DIAGNOSI DI SISTEMI INFORMATICI

Nel variegato mondo dell'informatica, denso di professionalita' **alternative**, nuove, nate dal nulla e spesso molto importanti sia a livello di marketing che operativo, ci ha colpito quella che sembra una "nuova professione" di indubbio fascino, anche perche' "**trasversale**" e sicuramente "difficile" sotto tanti punti di vista: quella del tecnico specializzato in "diagnosi".
Ne parliamo con **Carloalberto Sartor** di DigitalExpert.it, uno dei professionisti che opera da anni in questo particolarissimo settore.

Se ho capito bene, Carloalberto, se mi si blocca il computer io dovrei chiamarti, giusto?
"Dunque... no... non mi devi chiamare per questo... o meglio... mi devi chiamare solo dopo che il personale tecnico che gestisce i tuoi sistemi non e' riuscito a risolvere il problema, senza capirci un gran che'. Il mio lavoro non e' quello di intervenire a fronte di un problema. Molti problemi comuni sono normalmente risolti dai tecnici che si occupano di manutenzione. Mi puoi chiamare solo in casi particolari e quando e' evidente che "non se ne va fuori"

Quindi il tuo lavoro e' quello di arrivare li' dove gli altri "non ce la fanno"?
"Beh... si... in un certo senso si... c'e' un caso particolare, difficile... apparentemente impossibile... si chiama una persona che ha delle competenze particolari per affrontare una situazione particolare. Mi sembra che accada anche in altri ambiti... Ti rompi una gamba e il problema sembra sia particolarmente difficile da curare? Ti rivolgi ad un ortopedico specializzato, il quale ha appunto competenze particolari che l'ortopedico ospedaliero "classico" non e' detto che possieda.... anzi... che non ha nemmeno sensato motivo di possedere perche' per suo ruolo non e' un ortopedico specializzato in gambe mal fratturate, visto che un ortopedico ospedaliero deve poter mettere le mani su qualunque tipo di ossa fratturate. L'esempio che farei e' proprio quello dello specialista in rapporto ad un medico normale. Non c'e' un "io valgo piu' di lui", ma un semplice "io ho competenze per affrontare queste cose, lui ha competenze per affrontarne altre."

Non e' che stai lisciando il pelo ai tuoi colleghi che, spesso, vedendoti arrivare non e' che fanno propriamente dei salti di gioia?
"Quello dell'odio acerrimo tra chi gestisce i sistemi e chi viene chiamato ad effettuare interventi diagnostici d'urgenza e' decisamente un mito da sfatare. Nella maggior parte dei casi quando si arriva "sul luogo del sinistro" il primo ad essere contento del nostro arrivo e' proprio chi gestisce i sistemi e ne ha responsabilita'. Non vede l'ora che gli risolviamo il problema.
Quella della diagnosi d'urgenza effettuata da una persona del tutto estranea all'azienda in cui vi e' il problema da risolvere e' ovviamente un'occasione in cui, per certi versi, il gestore dei sistemi puo' avere la senzazione di essere "sotto esame". Come il medico a volte puo' farci delle domande sgradevoli per capire cosa c'e' che non va', cosi' ci si puo' trovare a porre delle domande a volte "urticanti" o che possono far percepire l'esistenza di una revisione critica delle attivita' svolte dal gestore stesso o dai suoi sottoposti. Ci si accerta di cosa e' stato fatto, come, perche'. Non sono domande tese a "misurare" le capacita' tecniche delle persone ma sono domande che fanno parte di un preciso percorso volto a capire cosa e' successo, come si e' sviluppata l'anomalia, quali segnali essa ha lanciato prima di "esplodere".....

Mi stai comunque dicendo che di fatto fai un vero e proprio processo sommario o sbaglio?
"No, no.... macche' processi.... e' piu' chi fa' questo tipo di interventi che e' costantemente sotto processo e sotto la lente d'ingrandimento di chi l'ha chiamato! Io farei sempre il parallelo col medico. Quando tu hai mal di pancia perche' hai stramangiato, il medico ti chiede cosa hai mangiato e tu, man mano lui ti chiede cosa hai preso di primo, di secondo, di contorno eccetera, e' chiaro che vedrai che alla lista dei secondi piatti comincia a guardarti strano o a far gesti dal chiaro significato tipo "... e ci mancava anche l'abbacchio, dopo l'arrosto e la fiorentina!"... Il medico non sta ridendo del tuo approccio al cibo, sta semplicemente ragionando in dettaglio su

