El concepto de Zero Trust o confianza cero es un concepto de la industria de la ciberseguridad que ha tomado fuerza en los últimos años, y es un nuevo modelo de arquitectura de seguridad que se opone a los viejos modelos.

Zero Trust consiste básicamente en dejar de confiar en la autorización de las personas a acceder a ciertos dispositivos o datos simplemente porque estas personas se encuentren ya dentro del perímetro. Esto quiere decir, que debemos asumir que incluso dentro de nuestro perímetro de seguridad ya hay actores maliciosos que han entrado, y por ello una vez pasado el perímetro no debemos prescindir de agregar más medidas de seguridad.

Esto va en contraposición de cómo se veían antes las infraestructuras de seguridad que básicamente iban por la lógica de que había que proteger el perímetro pero tod lo que se encontraba dentro de la red era bueno y estaba a salvo. Un ejemplo de esto son los firewalls de estado que permitían la conexión y una vez la conexión estuviera permitida, ya no controlaban que más entraba, con lo cual una persona que utilizara una conexión legítima para entrar, luego podía ejecutar actos maliciosos.

En contraposición a esto, el modelo Zero trust utiliza mecanismos como la asignación de permisos a cada usuario y factores de autenticación múltiple, para asegurarse de que la gente solo pueda acceder, incluso dentro de la red, a aquellas cosas a las que deberían acceder o a las que tienen permisos de ver, y que todas sus acciones queden registradas. Se eliminan así cosas como cuentas compartidas que no permiten la trazabilidad, o directamente la falta de autenticación para entrar a los distintos dispositivos.

Es difícil implementar esto en las OT, debido a que estos dispositivos fueron creados con una sola tarea en mente, y sus programas son muy básicos y rudimentarios. Añadir funciones extra no es tarea fácil, con lo cual la única opción para lograr mover estos a una nueva arquitectura sería reemplazarlos. La otra opción es rediseñar la arquitectura de red para que existan otros dispositivos que controlen la conexión a las OT y que logren implementar estas cosas, como una segmentación de red donde se agrupen todos los dispositivos OT, con su propio firewall y autenticaciones seguras.

Los cinco componentes clave de una arquitectura zero trust son: Identidad, Dispositivos, Redes, Aplicaciones y cargas de trabajo, y Datos.

Y Los siete pilares enumerados por el NIST 800-20 son:

1. Todas las fuentes de datos y servicios de computación se consideran recursos.

2. Todas las Comunicaciones deben ser aseguradas sin importar la ubicación en la red.

3. El acceso a los recursos individuales de la empresa se debe otorgar de nuevo cada sesión.

4. El acceso a los recursos se determina mediante una política dinámica.

5. La empresa monitoriza y mide la integridad y la postura de seguridad de todos los recursos que posee y que estén asociados a ella.

6. Todas las autenticaciones y autorizaciones son dinámicas y aplicadas estrictamente antes de permitir el acceso.

7. La empresa recolecta tanta información como le sea posible sobre el estado actual de los recursos, la infraestructura de la red y las comunicaciones, y utiliza estos datos para mejorar su postura de seguridad.