Noticias de Aon

Aon presenta el informe “Cyber Security Report 2019: What’s Now and What’s Next“

Destaca 8 áreas de riesgo que reflejan cómo el giro hacia lo digital está generando grandes oportunidades pero también mayores riesgos

19 de enero de 2019 – Aon plc (NYSE: AON), empresa global líder en servicios profesionales que ofrece un amplio abanico de soluciones de riesgos, capital humano y salud, ha presentado su informe anual sobre ciber riesgos **“Cyber Security Report 2019: What’s Now and What’s Next”.** El informe, que detalla las grandes amenazas y retos en materia de ciberseguridad a los que actualmente se enfrentan las organizaciones, reflexiona sobre cómo, a medida que las empresas continúan utilizando la tecnología para agilizar la transferencia de información, surgen oportunidades que pueden cambiar las reglas de juego pero también aumentan la exposición al ciber riesgo.

"En 2018, fuimos testigos de que un enfoque proactivo durante la preparación y planificación cibernética aportaba resultados realmente positivos a las compañías que decidieron invertir en ella, y en 2019, anticipamos que la necesidad de una planificación avanzada seguirá creciendo y aumentando", afirma J. Hogg, CEO de Cyber Solutions en Aon. "Los líderes deben trabajar para aislar mejor a sus empresas y sus procesos, al mismo tiempo que identifican las vías por las que pueden beneficiarse de las oportunidades que ofrece la tecnología y la transformación digital".

Hogg añade: “Nuestro informe 2019 también muestra que las organizaciones deben reconocer la necesidad de compartir información sobre amenazas no solo a través de su propia red, sino también a través de los terceros reconocidos. Si bien puede parecer contrario a los principios básicos de ciberseguridad, la colaboración dentro y entre empresas e industrias puede mantener protegidos los datos personales y la información confidencial de las sociedades. Trabajar juntos puede resultar en mejores esfuerzos para atrapar a los cibercriminales, al tiempo que eleva el nivel y hace que todas las partes estén más preparadas para el inevitable día en que ocurra un incidente de ciberseguridad".

El informe “What’s Now and What’s Next" se centra en ocho áreas de riesgo específicas a las que las compañías pueden enfrentarse en 2019. Los riesgos ilustran cómo, a medida que las organizaciones facilitan y promueven la transición a un enfoque digital en todas las transacciones, la superficie de ataque de los negocios globales se expande rápidamente y a veces de forma inesperada. En otras palabras, gracias a las rápidas mejoras y los constantes cambios en tecnología, los vectores de ataque a los que pueden acceder los ciberdelincuentes dentro de una empresa crecen de forma exponencial.

Principales Conclusiones: 8 áreas de riesgo

1. **Tecnología** – Aunque la tecnología ha revolucionado la forma en la que las organizaciones gestionan su negocio en la actualidad, su mayor uso también implica una mayor vulnerabilidad. Desde la publicidad o la automoción, todos los sectores están desarrollando nuevos servicios y modelos de negocio. Estas oportunidades generan también un conjunto de riesgos radicalmente diferente, que las organizaciones deben anticipar y gestionar dentro de sus procesos de transformación digital.

2. **Cadena de Suministro** - Dos tendencias principales relacionadas con la cadena de suministro intensificarán de forma importante los ciber riesgos durante el próximo año: una es la rápida expansión de los datos operativos expuestos a los ciber delincuentes desde dispositivos móviles, de red y el Internet of Things (IoT); otra es la tendencia creciente por parte de las empresas a confiar en terceras partes y proveedores de servicios externos. Ambas ofrecen a los atacantes nuevas brechas en la cadena de suministro y requieren una gestión de riesgos a largo plazo y con implicación de la alta dirección si se quieren llevar a cabo operaciones comerciales fiables y viables.

