Business Intelligence, ¿hacia donde crecerá?

El creciente desarrollo de los sistemas de BI durante los últimos años, ha permitido que los directivos pueden acceder a mucha más información, de más calidad y con mayor rapidez. Gestionar esta información se ha convertido, a día de hoy, en una herramienta clave para poder "jugar" en un mercado tremendamente dinámico y en constante cambio. Pero… ¿cuál serán los cambios que se avecinan dentro de BI?. Veamos algunos datos que arrojen un poco de luz al tema. La prestigiosa compañía de estudios IDC en su último informe de Junio 2015 (Worldwide Business Analytics Software Forecast, 2015–2019) indica que el mercado de software BI creció un 6,5% en 2014 llegando a algo más de $40 mil millones en todo el mundo. Según IDC se espera que este mercado crezca a una tasa anual del 8,0% en los próximos cinco años. Como podemos observar, son cifras nada desdeñables que nos indican que BI será una prioridad de futuro para los directivos. Otro dato a tener en cuenta, es que la mayor parte del crecimiento va a venir marcado por las nuevas tendencias que ya han irrumpido con fuerza en el mundo del BI y que son, precisamente, las que trataré de exponer en este post.

1. **Real Time BI:** Vivimos en tiempos en los que la velocidad y la capacidad de reacción para tomar decisiones se miden en fracciones cada vez más cortas. La información que nos aportan las redes sociales es instantánea y es vital poder analizarla en 'tiempo real'. Las Redes Sociales se han convertido en el máximo exponente de la comunicación humana en el que intercambiamos información sobre una gran variedad de temas que de otra forma no sería posible. Dicha información, ya está empezando a ser estructurada, almacenada y consultada prácticamente en tiempo real, directamente de los consumidores y generadores de opinión y tendencia. Esto hace, como no, que las empresas quieran poner en práctica nuevos sistemas de inteligencia competitiva que les den acceso "directo" a la mente de dichos consumidores. Sin embargo, el análisis de datos en tiempo real no solo se aplica cada vez más a la información proporcionada por las redes sociales, sino también a la gestión de almacenes, comercio electrónico, etc, lo que nos ayudará a conocer mejor y vigilar el mercado y a la temida competencia.

2. **Mobile BI:** Como su propio nombre indica, Mobile BI implica decisiones inteligentes desde cualquier lugar. Hoy en día "nadie" concibe su vida sin un móvil, tablet o portátil, esto sumado al creciente uso de la nube, están llevando a la implementación de nuevas herramientas business intelligence móvil. Gartner estima un 30% de crecimiento en el uso de este tipo de herramientas en dispositivos móviles para finales de 2016. Algunas ventajas ya disponibles en las empresas mediante esta tecnología, son por ejemplo:

   - El equipo de ventas puede acceder a todos los detalles de la cuenta del cliente, como esta su inventario o la información de productos mientras visitan sus instalaciones.
   - El distribuidor de la cadena de suministro puede acceder a datos sobre entregas en curso, disponibilidad de productos y todo ello desde cualquier lugar donde se encuentre.

   El auge del BI móvil va en aumento y está siendo alzado por grandes compañías de estudios en TI, que marcan las pautas a seguir para implementar con éxito este tipo de sistemas.

3. **Big Data**: Es algo que está de moda en boca de todos y es innegable que todas las empresas quieren subirse al carro e incorporar Big Data a su portfolio de soluciones, productos o servicios. Big Data parece salpicarlo todo, desde grandes empresas privadas hasta administraciones públicas, pasando por negocios de comercio electrónico y realidades futuristas como las Smart Cities. La cantidad de datos, fotos, videos y audio que subimos cada minuto a internet se multiplica exponencialmente y requiere enfrentarse a trabajar con grandes volúmenes de datos. Este es uno de los puntos que ha cambiado de forma radical la forma en que se plantea y planteara BI, la gran cantidad de datos que anteriormente no se analizaban. No se trata de otra cosa que de aprovechar todo esa gran cantidad de información en nuestro propio beneficio, bien como generadores o como explotadores de la misma y obtener mayor ventaja respecto a nuestros competidores. Mientras que el hardware es cada vez más barato y accesible, lo realmente difícil es encontrar especialistas para sacar partido a las soluciones Big Data, por lo que el factor humano es y será uno de los puntos clave para estar bien posicionados en el campo de BI.

