accenture

HfS Research

El estado de la ciberseguridad y la confianza en lo digital en 2016

Cómo identificar las brechas de ciberseguridad para repensar el concepto de "vanguardia".

Resumen ejecutivo

Resumen ejecutivo

Si bien la llegada de la tecnología digital ha impulsado nuevos modelos y oportunidades de negocios, también ha aportado un elemento de riesgo, ya que los activos valiosos se tornan menos tangibles, más distribuidos y más vulnerables a las ciberamenazas.

Hoy en día, las organizaciones se ven amenazadas por muchos tipos diferentes de ciberatacantes, desde individuos que trabajan solos ("lobos solitarios") hasta equipos a sueldo sumamente organizados y bien patrocinados, capaces de violar los sistemas de ciberseguridad más sofisticados y cuyo blanco son los secretos personales, corporativos o de estado.

En la ciberseguridad actual se debe repensar la naturaleza de la seguridad y realizar un cambio desde el enfoque que hace hincapié en la protección de los activos vulnerables hacia otro basado en el fortalecimiento de los activos, para hacerlos más resilientes, como parte de un proceso integral de ciberseguridad que aporte un mayor valor a la empresa

La ciberseguridad debe ser parte de un marco de valor más amplio que incluya tanto la gestión de riesgos como el desarrollo de la confianza en lo digital.

La confianza en lo digital no es una tecnología ni un proceso: es un resultado demostrado a través de relaciones seguras, transparentes y de compromiso entre la empresa y sus empleados, sus socios y sus clientes. Está impulsada por la manera en que se protegen y se utilizan los activos de datos y la información, y es lo que ayuda a que una marca digital siga siendo exitosa y memorable.

Sin embargo, ¿cómo puede una empresa alcanzar este objetivo en un entorno en el que la tecnología y las tácticas de vanguardia suelen estar en desventaja frente a un adversario involucrado en cibertácticas asimétricas? No necesita concentrarse en la vanguardia tecnológica, sino en la vanguardia como una mentalidad organizacional que evolucione y se adapte continuamente para contrarrestar las amenazas en constante evolución. Es necesaria una cultura de la ciberseguridad impulsada por los directivos en todo el ecosistema de la empresa. Y requiere un enfoque de seguridad integral que dé como resultado una "confianza en lo digital" compartida y un mayor valor para todos los involucrados.

La investigación muestra una serie de brechas clave que tanto los especialistas en ciberseguridad como los ejecutivos de negocios deben zanjar para construir una empresa digital exitosa en una economía basada en la confianza. Estas brechas incluyen deficiencias en cinco áreas clave: talento, tecnología (detección y respuesta), paridad organizacional, presupuestos y financiamiento y gestión.

Pero la ciberseguridad sigue siendo una profesión joven –el rol actual del Chief Information Security Officer (CISO) data de apenas una década– y la idea de la "confianza en lo digital" como base del éxito del negocio es aún un concepto emergente en la economía digital.

En marzo de 2016, HfS Research y Accenture encuestaron a 208 especialistas en seguridad corporativa en diversas geografías y sectores verticales de la industria. Nuestro objetivo principal era conocer cómo se perciben y contrarrestan las amenazas de ciberseguridad dentro de la empresa, con miras a entender tanto el estado actual de la ciberseguridad como los pasos que debe dar la empresa para facilitar una mayor confianza en lo digital en todo el ecosistema.

Los resultados de la encuesta sobre ciberseguridad de Accenture y HfS son preocupantes: los líderes en ciberseguridad no creen que las amenazas vayan a desaparecer. De hecho, esperan que aumenten y continúen impactando, o actuando como un inhibidor de la confianza en lo digital en toda la empresa. Si bien invierten en defensas tecnológicas básicas, como firewalls, y en nuevas tecnologías, como las herramientas de behavioral analytics, las organizaciones no tienen suficientes profesionales capacitados para aprovechar adecuadamente la tecnología de la seguridad. Hay claras diferencias entre dónde están la mayoría de las empresas y dónde creen que tienen que estar. Y, sin embargo, el 36 por ciento de los encuestados sostiene que los directivos consideran que los gastos en ciberseguridad son un costo innecesario.

