
MICROSYS
DIARIO
2021

Diario di un anno: 2021

Cari Lettori e Care Lettrici, ecco il nostro diario annuale, un'occasione per augurarvi un sereno Natale e un felice anno nuovo.

Negli ultimi due anni abbiamo vissuto delle esperienze difficili che hanno lasciato in molti la consapevolezza che da soli non si può vivere. Sono certa che collaborazione, generosità, responsabilità, empatia e comprensione potranno farci affrontare le situazioni che nessun muro può risolvere, mentre le cose positive accadute nel 2021 ci danno la forza per guardare al 2022 con maggiore fiducia ed ottimismo.

Gli articoli di quest'anno della rubrica Controcorrente sono leggermente cambiati, lo spunto è sempre il mondo informatico, ma mettono più in primo piano riflessioni etiche e valutazioni morali , con quella punta di ironia che non guasta.
Non perdetevi le ultimissime storie di successo in cui descriviamo con i nostri clienti i progetti di spicco sugli argomenti come la sicurezza informatica, l'automatizzazione dei processi, la customer experience ecc.

Infine la presentazione delle soluzioni, le App Dynamics Business Center e gli incontri dei programmi Pillole di Innovazione, Tech Bits e Licensing Track che potete rivedere sul canale YouTube Microsys Channel, sempre disponibile a chi fosse interessato.

Il prossimo anno Microsys compirà 30 anni; 30 anni in cui abbiamo cercato di restare sempre fedeli a noi stessi e di crescere con solidità, sicuri ed accoglienti con i nostri dipendenti e collaboratori, ponendo sempre particolare attenzione ai nostri clienti, seguiti passo dopo passo con cura e pazienza.

Posso affermare con orgoglio, che Microsys è un luogo dove è possibile vivere e lavorare sentendosi protetti e crescere professionalmente, aperti al mondo ed alle novità, rimanendo al passo con il progresso del mondo digitale. Ed anche un partner con cui lavorare costruendo una relazione di fiducia.

Avremo occasione per festeggiare insieme i 30 anni di Microsys e spero di ritrovarvi numerosi ed entusiasti agli appuntamenti 2022 di Pillole di Innovazione e TechBits.

Alessandra Galdabini

CONTRO CORRENTE

LA NUOVA MACCHINA DEL CAFFÈ

E ALTRE STORIE: CERTE VOLTE LA TROPPA INTELLIGENZA È APPUNTO TROPPA

Abbiamo una nuova macchina del caffè (in ufficio, non a casa).
Cromata, lucida, intelligente, veloce. Fa due caffè alla volta, con due sistemi indipendenti (ma una sola alimentazione), praticamente un sistema in alta affidabilità per una funzione che indubbiamente lo giustifica. Un Cerbero del caffè.
La mattina quando la si risveglia si lava accuratamente, il che è un po' un difetto, dobbiamo fare i turni a svegliarci prima per arrivare in tempo ad accenderla, altrimenti tocca aspettare. Ma poi è tutta una dimostrazione di intelligenza artificiale applicata alla mescita.
Per farsi un caffè si inserisce la cialda (la solita da ufficio) nella fessura. La macchina la sente, e... ti presenta un QR Code!

A questo punto hai due scelte

- Metodo classico: tocchi il QR Code (è touch!) e allora quello sparisce e ti compaiono le scelte (lungo, corto, ecc.). La macchina riconosce il tipo di cialda (rfid? Altro QR code nella cialda? Fotometro che rileva il colore?) e ti suggerisce la scelta migliore. Tocchi la tua preferenza e, magia, la macchina ti dice cosa stai per bere: no caffè banale, caffè con toni di nocciola dell'Himalaya e profumo di mirtillo acerbo, o qualche altra sofisticheria. Così ti intrattiene mentre fa il caffè. Ti pigli il caffè e ti godi la nocciola dell'Himalaya.
- Metodo moderno ("Modern coffeing"): leggi il QR Code col telefonino. Ti allontani dalla macchinetta (non obbligatorio, ma logico, altrimenti perché usare il telefonino?). Sul telefonino ti compare una perfetta riproduzione del touch screen della macchina, scegli l'opzione che ti piace (sperando che nel frattempo non ti abbiano fregato la cialda). Torni alla macchina e ti prendi il caffè, oppure telefoni a qualcuno che te lo porti. Ti bevi il caffè, verosimilmente freddo.

Abbiamo un nuovo orologio molto intelligente.
Si collega al telefono, sa dove sei, s'impiccia della mail e del whatsapp, ti misura i battiti e le calorie che consumi (o non consumi). Se sei bravo si complimenta facendo "piripì" e consegnandoti una coppa (virtuale). Ha una batteria che dura tantissimo (tipo una settimana), e usa la sua intelligenza per attivare solo quello che serve, solo quando serve. (*)
Per risparmiare batteria, e durare una settimana, l'orologio di solito sta spento. Se c'è sole il quadro si vede, altrimenti devi premere un bottone per vedere che ora è. Tutto sommato è ragionevole, ma se hai le mani occupate non è comodo.
Quando ti arriva un whatsapp (tipicamente irrilevante, ma questa è un'altra faccenda) l'orologio fa "piripì", e mostra il messaggio su uno schermo che è sì ad alta risoluzione, ma, ahimè, è della misura di un orologio. Ti mostra ben tre righe del messaggio in un carattere che riuscirebbe a leggere agevolmente solo un giovanotto con la vista di un'aquila. L'alternativa è usare gli occhiali, o meglio il monocolo da orologiaio. Quindi senti "piripì", cerchi gli occhiali, li metti, guardi il messaggio e scopri che per risparmiare batteria il coso l'ha già da tempo fatto sparire il messaggio. Tiri fuori il telefono e leggi quello che potevi leggere senza disturbare l'orologio.

