Tú eras el elegido

«*No pongas la confianza en todos los hombres, sino en los que son dignos; lo primero indica estupidez; lo segundo, sabiduría.*» — **Demócrito.**

En los comentarios del primer post, Rebeca Cortázar, nuestra profesora de Auditoria, Certificación y Calidad de Sistemas Informáticos, acentuó que, aunque mi enfoque en las personas había estado acertado, pero que no me olvidara de que debía centrar el tema en el entorno empresarial. Partiendo de este punto, perdóname, pues en este tercer post voy a llevarte un poco la contraria, pero considero que es necesario, y además mejorará bajo mi punto de vista el nivel del segundo post del que me he quedado con la sensación de que podía haber dado más.

Qué es una empresa al fin y al cabo, que un conjunto de personas que juntos desempeñan una serie de roles para que la empresa lleve a cabo sus fines. En mi opinión las personas son quienes empujan las empresas, siendo igual de importante el peón que hace el cemento para poder poner los ladrillos, que el arquitecto que diseñó la estructura del edificio, al fin y al cabo sin ninguno de los dos, el proyecto no avanza, lo mismo sucede entonces en una empresa tecnológica. De las personas que forman parte de la institución depende el porvenir de la empresa, para un director de desarrollo es importante elegir al personal mejor cualificado para el trabajo, pero también es importante saber elegir a la persona adecuada, me explico, me refiero a la persona adecuada a aquel que no solo está cualificado con las capacidades técnicas apropiadas para el puesto que se solicita, sino que también tenga una serie de capacidades como ser humano. No nos vale que el trabajador sea brillante si después se relaciona con los demás lo mismo que una planta, o que tenga un comportamiento agresivo hacia otros trabajadores, o que no sea de confianza.

Acaba de aparecer la palabra clave a la que quería llegar, confianza. Una empresa debe tener trabajadores en los que pueda confiar, pero la confianza no puedes dársela al primero que viene, la confianza debe estar basada en hechos que sostengan que se puede confiar en alguien, no solo lo digo yo, Demócrito opina lo mismo. Y en ocasiones, incluso teniendo razones para confiar, muchos empleados acaban demostrando que no se podía confiar en ellos, pues la mayoría de los ataques vienen desde dentro de la empresa no desde fuera, puedes poner muchas puertas, pero si el que las abre es alguien desde dentro, eso no servirá de nada, así que aquí tenemos un riesgo, un riesgo que la empresa debe asumir, no puedes tener la certeza total de que un empleado es de confianza cuando lo contratas, puedes hacerle firmar todos los papeles sobre confidencialidad que quieras, si alguien tiene la intención eso le va a dar igual. Entonces, ¿qué es lo que debe hacer una empresa para poder minimizar este riesgo?
La ciberseguridad es un reto a la que la auditoria de TI debe enfrentarse, cualquier empleado puede utilizar los privilegios de su identidad para acceder a datos confidencial
es con malas intenciones, y se deben tomar medidas para al menos minimizar este riesgo. Pero cuál es el motivo que empuja a un empleado a realizar esta acción, arriesgarse a perder su puesto de trabajo, su credibilidad como trabajador o incluso ir a la cárcel. Puede haber una gran cantidad de causas, aspectos psicológicos, colisión de ideales con la empresa, chantaje, dinero, desvelar los trapos sucios de la empresa (en este caso a mí me parece más que aceptable, caso de Eduard Snowden).

Las empresas tienen que hacer que los empleados se sientan parte de la empresa, cuando alguien siente que algo es suyo lo

cuida y protege, una de las noticias que he leído para hacer este post ha sido una entrevista con Alberto Corredera, Director TI de Room Mate Hotels, el cree que es fundamental la información de los empleados y hace que tomen conciencia a través de su intranet y newsletter, y hacen que cada uno contribuya, aunque sea con pequeñas medidas que ayuden en la ciberseguridad. Me pareció una muy buena idea al leerlo, cada uno aporta un pedacito de sí mismo en la protección de la empresa, lo que no solo lo hace más segura a ataques externos, sino que también, hace que la propia empresa esté formada por un poco de cada uno, haciéndola suya. Una vez más la confianza y la satisfacción del cliente es lo más importante, el cliente debe sentirse seguro, no solo es importante contar con las tecnologías adecuadas sino también minimizar el riesgo de que alguien se las salte desde dentro y pueda hacer un estropicio con los datos de los clientes.