Muchos equipos de ciberseguridad están intentando zanjar las brechas existentes, experimentando con tecnologías cognitivas y otras tecnologías de inteligencia artificial avanzadas, mientras hacen esfuerzos por hallar el talento en materia de seguridad que pueda llevar a cabo eficazmente las acciones básicas. Establecer la confianza en lo digital, que se considera crucial para el éxito competitivo, requiere claramente de un nuevo modo de trabajar y no solo de una mejora incremental.

Entre las principales conclusiones del estudio se encuentran las siguientes:

El estado de las ciberamenazas

- El robo de "información corporativa por parte de agentes externos" y de "información personal por parte de agentes internos" domina el debate, y el 35 por ciento de los encuestados manifestó haber estado "muy preocupado o sumamente preocupado" por estas dos amenazas en los últimos 12 meses. Sin embargo, si avanzamos un poco más, la pérdida o la destrucción general de datos se vuelve una preocupación primordial: el 41 por ciento de los encuestados manifiesta una preocupación marcada o crucial para los próximos 12 a 18 meses.
- Las fuentes de amenazas que más preocupan a los especialistas en seguridad corporativa son los equipos privados y bien organizados, los delincuentes organizados y los profesionales patrocinados por el Estado, con planes de espionaje corporativo y el foco en la infraestructura crítica como sus principales inquietudes.
- La reputación de la marca y el soporte al cliente se valoran como los objetivos de negocio más vulnerables; el 43 y el 37 por ciento (respectivamente) de los encuestados revelaron que la seguridad de los datos era de suma importancia para respaldar estos esfuerzos.
- Cloud computing, la cultura de concientización acerca de la ciberseguridad, y el almacenamiento en la nube se valoran como las iniciativas corporativas más importantes, mientras que la conectividad móvil encabeza la lista de iniciativas en riesgo: el 47 por ciento de los encuestados mencionó la violación de datos o la pérdida del servicio asociado a dispositivos móviles como de máximo riesgo para la marca de la empresa.
- El 69 por ciento de los encuestados había presenciado una tentativa o concreción de robo o corrupción de datos por parte de agentes internos; las compañías y las agencias de medios de comunicación y tecnología de la región de Asia y el Pacífico arrojaron las tasas más altas en este sentido (77 por ciento y 80 por ciento, respectivamente).

La confianza en lo digital es más importante que nunca, y la ciberseguridad no es solo una expectativa de los consumidores: hoy es una demanda de toda economía digital basada en la confianza.

"En el entorno de negocios digitales de hoy, la confianza se basa en dos componentes principales: la ética y la seguridad. La confianza es la piedra angular de la economía digital".

Fuente: Accenture Technology Vision 2016 Survey, People First: The Primacy of People in the Digital Age www.accenture.com/technologyvision, #techvision2016

El estado de la ciber-respuesta

CINCO BRECHAS QUE SOCAVAN LA CONFIANZA EN LO DIGITAL

BRECHA DE TALENTO

- Los equipos de ciberseguridad están en plena batalla. El 42 por ciento de los encuestados cree que, si bien tiene suficiente presupuesto para afrontar la tecnología de seguridad, necesita un presupuesto adicional para la contratación de talento y capacitación en seguridad. El 31 por ciento de los encuestados mencionó la falta de presupuesto para contratar o capacitar personal como el inhibidor principal que les impide estar preparados para enfrentar los riesgos de la ciberseguridad.
- Solo el 20 por ciento de los encuestados cree que su proveedor de servicios de seguridad (Managed Security Services Provider, MSSP) es un verdadero socio que lidera a través de la innovación, mientras que el 31 por ciento cree que su MSSP podría ofrecer más innovación.
- El 76 por ciento de los encuestados cree que necesita un cierto nivel de mejora en su capacidad para llevar a cabo evaluaciones de amenazas y vulnerabilidad, mientras que el 24 por ciento restante considera que está a la vanguardia.

BRECHA TECNOLÓGICA

- Para hacer frente a las ciberamenazas, las empresas se basan en la misma tecnología estándar, como firewalls y encriptación de datos, pero las áreas de crecimiento más importantes son lo cognitivo /la IA, la anonimización de los datos, el seguimiento del comportamiento y la automatización: áreas que involucran nuevos gastos y nuevas habilidades.

