HIGH PERFORMANCE SECURITY
REPORT 2016

GENERAR CONFIANZA

PARA ENFRENTARSE AL PROBLEMA DE LA CIBER-SEGURIDAD

Accenture Security

UNA DESCONEXIÓN PELIGROSA

Uno de cada tres intentos de cíber-ataques intencionales tiene éxito; sin embargo, la mayoría de las organizaciones “confían” en su capacidad de proteger a la empresa.

En la actualidad, la reacción ante los cíber-ataques es una realidad operativa a la que se enfrentan la mayoría de las organizaciones, conjuntamente con un nivel cada vez mayor de caos y contradicciones. Una reciente encuesta realizada por Accenture a 2.000 ejecutivos responsables de la seguridad en grandes empresas de todo el mundo reveló que aproximadamente uno de cada tres intentos de cíber-ataques intencionales tiene éxito; sin embargo, los encuestados confían en que están haciendo lo correcto en términos de cíber-seguridad. El 75 por ciento indica que confía en sus estrategias de cíber-seguridad. Esta contradicción puede provenir, en parte, de intentos por conformarse con lo que tienen, pero revela una desconexión.

El índice de vulnerabilidad es extremadamente alto, y se amplía aún más al entender el volumen propio de los ataques. Además de los miles de millones de intentos aleatorios que las redes de una empresa repelen cada semana, en promedio una organización se enfrentará a más de cien intentos intencionales y dirigidos cada año. Los encuestados dicen que uno de cada tres de estos intentos vulnerará la seguridad. Se trata de dos a tres ataques efectivos por mes.

El tiempo que lleva detectar estos ataques a la seguridad suele agravar el problema. Según los resultados que arrojan otros estudios, el 51 por ciento de los encuestados por Accenture admite que detectar los ataques exitosos demora “meses”, mientras que otro 17 por ciento los identifica como “dentro del año” o más tiempo aún.

Además, los equipos de seguridad interna descubren sólo el 65 por ciento de los ataques exitosos, siendo los empleados, las autoridades y los “white hats” (hackers de “sombrero blanco” o hackers “éticos”) los que descubren la mayoría del resto.

Parte del desafío referido a la seguridad es priorizar adónde focalizar los recursos para proteger a la organización con efectividad. Más del 50 por ciento de los encuestados indicó que el mayor impacto en la cíber-seguridad son los ataques ocasionados por personal interno con intención de causar daño. Aun así, dos de cada tres encuestados manifestaron que carecen de la confianza en las capacidades de monitoreo interno de la organización para evitar ataques que vulneren la seguridad.

Más aún, a pesar de este reconocimiento explícito del impacto que tienen las amenazas internas, la mayoría de los participantes de la encuesta sigue concentrado en los problemas externos relacionados con la seguridad. Por ejemplo, el 58 por ciento prioriza tener mejores capacidades en controles perimetrales contra ataques externos, en lugar de abordar las amenazas internas de alto impacto. Básicamente, muchos siguen sin estar seguros de su capacidad de manejar las amenazas internas que causan el mayor impacto en la cíber-seguridad incluso aunque sigan priorizando las iniciativas externas que producen la menor rentabilidad sobre las inversiones.

Uno de cada tres intentos de ciber-ataques intencionales tiene éxito.

CONFIANZA MAL DEPOSITADA A PESAR DE LOS ATAQUES DE ALTO IMPACTO

Uno de cada tres intentos de cíber-ataque intencionales tiene éxito; los ataques internos tienen un impacto mayor y los equipos a cargo de la seguridad admiten que carecen de las herramientas necesarias para detectar vulnerabilidades (y, en un tercio de los casos, nunca las descubren). Sin embargo, tres de cada cuatro encuestados expresan confianza en su capacidad de proteger a sus organizaciones ante cíber-ataques. No sólo eso, el 70 por ciento dice que la cíber-seguridad está completamente arraigada en sus culturas, y que se trata de una inquietud a nivel Directorio que cuenta con el soporte de los ejecutivos de mayor jerarquía.

