
MICROSYS

Diario di un anno 2020

Cari Lettori e Care Lettrici,

mai come quest'anno si sente il bisogno di un sorriso che aiuti a superare problemi e difficoltà.

Spero che la lettura degli articoli pubblicati sul Controcorrente online e raccolti in questo quaderno, ne sia occasione.

Controcorrente che vuole, in modo ironico ma concreto, descrivere e commentare gli scenari e la tecnologia con l'obiettivo di offrire nuovi spunti di riflessione e di innovazione digitale.

All'interno troverete anche alcune delle ultime storie di successo raccontate dagli stessi protagonisti come:

Gruppo A2A, AIPB, Ca' Zampa, illimity e The Level Group.

Le storie di Gruppo A2A e The Level Group sono tratte dal report dell'Osservatorio Big Data & Business Analytics del MIP, di cui anche quest'anno siamo sponsor, e ne sono particolarmente orgogliosa.

Non dimentichiamoci poi delle APP Microsys per Dynamics BC che trovate sul market place APP SOURCE di Microsoft.

Auguro a tutti voi un Buon Natale e un nuovo anno ricco di prospettive e di speranze.

Alessandra Galdabini

CONTROCORRENTE

MFA

Due personaggi (tutsi, abissini, bantù, ???) camminano nella steppa, a piedi scalzi. Chiacchierano distrattamente del più e del meno. D'improvviso alzando lo sguardo si trovano di fronte un leone minaccioso, affamato (nel filmato, a dire il vero, pare un cucciolone, ma immaginatelo minaccioso).
Si bloccano, sanno che scappare sarebbe un errore. Poi uno dei due, con movimenti lentissimi, prende dalla sacca un paio di sneakers, e inizia a calzarle.
E l'altro: "non crederai di poter correre più forte di lui?".
"No, ma di te sì"

Faster than a lion? No, but faster than you (*).

Qualche settimana fa è entrata in vigore anche in Italia una direttiva europea che impone alle banche l'uso di sistemi di autenticazione multi-fattore per l'approvazione remota di transazioni bancarie, e più in generale per l'accesso ai servizi della banca.
Il motivo è chiaro, ormai la sola password non basta più. Non è una questione di complessità, di cambiare password, di tenere il post-it in cassaforte. Non c'è nulla da fare, se la cosa è importante la sola password non basta.

La password è insufficiente perché noi stessi non riusciamo a tenerla segreta. Siamo sempre più abituati ad accedere a sistemi on-line che ci chiedono user e password, e ogni tanto non prestiamo abbastanza attenzione a dove la stiamo mettendo. Ed è facile cascare in una trappola e immetterla in un falso sito della banca, o di Amazon, o di Office 365...
E in questo modo la raccontiamo al truffatore, che poi la usa per fare transazioni o per mandare mail a nome nostro ordinando bonifici verso una banca dell'est, ecc.

Quindi se la sola password è insufficiente allora le affianchiamo un secondo fattore: la password più il telefono ad esempio. O la password

* https://www.youtube.com/watch?v=NaDezMcSHqg&feature=youtu.be

più la chiavetta dell'home banking (ora bandita). O la password più il telefono che a sua volta ti riconosce con l'impronta. E così via.
Da un punto di vista puramente statistico la cosa ha senso perché le probabilità che ti scardinino sia la password che il secondo fattore, qualunque esso sia, sono il prodotto delle singole probabilità indipendenti, quindi bassissime.
Qui stiamo ipotizzando che la cattura della password sia un elemento più o meno casuale. Mandano milioni di mail e vedono chi ci casca. Allo stesso tempo rubano un sacco di telefonini. Poi se tra quelli che ci cascano uno ha un account interessante provano a rubare da lì, e se per caso hanno il telefono giusto ci riescono. Ovviamente le probabilità che gli finisca in mano proprio il telefonino di quella persona sono quasi nulle. Quindi la protezione via SMS funziona.

Ma è proprio così?
Non tanto.

Se il primo evento può essere casuale, il secondo potrebbe non esserlo. Becco la password di un personaggio che controlla un account importante. Poi gli rubo il telefono. Quello, non un telefono qualunque. Siccome quasi sempre il telefono mostra un sms in arrivo anche senza chiedermi il pin o l'impronta, il secondo fattore lo aggiro facilmente.
Se rubo quello specifico telefono.
Quindi devo essere nella stessa città della vittima, o andarci, o trovare un socio in quel posto.
Oppure agisco sull'operatore e lo convinco che sono il proprietario di quel numero e che ho perso la sim. Devo essere capace di truffare l'operatore, ma in compenso non serve avvicinare la vittima.

Anche i meccanismi basati sull'impronta digitale (e non sms) sono aggirabili. Posso mettere in piedi un sito che finge di essere la banca e che chiede di verificare l'impronta, mentre dietro le quinte fa una transazione e quindi scatena una vera richiesta di verifica. È più difficile, costoso e soprattutto deve essere un attacco mirato. Devo indentificare una vittima e lavorare su quella.

Il secondo fattore non è imbattibile, tutt'altro. Un attacco mirato, e piuttosto sofisticato può aggirarlo, ma una semplice mail di phishing non sarà sufficiente, ci vuole una organizzazione, competenza e servono investimenti.

Un interessante approfondimento sull'argomento lo si può trovare

qui: https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/All-your-creds-are-belong-to-us/ba-p/855124.
La sicurezza non è mai assoluta. È sempre relativa. Le probabilità di essere vittima di un furto possono essere più o meno alte, in funzione di quanto sono sofisticate le difese, ma non saranno mai nulle.

E il leone?
Cosa c'entra il leone?

È semplice: ci basta rendere le nostre sicurezze abbastanza buone da spingere il ladro a rubare da qualche altra parte, perché è più facile. Sarà un po' cinico, ma è così. E questo obiettivo lo raggiungo in pieno con la MFA.

Proprio come col leone.

È L'ALGORITMO, STUPIDO

O È L'ALGORITMO A ESSERE STUPIDO?

Secondo wikipedia la frase "The economy, stupid" è stata coniata da James Carville, uno stratega della campagna elettorale di Bill Clinton. È sicuramente così, ma a noi piace pensare che sia stata ispirata dal mitico "giù la testa, coglione" di Giù la testa, il film di Sergio Leone. Ma non importa, e non c'entra.

Qualche settimana fa David Heinemeier Hansson (@DHH) ha twittato questo:

Ne sono seguiti una serie di aggiornamenti sulla assurda posizione di Apple e di Goldmann Sachs (che in effetti emette la carta) e sulla loro incapacità di spiegare come fossero arrivati a una simile conclusione e come giustificavano l'ovvia disparità di trattamento apparentemente legata al genere.

