CYBERSECURITY
by itwarelatam.com

Edición - Nº 11

La revista de Cloud Security

NOTA DE TAPA

Comprar online seguro

INFORME ESPECIAL

Ciberseguridad en la industria financiera

MÁS TEMAS

Especial: Ekoparty 2021

Riesgos en apps de celulares

Desafíos a la seguridad de Big Data

EDICIÓN N°11

NOTA DE TAPA

COMERCIO ELECTRÓNICO COMPRAR ONLINE SEGURO

06

SUMARIO

INFORME ESPECIAL

18 Ciberseguridad en la industria financiera: Tendencias y desafíos de cara a 2022

INFORME ESPECIAL

26 Ciberataques al sector financiero: ¿Cómo anticiparse?

EKOPARTY 2021

32 criptomonedas, electricidad y otras vicisitudes

SECURITY ARCHITECTURE

38 Desafíos a la seguridad de Big Data

NOTA PATROCINADA

39 Caso de éxito: Noanet concientiza a su equipo en ciberseguridad

RISK ASSESSMENT

42 Riesgos de seguridad en aplicaciones para Celulares

SECURITY OPERATION

44 Lo que le pasó a Facebook

SECURITY OPERATION

46 Ataques DDOs a Bancos

FRAMEWORK AND STANDARDS

48 Reglamento de Ciberseguridad

CAREER DEVELOPMENT

50 La iniciativa española #LadyHacker

Comercio electrónico y seguridad digital

Todavía en pandemia, más liviana, con menos restricciones, pero aún no ha terminado. Eso no implica que no hayamos seguido trabajando. Precisamente una de las consecuencias de la pandemia y, especialmente, de las restricciones a las salidas, fue el incremento notable del comercio electrónico.

La necesidad de comprar online hizo que la transacción electrónica se popularizara, por lo menos en cierto estamento social. Y esa popularización, como siempre ha sucedido, conspira contra la seguridad informática. De ahí que dedicáramos este número, precisamente, a la ciberseguridad en el comercio electrónico. Si bien no logramos conseguir la palabra de los referentes más importantes del comercio electrónico, por lo menos en la Argentina, hemos podido conseguir opiniones relevantes de parte de algunos de los miembros de la cadena de transacciones que se forma cuando un consumidor elige comprar en línea un producto.

Consecuentemente con esto, el informe especial de este número está dedicado a las fintech, este nuevo tipo de negocios financieros exclusivamente digital. Además de los cambios de comportamiento de consumo a partir de la pandemia, el sector financiero enfrenta constantemente desafíos de riesgo cibernético: cómo mantener protegidos los datos personales y la información sensible de cientos de miles de usuarios, clientes y consumidores que confían en él para realizar sus transacciones cotidianas.

Además, en noviembre se llevó a cabo Ekoparty 2021, el mayor evento de seguridad informática y hacking que se realiza en la Argentina y tenemos un reporte especial de nuestro corresponsal en el evento.

Y, por supuesto, más notas de las que a usted le importan, como los desafíos a la seguridad en Big Data, seguridad en aplicaciones para celulares y ataques DDOs a bancos, entre otras.

Hasta la próxima.

itseller enfasys ITWARE LATAM.COM

Buenos Aires - Av. Jujuy 2073, 2ºB, Distrito Tecnológico, Buenos Aires, Argentina
Tel.: +5411-4308-6642

Matías Perazzo
Director Editorial
mperazzo@mediaware.org

Ricardo Goldberger
Contenidos
rgoldberger@mediaware.org

Leonardo Devia
Cybersecurity
Consultant - **CSA**

Suscripciones:
info@itwarelatam.com

Para publicar en este medio:
ventas@mediaware.org
www.itwarelatam.com

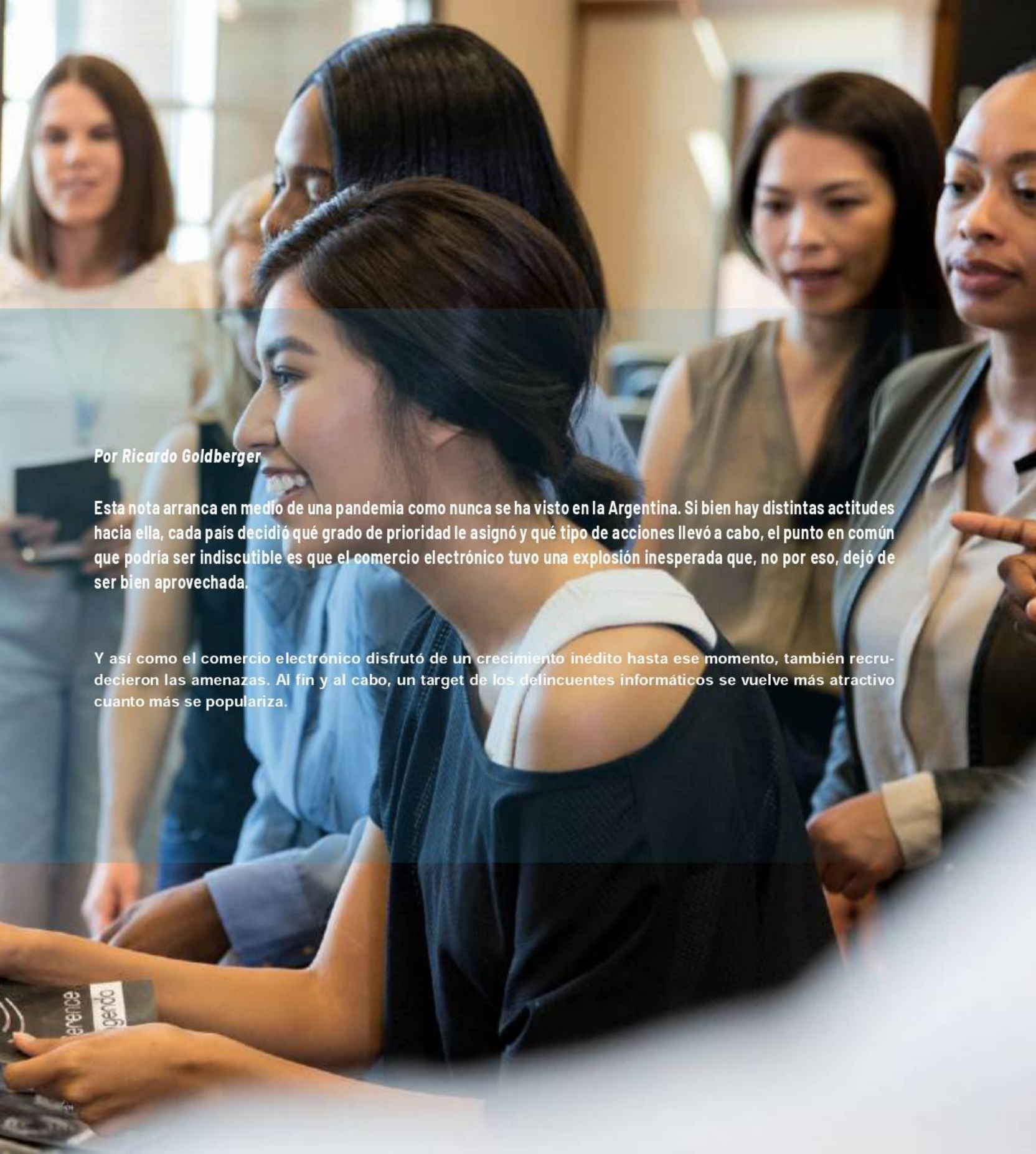
Consultar por suscripción anual

Puede leer y descargar la versión digital de esta revista en www.itwarelatam.com.com

Edita, diseña, comercializa y distribuye Mediaware Marketing

mediaware MARKETING

Comprar online seguro



Por Ricardo Goldberger

Esta nota arranca en medio de una pandemia como nunca se ha visto en la Argentina. Si bien hay distintas actitudes hacia ella, cada país decidió qué grado de prioridad le asignó y qué tipo de acciones llevó a cabo, el punto en común que podría ser indiscutible es que el comercio electrónico tuvo una explosión inesperada que, no por eso, dejó de ser bien aprovechada.

Y así como el comercio electrónico disfrutó de un crecimiento inédito hasta ese momento, también recrudecieron las amenazas. Al fin y al cabo, un target de los delincuentes informáticos se vuelve más atractivo cuanto más se populariza.

Algunos resultados

Según el estudio de medio término de la CACE (Cámara Argentina de Comercio Electrónico), realizado por la consultora Kantar, durante el primer semestre de 2021 se registró una facturación de 631.788 millones de pesos, lo que representa un crecimiento del 101% en comparación a MID 2020. En distintas unidades también se registró un incremento importante:

- 47% más de órdenes de compra generadas en MID 2020
- El ticket promedio aumentó un 53% más que en MID 2020
- Se vendió un 31% más de productos que en MID 2020

Entre otros resultados, continúa creciendo el ecommerce propio en el rubro electrónica (77%), mientras que en la categoría de alimentos y bebidas se incrementa el uso de Marketplace (16%), principalmente por la gran oferta que incorporó en el último año el líder del canal. Además, el 77% del tráfico se verificó a través de dispositivos móviles, típicamente celulares.

Rapyd, Fintech-as-a-Service (FaaS) global y unicornio israelí, realizó un estudio en agosto de 2021 en México, Colombia, Argentina y Brasil, para analizar qué tan abiertos estamos en Latinoamérica a acoger el canal del social commerce.

Un 63% de los brasileños encuestados dijo ya haber hecho compras por redes

Edgardo Bertazzoni - Geopagos

sociales (IG/FB), no muy lejos están los mexicanos con un 57%, y colombianos con un 54%. Los argentinos fueron los que se mostraron más reticentes a este nuevo canal con sólo el 38% de los encuestados respondiendo afirmativamente.

Para las compras por redes sociales, tanto en Colombia (61%) como en México (54%), el método de pago más utilizado es la transferencia bancaria, mientras que en Brasil predomina la tarjeta de crédito con un 67%. En Argentina el podio lo comparten la transferencia bancaria y el pago en efectivo en tiendas de conveniencia; ambas opciones con un 41%. En segundo lugar, en Brasil (46%), México (51%) y Colombia (41%) queda PayPal, mientras que para los argentinos (35%) es la tarjeta de débito.

La mayor preocupación de comprar online para México (67%), Colombia (66%) y Argentina (59%) es que el comerciante sea un estafador, mientras que para los brasileños (62%) es que sus datos no estén seguros. Para Argentina (58%), México y Colombia (ambos 53%), la seguridad de los datos rankea en segundo lugar.

Pero en cuanto al pago seguro: un 52% de los encuestados mexicanos, 49% de los brasileros, 46% de los colombianos y el 45% de los argentinos destacaron la preocupación por la seguridad de los pagos. Esto realza no sólo la importancia de la diversidad de opciones de pagos sino también seguridad para un social commerce exitoso.

Que casi la mitad de la población que usa las redes sociales para hacer compras esté preocupada por la seguridad de sus transacciones comerciales, significa que más de la mitad no lo está.

Lo que implica que todavía hay un largo camino a recorrer en cuanto a la difusión y capacitación del consumidor online.

Lamentablemente, varios de los referentes más importantes del comercio electrónico, por lo menos en la Argentina, declinaron responder. Sin embargo, hemos podido conseguir opiniones relevantes de parte de algunos de los miembros de la cadena de transacciones que se forma cuando un consumidor elige comprar en línea un producto en algún marketplace, seleccionarlo, ingresar sus datos demográficos y financieros, validarlos por medio de alguna organización, devolver la respuesta al marketplace para que éste, finalmente, libere y envíe (si es el caso) el producto comprado.

Como se puede apreciar, los puntos de ataque de los delincuentes informáticos son varios, variables y sujetos a distintas modalidades de protección y prevención, cuando no de remediación.

> La mayor preocupación de comprar online para México (67%), Colombia (66%) y Argentina (59%) es que el comerciante sea un estafador, mientras que para los brasileños (62%) es que sus datos no estén seguros.

Lo que más preocupa

Comenzamos preguntando cuáles deberían ser, a su criterio, las principales preocupaciones del responsable de la seguridad en el comercio electrónico. He aquí las primeras respuestas.

Edgardo Bertazzoni, Information Security Manager de Geopagos, respondió: "La aceleración de la digitalización de la economía que atravesamos desde el inicio de la crisis del Covid-19 no tiene precedentes, y si bien la tecnología demostró estar a la altura de las circunstancias, el crecimiento de este mercado lleva consigo grandes desafíos. A partir de Covid-19 se vió un incremento en su adopción nunca antes visto para la industria.

"Algunas empresas, ya contaban con preparación para volcarse al comercio electrónico, otros estaban en medio de preparativos y otros, tuvieron que hacerlo de forma abrupta, en algunos casos, como la única opción de continuidad para su negocio, incluso pequeños emprendimientos personales, como única opción de supervivencia.

"Este escenario que requirió una rápida adopción de los canales digitales por parte de usuarios sin una experiencia previa y sin conciencia de seguridad, y por parte de empresas, en algunos casos con controles insuficientes, fue propicio para el aumento del riesgo y materialización de estafas.

"Dicho esto, la principal preocupación de los responsables de seguridad de información es asegurar que las metas del negocio y la seguridad de información se encuentren correctamente alineadas y gestionadas. Esto quiere decir, que se deben tratar de manera oportuna y mantener a un nivel de riesgo aceptable, en base al apetito de riesgo definido."

Sebastián Wilke, Cyber Security Leader de Bco Galicia, por su parte, contestó: "Las principales preocupaciones de un profesional de ciberseguridad dentro del comercio electrónico abarcan desde seguridad lógica y disponibilidad adecuada en las infraestructuras que soportan las

Sebastian Wilke - Bco. Galicia

aplicaciones de ecommerce, pasando por identificaciones de los clientes hasta las transacciones que se realizan en el mismo.

"Mantener controles de seguridad sobre la capa de aplicación también debería ser un foco de atención primario, en donde es necesario poder detectar y evitar cualquier situación que haga que nuestra aplicación de ecommerce funcione de una manera no deseada. Utilizar soluciones de web application firewall para prevenir ataques sobre la aplicación y, servicios de consultoría de pentesting para verificar el funcionamiento de la plataforma, y de esta manera encontrar punto de falla que pueden ser explotados.

"Los procesos de autenticación y validación de usuarios de la plataforma ecommerce, en donde es necesario poder asegurar que cualquier manipulación de datos que se intente realizar sea detectada y descartada en el momento para evitar cualquier tipo de suplantación de identidad de los usuarios. Lo mismo aplica para

los procesos de recuperación de contraseña de los usuarios de la plataforma."

A su vez, **Victor Borga** Regional Sales Manager, Latinoamérica en Auth0, manifestó que "en la toma de decisiones, la privacidad de los datos debe estar siempre en el medio. Sin embargo, es importante que también pueda aprender del comportamiento del cliente. Estar dispuesto a probar nuevas tecnologías que mejoren la experiencia del usuario y superen sus expectativas, puede ser la solución para mejorar las tasas de conversión.