quella parte dello "schema a blocchi" in cui chi si mangia tutta quella roba e' evidente che non puo' star bene! Faccio un esempio "tecnologico" che e' capitato spesso. Sbadatamente qualcuno ha cancellato dei files importanti di sistema. A quel punto spegnere ed accendere vuol dire quasi sicuramente "perdere" il funzionamento del sistema stesso, mentre mantenendolo acceso e sapendo cosa si e' cancellato, magari si riesce a recuperare il danno senza grandi problemi. Ecco quindi che davanti al tecnico che ti dice: "dopo aver cancellato erroneamente i files, ho immediatamente riavviato il computer e.... trac!"..... e tu a qul punto alzi le braccia, ovvio! Perche' per la tua esperienza era ovvio che non doveva fare cosi', mentre per l'esperienza dell'utente, questa ovvieta' non c'e'. Non e' questione di ignoranza, perche' fino a che non hai fatto l'esperienza in questione, non puoi sapere quanto lo spegnimento e' "bloccante". Ribadisco il fatto che viviamo delle nostre esperienze o di quelle altrui se ci vengono riferite. Poi e' vero che a determinate considerazioni dovremmo e potremmo arrivarci con un pizzico di ragionamento e di logica. Ma purtroppo non sempre e' facile farlo, non sempre ci sono le migliori condizioni e ci vuole veramente poco per fare l'operazione sbagliata nel momento sbagliato! Poi ovvio che siamo degli esseri umani e che possiamo trovare estremamente comico "il film di chi a quel punto spegne" e magari ci scappa la battuta... Per quanto si stia parlando di tecnologia, qui le questioni sono soprattutto "umane"

Ecco... tecnologia: parliamo un po' di questo, altrimenti sembra che stiamo parlando di psicologia e non di sistemi piantati! Cosa mi dici delle tecnologie che utilizzi?

"Eh... beh... chiaro che tecnologie se ne usano, ed anche parecchie! Pero' se e' vero che le tecnologie sono importanti, io concentrerei piu' il discorso sulla sinergia tra strumenti e metodi, piu' che di mera tecnologia. Si ha spesso l'errata percezione che una buona diagnosi abbia solo bisogno di un buon programma diagnostico ma questo e' solo parzialmente vero, anzi, spesso non lo e' poi molto, perche' gli strumenti vanno diretti, vanno scelti, vanno messi in opera percorrendo una certa logica, scomponendo il problema in elemti specifici.... gli strumenti danno dei numeri che spesso vanno letti ed interpretati all'interno di quello che puo' essere un complesso "puzzle" di azioni, effetti e controreazioni.

Bel discorso, pero' non mi hai fatto un nome, non mi hai citato uno strumento! Chi ci legge arde dalla voglia di sapere cosa si usa, dai!

"Non volevo eludere la domanda, stavo ambientando la risposta, che non e' semplice ne' stringata..... Che strumenti uso? Ne uso molti e comunque non c'e' uno schema completamente fisso e ripetibile.... uso un insieme di strumenti che vanno dagli analizzatori del traffico agli strumenti di lettura di "telemetrie" di apparati e sistemi. Uso degli strumenti che catalogano la realta' in cui avviene il problema, secondo vari aspetti, piu' o meno mirati al caso specifico. In ogni caso ci sono delle necessita' preliminari di avere un quadro di insieme del contesto in cui si presenta il problema, quindi sostanzialmente una prima azione abbastanza frequente e' quella dell'inventario di rete, sia in termini di mera esistenza che di ruolo. Abbiamo gli erogatori di servizio, abbiamo chi il servizio lo utilizza, abbiamo apparati che gestiscono le comunicazioni tra erogatori e fruitori, giusto per dare un elemento.

Conosco i software di inventario. Vuoi dire che ti passi tutti i computer per installarci quel software? Ci metterai una vita!

"No... certo che no.... la prima regola e' di non installare nulla.... il campo operatorio va osservato senza introdurre variabili...."

Bacchetta magica, allora?

"eh, magari esistesse.... io di solito faccio un inventario passivo e solo dopo aver capito che posso permettermi il lusso di farlo, eseguo un inventario "attivo" con cui capire esattamente come e' composta la rete del cliente. Queste operazioni mi permettono di avere sia la composizione del puzzle che il come i vari componenti interagiscono tra loro... e se ci sono nodi che non interagiscono, li vado a cercare con particolari strumenti...."

