CASO 6

GénieSEC, riesgos a todo nivel

Álvaro A. Cuervo

Introducción

El sistema finalmente colapsó... el administrador queda petrificado unos segundos, toma su cabeza a dos manos y el pánico es el único sentimiento que lo embarga... después de tanto esfuerzo, de tanta precaución, trasnochar y trasnochar, no ha valido de nada el estudio, pruebas, tecnología y aquel curioso intruso tomó el sistema tan fácilmente como quien escribe su primer código... pero esta vez desplegando ¡Hola Incrédulo!

Situaciones como esta podrían ocurrirle de un momento a otro a electroLibros.com, todos lo saben pero nadie pareciera tener el interés de prevenirlo...

Historia

Transcurría el año de 1994, Internet era novedad y todos hablaban de esta gran fuente de información, Antoine Martineu, inmigrante francés, cursaba octavo semestre de Ingeniería de Sistemas en una de las universidades más reconocidas del país; ya a estas alturas dominaba casi a la perfección el español además del inglés y por supuesto, el francés. Pertenecía a una familia acomodada que veía en su hijo un futuro profesional con una excelente proyección debido a su constancia y pasión

por la carrera que este había elegido mucho antes de finalizar sus estudios de bachillerato.

Por esa misma época, meditabundo frente al monitor se encontraba Nikolai Petrov, estudiante de cursos libres de matemática e informática de un instituto Ruso, aunque sentado allí en la sala de computadores la expresión de su rostro pareciese demostrar una profunda reflexión, lo cierto es que trata de recordar el nombre del software que utilizó hace ya varios meses para efectuar un ataque de fuerza bruta; finalmente no logra recordarlo, se siente como un principiante, golpea con fuerza su monitor y sale abruptamente de la sala ante la mirada atónita de sus compañeros y del administrador de la sala.

Cada uno tiene el tiempo suficiente para refinar sus intereses; por un lado, Antoine finaliza sus estudios formales mientras Nikolai toma con gran interés cursos de programación de computadores, redes y administración de sistemas, aunque su educación no es la mejor de Rusia combina a la perfección la orientación en el instituto con una alta personalidad autodidacta, escucha las clases pero no le agrada preguntar a sus maestros, así que opta por el autoestudio de cada tema que le es distante del entendimiento, ensayo y error cada noche, lectura y prueba, paciencia y perseverancia...

Él mismo siente su evolución, ya no es de su interés descargar software para utilizarlo en la red, lo cree facilista, ahora se ve a sí mismo como una especie de artesano digital, crea sus propias herramientas, las prueba, refina y consigue sus objetivos; igualmente se declara así mismo como un fan de la ingeniería social, su frase favorita es "Soy especialista en ingeniería social porque no existen parches para el descuido humano".

Corría el verano de 1996, el auge y alta proliferación de Internet y las TICs llevan a Antoine a plantearse varios interrogantes sobre el uso seguro de la información, sin lugar a dudas le llama la atención el tema y decide realizar una especialización en la universidad del país, con mayor experiencia en el tema;

paralelamente consigue un trabajo en una compañía de dicho sector con la convicción de que ésta organización será una gran escuela con miras a formar su propia idea llegado el momento. Hacia finales de los años 90 decide fundar su propia empresa, GénieSEC, con el objetivo de brindar soluciones de seguridad informática eficaces a todo tipo de empresas. Gracias a fondos propios constituidos de la herencia familiar, decide establecerse en una zona exclusiva de la ciudad y contratar una administradora y tres consultores. La empresa comienza operaciones oficialmente el 21 de octubre de 1999, rápidamente consiguen su primer trabajo por medio de las relaciones públicas que Antoine ha desarrollado en el ámbito universitario de sus estudios especializados, GénieSEC comienza a abrirse espacio en el mercado.

Zoom al capital humano GénieSEC

Antoine es una persona metódica y reflexiva, lee constantemente sobre temas de informática y especialmente del área de seguridad, siempre ha tenido claro que GénieSEC no será una empresa familiar, prefiere separar la sangre del mundo de los negocios, es bastante comprometido con sus actividades como gerente de GénieSEC y el nivel de exigencia es bastante alto para todo el equipo de trabajo, aunque todos reconocen que las condiciones laborales son muy favorables, esto debido a que Antoine ha procurado extraer varios aspectos del modelo de negocio de una de las empresas que más admira del mundo de tecnología, Google, así es como los empleados tienen oficinas modernas y confortables; Antoine ha realizado las entrevistas de personal y sólo contrata personas con sobresalientes calificaciones universitarias, los salarios son competitivos, existe un espacio de ocio y se tiene planeada una reunión mensual para que cada equipo de trabajo proponga metodologías y/o productos que impulsen el tema de innovación en la

organización; aún no puedo ofrecer almuerzos gratis preparados por *chefs* ni salones de masajes -piensa- pero confía en que estas ideas podrían materializarse en un futuro.