Victor Borga - Auth0

"Según nuestra reciente encuesta global de Gestión de Identidad y Acceso al Cliente (CIAM, por sus siglas en inglés), el 84% de los argentinos abandonan los carritos de compras online cuando el proceso de inicio de sesión es demasiado complicado.

"El Software como Servicio (SaaS, por sus siglas en Inglés) le da al equipo de seguridad la capacidad de experimentar y realizar cambios menores en sus sitios rápidamente, optimizando enormemente la experiencia de inicio de sesión."

> "La principal preocupación de los responsables de seguridad de información es asegurar que las metas del negocio y la seguridad de información se encuentren correctamente alineadas y gestionadas."

Dean Coclin, director senior de desarrollo empresarial en DigiCert, sostuvo: "Sin duda, el responsable de la seguridad en el comercio electrónico debe tener en cuenta las nuevas estafas creadas por los ciberdelincuentes, dado el aumento de compras online que ha provocado la pandemia y las fiestas de fin de año.

"Según el último estudio anual de comercio electrónico realizado por la CACE (Cámara Argentina de Comercio Electrónico), el 92% de las ventas totales se realizaron a través de tarjeta de crédito. Por lo tanto, es importante que tanto los vendedores como los compradores estén atentos para evitar el fraude y ayudar a que el comercio electrónico siga creciendo.

"Los equipos de TI de la región informaron que el phishing aumentó en México en un 61%; en Colombia 66%; y 69% en Chile. En este contexto, es importante que los gerentes de comercio electrónico comprendan cómo proteger los sitios web de las estafas, ahora y en el futuro."

Dean Coclin - Digicert

Las principales amenazas

Si bien los voceros coinciden en unos cuantos puntos, cada uno de ellos tiene una mirada diferente, de acuerdo a qué lugar en la cadena de pagos se encuentra.

Auth0, por ejemplo, es uno de los principales agregadores de datos de identidad y de inicio de sesión, como para tener la capacidad de ver tendencias masivas. "En la actualidad —dice Borga—, aproximadamente el 67% de nuestro tráfico de autenticación se considera sospechoso, es decir que se trata de intentos de fraude".

El registro fraudulento y lo que llaman Account Takeover (ATO) es lo más frecuente. El primero involucra a un actor de amenazas que crea cuentas de títeres. El segundo es cuando un atacante obtiene acceso a la cuenta de un usuario existente.

"El uso de credenciales robadas —continúa Borga— es uno de los métodos más comunes utilizados en las filtraciones de datos observadas. El relleno de credenciales es cuando los atacantes toman credenciales digitales robadas y las prueban en masa con otros sitios web para encontrar combinaciones que están siendo reutilizadas para poder tomar control de las cuentas de los usuarios. Los atacantes hacen esto de forma automatizada, de modo que puedan probar miles de credenciales a lo largo del tiempo. Realmente es un juego de números. Si el 0,01% de una lista masiva de credenciales se reutiliza en un segundo sitio web, aún podrían estar robando una cantidad significativa de cuentas.

"Por lo tanto, las empresas digitales ya no pueden sorprenderse de que las organizaciones sigan siendo hackeadas. A medida que aumentan los ataques relacionados con las identidades digitales, las organizaciones deben intensificar y priorizar la educación en ciberseguridad, así como invertir en soluciones de seguridad integradas, incluida la autenticación multifactor, que disminuye el riesgo de ataques relacionados con las credenciales en el futuro al proteger la identidad."

Wilke coincide con Borga, pero plantea otra metodología: "Una de las principales amenazas tiene que ver con la usurpación de identidades y los métodos que suelen utilizarse para hacerse de una identidad. El más utilizado para estos fines es el phishing, en donde se acude mucho al desconocimiento de los usuarios. A través de links en correos electrónicos se los redirige a páginas o sitios que simulan ser auténticos, pero en realidad son sitios apócrifos en los que se piden credenciales de acceso. Una vez entregadas las credenciales, la identidad del usuario será utilizada por los perpetradores en los sitios auténticos de ecommerce. Si, además, tenemos en cuenta que muchos sitios de ecommerce permiten dejar almacenados en los perfiles de usuario, sus medios de pago, un simple ataque de phishing podría permitir usurpar identidad y realizar compras en un solo paso."

Más allá del fraude y del robo de información, en lo que todos coinciden, Bertazzoni agrega dos más:

"Denegación de servicio: En el e-commerce, la denegación de servicio se traduce directamente en un impacto económico. Por esto, es importante contar con protecciones que mitiguen ataques de denegación de servicio, incluyendo los distribuidos los que, sin herramientas específicas, son muy complejos de mitigar. Suelen ser protecciones con un alto costo, pero el negocio que se desea proteger, lo vale.

"Baja concientización: Tanto los colaboradores internos, como los terceros, los clientes y los usuarios finales, deben ser conscientes de los cuidados que se deben tener para proteger la información personal y financiera que utilizan, ya sea propia o de otras personas/empresas. Ser conscientes al momento de abrir o seguir el link de un correo que podría ser phishing solicitando información de acceso o datos de tarjeta, llamados telefónicos ofreciendo servicios y solicitando datos, la manera en que almacenan sus claves de acceso, las buenas prácticas de desarrollo de aplicaciones basadas en estándares de industria, así como los requerimientos legales y normativos."

> "Una de las principales amenazas tiene que ver con la usurpación de identidades y los métodos que suelen utilizarse para hacerse de una identidad. El más utilizado para estos fines es el phishing, en donde se acude mucho al desconocimiento de los usuarios."

Cybermonday, Black Friday, Hot Sale y otras yerbas

Se consultó a los expertos si estos días especiales requieren medidas especiales, y esto nos respondieron.

Borga enfatiza: "El cuadro de inicio de sesión, es donde se encuentran la experiencia del cliente, la seguridad y la privacidad. Por lo tanto, es fundamental que los comercios coloquen la identidad digital en el centro de su estrategia a medida que nos adentramos en la época de compras navideñas. Nuestra investigación muestra que los comercios tienen una gran oportunidad de aumentar las conversiones y retornos sólo prestando atención a las experiencias de identidad que desean sus clientes. Un cuadro de inicio de sesión seguro y simple podría ser el factor diferencial de una marca esta temporada."

"En estos días especiales —responde Wilke— hay varios temas a los cuales debemos prestar atención; entre los principales está la disponibilidad de la plataforma porque son fechas con muchísima demanda. En estas ocasiones, es muy importante estar atentos a si tenemos demasiadas peticiones desde la misma dirección IP o geolocalización en períodos de tiempo muy cortos y, tomar medidas al respecto a través de dispositivos de seguridad perimetral.
"Exigir un mayor control en las validaciones de usuario, para asegurarse que el usuario que está en la sesión es realmente quien dice ser; si bien puede ser un punto de rispidez con el usuario, la utilización de un segundo factor de autenticación, o de un captcha, puede evitar que se realicen transacciones sobre identidades usurpadas.

"Finalmente, contar con mecanismos que nos permitan detectar de la forma más proactiva posible, perfiles falsos en redes sociales y sitios de phishing. Se aprovechan estas fechas para lanzar campañas masivas de promociones para sitios de ecommerce, tanto de sitios auténticos como de phishing, y muchos usuarios todavía no están entrenados para distinguir una campaña real de una fraudulenta".

"En empresas que tal vez, no tienen implementados controles de prevención de fraude, o mitigaciones para ataques de fuerza bruta, DDOS, es recomendable aumentar el nivel de monitoreo e implementar de manera oportuna estas protecciones. Incluir en la campaña de concientización anual el aumento de riesgos de fraude en estas fechas, para minimizar efectos de técnicas de ingeniería social, que también vemos incrementado en estas fechas." aseguró Bertazzoni.

¿Será el tiempo del dinero virtual?

Coclin es confiado: "Las criptomonedas han atraído mucha atención en los últimos años, ya que los consumidores, especialmente en los mercados emergentes, buscan encontrar una moneda que pueda ser más estable que la de su país de origen. Sin embargo, existen muchos riesgos asociados con las criptomonedas que deben tenerse en cuenta. Por ejemplo, las fluctuaciones en el valor pueden causar más ansiedad que la moneda del mercado local del consumidor. Además, los usuarios de criptomonedas deben usar una billetera digital en la que confíen y deben mantener segura la contraseña de su clave privada, al mismo tiempo que la guardan en un lugar seguro. Si se olvida la contraseña, se perderá el valor de la criptomoneda. No obstante, esperamos que las criptomonedas continúen desempeñando un papel en el futuro del comercio electrónico."

Borga, en cambio, previene: "Las criptomonedas siguen siendo extremadamente volátiles. Aún no son lo suficientemente estables como para ser una unidad de cuenta. Pueden contener valor, pero el valor fluctuará drásticamente. En el transcurso de minutos que le dediqué a esta respuesta, mi billetera de cripto podría haber bajado un 10%, pero volverá a subir en un par de horas más. Además, la falta de regulaciones hace que sea casi imposible de predecir, lo cual es difícil para las empresas."

Para Wilke, en cambio, es un "sí, pero...": "Sí. Todo dependerá de qué manera se adopten para realizar los pagos. En algunos casos hoy existen tarjetas de crédito prepagas en las que se puede cargar saldo con crypto, pero en realidad lo que se está haciendo es vendiendo la crypto en pesos


Crédito: jannoon028 en Freepik

> Las criptomonedas han atraído mucha atención en los últimos años, ya que los consumidores, especialmente en los mercados emergentes, buscan encontrar una moneda que pueda ser más estable que la de su país de origen.

y se carga ese saldo en pesos para ser consumido por la compra con TC.

"Luego, si se adopta directamente una crypto o una blockchain en donde se realicen los pagos y directamente la transferencia vaya a una dirección de la blockchain adoptada perteneciente al ecommerce, se deberá tener en cuenta cómo esa blockchain calcula las comisiones de transferencias (gas fee) y en qué tiempos queda confirmada esa transacción dentro de la blockchain. Es decir, en parte estas dos variables, comisiones y tiempos de confirmación serán determinantes a la hora de elegir una blockchain/crypto moneda en un ecommerce."

Bertazzoni, por su parte, es optimista: "Sí, definitivamente. Con el auge de las billeteras virtuales y el interés en los cripto activos, es inevitable que el mundo del dinero fiat y el basado en criptos comiencen a interactuar entre sí. En varios países algunas de las principales marcas de tarjetas, ya ofrecen tarjetas de crédito para realizar pagos con bitcoins. Su adopción global, dependerá de la adecuación de las leyes y normativas locales de cada gobierno, en definitiva, de los controles que puedan implementarse para asegurar el origen y destino de los fondos, así como el gravamen de impuestos."

En síntesis, el ecommerce es un ejemplo de lo que hay que tener en cuenta para llevar a cabo transacciones de manera segura. Por supuesto que hay amenazas, por supuesto que ningún método o procedimiento es infalible o invulnerable, por supuesto que hay circunstancias en las cuales el cuidado y la prevención deben incrementarse. Aún así, el comercio electrónico no sólo llegó para quedarse —ya hace tiempo, dicho sea de paso— sino que presenta signos y señales de que, en un futuro no muy lejano, será un método de adquisición predominante lo que, por supuesto, va a implicar mayor atención en la ciberseguridad.

Blockchain puede revolucionar el comercio electrónico

A medida que la tecnología blockchain se va convirtiendo en una fuerza impulsora de la economía mundial, también va ganando adeptos en el segmento del comercio electrónico. Se encuentra entre los sectores que utilizan cada vez más las tecnologías blockchain para facilitar las transacciones financieras.

La tecnología de contabilidad distribuida que se utiliza en las cadenas de bloques es actualmente fundamental para resolver los retos a los que se enfrenta el sector del comercio electrónico. Hay mucho que esperar de las cadenas de bloques en cuanto a su aplicabilidad en el comercio electrónico.

Blockchain en el comercio electrónico

Blockchain hace que las transacciones sean más seguras y rápidas, en la medida en que las actividades de comercio electrónico dependen de ellas. La tecnología blockchain permite a los usuarios compartir y almacenar de forma segura activos digitales tanto de forma automática como manual. Esta tecnología tiene la capacidad de gestionar actividades de los usuarios como el procesamiento de pagos, la búsqueda de productos, la compra de productos y la atención al cliente.

Las tecnologías blockchain más utilizadas en el mercado del comercio electrónico son Ethereum y Bitcoin. Bitcoin, una criptomoneda, llevó a la creación de la tecnología blockchain. Los consumidores la utilizan para realizar compras en determinadas tiendas online que aceptan Bitcoin como forma de pago. Ethereum, por su parte, proporciona una plataforma práctica para los sitios web de comercio electrónico que quieren gestionar sus propias cadenas de bloques.

Ventajas de Blockchain en el comercio electrónico

Lo interesante de la tecnología blockchain en el comercio electrónico es que es beneficiosa tanto para los minoristas como para los compradores. Ofrece soluciones convenientes a las amenazas cibernéticas y a las preocupaciones de seguridad financiera. Además, reduce los gastos de gestión de inventario y de procesamiento de pagos.

Reducción de costos

Con blockchain, las empresas de comercio electrónico pueden combinar cómodamente la gestión del inventario, el procesamiento de los pagos, las descripciones de los productos y las imágenes con otras actividades comerciales. A cambio, consiguen gastar menos en el mantenimiento de los sistemas que facilitan estas actividades o en la contratación de personal de apoyo informático para mantener los sistemas. Las criptomonedas, como el Bitcoin, reducen las comisiones que las instituciones bancarias cobran por facilitar las transacciones.

> “La tecnología blockchain tiene la capacidad de gestionar actividades de los usuarios como el procesamiento de pagos, la búsqueda de productos, la compra de productos y la atención al cliente.”

Crédito: Worldspectrum en Pexels

Amenazas cibernéticas

La mayoría de los minoristas en línea experimentan dificultades al tratar de mantenerse al día con su competencia y las crecientes expectativas de los clientes. Además de estos retos, también corren el riesgo de perder los datos de los clientes y millones de dinero en efectivo debido a los ciberataques. La tecnología Blockchain es perfecta para resolver estos retos a los que se enfrentan los minoristas online. La tecnología ofrece el más alto nivel de seguridad en forma de libros de contabilidad distribuidos para los sistemas de gestión de bases de datos de comercio electrónico.

Transacciones rápidas

Gracias a las tecnologías de cadena de bloques, como Waves, los clientes de los sitios de comercio electrónico pueden realizar pagos rápidos en línea. A diferencia del pasado, cuando los compradores solían esperar varias horas o días para realizar los pagos, las cadenas de bloques les ofrecen la comodidad que necesitan cuando compran en línea. En este caso, pueden hacer que sus productos sean enviados después de realizar los pagos requeridos.

Impulso al comercio en países del tercer mundo

Es sorprendente cómo las tecnologías de cadena de bloques están ofreciendo a los países del tercer mundo la oportunidad de comerciar en línea. A través del sistema peer-to-peer de Bitcoin, los consumidores de estos países no necesitan un intermediario para procesar sus solicitudes de pago. Además, estas tecnologías están abriendo las puertas a los minoristas en línea para

aprovechar los mercados de consumo de los países en desarrollo.

