Nexia International

Global Cybersecurity

2017

Audalia Nexia

Conclusiones del infome

Las ventajas de estar conectados a Internet también conlleva riesgos que deberán ser gestionados para asegurar que las ventajas económicas y sociales no son transformadas en una desventaja o un potencial desastre.

Las economías, industrias y mercados competitivos globales requieren que estemos cada vez más interconectados unos con otros. Tanto a nivel personal como profesional, estamos llegando a altos niveles profundos de conectividad entre múltiples comunidades y dispositivos a través de portátiles, televisores, termostatos, sistemas de seguridad, electrodomésticos, dispositivos móviles y de música, equipos comerciales, sistemas de administración de edificios y la lista continúa. Este sinfín de conectividad entre dispositivos se conoce como Internet of Things. (IoT).

La iterconexión entre sistemas, clientes, empleados, socios comerciales y diferentes equipamientos reporta beneficios económicos y de seguridad, y son los caminos más impotantes para hacer negocios y ser competitivos en la actualidad. En las palabras de John Chambers, anterior CEO de Cisco, "...viviendo en un mundo donde todo está conectado, y las posibilidades que crea son infinitas, la industria se encuentra al principicio de una explosion de IoT – productos y servicios relacionados llegando al Mercado."

La creciente interconectividad de los sistemas personales, de infraestructura y comerciales, y un mercado creciente y cada vez más abierto a datos robados son solo algunas de las razones por las cuales está creciendo a un ritmo exponencial el panorama de ciberriesgo y el número de empresas e individuos vulnerables a los ataques.

La ciberseguridad es un gran negocio. Por ejemplo, hace solo unos años, el concepto y el riesgo percibido de un ataque de rescate era bastante raro y remoto; sin embargo, de acuerdo con el Informe Anual de Ciberseguridad de Cisco 2017, el ransomware está creciendo a una tasa anual del 350%.

Esta interconexión establece una especie de cadena de suministro cibernético que conecta nuestros dispositivos corporativos y domésticos con otros innumerables elementos . Simplemente considere por un momento cuántas conexiones individuales, corporativas, sociales o de compras en Internet que tiene sólo usted. ¿Tiene conectado su termostato, sistema de iluminación, sistema de seguridad, la puerta de garaje o su nevera? Ahora imagine cuántos sistemas están conectados en un negocio, centro comercial, instalación deportiva u hospital.

La evidencia nos muestra que las organizaciones como bancos, agencias gubernamentales, instituciones de salud y grandes corporaciones, mantienen datos de gran valor y tienen más probabilidades de ser atacadas con

más frecuencia que la mayoría. La realidad es que ninguna industria, emplazamiento, organización o individuo está seguro. Como dice Chamber's, "hay dos tipos de empresas: las que han sido pirateadas y las que aún no saben que han sido pirateadas". Si bien no podemos confirmar o negar esta afirmación pero sabemos con certeza que la piratería y las violaciones de datos están aumentando en frecuencia e impacto.

Esta tendencia abarca a todas las industrias y empresas de diferentes tamaños, e incluso ahora las organizaciones consideradas de bajo riesgo para una violación de datos se encuentran víctimas de ransomware o campañas de phishing. Los ataques se están llevando a cabo a gran escala por una gran cantidad de actores como hacktivistas, crimen organizado, estados nacionales y/o aficionados.

Algunos ataques recientes incluyen el ransomware "Wannacry" del 12 de mayo de 2017. Enviado a través de un correo electrónico de phishing, este ataque se extendió por todo el mundo en cuestión de horas, llevado a cabo por usuarios desatentos y causando daños a sistemas con insuficientes parches.

El ataque ransomware Petya del 27 de junio de 2017 fue otro gran ataque que paralizó empresas, aeropuertos, bancos y departamentos gubernamentales en todo el mundo. Las razones para atacar son tan variadas como la cantidad de perpetradores y, a veces, la motivación es simplemente "solo porque podemos". También hay ataques deliberados preparados por organizaciones sofisticadas que están diseñadas para encontrar maneras de infiltrarse en una organización.

Dado el impacto económico y las posibles consecuencias de los ciberataques, la falta de atención e inversión en ciberseguridad es un área que merece considerable atención. Según el Ponemon Institute, el coste promedio de una violación de datos es de $3.62 millones de dólares, lo que equivale a un promedio de $141 USD por pérdida o robo de registro. Estos son simplemente los costes directos (es decir, abogados, notificaciones, consultores, etc.) y no reflejan la falta de confianza del consumidor que pueda surgir de este ataque. Cuando se atacan a grandes corporaciones que cotizan en bolsa, es probable que su precio de las acciones se vea afectado. Estas grandes corporaciones, cuentan con los suficientes recursos que las permita recurperarse pero las pequeñas o medianas organizaciones puede que no tenga tanta fortuna.

