC Data Protection cumple este objetivo al ser una solución de protección de datos convergente, simple, integrada y eficaz, con el menor costo de la industria.

Las empresas se enfrentan a la necesidad de proteger una cantidad de datos cada vez mayor, en un ecosistema de aplicaciones en crecimiento y sobre infraestructuras heterogéneas, que hoy se expanden rápidamente hacia la nube pública y privada.

De acuerdo a Adolfo Tassara, CEO de ANIDA, Planitum Partner Dell Technologies, "históricamente la protección de datos ha sido un desafío complejo, porque las compañías utilizan múltiples productos de distintos proveedores, lo que se traduce en implementaciones lentas, administraciones complejas y operaciones costosas".

Cambiar este paradigma es posible utilizando las soluciones de protección de datos de Dell Technologies, especialmente diseñadas para incorporar almacenamiento de datos, software de protección y motores de búsqueda y análisis; todo en un mismo dispositivo que brinda protección de datos en un ecosistema de aplicaciones amplio, que incluso considera la protección hacia la nube.

Protección líder en la industria

Como explica Adolfo Tassara, Dell EMC Data Protection es una solución integral, robusta, integrada y económica, cuya implementación, administración y operación son simples y fáciles de adoptar. "Ofrece tiempos de protección de datos 10 veces más rápidos que el promedio de la competencia, con una tasa de deduplicación líder de 55:1, lo que se traduce en ahorros por concepto de inversión y mayores capacidades de protección de datos".

A través de su equipo de consultores, ANIDA garantiza la implementación rápida, simple y sin contratiempos de Dell EMC Data Protection, con demostraciones previas que permiten a los clientes probar todas sus funcionalidades. Este proceso de venta y preventa se potencia con los modelos de leasing financiero y operacional que ANIDA y Dell Technologies ponen a disposición de las compañías, que provee financiamiento de 12 a 36, con pago de cuota inicial de hasta 90 días.

GENTILEZA REVISTA CHANNEL NEWS

Adolfo Tassara, CEO de ANIDA.

Las empresas prefieren Dell EMC Data Protection

Las soluciones de protección de datos de Dell Technologies están presentes en grandes y medianas empresas alrededor del mundo. Sobresalen sus capacidades de:

* **Implementación y administración simplificada, con potentes funcionalidades de protección de datos empresariales, al menor costo.**
* **Funcionalidad completa de copia de seguridad, replicación, recuperación, deduplicación, acceso y restauración instantánea; y búsqueda, análisis y una estrecha integración con VMware, además de preparación para la nube y recuperación ante desastres.**
* **Eliminación de silos mediante un dispositivo único, para entregar una protección de datos integral y una implementación 10 veces más rápida que una solución tradicional.**
* **Protección en un amplio ecosistema de aplicaciones, en entornos físicos, virtuales o de nube, y compatible con múltiples hipervisores.**
* **Integración con herramientas de administración nativas de VMware, SQL, Oracle y SAP.**
* **Protección de datos con interfaz de administración, que simplifica las copias de seguridad y automatiza el monitoreo y la generación de informes desde un tablero personalizable.**

Confianza Digital -
6 puntos claves en la ciberseguridad

La ciberseguridad en las empresas se ha convertido en un factor estratégico debido a que no hacerlo representa una amenaza importante en la continuidad de la operación, el valor de marca, y la sustentabilidad futura del negocio, sin ciberseguridad, es imposible abordar la transformación digital con éxito. En el contexto actual, donde a partir de una pandemia por COVID-19, se genera por defecto el aumento del teletrabajo y uso de los canales digitales, no es suficiente dejar este tema a cargo de los departamentos de TI, o enfocarse en proteger la red interna y externa de Internet; se vuelve crítico consolidar una cultura de seguridad en las empresas en la que participan todos los colaboradores. ESign como experto en el mundo de la Confianza Digital, con más de 15 años en el mercado, expone puntos 6 claves para optimizar la ciberseguridad en las empresas.