Cómo Blockchain revolucionará el comercio electrónico

Las tecnologías Blockchain y los sitios de comercio electrónico están formando un ecosistema económico que es viable tanto para los consumidores como para los minoristas en línea. A medida que estos adoptan rápidamente la tecnología del libro de contabilidad distribuido en sus procesos comerciales, se dan cuenta de nuevas formas de servir a sus clientes. Las cadenas de bloques les ofrecen una forma eficaz de mejorar su experiencia. He aquí otras oportunidades que las tecnologías blockchain crearán en el mercado del comercio electrónico.

Contratos inteligentes

Los smart contracts actúan como programas informáticos capaces de automatizar ciertas tareas basadas en reglas preestablecidas. Dado que las cadenas de bloques son fundamentales para almacenarlas, los contratos inteligentes también pueden automatizar los procesos relacionados con el comercio electrónico. Pueden hacer crecer una empresa de comercio electrónico reduciendo los costes necesarios para contratar personal que realice las tareas que los programas informáticos pueden automatizar. Los contratos inteligentes también pueden facilitar la gestión del inventario. Esto significa que los minoristas en línea pueden gestionar el control de los artículos del inventario.

Facilidad de acceso a recibos y garantías

La tecnología Blockchain también proporciona a los minoristas online y a sus clientes la comodidad de almacenar los recibos y las garantías de los productos. Al realizar compras en línea, uno de los retos a los que se enfrentan los compradores es la pérdida de los recibos en papel. A veces, los compradores también experimentan frustración cuando intentan demostrar la cobertura de la garantía de ciertos productos adquiridos. Gracias a las cadenas de bloques, los compradores y los minoristas podrán acceder a los recibos y a los datos de la garantía y validar la prueba de propiedad fácilmente.

Pagar a los creadores de contenidos

Los creadores de contenidos desempeñan un papel crucial en el desarrollo de los sitios de comercio electrónico, y sus esfuerzos no deberían pasar inadvertidos. Una de las cosas interesantes que la tecnología blockchain tiene reservada para los sitios de comercio electrónico en el futuro, es el pago a los creadores de contenidos. Esto significa que los curadores de contenidos ganarán tokens digitales cada vez que

creen y publiquen contenidos atractivos en estos sitios por cortesía de las cadenas de bloques. Los minoristas en línea utilizarán carteras digitales para pagarles. Los monederos digitales admiten criptomonedas como el Bitcoin y permiten a los usuarios convertir los tokens digitales en sus monedas preferidas.

Programas de fidelización y ofertas personales

Cuando los minoristas online adoptan las tecnologías blockchain en sus procesos de negocio, pueden emitir fácilmente puntos de recompensa canjeables a sus clientes cada vez que alcanzan ciertos umbrales de gasto. Los minoristas en línea también pueden hacer que estos puntos de recompensa sean canjeables en diferentes sitios de comercio electrónico. Los clientes también pueden beneficiarse de ofertas y descuentos personalizados que los minoristas ofrecen gracias a la tecnología blockchain. Las empresas de comercio electrónico pueden utilizar estos programas de fidelización para atraer a más clientes y ampliar el alcance de sus productos.

Control de la cadena de suministro

Con una cadena de suministro confiable, las tiendas en línea pueden alcanzar sus objetivos comerciales deseados. Esto se debe a que las cadenas de suministro permiten a los operadores de las tiendas conocer las existencias que están en proceso y cuándo deberían llegar. Las cadenas de suministro también ayudan a los operadores de las tiendas a verificar el tipo de productos que les suministran los proveedores. Cuando estos operadores utilizan blockchain para supervisar la cadena de suministro, pueden evitar que los proveedores sustituyan determinados productos y fomentar la transparencia en todo el proceso.

Generación de reseñas genuinas

Los operadores de tiendas online pueden confiar en la tecnología blockchain para verificar las reseñas sobre sus productos o servicios. Cada vez hay más dudas sobre la legitimidad de la mayoría de las reseñas de productos y servicios que se encuentran en Internet. La reputación de una empresa depende de la legitimidad de sus reseñas, de ahí la necesidad de que los sitios de comercio electrónico utilicen la tecnología blockchain en el futuro.

Comerciantes de diferentes partes del mundo están recurriendo al comercio electrónico como vidriera para sus negocios. Las cadenas de bloques están actuando como la columna vertebral de las ventas y los pagos en línea. Además de ser más rápidas y baratas, las cadenas de bloques facilitan todas las actividades que permiten los sistemas de comercio actuales. Como el futuro es inminente, sólo podemos democratizar la economía haciendo que las finanzas y el comercio sean más transparentes.

> “Las tecnologías Blockchain y los sitios de comercio electrónico están formando un ecosistema económico que es viable tanto para los consumidores como para los minoristas en línea.”

La tecnología blockchain busca capturar el poder de las instituciones financieras para permitir que las personas tengan el control de sus transacciones.

Fuente: Sergii Shanin en eTeam (https://www.eteam.io/blog/blockchain-and-ecommerce).

El Top 5 de Amenazas en eCommerce

Las amenazas a la seguridad en el comercio electrónico van en aumento debido al rápido y constante crecimiento del sector: en 2021, se prevé que las ventas mundiales de comercio electrónico alcancen los 4,9 billones de dólares.

Teniendo en cuenta que el 33% de los clientes dejaría de comprar en un comercio minorista vulnerado durante al menos tres meses (el 19% lo dejaría definitivamente), hay mucho en juego.

Para ayudarle a evitar problemas de seguridad, echemos un vistazo a las cinco principales ciberamenazas para el comercio electrónico a las que debe prestar atención en 2021.

Bots malos: Más en número y sofisticación

Según una investigación de Imperva, el tráfico de bots malos aumentó hasta un récord del 24,1% en 2019, en comparación con el 18,6% en 2015. Ahora, casi una de cada cuatro solicitudes web proviene de bots malos y esta cifra está destinada a aumentar aún más.

En los sitios de comercio electrónico específicamente, el tráfico de bots malos fue medido en un 17,7% por el mismo estudio, y el nivel de sofisticación promedio de los bots ha aumentado en un 2,1% de 2018 a 2019.

Los bots malos pueden ser utilizados por los competidores para distorsionar precios para que luego puedan vencerte con precios más bajos, o por los delincuentes para hacerse con las cuentas de los clientes y robar información personal o probar los datos de las tarjetas de crédito robadas.

Para proteger a su empresa de comercio electrónico de los bots malintencionados, debe supervisar los intentos fallidos de inicio de sesión, examinar cuidadosamente las fuentes de tráfico y bloquear determinadas direcciones IP cuando sea necesario.

El robo electrónico aumenta en frecuencia y alcance

Como ocurre con la mayoría de las formas de ciberdelincuencia últimamente, también se ha producido un aumento de los casos de e-skimming. No sólo es más frecuente, sino que el alcance de los ataques de e-skimming también se está ampliando, debido a la automatización.

Básicamente, el e-skimming es un fraude con tarjetas de crédito en el que los atacantes aprovechan una brecha de seguridad e instalan software malicioso en la página de procesamiento de pagos. De este modo, obtienen acceso en tiempo real a las credenciales de acceso de los clientes, a sus datos personales y a la información de sus tarjetas de crédito.

> “Este enorme aumento de los ataques y los daños se debe sobre todo a que las víctimas están dispuestas a pagar el rescate.”

Mantenerse a salvo del e-skimming puede ser complicado, ya que puede ser difícil de reconocer, pero en general, debe asegurarse de que visita páginas web con certificados SSL válidos y vigilar sus gastos.

El ransomware es cada vez más frecuente y provoca mayores daños

En 2021, se predijo que se producirá un ataque de ransomware a empresas cada 11 segundos. Para comparar, en 2016 esta cifra solía ser cada 40 segundos, y se estima que el daño total de los ataques de

ransomware alcanzará los 20.000 millones de dólares, 57 veces más que en 2015.

Este enorme aumento de los ataques y los daños se debe sobre todo a que las víctimas están dispuestas a pagar el rescate.

Los proveedores de servicios gestionados (MSP) son un objetivo especialmente importante, ya que toda la base de clientes que utilizan el servicio se verá afectada. Así que, por ejemplo, si utiliza un MSP para alojar su tienda de comercio electrónico, debe asegurarse de seleccionar un servicio de alojamiento con medidas de seguridad decentes y un gran servicio al cliente. Además, debería tener esto en cuenta para cualquier servicio gestionado que su tienda online esté utilizando.

Los ataques de fuerza bruta tienen más objetivos

La tendencia a la personalización en el ecommerce ha ayudado a traer un enfoque basado en el usuario: te registras en una cuenta, creando un nombre de usuario y una contraseña.

Sin embargo, según el Informe Global de Riesgo de Datos 2019 de Varonis, el 38% de los usuarios tiene contraseñas que nunca caducan. En comparación con 2018, esta cifra experimentó un aumento del 10%.

Este es un terreno fértil para los atacantes, ya que es mucho más fácil descifrar contraseñas débiles con fuerza bruta, mientras que las contraseñas que no caducan proporcionan una ventana de oportunidad infinita.

Como hoy en día se considera un riesgo para la seguridad cambiar las contraseñas con frecuencia, debería asegurarse de que sólo utiliza contraseñas seguras y, posiblemente, incluso la autenticación de dos factores, independientemente de si es propietario de un sitio web de comercio electrónico o simplemente tiene una cuenta en el negocio online de otra persona.

Los ataques de phishing siguen siendo fuertes

El phishing sigue siendo una de las amenazas de seguridad más comunes. Es una de las formas más antiguas de ciberataque y se sigue utilizando de diversas maneras para obtener datos sensibles, como los de las tarjetas de crédito, o infectar a las organizaciones con ransomware u otro malware.

Como el 58% de los consumidores espera hacer más compras en línea después de la pandemia del COVID-19 que antes, los negocios fuera de línea tienen más incentivos para iniciar su presencia en línea. Los atacantes están ansiosos por explotar cualquier plataforma de comercio electrónico que no haya invertido en una formación adecuada sobre la concienciación del phishing y otras amenazas de ciberseguridad.

Si un ciberdelincuente se hace con el control de la cuenta de un administrador


Crédito: snowing en Freepik

de su tienda online, su negocio podría sufrir muchos daños. Para evitarlo, asegúrese de que su personal está bien formado para reconocer y evitar los intentos de phishing. Como cliente, utilice un software antivirus y no comparta nunca sus credenciales de acceso u otra información sensible con nadie.

En 2021, el sector del comercio electrónico creció rápidamente. Como demuestran las amenazas descritas anteriormente, veremos un crecimiento continuo en el número y la complejidad de los ataques, así como su impacto financiero. Además, un número cada vez mayor de ataques serán automatizados y estarán más extendidos.

Esté atento a estas cinco amenazas a la seguridad del comercio electrónico y manténgase a salvo.

Fuente: Kristina Tuvikene en Infosecurity Magazine (https://www.infosecurity-magazine.com/next-gen-infosec/five-ecommerce-security-threats/)

Ciberseguridad en la industria financiera:

Tendencias y desafíos de cara a 2022

Por Rocío Bravo

El escenario actual ha exigido al sector financiero convertirse en uno con los mayores índices de digitalización posible. Esto puede ser muy atractivo desde el punto de vista del negocio, pero también muy riesgoso. ¿Cómo hacer frente a un contexto donde los ciberatacantes ven en la banca el principal objetivo?

Desde su aparición hace casi dos años, el Covid-19 ha generado un acelerado proceso de cambios en todo el mundo entre los que se incluye un aumento sin precedentes de la digitalización. Impulsado por las demandas del consumidor actual, el sector financiero es uno de los que más ha acelerado la transformación digital por lo que enfrenta también desafíos de riesgo cibernético de manera constante.

Una de las mayores preocupaciones del sector es cómo mantener protegidos los datos personales y la información sensible de sus clientes. Los distintos tipos de ataque a los que se ven expuestas y las consecuencias potenciales para sus clientes y sus operaciones, convierten a la ciberseguridad en un foco de constante atención para las entidades. Según datos de la última edición del informe anual que realiza IBM "Cost of a Data Breach Report", el costo promedio de una brecha de datos en el sector de servicios financieros fue de 5.85 millones de dólares en 2020, una cifra superior a la de 3.86 millones de dólares que manifestaron los encuestados del resto de los sectores económicos.

"La transformación digital impulsó un nuevo paradigma para la industria de servicios financieros", plantea **Marcelo Felman, director de Ciberseguridad de Microsoft Latinoamérica.** "Ahora,


A1

Marcelo Felman - Microsoft

casi todos los productos y servicios ofrecidos por las instituciones financieras dependen de la tecnología. Esto significa que tienen que automatizar sus procesos y operaciones, confiar en tecnologías como la IA, apalancarse en el uso de datos, ser más ágiles y seguras. Todo esto permite aumentar la productividad de los empleados, empoderándolos, conocer mejor a los clientes para adquirirlos, atraerlos, mejorar los productos que se ofrecen y optimizar las operaciones, por ejemplo, eliminando los trámites manuales".

Para avanzar en estas transformaciones y potenciar la ciberseguridad, la IA es una tecnología clave. Hoy en día se utiliza, principalmente, para ofrecer mejores servicios a los clientes y detectar fraudes. Según el estudio Microsoft Digital Defense Report 2021 las medidas de "higiene digital" pueden proteger a las organizaciones del 98% de los ataques. Por su parte, el informe FortiGuard Labs, arroja que en América Latina se contabilizaron más 91 mil millones de intentos de ciberataques en el primer semestre del 2020. La actividad semanal promedio de ransomware en junio de 2021 fue diez veces mayor que los niveles de hace un año.

"El sector bancario es un objetivo llamativo, no solo por ser entidades que manejan grandes cantidades de dinero, sino también por la información sensible con la que cuentan", complementa **Martina Lopez, Especialista en Seguridad Informática de ESET Latinoamérica.** "En este sentido, y de manera interna, podemos encontrar aquellas amenazas que tienen como objetivo robar y exfiltrar información, como las piezas de software espía, troyanos y ransomware. Esta última es de las más temidas, y no faltan razones para ello. El negocio del cibercrimen ha creado bandas que desarrollan familias de este tipo de amenazas, manejándose como organizaciones,

Martina Lopez - ESET

teniendo muchas de estas objetivos específicos como los bancos.

También, sigue la vocera, "debemos tener en cuenta aquellos ataques que suplantan la identidad de las compañías bancarias y financieras. Si bien estos no tienen como objetivo la infraestructura o servicios críticos de las mismas, afectan de manera indirecta al negocio, ya sea por la pérdida de clientes, dinero o confianza de sus usuarios".

Hernan Conosciuto - Red Hat Arg.

