Los líderes en BI

Ya que estamos en medio de la elección de qué herramienta BI escoger dentro de nuestra actividad en el aula, me ha parecido adecuado buscar opiniones respecto a los líderes del sector: SAP, IBM, Oracle, Microstrategy y QlikView.

El caso es que en mi búsqueda han aparecido varios resultados mencionando una serie de encuestas realizadas por Gartner a usuarios de estas herramientas, y los resultados me han sorprendido. En el informe se detalla la principal preocupación de los usuarios respecto a estas herramientas: su facilidad de uso. El usuario pone esto por encima de cualquier otra característica. Y luego lo inesperado, en las encuestas ninguno de los líderes sale muy bien parado.

De la herramienta de SAP Business Objects se dice que las implantaciones son muy complejas, el 40% de sus usuarios declaran problemas de rendimiento y para rematar, la experiencia de usuario y la calidad del soporte son bastante malas.

En cuanto a la herramienta IBM Cognos un 33% de los encuestados tiene problemas de rendimiento. La implantación es bastante más compleja que la del resto de competidores según los informes. El tema es grave, tanto es así que el 20% de los encuestados admite su intención de dejar de usarlo.

De Oracle en el informe se expone que los ciclos de desarrollo son larguísimos. Otros puntos negros son que su funcionalidad en memoria es escasa y que su visualizador de datos es algo justito.

Las quejas para con Microstrategy son en cuanto a la capacidad de realizar reportes y que la curva de aprendizaje de la herramienta es elevada. Por último, los usuarios destacan que su coste es notable.

En el caso de QlikView, se puede decir que es la herramienta con mejores resultados. Las quejas pasan por su dificultad de implantación a nivel corporativo, alto precio y el 12% de encuestados asegura problemas de rendimiento.

Por lo tanto, como conclusión, parece claro que la herramienta perfecta no existe. Que por mucho que se nos vendan las bondades de estas, todas ellas tienen sus fallos o puntos negros. Quizá sea esta la razón de que muchos proyectos BI fracasen, y es que la empresa que espere poder solucionar todos sus problemas a través de la adopción de "X" herramienta cae en un error grave. La herramienta no garantiza el éxito, es el modelo de la organización el único que lo puede garantizar.

¿Invierto en CRM?

Lo primero es dejar las cosas claras, un CRM no es software y ya esta, es una forma de representar la cultura de trabajo de una empresa. Un CRM combina por así decirlo lo que se ha hecho toda la vida en una típica tienda de barrio con las nuevas tecnologías. Y es que en una tienda de barrio raro es que el dueño no conozca los gustos de sus clientes de memoria ya que su número de clientes es reducido. Pero en las empresas con una cartera de clientes aceptablemente amplia esto de «saber los gustos» de tus clientes de memoria se complica o es imposible. Aquí aparecen los CRM, la tecnología permite continuar con esta forma de trabajo.

Entonces, ¿podemos decir que un CRM solo nos va a traer beneficios? Para nada. Si esto implica cambiar los hábitos de trabajo puede traer pérdidas de tiempo y problemas de adaptación, lo que se traduce en costes para la empresa. Para que tenga éxito, la empresa primero debe tener una estrategia propia para con sus clientes y a partir de ese punto un CRM puede llevarla a otro nivel. Entre los beneficios que se pueden obtener de una implantación exitosa están:

- Marketing automatizado
- Disminución de costes en ventas
- Simplificación de procesos comerciales
- Aporte de información clara, ordenada y actualizada. El activo mas importante para cualquier organización
- Seguimiento de las actividades
- Mejora servicio al cliente
- Explorar nuevos clientes

Y después de todo esto, ¿invierto en CRM? Sí, pero el mensaje es el siguiente: el CRM se tiene que adaptar a tu empresa y no al revés.

Playbook del hacker: me cuelo en tu dispositivo médico (Parte 4/4)

Hoy acabamos con el Playbook. Tened en cuenta que existen muchas más formas con las que los hackers aprovechan las vulnerabilidades de estos aparatos, pero según San Google y sus resultados, son los escenarios más comunes. Hasta ahora hemos visto escenarios de DDoS, ataque centrado al paciente y robo de información de centros hospitalarios. Hoy vemos el 4º

y último escenario:

Mantener como rehenes a hospitales mediante ataques ransomware.

