INFORME DE LA LÍNEA DE TRABAJO ANTICIPACIÓN DE TECNOLOGÍAS FUTURAS EN CIBERSEGURIDAD

SEGURIDAD Y PRIVACIDAD EN ENTORNOS DISTRIBUIDOS (EDGE & FOG COMPUTING)

COMISIÓN DE CIBERSEGURIDAD DE AMETIC

MAYO 2023

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

aniversario 50 1973 - 2023

Introducción

Los conceptos ***Edge Computing*** y ***Fog Computing*** llevan la tecnología y servicios *Cloud* (datos, computo, almacenamiento y aplicaciones) hacia el borde de la red y los dispositivos finales (*end-points*), proporcionando al usuario unas mejores prestaciones en cuanto a latencia, *jitter*, etc., en definitiva, mejorando la calidad del servicio (QoS). Por otro lado, este desplazamiento de la tecnología y los servicios hace que pasemos a tener entornos descentralizados, donde se utilicen redes inalámbricas, los nodos puedan tener movilidad, haya menos protección hardware, los recursos computacionales y de memoria estén limitados, y no exista un perímetro claro que proteger. El uso de tecnologías inalámbricas relaciona la ciberseguridad de estos entornos con la vulnerabilidad de esas redes.

Los ámbitos de seguridad que más preocupan en este tipo de entornos son cuatro: el control de acceso, la autenticación de la identidad, la securización de la información (confidencialidad e integridad de datos), y la protección de la privacidad. Sin embargo, es importante trabajar en soluciones que permitan una experiencia de usuario optima y segura en el proceso de autenticación, identificación y acceso, el interface principal utilizado por el usuario para acceder a los sistemas, con capacidades de detección de amenazas y respuesta ante esas situaciones, todo ello teniendo en cuenta la complejidad del ecosistema, la falta de recursos en los dispositivos, y el "empoderamiento digital" del usuario que utiliza la tecnología, pero que en la mayoría de los casos desconoce cómo funciona. En este sentido la aplicación de inteligencia artificial desempeñará un papel importante.

Expectativas (ventajas)

Estos nuevos paradigmas proporcionarán mejoras significativas en múltiples servicios existentes y la resiliencia de los mismos permitiendo a la vez que las infraestructuras puedan soportar nuevos servicios y tecnologías más demandantes de inmediatez, capacidad u otras características. De esto se van a aprovechar la Industria 4.0, las *Smart Cities*, la movilidad autónoma, etc., permitiendo que se consigan muchos de los retos tecnológicos que se tienen por delante.

Obstáculos (inconvenientes, carencias de desarrollo)

Al igual que otros paradigmas o tecnologías que utilizan y/o están expuestas a Internet, *Fog Computing* y *Edge Computing* son propensos a ciertas amenazas de seguridad y privacidad. Además, la distribución de este tipo de entornos también hace que existan otras amenazas que tener en cuenta. A continuación, se explican algunos ejemplos:

- **Ataque de canal lateral (*Side-channel Attack*)**: se saltan las medidas criptográficas del dispositivo gracias a la recopilación de información sobre el algoritmo criptográfico implementado.
- **Confabulación (*Collusion*)**: dos o más grupos confabulan para engañar a los usuarios legítimos.
- **Denegación de servicio (*DoS*)**: los atacantes envían datos falsos (solicitudes) hacia los nodos de la red con la intención de saturarlos y que no estén disponibles para los usuarios legítimos.
- **Espionaje (*Eavesdropping*)**: el atacante ve los datos confidenciales de los usuarios del canal de transmisión sin que ellos lo sepan.
- **Falsificación (*Forgery*)**: el atacante copia la identidad y el comportamiento de otra persona para engañar a un sistema de seguridad o a otras personas mediante la generación de información falsa.
- ***Jamming Attack***: los atacantes generan una gran cantidad de paquetes de datos en la red para bloquear los canales de transmisión y ocupar los recursos provocando una indisponibilidad del servicio.

- ***Man-in-the-Middle Attack***: el atacante se interpone entre dos nodos durante la comunicación para escuchar y robar información útil de los usuarios sin que ellos lo sepan. Hay que tener en cuenta que cada vez se usa con mayor frecuencia Federated Machine Learning en la capa edge, garantizando la privacidad mandando los pesos de los modelos a un sistema centralizado, en lugar de los datos y una vez reentrenado el modelo recogiendo en la capa edge el modelo actualizado. Si se suplantase uno de los nodos de la capa edge, se podría introducir ruido al modelo con datos falsos empeorando su desempeño, y, si lo que se suplantase fuese el nodo del servidor, se podrían mandar modelos "engañosos" a los nodos destino en la capa edge, potenciando una toma de decisiones en borde inadecuado, algo catastrófico para sistemas críticos.
- **Manipulación (*Tampering*)**: los atacantes alteran los datos a transmitir por la red.
- ***MFA (Multi-Factor Authentication) Fatigue Attack***: los atacantes envían múltiples requerimientos de autenticación al usuario que finalmente puede aceptar pensando que son lícitos.
- **Robo de credenciales**: los atacantes se hacen con las credenciales de un usuario para acceder al sistema y desde dentro escalar privilegios.
- **Secuestro de sesión (*Session Hijacking*)**: el atacante intercepta y secuestra la sesión de un usuario para obtener acceso a los datos y servicios confidenciales del mismo.
- ***Spam***: el spam son los datos no deseados que generan los atacantes, incluidos los datos falsos recopilados de los usuarios y otra información. El spam conduce al consumo de recursos de red, a la violación de la privacidad y/o al engaño.
- **Suplantación de identidad (*Impersonation*)**: el atacante se hace pasar por un nodo genuino para engañar a los usuarios ofreciéndoles servicios falsos o maliciosos, normalmente con el objetivo de robarles datos confidenciales.
- ***Sybil Attack***: los atacantes utilizan una identidad falsa para controlar la eficacia y el rendimiento de la computación en la red y afectan a la confiabilidad de los nodos.