1. Principales Riesgos, Amenazas y ciberataques en tiempos de pandemia

La pandemia ha significado un cambio radical en la forma en cómo se entregan productos y servicios. Hay una cantidad muy importante de personas trabajando desde sus casas, y el canal principal de comunicación con clientes es ahora remoto. Este cambio imprevisto y rápido ha ocasionado varios efectos:

a. Las personas que trabajaban en un ambiente controlado de TI ahora están fuera del perímetro protegido, por lo tanto ya no se encuentran disponibles los cortafuegos, antivirus, aplicación de parches y control de navegación.

b. Las personas han tenido que utilizar computadores personales para trabajar. Y esos dispositivos no tienen políticas de control para instalación de software o modificar permisos de acceso. Otras veces tienen que compartir dispositivos corporativos con sus familiares que están estudiando, y esos usuarios no están preparados para reaccionar ante engaños.

c. Los sistemas para conectarse a los recursos de la empresa fueron diseñados para usuarios avanzados quienes utilizaban conexiones VPN. La gran parte de la fuerza laboral que las utiliza hoy en día, no cuentan con el conocimiento necesario, y saturan los dispositivos con su tráfico laboral normal, más el tráfico de los otros usuarios de sus casas, incluyendo plataformas de Streaming y videoconferencia.

d. El acceso a repositorios corporativos de información en muchos casos no gestiona adecuadamente los permisos de las personas, y por tanto restringe accesos innecesariamente y también los otorga a personas indebidas, por lo que los documentos corporativos no están protegidos en su totalidad.

En este escenario, las principales amenazas que estamos viendo hoy tienen que ver con el robo de credenciales para acceder a los sistemas de la empresa, y escalar privilegios. Dos de las principales metodologías son: Phishing, donde un sitio parece ser legítimo y el usuario introduce sus credenciales de forma inadvertida y los correos fraudulentos, que traen adjuntos contaminados con malware. Solo el hecho de abrirlos implica la toma de control de ese dispositivo por el atacante.
Para las empresas que ahora se comunican con sus clientes en forma virtual, el ransomware sigue siendo una amenaza creciente. Con los colaboradores en sus casas, sin filtros de correo, aumenta la probabilidad de que alguien caiga en un engaño.

2. Sectores más atractivos y vulnerables para ciberdelincuentes

Los sectores más atractivos para los ciberdelincuentes siguen siendo aquellos en que pueden monetizar más fácilmente la actividad delictiva, como las instituciones financieras y los grandes comercios. Sin embargo, la tendencia se mantiene en el uso de técnicas de ingeniería social para atraer a los consumidores, algunos ejemplos utilizados de pequeños fraudes masivos son:

- Correos o SMS muy sofisticados con mensajes engañosos.
- Correos de bancos solicitando actualizaciones de datos.
- Correos con adjuntos maliciosos o extorsiones personales.

Hoy en día, el tema más atractivo utilizado por los ciberdelincuentes es la contingencia de salud mundial. De esta manera usan las necesidades de los consumidores y ofertan mascarillas e insumos de protección y prevención ante el COVID-19, las cuales luego de realizar el pago, nunca llegan al consumidor final

3. Avances en las soluciones de seguridad cibernética

La ciberseguridad es el resultado de la aplicación de políticas, entrenamiento de profesionales y la aplicación de buenas herramientas tecnológicas. Afortunadamente hemos visto un avance importante en la migración de las herramientas de ciberseguridad hacia la nube, la aplicación de tecnologías de análisis de datos más sofisticadas, y una visión de integrar dispositivos que antes se compraban, instalaban y operaban por separado. Usar herramientas integradas no solamente facilita su despliegue, sino que minimiza los costos de configuración y tiene menos posibilidades de incurrir en errores humanos.

4. Claves para aumentar la seguridad en plataformas de comunicación a distancia

Dado que es fundamental cifrar/encriptar la comunicación a distancia, en un contexto de confinamiento, la identidad segura juega un rol esencial en la ciberseguridad.
El uso de prácticas robustas de identidad digital como certificados digitales individuales emitidos por una entidad certificadora como ESign y contar con certificados de sitio web seguros (SSL), permiten disminuir los fraudes y proteger la información, para aumentar la confianza en las plataformas digitales, generando importantes beneficios para empresas y usuarios

5. Buenas prácticas empresariales y rol de alta gerencia en ciberseguridad

La ciberseguridad es un proceso diseñado y ejecutado por las personas. La falta de profesionales en ésta área de la tecnología se calcula en 12.000 personas para nuestro país. En contraposición, los cibercriminales generan, para un mismo malware de base, miles de variantes que hacen fallar los métodos de detección de firmas, resultando en amenazas que sólo se pueden detectar mediante el comportamiento que presentan. La ayuda de la Inteligencia Artificial o el Machine Learning, es muy importante para distinguir las probables amenazas en un océano de datos, pero el rol de las personas sigue siendo esencial para confirmar y mitigar dichos riesgos. Las prácticas de retención y perfeccionamiento del talento interno, y la profundización de las alianzas estratégicas con proveedores de confianza como lo es ESign, en el campo de la ciberseguridad, deben contar con el apoyo y el control de la alta gerencia y los directores de las empresas, y ser parte del proceso habitual de governance.