El año que acabamos de dejar atrás, ha traído cambios significativos al mundo de la inteligencia de negocio, así lo dicen los expertos. Las normas de BI seguirán evolucionando, produciendo a su vez, numerosos cambios en muchos entornos laborales. Este cambio no solo se verá impulsado por la velocidad de los avances tecnológicos, sino también por algunas de estas tendencias de BI que hemos visto en este post y que permitirán obtener más valor a partir de los datos. Estoy seguro que esto supondrá una gran oportunidad para muchas empresas y para el BI en general !!

Incidentes en los Sistemas de Control Industrial

 En el post anterior, hable sobre las amenazas que se ciernen sobre los Sistemas de Control Industrial (SCI) y de cómo algunas herramientas que existen en el mercado pueden ayudar a explotar sus vulnerabilidades. Enlazando un poco con el tema y aprovechando la interesantísima ponencia sobre seguridad de la información que nos ofrecieron la semana pasada, me gustaría adentrarme un poco más en el impacto y consecuencias que podría tener un incidente en este tipo de sistemas. Ya no sólo en la organización, sino también en la propia sociedad, llegando incluso a poder poner en peligro vidas humanas o afectar al medioambiente.

Si echamos un vistazo al informe anual sobre amenazas de la compañía Dell podemos ver que el año pasado se registraron el doble de ataques en los sistemas SCADA en comparación al 2013 y que la mayoría de ellos tuvieron lugar en Finlandia, Reino Unido y Estados Unidos. Podríamos decir entonces, que los ataques contra dichos sistemas son “reales” y están en el ojo del huracán, aunque muchas veces pasan desapercibidos para nosotros, los usuario de a pie. Esta laguna de información se debe a que las empresas solo suelen reportar las brechas que involucran datos del personal o a informaciones de pagos. Actualmente no existe una ley europea sobre “ciberseguridad” y sólo los operadores de telecomunicaciones están sujetos a requisitos de notificación de incidentes. Esperemos que esto cambie con la aprobación de la llamada Directiva sobre la Seguridad de las Redes y los Sistemas de Información (SRI), que les obligará a adoptar medidas estrictas de seguridad y a informar a las autoridades nacionales de violaciones de seguridad graves en sus redes y sistemas. A ver si es verdad, y de una vez por todas salimos de la sombras y empezamos a hacer las cosas de manera transparente.

Este tipo de amenazas suelen ser de naturaleza política y su objetivo es hacerse con las capacidades operativas de plantas energéticas, refinerías, gasoductos, etc. La diferencia con los ataques informáticos tradicionales que producen un daño “no físico”, es que los dirigidos a este tipo de sistemas pueden afectar no sólo a los datos corporativos, sino también producir daños “físicos” significativos, haciendo de estos un objetivo especialmente atractivo para los hackers de otros países. Los ataques de denegación de servicio, malware o la explotación exitosa de alguna vulnerabilidad podrían tener impactos de diversa índole. Vamos a ver cuáles serían algunos de los

más relevantes:

- **Impactos sobre la seguridad física y el entorno:** Este tipo de impactos pueden ser muy críticos por la pérdida de vidas humanas o lesiones personales. Incluyendo también el daño hacia el medio ambiente.
- **Impactos económicos:** Las pérdidas económicas pueden afectar al correcto funcionamiento de la empresa, debido a daños en dispositivos o infraestructuras, o bien llegando a parar la producción o distribución del servicio.
- **Impactos sociales y mediáticos:** La pérdida de confianza en una organización afecta directamente a su imagen lo que se traduce en pérdida de clientes, de crecimiento y de competitividad.