3. **IoT** – Los dispositivos IoT están en todas partes, y su presencia en el lugar de trabajo supone un potencial riesgo para la seguridad. Muchas organizaciones no gestionan de forma segura o ni siquiera cuentan con un inventario que incluya todos los dispositivos IoT relacionados con su actividad, lo que ya está derivando en importantes brechas de seguridad. A medida que pasa el tiempo, el número de terminales IoT se incrementa drásticamente, a lo que contribuye el lanzamiento actual de dispositivos IoT y la próxima transición al 5G.

AON
Empower Results®

4. **Operaciones de Negocio** – La conectividad a Internet mejora de forma significativa las tareas operativas pero una mayor conectividad también genera nuevas vulnerabilidades. La superficie de ataque se amplía de forma importante, facilitando a los atacantes el movimiento lateral dentro de una red completa. Además, los accesos directos operativos o los procesos de backup inefectivos pueden amplificar aún más el impacto de un ciberataque. Las organizaciones deben conocerse mejor y estar preparadas para el ciber impacto derivado de una mayor conectividad.

5. **Empleados** – Los empleados siguen constituyendo una de las causas más comunes de brechas de seguridad, aunque muchas veces ellos mismos no son conscientes de la amenaza que suponen para la ciberseguridad de su organización. A medida que la tecnología continúa impactando en todas las funciones, desde el CEO a los recién incorporados, es fundamental que la organización establezca un enfoque integral para mitigar los riesgos internos, incluyendo una sólida gestión de datos, políticas de comunicación en materia de ciberseguridad e implementación de controles efectivos de acceso y protección de datos, así como de servicios de concienciación.

6. **Fusiones y Adquisiciones** – Las previsiones anticipan que el valor de las operaciones de fusión y adquisición habrán alcanzado los 4 billones de dólares en 2018, lo que supone la cifra más alta en cuatro años [1]. El problema que esto plantea a las empresas que adquieren otros negocios es que mientras ellos pueden tener un enfoque correcto en relación con la gestión de riesgos relacionados con la ciberseguridad, no existe garantía de que sus objetivos de compra también lo tengan. Los actores que intervienen en la operación deben contar con una estrategia específica de ciberseguridad en sus planes de fusiones y adquisiciones si quieren garantizar una transición sin problemas en el futuro.

7. **Regulación** – Mayor regulación, leyes, normas y estándares relacionados con cuestiones ciber se están diseñando para proteger y aislar negocios y clientes. El ritmo de la presión regulatoria se ha incrementado en 2018, fijando el escenario para un mayor riesgo de cumplimiento en 2019. La regulación y el cumplimiento, no obstante, no pueden constituir el único objetivo. Las organizaciones deben mantener un equilibrio entre las nuevas regulaciones y la evolución de las amenazas cibernéticas, lo que requerirá de un seguimiento desde todos los ángulos.

8. **Comité de Dirección** – La negligencia en materia de ciberseguridad continúa siendo un punto importante para los comités de dirección y administradores, pero la historia reciente muestra un aumento de los riesgos personales. La alta dirección debe seguir ampliando su foco y manteniendo un enfoque exigente dentro de la compañía, no solo en relación con las acciones desarrolladas tras un incidente sino también en lo relativo a la preparación y planificación.

Acceda al informe completo en **Aon's 2019 Cyber Security Risk Report**.

[1] IMAA Institute's M&A Statistics

Acerca de Aon
Aon plc (NYSE: AON) es una empresa líder en servicios profesionales globales que ofrece un amplio abanico de soluciones de riesgos, capital humano y salud. Nuestros 50.000 empleados en 120 países desarrollan al máximo las posibilidades de nuestros clientes utilizando data & analytics propios que nos permiten ayudar a reducir la volatilidad y mejorar los resultados. Para conocer más visite http://www.aon.es.

Sigue a Aon España en las redes sociales:
www.twitter.com/Aon_Espana / www.facebook.com/aon.espana1 / https://www.linkedin.com/company/aon

Contacto:
Aon /Dirección de Comunicación
91 340 51 41 / 629 66 50 63
dcomunic@aon.es

Empower Results®