

SealPath apunta 3 razones ineludibles para optar por un modelo de seguridad Zero Trust

Un perímetro de la empresa cada vez más difuso y favorecido ahora por el teletrabajo, un alarmante incremento de ciberataques y el salto cada vez mayor a aplicaciones en cloud hacen que las empresas deban replantearse el tradicional modelo de seguridad de “foso y castillo”, por el nuevo modelo Zero Trust.

Según un estudio reciente publicado por [IBM y Ponemon Institute](#), más del 70% de las organizaciones consideran que el trabajo en remoto va a incrementar el riesgo de sufrir fugas de información y hacer más difícil la respuesta frente a una potencial brecha de seguridad. Como hemos visto una buena parte de las empresas tuvieron que habilitar el trabajo remoto de forma acelerada, multiplicando el acceso a la información vía VPN, aplicaciones cloud, etc.

Continuamente se producen destructivos ataques de ransomware que afectan a empresas de cualquier tamaño y sector, donde ya no sólo se cifran los datos y se pide un rescate por acceder a ellos, sino que el rescate se pide por no hacer pública la información confidencial extraída de la empresa.

Los atacantes centran todos sus esfuerzos en ver la forma de adentrarse en la red de la empresa y pasar desapercibidos. A menudo seleccionan empresas, objetivos concretos, y se toman su tiempo para acceder a lo que desean (propiedad intelectual, datos personales de clientes, información financiera, etc.). Según el anterior estudio, las desconfiguraciones de aplicaciones Cloud constituyen un vector de ataque importante de fuga de datos, siendo los datos de clientes, empleados y propiedad intelectual los objetivos más habituales. Tampoco se puede pasar por alto el origen interno de muchas fugas de información, sea por negligencias, errores humanos de la empresa o sus proveedores.

En este contexto, donde debemos permitir el acceso a la red a usuarios internos desde casa y con dispositivos personales, a proveedores, y donde los atacantes externos se comportan como internos una vez que han entrado a la red, ¿podemos seguir manteniendo un modelo de seguridad de “foso y castillo” para protegerla?

Es ahora cuando más sentido tiene seguir en la empresa un modelo de seguridad Zero Trust (Confianza Cero). Este modelo no es ni mucho menos nuevo. Fue ideado por un analista de Forrester hace más de una década y ha ido evolucionando, partiendo siempre de la premisa de que se ha difuminado la barrera entre lo que es confiable y lo que no es confiable en una red corporativa.

Venimos de un modelo de seguridad con un enfoque de “Confía pero verifica” (“Trust but Verify”), donde una vez que se ha definido quién es confiable, por ejemplo, los usuarios internos en la red, y no confiable, todos los externos, podemos permitir el acceso a los recursos de red por parte de los usuarios confiables, pero monitorizándolo. Sin embargo, la experiencia ha ido demostrando que se confía el acceso a los recursos de red, pero luego no se verifica o monitoriza: Se confía mucho, pero se verifica poco.

No confíes en nadie

El modelo de seguridad Zero Trust se basa en que nadie ni nada es confiable. Se sigue el modelo de acceso del “menor privilegio” de forma que se da acceso a una persona sólo a los recursos que necesita para realizar su trabajo y se le impide el acceso al resto. De esta forma, se evita que acceda a información que no debe y que, si su identidad es comprometida, un atacante pueda tener acceso a todo. Es necesario controlar el acceso a la información sensible, controlando la identidad, el dispositivo, aplicación y en definitiva el contexto desde el que se intenta acceder.

Todos los recursos de una empresa (datos, documentos, equipos, etc.) deben ser accedidos de forma segura con independencia de su ubicación, tanto si se accede a ellos desde el interior de la red, como desde fuera. Toda conexión es no confiable hasta que no se demuestre lo contrario, y se debe inspeccionar y registrar todos los accesos y comportamientos anómalos.