Un posible contribuyente a esta contradicción es que sigue habiendo demasiado énfasis en el cumplimiento, en parte porque parece ser más tangible y mensurable. Muchos departamentos de cíber-seguridad miden el desempeño en base al logro de los objetivos de cumplimiento, en lugar de hacerlo respecto de la mitigación de los impactos negativos en el negocio. Los marcos de control de la seguridad y los programas de cumplimiento son extremadamente útiles para definir el pensamiento primario; sin embargo, suelen no reflejar la dinámica del mundo real. Así como cumplir con los principios contables generalmente aceptados no asegura la protección contra fraude financiero, el mero cumplimiento de la normativa referida a la cíber-seguridad tampoco protegerá a una empresa de ataques exitosos.

Más aún, el sentimiento entre los encuestados sugiere que las organizaciones deberían esperar más de lo mismo. Por ejemplo, en caso de tener presupuesto adicional, entre el 44 y el 54 por ciento de los encuestados redoblaría sus actuales prioridades en materia de cíber-seguridad — inversiones que no logran evitar la vulnerabilidad. Estas prioridades incluyen: proteger la reputación de la empresa (54 por ciento), proteger la información de la empresa (47 por ciento) y proteger los datos de los clientes (44 por ciento). Una cantidad mucho menor de organizaciones invertirían ese dinero extra en esfuerzos que afecten más directamente sus resultados, como por ejemplo mitigar pérdidas financieras (28 por ciento) o invertir en capacitación referida a las cíber-seguridad (17 por ciento) — un área que la investigación de Accenture revela como un pilar cada vez más importante. En nuestro “Estado de Cíber-seguridad y confianza digital”[1], un estudio publicado en junio de 2016, el 31 por ciento de los encuestados identificó a la falta de presupuesto para capacitación o contratación de personal como el inhibidor más grande que obstaculiza su capacidad de abordar la cíber-seguridad.

Otro ejemplo de posible disonancia cognitiva: si bien tres cuartos de los encuestados manifiestan que tienen altos niveles de confianza referidos a la cíber-seguridad, una cantidad mucho menor indica una confianza similar en la capacidad que tiene su organización para tratar las violaciones a la seguridad. Por ejemplo, sólo el 37 por ciento manifiesta tener confianza en la capacidad que tienen sus organizaciones de detectar vulnerabilidades y el 36 por ciento opina lo mismo con relación a minimizar las disrupciones.

1 The State of Cybersecurity and Digital Trust: 2016, Copyright © 2016, Accenture and HfS Research, Ltd
www.accenture.com/cybersecurity2016ve

FORZAR LA PERCEPCIÓN PARA ENFRENTAR LA REALIDAD

Para sobrevivir en este contexto contradictorio y cada vez más riesgoso, las organizaciones deben reiniciar sus enfoques frente a la cíber-seguridad.

Para proteger a una empresa es preciso contar con un enfoque completo que considere las amenazas en toda la cadena de valor específica para la industria y el ecosistema de la compañía, identificando y minimizando la exposición del negocio y concentrándose en proteger los activos prioritarios. Las acciones que se indican a continuación pueden ayudar a las organizaciones a superar las percepciones limitadas y manejar con efectividad las cíber-amenazas de alto impacto a las que se enfrentan.

DEFINIR EL ÉXITO DE LA CIBER-SEGURIDAD

Para reformular sus percepciones relativas a la cíber-seguridad y desarrollar una nueva definición del éxito, las organizaciones deben hacerse varias preguntas fundamentales:

- **¿Considera que ha identificado y localizado todos los datos prioritarios para su negocio?**
- **¿Puede defender a su empresa de un adversario motivado?**
- **¿Cuenta con las herramientas y técnicas que le permitirán reaccionar y responder ante un ataque intencional?**
- **¿Sabe qué persigue verdaderamente su adversario?**
- **¿Con qué frecuencia "practica" su organización el plan de defensa para mejorar la capacidad de respuesta ante ataques?**
- **¿Cómo afectan estos ataques a su negocio?**
- **¿Cuenta con la alineación, la estructura, los miembros del equipo y otros recursos adecuados para llevar a cabo su misión?**

Creemos que las organizaciones dedicadas a la seguridad deben mejorar la alineación de sus estrategias con los imperativos del negocio. Y si bien muchas organizaciones están progresando con relación al cumplimiento y la gestión de los riesgos, los programas de seguridad deben continuar mejorando la detección y prevención de escenarios de ataques más avanzados.