Una vez vistos los impactos que pueden darse si se produce un incidente, nos podemos hacer una idea de que la lista de posibles consecuencias es enorme. Entre ellas podemos encontrar algunas como la reducción o pérdida de producción, daños en el equipamiento, lesiones a personas, violación de la legislación, contaminación, pérdida de información confidencial, y así un larguísimo etc. Aunque esto nos pueda parecer lejano y nos suene un poco a ciencia ficción, todos estos impactos y consecuencias tienen su correspondiente traducción al mundo real, y si no, hagamos un pequeño repaso de los incidentes más relevantes que se han dado hasta el momento.

- **En 1982** la CIA se vio envuelta en la venta de equipos ‘alterados’ a la Unión Soviética. Un Troyano camuflado causó una explosión en un gaseoducto transiberiano.
- **En 1985** la fuga de químicos en la empresa Union Carbide en Virginia fue uno de los primeros incidentes detectados y confirmados de la historia en el que 134 personas tuvieron que ser hospitalizadas.
- **En 2000** un ex empleado de la planta de tratamiento de aguas de Maroochy en Australia fue acusado de acceso ilegal al sistema de control de alcantarillado del Condado tras ser despedido. El resultado, litros y litros de aguas residuales vertidas en ríos y parques.
- **En 2003** el gusano Slammer infectó la central nuclear de Davis-Besse en Ohio, afectando a varios SCI causando problemas en el sistema de monitorización de seguridad y bloqueando el sistema durante varias horas. El gusano se introdujo a través de un ordenador portátil de una subcontrata.
- **En 2010** se detectó Stuxnet en centrales nucleares. Gracias a la explotación de vulnerabilidades de día cero, logró parar la central nuclear de Natanz en Irán, destruyendo una quinta parte de los centrifugadores nucleares.
- **En 2012** la petrolera Saudi Aramco, sufrió el peor ciberataque de la historia en el que 35.000 ordenadores fueron borrados y la capacidad de la compañía para suministrar el 10% del petróleo de todo el mundo estuvo en peligro.
- **En 2014** un ataque dirigido a una importante empresa siderúrgica alemana provocó graves daños a la misma. Los atacantes utilizaron phishing e ingeniería social para acceder al sistema.

Creo que ya ha quedado claro con los ejemplos expuestos, que las intrusiones son posibles y se dan en infraestructuras de todos los países llegando a

causar graves destrucciones físicas. Si repasamos la cronología observaremos que las amenazas en los sistemas de control no son algo nuevo y han existido desde que estos se implantaron. Aprender de ellas, como en el caso de la planta de tratamiento de aguas de Maroochy (donde un simple cambio de las contraseñas habría evitado el incidente) es vital para no tropezar dos veces en la misma piedra. Lo que me parece preocupante es el creciente desarrollo de herramientas que permiten divulgar información sensible que facilita la explotación de las mismas y coincido con la opinión de los expertos, en que la evolución de este tipo de ataques ira en aumento. Esperemos que las compañías se preparen a conciencia ante su inminente proliferación……

El buscador mas terrorífico del mundo

Está claro que Stuxnet no fue el primero pero marcó un antes y un después. Su objetivo, reprogramar las centrales nucleares Iraníes para conseguir acabar con el plan de enriquecimiento de uranio. Años más tarde se descubrió que EEUU e Israel estaban detrás del arma de ciberguerra más sofisticada descubierta hasta ese momento. Este fue el punto de inflexión que puso el foco en los sistemas de control industrial (SCI) y abrió nuevas vías de investigación en este tipo de entornos que hasta entonces no habían sido atacados de forma tan arrolladora. A partir de entonces se han desarrollado numerosas herramientas para facilitar la búsqueda de vulnerabilidades y a su vez exploits que aprovechan esas vulnerabilidades encontradas en los dispositivos. A día de hoy una de las herramientas más conocidas y que tiene su aplicación en temas de auditoría y pentesting en los sistemas de control industrial es Shodan.

