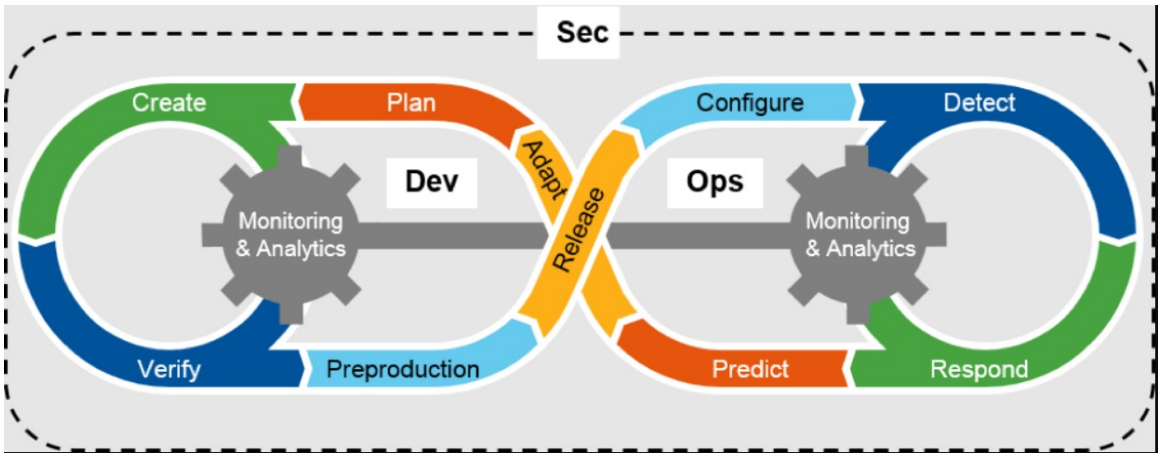
DevOps – Seguridad por Transparencia

Published on January 25, 2022



Fernando Castro
Senior Manager DevOps en EdgeUno

Hoy en día cuando se cree que el Internet es cada vez más hostil crece también en el ámbito de seguridad la paranoia, pero no las buenas prácticas, a esto yo le llamo Seguridad por oscuridad.

Esta práctica de seguridad basada en la paranoia, en la desconfianza y en decir que en Internet es una selva impenetrable y peligrosa es el argumento base para que crezcan en la empresas políticas que en cierto escenarios pueden ser más perjudiciales que benéficas para la compañía en general, un ejemplo de estas políticas son las siguientes:

1. Desconfiar en los empleados a toda costa, la seguridad por oscuridad invita al empleador a creer en enemigos internos, de ninguna forma se fomenta en construir un ambiente de confianza en donde un empleado nunca te atacará internamente por como se ha construido una cultura basada en el respeto y la confianza, no acá cualquier empleado puede convertirse en tu enemigo en cualquier momento y de ahí las políticas de las VPN, las contraseñas “super-seguras” entre otras medidas que dificultan al empleado conectarse a hacer su trabajo, pero claro, como se trata del secretismo, la seguridad por oscuridad no se ocupa de capacitar a los empleados en buenas prácticas de seguridad para el manejo de sus credenciales, como tener un acceso seguro a las plataformas de la empresa y por qué la importancia de implementar medidas para trabajar de forma segura.

Muchas veces se trata solo del ego de quien sea responsable del equipo, no hay discusiones con los demás equipos sobre las medidas a implementar, en este modelo solo importa que se aplique lo que el equipo de seguridad pide sin importar si se afectan los clientes de la empresa.

2. Cerrado por defecto. Esta es una medida típica de la seguridad por oscuridad, la excusa es reducir la superficie de ataque, cerrar puertos, cambiar el puerto a uno más “alto” que no sea estándar y medidas que están orientadas a una práctica en donde esconder es la mejor forma de defensa. Por ejemplo los equipos de seguridad por oscuridad suelen sugerir cambiar el puerto de SSH a un puerto XXXXX pero este sigue expuesto a Internet o poner el servicio SSH detrás de una VPN, sin importar si quizás el equipo de desarrollo de la empresa pueda necesitar el servicio SSH para conectar algunos servidores con herramientas de CI/CD.

La seguridad por oscuridad es una práctica que está lejos de ser analítica con las necesidades de las empresas, es por eso que desde hace varios años y basado en mi experiencia en implementación de servidores, para plataformas que manejan miles de usuarios y tener un record de cero hackeos es que he estado proponiendo empezar a hablar de seguridad por transparencia. (Debo aclarar que no se trata de ser optimista, se trata de ser realista y usar las mejores prácticas posibles).

La seguridad por transparencia se basa en los siguientes principios:

1. Por defecto tus empleados no son enemigos, si tienes un buena cultura empresarial basada en la confianza en donde aunque dejen de ser empleados las relaciones terminen en buenos términos el empleado no revelará tus secretos.

- Es necesario cerrar todos sus accesos y cuentas al momento de una salida.

2. Primero que todo las buenas prácticas. Aquí debo ir con ejemplos:

A. Si quieres puedes exponer el servicio SSH a Internet, incluso en el puerto por defecto, pero eso si asegúrate que los accesos con contraseña estén prohibidos, que solo se puede ingresar usando llaves, que tengas limitado los usuarios que pueden conectar vía SSH y muy importante que uses una herramienta con Fail2Ban para bloquear los intentos fallidos de acceso a tu SSH.

B. Nunca expongas un servidor web directamente a Internet, por más básico que parezca usar un Proxy Reverso, con herramientas como NGINX o HaProxy pueden ayudarte a crear un WAF que asegure tu

infraestructura de una forma sencilla y limpia, ademas que te ayudará a gestionar todos tus certificados SSL entre otros buenos beneficios.

(En el futuro compartiré una guía de buenas practicas para todo tipo de servicio basado en la idea de Seguridad por Transparencia)

La seguridad por transparencia demás requiere de un conocimiento profundo del entorno en donde se aplicará su modelo, se tienen en cuenta cada detalles de funcionamiento interno, las posibles afectaciones a la continuidad del negocio y se crean políticas que son discutidas con los diferentes equipos que serán afectado, su objetivo es el trabajo en equipo y la creación de forma colectiva de un ambiente seguro y claro para todos.

Aunque Internet puede ser un ambiente hostil, también es un lugar maravilloso en donde se desarrollan cosas geniales para todos, la seguridad no tiene que ser una camisa de fuerza para crecer, tampoco se trata de ser ingenuos, es claro que hay amenazas y muchas, pero el enfoque correcto no es necesariamente esconderse y desconfiar, ambientes seguros también son sanos en la forma en cómo se comunican los incidentes, en cómo se entrenan a los diferentes equipos en elementos de seguridad, en ocasiones se corre más riesgo de ser

hackeado creando un ambiente hostil en donde la gente no le guste las políticas de seguridad a que si de forma clara, amable y transparente creamos este ambiente en nuestras compañías o espacios de trabajo.

Published by

Fernando Castro
Senior Manager DevOps en EdgeUno
Published • 29m

9 articles ✓ Following

#DevOps #Seguridad #Security #OpenSource #Linux

Like Comment Share

0 Comments

Fernando Castro
Senior Manager DevOps en EdgeUno

✓ Following

More from Fernando Castro

DevOps - Automatización

Fernando Castro on LinkedIn