Un tipo de ataque especialmente perjudicial que es cada vez más común el ataque ransom o de rescate. Como en los anteriores, los hackers acceden al sistema mediante un dispositivo para acceder a la red del hospital. Una vez dentro, encriptan datos sensibles y posteriormente demandan dinero a cambio de una contraseña que desencripte esos registros. Los centros médicos que se enfrentan a este tipo de ataques se pueden encontrar de repente con toda la información de sus pacientes encriptada, haciendo imposible el acceso a registros como la prescripción al paciente, informes de patologías, diagnósticos y otras informaciones críticas para atender al paciente. Como el origen de estos ataques tiende a ser internacional y por lo tanto difícil de trazar y enjuiciar, la mayoría de víctimas acaban pagando.

En el año 2012, un grupo de hackers rusos mantuvo "secuestrado" un centro médico en Gold Coast (Australia), el Miami Family Medical Centre, después de que lograran encriptar miles de registros de pacientes en el propio servidor del centro. Los hackers demandaron un rescate de 4000$, unos 3700€, para desencriptar la información. Este precio, que puede parecer bajo, es una estrategia habitual para aumentar la posibilidad de que los afectados paguen, y dadas las dificultades de trazabilidad expertos en seguridad TI reconocieron que quizás su única opción era pagar. ¿Que paso al final? Una compañía de servicios IT, Essential IT Services, consiguió restaurar su sistema. Una de las enseñanzas que deja este caso particular es que los backups nunca deben estar en el mismo servidor ni conectados a internet. El centro tenia backups, pero estos también estaban encriptados. La casualidad hizo que un miembro del staff técnico del centro se llevara a casa uno de los backups de los datos, pero al no tratarse de un backup del sistema completo, esto hizo que la tarea de

devolver el funcionamiento del sistema llevara su tiempo.

Por cierto, esto es Gold Coast. Me parecía necesario enseñar y compartir este lugar.

Hasta aquí llega el Playbook del hacker, espero que os haya gustado.

Playbook del hacker: me cuelo en tu dispositivo médico (Parte 3/4)

Previamente, en el Playbook del hacker… En el capitulo 2 vimos como a través de un dispositivo médico se podía interrumpir la actividad de un hospital mediante ataques DDoS. Hoy os publico el tercer escenario:

Robo de datos en red a través de dispositivos médicos.

Los hospitales almacenan miles de registros que contienen información sensible de índole financiera, médica y de identidad, lo que los hace convertirse en un objetivo tentador para los ciberdelincuentes. Estas redes por lo general están fuertemente protegidas, haciéndolas objetivos difíciles de atacar. Pero, ¿qué pasa cuando conectamos un dispositivo inseguro en la robusta red de un hospital? Los hackers buscan estas alternativas inseguras para una vez dentro de ellas pivotar y entrar dentro de la propia red. Con esto se deduce que la motivación principal de hackear un dispositivo médico sea el robo de datos. En la mayoría de casos, los hackers no

buscan la información médica que almacenan estos dispositivos, si no una entrada a los registros que contienen información financiera y de identidad que puedan vender en el mercado negro.

TrapX Security, una compañía especializada en ciberseguridad, ha encontrado y analizado 3 incidentes en distintas instituciones médicas que han sido objeto de ciberataques a través de sus dispositivos médicos.

1. En el primer ataque analizado el ataque se hizo por medio de tres analizadores de gas en sangre. Los atacantes usaron estos dispositivos como puerta trasera a la red del hospital
   . Además, instalaron malware adicionalmente, como Zeus y Citadel, y robaron una cantidad indeterminada de datos sin ser detectados. La información robada se llevó a un servidor en Europa.
2. El segundo caso es un ataque al sistema de archivo y comunicación de imágenes (SACI). Este sistema provee imágenes al departamento de radiología

Máquina de rayos X

de múltiples dispositivos (como ejemplos: equipos de Rayos X, ultrasonido, resonancia magnética y tomografía computarizada), y por lo tanto está conectado a la red de la organización. Esto hace que sea un objetivo perfecto para ciberataques. Infectando el SACI, los atacantes lograron acceso no autorizado al puesto de trabajo de una enfermera, extrayendo datos de este sin ser detectado. Los datos robados esta vez fueron a parar a un servidor chino. Los investigadores determinaron que los atacantes violaron la seguridad después de que un empleado visitara una web maliciosa preparada para enviar malware. La amenaza fue eliminada por los

sistemas de seguridad del hospital, pero no antes de que infectara el SACI, y como el SACI no podía ser escaneado ni remediado, el sistema se convirtió para los ciberdelincuentes en un punto sobre el que pivotar.