Vi risparmiamo l'infinità di tweet e articoli che sono scaturiti da que-

sta prima osservazione. Moltissimi hanno detto di aver subito lo stesso trattamento, molti politici hanno detto l'ovvio, che non era giusto.

Alcuni hanno risposto con insulti di vario tipo (ma perché c'è sempre qualcuno pronto a insultare sui social?). Il New York State Department of Financial Services ha aperto una inchiesta per stabilire se ci siano state discriminazioni basate sul genere, che sarebbero vietate dalla legge. Senza entrare nei dettagli, proviamo a riassumere alcune affermazioni e giustificazioni di Apple:

- Non sappiamo perché ha fatto così, ma il genere non c'entra. Davvero. Lo giuro!
- Gli elementi di validazione sono molteplici, forse non tutti erano uguali tra DHH e la moglie
- Non possiamo dire quale parametro ha determinato questo risultato
- Aumentiamo il fido di sua moglie (ma la smetta di massacrarci con Twitter)

Queste sono le risposte che hanno dato direttamente a DHH, ma per molto tempo hanno evitato qualsiasi dichiarazione pubblica sulla faccenda.

Ora, consideriamo che per la legge americana non si potrebbe negare un credito solo sulla base di un algoritmo, senza poi giustificare la decisione, mentre il GDPR esplicitamente dice che l'utente deve poter chiedere una valutazione non automatizzata. Quindi queste risposte sono in ogni caso contrarie a quella che dovrebbe essere la regola.

Ma tutto questo non è il punto di cui vorremmo parlare. Vorremmo parlare dell'elefante nella stanza: l'Algoritmo.

Algoritmo: un procedimento a passi per risolvere un problema o raggiungere uno scopo (Merriam-Webster), oppure, dalla Treccani: l'espressione in termini matematicamente precisi di una procedura generale, di un metodo sistematico valido per la soluzione di una certa classe di problemi.

Ok, quindi l'Algoritmo è l'insieme di operazioni da fare per raggiungere un certo risultato. Il computer è l'esecutore dell'algoritmo. Una volta che ho definito e correttamente implementato l'Algoritmo lo posso eseguire su dati diversi per ottenere i risultati che mi servono.

Ovviamente di algoritmi interessanti o meno ce ne sono tantissimi, da per esempio quello per sommare due numeri interi (lo ricordate? lo

insegnavano alle elementari... ma chi lo usa più?) a cose molto complesse che oggi chiamano AI (sarebbe intelligenza artificiale, ma evidentemente non riusciamo a usare l'italiano nemmeno negli acronimi) e che sono per esempio sofisticate analisi statistiche, complesse reti neuronali, o semplici alberi decisionali che di intelligente hanno poco.

Gli algoritmi di cui parliamo oggi devono affrontare problemi del tipo "Diamo un mutuo a questo signore?", "Che massimale mettiamo in questa carta di credito?", "cosa potrei vendere a questo cliente?", "E' il caso di assicurare questo automobilista?". In ingresso riceveranno delle caratteristiche della persona in oggetto, in uscita produrranno un responso di qualche tipo.

Ma come è costruito un algoritmo che fa questo?
Alla fine si tratta sempre di varianti di un procedimento che parte da prendere dati storici, raccolti in vari modi, insieme con le risposte corrette per ogni dato, e metterli in un gigantesco "tritadati" (*), per costruire un meccanismo che dia le risposte giuste per quei dati, e che quindi ci aspettiamo dia risposte giuste anche per dati nuovi, come per analogia. E non sempre le ragioni per cui l'algoritmo emetterà un certo verdetto saranno ovvie, anzi certe volte saranno incomprensibili o addirittura illogiche (**).
Il che non è poi tanto diverso da come funziona l'intelligenza vera, che per giudicare le persone si basa anche su quello che l'esperienza ci ha insegnato. Alcune volte è inconscio (ho paura dei cani perché da piccolo sono stato morso, ma nemmeno lo ricordo), altre è ragionato, logico (in auto con maschio, giovane, neopatentato = meglio se guido io).

* un'interessante considerazione relativamente ai modelli di intelligenza artificiale, è che la fase di messa a punto dell'algoritmo (l'allenamento, "training") è molto più costoso in termini di soldi e energia di quanto si possa aspettarsi: https://www.technologyreview.com/s/613630/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes

** Certe volte il modo di ragionare dell'Algoritmo può essere anche sbagliato, ma l'errore potrebbe non essere evidente: "Un esempio che mi viene sempre in mente è di come una rete neuronale aveva imparato a distinguere cani da lupi. Non aveva imparato la differenza tra cane e lupo, ma invece aveva scoperto che i lupi stanno nella neve, i cani sull'erba". Ovviamente c'era un errore sistematico nelle foto usate per allenare l'algoritmo. https://hackernoon.com/dogs-wolves-data-science-and-why-machines-must-learn-like-humans-do-41c43bc7f982

L'Algoritmo tutto sommato fa la stessa cosa. Si basa su quello che è stato (le statistiche, i dati storici) per predire quello che, secondo l'Algoritmo, probabilmente succederà (questo signore potrebbe essere un truffatore!).

L'implicazione però non è trascurabile: vogliamo essere giudicati per quello che siamo e per chi siamo, oppure per quello che sono coloro che si assomigliano a noi? Perché in effetti l'Algoritmo ragiona proprio così, ti attribuisce pregi e difetti di chi ti assomiglia: ad esempio se spesso una persona residente in un certo rione non era economicamente affidabile, allora raccomanderà di dare un basso limite di credito a un richiedente che abita lì. Ma non perché QUELLA persona non pare affidabile.
Se andassimo in banca a chiedere un mutuo, il funzionario che deciderà se approvare o no si baserà su molti fattori, alcuni simili a quelli che usa l'Algoritmo, altri (il suo giudizio personale) meno definiti, ma non meno importanti. E se dovessimo sentirci dire di no, potremmo anche provare a convincerla, confutando alcune delle motivazioni per cui ce lo dicono. Non a caso il GDPR dice proprio che la persona deve poter chiedere di essere valutata da una persona, appunto.
Dicevamo prima che in teoria l'Algoritmo non deve fare discriminazioni di genere. Il che è come dire che il genere non deve essere nei dati storici usati per costruirlo e metterlo a punto. Benissimo. Ma se tra questi dati vi fosse ad esempio un attributo come "che rivista preferisce" con due alternative "Grazia" e "Quattroruote", sarebbe tanto diverso? Il fatto è che certe volte alcuni attributi, soprattutto se presi insieme, implicano il genere, anche se non vi sono direttamente collegati. Ad Apple e Goldman Sachs deve essere successo qualcosa di simile, e loro non necessariamente sanno quale insieme di attributi ha portato ad abbassare tanto il credito della moglie di David Hansson. Esattamente lo stesso può succedere per la profilazione basata sulla razza (cosa ovviamente vietatissima) ma che potrebbe essere un effetto collaterale ad esempio del rione di residenza.

