<!DOCTYPE markdown>

El escalamiento del ransomware

En Colombia, el 2023 ha sido el año del secuestro de información por ataques con *ransomware*. Desde empresas privadas importantes para el sector de la salud hasta entidades de carácter público como la Fiscalía General de la Nación, el Metro de Medellín y Empresas Públicas de Medellín, las víctimas de este tipo de ataque no han dejado de aumentar.

La última semana se presentó un ataque a la cadena de suministro, es decir, a los proveedores del servicio de *nube*. En este caso el afectado fue IFX Networks, uno de los principales proveedores del Gobierno y las grandes empresas privadas en Colombia. Este ataque, que además se propagó por países como Chile, Argentina y Panamá, es quizás uno de los más grandes que se han perpetrado al día de hoy en toda la región.

A pesar del alcance regional, el Gobierno de Colombia ha resultado especialmente afectado. Durante más de una semana, los sistemas de la rama judicial y sistemas de importancia crítica para la prestación de los servicios de salud en el país han estado funcionando con problemas, evidenciando que el proceso de restauración de los mismos no ha funcionado a la altura del reto.

Ante la gravedad de este ataque, hay que destacar el hermetismo de IFX. Esta empresa ha respondido entregando poca información a los medios y su cooperación con el Gobierno también puede considerarse deficiente, dada la evidenciada lentitud en la restauración del funcionamiento de los sistemas de la nación dependientes de sus servicios. Más allá de todos los riesgos implicados en que la información de los Colombianos se filtre a Internet por el no pago del secuestro, este ataque evidencia una serie de problemas estructurales en la manera como las entidades gubernamentales e incluso la empresa privada enfrentan las amenazas de ciberseguridad que se ciernen hoy sobre la red:

1. La confianza ciega en el software empresarial que nos ha vendido la publicidad
    - Es el caso de VMWARE específicamente. Desde principio del año varios expertos en seguridad han estado liberando información sobre riesgos, amenazas y problemas de seguridad en toda esta plataforma, desde sus ESXI a toda la capa de aplicación que hace funcionar los cluster de virtualización. Casos como el de IFX y MGM evidencian las malas practicas que suelen tener estas empresas en el manejo de parches de seguridad sobre sus plataformas, lo que causa un riesgo muy alto para sus usuarios. Las empresas y los gobiernos suelen estar convencidos de que al utilizar este tipo de software van a tener mejor soporte e incluso mejor seguridad, pero lo que realmente pasa es que entran a formar parte de una cadena de tercerización de servicios que termina impactando la seguridad de sus sistemas y la eficiencia de sus operaciones, con consecuencias económicas y políticas en el caso de los estados.
2. El IaaS y el PaaS en gobiernos están sobrevalorados. La necesidad de la soberanía en ciberseguridad
    - El caso del impacto de la falla de IFX en las plataformas del Gobierno de Colombia demuestra que la tercerización de todos los servicios de tecnología, más que una solución, representa un riesgo grave para los estados. Incluso puede implicar problemas de seguridad nacional, ya que si cae la empresa a la que un gobierno ha confiado todas sus plataformas, sus respaldos de información y hasta la seguridad perimetral e interna, se vuelve inevitable que todos los sistemas caigan y que partes vitales del gobierno dejen de funcionar. Corriendo el riesgo a largo plazo, además, de que haya pérdidas de

información valiosa e irrecuperable, en manos de terceros.
    - Las entidades del Estado, por tanto, deberían tener un control absoluto sobre su plataforma tecnológica —una función que podría entenderse dentro de la obligación estatal de proteger la soberanía nacional—; y deberían tener la capacidad de saltar de un proveedor a otro en caso de ser necesario o, incluso, de tener sus propios datacenter de desborde en el caso de perder a los proveedores en la nube.
    - El problema, por supuesto, es que esto implica contratar profesionales con la capacidad necesaria para estas tareas. Algo que, lamentablemente, es difícil debido a los bajos salarios que puede pagar el estado colombiano. En el estado actual de cosas, los profesionales de muchas entidades estatales tienen pocos conocimientos en ciberseguridad y en tecnología, limitando su capacidad de actuación a la función administrativa y la contratación de servicios.
3. La fragilidad de las certificaciones
    - Todas las empresas que hoy en día se presentan como grandes operadores, tal el caso de IFX, han invertido grandes sumas de dinero en certificaciones de seguridad como la ISO27001 o la ISO27002. Además, se afirman ratificadas por grandes empresas de seguridad como Fortinet y exhiben el ser socias prioritarias de proveedores como VMWARE. Sin embargo, cuando una situación como la que se presentó en la ultima semana llega, se demuestra que todas estas certificaciones y ratificaciones no son más que parte de un un modelo de negocios que no ofrece garantía ninguna a los gobiernos y sus naciones.
    - Cualquier empresa con el capital necesario puede pagar las certificaciones que la acrediten para ser prestadora de servicios a entidades gubernamentales. La pregunta que nos debemos hacer es qué tanto se validan la aptitud de las empresas más allá de haber presentado la documentación necesaria. ¿Se verifica la capacidad e idoneidad de las personas encargadas de la plataforma? ¿Se realiza un seguimiento a la aplicación de las buenas practicas sugeridas por los fabricantes? ¿Cómo se garantiza que se están siguiendo las medidas de seguridad necesarias para prevenir y mitigar ataques como el *ransomware*?
    - Otro gran problema es la calidad de los programas de entrenamiento en tenmas de seguridad a los empleados de todos los niveles en las empresas y entidades. Según algunos de los contratos que se han revisado, IFX debía impartir entrenamientos de seguridad para varias entidades. ¿Quién verifica su calidad y que las personas realmente adquieran y practiquen los conocimientos necesarios en su labor diaria?