Shodan es, en pocas palabras, un buscador de direcciones HTTP, algunas de las cuales pertenecen a la llamada deep web y no las encontrareis en las búsquedas “normales” de Google o Bing. Su propio creador John Matherly lo ha

definido como “el buscador mas aterrador del mundo”. Por algo le puso el nombre de la inteligencia artificial malvada del mítico videojuego System Shock. La verdad es que es sorprendente la cantidad de dispositivos visibles que podemos encontrar en la red a través de este buscador del “Internet de las cosas”. Podemos encontrar desde alarmas, cámaras de seguridad, webcams, wearables, y cualquier otro dispositivo conectado que se nos ocurra. Lo llamativo del asunto es que también podemos localizar sistemas Scada o PLCs de infraestructuras críticas como sistemas de refrigeración, centrales nucleares y hardware que controla todo tipo de redes eléctricas, semáforos, etc.

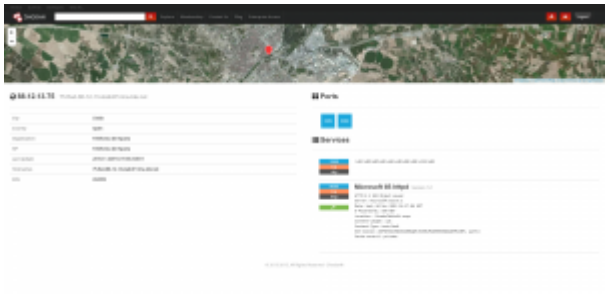
En realidad Shodan no hace nada ilegal por sí solo, porque lo único que hace es recopilar enlaces a dispositivos conectados a Internet y una serie de datos relativos al sistema. Se calcula que a día de hoy, añade más de 600 millones de registros al mes, casi nada ehhh!!. Su creador dice que da miedo, pues sí, la verdad es que a mi si me da un poco al pensar en lo que se puede hacer con toda esa información. No hace falta ser un genio para deducir lo que alguien malintencionado podría hacer con la dirección IP de aplicaciones servidoras que controlan desde una central hidroeléctrica, cámaras de circuito cerrado de infraestructuras críticas o hasta el ordenador de una planta de tratamiento de aguas. Especialmente teniendo en cuenta que algunos de estos dispositivos podrían estar funcionando aun con contraseñas por defecto, o de un bajo nivel de seguridad como se ha demostrado en algunas auditorías de seguridad.

Vamos a ver qué podemos hacer con esta potente herramienta. Para manejar Shodan no es necesario tener grandes conocimientos ni habilidades en materia de ciberseguridad a nivel industrial porque su uso es muy intuitivo. Yo ya lo había utilizado antes para realizar otro tipo de búsquedas y os voy a mostrar una pequeña prueba de su potencial para que os hagáis una idea de los sistemas que tenemos accesibles a un solo click de ratón. Solo tenemos que teclear en el buscador la clase de dispositivo que queremos encontrar (scada, hmi, plc, boa, eig, energyICT, etc..) y jugar con alguno de los filtros que tenéis a continuación:

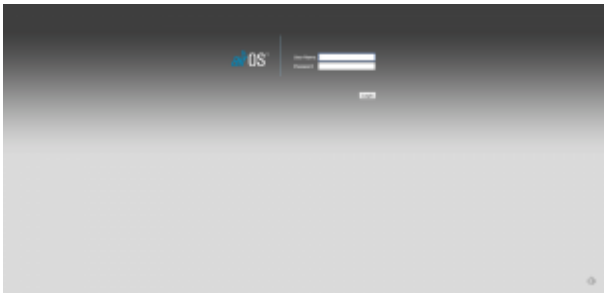
- country: Filtra resultados por país
- city: Filtra resultados por ciudad
- port: Filtra por puerto
- hostname: filtra los resultados por dominio
- org: Filtra por el ISP
- hostname: Filtra los resultados por dominio
- net: Filtra una ip específica o rango de ips
- os: Filtra por un OS en específico

Como podréis comprobar si hacéis la prueba, la cantidad de resultados (si aplicamos los filtros correctamente) es bestial. En el siguiente ejemplo, es de aquí cerquita, podemos ver un panel scada que controla una serie de depósitos para tratamiento de aguas en diferentes zonas de la localidad de Lleida. Y también tenemos acceso a una serie de datos relativos al servicio como: ISP, ubicación, sistema operativo, puertos, nodo de acceso, etc..

http://88.12.13.75:8080/Scada/Scada/SynopticForm.aspx



Este es solo un ejemplo, pero podéis encontrar más repartidos por todo el mundo. En estas otras capturas de pantalla sacadas ayer mismo, se muestran algunos de los muchos portales de login que dan acceso a controlar sistemas industriales de tipo Scada o PLCs.