BRECHA DE PARIDAD

- Siguen persistiendo diferencias entre las distintas unidades y funciones de la empresa. Concretamente, los equipos de TI se consideran los más seguros y los equipos de ventas, los menos seguros (el 25 por ciento de los encuestados indicó que su equipo de ventas era "no muy seguro" o "solo un poco" seguro).
- Entre el 35 y el 57 por ciento de las empresas declaró que examina a los socios del ecosistema en busca de ciberintegridad y preparación; en este sentido, los socios de BPO son los menos escrutados y los de crédito, los más investigados.
- Las diferencias en la preparación en materia de ciberseguridad entre unidades de negocio, geografías e industrias verticales siguen demostrando que no todos los socios del ecosistema están al mismo nivel de preparación en términos de ciberseguridad.

BRECHA DE PRESUPUESTO

- El 70 por ciento de los encuestados mencionó la falta o la insuficiencia de financiamiento, ya sea para la tecnología de la ciberseguridad o para obtener talento en la materia (incluida la capacitación).
- Un 12 por ciento adicional de los encuestados declaró que tiene niveles de financiamiento / personal insuficientes o solicitudes de recorte en estas áreas.

Si estas brechas no se abordan de manera proactiva, la seguridad corporativa podría debilitarse significativamente, lo que retardaría la madurez en ciberseguridad y generaría un riesgo mayor para la empresa.

BRECHA DE GESTIÓN

- Mientras que el 54 por ciento de los encuestados estuvo de acuerdo o muy de acuerdo en que la ciberseguridad es un facilitador de la confianza en lo digital para los consumidores, el 36 por ciento cree que los directivos consideran que la ciberseguridad es un costo innecesario.
- Las grandes empresas (de más de 50.000 empleados) tienen el mayor porcentaje de especialistas en ciberseguridad que creen que los directivos consideran a la ciberseguridad como un costo innecesario (48 por ciento), cifra que coincide en organizaciones del sector público / gubernamentales / no gubernamentales.
- Solo un tercio (36 por ciento) de los especialistas en ciberseguridad tiene una línea de reporte directo al CEO. Los especialistas en ciberseguridad anticipan un cambio de dirección en la estructura de reporte que pasaría del CEO y del CIO al COO y al CRO.
- Solo el 5 por ciento de las organizaciones encuestadas tiene un ejecutivo de riesgos (o de confianza) que reporta directamente al CEO o al Directorio.

Entre las recomendaciones clave que surgen de analizar los resultados del estudio se encuentran las siguientes:

La dirección ejecutiva debe asumir una posición visible, vocal y comprometida sobre la ciberseguridad, de manera tal de impulsar una cultura que valore y potencie la confianza en lo digital en toda la empresa.

El talento existente en materia de ciberseguridad se debe ampliar y capacitar, a fin de impulsar las prácticas de seguridad integrales y las tecnologías emergentes para abordar mejor la cantidad y la sofisticación de los ciberataques.

Las operaciones de ciberseguridad y la dirección ejecutiva deben colaborar para identificar y eliminar las brechas entre los requisitos de seguridad y la capacidad de ejecución en áreas tales como talento y capacitación, tecnología y procesos, y presupuestos y finanzas, con miras a garantizar un alto nivel de preparación en materia de seguridad en toda la empresa.

Los equipos de ciberseguridad de las empresas deben establecer capacidades de innovación y pruebas para identificar, examinar y evaluar, de manera rápida y rentable, tecnologías nuevas y emergentes (como los sistemas de análisis del comportamiento, la automatización, la tecnología cognitiva y la integración física /digital) para poder seguir el ritmo de la evolución de las ciberamenazas.

Las empresas deben contemplar un cambio en la forma en que consideran al financiamiento de la ciberseguridad y evitar tratar a los costos como gastos generales. En lugar de ello, se debe seguir un enfoque holístico que incluya los costos de protección y uso de los datos como parte de los requisitos financieros generales de la iniciativa del negocio.

La vanguardia en ciberseguridad es un enfoque, una actitud, y no una implementación o un resultado tecnológico final. Evoluciona y se adapta, a medida que cambia el valor de los activos y el tipo o el nivel de las amenazas.

accenture

HfS Research

El estado de la ciberseguridad y la confianza en lo digital en 2016

Cómo identificar las brechas de ciberseguridad para repensar el concepto de "vanguardia".

Resumen ejecutivo