ECONOMIA, ULTIMAS NOTICIAS

La confianza excesiva en el software es la mayor debilidad para las amenazas cibernéticas

16 septiembre, 2019 10:39 am

Las empresas han volcado miles de millones de dólares en tecnología y software que promete mantener alejadas las amenazas cibernéticas. La inversión global total en software de antivirus, por ejemplo, alcanzará US$3.77 billones en 2019, según el grupo de investigación de mercado ARC.

El software sin dudas tiene un rol importante en el combate contra las amenazas digitales, pero otras áreas han sido descuidadas. Reveladoramente, los líderes de negocios encuestados en el International Business Report (IBR) de Grant Thornton dicen que la confianza excesiva en el software es su mayor debilidad a la hora de

manejar amenazas cibernéticas y de privacidad. Combinándolas, definimos a las amenazas de ciberseguridad y de privacidad de la información como amenazas digitales.

Es alentador que los líderes de negocio reconozcan esto. Pero ahora deben actuar, mejorando sus habilidades digitales y la conciencia de ciberseguridad de todos sus empleados. También deberían explorar los seguros de ciberseguridad.

Esto no significa desembolsar más dinero. En muchos casos, podrán reducir el gasto en software a medida que refuerzan sus capacidades humanas y provisiones de seguro. Reveladoramente, ARC predice que los ingresos del mercado de los software de antivirus se reducirán en un -1.2% de tasa de crecimiento anual compuesto durante los próximos 5 años.

Impulsar la conciencia, pulir las habilidades

Nuevas formas de generar conciencia

Las empresas pueden haber sofisticado su software de ciberseguridad, pero eso no prevendrá el error humano que se encuentra detrás de muchas filtraciones. Después de todo, es la fuerza de trabajo humana quien responde a los emails de phishing e instala software no autorizado.

Pero las empresas gastan mucho más en software de ciberseguridad que en educar a sus empleados, así que no sorprende que vean la confianza excesiva en la tecnología como una desventaja clave en el manejo del riesgo digital.

Pueden hacer frente a esto aumentando la conciencia de ciberseguridad de todos los empleados. ¿Pero cómo? Después de todo, las empresas han realizado *webinars* sobre ciberseguridad y programas de capacitación obligatorios durante años, sin embargo el error humano continúa exponiéndolos a los ciberataques. Una nueva forma de educación es necesaria.

Christos Makedonas, líder de riesgo digital en Grant Thornton Chipre, dice que un formato de capacitación más corto podría ayudar. "Nadie tiene tiempo de mirar horas de video," dice. "Deberían acortarse a un máximo de dos minutos. También necesita recordatorios visuales – como banners en la oficina y mensajes en las pantallas – para recordarle las mejores prácticas a las personas.

"Las empresas deberían similar intentos de phishing, y se podría capacitar más a los empleados que responden a ellos. Hemos visto que estos tipos de programas de entrenamiento son mucho más exitosos que los *webinars* tradicionales."

Primero identifique vulnerabilidades, luego invierta

Las empresas necesitan entender dónde son vulnerables a los ciberataques y a las filtraciones de información antes de invertir en software preventivo. Esto requiere de habilidades especializadas que la mayoría de las empresas no tiene.

"Las empresas necesitan de conjuntos de habilidades relacionadas a la privacidad que les ayuden a visualizar su información y entender sus requerimientos regulatorios – especialmente en un contexto en la nube," dice Mike Harris, socio de servicios de ciberseguridad en Grant Thornton Irlanda. "También necesitan habilidades de cibertecnología alrededor de las tecnologías que están usando.

Ultimas Noticias


El presupuesto en Seguridad se ajusta para priorizar educación y salud


El Nuevo Orden Social


La confianza excesiva en el software es la mayor debilidad para las amenazas cibernéticas


Bárbaro: "La campaña es un tiempo de cosechas para el Pays"

VER MÁS ULTIMAS NOTICIAS >>

Cotizador

CotizacionDolar.com.ar

16/09/19	compra	venta
Dólar	54.68	58.98
Euro	61.76	65.87
Real	13.07	14.80

"Por ejemplo, si está usando servicios de nube proveídos por Amazon o Azure, necesita tener las habilidades de seguridad internas para descifrar qué harán y qué no en términos de ciberseguridad. Ese componente de las habilidades suele pasarse por alto."