6. ¿Dónde focalizar las inversiones?

ESign como experto, recomienda capacitar a los colaboradores en temas de ciberseguridado o en Ingeniería Social, en la medida que se sientan respaldados y preparados, podrán detectar más fácilmente los engaños en sus correos y mensajes. Desarrolle prácticas de análisis y mecanismos de ciberdefensa, y entrene regularmente a su gente en ellos.
Por otro lado, es fundamental definir sus activos esenciales junto con la realización de un plan de recuperación en caso de desastres, genere y supervise indicadores de sus procesos. Invierta en tecnología para filtrar las posibles amenazas del entorno. Avance hacia el Zero Trust, con apoyo importante en Identidad Digital y evolucione a modelos de Security as a Service. Por último, nunca confíe en las claves e implemente la Identidad Digital protegida por múltiples factores de autenticación

LAS LECCIONES QUE TRAJO LA PANDEMIA A LAS EMPRESAS

La rápida reacción de las compañías para implementar herramientas de teletrabajo o e-commerce dejaron en segundo plano a la ciberseguridad. Ahora, dicen los expertos, es tiempo de priorizarla.

POR CLAUDIA MARÍN

Las cifras son claras: los ataques de *phishing* entre febrero y marzo aumentaron 19,7% en el país en todas las plataformas, mientras que sólo en dispositivos móviles crecieron 83% en el mismo lapso, según datos de Kaspersky Lab.

Pero no sólo eso. A nivel de protocolos de escritorio remoto, utilizados para permitir a los empleados trabajar a distancia, si en febrero se registraron más de 683 mil casos, en marzo esta cifra se elevó más allá de 4,3 millones, solamente en Chile.

Y es que la pandemia ha sido una oportunidad para los ciberatacantes, pues, en muchos casos, las empresas tuvieron que adaptarse sobre la marcha hacia entornos digitales que les permitieran seguir operando, lo que determinó nuevas vulnerabilidades y riesgos no controlados.

"El escenario de pandemia genera una carga de estrés e impacto emocional muy alto en las personas, lo cual, mediante técnicas de ingeniería social combinadas con tecnologías creadas para el daño, facilitan los ataques de *phishing*, suplantación de identidad, *malware* o similares", explica Marco Zúñiga, director de la Alianza Chilena de Ciberseguridad (ACC).

Según datos entregados por HP, el 50% de los links relacionados al Covid-19 tiene mayor probabilidad de ser malicioso. De hecho, un informe del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSRIT), del Ministerio del Interior, observó que en marzo se registraron en Chile 178 dominios relacionados con el Covid-19 y la mitad de ellos se inscribió entre el 17 y el 27 de marzo.

4,3
MILLONES DE ATAQUES DE PROTOCOLOS DE ESCRITORIO REMOTO SE REGISTRARON EN MARZO, SÓLO EN CHILE, SEGÚN KASPERSKY LAB.

50%
MÁS DE PROBABILIDADES DE SER MALICIOSOS TIENEN LOS LINKS RELACIONADOS AL COVID-19, SEGÚN HP.

"Hemos detectado un aumento en la propagación de troyanos bancarios (códigos maliciosos que buscan robar la información financiera de los usuarios)", detalla Cecilia Pastorino, Security Researcher de ESET Latinoamérica.

Riesgos a distancia

Pero no sólo el miedo al nuevo coronavirus ha sido el gatillante del aumento en los riesgos. El trabajo remoto ha sido la solución para que muchas empresas, ante las restricciones de circulación, continúen operando. Según una encuesta realizada a mediados de abril por la Asociación Chilena de Seguridad a 468 compañías, el 95,3% de ellas implementó teletrabajo y casi la mitad lo hizo para todos sus trabajadores. Además, el 81,3% dijo haberlo hecho a raíz del Covid-19.