El riesgo de cara al cliente

Según **Hernan Conosciuto, Principal Specialist Solution Architect Automation CyberSecurity Cloud Storage de Red Hat Argentina**, "en muchos casos, este tipo de ataques terminan generando indisponibilidad de servicio, ya que cualquier empresa del sector financiero necesita tener el historial de transacciones de cada uno de sus clientes, es decir, no puede operar 'a ciegas'. Esto termina generando la

imposibilidad de usar los sistemas por parte de los clientes, e incluso de los mismos empleados de la compañía".

"El principal riesgo de los ciberataques tiene que ver con los datos, el mayor activo de las organizaciones en la era digital, y la seguridad de la información es crítica para millones de entidades de todos los tamaños y sectores", agrega el responsable de Microsoft. !En este sentido, un ataque cibernético, dependiendo de su magnitud, puede generar un un gran impacto operacional, reputacional o incluso legal, estos delitos les cuestan a las compañías cerca de mil millones de dólares al año y las organizaciones pueden demorarse en promedio 7 meses en detectarlo, cuando ya es tarde para reparar los daños".

En línea con esto, uno de los principales factores de riesgo tiene que ver con las contraseñas. Según un estudio de Microsoft, actualmente se realizan 579 ataques de contraseña por segundo, es decir, 18.000 millones al año. "Esta realidad nos obliga a replantearnos las estrategias para proteger a las organizaciones ante posibles amenazas cibernéticas, ya que los ataques maliciosos han aumentado en su número y en su sofisticación", sugiere Felman.

Para la ejecutiva de ESET, "no solo existe el riesgo obvio de la vulneración de sus cuentas bancarias, sino también el peligro de la exposición de datos sensibles. Todo banco, para operar, requiere de una gran cantidad de información crítica de una entidad, ya sea un individuo o compañía, como identificadores gubernamentales o direcciones de residencia".

Es por esto, destaca Lopez, "que el esfuerzo de las entidades bancarias por mitigar los ataques, de cara a sus clientes, es cada vez mayor. Desde la comunicación constante anunciando los canales oficiales de la compañía para prevenir ataques de phishing, pasando por la creación de canales de denuncia para este tipo de delitos, hasta la transparencia en el caso de sufrir algún ataque de este tipo".

Martín Malievac - Napse

El factor humano

Uno de los pilares actuales de la protección a los ciberataques se basa en la educación del usuario. Según el vocero de Red Hat, el factor humano es tan o más relevante que el técnico. "Es imposible prevenir el 100% de los ataques, por eso, es sumamente importante que los usuarios estén informados y actualizados para no caer en engaños que terminan otorgando acceso a la red de la empresa", remarca. "Por otro lado, la parte técnica está en una mejora permanente. Hoy ya no hay sólo un par de personas detrás de estos eventos, sino organizaciones que lucran de manera considerable con estos ataques y rescates".

Martín Malievac, Director de Investigación y Desarrollo de Napse, comparte la idea de que el factor humano tiene una relevancia fundamental. Por un lado, dice, "se trata de ayudar a las personas y clientes a que cada vez más aprendan a evitar estas técnicas de fraude. El hábito se forma por una serie de repeticiones, por eso creo que informar en todo momento, todos los días, creará con el tiempo acciones destinadas a reducir la posibilidad de ocurrencia. Por otro, como empresa debemos contar con soluciones preparadas. Por ejemplo, vemos cada vez más el token de seguridad, que actúa como un segundo validador al momento de ingresar en un sitio web, portal bancario o para autorizar determinadas acciones. El celular se ha transformado también en una herramienta de seguridad, ya que muchas soluciones envían SMS, WhatsApp o incluso un llamado para validar la identidad del cliente".

"Si bien existen ataques que se aprovechan de factores técnicos, como vulnerabilidades en programas utilizados sin actualizar, una muy buena parte de estos ataques utilizan las debilidades humanas para ingresar a los sistemas", complementa la experta de ESET. "No solo es más sencillo y menos costoso, sino que también es más efectivo para los cibercriminales. Engañar a un mando medio utilizando técnicas de ingeniería social para que descargue un archivo malicioso o ingrese sus credenciales en un sitio fraudulento, suele tener más casos de éxito que encontrar una vulnerabilidad y poder explotarla, teniendo en cuenta que la mayoría de los controles tecnológicos se basan en detener el aspecto técnico de los ataques".

Norberto Marinelli - CertiSur

La oferta para estar protegidos

"Desde el laboratorio de ESET, fomentamos el cambio de cómo las organizaciones perciben a la seguridad", dice la ejecutiva de la empresa. "Por la velocidad en la cual las amenazas se transforman e implementan técnicas nuevas, se debe abandonar la idea de que la seguridad corporativa consta de seguir una serie de reglas o protocolos. La seguridad debe formar parte de la cultura y percepción del negocio de la organización, así como el día a día de los colaboradores que la componen".

Un ejemplo de ello es la adopción de la gestión Zero Trust. Este modelo parte de la idea de que, por defecto, las organizaciones nunca deberían confiar en ninguna entidad interna o externa que ingrese a su perímetro físico o virtual. Muchas de las herramientas y técnicas necesarias para comenzar a implementar Zero Trust ya son utilizadas, como controles de accesos basados en el principio del menor privilegio, la gestión de activos y clasificación de la información, la segmentación de redes, entre otros. A estos controles basta con añadir una capa crucial: automatización y orquestación; y visibilidad y análisis.

Por el lado de Microsoft, plantea su vocero, "adoptamos una visión integral con respecto a la ciberseguridad, que se apoya en el Principio de Confianza Cero, como su principal pilar. Microsoft Azure puede creacapacidades de detección de fraude en línea con Cortana Intelligence Suite que funcionan para detectar el fraude bancario en línea de forma más rápida y precisa".

Además, sigue, "creemos que es fundamental brindar transparencia en nuestras plataformas y servicios en la nube, no solo para los clientes, sino también para los reguladores. Con respecto a esto último, nuestro Programa de Cumplimiento de Servicios Financieros permite a las partes interesadas de la industria examinar profundamente nuestros sistemas, servicios y procesos en la nube. Incluye acceso a auditorías de terceros, prácticas de gestión de riesgos, manejo de datos y políticas de seguridad, informes de pruebas de penetración, revisiones de incidentes de seguridad, evaluaciones de amenazas y cualquier información que sea crítica para el cumplimiento".

"Las empresas deben mejorar las señales que los identifican en la web, e instruir a sus clientes para que las respeten y busquen", plantea **Norberto Marinelli, CEO de CertiSur.** "Un sitio seguro, con un certificado EV, le brinda garantía al cliente que se está comunicando con el banco. Es un signo fácil de distinguir y respetar".

También, agrega, "es necesario que

CYBERARK®

A medida que el perímetro se disuelve,

¿cómo pueden proteger las organizaciones el acceso a sus recursos más valiosos (datos, aplicaciones e infraestructuras) de forma local o en la nube?

El 97 % **afirma que el robo de credenciales va en aumento**

Los ponentes de la "Visión de los CISO" recomiendan proteger a los usuarios finales con un acceso de alto valor

El 94 % **se enfrenta a retos operativos de seguridad para endpoints**

Los ponentes de la "Visión de los CISO" recomiendan minimizar el acceso del administrador local y restringir la instalación del software

El 88 % **afirma que la transición a la Confianza Cero es "importante" o "muy importante"**

El 45 % afirma que la máxima prioridad es implementar controles IAM

El 87 % afirma que reducir los privilegios permanentes es "importante" o "muy importante"

El 86 % **afirma que la optimización de la experiencia del usuario (86 %) es "importante" o "muy importante"**

Los ponentes de la "Visión de los CISO" (CISO View) indican métodos de autenticación que introducen la fricción del usuario final que pueden provocar fatiga en la seguridad y hábitos de riesgo

El único plano de control práctico para redes, dispositivos, usuarios, aplicaciones, etc. son controles centrados en la identidad. Con la Confianza Cero, no se confía en ningún actor a menos que se verifique continuamente. El enfoque estratégico e integral de la seguridad garantiza que los dispositivos a los que se concede acceso sean quiénes y los qué dicen que son. Descargue el e-book.

CyberArk.com

los usuarios reconozcan los correos firmados por la institución, y que rechacen cualquier instrucción que reciban por mensajes sin firma. Para ello, CertiSur provee desde hace 20 años un servicio altamente probado y confiable; el de certificados digitales para usuarios finales. Varias entidades financieras del mercado cuentan con este servicio orientado a Banca Empresa por el cual los apoderados de las mismas se autentican de una manera robusta y al mismo tiempo firman digitalmente las operaciones en Home Banking e incluso a través de la app Mobile".

Ciberataques: A qué nos enfrentaremos en 2022

Año a año, el cibercrimen aumenta y se fortalece como negocio, aclamando millones y millones de dólares. "Teniendo en cuenta que esta tendencia no se detendrá, en 2022 veremos una mayor cantidad de cibercriminales, bandas con su infraestructura y ciberataques utilizando técnicas que los identifiquen. Negocios como el ransomware como servicio, en donde la amenaza es puesta en "alquiler" para tercerizar las infecciones, y la venta de información robada seguirán estando detrás de las principales preocupaciones de entidades financieras y bancarias", anticipa Martina Lopez, de ESET.

En cuanto a la lucha contra el cibercrimen en las organizaciones, se verán nuevas tecnologías como protagonistas. "La implementación de tecnologías potentes como blockchain y machine learning a la ciberseguridad, resultan claves para hacer frente al panorama de amenazas actuales y las que están por venir. En primer lugar encontramos al blockchain, que funciona como el libro de un escribano,

Crédito: rawpixel.com en Freepik

garantizando integridad, disponibilidad y confidencialidad de la información almacenada. Si bien el uso de blockchain está fuertemente asociado a las criptomonedas, esta tecnología se puede utilizar para otro tipo de activos digitales, como las transacciones financieras o el resguardo de información crítica", detalla la vocera.

Por su parte, el machine learning se ha establecido como medio para luchar contra las ciberamenazas. Los ciberataques no son estables, ya que todo el tiempo los cibercriminales mejoran sus técnicas y herramientas y evolucionan las amenazas. En este contexto, el machine learning es definitivamente una herramienta ideal para combatirlas, dadas sus capacidades de adaptación y de aprendizaje. Esta tecnología se puede utilizar, por ejemplo, para detectar fraude online en tiempo real o encontrar vulnerabilidades en los sistemas.

De acuerdo con el ejecutivo de Red Hat, existen mejoras constantes en la creación del malware utilizado, esto está impactando en paquetes provenientes del Open Source e incluso generando scripts que, por un lado, escapan a la vista de los sistemas de seguridad, y, por otro, utilizan técnicas de ingeniería social dentro mismo. "Todo esto genera de manera imperativa la necesidad del constante chequeo de los sistemas, el análisis de comportamientos extraños y la acción automática como respuesta a cualquier evento".

También, sigue el vocero, "será sumamente importante el armado de arquitecturas que permitan trabajar aún teniendo parte de la solución comprometida, la optimización de los planes de restauración, su automatización y testeo periódico para garantizar que ante un incidente se pueda seguir atendiendo el negocio lo antes posible, o incluso sin interrupción".

Por último, plantea Martín Malievac, de Napse, "en la era post pandemia, ciertos hábitos que se intensificaron serán una norma. El teletrabajo, por ejemplo, permite a los empleados acceder a información de la empresa de manera remota y esto supone un riesgo y un cuidado mayor a lo que se solía tener históricamente. Para ello, la utilización de técnicas de "menor privilegio" son iniciativas que cobran cada vez más relevancia".

"La nueva normalidad ya llegó, los hábitos tecnológicos adoptados en la pandemia son parte de nuestro día a día y como habitantes de esta era digital debemos estar preparados para detectar naturalmente este tipo de estafas que seguirán existiendo y evolucionando", concluye el vocero.

Ciberataques al sector financiero: ¿Cómo anticiparse?

Andrés Mendoza - ManageEngine

En cuanto a los principales ciberataques que recibe el sector financiero, Andrés Mendoza, Jefe Técnico Regional de ManageEngine LATAM, enumera: "La ingeniería social y los ciberataques son los primeros en la lista, siendo el phising uno de los métodos más utilizados desde hace varios años. La suplantación de sitios web para la captura de datos personales es una de las principales amenazas a las que se ve enfrentado el usuario de la banca móvil o aquellos que realizan transacciones en Internet de forma frecuente. Por otro lado, el ransomware y la no utilización de tráfico encriptado acompañan el top de la lista".

Según un estudio realizado por Deloitte, el 88% de los ciberataques en el sector financiero es exitoso en menos de un día, pero solamente el 21% de ellos son detectados durante el primer día. El impacto económico que producen estas agresiones en las organizaciones varía considerablemente, según el momento en que los mismos son detectados y contrarrestados. En el caso en que la detección se produzca en el mismo día, puede costar algunos miles de pesos, pero ese impacto sube a millones de pesos cuando se trata de más de tres días. A pesar de que la industria financiera lleva años invirtiendo en ciberseguridad, los estudios más recientes muestran que sigue siendo un desafío poder identificar y estar a la altura de las ciberamenazas actuales, debido al número y complejidad de su evolución.

La propuesta de ManageEngine

"El sector de servicios financieros es el blanco más común de los ataques cibernéticos, lo que significa que necesitan una seguridad hipervigilante. Los clientes les confían su futuro, por lo que no pueden arriesgar la seguridad de la información y otros recursos de TI", enfatiza el ejecutivo. "Desde ManageEngine podemos ofrecer a estas entidades financieras la capacidad de gestionar su seguridad en modo piloto automático, permitiendo reducir riesgos en todos los niveles de su organización con un monitoreo constante de incumplimiento de las normas, accesos no autorizados y actividad sospechosa.

"Con las inmensas posibilidades de la nueva tecnología, desde wearables hasta IoT, los errores en la seguridad son inevitables", sigue. "De ahí, la importancia de monitorear todos los dispositivos de su organización para evitar posibles problemas de seguridad y mantener su TI funcionando sin problemas en todo momento. Contamos con una guía de soluciones en ciberseguridad y una guía para la implementación de los controles CIS, entre otros recursos gratuitos que pueden aportar a la estrategia de seguridad informática en las empresas".

ManageEngine

El nuevo perímetro de seguridad de las empresas está en los hogares de los trabajadores.

¿Cómo está gestionando los dispositivos remotos?

Conozca el amplio portafolio de ManageEngine para la gestión de servicios de TI, gestión unificada de endpoints, gestión de operaciones y ciberseguridad, entre otros dominios.

Alineamos TI con su negocio.

www.manageengine.com/latam

Ciberataques: Concientizar como parte de la estrategia

Miguel Llerena - Tanium

El aumento de la digitalización y las tendencias como las plataformas de banca abierta, que han experimentado un crecimiento impresionante en la región, ofrecen beneficios a los clientes finales, pero también aumentan las amenazas a la infraestructura. Los ataques de ransomware continúan aumentando a nivel mundial y aún más después de una pandemia, donde se ven técnicas de ataque más sofisticadas. Este tipo de delitos que amenazaban con liberar datos robados están aumentando y el 72% de las organizaciones tienen al menos un incidente de ciberseguridad en los últimos 12 meses según un estudio realizado por la Comisión Económica de la ONU para LATAM y el Caribe (CEPAL).