PROBAR EXHAUSTIVAMENTE LAS CAPACIDADES DE CÍBER-SEGURIDAD TAL COMO LO HACEN LOS ADVERSARIOS

Las organizaciones deben evaluar realmente sus capacidades para protegerse de las amenazas de alto impacto, tanto internas como externas. Las pruebas exhaustivas de las defensas que tiene una organización pueden ayudar a los líderes a entender si pueden soportar un ataque intencional y dirigido. Con el mismo efecto que los programas militares de entrenamiento con fuego real, las organizaciones pueden contratar a hackers externos de "sombrero blanco" para que actúen como entrenadores prácticos de sus equipos de cíber-seguridad con el objetivo de evaluar su preparación y capacidad de respuesta.

PROTEGERSE DESDE ADENTRO HACIA AFUERA

Muchas organizaciones no logran limitar el acceso interno a la información clave, detectar actividades inusuales de los empleados con relación a la red o revisar periódicamente los accesos. Los adversarios saben lo que quieren, pero no saben adónde residen los activos claves. Por el contrario, los profesionales a cargo de la cíber-seguridad tienen la ventaja de conocer qué activos clave deben protegerse.

Al enfocar su energía en estos activos, las organizaciones pueden desarrollar bases más efectivas: en lugar de intentar anticipar una variedad casi infinita de posibilidades de violaciones a la seguridad provenientes de fuentes externas, las organizaciones pueden concentrarse en la cantidad relativamente menor de incursiones internas que tienen el mayor impacto.

INVERTIR PARA INNOVAR Y SER MÁS HÁBIL QUE LOS CÍBER-ATACANTES

En materia de cíber-seguridad, quedarse quieto ya no es una opción. Las organizaciones deben innovar continuamente para estar siempre a la vanguardia de posibles atacantes. Para ello, es posible que tengan que re-direccionar algunos recursos hacia nuevas estrategias y programas en lugar de invertir más en los programas actuales.

¿Pero adonde deben invertir?

Las organizaciones que buscan identificar oportunidades para invertir en innovación de cíber-seguridad pueden examinar siete dominios clave. Con este enfoque, mejorarán la capacidad de la organización y fortalecerán su resiliencia ante los cíber-ataques, pero es posible que precisen realizar inversiones continuas y sistemáticas en seguridad.

Sólo alrededor de un tercio de los encuestados expresó confianza en sus capacidades en alguno de los siete dominios relacionados con la cíber-seguridad, lo que destaca la necesidad de convertir la inversión en estas áreas en una prioridad.

La alineación con el negocio evalúa los escenarios relacionados con los incidentes de cíber-seguridad para comprender mejor aquellos que podrían afectar substancialmente al negocio e identificar factores que puedan generar estrategias de remediación y transformación, así como las posibles barreras que podrían obstaculizar su aplicación.

El contexto estratégico de las amenazas explora las amenazas de la cíber-seguridad, incluyendo un análisis de los riesgos competitivos y geopolíticos y otras áreas para alinear los programas de seguridad con la estrategia de negocios.

El ecosistema extendido debería estar listo para cooperar durante la gestión de una crisis, desarrollar cláusulas y acuerdos con terceros relativos a la ciberseguridad y focalizarse en el cumplimiento de la normativa regulatoria

El gobierno y liderazgo se concentra en la responsabilidad final por la seguridad, instaura una cultura orientada a la seguridad, mide e informa el desempeño referido a la cíber-seguridad, desarrolla incentivos atractivos para los empleados y crea una cadena clara de comando en la materia.