No podemos subestimar la cantidad de conocimientos técnicos que realmente se necesitan para pasar del descubrimiento del sistema a la explotación de una vulnerabilidad en el mismo. Todo aquel al que le gusten los temas de seguridad informática como a mi, sabe de lo que hablo. No es tan fácil como en las películas, en las que un adolescente se apodera de una base militar y la maneja a su antojo. Aun así, me sorprende que algunos de estos sistemas ni siquiera implementen algunas medidas “básicas” de seguridad como: filtrado de IPs (whitelist), acceso VPN o conexiones cifradas. Que algunos hasta tienen telnet habilitado!!!. ¿Me pregunto si no saben que existen multitud de herramientas como Hydra o Medusa?. Que si, seguramente estarán cubiertos, y puede que sus contraseñas sean lo suficientemente robustas como para soportar un ataque de diccionario, pero, ¿y si no lo son?. Puede que necesiten tener acceso a su administración de forma remota por una causa justificada, pero no creo que tener estos servicios tan “visibles” sea lo más inteligente, la

verdad.

Con este post solo he querido indagar un poco más sobre las amenazas que se ciernen sobre los Sistemas de Control Industrial. Pero ahora me gustaría dar un giro y recordar que casi todos los dispositivos que tenemos a nuestro alcance ya vienen con conexión a Internet y que ello tiene implicaciones de seguridad. Recordemos que aunque no aparezcan en una búsqueda de Google, no significa que no sean “accesibles”…

¿Te atreves a soñar?

El otro día en clase, vimos un vídeo (inknowation) muy chulo donde explican con una animación gráfica como la “zona de confort” es un estado mental que no permite nuestro crecimiento personal. La verdad es que el vídeo te hace pararte a pensar y voy a dedicar unos minutos a escribir las ideas que se me pasaron por la cabeza al verlo.

A modo anecdótico diré que opinar sobre el tema puede tener su puntito de ironía, sobre todo si lo analizamos desde el punto de vista de un “informático”, que generalmente se ciñe al modus operandi de que: “si algo funciona mejor no cambiarlo”. No lo digo concretamente por mi, porque por suerte o por desgracia, me ha tocado salir fuera a explorar en más de una ocasión. Unas veces por propia decisión y otras veces ha sido la propia vida la que me ha sacado de repente de mi zona de confort (enfermedad, accidente, pérdida de empleo, etc,,) y os aseguro por propia experiencia que no suele hacerlo con amabilidad. Lo digo, porque que he oído tantas veces lo de “hay que salir de la zona de confort” y después veo que son muy pocas las personas que lo llevan a cabo por su propia voluntad, que al final acaba sonando un poco a tópico. Creo que es una de esas cosas que todos sabemos que deberíamos hacer pero que en general no las solemos hacer hasta que nos pasa “algo” que cambia nuestra percepción de aquello que nos rodea.

En fin, algo que no podemos negar es que nuestro cerebro funciona desde pequeños creando patrones que repetimos una y otra vez y si no lo forzamos un poco le gusta quedarse ahí, en la zona “cómoda”, en ese lugar donde podemos poner en marcha dichos patrones de manera automática y donde tomar una decisión no requiere pensar demasiado, solo hay que dejarse llevar y actuar como lo hacemos siempre. Por lo tanto, podríamos decir, que dentro de la zona

