El rol de la seguridad en la transformación digital

En otros post hemos señalado que está bien ir en pos de nuevas maneras de pensar nuestros negocios y empresas, que todo esté alineado con el uso de estrategias digitales, TI, que haya uso de Agile y DevOps en todos los departamentos, buen hardware y un software destacado en ejecución.

Por supuesto que es importante ir en esa línea con un gran optimismo y superando nuestros logros día tras día. Sin embargo, si no admitimos desde el comienzo que hay un riesgo digital inherente, que la superficie de vulnerabilidad se puede agigantar también y que es preciso hacer algo para limitar su exposición, todo el castillo de naipes se nos puede caer.

Hay demasiados dispositivos interconectados, demasiadas plataformas compartiendo información, demasiados puertos y permisos que pueden verse comprometidos.

Hemos ido más allá del perímetro tradicional para el mantenimiento de la seguridad de nuestros sistemas. La transformación digital es un reto en términos de seguridad informática. No todo es color de rosa. Al volumen y flujo de información del que podemos disponer en esta senda se le añade, todo lo que mostramos ante ciberataques, bots y malware en general.

Defensa en profundidad

Este concepto no es nada moderno, por cierto, pero ha ido evolucionando y perfeccionándose sobre todo en estos tiempos

de Internet de las cosas, Big data y la ciencia de datos.

En la edad media los castillos disponían de fosos, puentes, muros y torres por ejemplo; habían diferentes capas de seguridad para evitar que un invasor llegara a los residentes del sitio que defendemos.

También lo usamos en el mundo de la ciberseguridad. Contamos con defensas y controles de aplicaciones, defensas / controles de red, usuario y endpoint y web y todo tipo de capas de defensa.

¿Cuantas capas o barreras son lo recomendado?

Depende de muchos factores pero si una empresa grande, del listado de fortune 500, dispone de hasta 56 líneas de control,¿Porqué la suya no dispone ni siquiera de 50? ¿Se ha cuestionado respecto a esto?

Defensa orquestada

Si cada capa de seguridad no se comunica con la otra de forma eficiente y precisa, los agentes maliciosos pueden moverse con libertad entre estos espacios hasta encontrar resquicios, vulnerabilidades o zonas mal defendidas.

Entonces, resulta crucial que se trabaje la seguridad de la compañía como un gran frente, donde no hayan múltiples y fragmentarias soluciones sino donde haya un manejo verdaderamente holístico, donde se compartan entornos, feedbacks y posibles consecuencias.

Si un malware vulnera nuestra capa de seguridad 1 y quiere llevarse nuestras contraseñas, hay un plan de acción y reacción pero también hay información fluida para que las capas 2-3-4-5 y 6 por ejemplo ya dispongan de elementos de

juicio para trazar sus posibles escenarios y endurezcan sus medidas, si bien lo ideal es que la amenaza no logre superar está primer barrera trazada por nuestros estrategas de seguridad.

De alguna forma esto que mencionamos tiene que ver con capas inteligentes, proactivas, que sepan qué tipo de amenazas esperar, los posibles patrones o características, los cursos de acción pertinentes y los flujos de comunicación idóneos y constantes entre estas barreras y también, con el comando central. Hay mucho de prevención y otro componente de acción.

Un pequeño ejemplo

Cuando una empresa dispone de dos equipos de cómputo nada más para funcionar y solo emplea software sencillo del tipo Office, es factible que un antivirus con licencia en cada máquina con su respectivo firewall sea más que suficiente.

Si añadimos una página web, un ecommerce con su respectiva pasarela de pagos y una cuenta de correo institucional, tal vez sea preciso añadir, certificados SSL estrictos, un registro Dkim y un Spf, así como asegurar en general estos componentes. Tal vez un proxy sirva en este sentido, un firewall lógico o uno físico, etc. etc. Y así sucesivamente se van complicando las cosas.

Como es un ejemplo, no tiene todas las aristas expuestas, todos los problemas que pueden presentarse pero es para que cada quien extraiga sus propias consecuencias.

Preguntas importantes

Estas son algunas de las preguntas clave que debe hacer: ¿Cómo gestiona la organización los datos, los protege, los controla y los utiliza para obtener ventajas estratégicas? ¿Dónde están los datos, dónde están las islas de datos, dónde están las

diferentes nubes? ¿Puede la organización ganar visibilidad de los datos dondequiera que se encuentren para garantizar la gobernanza, la confidencialidad, la privacidad y la protección?

Integrando la ciberseguridad en la transformación digital

Es muy importante para las organizaciones hacer de la seguridad el punto de partida y no una ocurrencia tardía. A pesar de la abundancia de violaciones de datos en todo el mundo, la seguridad sigue siendo una idea de último momento para la gran mayoría de las actividades de transformación digital que realizan las empresas actuales como: movilidad, servicios en la nube y programas de experiencia del cliente.

Lamentablemente, se considera que la seguridad ralentiza un proyecto, en lugar de permitir su éxito. Sin embargo, es comprensible que con la presión del tiempo para poner en marcha un proyecto, la falta de consideraciones de seguridad sensatas es un problema para las organizaciones que luchan por una verdadera resistencia y vigilancia cibernéticas.

Como es evidente en el clima digitalizado actual, con la creciente frecuencia y publicidad de los ataques cibernéticos cada vez más importantes y complejos, las empresas deben darse cuenta de que sus clientes son más conscientes que nunca de los problemas cibernéticos.

Incorporar una estrategia de ciberseguridad en este momento es una ventaja competitiva crítica.

Conclusiones

Tomarse el tiempo para identificar y conocer los riesgos,

departamento por departamento. Haga un esquema de esto, sobre lo que existe. Realice un estudio de los cambios que se avecinan, por ejemplo, la implementación de CRM, qué tipo de actividades TI a la sombra pueden ejecutarse, cómo pueden quedar los datos expuestos en una circunstancia A o en evento B.

¿Cuál es la estrategia de seguridad para respaldar estos movimientos? La automatización de las soluciones de ciberseguridad es clave para hacer frente al creciente número y sofisticación de las amenazas de ciberseguridad. Esto da lugar a la implementación de sistemas de aprendizaje automático, que son capaces de detectar patrones de ataque de forma total o semiautomatizada. También existe una tendencia hacia el empleo de tecnologías de inteligencia artificial y aprendizaje profundo para identificar indicadores de ataques complejos, que apenas son identificables según el aprendizaje automático convencional.

Leer también: La transformación digital vista en el mundo de la TV ; Capex y Opex en el furor del IaaS