In definitiva l'Algoritmo è la formalizzazione dello stereotipo, del dimmi con chi vai e ti dirò chi sei, insomma di un modo di giudicare il prossimo che sembra l'opposto di quello vorremmo si facesse nel giudicare noi.

Perché in verità l'intelligenza artificiale sarà anche molto intelligente, ma è certamente artificiale. E quindi le manca un ingrediente, che speriamo continui a mancare, che però fa tutta la differenza: l'umanità.

IL VENTINOVESIMO DEL GDPR

LA CENERENTOLA DEL GDPR, FORSE PERCHÉ È IL PIÙ PICCOLO, O È IL MENO CAPITO?

Viviamo in un paese dove un'ordinanza (*) del sindaco di due righe e mezzo, ha bisogno di due pagine di premesse e 4 pagine di esclusioni e precisazioni.

È anche un posto dove lo spirito delle regole e leggi le devono rispettare gli altri, mentre a noi stessi applichiamo solamente la lettera, e ci concediamo sempre l'interpretazione che ci fa comodo. E quindi ci aspettiamo che così si comportino tutti.
Infine rispettiamo le regole esclusivamente se è impossibile "fisicamente" fregarsene. I divieti di sosta necessitano dell'infausto dissuasore a panettone in cemento, le fatture devono essere elettroniche, il limite di velocità deve avere il tutor, ecc.

Sarà forse anche per questo che aziende come Microsys vengono continuamente incaricate del trattamento di dati che non trattano, e insieme a questo incarico ricevono requisiti più o meno assurdi, tipo "dovrai avere tripla ridondanza galattica e fare un test di failover al mese fornendo ampia e dettagliata documentazione delle risultanze" (è vero, abbiamo un poco esagerato, non ci hanno mai chiesto la ridondanza tripla). E se gli si risponde "ma davvero gli altri tuoi fornitori fanno questo?" allora ci si sente dire "ovviamente no. È solo una formalità, il documento l'ha scritto l'ufficio legale, nessuno si aspetta che tu davvero faccia quelle cose". Apparentemente certi requisiti esistono solo come formalità, non per essere rispettati...

Quindi non c'è da stupirsi che un breve articolo del GDPR, nascosto tra il 28 e il 30, che timidamente dice qualcosa senza minacciare sventu-

* https://www.comune.milano.it/documents/20126/66482274/PG+0056366_2020.pdf/9b53470a-a2d2-154e-a855-18eaa805afbe?t=1580823572144

ra e senza imporre procedure assurde di controllo, venga ignorato da tutti, e tirato raramente in ballo solo per sostenere tesi che con l'intento di quell'articolo poco hanno a che fare.

Il codice della strada non impone la patente a tutti gli appartenenti a una famiglia dove è disponibile un'auto. È sufficiente che la patente l'abbia chi quell'auto la guida. Che in teoria potrebbe pure essere un autista esterno, che si presenta solo quando serve.
Questo anche se chi abita in quella casa avesse accesso alle chiavi dell'auto, ad esempio perché tenute in un posto alla portata di tutti. Poi se qualcuno, maggiorenne, prendesse le chiavi e se ne andasse in giro pur non avendo la patente, ne pagherà le conseguenze.
Ovvio.
O no?

L'articolo 29 del GDPR:
Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Abbiamo notato una certa ambiguità in "istruito in tal senso" che potrebbe riferirsi a "formato" oppure "abbia ricevuto indicazioni". Per aiutare nell'interpretazione aggiungiamo quindi anche il testo inglese, che forse è più diretto:

Processing under the authority of the controller or processor
The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Non ci permetteremmo mai, dal profondo della nostra ignoranza legale, di offrire una interpretazione di questo articolo, di cui apparentemente nessuno parla mai.
Ma vorremmo portare all'attenzione di chi legge alcune considerazioni di buon senso, che potrebbero essere rilevanti nello stabilirne le implicazioni.

Prima di tutto il GDPR in generale è un documento sensato, ragionevolmente chiaro e sintetico, dove lo spirito di ogni articolo appare generalmente evidente. Quindi crediamo si possa dire che:

- Se un articolo è presente è perché dice qualcosa che non è già detto altrove.
- L'interpretazione "semplice" è generalmente quella giusta.

C'è una cosa (anzi, una cosa che non c'è) specifica nell'art. 29 che vale la pena di evidenziare: l'articolo ipotizza che possano esserci persone che pur avendo accesso ai dati, non possono trattarli, perché non gli è stato detto di farlo. E, nota bene, non si dice che queste persone devono essere istruite in tal senso. Si dice che se non sono istruite non possono trattare.

Come per la storia dell'automobile: il fatto che io possa (nel senso che mi sarebbe possibile, ma non permesso) prendere l'auto, non implica che io sia obbligato ad avere la patente. Implica che se non sono abilitato non devo prendere l'auto e che se lo faccio commetto una violazione.

Ora, chi potrebbe essere questo misterioso personaggio che potrebbe (ma non deve) trattare i dati? Qui azzarderemo una ipotesi: pensiamo si tratti dei sistemisti e degli sviluppatori, che potrebbero effettivamente mettere il naso nei dati, ma che non devono farlo (e non certo perché lo dice il GDPR).

Morale: forse gli sviluppatori e i sistemisti non trattano i dati, anzi gli è fatto divieto di farlo. E non sempre i fornitori di servizi informatici vanno incaricati del trattamento dati. Anzi, il più delle volte non andrebbero incaricati, perché non devono trattare i dati, ma devono solo occuparsi dei sistemi.

(SMART)WORKING

DICEVA UN CLIENTE: "È INDUBBIAMENTE WORKING. RIGUARDO ALLO SMART, NON SAPREI"

Un aspetto positivo dell'esperienza di questi ultimi mesi è l'aver smarcato il lavoro da casa, agile, "smart" (ma chi l'ha coniato?).
L'anno scorso tutti ne parlavano, la maggioranza delle aziende non lo faceva, quelle poche che lo facevano ne traevano scarse soddisfazioni... (*) (da una vecchia battuta che girava tanto tempo fa in IBM: client-server like teenage sex). E i capi lo vedevano con sospetto, immaginandosi i dipendenti in casa a fare baldoria alle loro spalle.
Poi è successo il pasticcio. E siamo rimasti tutti a casa. E chi poteva lavorava da casa e tutti erano contenti se riuscivano a combinare qualcosa, qualunque cosa...

Anzi, si è scoperto che nonostante i gatti che camminano sulla tastiera, i bambini che giustamente pretendono attenzione, i portali di e-learning che sono più complessi di certe piattaforme di procurement, mariti mogli e figli che ti consumano quella poca banda che il provider ha condiviso con tutto il quartiere, nonostante la necessità di passare ore in coda al supermercato per poi non trovare nulla (ma siamo stati in guerra???), nonostante altre mille difficoltà continue, moltissimi hanno continuato a lavorare come prima, anzi più di prima.