de confort lo único que hacemos es reaccionar, arrastrados por aquello que ya hemos vivido, independientemente del resultado que hayamos obtenido anteriormente. Según dicen los expertos en psicología, el cerebro además de crear rutinas persigue alcanzar un estado de bienestar, con un gasto mínimo de energía y asegurar la supervivencia. Por eso, tendemos a la repetición y a rechazar o ignorar aquello que se sale de nuestro guión, lo que nos lleva a marcarnos unos límites que acotan nuestra visión y expectativas ante la vida. Esto nos puede mantener estancados en una de las dos caras que conforman la moneda. En la cara o "zona de confort" donde estamos relajados y viviendo bien, pero sin avanzar. Por ejemplo, cuando tienes un trabajo en el que te pagan bien y llevas una rutina cómoda, pero no acaba de llenarte. O en la cruz, o (no se como llamarlo) "zona de no-confort" donde tu situación es realmente mala pero tampoco te atreves a cambiar por temor a perder tu seguridad y por miedo a lo desconocido. Por ejemplo, si te explotan en tu trabajo pero al final piensas "más vale lo malo conocido…."
Lo que está claro que en ambos casos necesitarías un cambio, sino nunca tendrás la posibilidad de crecer o de mejorar tu vida.
Vale !!, si ya hemos identificado que necesitamos un cambio, para "bien" o para "mejor" (ser positivos es algo fundamental en todo esto), ¿que podemos hacer al respecto?. La verdad es no soy un experto en el tema y seguro que un psicólogo o coach (que ahora están tan de moda) te podrían dar mejores pautas y consejos a seguir, estoy segurisimo. Aun así, me voy a aventurar y poner algunas que a mi me han funcionado, o al menos eso creo yo

- **Analiza tus propias excusas para no hacer algo**
  Sin dudarlo, me parece que el mayor problema a la hora de salir de la zona de confort son las excusas. Se auto-crítico y pregúntate si de veras son creíbles esas excusas que te pones, pero como si seria otra persona la que te las está contando. A lo mejor te das cuenta que pueden ser absurdas y no basarse en la realidad, y aun así, te las llegas a creer y actúas en base a ellas.
- **Márcate metas continuamente**
  Obvio, ¿no?. Creo que la clave del éxito está en fijarse una meta y despertar un desafío en nosotros mismos que nos ayude a superar los retos que surjan en el camino hacia esa meta. Lo dificultad está en encontrar tu propio desafío, algo que de verdad te motive, que te motive tanto que haga que no quieras tirar la toalla en los momentos verdaderamente difíciles. Y eso amigo, es algo que nadie mas podrá hacer por ti.
- **Estate en continuo movimiento**
  Es fácil creer que cuando ya has alcanzado lo que para ti es el éxito (esto ya es percepción de cada uno), ya tenemos el éxito de por vida y esto puede hacer que pierdas tu espíritu luchador y te acurruques en tu zona de confort a contar ovejitas. Por eso, debemos mantenernos siempre en movimiento, para que ese esfuerzo nos mueva en dirección a nuestras metas y porque como he dicho antes , la vida puede sacarte en cualquier momento de tu zona mágica y es mejor que te pille preparado.

Puede que a veces no te des cuenta de que ya estás cautivo de tu peor enemiga (la rutina) hasta que ya es demasiado tarde. Puede que simplemente, no sepas hacia donde ir o que no tengas un objetivo marcado. En cualquier caso, no te

quedes ahí parado mirando como pasa todo a tu alrededor, prueba a hacer algo distinto porque al final, todo lo que consigas dependerá de lo que tu creas….

¿Te atreves a soñar?

Realidad o ficción, ¿como es nuestra vida en Internet?

La verdad es que esta reflexión, no se si tiene mucho que ver con la asignatura de Sistemas de Información pero me lleva rondando por la cabeza desde hace tiempo y voy a aprovechar este post para dar mi opinión al respecto. Después de haber visto en clase lo que las empresas pretenden transmitir al publicar su visión, misión, valores… me ha parecido interesante extrapolarlo al entorno de los mortales y mostrar como, sin una «planificación estratégica» de lo que publicamos de nosotros mismos en la red, los demás pueden tener una imagen distorsionada de como somos en realidad.