"Este es un suceso sin precedentes porque siempre las compañías eran las que decidían si es que sus empleados podían o no trabajar remoto, incluso muchas empresas explícitamente se oponían a esta modalidad", recalca Dmitry Bestuzhev, director de Investigación y Análisis de Kaspersky Latinoamérica. "Ahora todos están con esta nueva normalidad de que si quieren continuar a flote, deben permitir el trabajo remoto".

El problema, dice César Pallavicini, gerente general de Pallavicini Consultores, es que "la pandemia hizo que la mayoría de las empresas tuviera que recurrir al teletrabajo en forma apresurada, sin procedimientos ni herramientas tecnológicas probadas con el objetivo de seguir su operación".

A juicio de Rolando Martínez, gerente comercial de E-Sign, las compañías locales adquirieron primero habilitantes para el trabajo a distancia y luego restringieron los presupuestos debido al shock de la paralización. "Es muy difícil modificar procesos, tecnología y personas para adaptarse a una situación repentina y urgente como ésta", reconoce, y alerta que las empresas que no tenían experiencia en este tema están en un "proceso de adaptación relativamente traumático".

Así, mientras algunas han salido bien paradas, el resto ha tenido que reinventarse. "Las empresas han ido cubriendo poco a poco los *gaps* de seguridad que ha generado el trabajo remoto y muchas de ellas están estableciendo sus planes de mejoras", acota Walter Montenegro, gerente de Ciberseguridad de Cisco Chile.

Ventas online

Desafíos similares ha generado el fuerte impulso del e-commerce a partir de la pandemia. Datos de la Cámara de Comercio de Santiago y Transbank indican que las ventas online del comercio subieron 150% en abril respecto al mismo mes de 2019, con un crecimiento de 214% en un año.

"Hemos sido testigos de un despliegue e inversión importante en este canal, tanto tecnológico como en personal, pero en materia de ciberseguridad no se ha visto igual incremento", señala Hugo Galilea, director de la ACC. Tras asegurar la continuidad operacional, ahora las empresas pueden centrarse en este punto, "desde proteger sus páginas de ataques tan básicos como la denegación distribuida de servicio hasta contar con sofisticadas herramientas que permitan evitar el fraude de identidad digital".

Plataformas para generar correlación de todos los datos que pasan por la red, en el *endpoint* y en la nube privada son claves hoy, señala Adolfo Tassara, CEO de Anida Latam. "Se requiere comprender los ataques, el *modus operandi* de los ciberdelincuentes y las técnicas utilizadas para penetrar los sistemas, y sobre esa base centrar los esfuerzos en lo verdaderamente importante, ya que hoy en día se generan muchos falsos positivos".

En paralelo, se requiere una mayor capacitación de los usuarios, quienes "deben ser entrenados para el cifrado de disco completo garantizando que, incluso si el dispositivo cae en las manos equivocadas, no se pueda acceder a los datos de la compañía", explica Cristián Maulén, director del Observatorio de Sociedad Digital Unegocios, FEN Universidad de Chile.

Lo ideal, agrega Maulén, es que los empleados revisen las vulnerabilidades de su propio entorno doméstico antes de conectar los dispositivos de trabajo, mientras que la empresa debe determinar si los colaboradores necesitan acceso a la red interna o simplemente a servicios y correo electrónico basados en la nube, para acotar los riesgos.

"En medio de la crisis desatada por el Covid-19 hemos podido entender que la transformación digital era un punto que no podía seguir a paso lento", recalca Fernando Arnay, gerente de Ingeniería y Continuidad Operativa de NovaRed.

"Los piratas informáticos no descansan, al contrario, ante la más mínima oportunidad, no dudan en llevar a cabo su cometido. Asimismo, hemos visto cómo las compañías van comprendiendo la importancia de la continuidad operativa, sea cual sea el panorama mundial", concluye. ■

Pallavicini

desde 1998

Consultoría en Gestión de:

- Riesgo Operacional
- Seguridad de la Información
- Ciberseguridad
- Continuidad de Negocio
- Cumplimiento

www.pallavicini.cl

Sistema de Gestión ISO 9001:2015

TÜVRheinland CERTIFICADO

www.tuv.com ID 9108643838

+56 2 3223 2147

Luis Thayer Ojeda 95, Providencia