Las diferencias generacionales aumentan el riesgo de seguridad de la información corporativa

El 55 % de los encuestados creen que los empleados millennial probablemente planteen el mayor riesgo de seguridad, según la encuesta sobre TI de Citrix y The Ponemon Institute

Según una encuesta reciente llevada a cabo por The Ponemon Institute y Citrix, existen dos riesgos de seguridad informática importantes para los que las empresas deben prepararse: los empleados *millennial* y el Reglamento General de Protección de Datos (GDPR), que próximamente entrará en vigor. El estudio global de más de 4000 profesionales de TI, de seguridad y de negocios arrojó que los *millennials* usan una cantidad cada vez mayor de aplicaciones, dispositivos móviles y nuevos métodos para compartir la información y colaborar, que plantean nuevos riesgos de seguridad a las empresas. El estudio también mostró que la mayoría de las compañías dudan de su capacidad de cumplir con los rigurosos requisitos de seguridad y cumplimiento del Reglamento GDPR propuesto.

La fuerza de trabajo actual está conformada por tres generaciones distintas, y cada una tiene una visión diferente sobre cómo compartir la información, la colaboración, la tecnología y el rol que desempeña la seguridad en cada uno de estos aspectos. El estudio muestra que cada generación también es susceptible a distintos tipos de vulnerabilidades en materia de seguridad:

- El 55% de los encuestados dedicados a la seguridad y a los negocios dijeron que los *millennials*, nacidos entre 1981 y 1997, suponen el riesgo más grande de eludir las políticas de seguridad informática y usar aplicaciones no autorizadas en el lugar de trabajo.
- El 33% dijeron que la generación conocida como *baby boomers*, nacidos entre 1946 y 1964,son los más susceptibles a las estafas de *phishing* e ingeniería social.
- El 32% dijeron que los miembros de la llamada Generación X, nacidos entre 1965 y 1980,son los que tienen más probabilidades de eludir las políticas de seguridad y usar aplicaciones y dispositivos no aprobados en el lugar de trabajo.

El Reglamento impone más requisitos en materia de seguridad

El Reglamento GDPR, que entrará en vigor en mayo de 2018, es una medida de la Unión Europea (UE) que apunta a proteger la información corporativa y los datos de los empleados ahora que los trabajadores están cruzando las fronteras digitales y físicas en todo el mundo. El Reglamento afectará a las empresas de todo el mundo, incluyendo a toda organización dentro y fuera de la UE que comparta datos o venda productos o servicios en la región. A medida que las empresas se preparan, deben sortear algunos obstáculos. El estudio de Citrix y The Ponemon Institute arrojó que el 67% de las empresas globales encuestadas están al tanto del GDPR, pero que sólo un 50 %, aproximadamente, han comenzado a prepararse para el nuevo reglamento. Los obstáculos más importantes son:

- **Las empresas con actividad comercial en Europa deben adaptarse:** El 74% de los encuestados dicen que el GDPR tendrá un impacto importante y negativo en las operaciones de negocios. El 65% están preocupados por las nuevas multas de hasta 100 millones de Euros o entre el 2% y el 4% del ingreso mundial anual.
- **Las tecnologías deben proteger toda la información en todo lugar:** El 52% de los encuestados

considera que su infraestructura de seguridad no facilita el cumplimiento y la aplicación del reglamento con un enfoque centralizado del control, monitoreo y elaboración de informes sobre los datos.

- **Repercusiones globales:** Al 53% les preocupa el aumento de los efectos globales que traerá aparejado el GDPR, dado que impactará a más negocios, incluyendo a muchos que están fuera de la UE.

Stan Black, Director de Seguridad CSO de Citrix

"Todos somos susceptibles a una vulneración de seguridad. Las organizaciones no pueden tomarse su tiempo para implementar estrategias inteligentes de seguridad. La seguridad es una preocupación global, y ya sea una organización gubernamental grande o una pequeña empresa, el momento de actuar es ahora. Mientras se implementan estas normas más estrictas, se debe adoptar un enfoque estratégico, poner las cosas en perspectiva, educar a la fuerza de trabajo para crear una cultura consciente de la seguridad y buscar soluciones integrales que satisfagan las necesidades únicas de cada empresa. La arquitectura de seguridad del futuro es predictiva y adaptativa, y aprovecha los beneficios de las tecnologías emergentes para resolver los desafíos de seguridad empresariales".

Tim Minahan, Director de Marketing CMO de Citrix

"Desde que la transformación digital llevó a que el lugar de trabajo sea cualquier lugar, el acceso ya no se limita a las redes corporativas. Y si bien la fuerza de trabajo actual es más flexible y productiva, los enfoques tradicionales de la seguridad también deben evolucionar. Los datos cruzan fronteras digitales a cada minuto, y las arquitecturas de seguridad deben tener en cuenta esta fusión de la vida personal y la vida laboral. Una arquitectura de seguridad inteligente también tiene en cuenta las necesidades de la fuerza de trabajo, incluyendo las diferencias generacionales, para eliminar las amenazas a la seguridad que deberían ser fáciles de controlar para que las empresas puedan enfocarse en el negocio y en los clientes".

Metodología de la encuesta

El informe llevado a cabo por The Ponemon Institute y auspiciado por Citrix, "La necesidad de una nueva arquitectura de seguridad informática: estudio global" analizó tendencias mundiales en materia de riesgos para la seguridad informática y los motivos por los que las prácticas y políticas de seguridad deben evolucionar para manejar las amenazas de las tecnologías disruptivas, los delitos cibernéticos y las exigencias relativas al cumplimiento de normas. La investigación recoge los testimonios de más de 4.200 profesionales de TI y seguridad informática de Australia/Nueva Zelanda, Brasil, Canadá, China, Alemania, Francia, India, Japón, Corea, México, Países Bajos, Emiratos Árabes Unidos, Reino Unido y Estados Unidos.

Síganos

- Twitter: @CitrixLatAm
- Facebook: Citrix LAC

Acerca de Citrix

Citrix (NASDAQ:CTXS) tiene el objetivo de crear un mundo donde las personas, las organizaciones y las cosas estén conectadas y sean accesibles de forma segura para hacer posible lo extraordinario. Gracias a su tecnología se puede acceder

de forma segura y fácil a las aplicaciones y datos de todo el mundo, impulsando a las personas a trabajar desde cualquier lugar, en cualquier momento. Citrix ofrece una cartera completa e integrada de soluciones de espacio de trabajo como servicio, entrega de aplicaciones, virtualización, movilidad, sistemas de entrega en redes e intercambio de archivos que permite a los sectores de TI garantizar el acceso a sistemas críticos para los usuarios a través de la nube o en las instalaciones de la empresa, desde cualquier dispositivo o plataforma. Con ingresos anuales de USD 3.420 millones en 2016, más de 400.000 organizaciones y 100 millones de usuarios de todo el mundo utilizan las soluciones de Citrix. Conozca más en www.citrix.com.