Daniela es una administradora de empresas con más de seis años de experiencia, según sus propias palabras desea en algún momento comenzar a estudiar Ingeniería de Sistemas o Electrónica, su gusto por temas tecnológicos fue decisivo en el momento de la selección de personal, por ser una persona organizada y manejar buenas relaciones interpersonales.

Manuel y Laura son consultores senior, aunque salieron de universidades donde aparentemente el grado de calidad es bastante desigual a cada uno le formó en gran parte su espíritu investigativo y autodidacta, demostrando que lo más costoso no es necesariamente lo mejor; tienen una buena amistad y conforman un sólido y conocedor grupo de trabajo en el campo de la seguridad informática, ambos son ingenieros de Sistemas, aunque Laura posee estudios especializados en Auditoría de Sistemas; ella tiene más de cinco años de experiencia en el campo, en tanto que Manuel lleva ocho años ejerciendo.

Pablo es el más nuevo del equipo GénieSEC, es un estudiante de último semestre de Ingeniería de Sistemas, es hábil para el análisis de problemas más no en igual medida para trabajar bajo presión. Aunque Antoine ha comenzado a detectar este aspecto confía en que su aprendiz pueda encaminar sus capacidades sobre la marcha, además se debe ser muy brillante para estar becado en una universidad de tan alta calidad.

El gerente de GénieSEC considera que el equipo conformado es el idóneo, dentro de sus planes está el de incentivar a los consultores para obtener varios tipos de certificaciones, las cuales les contribuirán -asegura- a tener un mayor grado de credibilidad frente a sus clientes y proveedores.

Primer proyecto

El primer proyecto de la empresa se convirtió en un reto para el equipo de trabajo, no sólo exigía para Antoine de alguna manera la presión de empezar con pie derecho su emprendedora idea sino además, su credibilidad frente a su colega de especia-lización, Camilo Ruíz, dueño de una tienda en línea que vendía libros electrónicos con editoriales de convenio, disminuyendo el costo para el lector y buenos dividendos para www. ElectroLibros.com, el era administrador de empresas de profesión, cursó sus estudios de especialización con la idea de consientizarse en mayor medida de los problemas de seguridad que podría afrontar su negocio, aunque su interés no tras-ciende hasta los temas eminentemente técnicos que muchas veces abruman y confunden a profesionales ajenos a este tipo de ámbitos.

ElectroLibros.com tenía apenas un poco más de un mes de operación, contaba en total con ocho empleados (el gerente, un diseñador, tres programadores, un administrador de servidores y dos personas para el departamento administrativo) y pocas transacciones *online* que se podían contar con los dedos de la mano, aunque era de recalcar el que aún no se había llevado a cabo una estrategia de mercadeo. Camilo había tomado la decisión de dar a luz su proyecto a pesar de no haber afinado todos los detalles debido a que quería ser el primero en la red en exponer lo que para él era una idea única, innovadora y de gran aceptación para el público en general.

La necesidad del cliente era fácil de resumir, no tanto así el trabajo que significaría para GénieSEC; era imprescindible evaluar toda la solución que ElectroLibros.com había implementado para su puesta en funcionamiento; esta primera fase de consultoría exigía presentar al cliente un plan de trabajo detallado junto con los tiempos empleados para cada actividad, posteriormente y una vez realizado el análisis de toda

la solución las partes acordarían la manera de afrontar las fallas y deficiencias encontradas de manera tal que ElectroLibros.com se caracterizará en un futuro no muy lejano por la importancia que daba al manejo de la información de sus clientes actuales y futuros.

Para Antoine fue evidente que el mayor problema que afrontarían era que, aunque Camilo tenía una clara visión de su negocio, su conocimiento técnico no era el mejor y sus antiguos socios, los cuales inicialmente tuvieron la concepción tecnológica de la idea ya no pertenecían a su equipo de trabajo, dejando un negocio con gran potencial pero sin documentación explícita de ningún tipo.

Una vez firmado el proyecto, no pasó mucho tiempo para que el equipo de trabajo de GénieSEC se reuniera a discutir las etapas que debería tener la primera fase del mismo; por consenso acordaron las siguientes:

1. Levantamiento de información de la infraestructura de solución de ElectroLibros.com (hardware y software).

2. Para los casos pertinentes, verificar posibles fallos de seguridad de equipos físicos.

3. Catalogar el software adquirido (licenciado o libre) por la empresa, los desarrollos internos y evaluar las posibles falencias en temas de seguridad que presentan.

4. Evaluación integra del sistema simulando ataques realizados desde Internet.

5. Verificar las políticas de seguridad, para esto tendrían en cuenta las normas existentes para el manejo de equipos de cómputo, accesos restringidos, instalación de nuevo software, entre otros.