Desde Tanium, opinan que estos ataques interrumpen una variedad de servicios, impactan su infraestructura crítica con efectos devastadores, en algunos casos paralizan sus operaciones y secuestran sus datos. "Si bien algunas empresas optan por pagar con el pago promedio en Estados Unidos de aproximadamente 250.000 dólares, el impacto material para estas instituciones se puede cuantificar en la pérdida de ingresos, clientes e impacto en su reputación y marcas", expresa Miguel Llerena, Vicepresidente Regional para LATAM de Tanium.

Por otro lado, el factor humano es fundamental y se está produciendo una transformación y educación en muchos niveles. "Las campañas de concientización para el público y los empleados sobre cómo proteger los datos personales deben ser parte de la estrategia", destaca Llerena. "En lo que respecta al lado tecnológico de la ecuación, las empresas necesitan mejorar sus herramientas de respuesta a incidentes para tener una mejor visibilidad mediante la adopción de soluciones de gestión de terminales, que puedan monitorear proactivamente sus redes y ayudar a remediar la señal de intrusión".

A partir de este escenario, Tanium propone adherirse a las mejores prácticas fundamentales de higiene cibernética. "En términos de prioridad, primero llene las lagunas de visibilidad que identifique. La visibilidad proporciona una base y un multiplicador de fuerza para todas las demás actividades. Debe desarrollar visibilidad sobre los activos en su entorno, ya sea que estén administrados o no, y si viven en las instalaciones, en redes remotas o se mueven dentro y fuera de la red", plantea el ejecutivo.

Un 2022 desafiante para la ciberseguridad

Según Llerena, "la fuerza de trabajo y los lugares de trabajo híbridos continuarán, y hemos visto a muchas organizaciones anunciar su regreso a la oficina en algún momento de 2023. Este espacio de trabajo flexible requerirá una ciberseguridad efectiva que esté fuera de las paredes de la oficina y traiga nuevas amenazas a las organizaciones. Una postura sólida de ciberseguridad comienza con saber qué está sucediendo en su entorno en cualquier momento".

Ataques sofisticados de DDoS, phishing y ransomware: los enemigos del sector financiero

Adam McCord - Cyberark

De acuerdo con Adam McCord, Vice President Latin America and Caribbean de Cyberark, la fuga de clientes debido a la merma en la confianza producida por las interrupciones de servicio y los robos de dinero e información son los principales riesgos que atraviesa una entidad financiera a partir de los ciberataques.

"El factor humano es altamente relevante y muchas veces señalado como el eslabón más débil", asegura el vocero. "A veces el humano deja una puerta abierta mientras el factor técnico también juega un rol importante al exponer potenciales vulnerabilidades que requieren permanente revisión y corrección".

Frente a esto, la propuesta de la empresa es asegurar, en forma proactiva y en lo posible automatizada, la operación incluyendo la identidad de los usuarios para así apoyar las nuevas oportunidades sin arriesgar la reputación de la empresa o incurrir en incumplimientos.

La oferta incluye:

- Protección de accesos privilegiados en todos los entornos
- DevSecOps
- Detección y protección efectiva contra millones de variantes de Malware/Ransomware
- Análisis de comportamiento
- Seguridad de la identidad con autenticación robusta y asistida por IA

Tendencias 2022

De cara al próximo año, desde Cyberark entienden que la identidad se establece como el perímetro a proteger y los usuarios exigen métodos remotos y sin contacto lo cual se traduce en la necesidad de fortalecer este eslabón fundamental en la cadena de un ataque sofisticado.

Luego, se vislumbra la consolidación de soluciones de autenticación para poder minar en forma centralizada la información recolectada en estos eventos; "Shift left" toma fuerza en la medida que las empresas reconocen el menor costo de integrar la seguridad desde el principio del ciclo de vida de desarrollo de sus aplicaciones; los entornos multi-cloud complejizan la tarea de asegurar una operación bajo la buena práctica del "mínimo privilegio"; y no hay más accesos permanentes.

Netskope mitiga el gran riesgo de abuso de las cuentas en la nube mal protegidas

Como muchos otros, el sector financiero confía en el cloud para gestionar sus cargas de trabajo. Sin embargo, las cuentas en la nube se han convertido en un objetivo codiciado para los ciberdelincuentes, no solo por los beneficios que un entorno IaaS comprometido ofrece, sino también, porque esa misma infraestructura procura un entorno de confianza desde el que dirigir ataques contra otros objetivos.

A este respecto, un reciente informe elaborado por el Equipo de Acción de Ciberseguridad de Google recoge los motivos que llevan a los ciberdelincuentes a explotar las cuentas de Google Cloud Platform (GCP): el 86% fueron utilizadas para llevar a cabo minería de criptomonedas, un 10% para realizar escaneo de puertos en otros objetivos, mientras que un 8% y un 6% para lanzar ataques contra diferentes blancos y para alojar malware, respectivamente.

En cuanto a los vectores de acceso más recurrentes, las contraseñas débiles y las APIs no autorizadas son los más empleados (48%), seguidos de las vulnerabilidades en el software de terceros (26%), las malas configuraciones y otros problemas (ambos con un 12%).

Netskope, una solución de seguridad cloud

Para evitar que los atacantes realicen abusos sobre las cuentas en la nube mal protegidas, las empresas financieras pueden recurrir a Netskope Public Cloud Security, una solución que detecta los errores de configuración en entornos IaaS como AWS, Azure y Google Cloud Platform que pueden ser explotados por los ciberdelincuentes.

A través de un conjunto de perfiles predefinidos, Netskope Public Cloud Security facilita que los usuarios puedan cumplir con las mejores prácticas y estándares de la industria como NIST CSF, PCI-DSS y CIS. Además, permite construir fácilmente reglas personalizadas con el Lenguaje Específico de Dominio. Esta misma protección también está disponible para las aplicaciones SaaS gracias al nuevo módulo SSPM

Paolo Passeri - Netskope

(SaaS Security Posture Management).

Por otro lado, y ante el incremento de los ataques de fuerza bruta o de password-spraying contra los servicios de acceso remoto mal configurados (como RDP o SSH), Netskope Private Access es la solución para mitigar este riesgo, permitiendo a las organizaciones publicar sus servicios (alojados en una nube pública o en un centro de datos on-prem) de forma segura, adoptando el paradigma de acceso de confianza cero.

Por último, Netskope Advanced Analytics proporciona cuadros de mando específicos para evaluar el riesgo de las malas configuraciones de cuentas en la nube, con abundantes detalles y perspectivas, apoyando a los equipos de seguridad en el proceso de remediación.

Ekoparty 2021: criptomonedas, electricidad y otras vicisitudes

Por Rubén Borlenghi

Impulsada por la pandemia, la Ekoparty 2021 (número diecisiete) fue virtual, tal como la del año anterior. Se desarrolló entre el martes 2 y el sábado 6 de noviembre, y sus únicas actividades presenciales fueron experiencias de Wardriving por las calles de Buenos Aires catalogando puntos de acceso Wifi, y dos reuniones para socializar en locales también de Buenos Aires, en las noches del viernes y el sábado.

La organización estuvo a cargo de un nutrido equipo comandado por Leonardo Pigñer, CEO y cofundador de Ekoparty, y los demás cofundadores de la Eko: Federico Kirschbaum (CTO de Faraday), Jerónimo Basaldúa (director de Base4 Security) Francisco Amato (CEO de Faraday) y Juan Pablo Daniel Borgna.

En esos cinco días los asistentes, cercanos a los mil por día, pudieron elegir entre poco más de 140 presentaciones y 10 workshops que, en algunos casos, se repitieron en horarios diferentes, a fin de permitir el ingreso a más espectadores; tal acceso a la plataforma de transmisión hizo que los organizadores lo calificaran como "el evento de tecnología más grande de Latam", con más de 5000 visitantes entre todas las plataformas.

Luego de una bienvenida a cargo de Leonardo Pigñer, tras su saludo se exhibió una video parodia de "Terminator", donde un enviado del futuro llega para conectarse con hackers de Buenos Aires, frente al inminente Fin del Mundo, para que lo lleven con la mujer que salvará al planeta: en este caso, la brillante investigadora (real) Sheila Berta.

Por analizar la cantidad de material puesto a disposición del público asistente se puede deducir el esquema temático que animó la organización del evento, en cuanto a sus actores posibles: el hacker como profesional independiente que necesita herramientas y entrenamiento; el profesional de seguridad informática que interactúa con empresas; el equipo de integrantes de empresa que deben ejecutar funciones de seguridad para asegurar la continuidad del negocio, y los miembros de los organismos de Infraestructura Crítica que deben mantener el funcionamiento de servicios esenciales bajo ataque.

Los y las especialistas convocados para exponer su material tuvieron como origen varios países de Europa, Estados Unidos y Latinoamérica. Varios de ellos son expertos ya conocidos por el público que tiene años presenciando la Eko.

> En esos cinco días los asistentes, cercanos a los mil por día, pudieron elegir entre poco más de 140 presentaciones y 10 workshops que, en algunos casos, se repitieron en horarios diferentes, a fin de permitir el ingreso a más espectadores.

Criptomonedas, software y cuántica

En cuanto a la temática de las presentaciones y workshops, también pueden

separarse por disciplina: se pudo obtener entrenamiento básico sobre Criptomonedas, como en el caso de "Blockchain: Desde su origen hasta la reformulación del sistema financiero", presentada por Nicolás Colombo, y "Open blockchain" por Camilo Rodríguez, hasta el ataque a los usuarios de criptomonedas, detallado en "All your Ether are belong to us (a.k.a Hacking Ethereum-based DApps)" presentado por Luis Quispe Gonzales.

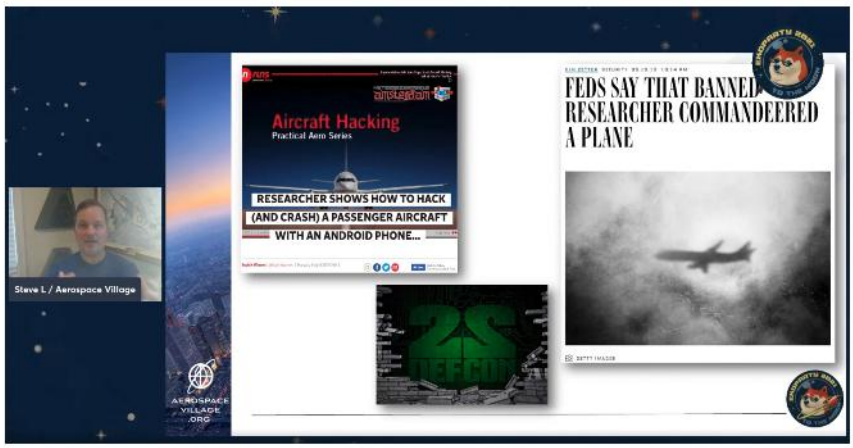
El futuro ya cercano de la computación cuántica, y sus conexiones con la seguridad informática, también estuvieron presentes con "Criptografía Post-Cuántica integrada en HTTPS", a cargo del ingeniero mendocino Diego Córdoba, o la detallada explicación de fundamentos matemáticos en "The silent partners" de parte de Luciano Bello y Carlos Benitez, que presentaron al público el algoritmo que actúa como el componente fundamental del de Shor, así como otros algoritmos de computación cuántica: la Transformada Cuántica de Fourier.

Los ataques al software de uso extenso entre corporaciones o entre usuarios en general también estuvo presente, como en "De 0 a millones de dólares en un par de paqueles: Comprometiendo sistemas SAP en Internet sin autenticación", a cargo de Ignacio Favro, quien comentó detalles de tres vulnerabilidades en SAP publicadas durante 2020. También el Visual Studio de Microsoft estuvo representado, con "1-click to infiltrate your organization via vulnerable VS Code extensions", donde Kirill Efimov y Raul Onitza-Klugman detallaron técnicas para atacar la cadena de suministros de una empresa con un clic, aprovechando vulnerabilidades descubiertas en extensiones de Visual Studio que son muy usadas por los programadores.

Y tampoco podía faltar uno de los mayores expertos del descubrimiento de fallas en el software que provee Apple en las Mac: Bundles of Joy: Breaking macOS via Subverted Applications Bundles, que presentó Patrick Wardle (uno de los anotados permanentes a Ekoparty). En este caso se trata de una vulnerabilicad reciente —CVE-2021-30657— descubierta en el conjunto de procedimientos ce software de protección que Apple insertó en el Mac OS. En esta ocasión, un atacante puede diseñar una APP que contenga código malicioso, que no será descubierto, y podrá causar el compromiso de la computadora.

Si los productos comerciales más tradicionales, como Wordpress, fueron explorados y atacados por los especialistas, también un software relativamente nuevo, pero de extenso uso durante la pandemia, como Zoom, mereció su atención. Fue el investigador Thijs Alkemade quien, con "Hacking the pandemic's most popular software: Zoom" mostró cómo (por una falla de diseño del software) se podía tomar el control de la computadora de un usuario de Zoom. Alkemade trabajó junto con Daan Keuper y ganó

> Si los productos comerciales más tradicionales, fueron explorados y atacados por los especialistas, también un software relativamente nuevo, pero de extenso uso durante la pandemia, mereció su atención.



200.000 dólares en abril de este año, en una competencia de especialistas por el premio a un exitoso ataque, en la categoría "Enterprise Communications".

Para recordar que los equipos del tipo mainframe siguen utilizándose, sobre todo en el entorno bancario, Carlos Pose y Juan Aguayo presentaron "Mainframe - Un entorno con permanencia y solidez, historia, presente y futuro", donde se hizo primero un recuento histórico de los equipos de ese tipo empleados en el banco donde se desempeñan, y luego se detalló la estructura de equipos de trabajo que los atienden.

Ataque a los fierros

También el ataque al hardware estuvo presente en esta Ekoparty, con varias instancias. Entre ellas, se programaron talleres prácticos, como el de "Introducción al Hardware Hacking", de Emmanuel Seoane, donde se enumerarían herramientas y procedimientos, o presentaciones como "IoT- ¿Son los Electrodomésticos la próxima Skynet?", con Cristian Borghello, en la que se mencionan las fallas de seguridad, y de resguardo de la privacidad, presentes en cantidad de productos; o "Assessing IoT with EXPLIoT Framework" por Aseem Jakhar, quien además de explicar el uso de EXPLIoT para estudiar las posibles fallas de seguridad de un firmware en un producto IoT, mostró ejemplos del empleo de DIVA, una placa con microprocesador y conexión 802.15.4 (ZigBee), de corto alcance y baja capacidad de transmisión, que suele estar presente en redes de productos IoT.