Tengo amigos y conocidos, que a veces me parecen desconocidos (que no se enfade nadie, no es nada personal, os lo aseguro). Porque digo esto, pues porque veo sus vidas a través de internet y no les reconozco. Esto me hace plantearme quiénes son realmente, ¿ese perfil del cara a cara? o ¿el perfil de internet?, a veces me asalta la duda. Seguro que todos tenemos a alguien así a nuestro alrededor, solo hay que fijarse bien, y si no echa un vistazo. La verdad es que algunos dejan documentado cada paso que van dando: su perfecto desayuno, sus idílicas vacaciones, su perfecta familia, su perfecto "todo"… y aunque no quieras acabas viéndolo. Sí, ya sé lo que me vas a decir, puedes configurar tus perfiles en las redes sociales para ver según qué contenido, y es verdad, tienes razón, pero eso es elección de cada uno. Solo hay que mirar las fotos que se cuelgan, algunas hasta editadas con Photoshop o algún otro programa de retoque fotográfico que ya incluye la propia cámara o móvil. Lo que vemos es solo una parte de la historia y no sabemos si ese sol tan radiante que aparece en la foto acababa de salir y llevaba un mes lloviendo, si esa fiesta no fue tan divertida, o si la rubia que está a su lado es su prima. Nuestra imaginación rellena el resto de la historia, pero

no te la creas demasiado porque las cosas no son siempre lo que parecen. Lo que ves en esas fotos dura los mismos segundos que tarda la cámara en sacarlas y del resto del día no tienes ni idea. Hay muchos estudios que demuestran que en las redes sociales tendemos a exponer lo mejor de nosotros mismos para buscar la aprobación de los demás y publicamos cosas susceptibles de recibir un «me gusta», mientras que evitamos compartir otras menos atractivas a la vista de los demás. Vale, está claro que esto es propio de la conducta humana, pero me pregunto donde esta el limite y si en algunos casos esta conducta se vuelve adictiva, estoy seguro que sí.

Otro punto a tener en cuenta es que los usuarios somos conejillos de indias. Hubo un caso hace un par de años que levantó mucha polémica. Facebook manipuló en secreto las cuentas de 700.000 usuarios para estudiar el impacto de sus emociones ante lo que se publicaba en su newsfeed. Al final, los investigadores concluyeron que los usuarios utilizaban palabras positivas o negativas dependiendo del tipo de contenidos a los que habían sido "expuestos". El de Facebook es solo un ejemplo pero si buscas en internet puedes encontrar muchos más. Así que, entre lo que manipulamos nosotros y lo que manipula la red de redes, que imagen se crea de nosotros hacia los demás. Estoy seguro que es muy distinta de la realidad y no quiero ni pensar en la cantidad de complejos y envidias que esto puede crear en personas inseguras o con una baja autoestima. Las cifras nos dicen que una de cada tres personas se siente peor y más insatisfecha con su vida personal después de visitar las redes sociales. Las fotos de las vacaciones o eventos son el elemento que genera más resentimiento, mientras que en segundo lugar están las interacciones sociales: el número de «me gusta», felicitaciones o los comentarios recibidos. Y hay más, ser testigo de las exitosas vidas de otros puede provocar frustración, sensación de soledad y enfado, al compararlas con la nuestra propia.

Esta distorsión se traduce también a los perfiles de tipo Linkedin o portafolios. Un día hablando con un amigo sobre este tipo de redes profesionales le anime a crearse un perfil profesional. Al de unos días me llega el típico mensaje de correo, "Mira el perfil de … ". Pues nada vamos a echarle un vistazo. Madre mía !! si te conozco de toda la vida, pero donde estabas tu escondido. Vamos que si soy un reclutador de la NASA ni me lo pienso, te contrato fijo. Está claro que se lo comente al día siguiente, y su respuesta fue: "Hombre, hay que venderse…". El problema es que se lo había creado demasiado "profesional", ya me entendéis. Pero bueno, al menos nos reímos un rato.