La cíber-resiliencia es la excelencia operativa frente a los cíber-adversarios disruptivos. Desde las bases tecnológicas y de procesos, hasta el desempeño en la recuperación ante incidentes, la empresa busca entender el actual contexto de las amenazas cibernéticas, diseñar enfoques para proteger los activos claves y utilizar técnicas de “diseño para lograr resiliencia” que apunten a limitar el impacto de los cíber-ataques

La capacidad de respuesta ante los cíber-ataques significa contar con un plan de respuesta fuerte, comunicaciones sólidas en caso de incidencias cibernéticas y la capacidad de asegurar la participación de todos los involucrados en las diferentes funciones del negocio.

La eficiencia de las inversiones significa entender el aspecto financiero de las inversiones realizadas en los dominios de la cíber-seguridad, la asignación de fondos y otros recursos, y compararlas con los puntos de referencia de la industria, los objetivos de negocios a nivel organizacional y las tendencias en materia de cíber-seguridad.

LA SEGURIDAD ES TRABAJO DE TODOS

Los empleados también desempeñan un papel fundamental en la detección y posible prevención de estos ataques. El 98 por ciento de los encuestados indicó que cuando las violaciones no fueron detectadas por el equipo de seguridad, fueron los empleados quienes más frecuentemente las detectaron. De hecho, la gente representa su primera línea de defensa, es por eso que la organización debe priorizar la capacitación y actualizar continuamente el cíber-talento en todo el negocio.

98% **de violaciones no detectadas por el equipo de seguridad fueron descubiertas por los empleados.**

Para desarrollar una cultura con conciencia de cíber-seguridad, las organizaciones deberían considerar a la ciberseguridad más avanzada como una actitud de la organización— que sea capaz de evolucionar continuamente y adaptarse a las contra-amenazas en constante cambio. Para promover una cultura de cíber-seguridad y confianza digital, las organizaciones deben enfatizar un enfoque de evolución y adaptación que les permita abordar todos los aspectos de la seguridad en forma continua.

Muchos equipos de cíber-seguridad de las empresas tienen dificultades para superar la brecha que existe entre el talento que necesitan y el que está disponible. En otro estudio realizado por Accenture sobre la confianza en lo digital, el 42% de los encuestados indicó que tenía suficiente presupuesto para tecnología de seguridad, pero necesitaba presupuesto extra para contratar y capacitar al personal en ese aspecto.

42% **de las organizaciones necesitan presupuesto adicional para contratar y capacitar al personal sobre la seguridad**

LIDERAR DESDE ARRIBA

Si bien el problema de la cíber-seguridad captó la atención total de las empresas, muchos Chief Information Security Officers (CISOs) siguen sintiéndose excluidos del plano directivo. Esto no es necesariamente un desaire consciente; es más una cuestión referida al nivel de madurez de la organización de seguridad. Para tener éxito, los CISOs tienen que trascender sus zonas de confort (es decir auditorías de cumplimiento y cíber-tecnología) y comprometerse substancialmente con los líderes de la empresa en forma diaria para discutir los problemas de negocios en el núcleo de la cíber-seguridad.

Deberán hablar el idioma del negocio para exponerles que el equipo de seguridad es un pilar esencial en la batalla para proteger el valor de toda la empresa. Al mismo tiempo, el CISO debe desarrollar conocimiento tecnológico en el directorio, con el objetivo de convertirlo en una prioridad que tenga la misma relevancia que la evaluación de los riesgos de negocios.

Desarrollar conocimiento tecnológico en el directorio, con el objetivo de convertirlo en una prioridad que tenga la misma relevancia que la evaluación de los riesgos de negocios.