Otro ejemplo importante de ataque a hardware, que podría tener efectos muy graves sobre la salud de una víctima, fue "Overmedicated: Breaking the security barrier of a major infusion pump", a cargo de Philippe Laulheret y Douglas McKee (ambos trabajan para McAfee Research). Se dedicaron a estudiar una bomba de infus ón de uso frecuente en hospitales de Europa y EE.UU, la Braun Infusomat modelo 871305SU. Según la definición que les proveyó la FDA, "una bomba de infusión es un dispositivo de uso médico que provee fluidos, tales como nutrientes y medicación, en el cuerpo de un paciente, en cantidades controladas". Encontraron que se comunicaba con el exterior (y recibía órdenes) por Wifi. Y también encontraron la manera de ordenar a la máquina que proveyera al paciente una sobredosis. El fabricante afirmaba que el sistema interno no podía alterarse.

Hay paneles y paneles

En el caso de Infraestructura Crítica, también hubo presentaciones con detalle de procedimientos. Para una aproximación al tema, se anunció "Introducción a la captura de amenazas en entornos industriales", por Sergio Vidal, y atrajo a muchos participantes el Panel: "CiberSeguridad en el sector Eléctrico", en el cual intervinieron varios miembros del CoNCiME, Comité Nacional de Ciberseguridad del Mercado Eléctrico. Ese panel estuvo integrado por Claudio Caracciolo (Auravant); Santiago Julian Lopez Galanes (CISO Pampa Energía); Agustín Zorgno (CISO Edenor); Walter Heffel (CISO ENERSA) y Nora Alzua (Coordinadora del Centro de Ciberseguridad Industrial CCI-Es)

Iniciaron la reunión indicando que la formación de ese comité nacional se concretó con la intención de impulsar y fomentar la creación e implementación de políticas, procesos y mejores prácticas que contribuyan a gestionar el nivel de ciberseguridad de las infraestructuras críticas y sus activos.

Dado que varios de ellos se conocían desde hace años, tuvieron la decisión de reunirse para impulsar una mejora continua de procesos, investigar los temas de ciberseguridad en el mundo eléctrico, no los del mundo IT, dado que se manejan en las empresas de producción, transporte y distribución de energía eléctrica. También fomentar y ayudar a que las empresas crezcan en su nivel de madurez respecto a esos temas de ciberseguridad conocidos por todos nosotros.

> “Fue decisión de ese grupo tomar el impulso y avanzar en la producción de un documento que sea útil en este tema, dado que en nuestro país no existe regulación ni para el mercado eléctrico ni para la industria en sí.”

No es una organ zación que se forma a partir de un requisito gubernamental. Fue decisión de ese grupo tomar el impulso y avanzar en la producción de un documento que sea útil en este tema, dado que en nuestro país no existe regulación ni para el mercado eléctrico ni para la industria en sí. Este impulso surge de un tema colaborativo, y para ver cómo entre todas las empresas pueden auxiliar para sacar lo mejor de sí.

“En esta industria, cuando había un incidente nadie se enteraba; en charlas durante viajes al exterior, nos decían que tratáramos de colaborar entre nosotros, y así nació este comité. Nuestra actividad es ad honorem, lo hacemos porque nos gusta y somos apasionados...”. Sobre los sistemas involucrados: “estos sistemas no nacieron con seguridad; esto es algo nuevo, una de nuestras misiones es explicar el riesgo, trasladarlo al negocio, ver qué importante es tener información en tiempo real, ser colaborativos”.

Hoy casi no hay proyecto en el cual no llamen a seguridad; antes eso no existía. “Los profesionales de ciberseguridad tenemos un desafío, independientemente que pertenezcamos al palo de TI o de TO: es dejar de estar en el detalle, en el día a día, y empezar a tener una visión más estratégica de cara al negocio, de cara a la industria; eso nos obliga a incorporar habilidades, cosas que tal vez la facultad o la preparación más dura, técnica o informática en ciberseguridad, no nos da, y que tiene que ver con habilidades comunicacionales, poder hablar el lenguaje del negocio para hablar con ese directivo con el cual podemos tener dos minutos; y en ese tiempo hacer un pantallazo de necesidades, no tremendista, y poder responder al ‘¿y eso cuánto cuesta?; explicar porqué eso es importante y cómo afecta el negocio, explicar a nivel de riesgo y explicar la cada vez mayor vinculación entre el mundo virtual y el mundo real, cómo el mayor nivel de automatizac ón es muy conveniente, pero también nos impone nuevos riesgos que deben ser gestionados controlados, de alguna manera administrados para poder tener mayores certezas en cuanto a la gestión, o en el caso de las Infraestructuras Criticas, a la prestación de servicios esenciales. Es necesario generar un lenguaje común que facilite el entendimiento."

Por las nubes, la Nube

Los riesgos de la Nube tampoco estuvieron ausentes de la Ekoparty, y también en este caso había material para iniciar la tarea, y para dedicarse a riesgos específicos. Por ejemplo, "Cloud Security concepts for blue teamers", un taller a cargo de Santiago Abastante; "Extracting all the Azure passwords", donde Karl Fosaaen muestra el uso de una herramienta de obtención de contraseñas, y "DIAL: A centralized security misconfiguration and threat detection framework on AWS" en que Harsh Varagiya, Divyanshu Mehta y Saransh Rana explican el uso de otra herramienta, en este caso para verificar políticas de autorización en AWS. También Leonardo Cuozzo explica, en "The Kerberos Key List attack: The return of the Read Only Domain Controllers", cómo aprovechar una nueva funcionalidad de Azure que permite autenticación sin contraseña... para encontrar un nuevo vector de ataque. Otro que se dedicó a Azure, en este caso con "Offensive Azure Security", fue Sergey Chubarov, que explicó cómo sobrepasar la autenticación y obtener acceso a la base de datos SQL de Azure.

En cuanto a Big Data, la encargada de explicar vulnerabilidades fue Sheila Berta, Jefa de Security Research en la empresa suiza Dreamlab Technologies. Con "The Unbelievable Insecurity of the Big Data Stack" realizó un cuidadoso despiece de una infraestructura de Big Data, detallando cada componente, mostrando la estructura completa, sus capas y administración (Data Ingestion, Data Storage, Data Processing y Data Access, y el Cluster Management), la gran cantidad de aplicaciones necesarias para organizar el flujo de información (entre ellas, Zookeeper, Ambari, Hadoop...), y qué vulnerabilidad encontró en cada una de esas aplicaciones. Mostró el uso de una herramienta empleada (Yarn), exploró Apache Spark y Sqoop, y detalló algunas recomendaciones de seguridad: reducir la superficie de ataque, instalar un firewall, asegurar las credenciales, implementar autenticación, administrar la autorización aplicando el principio de mínimo privilegio, y asegurar los canales de comunicación entre diferentes tecnologías.

> "La actividad aérea y los ataques de hacking a aeronaves comerciales, verdaderos o exagerados por la prensa, fueron parte de Ekoparty."

La actividad aérea y los ataques de hacking a aeronaves comerciales, verdaderos o exagerados por la prensa, fueron parte de la intervención de Steve Luczynski, miembro del Aerospace Village de DEFCON, en "Talking to Hackers: Building Relationships to Mitigate Cyber Risk", donde explicó cómo trabajó para tomar contacto con los investigadores interesados, cómo explicó con claridad en muchas presentaciones cuáles sistemas de un avión no deben ser intrusados en vuelo (son muy pocos) y en otra presentación, el experto Ken Munro (Hacking airplanes: The reality vs the hype) además de señalar en qué casos algún publicitado "hacking a un avión" no había sido tal como se publicó, y cómo se puede conseguir equipos de aviones en desarme, a fin de examinar la

posibilidad de encontrar fallas en sistemas. Especialmente señaló el problema de la Electronic Flight Bag, el dispositivo donde los pilotos registran parámetros de un vuelo y hacen cálculos. Este dispositivo puede ser una tablet, o un equipo fijo en el avión. Y en ambos casos hay posibilidad de atacarlo y mocificar parámetros.

La actividad satelital también se agregó a los temas de la Eko, con varias intervenciones de personal de Satellogic. En una de ellas, Juan Ignacio Bousquet entrevistó a Gerardo Richarte (Gera), CTO de Satellogic, quien presentó la empresa que, en la actualidad, con su fábrica en Uruguay donde se trabaja en hasta doce satélites simultáneamente, se dedica a la analítica geoespacial, y provee imágenes terrestres (y video) de muy alta resolución desde órbita, en diferentes rangos del espectro, para ayudar a gobiernos y empresas a tomar decisiones. También transportan en sus satélites instrumental provisto por los clientes.

Rojo, azul y violeta

Muchas de las actividades de esta Ekoparty estuvieron ordenadas bajo los conceptos de Red Team (atacantes), Blue Team (quienes preparan defensas) o Purple Team (coordinación de los anteriores) y además se prestó atención al Bug Bunty, la caza de recompensas, indicando cómo se debe entrenar un especialista en buscar y detectar vulnerabilidades, y cómo contactar, a través de organizaciones especializadas, con las empresas fabricantes del software afectado, a fin de obtener un pago a cambio de a información sobre la falla y una posible solución o parche.
También formó parte de la Ekoparty un paso por temas de ingeniería social, y de Fake News, con exhibición del uso de software destinado a auditar archivos de audio, fotografía o video a fin de verificar si han sido modificados. También se dieron elementos de esteganografía, a fin de conocer métodos para insertar textos ocultos en imágenes.

Otra actividad que tuvo mucho éxito en Ekoparty anteriores y se repitió en esta fue el Ekodating: se organizaron espacios de conexión, donde un asistente podía conocer a un representante de alguno de los patrocinadores de la Eko, compañías en su gran mayoría relacionadas con las diferentes facetas de la seguridad de IT.

De entre la lista de empresas se destacaron Banco Galicia, Dreamlab, Entel -Faraday, ESET, Naranja, Secureauth, Aquasec, Thales, Baufest y Base 4.

El sábado terminó la actividad de la muestra, con una despedida a cargo de los fundadores de Ekoparty y el numeroso personal que participó en la organización del evento, y con la invitación a quienes estaban en Buenos Aires, para encontrarse en un local nocturno.

Desafíos a la seguridad de Big Data

La seguridad de los macrodatos es el término colectivo para todas las medidas y herramientas que se utilizan para proteger tanto los datos como los procesos de análisis, de ataques, robos u otras actividades maliciosas que podrían dañarlos o afectarlos negativamente. Al igual que otras formas de seguridad cibernética, la variante de big data se ocupa de los ataques que se originan en las esferas en línea o fuera de línea.

Para las empresas que operan en la nube, los desafíos de seguridad de big data son mult facéticos.

Estas amenazas incluyen el robo de información almacenada en línea, ransomware o ataques DDoS que podrían bloquear un servidor. El problema puede ser aún peor cuando las empresas almacenan información sensible o confidencial, como información de clientes, números de tarjetas de crédito o incluso simplemente datos de contacto. En forma adicional, los ataques al almacenamiento de big data de una organización podrían causar graves repercusiones financieras, como pérdidas, costos de litigios y multas o sanciones.

Hay tres mejores prácticas principales de seguridad de big data o más bien desafíos que deberían definir cómo una organización configura su seguridad de BI.

El primer desafío son los datos entrantes, que podrían ser interceptados o corrompidos en tránsito. El segundo son los datos almacenados, que pueden ser robados o retenidos como rehenes mientras descansan en la nube o en servidores locales. El último son los datos que se están generando, que parece poco importante pero que podría proporcionar un punto de acceso para piratas informáticos u otras partes malintencionadas.
Estas tres preocupaciones deberían desempeñar un papel central en la creación de una filosofía de seguridad de big data flexible de extremo a extremo para cualquier organización.

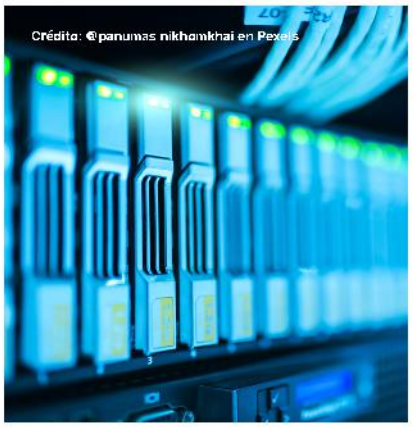
Implementar seguridad de Big Data

Una de las herramientas de seguridad más comunes es el cifrado, una herramienta relativamente simple que puede ser muy útil. Los datos cifrados son inútiles para los actores externos, como los piratas informáticos, si no tienen la clave para desbloquearlos. Además, el cifrado de datos significa que tanto en la entrada como en la salida, la información está completamente protegida.

La construcción de un firewall fuerte es otra herramienta útil de seguridad de big data. Los cortafuegos son eficaces para filtrar el tráfico que entra y sale de los servidores. Las organizaciones pueden prevenir los ataques antes de que ocurran mediante la creación de filtros sólidos que eviten a terceros o fuentes de datos desconocidas.

Finalmente, controlar quién tiene acceso root a las herramientas de BI y las plataformas de análisis es otra clave para proteger los datos. Desarrollar un sistema de acceso por niveles, puede reducir las oportunidades de un ataque.

> “Para las empresas que operan en la nube, los desafíos de seguridad de big data son multifacéticos.”



Caso de éxito: Noanet concientiza a su equipo en ciberseguridad

Con presencia en Jujuy y Tucumán, Noanet es una empresa dedicada al desarrollo de soluciones TIC que forma parte del grupo energético Fundación Noroeste.

Integrado por cinco compañías del norte argentino, la entidad cuenta con más de 1500 agentes. En 2012, el grupo lanzó una política de seguridad en donde las personas debían ser incluídas en un proceso de formación, algo que generó ciertos inconvenientes debido a la dispersión de los agentes con una cobertura de 700 km.

Para 2016 la empresa había generado formación personalizada, con grandes esfuerzos y horas dedicadas. Surgió entonces la oportunidad de buscar otras herramientas que facilitaran la tarea teniendo en cuenta los siguientes aspectos: la provisión de contenidos predefinidos sobre ciberseguridad; la posibilidad de personalizar los contenidos; el idioma adecuaco a las terminologías y usos propios de Argentina; y la autenticación con Active Directory.

SMARTFENSE, la respuesta a la necesidad de concientizar

Ante la necesidad de Noanet, SMARTFENSE garantizaba todos los requerimientos, además de brindar un portal de gestión multitenant, o de múltiples instancias, facilitando la gestión de varias organizaciones. Estas características fueron cruciales para que Noanet tomara la decisión final.

Se lanzaron campañas de simulación de Phishing y Ransomware para grupos reducidos y los resultados ayudaron a entender el estado inicial, comprobando que muchos colaboradores caían en las trampas. "Se pudo demostrar al directorio que se debía transitar un proceso de concientización", aseguran desde la empresa. "Luego, se lanzaron campañas con módulos interactivos y newsletters para exponer las políticas de seguridad y generar hábitos seguros".

En 2019, una vez alcanzado cierto nivel de madurez, Noanet logró formalizar un plan de concientización con acciones mensuales y momentos educativos que se presentaban a cada usuario que caía en un trampa.