Teams è poi particolarmente adatto ad essere usato in questi contesti, con la possibilità di nascondere lo sfondo o persino di metterne uno farlocco e più professionale. Mancano solo i pantaloni sintetici (non di stoffa sintetica, sintetizzati nell'immagine) e la capacità di filtrare le urla dei bambini, abilissimi a mettersi a litigare nei momenti meno opportuni.

* In realtà non è del tutto vero. Maire Tecnimont lo fa da tempo e pure con grande soddisfazione, e non è l'unica. Ma è vero che in molti casi la cosa è rimasta sostanzialmente sulla carta.

E alle aziende è piaciuto, giustamente. Sicuramente a questo punto non torneremo del tutto indietro, sicuramente abbiamo superato la diffidenza e abbiamo scoperto che chi ha voglia di lavorare non la perde perché è a casa, e che chi non ha voglia di lavorare alla peggio continua a non averla. E ora abbiamo stabilito con certezza che per molti è possibile lavorare da casa senza perdere efficienza, anzi in effetti con maggiore efficienza, se non altro perché ci si risparmia il tempo di trasferta.

Tanto che molte aziende stanno già dicendo che manterranno questo modo di lavorare, che non vogliono più tornare tutti in ufficio perché non serve, che si può avere un ufficio molto più piccolo di quello attuale. E ovviamente i veri vantaggi non saranno per l'azienda, ma per la comunità e di conseguenza per le persone.

Quindi, viva lo smart working?

Non proprio. Forse perché vogliamo essere coerenti con il titolo e con lo spirito di questa rubrica, ma ci sentiamo di spezzare una lancia a favore del caro vecchio "classic working" (coniato ora, l'alternativa ovvia non ci piaceva). Perché come sempre le esagerazioni non fanno mai bene, non solo nel cibo.

Il fatto è che essere parte di un gruppo e sentirsi parte dell'azienda, sono cose importanti. Tanto che il "senso di appartenenza" è sempre stato un obiettivo del tipico ufficio personale. Ed essere "colleghi" in Teams è un po' come essere "amici" in Facebook, una pallida copia della vera relazione umana. Più che colleghi, diventiamo scolleghi...
Certo, Teams è meglio di Facebook, anche perché le amicizie Facebook sembrano essere usate troppo spesso per incanalare cattiverie, cosa che in azienda succede meno. Ma rimane il fatto che il contatto mediato dallo strumento informatico è freddo, allontana le persone e rende difficile se non impossibile "leggere" l'interlocutore.
Quindi funziona tutto alla perfezione per quanto riguarda la comunicazione formale, funziona la collaborazione, funziona il trasferimento di informazione. Ma c'è poca umanità, si fa fatica a trasmettere o a sentire un'atmosfera.
Tutto questo non è un problema quando colleghi che hanno sempre lavorato insieme si trovano improvvisamente separati da un evento che impone le distanze, come ci è successo in questi mesi. Sono persone che già si conoscono e che già appartengono ad un gruppo. Ma far entrare persone nuove ci sembra sia molto più difficile. Non cono-

scono nessuno, non vedono nessuno, non hanno occasione di respirare l'aria aziendale.
E sospettiamo che se si mantengono le distanze per molto tempo, finiremo tutti per perdere tutti quel senso di appartenenza, quello spirito di gruppo, che riteniamo sia essenziale perché le persone si sentano parte di una famiglia, non di un database.
In effetti lavorando da casa e non vedendo mai nessuno, a parte l'orribile monotonia e solitudine, si finisce a essere solo imprenditori di se stessi, e non tanto del gruppo. Non ci sarà più "un posto di lavoro" ma solo "un lavoro". E a questo punto, uno vale l'altro, tanto sono comunque prevalentemente a casa.
Crediamo quindi che l'eccesso di smart working possa portare a un aumento della rotazione e con questa a lungo termine a un peggioramento della qualità, sia del prodotto che del lavoro.

Quindi evviva lo smart working, ma con la giusta moderazione, e condito da frequenti sane classiche interazioni umane. In ufficio!

I MOVIMENTI LATERALI?

OVVERO LA MINACCIA DEL RICATTATORE HACKER

Due recenti articoli pubblicati tra i blog Microsoft sulla sicurezza hanno attirato la nostra attenzione: parlano di una nuova minaccia a cui ci pare si debba porre attenzione.
Per chi è interessato agli aspetti più tecnici della faccenda, troverete in fondo i link, ma qui non vorremmo parlare di tecnica, ma del problema e dei risvolti che ha.

Innanzi tutto una premessa: il cloud non c'entra, anzi forse il cloud è abbastanza immune da questo tipo di attacco. Sono le cose che teniamo nella rete locale, ed in particolare i file server (ma non solo quelli) a essere a rischio.

L'argomento è già stato visto e rivisto: il ransomware (*). Succede: vado su un sito, magari seguendo un link in una mail, e senza saperlo scarico un pezzo di software che cripta tutti i documenti che trova nel mio pc o nei dischi di rete. Poi mi chiede dei bitcoin per darmi la chiave con cui decrittare e recuperare i miei file. Questo tipo di attacco è certamente pericoloso, ma tutto sommato è abbastanza facile difendersi, o almeno avere un sistema che mi consenta di recuperare i dati. Ad esempio posso avere dei backup, o tenere le shadow copy del file system, in modo da poter recuperare la versione precedente dei documenti. È una scocciatura, ma posso salvarmi.

La novità è che da qualche tempo gli attacchi di questo tipo si stanno trasformando. Non sono più l'equivalente di un virus, che si propaga come riesce, e che colpisce dove colpisce, a casaccio. Certo anche

* Il ransomware (ransom malware), è un tipo di malware che blocca l'accesso a sistemi o file degli utenti e chiede il pagamento di un riscatto per renderli nuovamente accessibili. Ad esempio: WannaCry, Petya, Cerber, Cryptolocker e Locky.

così si possono fare danni, ma ci si difende, mentre un attacco mirato fa molto più paura.

La novità è che invece di un virus c'è una persona, in carne e ossa, che entra nella rete e che va a caccia dei dati. Proprio come hanno sempre fatto gli hacker che entravano (tuttora entrano) nelle reti a caccia di segreti. Come quelli che hanno rubato i numeri delle carte di credito di Target.
Quelli però normalmente cercano dati interessanti, ad esempio da vendere ad altri. E quindi se non custodiamo nulla di interessante o rivendibile possiamo pensare "beh, nel mio caso non corro rischi, i miei dati non hanno valore se non per me". Un po' come se in casa tenessimo solo vecchi ricordi, non oggetti preziosi, e quindi non temessimo i ladri. Non più. Oggi non possiamo più cavarcela così facilmente, proprio perché i miei dati hanno valore **per me**.

