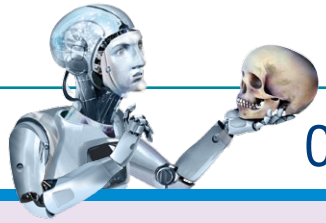

Idea para emprendedores: despliega redes de confianza cero

En los últimos días, Santiago Moral ha publicado un artículo en "IT Digital Security" sobre las redes de confianza cero. Afirma que cada vez son más las empresas que implementan este modelo alternativo de seguridad en redes, incluyendo la administración federal norteamericana, especialmente desde la publicación este pasado septiembre de 2019 por parte del NIST de Estados Unidos de su borrador 800-207 sobre arquitecturas de confianza cero ("Zero Trust Architecture", ZTA, en inglés). Un documento que define las ZTAs como un elemento crítico para eliminar incertidumbre.

Animo a los emprendedores a "ponerse las pilas" y crear procesos y servicios que faciliten la transición de las organizaciones de un modelo en el que "confiamos en lo que sucede en nuestra red local" a uno muy distinto en el que se protegen los recursos uno a uno y no diferentes segmentos de red.

Para aquellos interesados en este potente modelo, Luis Saiz ha publicado en LinkedIn como comentario a ese artículo toda una lista de referencias relacionadas, empezando por la del foro Jericho de 2007. Las ZTAs requieren un uso distinto de las técnicas actuales de autenticación y autorización.

A continuación enumero los principios más importantes de la ZTA:

- Asume que tu red es un entorno hostil no confiable. Ningún dispositivo es confiable por defecto.
- Tu objetivo es 'securizar' cada recurso de tu red y todas las comunicaciones entre ellos, independientemente de su localización.
- Autoriza el acceso a tus recursos individualmente y de forma dinámica, por conexión, basándote en una política que tiene en cuenta el estado actual de la identidad del usuario y un suficiente número de parámetros ambientales.
- Realiza una continua monitorización de tus recursos y de su accesibilidad.
- Técnicamente, esta arquitectura se apoya en funcionalidades proporcionadas por "proxies" y agentes. Posiblemente muchos de ellos, en especial los dedicados a recursos de redes en nubes públicas, aún por desarrollar ya que éste es un nuevo y complejo escenario.

Por un lado, animo a todos aquellos emprendedores, que los hay, y muy buenos, dentro de nuestra profesión, a "ponerse las pilas" en este paradigma de seguridad y crear procesos y servicios que faciliten la transición de nuestras organizaciones de un modelo en el que "confiamos en lo que sucede en nuestra red local" a uno muy distinto en el que se protegen los recursos uno a uno y no diferentes segmentos de red.

Por otro lado, esta es una de esas raras ocasiones en las que "el que llega en última posición, tiene una gran ventaja". Esto es, actualmente una empresa de nueva creación debería diseñar sus redes y proteger sus recursos usando este modelo de confianza cero. Una labor claramente menos compleja que la de evolucionar una red ya existente para que no permita movimientos laterales.

Alberto Partida
Analista en Ciberseguridad
itsecuriteer@gmail.com
@itsecuriteer en twitter
https://linkedin.com/in/albertopartida