Finalmente, gracias a la presentación de los resultados, se pudieron detectar comportamientos no deseados, así como identificar un entendimiento cada vez mayor sobre ciberseguridad. "Se nota que el usuario ya no cae en las trampas, aún cuando quizás pueda abrir el email. Los usuarios ya no hacen clic en los links o no descargan archivos maliciosos. Muchos se comunican con el área de IT para reportar los casos sospechosos. Esto muestra en forma directa la conducta responsable y los cambios de hábitos", expresa Jorge Gallardo, responsable de la Seguridad de la Información de Noanet

Jorge Gallardo

> “Es un gran placer para mí interactuar con una empresa tan profesional como SMARTFENSE porque se percibe la sensibilidad en el tema de Seguridad de la Información”

Riesgos de seguridad en aplicaciones para Celulares

Cuando se habla de aplicaciones móviles, debemos estar familiarizados con los probables riesgos de seguridad que podría enfrentar una aplicación móvil. Conocer los potenciales riesgos hace que sea más fácil evitar algunos errores, por ende escribir aplicaciones más seguras.

OWASP (Open Web Application Security Project) es una comunidad en línea de especialistas en seguridad que ha creado materiales de aprendizaje, documentación y soluciones disponibles gratuitamente para ayudar a crear aplicaciones web y móviles seguras. Entre otras, han compilado una lista de las diez amenazas más comunes para las aplicaciones móviles.

Las aplicaciones más populares en la tienda de aplicacicnes y de Google Play no deberían ser vulnerables a estos riesgos... ¿Correcto? Desafortunadamente lo son.

De estas aplicaciones, por lo menos la mitad tiene un almacenamiento de datos de forma insegura, y casi la misma cantidad de aplicaciones utiliza una comunicación insegura.

1. Uso inadecuado de la plataforma

Uso indebido de una función de la plataforma o falta de uso de los controles de seguridad de la plataforma. Se podría incluir:

- Intenciones de Android,
- Permisos de plataforma,
- Mal uso de TouchID,
- Hacer un mal uso del llavero,
- Mal uso de otros controles de seguridad.

2. Almacenamiento de datos inseguro

Cubre el almacenamiento de datos inseguro y la fuga de datos no intencionada. Se podría incluir:

- La opción de accesibilidad de llaves incorrectas, (p. ej., kSecAttrAccessibleWhenUnlocked contra kSecAttrAccessibleAlways),
- Protección de datos de archivo insuficiente, (p. ej. NSFileProtectionNone contra NSFileProtectionComplete),
- El acceso a recursos de privacidad cuando se utilizan estos datos de forma incorrecta.

3. Comunicación insegura

Se podría incluir:

- "el apretón de manos deficiente" o mejor dicho la "negociación débil", (p. ej., falta de fijación de certificado)
- Versiones de SSL incorrectas,
- Comunicación en texto claro de activos sensibles,
- HTTP en lugar de HTTPS.
- La comunicación no se cifró y no se autenticó correctamente.

4. La autenticación insegura

Problemas para autenticar al usuario final o mala gestión de la sesión.

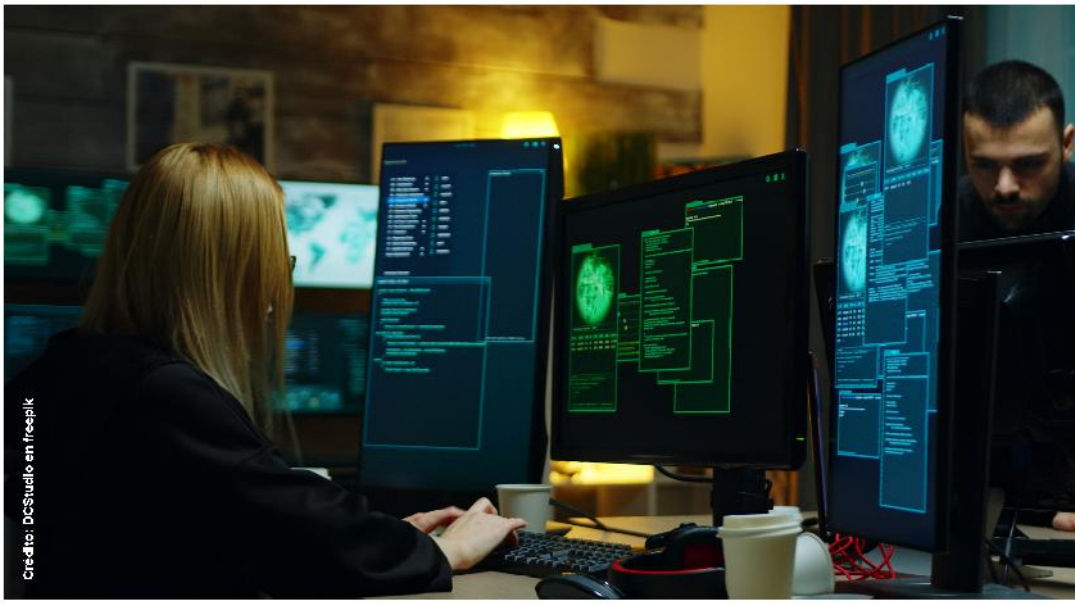
- no identificar al usuario en absoluto cuando debería ser necesario,
- no mantener la identidad del usuario cuando se requiere,
- debilidades en la gestión de sesiones.

5. Criptografía insuficiente

En estos riesgos, de alguna forma la criptografía implementada para la aplicación fue insuficiente. Por ejemplo, el programador podría haber usado un algoritmo criptográfico desactualizado; o haber escrito un algoritmo vulnerable, personalizado.

Estos riesgos pueden generar que las solicitudes, entre la aplicación y el servidor, puedan interceptarse y solicitar otras.

> Las aplicaciones más populares en la tienda de aplicaciones y de Google Play no deberían ser vulnerables a estos riesgos… ¿Correcto? Desafortunadamente lo son.



6. Autorización insegura

Se podría incluir:
- Fallas o errores en la autorización, (por ejemplo, decisiones de autorización en el lado del cliente, navegación forzada, etc.),
- La capacidad de ejecutar funciones con privilegios excesivos,
- Es distinto a los riesgos o problemas de autenticación (p. Ej., Inscripción de dispositivos, identificación de usuarios, etc.).

7. Calidad del código del cliente

El "Catch-all" para problemas de implementación a nivel de código en el cliente móvil. Se podría incluir:
- Desbordamientos de búfer,
- Formatear las vulnerabilidades de las cadenas,
- Diversos errores a nivel de código donde la solución es reescribir algún código que se está ejecutando en el dispositivo móvil.

8. Manipulación de código

En estos riesgos se podrían incluir:
- El parcheo binario,
- La modificación de recursos locales,
- El método de enganche y swizzling,
- La modificación de memoria dinámica.

9. Ingeniería inversa

Se podría incluir un análisis binario para identificar su:
- Código fuente,
- Bibliotecas,
- Los algoritmos,
- Demás activos, etc

La ingeniería inversa facilita la explotación de otras vulnerabilidades en la aplicación. Puede revelar información sobre servidores backend, constantes y cifrados criptográficos y propiedad intelectual.

10. Funcionalidad extraña

Se podrían indicar, por ejemplo:
- La funcionalidad de "puerta trasera oculta",
- Demás controles de seguridad de desarrollo de índole interna, no destinados al entorno de producción.

Conclusiones

Es necesario, como especialistas de seguridad de la información, tener en cuenta estos riesgos al desarrollar una aplicación móvil. Se recomienda profundizar la lectura de las mejores prácticas elaboradas por OWASP.

MEJORES PRÁCTICAS PARA EVALUACIONES DE RIESGOS DE TERCEROS

Los contratistas externos, especialmente los proveedores de tecnología, están cada vez más integrados en todas las funciones empresariales y en todos los sectores, incluidas las funciones core. La subcontratación de trabajos hace posible que las empresas tengan capacidad de respuesta y sean ágiles en un entorno disruptivo. Pero los terceros también introducen riesgos, en toda la cadena de suministro.

> “Para producir evaluaciones de terceros más eficaces y agilizar el proceso de evaluación, es útil aplicar las lecciones de otras organizaciones.”

El riesgo de terceros es único, y se requiere una evaluación del riesgo de terceros para garantizar que se cumple la diligencia debida, no sólo en el momento de la incorporación, sino de forma continua. Además, las nuevas normas de cumplimiento exigen una documentación continua que justifique la renovación de la relación contractual.

Una plantilla de evaluación de riesgos es útil para guiar el proceso de auditoría. Hemos elaborado la siguiente plantilla de nueve pasos, a partir de las lecciones aprendidas de nuestra experiencia ayudando a clientes de éxito a establecer y ejecutar programas de evaluación de riesgos.

Para producir evaluaciones de terceros más eficaces y agilizar el proceso de evaluación, es útil aplicar las lecciones de otras organizaciones.

A continuación, se exponen nueve formas basadas en la experiencia para poner en marcha un programa de evaluación de terceros racionalizado.

1. Comprenda su apetito de riesgo: Los organismos reguladores suelen indicarle a quién debe evaluar y con qué frecuencia. Sin embargo, la determinación de las preguntas que hay que hacer en la evaluación suele dejarse en sus manos. ¿Cómo se decide? ¿Cómo pueden afectar los resultados a las políticas y procedimientos de la empresa? Construya y pruebe su programa de evaluación de terceros internamente utilizando cuestionarios que reflejen el apetito de riesgo de su empresa.

2. Clasifique a sus proveedores: Desarrolle un método para clasificar a los proveedores con el fin de identificar a los terceros que están dentro del ámbito de aplicación y que requieren evaluaciones. Esto ayuda a garantizar que no se evalúa a los terceros innecesariamente o que se no se pierde a los que suponen un riesgo para su organización.

3. Mejorar los datos recopilados: La obtención de datos es uno de los mayores retos en la gestión del riesgo de terceros y una evaluación de alta calidad es clave. Para mejorar la calidad de sus cuestionarios, comience con una evaluación ampliamente aceptada, como el cuestionario de recopilación de información estándar (SIG) de Shared Assessments y adáptelo a sus necesidades y procesos empresariales específicos.

4. Facilite la gestión de las evaluaciones: Si hace negocios con una multitud de terceros, necesita una forma de facilitar la gestión de las evaluaciones. Acelere el proceso de evaluación dando a todos los terceros una evaluación de bajo umbral con unas pocas preguntas


Crédito: navexglobal.com

de marcación. Para todos los terceros marcados, envíe una evaluación de mayor nivel y profundidad para la debida diligencia sobre el riesgo. Es un proceso más fácil y a menudo más completo para evaluar a los terceros.

5. Prepárese para el mundo de la evaluación: Las evaluaciones son algo que se hace de forma continua y a menudo con los mismos proveedores. Si su motor de evaluación rellena previamente los datos, la entidad que está evaluando sólo tiene que ocuparse de los cambios. Es menos trabajo para ellos y para usted, e incluso puede mejorar el índice de respuesta.

6. Evalúe el rendimiento, no sólo el riesgo: Con la plataforma adecuada, puede cargar los acuerdos de nivel de servicio (SLA) y hacerlos parte del proceso de evaluación. Compare los datos de la evaluación con los acuerdos de nivel de servicio y utilice el análisis para proporcionar información al tercero, aprovéchelo en la renovación del contrato o utilícelo para apoyar el cambio a otro proveedor de servicios.

7. Reevaluar en función de la ampliación de la oferta del tercero: Cuando los terceros amplían sus servicios a su empresa, cambia su perfil de riesgo. Una de las mejores formas de abordar esto es evaluar periódicamente a los terceros para ver si hay cambios y actualizar los perfiles de riesgo en consecuencia. De este modo, su perfil de riesgo de terceros está siempre actualizado.

8. Mire más allá de los riesgos financieros con terceros: La mayoría de las organizaciones evalúan a los terceros para gestionar el riesgo financiero. A veces, los pequeños riesgos abren la puerta a consecuencias más graves. La pérdida de ingresos puede causar problemas, pero es recuperable. Perder la reputación puede no serlo.

9. La dependencia crea un riesgo de continuidad del negocio: Cualquier tercero puede ser un riesgo para la continuidad del negocio. La prueba de fuego es que, si su servicio se detiene, interrumpiría el suyo. Tal vez sea el proveedor de servicios de TI o un proveedor con un papel c ave en la cadena de suministro. Los terceros de los que depende en gran medida pueden plantear riesgos de continuidad del negocio que pueden identificarse mediante una evaluación de riesgos.

Utilice estos nueve consejos cuando ponga en marcha o perfeccione su programa de evaluación de riesgos para que sea más eficaz y satisfaga los requisitos.

Fuente: Mike Ogden en NAVEX Global (https://www.navexglobal.com/blog/article/third-party-risk-assessment-nine-tips/)

Lo que le habría ocurrido a Facebook, WhatsApp e Instagram

La interrupción del 4 de octubre pasado de Facebook es, por mucho, la más larga y extrema en años. Más o menos desde las 9 a.m. en la costa oeste de Estados Unidos, donde tiene su sede el gigante social, Facebook, WhatsApp, Instagram y Facebook Messenger parecieron desaparecer de Internet. La interrupción continuó hasta el cierre del mercado, y las acciones de la compañía cayeron alrededor de un 5% por debajo de su precio de apertura el lunes. A media tarde, los servicios comenzaban a reanudarse después de que, según se informa, Facebook envió un equipo a su centro de datos de Santa Clara para "restablecer manualmente" los servidores de la empresa.

> "Facebook "desapareció de Internet en una ráfaga de actualizaciones de BGP" en una ventana de dos minutos."

Pero lo que hace que la interrupción sea única es lo extremadamente desconectado que estaba Facebook.

Por la mañana, Facebook envió un breve tweet para disculparse de que "algunas personas tienen problemas para acceder a nuestras aplicaciones y productos". Luego, surgieron informes de que la interrupción estaba afectando no solo a sus usuarios, sino a la propia empresa. Según los informes, los empleados no pudieron ingresar a sus edificios de oficinas, y el personal lo llamó un "día de nieve": no pudieron realizar ningún trabajo porque la interrupción también afectó a las aplicaciones de colaboración interna.

Aunque Facebook ha comentado que la causa de la interrupción se debió a un "simulacro de tormenta" (desconectan partes de la Red para simular fallas importantes), los expertos en seguridad dijeron que la evidencia apuntaba a un problema con la red de la compañía que cortó a Facebook de Internet en general y también a sí mismo.

Las primeras señales de problemas fueron alrededor de las 8:50 A.M. en California, según Cloudflare, quien dijo que Facebook "desapareció de Internet en una ráfaga de actualizaciones de BGP" en una ventana de dos minutos. Se estaba refiriendo a BGP, o Border Gateway Protocol, el sistema que utilizan las redes para descubrir la forma más rápida de enviar datos a través de Internet a otra red.

¿Fue BGP?

El Border Gateway Protocol es un mecanismo que permite intercambiar información de enrutamiento entre sistemas autónomos en Internet. Es decir, permite que una red como la de Facebook "anuncie" su presencia a otras redes que forman parte de la web.