Con esto no pretendo juzgar a nadie, ni mucho menos, pero si sirve para que alguien abra los ojos y le ayude a bajar al "suelo" de internet me doy por satisfecho. No hace falta estar siempre arriba tocando techo, por abajo también pasan cosas interesantes que nos perdemos por nuestra vanidad. Mi humilde consejo es que trates menos de parecer feliz y perfecto virtualmente y más de serlo en la vida real, y si de verdad quieres conocer a alguien, procures pasar más tiempo con el.

Pero como he he dicho al principio del post, esto es solo una opinión personal…..

Welcome to the real world…..

Repositorios de información para el ciberataque.

Durante la búsqueda de información para documentar mi trabajo de sistemas de control industrial y sus riesgos asociados, me he topado con esta noticia que me ha resultado muy interesante…. y que en parte, nos afecta a nosotros por estar vinculados al mundo universitario. Esta noticia fue publicada el año pasado y aquí os dejo el link por si queréis echarle un vistazo en profundidad o queréis descargaros directamente el informe que incluye.

http://www.efefuturo.com/noticia/alimentacion-industria-quimica-y-agua-vulnerables-a-ciberataques/

En resumen, la noticia viene a describir las conclusiones recogidas en un informe técnico sobre “Protección de Infraestructuras Críticas” publicado por la empresa de ciberseguridad “S2 Grupo”, que se centra especialmente en los procesos y gestión de seguridad de dichas instalaciones. Según S2 Grupo, los sectores de la alimentación, la industria química y el agua son los más vulnerables ante ciberataques dentro del sector industrial español, y en el lado contrario sitúa a los sectores sanitario y aeroespacial como los más precavidos a la hora de controlar la publicación de sus datos en internet para garantizar su seguridad.

Hasta aquí, nada raro ¿no?, o por lo menos a mi no me sorprendió especialmente. Si lo comparamos con otros informes similares realizados por otras empresas de consultoría, más o menos viene a decir lo mismo. Lo que más me chocó, es como se describen casos particulares de empresas (sin dar nombres por motivos de confidencialidad) que definen como “vulnerables” a causa del esparcimiento de sus datos sensibles que podrían resultar útiles a un atacante, y todo ello con una simple búsqueda a través de internet. Me hace gracia que digan que no publican los nombres de las empresas por motivos de confidencialidad y sin ir más lejos, por poner un ejemplo, muestren la imagen de la portada de un proyecto fin de carrera con su logo universitario, la temática del proyecto y hasta la fecha de publicación, en el que se

detalla un sistema cuyo mal funcionamiento podría dejar fuera de servicio las instalaciones de una gran organización dentro del ámbito químico Español. Me picaba la curiosidad y me he puesto a buscarlo. Solo me ha llevado un minuto encontrar el proyecto (bueno cinco o diez, jeje). He buscado en imágenes de Google el logo de la universidad, después proyectos asociados a esa universidad, y…. !! Vualá !!!, aquí lo tenéis:

http://deeea.urv.cat/public/PROPOSTES/pub/pdf/1195pub.pdf.

Con esto no pretendo incitar a que alguien haga alguna “travesura”, no me malinterpretéis, ¿ehhh?, (sed buenos por favor), ni tampoco quiero tirar por tierra el trabajo de “S2 grupo”. Mi intención era ver, si tan fácil es poder acceder a este tipo de información comprometida. Pues si !!! , y este es solo un ejemplo.

A lo que íbamos , que me desvío del tema. Lo alarmante del caso es que muchos de estos datos se publican en proyectos de fin de carrera y tesis doctorales con una descripción exhaustiva de componentes, instalaciones y sistemas de control vulnerables. De hecho, algunas universidades se han convertido en auténticos repositorios de información técnica muy específica y fácilmente accesible por cualquiera, sin ser conscientes de la responsabilidad que implica manejar correctamente este tipo de información sensible. En la otra cara de la moneda nos encontramos nosotros, los estudiantes, que al fin y al cabo somos los que realizamos el trabajo de investigación y lo exponemos al mundo. En mi opinión, somos nosotros, quienes mayor cuidado deberíamos tener con aquello que publicamos, porque quizás sin darnos cuenta, le estamos facilitando el trabajo a los “malos”….