No es un modelo en el que se pueda seguir utilizando sólo una única tecnología, sino que varias ayuda a migrar a una arquitectura Zero Trust. Sí, podemos decir que la tecnología existe ahora y estamos en un buen momento para dar un salto progresivo a este modelo por las siguientes razones:

- **El perímetro de la empresa está más difuso que nunca:** Con trabajadores accediendo desde sus dispositivos personales y proveedores o colaboradores externos accediendo a aplicaciones

corporativas, etc. es difícil decir que es estar dentro y fuera de la red corporativa. Tal y como propone el modelo Zero Trust, debemos controlar el acceso a cada recurso independientemente de dónde se ubique y desde dónde se intente acceder, sin dar por sentado que el acceso desde la LAN es seguro.

- **El alarmante incremento de ataques de ransomware:** Una vez dentro, el ransomware se extiende dentro de la red accediendo como un interno más a nuestros datos corporativos. Y no se detiene con cifrarlos, sino que los extrae; y una vez que los ha conseguido, incluso puede pedir rescate por no hacerlos públicos. No olvidemos que sólo en un 2-4% de las fugas de información, los datos estaban cifrados y eran inaccesibles una vez extraídos. Es necesario cifrar nuestros propios datos y “compartimentalizar” al máximo su acceso permitiendo sólo el uso a aquellos que realmente deban acceder.
- **El paso acelerado a aplicaciones Cloud:** Las empresas han movido sus datos a la nube de forma acelerada y como el estudio de IBM y Ponemon Institute revela, las malas configuraciones en los servicios Cloud son un vector muy importante de ataque sobre nuestros datos. Al igual que con datos de la red interna, es necesario tenerlos protegidos dejando acceder sólo a quien deba tener acceso. Una fuga por una mala configuración donde se extraigan, por ejemplo, datos personales puede llevar a incumplimiento graves de regulaciones como GDPR.

Desde SealPath, compañía especializada en la protección de datos corporativos, su CEO, Luis Ángel del Valle, comenta que: “Este es un modelo de seguridad centrado en los datos, donde la seguridad de los datos está en el corazón del propio modelo. Hay que tener en cuenta que el objetivo último de las organizaciones no es proteger la red, ni los sistemas o los dispositivos, sino proteger lo más valioso, que son nuestros datos sensibles, y además protegerlos en sus tres estados: En reposo, en tránsito y en uso. El binomio identidad/datos es el verdadero perímetro de la empresa, lo que debe ser monitorizado y controlado. La empresa tiene que determinar quién debe acceder, a qué datos, con qué permisos y desde dónde”.

Poner en marcha un enfoque de seguridad Zero Trust puede suponer una serie de ventajas importantes para el negocio como facilitar la innovación e implantación de nuevas demandas de negocio permitiendo mejorar la colaboración con proveedores, clientes, etc. de forma segura en este nuevo entorno “desperimetralizado”. También responder de forma eficaz frente a amenazas y cumplir regulaciones: Saber de forma rápida y eficiente dónde se ha producido una posible fuga de información, y remediarla, puede suponer que el negocio no se vea afectado. Además, se ponen los medios y controles para facilitar el cumplimiento de regulaciones como EU-GDPR.

Por último, otro de los datos revelados en el estudio anterior indica que el 46% de las organizaciones

encuestadas hacen responsable al CISO en el caso de una brecha de seguridad. Es responsabilidad del área que gestiona la seguridad de la empresa moverse de un modelo de seguridad tradicional basado en proteger la “fortaleza” exterior a un modelo donde se pueda controlar el acceso a cada dato, cada documento o recurso de red, identificando posibles alertas de seguridad y revocando el acceso a personas que ya no deben tenerlo.

Como se ha comentado, la tecnología existe: Seguridad centrada en los datos, control de identidad, etc. pero se requiere un cambio de mentalidad para ir dando pasos hacia un modelo Zero Trust, sepamos aprovechar la oportunidad que ha traído el confinamiento favoreciendo el trabajo remoto, que se presenta como un escenario adecuado para acelerar el paso hacia este enfoque de seguridad.



Contacto de prensa:

JAVIER MODUBAR ALVAREZ

info@ingecom.net

944395678

<http://www.ingecom.net>