En general, lo que vemos en casos como el de la propagación de *ransomware* en la cadena de suministro son un conjunto de malas prácticas y responsabilidades entre proveedor y cliente que no se cumplen a cabalidad. La responsabilidad de la infección cae en un área gris, ya que estos malware se pueden propagar por un simple correo que alguien abrió, ejecutando algo que le enviaron por medio de una campaña de phishing; o por la explotación de una vulnerabilidad en un sistema al que no se le ha aplicado el ultimo parche de seguridad, ya sea sobre un software a nivel de usuario o de una plataforma que tiene acceso directo a los hipervisores del proveedor, como es el caso de IFX y MGM en donde los agentes que corren en las maquinas virtuales permitieron la propagación del malware por medio de la explotación de una vulnerabilidad conocida que no había sido parchada.

Una de las soluciones a varios de los problemas mencionados desde el punto de vista técnico es fomentar la idea de que en el mundo empresarial y estatal el software 100% libre tiene un rol muy importante para la mitigación de riesgos de seguridad. Por un lado, el dinero ahorrado en licencias podría invertirse en personal mejor capacitado, por otro lado, la capacidad que ofrece el software libre de conocer el código hace que sea mas fácil de auditar su implementación, además de que los ciclos de implementación de parches y mejoras de seguridad son mucho más rápidos que en

plataformas de uso privativo.

Si bien el software libre trae muchos retos desde el punto de vista de la usabilidad y el aprendizaje para las personas que deben implementarlo, al final de la curva de aprendizaje las ventajas superan el costo de dificultad, dada la posibilidad de personalizar y adaptar el software a la medida de las empresas y su plataforma.

Con esto no quiero decir que sea la solución única a problemas como el *ransomware*, ya que la solución a este problema tiene un componente humano muy fuerte que implica el entrenamiento de nuestros colaboradores en temas de seguridad, para que nuestros sistemas sigan buenas practicas. No obstante, lo cierto es que el nivel de seguridad de los sistemas de empresas y gobiernos se pueden mejorar bastante usando tecnologías libres, no solo porque se pueden amoldar a las necesidades específicas, sino porque tal amoldabilidad se deriva de un factor fundamental: la posibilidad de poseer el control completo del sistema y su funcionalidad, algo que en el caso de los estados juega un papel directo en el mantenimiento de su seguridad nacional y soberanía.

Referencias

- https://osintcorp.net/hackers-behind-mgm-cyberattack-thrash-the-casinos-incident-response/
- https://osintcorp.net/hackers-behind-mgm-cyberattack-thrash-the-casinos-incident-response/
- https://csirt.gob.cl/noticias/10cnd23-00108-02/
- https://muchohacker.lol/2023/09/pequena-y-mediana-empresa-victimas-invisibles-de-incidente-digital-de-ifx/
- https://muchohacker.lol/2023/09/lista-de-sitios-web-con-el-dominio-go-co-que-estarian-afectados-por-ataque-ransomware-a-ifx-network/
- https://muchohacker.lol/2023/09/medidas-de-seguridad-basicas-para-no-expertos-que-se-deben-tener-en-cuenta-debido-al-ataque-a-ifx-networks/

From:
https://wiki.calleancha.co/ - **Calle Ancha**

Permanent link:
https://wiki.calleancha.co/edicionalvuelo/rasomware

Last update: **2023/09/30 10:31**