APRENDER DEL PASADO

Para lograr una cíber-seguridad efectiva, las empresas deben alcanzar una mayor madurez respecto del rol principal de la organización que se dedica a la seguridad: proteger al negocio de pérdidas devastadoras. Afortunadamente, las organizaciones lo han hecho antes, con esfuerzos como por ejemplo la mejora de la calidad que se logró en los últimos treinta años. Para muchas organizaciones, la calidad seguía siendo una ocurrencia tardía hasta que llegaron nuevos competidores ofreciendo calidad superior a menor precio. Al sentir el impacto que estas incursiones tenían en los resultados, las organizaciones comenzaron a actuar. Una reacción similar está ocurriendo ahora con la cíber-seguridad.
A medida que sus estrategias y organizaciones de seguridad digital maduren y surjan nuevas soluciones, las organizaciones que vinculen los esfuerzos relacionados con la seguridad con las necesidades reales del negocio tendrán suficiente confianza en su capacidad para enfrentarse a las cíber- amenazas.

ACERCA DE ACCENTURE

Accenture es una compañía global líder en servicios profesionales que provee una amplia gama de servicios y soluciones en estrategia, consultoría, desarrollos digitales, tecnología y operaciones. Combinando su experiencia inigualable y sus habilidades especializadas en más de 40 industrias y en todas las funciones de negocios —respaldadas por la red de Delivery Centers más importante del mundo— Accenture trabaja en la intersección del negocio y la tecnología para ayudar a sus clientes a mejorar su desempeño y crear un valor sostenible para todos los involucrados. Con aproximadamente 384.000 empleados que prestan servicios a clientes en más de 120 países, Accenture impulsa la innovación para mejorar la manera en que el mundo trabaja y vive. Visítenos en www.accenture.com

ACERCA DE ACCENTURE RESEARCH

Accenture Research es un equipo global de analistas especializados en lo digital y la industria, que crean perspectivas basadas en datos para identificar disruptores, oportunidades y riesgos para Accenture y sus clientes. Utilizando técnicas innovadoras de investigación de negocios, como por ejemplo la modelización del valor económico, analytics, crowdsourcing, redes de expertos, encuestas, visualización de datos e investigación con socios académicos y de negocios, pueden elaborar cientos de puntos de vista que se publican cada año.

ACERCA DEL ESTUDIO "ACCENTURE GLOBAL HIGH PERFORMANCE SECURITY"

En 2016 Accenture Security encuestó a 2,000 ejecutivos de 12 industrias en 15 países de América del Norte y del Sur, Europa y Asia Pacífico. El objetivo de la encuesta era entender en qué medida las empresas priorizan la seguridad, cuán exhaustivos son los planes de seguridad y cuán resilientes son las empresas con respecto a la seguridad y el nivel de gasto asociado. La encuesta apuntó a medir las capacidades de seguridad en siete dominios estratégicos referidos a la cíber-seguridad identificados por Accenture: alineación con el negocio, capacidad de respuesta ante los cíber-ataques, inteligencia estratégica de las amenazas, cíber-resiliencia, eficiencia de las inversiones, gobierno y liderazgo y el ecosistema extendido. Más del 50 por ciento de los encuestados eran responsables claves en la toma de decisiones sobre estrategia y gasto en cíber-seguridad, incluyendo ejecutivos con nivel de director y superior del negocio, de TI y de seguridad en empresas con ingresos iguales o superiores a US$1.000 millones.

COLABORADORES

Kevin Richards, Managing Director, Norteamérica
Ryan M. LaSalle, Managing Director, Growth & Strategy
Rik Parker, Managing Director
David M. Cooper, Senior Manager

Copyright © 2016 Accenture
Todos los derechos reservados

Accenture, su logo y High Performance Delivered son marcas registradas de Accenture.

Este documento hace referencia a marcas comerciales que pueden pertenecer a terceros. El uso de dichas marcas comerciales no constituye una aseveración de la titularidad de dichas marcas por parte de Accenture ni intenta representar o implicar la existencia de una asociación entre Accenture y los titulares legítimos de dichas marcas comerciales. La información relacionada con los productos, servicios y organizaciones de terceros fue obtenida de fuentes públicamente disponibles y Accenture no puede confirmar la precisión o confiabilidad de dichas fuentes o información. Su inclusión no implica el aval de ningún tercero.

Los puntos de vista y las opiniones vertidas en este artículo no deben ser consideradas como asesoramiento profesional con respecto a su negocio.