Todas estas amenazas las podemos clasificar en alguna de las tres áreas de seguridad siguientes: los servicios de red, el procesamiento de los datos, y la privacidad de los datos. Cuando hablamos de los servicios de red hacemos referencia a la gestión de la confianza, el reenvío de paquetes, los sistemas de detección de amenazas, los sistemas de control de acceso y de autenticación. En el procesamiento de datos también tendríamos en cuenta la distribución de los datos, la protección de los datos y la distribución de contenido. La privacidad de los datos también hace referencia a la privacidad del uso de los sistemas, la privacidad de la ubicación, la privacidad de la red, la privacidad de la identidad o la del usuario.

Oportunidades de negocio y mensajes para los primeros receptores (Comisión Ciberseguridad)

A medida que los entornos distribuidos basados en *Edge Computing* y *Fog Computing* se están extendiendo, van apareciendo nuevos retos de seguridad y privacidad que requieren nuevos enfoques y nuevas herramientas. Estas nuevas soluciones deberán ser más inteligentes, más autónomas, y más colaborativas. A continuación, vemos algunos ejemplos de tecnologías o soluciones que se pueden adaptar bien a los entornos distribuidos.

Los Sistemas Inmunológicos Artificiales (*AIS, Artificial Inmune Systems*) aportan características de gran valor: seguridad, resiliencia, descentralización, distribución y memoria. Su capacidad de conocimiento y caracterización de comportamientos sospechosos en un contexto de sistemas dinámicos y amenazas de rápida evolución es un factor fundamental. En las últimas dos décadas la evolución de los AIS ha sido significativa. Los AIS presentan características que los hacen interesantes por tareas de optimización o detección de intrusiones, especialmente por su capacidad de autoadaptación, autoaprendizaje, autoorganización, procesamiento en paralelo y coordinación distribuida. Los AIS presentan otros mecanismos interesantes, como el mecanismo de autorregulación, así como su probabilidad de reproducción. Ajustando estos parámetros, el

rendimiento de los AIS puede mejorar significativamente, permitiendo que el sistema se adapte a entornos cambiantes, como suele suceder en la mayoría de los entornos distribuidos.

Las Plataformas Distribuidas de Engaño (*DDP, Deception Distributed Platforms*) son una herramienta muy potente para defenderse de atacantes cada vez más sofisticados, con más recursos y mejores armas. En ellas los atacantes son deliberadamente dirigidos a un entorno ficticio, controlado y especialmente creado para observarles sistemáticamente y llegar a conocer su motivación, métodos y, en algunos casos, incluso su identidad y clientes. Idealmente, esto se hace incluso antes de que hayan podido penetrar en la infraestructura real de la empresa.

El *Zero Trust*, o marco conceptual de confianza cero, ya se está implantando en centros de procesamiento de datos o en redes de muchas organizaciones, también empieza a verse en entornos *Cloud*, pero en un futuro próximo también darán forma a los entornos *Fog Computing* y *Edge Computing*. Este concepto exige una identificación y autenticación rígidas para cada dispositivo, sistema e individuo que intenta acceder a los recursos de una red privada. Este modelo se aplica independientemente de que se encuentren fuera o dentro del perímetro de la red. La seguridad de las redes de datos clásica confía en todos y en todo dentro de la red; por el contrario, un enfoque de confianza cero no confía en nada, ni en nadie. Gracias a la implementación de este enfoque, el propietario de la infraestructura tiene, o conoce:

- Cómo se genera, comparte y utiliza la información que se almacena en la ella.
- Quién está utilizando sus datos y aplicaciones, e incluso qué dispositivos están utilizando las personas para acceder a ellos (como *tablets*, ordenadores portátiles, o *smartphones*).
- Datos forenses detallados que pueden ayudar en la investigación de incidentes, y que a menudo se necesitan para fines de cumplimiento normativo.

Asimismo, se pueden utilizar agentes ligeros de monitorización para analizar los recursos y eventos de los nodos edge y detectar posibles vulnerabilidades y amenzas.

En relación con los sistemas de autenticación, es necesario que el sistema pueda requerir un factor o factores de autenticación específico (MFA) a las características y al contexto de la conexión, de una manera dinámica y adaptativa al nivel de riesgo soportado, criticidad del entorno, etc., siempre a través de una experiencia de usuario óptima. Igualmente, la tendencia es la eliminación de credenciales y la evolución a sistemas de tipo *Passwordless*. El sistema deberá tener capacidades de visibilidad y reacción (inteligencia) ante posibles cambios de la "*Security Posture*" de la conexión, siguiendo el modelo *Zero Trust*.