Un ipotetico attacco potrebbe andare circa così:
- Un utente riceve una mail di phishing e "ci casca" rilasciando le proprie credenziali ad un estraneo
- Costui le usa per entrare da qualche parte. Lì con tecniche varie, sfruttando debolezze di sistemi non aggiornati o configurazioni imperfette, riesce ad accedere e a controllare un server, sempre che l'utente originale già non lo potesse fare
- Da quel server, sempre sfruttando debolezze o anomalie varie, ricava delle credenziali privilegiate, o eleva il proprio account e guadagna autorità amministrative
- A questo punto l'estraneo si mette a girare in rete e a cercare dati. Gli interessano dati che hanno l'aria di essere importanti per noi, non per lui. Ad esempio se li abbiamo protetti bene evidentemente ci teniamo…
- Ora si dà da fare e cancella i backup (se li trova), elimina le shadow copies, insomma fa in modo che non ci siano copie alternative di quei dati
- E a questo punto cripta i dati e lascia in giro un post-it virtuale, con una richiesta di riscatto

Quindi il contenuto non interessa all'intruso. Non perde nemmeno tempo a capire se può essere interessante, gli basta sospettare che sia importante per l'azienda. Ad esempio potrebbe entrare in un server hyper-v, fermare i servizi, e criptare intere macchine virtuali, rendendole inservibili e bloccando contemporaneamente l'accesso ai dati e ai servizi.

Microsys l'ha visto succedere in almeno due casi, forse tre (il terzo potrebbe avere origini diverse dal desiderio di rubare denaro). E in questi casi il danno è stato grave, molto più del tipico attacco di ransomware. Non tanto per il costo del riscatto (non ci risulta che abbiano pagato) ma nel costo di ricostruire i sistemi.
La cosa importante di questa storia è che qui siamo di fronte a un umano che con santa pazienza si mette a scartabellare tra la nostra roba, col solo intento di renderla per noi inaccessibile, per poterci ricattare. Come uno che entrasse in casa vostra non per rubarvi la cassaforte, ma per cambiarle la combinazione e chiedere poi soldi per svelare quella nuova.

Ci si può proteggere?

Certamente sì. Soprattutto ci si può provare. Come abbiamo detto altre volte la sicurezza non è perfetta, ma se riduciamo le probabilità che un attacco abbia successo già abbiamo ottenuto qualcosa.
Per farlo dobbiamo sia ridurre le possibilità che qualcuno possa entrare, che ridurre la sua libertà di muoversi all'interno della rete. Inoltre è possibile sfruttare i "movimenti laterali" (i salti da un server all'altro che l'intruso farà) come indicatore di qualcosa di anomalo e di conseguenza far scattare allarmi automatici.

Oltre a quanto discusso nei due articoli, anzi, ancora prima di mettersi a fare quello che dicono, è importante mantenere aggiornati i sistemi e prendere sempre sul serio le buone pratiche di sicurezza. E tenere presente che se gli utenti hanno strumenti che consentono loro di entrare in rete dall'esterno, allora li potrebbe avere anche un estraneo che riuscisse a procurarsi le credenziali ad esempio tramite un attacco di phishing. Se gli utenti possono accedere da fuori allora lo possono fare pure gli hacker. A questo punto entra in gioco il movimento laterale e l'elevazione dei privilegi. Qui per difendersi occorre impostare la sicurezza come se non ci si potesse fidare gli uni degli altri (che è esattamente il punto), partizionare la rete, aggiornare i sistemi, controllare i profili privilegiati, ecc.

Una nota: un backup fatto su Azure con DPM può essere cancellato da un amministratore, ma rimane comunque disponibile per 14 giorni. E il responsabile riceverà immediatamente una mail di allerta se qualcuno cancella un backup...
Una seconda nota: usare le VPN probabilmente non semplifica, ma anzi complica.

E un'ultimissima: il bitcoin fa male anche a te. Digli di smettere.

A proposito dei blog a cui abbiamo accennato:
Human-operated ransomware attacks: A preventable disaster (https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/) è un dettagliato resoconto di come avviene l'attacco e di cosa normalmente fanno alcuni dei gruppi che operano in questo modo.
Inside Microsoft Threat Protection: Attack modeling for finding and stopping lateral movement (https://www.microsoft.com/security/blog/2020/06/10/the-science-behind-microsoft-threat-protection-attack-modeling-for-finding-and-stopping-evasive-ransomware/) discute la questione dei movimenti laterali e di come rilevarli.

VPN, VDI, WVD, O NULLA?

DENTRO, FUORI O IN ANTICAMERA?

Ora che siamo a metà del guado, quello che ci porta da essere sempre in ufficio a lavorare spesso da casa o da ovunque, è il caso di ragionare su come lavoriamo da fuori, e se sia il modo migliore di farlo.

Una premessa.
Da parte nostra, e siamo in una ampia compagnia, crediamo che prima di tutto dovremmo ragionare sulla questione "dentro o fuori": da quando esiste internet i sistemi informativi sono costruiti intorno a questo paradigma. La rete interna, il dentro, in cui si può fare tutto e tutti sono buoni. E poi il fuori, dove tutti sono potenzialmente cattivi e non ci si deve fidare di nessuno.

Questa distinzione evidentemente è la causa di uno dei problemi del lavorare "da fuori". Non dovrei fidarmi, ma se si tratta di un dipendente devo consentire l'accesso al "dentro". E se mi sbaglio sono guai.

Crediamo che la distinzione vada tolta. Ma non nel senso che mi fido di tutti, anzi l'opposto. Non mi fido di nessuno. Non c'è più il dentro, ma solo il fuori. Perché nell'istante in cui mi fido e faccio entrare qualcuno, posso sbagliarmi. Quindi "zero trust". Non mi fido di nessuno.

A parte questo, il problema dell'accedere "da fuori" rimane. Come faccio? Anzi, le domande sono probabilmente molte, tra cui queste due:

1. Come deve essere fatta una applicazione perché sia facile esporla in sicurezza, renderla accessibile da fuori?
2. Per le applicazioni che ho già, cosa posso fare per esporle senza espormi, e senza rifarle?

Alla prima sappiamo più o meno come rispondere, almeno genericamente. Fai una applicazione web, la esponi con un reverse proxy o con un gateway che ti piace, usi Azure AD per pre-autenticare gli accessi e abilitare MFA (autenticazione a più fattori) e conditional access (acce-

do solo se lo faccio da un posto compatibile col mio ruolo, ad esempio). Con questo dovrei essere ragionevolmente al sicuro da attacchi, di phishing o diretti all'applicazione.

Il problema è la seconda, perché non tutte le applicazioni soddisfano i requisiti per essere esposte in sicurezza, e molte nemmeno se si rinuncia alla sicurezza. E non posso pensare di rifare tutto.