Ah, certo, gli scanner. Una volta ne ho lanciato uno in rete e mi si e' bloccata tutta l'azienda. Non userai mica robe del genere?

"Io uso strumenti miei... realizzati con una maniacale attenzione ad evitare effetti inattesi... anche a costo di lavorare con velocita' inferiore rispetto a quella di altri strumenti.... impatti di basso profilo sono indispensabili non solo perche' per il principio di indeterminazione di Heisenberg ogni interazione introduce una alterazione ma soprattutto perche' la misura effettuata con uno strumento di "basso profilo" e' sempre piu' accurata di una misura effettuata "brute-force"...

Hai nominato Heisenberg. So benissimo che non e' un cantante rock. Qual e' il rapporto tra questo tipo di interventi e le conoscenze "accademiche" sul funzionamento dei computer?

"Mi fai una domanda scabrosa.... l'esperienza insegna che le realta' operative non sono sempre "coperte" da teorie e leggi "esatte" che ne spiegano il funzionamento. L'informatica e' di fatto piu' una tecnologia che una scienza, anche se ovviamente ci sono solidissime basi scientifiche che ne descrivono vari comportamenti. Di fatto quando fai diagnosi ti ritrovi molto spesso a doverti arrangiare e abbastanza raramente la componente "scientifica" ti da una mano. Provo sempre ad allacciarmi all'esempio del medico: il medico studia gli organi, il loro funzionamento specifico, le interazioni, anche... poi pero' quando si trova ad esaminare il paziente non e' detto che risolva il caso partendo da casi precedentemente definiti nelle pubblicazioni scientifiche..... le basi teoriche sono degli strumenti con cui affrontare un caso e, possibilmente, risolverlo.... ma non c'e' quasi mai un libro dove c'e' scritto quello che succede nella rete che stai esaminando!
Questo aspetto rende da una parte il lavoro sicuramente "non facile" pero' unendo esperienza, conoscenze e metodo, percorri una possibile ipotesi, la verifichi o la scarti. Quindi ti serve tutto, ti serve la conoscenza, ti servono gli strumenti, ti serve il metodo, ti serve l'esperienza. Ti direi anzi che la maggior parte delle persone che fa diagnosi, alla fine osserva dei comportamenti, definisce dei modelli e, molto spesso, produce documentazione scientifica su cio' che ha osservato."

Tu magari speravi di tranquillizzarmi, ma mi dai sempre piu' l'impressione che in mano hai soprattutto un bastone piegato ad 'Y', te ne rendi conto?

"No... rabdomanzia no, per carita'! Il problema e' che nei problemi "tosti", i meccanismi e le dinamiche che producono determinati effetti sfuggono alla percezione di chi gestisce i sistemi. Siamo talmente "virtualizzati" che abbiamo da tempo perso la visione di un sistema come se fosse composto da ingranaggi, motori, puleggie eccetera.... pensa che sembra incredibile ma anche i concetti "meccanici" o "elettrici" piu' elementari non fanno mai parte del know-how degli addetti ai lavori. E cosi' si stupiscono molto quando si rendono conto che molto banalmente determinati componenti non possono essere usati "contemporaneamente" ma che di fatto i sistemi serializzano in rapida sequenza le varie attivita', facendone comunque una alla volta... la "virtualita'" dell'informatica ha spesso effetti devastanti, perche' si perde il senso di "come lavora una cosa"... I computer sono apparecchiature estremamente stupide che eseguono quello che gli e' stato detto ma guai a non avere chiaro lo schema con cui un computer esegue un determinato compito.
Mentre nella vita reale appare ovvio il fatto di consultare un elenco telefonico usando determinati accorgimenti per trovare il piu' rapidamente possibile il numero che cerchiamo, nell'informatica spesso capita l'esatto contrario: c'e' un programma che "uno alla volta" legge i dati dell'elenco fino a trovare quello che cerchiamo. Peccato che se l'elenco e' piccolo ed il computer e' sufficientemente rapido, la ricerca e' sufficientemente rapida, diversamente la ricerca rischia di diventare lunghissima e di dare risultati quando ormai si ha accantonato l'idea di fare la telefonata in questione! La conoscenza dei metodi con cui sono fatti gli "ingranaggi" dei computer, dei programmi e delle periferiche e' quindi fondamentale per capire come si svolge l'attivita' che magari va piano o che si blocca!"