3. El tercer ataque analizado es similar, pero en este caso los cibercriminales se valieron de un sistema de Rayos X exclusivamente.

Considerando que ninguna de estas organizaciones detectaron estas brechas por su cuenta, TrapX cree que una gran mayoría de hospitales están actualmente infectados con malware sin detectar desde hace meses o incluso años.

Como ya he comentado con anterioridad, esta información sustraída acaba en el mercado negro. Rick Kam, presidente de ID Experts, organización que provee servicios y software para gestionar la ciberseguridad, cuenta que los datos médicos completos de un paciente son más valiosos en el mercado negro que las tarjetas de crédito. Según el FBI, se venden por entre 20 y 70 dólares (18 y 63 euros), mientras que una tarjeta puede costar tan solo 5 dólares (4,5 euros).

¿El motivo? Una cuenta bancaria es fácil de cancelar, pero hospitales y aseguradoras no suelen tener un procedimiento claro para ayudar a los pacientes si les roban su información médica. Además, los departamentos de tecnología en sanidad no están equipados como la banca y las finanzas para hacer frente a estas situaciones, por lo que se están encontrando debilidades que pueden ser explotadas.

Los ciberdelincuentes pueden crear una identidad falsa completa y operar con ella o estafar a las aseguradoras gracias a esos datos. Por ejemplo, pueden aprovechar esa identidad para adquirir medicamentos y venderlos posteriormente en la deep web.

Mañana último capitulo de la serie de blogs dedicados al

Playbook.

Playbook del hacker: me cuelo en tu dispositivo médico (Parte 2/4)

Ayer en el primer capítulo del Playbook del hacker ©, vimos cómo aprovechando las vulnerabilidades de los dispositivos médicos se podía llegar a ~~matar~~ hacer «pupa» a las personas. Hoy continuamos con el segundo de los escenarios:

Interrumpir las operaciones de un hospital mediante ataques de denegación de servicio.

Más a menudo, los hackers que tratan de irrumpir en un dispositivo médico buscan algo más grande que un paciente. Estos aparatos, en particular los de ámbito hospitalario, pueden proveer un acceso de puerta trasera o backdoor a la red del propio hospital.

Una vez dentro, los atacantes puede lanzar un ataque de denegación de servicio para causar una extensa interrupción en las operaciones del centro. Estos ataques pueden venir desde internos maliciosos, hacktivistas con una causa que promover o simples hackers en busca de objetivos sencillos con un gran impacto. Derribar la red de un hospital, aunque sea poco tiempo, puede comprometer seriamente la seguridad y la salud del paciente.

En el año 2014 el Boston Children’s Hospital sufrió un ataque

de denegación de servicio a su sistema desde el grupo hacktivista Anonymous, colapsando servicios como su página web, a forma de represalia al tratamiento y diagnóstico dado a una niña de 15 años a cuyos padres el estado de Massachusetts les había quitado su custodia.

Mañana a la misma hora, la tercera parte.

Playbook del hacker: me cuelo en tu dispositivo médico (Parte 1/4)

Recientes demostraciones de dispositivos médicos con conectividad a la red muestran vulnerabilidades y potenciales amenazas de ciberseguridad. Muchos de estos dispositivos, que son de soporte vital (monitores de pacientes, bombas de infusión, ventiladores, etc.), residen en las redes de hospitales a lo largo del mundo. Incluso son más los dispositivos accesibles a través de la tecnología wireless (bombas de insulina y marcapasos, por ejemplo).