La tecnología analítica avanzada necesita de mentes analíticas avanzadas

Muchas empresas han invertido mucho en tecnologías analíticas avanzadas de ciberseguridad que ayudan a identificar nuevas amenazas y vulnerabilidades.

Pero serán tan buenas como la fuerza de trabajo que pueda interpretar los resultados e implementar los cambios correspondientes.

"Muchas personas ven a la tecnología como una fórmula mágica, pero no lo es," dice James Arthur, socio y líder de consultoría cibernética en Grant Thornton Reino Unido. "Muchas empresas gastan mucho dinero en software de ciberseguridad impulsado por inteligencia artificial, o de analíticas de comportamiento, el cual puede ser muy útil en algunas circunstancias, pero sin embargo normalmente se necesita una enorme inversión de tiempo humano en capacitación para asegurarse de que nos traiga los resultados que queremos. Luego se necesita de un humano al final que pueda mirar ese resultado y hacer o aprobar los cambios."

El creciente caso de la cobertura cibernética

Asegúrese contra lo inevitable

"Sólo hay dos tipos de empresas: las que fueron hackeadas y las que lo serán. E incluso ambas están convergiendo en una sola categoría: empresas que fueron hackeadas y volverán a serlo."

Esas son palabras del anterior director del FBI, Robert Mueller, en 2012.

Su mensaje es claro – y es igual de relevante hoy que como lo fue hace siete años: una filtración es inevitable. Esto es una fuerte razón para invertir en un seguro para mitigar el impacto de los ciberataques, más que sólo en un software que los prevenga.

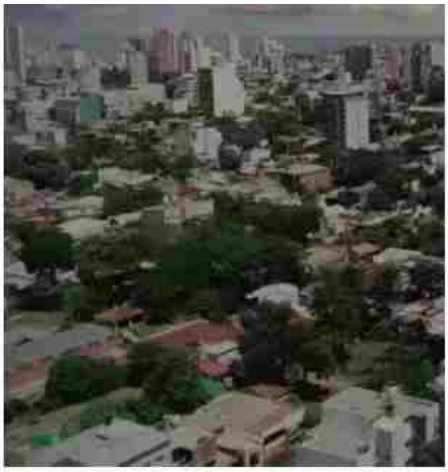
"Cualquier programa de riesgo digital razonable tiene que tener un elemento de detección, respuesta y cobertura, porque los incidentes cibernéticos sucederán," dice Mike Harris. "Vemos un crecimiento en la adopción de seguros que cubren ciberataques y filtraciones de información. Pero aunque sea imperativo y su uso esté creciendo, la mayoría de los negocios todavía no tienen este tipo de seguro."

Las empresas podrían asumir que su seguro general cubre los ciberataques. Pero se llevarían una fea sorpresa. Por ejemplo, la aseguradora Hiscox está disputando una demanda de la firma legal DLA Piper – probablemente de varios millones de libras – basada en que no tenía una política específica de ciberseguridad.

Desarmar la cobertura cual forense

Pero ni siquiera las empresas con cobertura cibernética no pueden ponerse cómodas. Las aseguradoras pueden rehusarse a pagar si ven el ataque como un acto de guerra, lo cual podría debatirse si fuera iniciado por agentes apoyados por el estado.

"La cobertura es genial, pero el enemigo está en el detalle," explica James Arthur. "Hemos visto aseguradoras intentando discutir para librarse de pagar porque el ataque



Ediciones Anteriores

septiembre 2019

L	M	X	J	V	S	D
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

« AGO

Entrevistas

Energía de Misiones: «Para surfear la crisis, lo que hicimos fue ordenar la empresa»

se rastreó hasta un grupo estatal." Mucho malware puede relacionarse con algún tipo de actividad estatal, así que las empresas realmente necesitan ver los detalles.

Además, las políticas cibernéticas pueden contener provisiones que requieran a las empresas el instalar actualizaciones y parches frecuentemente. El incumplimiento podría resultar en que los aseguradores no paguen en caso de un incidente.