La soluzione banale (almeno in teoria) è la VPN: in sostanza una connessione virtuale tra il pc dell'utente e la rete interna. Il pc, pur essendo remoto, è connesso alla rete interna proprio come se fosse "dentro".
Ma in pratica la VPN più che essere parte della soluzione finisce per essere parte del problema, per diversi motivi:

1. Non è semplice da far funzionare per l'utente.
2. Non sempre funziona, ad esempio certi firewall potrebbero bloccarla.
3. Mettere un pc "estraneo" nella rete interna non è di per sé cosa sicura o opportuna, e anche un pc "amico" che non vedo e non controllo non necessariamente è affidabile ("zero trust!").

Quest'ultimo limite è spesso mitigato dai produttori di soluzioni VPN con protezioni aggiuntive che oltre a realizzare la connessione VPN controllano lo stato del pc, aggiungono protezioni che garantiscano una autenticazione certa dell'utente, limitano il tipo di traffico che può attraversare la connessione. Tutto questo ha però l'effetto di acuire i primi due difetti.
Aggiungiamo anche che le VPN rallentano la connessione, proprio per applicazioni (quelle "vecchie") che non sono state progettate per accessi da remoto e che per questo spesso soffrono particolarmente di connessioni lente o con latenza elevata.

Un ulteriore limite delle VPN, almeno dal punto di vista di una azienda di consulenza, è la difficoltà di farne convivere più di una. Spesso i consulenti lavorano da remoto con collegamenti VPN forniti dai clienti. E se hanno molti clienti, ognuno con la sua soluzione sono costretti ad avere molteplici configurazioni, che spesso non convivono volentieri.
Per far connettere terze parti (clienti, fornitori, auditors ecc.) sarebbe quindi preferibile non usare VPN, per evitare di mettere in rete un pc estraneo e poco (affatto) controllabile, e per rendere più semplice la configurazione all'utente.

Da qui l'esigenza di una soluzione differente.

Un possibile approccio è di non mettere il pc remoto nella rete interna, ma di utilizzare in remoto un pc interno, trasmettendo solo il desktop. L'esperienza utente può essere molto simile all'utilizzo del pc locale, ma in questo modo si ottengono numerosi benefici:

1. Non serve la VPN. Si utilizza un unico accesso verso un singolo servizio, che per sua natura è adatto ad essere accessibile dall'esterno, un po' come un server web.
2. Non si proietta il pc remoto nella rete interna. Quindi non interessa (quasi) se sul pc remoto è presente malware e non è necessario preoccuparsi di come il pc è configurato.
3. Le applicazioni "girano" in macchine interne, in un ambiente controllato. Quindi il pc esterno può essere di qualsiasi tipo e con qualsiasi sistema operativo. Le applicazioni non ne saranno influenzate.
4. La trasmissione del solo desktop richiede molto meno banda rispetto a quanto necessario alle applicazioni, e non soffre della latenza. L'applicazione gira su una macchina vicina ai server e risponde con tempi che non dipendono dalla rete o dalla connessione.

Il modo classico, quasi vecchio, di fare tutto questo è utilizzare RDS (Remote Desktop Services), in sostanza un server che ospita diversi ambienti utente (diversi desktop). Sul server sono installate le componenti client delle applicazioni e gli utenti (anche molti contemporaneamente) le utilizzano in remoto.
Sebbene questa soluzione sia un netto progresso rispetto alla VPN rimangono (anzi sorgono) alcuni inconvenienti:

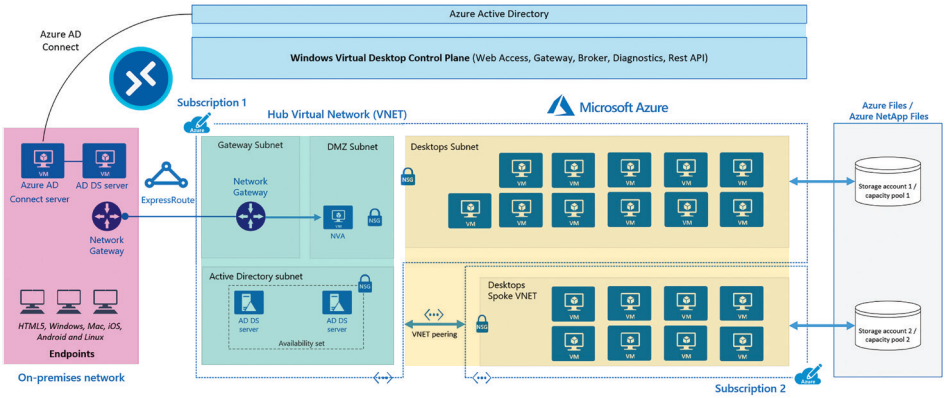
1. Non sempre una applicazione può essere utilizzata contemporaneamente da tanti utenti sulla stessa macchina. Un esempio banale potrebbe essere una applicazione che usa dei file di lavoro che stanno in un posto fisso con un nome fisso. Due copie dello stesso file non ci possono essere.
2. Il lavoro di un utente può disturbare quello di un altro, ad esempio eseguendo una applicazione che rallenta tutto il sistema.
3. Vecchie applicazioni possono richiedere autorità amministrative per l'esecuzione. Questo è poco compatibile con un ambiente condiviso (e poco opportuno in generale).
4. Un ambiente condiviso è necessariamente uguale per tutti, mentre utenti diversi con ruoli differenti facilmente hanno esigenze diverse. E spesso le vecchie applicazioni fanno fatica a convivere nello stesso ambiente. Si possono preparare tanti server RDS quante le configurazioni richieste, ma ci si complica la vita.

La soluzione più moderna a questo dilemma è di dedicare una macchina virtuale a ogni utente. L'accesso avviene sempre tramite RDS, non a un server condiviso ma a una sua macchina, configurata come serve a lui. Questa vm potrebbe essere dedicata a quella persona oppure essere condivisa, non nel senso che più utenti la usano contemporaneamente, ma che la vm non è "di proprietà", e che quindi possiamo immaginare che si possa cavarsela con un numero di vm pari al numero di utenti contemporanei.

L'inconveniente principale è il dover avere tante (tantissime?) macchine virtuali, più un insieme di strumenti che le gestiscano, le creino quando serve e ne garantiscano la configurazione.

Per questo parliamo di VDI -Virtual desktop infrastructure e di WVD-Windows Virtual Desktop.