Ti stai contraddicendo: stavi parlando di specialisti ma qui mi sembra che stai delineando una specie di "tuttologo" che deve conoscere vita morte e miracoli di hardware e software!

“I tuttologi non esistono, ovviamente.... pero' e' chiaro che se tu hai un server di posta che va piano prima o poi tu o chi fara' la diagnosi non puo' non sapere come funziona “dentro” quel server di posta.... e non potra' non conoscere come funziona “dentro” il computer stesso, il sistema operativo, la scheda di rete.... la rete stessa.... e via dicendo.... senno' come puo' fare una diagnosi? Come in un concerto eseguito male, dovra' andare a riascoltare ogni strumento con davanti lo spartito e vedere chi ha sbagliato e perche'. Poi e' altrettanto chiaro che a furia di ascoltare concerti e di cercare errori di esecuzione, prima o poi arrivera' al punto che captera' immediatamente la nota stonata, riconoscendola per essere quella del violoncello....
Tornando all'informatica, e' chiaro che se non conosco come lavora uno switch non potro' mai capire cosa sta andado male in una rete e perche'. Altrettanto non mi sara' possibile dirti perche' sei lento a navigare se non so come funziona un server web, una pagina, una linea ADSL, come funziona il tuo pc e come lavora il tuo browser..... paradossalmente potrei conoscere alla perfezione come funziona il software di posta elettronica “al suo interno” e magari potrei non saperlo usare “come utente”.... non sono un tuttologo, sono specializzato nelle cose che mi servono per fare il mio lavoro... Si deve anche aggiungere il fatto che durante le diagnosi si entra spesso nel merito di aspetti di sicurezza informatica, di utilizzo del software, di personalizzazioni e di aspetti prestazionali di hardware, software, reti, connettivita'....

Ma quanta roba devi conoscere, allora? Non e' che devi viaggiare con l'enciclopedia?
“Beh, ovvio che ci vuole una conoscenza “non superficiale” di come sono fatti i computer, l'hardware, il sistema operativo, gli strati di rete, le periferiche... poi ci sono i programmi, i sottosistemi, le varianti tra sistemi diversi Windows, Linux eccetera.... la rete dal punto di vista hardware, le schede, hub, switches, router, bridges... ovviamente l'hardware ha al suo interno anche del software ed e' quindi comunque simile ad un computer con il suo sistema operativo e come tale va considerato.... poi ci sono i programmi... tra server web, server di posta, server di database, application server di vario tipo.... e ovviamente poi ci sono le strutture complesse.... il cloud.... le virtualizzazioni... un virtualizzatore e' comunque un programma e non sfugge quindi dalla necessita' di essere valutato in quanto tale....
Mi rendo conto che questa “vision” e' completamente diversa rispetto a quella di chi scrive programmi o gestisce i sistemi... ma chi fa diagnosi non puo' certo essere “compatibile” con chi i problemi li crea o li subisce e deve per forza avere dei punti di vista diversi e distinti su cui lavorare in termini analitici... quindi mentre lo specialista di prodotto conosce la specifica applicazione a menadito ma magari non sa come funziona un disco, io diagnosta devo sapere come la tua applicazione lavora e devo anche sapere come funziona un disco.... devo anche sapere che la tua applicazione probabilmente avra' “manopole” da regolare e devo avere un quadro abbastanza chiaro di quante e quali possono essere le manopole necessarie... ma le stesse cose le devo conoscere per il disco e per qualunque altra cosa esistente nella tua rete....
Puo' sembrare incredibile ma chi fa diagnosi spesso “vede” un'infrastruttura come se fosse una macchina vera e propria, con i propri ingranaggi, con le cose che si muovono fisicamente.... solo con visualizzazioni del genere si puo' comprendere cosa succede in determinate condizioni....

Quindi la visione dei sistemi informatici che ha chi li gestisce, rispetto a quella di chi ne fa la diagnosi e' completamente diversa?
“Si, completamente diversa, si potrebbe dire complementare, in quanto chi fa diagnosi deve entrare nel merito di operazioni spesso sconosciute a chi fa gestione. Sono ambiti culturali diversi e spesso la difficolta' sta appunto nel mettere in comunicazione nel modo migliore la “vision” del diagnosta con quella del gestore... non sempre e' facile.... pero' del resto se chi gestisce vuole avere dei sistemi perfetti dovrebbe di fatto acquisire lo stesso know-how posseduto dal diagnosta.... e qui sorgono i problemi.... il mercato tra crisi, mancata formazione ed investimenti all'osso non agevola questa duale visione dei sistemi, con la conseguenza di funzionamenti non corretti ed anomali sempre piu' frequenti. Del resto, non investendo in formazione, le aziende non possono avere le cose fatte bene: non si puo' avere la botte piena e la moglie ubriaca!