"Algunas políticas le requieren a las empresas mantener su administración de los parches mucho más al día de lo que están acostumbradas – o de lo que quisieran, dada la disrupción que puede causar," agrega Arthur.

Las empresas deben entonces examinar los detalles de su cobertura cibernética cual forense, para asegurarse de que están cubiertas y de que pueden cumplir con sus requerimientos.

Colabore con las aseguradoras

El caso para la cobertura contra el riesgo digital ha crecido, pero la sofisticación de las ofertas de seguros no lo ha hecho. Esta es la opinión de los líderes de negocios encuestados en el IBR de Grant Thornton. Reveladoramente, más de dos tercios cree que la industria de los seguros necesita mejorar su oferta sobre riesgos de la privacidad.

"El mercado de los seguros contra filtraciones no es para nada maduro comparado con otros mercados de seguros," explica Christos Makedonas. "A las aseguradoras les está costando evaluar los riesgos porque las empresas tienen diferentes vulnerabilidades. Dos empresas del mismo sector y del mismo tamaño pueden tener distintas culturas y usar tecnologías distintas, lo cual hace muy difícil ponerle precio al riesgo.

"Pero es muy importante para las empresas el explorar esto y trabajar con las aseguradoras para impulsar el Mercado hacia Adelante."

Cinco recomendaciones para crear un enfoque balanceado para el manejo del riesgo digital

1. Los enfoques tradicionales a las capacitaciones cibernéticas no están funcionando. Las empresas deberían desarrollar videos regulares más cortos y similar intentos de phishing para educar mejor a sus empleados.

1. Las empresas necesitan capacidad para identificar y visualizar sus vulnerabilidades digitales. Necesitan reclutar personas con habilidades especializadas que complementen el software de ciberseguridad. Esto les asegurará que su inversión en software preventivo está enfocada en las áreas correctas.

1. Todas las empresas sufrirán un ciberataque – no importa cuánto inviertan en software preventivo. Una cobertura general puede no cubrir ciberataques, así que las empresas deben explorar seguros específicos de riesgo digital que cubran ciberataques y filtraciones de información.

1. Pero el Mercado de seguros digitales es relativamente inmaduro. Entonces, las empresas deberían pasar tiempo educando a las aseguradoras acerca de sus vulnerabilidades específicas para se le ponga un precio efectivo al riesgo.


Entrevista al CEO de Mercedes Benz: "Qué mejor que un argentino para trabajar en una crisis"


Entrevista exclusiva a Gerardo Díaz Beltrán, presidente de la CAME: "Creíamos que con Macri se venía una buena etapa para las pymes, pero al final no se concretó"


Florencia Gómez: "Antes que reforma agraria, hay que hablar de democratización del acceso a la tierra"


Cuando el rock es más fuerte

VER MÁS ENTREVISTAS >>

VER MÁS VIÑETAS >>

1. Una vez contratado el seguro, las empresas deben ser cuidadosas sobre la adhesión a los términos y condiciones. El no instalar actualizaciones podría anular la cobertura.

Estas recomendaciones deben implementarse en el contexto del ambiente de riesgo digital específico de la empresa. Entonces el primer paso para los líderes de negocio es entender sus vulnerabilidades y amenazas específicas. Sólo así pueden implementar las tecnologías más relevantes, iniciativas de capacitación y cobertura del seguro.

Dejar un comentario

*Tu dirección de correo electrónico no será publicada. Los campos obligatorios están marcados con **

Mensaje

Nombre *

Correo Electrónico *

Sitio Web

☐ **Guardar mi nombre, correo electrónico y sitio web en este navegador para la próxima vez que haga un comentario.**

reCAPTCHA

Habilita JavaScript para obtener un desafío de reCAPTCHA.

¿Por qué me sucede esto?

En foco

El acceso a la tierra, la experiencia en Misiones y el caso emblemático de Pozo Azul

Presupuesto 2020: Misiones prioriza la educación y la contención social en "un contexto difícil"

De las promesas al ajuste: radiografía del estado de la educación

¿Qué Coparticipación pide Misiones? Al menos lo mismo que Chaco, en julio fueron $2.000 millones menos

Un gran desafío para la industria turística: Llega este viernes el primer vuelo regular que conecta a Iguazú con Europa y Misiones se convierte en puerta de entrada al país

VER MÁS EN FOCO >>

Canal Economis

Se produjo un error.