Al presentar dicho plan de trabajo, Camilo, gerente de ElectroLibros.com no hizo mayor comentario al respecto, no demandó mayor explicación a GénieSEC y dio su entero aval para dar así inicio al proyecto, aspecto que desconcertó y hasta molestó a Antoine, quien esperaba una discusión profunda explicando al mayor detalle posible el trabajo próximo a realizar. Entre las partes se pactó igualmente que una vez se tuviera el diagnóstico definitivo resultante de la primera fase, se acordarían inmediatamente los tiempos y tareas de la fase siguiente.

Conociendo el campo de batalla

En reuniones realizadas al interior de GénieSEC se acordó dividir las tareas de manera tal que, entre todo el equipo llevarían a cabo el levantamiento de información de la infraestructura de solución, los posibles fallos de seguridad de equipos físicos y software estarían a cargo de Laura y Manuel, por su parte Pablo, apoyado por sus compañero de trabajo efectuaría las pruebas íntegras de simulación de ataques, todo esto complementado por la revisión que ejecutaría Antoine de las políticas adoptadas hasta el momento por la empresa.

Tal como lo había visto el gerente en sus pruebas de ingreso a GénieSEC, Pablo se sentía un poco incómodo y presionado por la labor encomendada, pensaba que el conocimiento que tenía no era el adecuado para semejante responsabilidad, sin embargo, Antoine organizó una capacitación intensiva de una semana para que el equipo de trabajo y su pupilo se adecuaran un poco mejor a la misión encomendada.

Debido a las diferentes tareas que tenía que efectuar cada recurso, Antoine decidió encomendar a Daniela el formateado de los documentos finales a presentar al usuario, así como una primera revisión de algunas herramientas comerciales y de

software libre para temas como Antivirus y *Firewalls*, tema del cual el creería que le sería de gran ayuda más adelante, Daniela aceptó con gran entusiasmo.

A medida que comenzaron a transcurrir las semanas de extenuante trabajo, Antoine comenzó a contemplar la posibilidad de un retrazo en el proyecto, se culpaba en silencio constantemente pensando que no había planteado un cronograma de trabajo adecuado, culpaba igualmente sin decir palabra alguna a Camilo por no haber revisado con detenimiento la propuesta, allí hubiese caído en cuenta de mi error -pensaba-, pero mientras más pensaba en ello más rápido pasaba el tiempo, así que los días de trabajo comenzaron a alargarse para todos y hasta se planteó la posibilidad de desatrazar trabajo fines de semana por lo que Pablo amenazó con abandonar el proyecto; definitivamente este no era el ambiente Google que el gerente de GénieSEC había estado buscando, sin embargo, y a pesar del panorama desalentador y por momentos chocante Antoine estaba decidido a no solicitar plazos de entrega, así que sesgó el alcance de algunas tareas por realizar en la primera fase, en especial el tema de políticas; recomendando normas generales que había aprendido en su curso de especialización, finalmente de esta manera, GénieSEC logró entregar el informe de diagnóstico en las fechas propuestas. Por supuesto el cliente se sentía satisfecho por el cumplimiento y el equipo de trabajo relajado por haber terminado días tan agobiantes.

Eslabones débiles detectados

Por increíble que le pareciese al grupo de trabajo, debido a la naturaleza del negocio y a los riesgos que estaban presentes día tras día en la red, en el informe final se encontraron falencias tales como:

- El servidor Web consiste en una CPU común de escritorio, su aplicación está desactualizada, así mismo el antivirus y el *firewall*.
- electroLibros.com no hace uso de SSL ni de ningún mecanismo seguro de intercambio de información.
- El servidor de base de datos tiene un porcentaje de ocupación de espacio de 98%.
- No existe un espacio único y restringido a los servidores.
- El código fuente de electroLibros.com no está debidamente administrado ni documentado.
- No existe información encriptada en la base de datos.
- El servidor *Web* posee programas que no están debidamente licenciados.
- No existe un plan de continuidad de la operación en caso de fallas.
- El *password* de acceso a los servidores es el mismo y no sobrepasa los cinco caracteres.
- Es posible realizar ataques de inyección SQL.
- Las sesiones de los usuarios logueados en el sistema de electroLibros.com se cierran correctamente únicamente cuando se da click en el *link* "cerrar sesión".
- El porcentaje de utilización de CPU del servidor Web es la mayor parte del tiempo de un 85%.

El día de la entrega del informe Antoine miraba y repasaba su contenido, no podía creer cómo alguien que dirigía una empresa de ese estilo y que había estudiado junto con él podía

llegar a cometer y/o permitir semejante volumen y gravedad de fallas en su empresa. Camilo recibió el informe, dió una ojeada, miró fíjamente a Antoine y acto seguido lo invitó a que conversarán detenidamente en tres semanas para plantear y desarrollar la segunda fase del proyecto.