L'infrastruttura (la VDI!) non è però banale. L'esempio qui sotto, preso dalla documentazione Microsoft per la VDI su Azure non lascia dubbi (https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop):
Alcune componenti sono fondamentali e rappresentano il punto di forza di questa soluzione quando realizzata su Azure: rendere quasi semplice ciò che potrebbe non esserlo affatto. Nel disegno, in alto (azzurro) si vedono i due strati di infrastruttura che fornisce Azure, oltre alle vm vere e proprie:



- **Azure Active Directory**: il meccanismo di autenticazione e gestione dei profili utente, che in questo caso immaginiamo sincronizzato con l'active Directory di sede tramite AD Connect
- **Web access**: il punto di ingresso web a cui si accede L'autenticazione è gestita da Azure Active Directory o dalla AD locale e consente anche l'autenticazione multi-fattore
- **Gateway**: il responsabile di girare il traffico verso la vm giusta. Si accede qualunque piattaforma (Windows, iOS, Linux, Android) e il traffico è incapsulato in un collegamento SSL
- **Broker**: accende le vm e associa le sessioni con le vm, decide quali vm usare e bilancia il carico. Inoltre il broker riconnette le sessioni che fossero cadute a causa di perdite connettività
- **Diagnostics**: memorizzazione e analisi degli eventi per identificare eventuali anomalie
- **Rest API**: punti di accesso per consentire la gestione da parte di applicazioni esterne o l'automazione di operazioni sulla infrastruttura

Sulla sinistra (rosso) sono gli utenti, che nel disegno sono immaginati in sede, ma possono altrettanto essere a casa loro. La connessione tra sede e Azure qui è immaginata come fatta da Express Route. Nel blocco centrale, (verde) a sinistra si vede il gateway che termina la connessione, con un firewall dedicato (NVA -Network Virtual Appliance). Subito sotto una copia di ADFS, che gestiscono l'autenticazione integrata con il dominio di sede. Poi i due blocchi (giallo) di macchine virtuali (chiaramente non è obbligatorio che siano due, possono essere uno solo, o tre...). Infine lo storage, che su Azure può essere ampio a piacere.

Chiaramente è possibile semplificare un po', ad esempio non è obbligatorio usare express route (una connessione dedicata tra Azure e la sede del cliente), si può rinunciare a partizionare la rete con il firewall, non serve avere tante sottoscrizioni. E il dimensionamento può essere ampiamente variabile, anche nel tempo, ed accomodare le esigenze sia di piccole aziende che di quelle grandi.

Una soluzione VDI basata su Azure consente l'accesso da fuori a tutte le applicazioni interne, a qualsiasi file server della rete interna e in generale a tutto quanto è normalmente disponibile agli utenti interni, ma senza esporre la rete e senza portare all'interno le macchine remote. In questo modo si mantiene il controllo della parte interna e si può rinunciare a controllare quella esterna, perché in realtà non ci interessa

come è configurata. Utilizzando l'autenticazione integrata con Acrive Directory e abilitando MFA si ottiene un elevato livello di sicurezza unito ad una ragionevole semplicità di accesso per l'utente.

Questa soluzione è anche molto efficace per garantire la sicurezza degli accessi da parte degli amministratori di sistema, da ovunque accedano. Le credenziali amministrative non vengono mai usate da macchine personali, ma sempre e solo dalle macchine virtuali dedicate agli amministratori, e solo dopo che l'identità del sistemista è stata verificata tramite MFA. In questo modo nemmeno un keylogger (un malware che "legge" quello che l'utente digita e di conseguenza è in grado di carpire una password) potrebbe aggirare le protezioni.

I costi dipendono dal tipo di soluzione. Fattori che li influenzano sono le caratteristiche delle macchine che vogliamo dare agli utenti e la tipologia di VM, se dedicate e persistenti o condivise e non persistenti. Per utenti Office, in funzione di questi parametri il costo mensile per utente può variare tra 15€ e 30€ al mese per utente attivo. Nel caso di ambienti condivisi conta il numero di utenti contemporanei, per cui se gli utenti accedono saltuariamente, come nel caso dei consulenti esterni, i costi si riducono ulteriormente.

CASI DI BUSINESS

AIPB

L'esperienza di smart working in AIPB, Associazione Italiana Private Banking, durante i mesi dell'emergenza Covid19, ha fatto emergere i benefici di una modalità lavorativa che fa leva sull'uso di piattaforme digitali allo stato dell'arte. AIPB era già passata da un paio di anni alla piattaforma cloud Microsoft Office 365. È stato nei giorni del lockdown generale, che AIPB ha fatto un reale balzo in avanti, arrivando a sfruttarne appieno tutte le potenzialità di comunicazione e centralizzazione dei dati. Un elemento critico per la riuscita del progetto di smart working in AIPB è stata la scelta di un partner come Microsys, che ha fornito dapprima la soluzione in cloud che copriva tutte le esigenze dell'Associazione, dalla robustezza della rete contro possibili attaccanti esterni, alla centralizzazione dei dati e alla gestione della collaborazione. Infine, fondamentale per la riuscita del progetto, è stato il supporto continuativo alle persone di AIPB anche nel periodo del lockdown.

CA' ZAMPA

Ca' Zampa, la prima rete in Italia di Centri completamente dedicati al benessere dei pet, costatando la possibile evoluzione delle richieste ed i processi, con il passaggio da una sola clinica veterinaria aperta alla gestione di dieci realtà previste, ha dovuto concludere che la soluzione gestionale precedentemente acquisita non soddisfaceva tutte le esigenze: in particolare, gli aspetti contabili andavano sviluppati diversamente e mancava tutta la parte di Business Intelligence legata al CRM e la componente di marketing automation. Dopo una attenta analisi l'azienda ha selezionato Microsoft Dynamics 365 che tra Business Central, Dynamics CRM e potenzialmente PowerBi supera tutti i requisiti e può sostenere una futura importante crescita. Al momento il sistema è utilizzato parzialmente in una clinica, mentre con le successive due l'avvio andrà in parallelo con la parte amministrativa. L'approccio di Microsys per la realizzazione del progetto è stato considerato ben strutturato, professionale, con un buon lavoro di squadra.