Intenta ver este video en www.youtube.com o habilita JavaScript en caso de que no lo tengas habilitado tu navegador.

120575 Las empresas han volcado miles de millones de dólares en tecnología y software que promete mantener alejadas las amenazas cibernéticas. La inversión global total en software de antivirus, por ejemplo, alcanzará US$3.77 billones en 2019, según el grupo de investigación de mercado ARC.
El software sin dudas tiene un rol importante en el combate contra las amenazas digitales, pero otras áreas han sido descuidadas. Reveladoramente, los líderes de negocios encuestados en el International Business Report (IBR) de Grant Thornton dicen que la confianza excesiva en el software es su mayor debilidad a la hora de manejar amenazas cibernéticas y de privacidad. Combinándolas, definimos a las amenazas de ciberseguridad y de privacidad de la información como amenazas digitales.
Es alentador que los líderes de negocio reconozcan esto. Pero ahora deben actuar, mejorando sus habilidades digitales y la conciencia de ciberseguridad de todos sus empleados. También deberían explorar los seguros de ciberseguridad.
Esto no significa desembolsar más dinero. En muchos casos, podrán reducir el gasto en software a medida que refuerzan sus capacidades humanas y provisiones de seguro. Reveladoramente, ARC predice que los ingresos del mercado de los software de antivirus se reducirán en un -1.2% de tasa de crecimiento anual compuesto durante los próximos 5 años.
Las empresas pueden haber sofisticado su software de ciberseguridad, pero eso no prevendrá el error humano que se encuentra detrás de muchas filtraciones. Después de todo, es la fuerza de trabajo humana quien responde a los emails de phishing e instala software no autorizado.
Pero las empresas gastan mucho más en software de ciberseguridad que en educar a sus empleados, así que no sorprende que vean la confianza excesiva en la tecnología como una desventaja clave en el manejo del riesgo digital.
Pueden hacer frente a esto aumentando la conciencia de ciberseguridad de todos los empleados. ¿Pero cómo? Después de todo, las empresas han realizado webinars sobre ciberseguridad y programas de capacitación obligatorios durante años, sin embargo el error humano continúa exponiéndolos a los ciberataques. Una nueva forma de educación es necesaria.
Christos Makedonas, líder de riesgo digital en Grant Thornton Chipre, dice que un formato de capacitación más corto podría ayudar. "Nadie tiene tiempo de mirar horas de video," dice. "Deberían acortarse a un máximo de dos minutos. También necesita recordatorios visuales – como banners en la oficina y mensajes en las pantallas – para recordarle las mejores prácticas a las personas.
"Las empresas deberían similar intentos de phishing, y se podría capacitar más a los empleados que responden a ellos. Hemos visto que estos tipos de programas de entrenamiento son mucho más exitosos que los webinars tradicionales."
Las empresas necesitan entender dónde son vulnerables a los ciberataques y a las filtraciones de información antes de invertir en software preventivo. Esto requiere de habilidades especializadas que la mayoría de las empresas no tiene.
"Las empresas necesitan de conjuntos de habilidades relacionadas a la privacidad que les ayuden a visualizar su información y entender sus requerimientos regulatorios – especialmente en un contexto en la nube," dice Mike Harris, socio de servicios de ciberseguridad en Grant Thornton Irlanda. "También necesitan habilidades de cibertecnología alrededor de las tecnologías que están usando.
"Por ejemplo, si está usando servicios de nube proveídos por Amazon o Azure, necesita tener las habilidades de seguridad internas para descifrar qué harán y qué no en términos de ciberseguridad. Ese componente de las habilidades suele pasarse por alto."
Muchas empresas han invertido mucho en tecnologías analíticas avanzadas de ciberseguridad que ayudan a identificar nuevas amenazas y vulnerabilidades.
Pero serán tan buenas como la fuerza de trabajo que pueda interpretar los resultados e implementar los cambios correspondientes.