Comincio a capirci qualcosa, ma mi rendo conto che e' un gran casino, comunque!
"Beh, certo non e' semplice... o meglio... non sempre.... ma, ripeto, la cosa piu' difficile e' mettere attorno ad un tavolo le conoscenze specialistiche di chi gestisce e di chi crea applicazioni e servizi con le conoscenze "complementari" possedute da chi fa diagnosi..... e' su questo tavolo che si sviluppa l'intervento, di fatto. Perche' alla fine il diagnosta puo' anche risolvere in autonomia il problema correggendo l'errore ma, cosi' facendo, non ha migliorato la conoscenza del gestore, ponendo consistenti ipoteche su possibili altre anomalie.... Quindi la cosa migliore e' condividere conoscenze ed esperienze, shakerare bene e si ha il miglior risultato.

Adesso capisco un discorso che mi avevi fatto tempo fa sulla diagnosi come momento di formazione...
"Si, proprio perche' il diagnosta porta sul campo delle conoscenze complementari che il gestore non ha, la diagnosi e' anche un momento di formazione e di crescita in termini di esperienza.... anche il vedere mettere in campo medodi e "trucchi" serve a far crescere il gestore, il quale arricchisce il suo gia' ricco "orticello" con una serie di conoscenze dell'orticello del diagnosta.... di fatto vai dal medico e ne esci guarito e con un po' piu' di conoscenza su come funziona o non funziona il tuo corpo....

Ok, ma in tutto questo Phalanx cosa centra? Che cavolo e'?
"Te pareva che non ti perdevi questa parte? Beh.. discorso molto complesso in realta'... Phalanx e' un insieme di strumenti, un framework orientato a dei compiti specialistici tipici degli interventi diagnostici.... dentro c'e' di tutto... agenti software, tools diagnostici di vario tipo, sniffers, scanners, console di gestione di monitoraggio.... c'e' dentro di tutto... saranno circa 300.000 righe di codice, parte in linguaggio C, parte in PHP.... il software nasce come strumento diagnostico, come attrezzo mio.... come tale e' altamente personalizzato ma si puo' anche "piegare" a specifiche esigenze..... descrivere Phalanx ci richiederebbe tantissimo tempo, comunque... nemmeno io mi ricordo tutto, pur avendolo fatto!!!"

Quindi e' uno strumento unico? Irripetibile? Che cos'ha di particolare? Anche Wireshark e' uno sniffer e NMAP e' uno scanner... perche' dovrei usare i tuoi strumenti?
"Beh, Phalanx nasce e si evolve costantemente ed essendo prima di tutto il mio "strumento di lavoro" si evolve in base ai lavori che faccio, alle sensibilita' diagnostiche che emergono.... quindi senza nulla togliere a wireshark che e' uno strumento eccezionale (e che mi capita anche di usarlo, per doverosi confronti e "tarature" strumentali), lo sniffer di Phalanx e' concepito in modo da poter essere usato fornendo determinati risultati, tra l'altro utilizzabili immediatamente anche da altri strumenti del framework.... ad esempio, uno dei vari sniffer di Phalanx puo' essere lanciato automaticamente su un nodo anche senza avere alcuna console remota e puo' essere mirato a compiti di rilevamento ben precisi, con outputs fatti apposta per deteminate esigenze.... nulla che possa fare wireshark.... anche attivandolo da remote desktop Wireshark risentirebbe del traffico del remote desktop, per cui a livello di analisi dettagliata del traffico e delle sue eventuali influenze da e verso altri nodi di rete Wireshark non puo' dare il supporto che serve. E' anche un programma che va installato, che attiva dei drivers, che quindi altera il contesto di misura in modo significativo... questo e' proprio per fare un banale esempio....

Grazie della pazienza e... buon lavoro, Carloalberto
"Grazie a te!"

Un'ultima cosa... sempre incrociando le dita... se scrivendo questo pezzo mi si blocca word, posso chiamarti?
"Neanche morto! Chiama Microsoft!!"