Pensando en que Internet es una red de redes y que cada red está constituida por gigantescas listas o rutas de acceso, llamadas ASN, entonces debe haber un protocolo que haga posible que éstas se conecten entre sí. Esto con el fin de que los usuarios accedan finalmente a los paquetes a los que se supone están destinados los enrutamientos. Para ello existe el protocolo BGP.

Las actualizaciones fueron específicamente retiros de la ruta BGP. Básicamente, Facebook había enviado un mensaje a Internet de que estaba cerrado al público, como cerrar el puente levadizo de su castillo. Sin ninguna ruta a la red, Facebook estaba básicamente aislado del resto de Internet, y debido a la forma en que está estructurada la red de Facebook, los retiros de la ruta tam-

bién eliminaron WhatsApp, Instagram, Facebook Messenger y todo lo que se encuentra dentro de sus muros digitales.

Unos minutos después de que se retiraron las rutas BGP, los usuarios comenzaron a notar problemas. El tráfico de Internet que debería haber ido a Facebook esencialmente se perdió en Internet y no llegó a ninguna parte.

Los usuarios empezaron a notar que sus aplicaciones de Facebook habían dejado de funcionar y que sites no se cargaban y reportaron tener problemas con el DNS o el sistema de nombres de dominio, que es otra parte fundamental del funcionamiento de Internet. Sin una forma de acceder a los servidores de Facebook, las aplicaciones y los navegadores seguirían provocando lo que parecían errores de DNS.

No se sabe exactamente por qué se retiraron las rutas BGP. BGP, que ha existido desde el advenimiento de Internet, puede ser manipulado y explotado maliciosamente de formas que pueden provocar interrupciones masivas.

Lo más probable es que una actualización de la configuración de Facebook haya salido terriblemente mal y su falla se haya extendido por Internet. Un hilo de Reddit ahora eliminado de un ingeniero ce Facebook describió un error de configuración de BGP mucho antes de que fuera ampliamente conocido. Por más de que la solución puede ser simple, la recuperación puede extenderse desde las próximas horas hasta los días siguientes debido al funcionamiento de Internet. Los proveedores de Internet suelen actualizar sus registros DNS cada pocas horas, pero pueden tardar varios días en propagarse por completo.

"A la gran comunidad de personas y empresas de todo el mundo que dependen de nosotros: lo sentimos", tuiteó Facebook alrededor de las 3:30 p.m. hora local. "Hemos estado trabajando arduamente para restaurar el acceso a nuestras aplicaciones y servicios y nos complace informar que ahora están volviendo a estar en línea. Gracias por aguantarnos ".

Pero... tal vez, ¿podría haber ocurrido otra cosa...?

Ataques DDOS a bancos

En términos informáticos, un ataque DoS (Denegación de servicio) o DDOS (Denegación de servicio distribuida) consiste en esfuerzos para interrumpir los servicios de un recurso específico de red, dejándolo temporalmente no disponible para sus usuarios.

Estos ataques generalmente tienen como objetivo detener los servicios de un host conectado a Internet, sin embargo, algunos intentos también pueden tener como objetivo una determinada máquina.

Los ataques de denegación de servicio de distribución difieren de los ataques de denegación de servicio en la forma en que se lanzan y sus lanzadores. Los ataques DDoS pueden ser enviados por varias personas, mientras que los ataques DoS los envía un sistema o una sola persona.

Según el **informe Informe Global de Amenazas DDoS** de AWS, la frecuencia global de ataques DDoS creció un 39% entre H1 2018 y H1 2019. Una vez más, vimos un crecimiento asombroso del 776% en ataques entre 100 Gbps y 400 Gbps.

No hay áreas fijas donde puedan ocurrir estos ataques; se dirigen a industrias de todo el mundo. Los ataques DDoS ocurren principalmente cuando el servidor al que se dirige está inundado de solicitudes de comunicación de atacantes o una red de bots.

El servidor que no puede controlar más las solicitudes HTTP, finalmente se apaga, lo que hace que sus servicios no estén disponibles para los usuarios legítimos por igual. Estos ataques normalmente no causan ningún tipo de daño al sitio web o al servidor, pero lo desactivan temporalmente.

Las aplicaciones de este método se han expandido mucho y ahora se utilizan con fines más maliciosos; como encubrir fraudes y disuadir a los paneles de seguridad, etc.

Ataques DDoS recientes a bancos

El año pasado, los principales nombres de "American Banking" fueron blanco de uno de los mayores y más complicados conjuntos de ataques DoS distribuidos. Al principio, las víctimas fueron Wells Fargo, United States Bancorp, JPMorgan Chase, Bank of America y la PNC de regreso.

Posteriormente, los sitios web comenzaron a fallar con frecuencia, las personas no pudieron realizar transacciones debido a que los servidores estaban

> “Los ataques demostraron que tener un dispositivo de mitigación o un firewall mantenido no será suficiente.”

inactivos y luego varios expertos en TI comenzaron a entrar en pánico. A continuación se presentan algunos puntos para considerar si se tienen en cuenta estos ataques.

• Los bancos más grandes, incluidos los nombres mencionados anteriormente, tienen el dinero para mantener la protección básica contra DDoS, pero ni siquiera sus medidas pudieron detener los ataques del año pasado. Con sus soluciones de seguridad, es probable que puedan detener el 90% de los ataques, menos de 1 Gigabyte por segundo de tamaño.

• Pero los ataques dirigidos a estos bancos van más allá de este límite, lo que los hace incapaces de controlarlo. Sin embargo, los bancos más pequeños con una protección DDoS mínima o nula pueden ser derribados por impactos mucho más pequeños.

• Un ataque DDoS de tamaño moderado puede paralizar sus funciones y operaciones. Para estos bancos locales vulnerables, las soluciones de terceros, como los servicios a pedido, son una buena apuesta.

Los ataques demostraron que tener un dispositivo de mitigación o un firewall mantenido no será suficiente. Para hacer frente a los ataques DDoS actuales, necesitamos un mayor ancho de banda, nuevas tecnologías y un personal de protección DDoS capacitado.

Con este combo, es posible que podamos detener los ataques basados en enlaces DNS y HTTP, junto con los impactos de la capa de aplicación que ahora se están volviendo tan populares.

Qué es el Reglamento de ciberseguridad del NYDFS

El Reglamento de ciberseguridad del NYDFS (23 NYCRR 500) es un nuevo conjunto de reglamentos del Departamento de Servicios Financieros de NY (NYDFS) que impone requisitos de ciberseguridad a todas las instituciones financieras cubiertas.

Las reglas incluyen 23 secciones que describen los requisitos para desarrollar e implementar un programa de ciberseguridad efectivo, que requieren que las instituciones cubiertas evalúen sus riesgos de ciberseguridad y desarrollen planes para abordar de manera proactiva esos riesgos. El Reglamento de ciberseguridad del NYDFS incluyó un proceso de implementación por fases, con cuatro fases distintas que permitieron a las organizaciones implementar políticas y controles más sólidos.

Quién está cubierto por NYDFS

El Reglamento de seguridad cibernética de NYDFS se aplica a todas las entidades que operan bajo licencia, registro o carta de DFS o que están reguladas por DFS, así como, por extensión, proveedores de servicios de terceros no regulados para entidades reguladas. Ejemplos de entidades cubiertas incluyen:

- Bancos autorizados por el estado
- Prestamistas autorizados
- Banqueros privados
- Bancos extranjeros autorizados para operar en Nueva York
- Compañías hipotecarias
- Las compañías de seguros
- Proveedores de servicio

Existen excepciones limitadas al Reglamento de seguridad cibernética del NYDFS. Las organizaciones que emplean a menos de 10 personas, produjeron menos de U$S 5 millones en ingresos brutos anuales de las operaciones de Nueva York en cada uno de los últimos tres años o tienen menos de U$S 10 millones en activos totales al final del año están exentas de ciertos requisitos del Reglamento.

Cómo funciona el Reglamento de ciberseguridad del NYDFS

El Reglamento de seguridad cibernética del NYDFS funciona imponiendo reglas estrictas de seguridad cibernética a las organizaciones cubiertas, incluida la entrega de un plan de seguridad cibernético detallado, la designación de un director de seguridad de la información (CISO), la promulgación de una política integral de seguridad cibernética y el inicio y mantenimiento de una Sistema de reporte continuo para eventos de ciberseguridad. Todos estos componentes se componen de varias subregulaciones y requisitos.

> “El Reglamento de seguridad cibernética del NYDFS funciona imponiendo reglas estrictas de seguridad cibernética a las organizaciones cubiertas, incluida la entrega de un plan de seguridad cibernético detallado”

Requisitos de la regulación de ciberseguridad de NYDFS

Un programa de ciberseguridad que cumpla con el nuevo Reglamento de ciberseguridad del NYDFS cumplirá varios requisitos clave, alineados con el Marco de ciberseguridad del NIST:

- Identificar todas las amenazas de ciberseguridad, tanto internas como externas.
- Emplear infraestructura de defensa para protegerse contra esas amenazas.
- Utilizar un sistema para detectar eventos de ciberseguridad.
- Responder a todos los eventos de ciberseguridad detectados.
- Trabajar para recuperarse de cada evento de ciberseguridad.
- Cumplir con varios requisitos para informes regulatorios.

Diseño de la política de ciberseguridad

La fase inicial del Reglamento de seguridad cibernética de NYDFS entró en vigor el 15 de febrero de 2018 y requiere que las organizaciones cubiertas desarrollen una política de seguridad cibernética, incluido un plan de respuesta a incidentes que incluya notificaciones de violación de datos dentro de las 72 horas. La política debe abordar las inquietudes en consonancia con las mejores prácticas de la industria y las normas ISO 27001. En particular debe cubrir:

- Seguridad de información
- Controles de acceso
- Planificación de recuperación ante desastres
- Seguridad de sistemas y redes
- Privacidad de los datos del cliente
- Evaluaciones periódicas de riesgos

Procedimientos de reporte

La segunda fase, que entró en vigor el 1° de marzo de 2018, requiere que los CISO preparen un informe anual que incluya:

- Las políticas y procedimientos de ciberseguridad de la organización.
- Los riesgos de seguridad de la organización
- La eficacia de las medidas de ciberseguridad existentes en la organización.

Las instituciones cubiertas deben desarrollar e implementar un programa de ciberseguridad que evalúe continuamente las vulnerabilidades, que no solo informa el informe anual, sino que también permite a la organización desarrollar respuestas proactivas a las amenazas.

Desarrollo del programa

La fase tres, que entró en vigor el 3 de septiembre de 2018, requiere que las instituciones cubiertas cuenten con un programa integral de ciberseguridad que contenga varios elementos clave, que incluyen:

- Una pista de auditoría que refleja las actividades de respuesta y detección de amenazas
- Documentación escrita de procedimientos, estándares y pautas para aplicaciones internas, así como procedimientos para evaluar aplicaciones de terceros.
- Documentación detallada de la política de retención de datos, incluida la forma en que se elimina la información personal no pública.
- Cifrado y otras medidas de control de seguridad sólidas

Seguridad de terceros

El último requisito restante entró en vigencia a partir del 1° de marzo de 2019. Este requisito establece que las instituciones cubiertas deben finalizar sus políticas con respecto a cualquier tercero al que se le pueda otorgar permisos para acceder a los sistemas y archivos cubiertos por la regulación. Las instituciones financieras cubiertas deben desarrollar una política escrita para la seguridad de terceros que señale:

- Evaluación de riesgos de proveedores de servicios externos
- Los requisitos de seguridad de la institución financiera cubierta de los proveedores de servicios externos que deben cumplirse para realizar negocios con esa entidad.
- Procesos para evaluar la efectividad de las prácticas de seguridad de un proveedor de servicios externo
- Evaluaciones periódicas de políticas y controles de terceros.

La iniciativa española #LadyHacker

Se calcula que la pandemia de coronavirus ha acelerado la digitalización entre 5 y 10 años. Esto significa que el sector tecnológico será el que más empleo neto genere en los próximos años, pero la brecha de género en este sector es una realidad que no se puede ignorar.

El campo de las carreras STEM (Ciencia, Tecnología, Ingeniería y Matemáticas), a diferencia de otros sectores, sigue siendo una carrera de obstáculos para las mujeres, y esto lo sienten las niñas desde una edad temprana. Se calcula que sólo el 30% de las mujeres del mundo estudian carreras STEM. Este porcentaje se reduce al 3% en las carreras de tecnologías de la información y la comunicación o al 8% en las carreras de ingeniería.

Esto se debe a varias razones; el entorno es muy influyente, además de tener referencias. Además, las mujeres que trabajan en campos STEM tienden a cobrar menos que sus homólogos masculinos y, lo que es más grave, la probabilidad de que abandonen sus carreras es muy alta, estimada en torno al 35% en Estados Unidos.

Múltiples informes muestran cómo las chicas están predispuestas, decepcionadas y desinteresadas por la tecnología.

La diversidad nos beneficia a todos: #LadyHacker

COVID-19 ha confirmado las fortalezas que las mujeres aportan en términos de liderazgo y ha demostrado que la diversidad de género, en los equipos y en la toma de decisiones, conduce a mejores resultados para todos. Según un reciente estudio de McKinsey, la igualdad de género añadiría 13 billones de dólares a la economía mundial de aquí a 2030.

Afortunadamente, no todo son datos negativos. Los niños, gracias a COVID-19, han podido ver por sí mismos la relevancia de la tecnología en su vida familiar, en la escuela, en los medios de comunicación, en las películas y en la literatura. Han empezado a ver mujeres de éxito en el campo de la investigación y la ciencia, epidemiólogas y científicas de la salud, analistas de datos y matemáticas. Y al ver a estas mujeres llegar a la cima, los niños ven el mundo con mayor respeto por todos e igualdad.

> “COVID-19 ha confirmado las fortalezas que las mujeres aportan en términos de liderazgo”

Promover la vocación tecnológica entre las niñas a través de acciones de sensibilización y orientación impartidas por mujeres profesionales del mundo de la investigación, la ciencia y la tecnología es precisamente el objetivo de la iniciativa global de Telefónica Tech #LadyHacker. Porque es importante ayudar a las niñas a cumplir sus sueños y demostrarles que no hay profesión imposible. Demostrarles que es posible llegar más lejos y mejor, aunque todavía queda mucho camino por recorrer.

Fuente: Sandra Tello en Think Big (https://business.blogthinkbig.com/the-covid-crisis-and-diversity-in-the-technology-field/)

SMARTFENSE

Nueva imagen, Misma esencia.

Gestiona el riesgo
más relevante
con un proceso de
Hardening de usuarios

SitioSimple

Crear tu página web es tan rápido como leer esta publicidad

Hoy podés tener tu página web o tienda online ¡sin programar y en menos de una hora!

- Más de 200 plantillas pre-diseñadas
- 0% comisiones por venta
- Lista para celulares
- Optimizada para Google
- Múltiples opciones de pago y envíos
- En pesos argentinos

ESCANEÁ
Y EMPEZÁ GRATIS

DonWeb.com