Nexia International realizó una encuesta global para evaluar el estado actual de la preparación cibernética. Uno de los objetivos principales de la encuesta es proporcionar información sobre qué opinan las organizaciones sobre el riesgo cibernético y lo que están haciendo al respecto, y cómo las organizaciones proporcionan a la administración ejecutiva los datos que necesitan para evitar o al menos mitigar un evento de seguridad.

Nuestro análisis de las respuestas a la encuesta indica que todavía se requiere una considerable educación e inversión para reducir el nivel de riesgo cibernético y mejorar la preparación y la capacidad de respuesta de las organizaciones en la mayoría de las industrias y geografías. También parece haber una gran necesidad de que muchas organizaciones mejoren su comprehensión general del panorama de riesgo de ciberseguridad.

> "Hay dos tipos de empresas: las que han sido pirateadas y las que aún no saben que han sido pirateadas"
>
> John Chambers, Ex-CEO de Cisco

Observaciones Clave

- Solo el 39% de los encuestados considera que la ciberseguridad es una prioridad.
- El 46% de los encuestados en América y el 50% de los encuestados de la región EMEA no tienen un programa de ciberseguridad. El 76% de los encuestados de la region APAC indicaron que tienen un programa de ciberseguridad.
- El 50% de los encuestados indicó que los hacktivistas, el crimen organizado y los empleados, tanto actuales como antiguos, son las fuentes de mayor ciberriesgo.
- El 20% de los encuestados no ha efectuado una evaluación de ciberseguridad, y solo el 25% de los encuestados ofrece formación a los empleados en seguridad cibernética al menos una vez al año.
- El 20% de los encuestados afirman que deberían tener un programa de seguridad cibernética basado en los requisitos del gobierno, la industria o los clientes y que actualmente no cuentan con él.
- El tiempo y presupuesto limitado junto con la falta de personal cualificado fueron las razones clave que se citaron para no tener un programa de ciberseguridad eficiente.
- Las organizaciones que tienen un programa de seguridad cibernética informaron haber experimentado más ataques que aquellas que no cuentan con este programa. Sin embargo, hay que señalar que las organizaciones que cuentan con este tipo de programas de seguridad tienen más probabilidades de identificar una violación y no se puede cuantificar la cantidad de violaciones no detectadas.

2017 Cost of a Data Breach Study – Global Overview. Benchmark research sponsored by IBM Security and independently conducted by Ponemon Institute LLC, June 2017.

- La mayoría de los encuestados indicó una que la inversión con la cuentan es insuficiente a la hora de afrontar iniciativas de seguridad cibernética avanzada, así como la implantación de planes de respuesta sólida a incidencias de seguridad para identificar, detectar y manejar las vulneraciones de seguridad incluyendo las violaciones de datos.

Todo esto, junto con el resto de los datos y respuestas de la encuesta, resalta una falta general de concienciación sobre la necesidad de contar con un programa integral de ciberseguridad. Si las crecientes amenazas cibernéticas y el aumento de las multas no son suficientes para que las empresas reconsideren sus programas cibernéticos, existen nuevas normativas que pueden proporcionar el ímpetu necesario.

Quizás la más restrictiva y vinculante de estas normativas es el Reglamento General de Protección de Datos de la UE (RGPD), que entrará en vigor en mayo de 2018. Esta norma impone criterios muy específicos para las organizaciones que poseen datos personales de ciudadanos de la UE. Dichos requisitos incluyen el nombramiento de un responsable de protección de datos, el cifrado de datos, la adhesión a estrictos estándares de privacidad y mucho más. Las multas en caso de incumplimiento y falta demostrada de cumplimiento podrían generar 20 millones de euros o el 4% de los ingresos corporativos del año anterior, cualquiera que sea mayor.

Estados Unidos ha visto un resurgimiento de las necesidades cibernéticas. Desde 2014, la Comisión de Bolsa y Valores ha estado indicando que la ciberseguridad es una de sus principales preocupaciones y ha llevado a cabo varias "busquedas" en el mercado financiero. Del mismo modo, el Departamento de Salud y Servicios Humanos ha realizado visitas a las entidades sanitarias para evaluar el cumplimiento de las normas de protección de datos y ha aumentado el número de investigaciones sobre si las organizaciones cumplen con los requisitos.

Si hay algo de positivo en todo esto, la mayoría de los expertos en seguridad dicen que todo se reduce a algunos controles básicos y que la mayoría de las infracciones son prevenibles. Es conocido que las contraseñas débiles, la mala gestión de filtros y vulnerabilidades, y la falta de concienciación por parte del usuario explican una gran cantidad de las incidencias de seguridad que aparecen en las noticias. Independientemente de las sofisticadas herramientas que las empresas utilizan para prevenir y detectar el pirateo informático, aún se requieren profesionales de la seguridad con una formación y management adecuados.

Si desea conocer el informe completo, puede acceder haciendo **click aquí.**

Global Cybersecurity Report 2017

Informe global sobre ciberseguridad 2017

Audalia Nexia

Closer to you

www.audalianexia.com

Audalia Nexia es miembro de la red independiente Nexia International

España, Dic. 2017