"Muchas personas ven a la tecnología como una fórmula mágica, pero no lo es," dice James Arthur, socio y líder de consultoría cibernética en Grant Thornton Reino Unido. "Muchas empresas gastan mucho dinero en software de ciberseguridad impulsado por inteligencia artificial, o de analíticas de comportamiento, el cual puede ser muy útil en algunas circunstancias, pero sin embargo normalmente se necesita una enorme inversión de tiempo humano en capacitación para asegurarse de que nos traiga los resultados que queremos. Luego se necesita de un humano al final que pueda mirar ese resultado y hacer o aprobar los cambios."
"Sólo hay dos tipos de empresas: las que fueron hackeadas y las que lo serán. E incluso ambas están convergiendo en una sola categoría: empresas que fueron hackeadas y volverán a serlo."
Esas son palabras del anterior director del FBI, Robert Mueller, en 2012.
Su mensaje es claro – y es igual de relevante hoy que como lo fue hace siete años: una filtración es inevitable. Esto es una fuerte razón para invertir en un seguro para mitigar el impacto de los ciberataques, más que sólo en un software que los prevenga.
"Cualquier programa de riesgo digital razonable tiene que tener un elemento de detección, respuesta y cobertura, porque los incidentes cibernéticos sucederán," dice Mike Harris. "Vemos un crecimiento en la adopción de seguros que cubren ciberataques y filtraciones de información. Pero aunque sea imperativo y su uso esté creciendo, la mayoría de los negocios todavía no tienen este tipo de seguro."
Las empresas podrían asumir que su seguro general cubre los ciberataques. Pero se llevarían una fea sorpresa. Por ejemplo, la aseguradora Hiscox está disputando una demanda de la firma legal DLA Piper – probablemente de varios millones de libras – basada en que no tenía una política específica de ciberseguridad.
Pero ni siquiera las empresas con cobertura cibernética no pueden ponerse cómodas. Las aseguradoras pueden rehusarse a pagar si ven el ataque como un acto de guerra, lo cual podría debatirse si fuera iniciado por agentes apoyados por el estado.
"La cobertura es genial, pero el enemigo está en el detalle," explica James Arthur. "Hemos visto aseguradoras intentando discutir para librarse de pagar porque el ataque se rastreó hasta un grupo estatal." Mucho malware puede relacionarse con algún tipo de actividad estatal, así que las empresas realmente necesitan ver los detalles.
Además, las políticas cibernéticas pueden contener provisiones que requieran a las empresas el instalar actualizaciones y parches frecuentemente. El incumplimiento podría resultar en que los aseguradores no paguen en caso de un incidente.
"Algunas políticas le requieren a las empresas mantener su administración de los parches mucho más al día de lo que están acostumbradas – o de lo que quisieran, dada la disrupción que puede causar," agrega Arthur.
Las empresas deben entonces examinar los detalles de su cobertura cibernética cual forense, para asegurarse de que están cubiertas y de que pueden cumplir con sus requerimientos.
El caso para la cobertura contra el riesgo digital ha crecido, pero la sofisticación de las ofertas de seguros no lo ha hecho. Esta es la opinión de los líderes de negocios encuestados en el IBR de Grant Thornton. Reveladoramente, más de dos tercios cree que la industria de los seguros necesita mejorar su oferta sobre riesgos de la privacidad.
"El mercado de los seguros contra filtraciones no es para nada maduro comparado con otros mercados de seguros," explica Christos Makedonas. "A las aseguradoras les está costando evaluar los riesgos porque las empresas tienen diferentes vulnerabilidades. Dos empresas del mismo sector y del mismo tamaño pueden tener distintas culturas y usar tecnologías distintas, lo cual hace muy difícil ponerle precio al

riesgo.
"Pero es muy importante para las empresas el explorar esto y trabajar con las aseguradoras para impulsar el Mercado hacia Adelante."
Estas recomendaciones deben implementarse en el contexto del ambiente de riesgo digital específico de la empresa. Entonces el primer paso para los líderes de negocio es entender sus vulnerabilidades y amenazas específicas. Sólo así pueden implementar las tecnologías más relevantes, iniciativas de capacitación y cobertura del seguro.