GRUPPO A2A

Il Gruppo A2A, la maggiore multiutility italiana, ha dato avvio ad un percorso di upgrade tecnologico, finalizzato a dotarsi di strumenti aggiornati con gli standard di mercato in ambito business analytics e gestione big data. Tali strumenti sono stati introdotti in azienda all'interno dell'area Information Technology Generazione, per offrire soluzioni innovative che permettessero di migliorare il monitoraggio delle performance tecniche, ed economiche, dei propri impianti di produzione, supportando gli utenti di business nell'estrazione del valore contenuto all'interno dall'enorme quantità di dati a disposizione, ad oggi già presenti e strutturati nei propri sistemi transazionali e industriali. Tra le aziende che hanno partecipato al progetto un elogio particolare va alla società Microsys per la competenza e professionalità dimostrata nello sviluppo delle soluzioni data warehouse e visual data discovery.*

GRUPPO LU-VE

Gruppo Lu-Ve, è uno dei maggiori costruttori mondiali nel settore degli scambiatori di calore, ha sempre posto in primo piano il tema della sicurezza. Avendo avuto di recente conoscenza indiretta dell'aumento di attacchi informatici andati a segno nel mondo industriale, con danni economici rilevanti per le aziende colpite, il management del gruppo decide di intraprendere una verifica dello stato della protezione e sicurezza del suo ambiente tramite un assessment, ovvero un'ampia e precisa attività di verifica volta a individuare eventuali vulnerabilità e proporne la risoluzione introducendo miglioramenti tecnici e organizzativi. La società trova chiara, soddisfacente e realistica la proposta di Microsys riassunta nell'offerta Cyber Defense 365, un concentrato di conoscenze ed esperienze con i recenti strumenti e servizi di sicurezza Microsoft. Oggi il Gruppo Lu-Ve ha una rafforzata sicurezza e precisa gestione delle identità privilegiate, oltre ad aver aumentato la sicurezza generale delle identità digitali e degli accessi ai servizi IT.

iLLIMITY

illimity, la banca di nuova generazione, per essere compliant agli obblighi normativi, aveva la necessità di dotarsi di una soluzione specifica che permettesse a tutti i dipendenti di accedere e consultare i documenti di Normativa interna in maniera rapida (per parole chiave, tipologia, ruoli) e di gestire un flow di costituzione e approvazione del contenuto dei documenti all'interno dell'azienda.
Per queste ragioni è nata la necessità di sviluppare un progetto specifico e user friendly finalizzato ad una gestione snella ed efficace dei documenti di normativa e dei relativi processi di redazione, pubblicazione e ricerca. Dopo una attenta analisi dell'esigenza di business, Microsys propone ad illimity la realizzazione di una soluzione specifica basata sulla piattaforma Microsoft Office 365 e la componente Power Platform. Lo sviluppo del progetto ha richiesto il coinvolgimento di tutta l'organizzazione aziendale, consentendo di usufruire della suite Microsoft 365, già utilizzata in azienda, potenziandone l'uso in tempi rapidi e con costi ridotti.

THE LEVEL GROUP

The Level Group, nata nel 2011, è un partner di eCommerce per brand. Uno dei brand cliente dell'azienda, nel suo percorso verso l'implementazione di una strategia omnicanale, ha riscontrato la difficoltà di far dialogare i sistemi aziendali del mondo offline con il proprio eCommerce. Da qui, è nata l'esigenza per The Level Group di integrare le proprie piattaforme tecnologiche per abilitare e supportare i propri clienti nell'offerta di un'esperienza che risulti realmente omnicanale. The Level Group, grazie al supporto di Microsys, ha introdotto un Enterprise Service Bus (ESB) in grado di fungere da middleware intermedio tra i sistemi informativi aziendali e i principali touchpoint di interazione con il consumatore. Tale piattaforma riceve molteplici informazioni in input dai sistemi di front-office, li elabora e li invia come output ai sistemi di back-end. La piattaforma è implementata totalmente in Cloud e utilizza componenti in modalità Software as a Service (SaaS), Platform as a Service (PaaS) e Infrastructure as a Service (IaaS). (*)

* Il case study è stato realizzato nell'ambito della Ricerca dell'Osservatorio Big Data Analytics & Business Intelligence, promosso dalla School of Management del Politecnico di Milano.

LE SOLUZIONI

ARXIVAR 365

Arxivar 365, integrazione efficace con il software di archiviazione documentale ARXivar, permette di archiviare automaticamente qualsiasi documento di Business Central, oltre che reperirne i cambi di stato. Inoltre, consente il ricevimento dei documenti passivi. Con una sinergia perfetta con la soluzione **SDI 365** può essere gestita anche la fatturazione elettronica attiva.

Perché scegliere **Arxivar 365**?

- Archiviazione di qualsiasi documento e gli aggiornamenti di stato
- Reperimento dei documenti passivi
- Setup ampio che concede la personalizzazione completa

DOC FINANCE 365

Doc Finance 365, la soluzione di integrazione con il software Doc Finance per la gestione della tesoreria. Gestisce uno scambio di file a 2 vie per la completa comunicazione tra i due software. Installazione semplice, setup guidato e nessuna attività sistemistica richiesta.

Perché scegliere **Doc Finance 365**?

- Integrazione con Doc Finance consolidata
- Installazione e setup rapidi e guidati
- Estrazione delle anagrafiche da Business Central

DOC TEMPLATE 365

Doc Template 365 è la soluzione Microsys per i documenti commerciali, fornisce un layout pulito, efficace ed estendibile, condiviso per tutti i documenti in uscita per garantire un'immagine aziendale unificata. Sono gestiti, oltre a tutti i documenti di vendita (compresa la spedizione), anche offerte, ordini e spedizioni di reso lato acquisto e le spedizioni di trasferimento.

Perché scegliere **Doc Template 365**?

- Un layout unificato per tutti i documenti
- Facilmente estendibile e personalizzabile
- Gestione di tutti i documenti in uscita

EXTRACONTABILE 365

Extracontabile 365, una soluzione completa e semplice per la contabilità analitica. Uno strumento realizzato da Microsys per avere un efficace controllo della gestione oltre che per ratei e risconti. Inoltre le soluzione integra le funzionalità per la generazione delle fatture da emettere e da ricevere.

Perché scegliere **Extracontabile 365**?

- Registrazione automatica in contabilità analitica per conto C/G
- Analisi per dimensione cumulati di consuntivi ed extra
- Situazioni contabili per confronto consuntivi ed extra

SDI 365

SDI 365, l'estensione per l'estrazione delle fatture elettroniche che rende disponibile una versione completa e personalizzabile dei documenti elettronici attivi. Un setup semplice ma efficace permette la valorizzazione e l'imputazione automatica del bollo, oltre che la compilazione automatica dei tag opzionali, lasciando inoltre all'utente la possibilità di aggiungerne su ogni fattura o nota credito.

Perché scegliere **SDI 365**?

- Compilazione automatica dei tag sulla base di regole
- Gestione automatica del bollo e della sua imputazione
- Inserimento automatico riga split payment al rilascio del documento

VIRTUAL DESKTOP INFRASTRUCTURE 365

Virtual Desktop Infrastructure 365, la soluzione di Microsys basata su tecnologia Microsoft Azure che ospita i desktop aziendali in remoto e consente agli utente di accedere in mobilità al proprio ambiente di lavoro.

Perché scegliere **Virtual Desktop Infrastructure 365**?

- Consente l'accesso da remoto alle applicazioni interne ed ai file server della rete interna aziendale
- Garantisce la sicurezza degli accessi da parte degli amministratori di sistema
- Semplifica la gestione dell'infrastruttura IT

Per saperne di più visitare il nostro sito:
https://msys.it/Pages/SoluzioniAppSource.aspx