De acuerdo con los resultados de la Encuesta de Prioridades de TI 2015 de Protiviti, consultora global que ayuda a las compañías a resolver problemas financieros, tecnológicos, operacionales, de gobernanza, riesgos y auditoria interna, el 63% de las empresas están experimentando una importante transformación de Ti, ante el alarmante aumento de los ataques maliciosos, redoblando su enfoque en la ciberseguridad. La información financiera es de los datos más abundantes que pueden encontrarse en formato digital, un empleado díscolo de un banco podría robar mucho dinero a los clientes del mismo sin que nadie se diera cuenta.

Protiviti ofrece una serie de normas y prioridades a seguir en caso de que la identidad digital de una empresa se haya visto comprometida, como comprobar si el ataque ha tenido éxito,

comprobar el nivel de penetración, actuar lo más rápido posible, escanear la vulnerabilidad y comprobar desde donde ha venido la amenaza. En caso de ser interna se deberá buscar al causante y tomar medidas para cerrarle el acceso.

Existe una página web, referenciada al final del post, llamada pedroamador.com que ofrece servicios de auditoria TI relacionados con la identidad digital corporativa de una empresa, la ayuda a crecer en el mundo digital, a través de creación de contenidos y su difusión, utilzación de CRM, etc. Ahora imaginemos por un momento que un empleado mal intencionado de esta empresa ha recibido la autorización de su cliente, otra empresa, para crear contenidos en su nombre y difundirlos. Este empleado podría publicar cualquier cosa en nombre de la empresa cliente, a la que ahora de cierta manera pertenece, no podría robar información interna ni nada por el estilo, este ataque no es de ese estilo, sino que podría manchar la imagen de una empresa representándola en el mundo digital, y esto puede ser igual de grave que cualquier otro tipo de ataque. El mismo caso puede darse si un empleado de una empresa recibe instrucciones para representarla en línea y este publica cualquier cosa en su nombre, desde hacer que la empresa de apoyo a causas poco aceptables ante los ojos de internet o publique información interna de la empresa como sus datos empresariales o datos sobre sus clientes. La identidad corporativa de una empresa le diferencia de los demás en el mundo digital afectando esta, directamente a su visibilidad, credibilidad e influencia sobre el entorno donde se mueve.

En definitiva, una empresa puede ser atacada tanto desde fuera, como desde dentro, siendo la segunda la más común, si un empleado se hace dueño de la identidad de la empresa puede acceder a datos muy importantes y que pueden ponerla en peligro a ella y a sus clientes. Formar a los empleados y hacerles sentirles parte de un mismo conjunto es un deber que la empresa debe realizar para evitar o al menos minimizar riesgos de seguridad, pues este tipo de suplantaciones podría

hacerle mucho daño, tanto a la credibilidad que tiene, como a la confianza de sus clientes, o como a sus principales fuentes de ingresos.

Referencias:

http://globbsecurity.com/security-talks-cso-alberto-corredera-39499/

http://www.pedroamador.com/identidad-corporativa-digital

Protiviti (2015). Amid Ongoing Transformation and Compliance Challenges, Cybersecurity Represents Top IT Concern in Financial Services Industry. IT leaders are battening down the hatches, according to Protiviti's latest IT Priorities Survey . Available at: https://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/SRCybersecurityRepresentsTopITConcerninFinancialServicesIndustry!OpenDocument [Accessed 01 sept. 2016].

Instituto Nacional de Ciberseguridad (2016). Ciberseguridad en la identidad digital y la reputación online. Una guía de aproximación para el empresario. España. Available at: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/guia_ciberseguridad_identidad_online.pdf [Accessed 01 sept. 2016].

https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node50.html