Estos dispositivos representan un arma de doble filo: tienen el potencial de transformar el cuidado de la salud pero a su vez exponen a los pacientes y a las organizaciones de la salud a riesgos de seguridad. Entre las consecuencias no intencionadas de la digitalización en el cuidado de la salud y el crecimiento de la conectividad en red están el ser hackeado, ser infectado con malware y ser vulnerable a accesos no autorizados.

En esta serie de 4 entradas, vamos a ver 4 formas/escenarios en los que los ciberdelincuentes se aprovechan de las

vulnerabilidades de los dispositivos de propósito medico.

Dañar a pacientes atacando dispositivos médicos.

Este es el escenario más temido de todos: un hacker se cuela en un dispositivo de un paciente e "inyecta" código malicioso que causa daños o incluso la muerte al que lo lleva.

Dick Cheney, un señor amigable

Famoso es el caso del entonces Vicepresidente de los EEUU Dick Cheney, que allá por el año 2007 tenía tal miedo de que los terroristas hackearan su marcapasos que decidió deshabilitar su conexión wireless para evitar intentos de asesinato.

Unos cuantos años después, en Diciembre de 2012, la serie de ficción Homeland – **ALERTA SPOILERS!!!** – en uno de sus capítulos trato este mismo tema, retratando la muerte del (¿casualidad?) Vicepresidente de los EEUU cuando una organización terrorista hackea su marcapasos.

El investigador en ciberseguridad Jay Radcliffe encontró una vulnerabilidad que podía servir para hackear una bomba de insulina y disparar una sobredosis. Este tipo de ataques pueden estar dirigidos a un paciente en particular o ser generalizados a todos los pacientes que usen un dispositivo en particular. Afortunadamente, este escenario es muy raro que se de, pero los dispositivos de los que dependen pacientes de forma crítica deben ser analizados en profundidad para minimizar riesgos.

Mañana a la misma hora tendréis la segunda parte del Playbook.

Nuevas tecnologías y fútbol, ¿compatibles?

Antes se hablaban por lo menos

Si hay algo que me apasiona es el fútbol. Me mantiene embobado los fines de semana con las ligas, entre semana con las competiciones europeas, los veranos con sus Mundiales, Eurocopas, Copas América, etc. Sí, ya se, os preguntaréis, ¿y el fútbol que tiene que ver con las tecnologías de la información? Pues parece que hoy día bastante más de lo que parece, resulta que hay gente más "obsesionada" con el deporte rey que yo al punto de ver muy útiles las nuevas tecnologías para sus propósitos. Entrenadores de talla mundial como Mourinho y Rafa Benítez (ojo, no soy fan de su estilo futbolístico, que quede claro) son asiduos a su uso desde hace años.

El fútbol profesional y las tecnologías

En una intervención en la sede de la Real Federación Española

de Fútbol, Rafa Benítez expuso que las nuevas tecnologías han facilitado el trabajo de su cuerpo técnico. Los programas para diseñar jugadas en dispositivos móviles resultan especialmente prácticos, permiten también diseñar ejercicios rápidamente, catalogarlos, almacenarlos y recuperarlos en cualquier momento. Incluso en situaciones como entrenar en otro país o con jugadores de diferentes nacionalidades resulta un gran beneficio, ya que permiten transmitir las instrucciones a los jugadores muy fácilmente.

También destacó lo útil que resulta trabajar con sistemas de vídeo y de recopilación de datos sobre parámetros del juego. Disponer de información detallada permite averiguar con más facilidad en qué está fallando el equipo, una línea de jugadores o un jugador en concreto y trabajar para hacer las correcciones necesarias mostrando todo con claridad. Además de eso resultan útiles para para analizar y preparar jugadas a balón parado, así como para obtener datos de los resultados de aplicar un sistema u otro para defenderlas.

Interpretar los datos

Como en las empresas, el uso y la interpretación que se den de los datos que se obtengan en estos sistemas es primordial. Benítez dio varios ejemplos al respecto, uno de ellos bastante significativo respecto a la distancia recorrida por un jugador en el campo. De primeras, si un jugador de un partido a otro aumenta significativamente esta cantidad, quiere decir que físicamente el jugador está preparado para ello, lo cual es bueno, pero si se tienen en cuenta otros datos como su posición en el campo puede que pase a ser un dato negativo, ya que querrá decir que el equipo estaba mal posicionado en el terreno de juego.