Abbiamo una nuova asciugatrice (a casa, non in ufficio).
Quando la accendi la prima volta ti chiede la password del WiFi. Fortunatamente non chiede la password Netflix, evidentemente si accontenta di guardare Youtube.
Una volta collegata, può parlare con il telefonino, col quale la accendi, spegni, le chiedi come sta, scegli il programma, ecc.
Evidentemente il modello di utilizzo è simile a quello della macchina del caffè:

- Metodo classico: metti la biancheria nella macchina, chiudi lo sportello, scegli il programma con l'apposito pomello, tocchi start (è touch!). Quando finisce senti "piripì" e ti pigli la biancheria.
- Metodo moderno ("Modern drying"): metti la biancheria nella macchina, chiudi lo sportello, metti l'apposito pomello nella posizione "remote", ti allontani (altrimenti che gusto c'è?), tiri fuori il telefonino e lanci l'apposita app, scegli il programma e avvii. Quando la macchina finisce il telefonino fa "piripì", ma la biancheria rimane nell'asciugatrice. Però c'è un'interessante opzione: se girando per casa trovi un calzino disperso puoi col telefonino dire all'asciugatrice di aspettare un attimo. Ma il calzino non lo puoi ficcare nel telefono, devi comunque portarglielo.

Abbiamo l'impressione che tante volte invece di inventare tecnologia per risolvere problemi, cerchiamo di inventare problemi da risolvere con la tecnologia.
È l'effetto del marketing moderno, che inventa problemi inesistenti e che applicato alla tecnologia produce oggetti con funzionalità di dubbia utilità, e applicato alla politica produce il populismo.

PS: è un po' diverso, ma anche questo è un esempio di come la tecnologia certe volte esagera. Microsoft Phone system è l'equivalente di un centralino, ospitato in Office 365. Tra le altre cose ha un semplice IVR (Interactive Voice Responder), quel coso che dice "premi uno per l'ufficio x, due per y, ...". Quello di Office 365 fa anche conversione da testo a vocale per cui gli dai il testo scritto, e lui lo legge. Gli devi solo dire la lingua da usare (probabilmente le conosce tutte, esclusi forse i dialetti più strani della Papuasia). Sarebbe perfetto se gli italiani parlassero in italiano. Ma non è così, per cui per ottenere un risultato comprensibile ti trovi a scrivere cose come questa: "per info su soluzioni per le logistiche prema uno, per info su digital sport innovescion e futboll innovescion prema due, per info su soluzioni per la mobilità elettrica gioinon prema tre, ..."

* Abbiamo anche un orologio molto meccanico, con una molla che si ricarica da sola, ma eviteremo facili ironie...

LA LUNA DI MIELE

IL LAVORO DA CASA: NE ABBIAMO ABBASTANZA

- Citibank promette ai dipendenti il venerdì senza Zoom
- Gli analisti di Goldman Sachs parlano di settimane lavorative di 95 ore.
- Kpmg dice che tra le 500 aziende top, quelle che intendono diminuire lo spazio per uffici sono passate dal 65% di un anno fa al 17% di un mese fa.
- Il Guardian parla di un nuovo fenomeno: quelli che rifiutano "Zoom".

Ora, trascurando il fatto che sembra che Zoom sia diventato il sistema di videoconferenza per antonomasia, ci pare evidente che molti stanno rivedendo la loro posizione relativamente allo smart working. Ne abbiamo parlato anche noi quasi un anno fa ((Smart) Working), ma allora pensavamo soprattutto al fatto che l'eccesso di lavoro da remoto distrugge il tessuto sociale aziendale.

Adesso emerge un nuovo aspetto: non ci sono più orari, tutti disturbano tutti gli altri in qualsiasi momento del giorno e della notte, non c'è più quella sacra (e tanto criticata) separazione tra casa, lavoro e riposo (che forse dovrebbe dividere le 24 ore in parti uguali). La pandemia ci ha portato via gli svaghi (perché ci sono vietati) e ci lascia solo lo schermo, per fare tutto, lavorare, socializzare, giocare.

E ne abbiamo abbastanza.
Siamo passati dalla luna di miele col telelavoro, dove tutti erano entusiasti del poter lavorare da casa, alla crisi del settimo anno. E speriamo di arrivare presto a una separazione consensuale, in amicizia, ma con diritti di visita non troppo frequenti.

UBER, GOOGLE E LE "AUTO"-MOBILI

ANTHONY LEVANDOWSKI E I PROGETTI COPIATI

Anthony Levandowski era un importante ingegnere della divisione di Google che studiava le automobili a guida autonoma. Oggi quel progetto è vivo e vegeto (Waymo), ma Levandowski non ne è più parte, perché ha prima abbandonato Google per fondare la sua azienda (Otto) che ha poco dopo venduto a Uber. Poi è stato trascinato in una causa per furto di proprietà intellettuale tra Google e Uber, che è risultata per lui in una condanna a 18 mesi di reclusione (Donald Trump l'ha perdonato l'ultimo giorno della sua presidenza).

Anthony non ha ammesso di aver copiato i documenti di progetto di Google, o più precisamente non ha ammesso di esserseli portati via e averli dati a Uber. Ma siccome ha acceduto a un singolo documento Google, non tecnico, quando non era più dipendente, (cosa che di per sé non poteva essere poi così grave) è stato condannato, un po' come Al Capone: la condanna è formalmente per un illecito minimo in confronto a quello che "tutti sanno che ha fatto" ma che nessuno è riuscito a dimostrare sia stato fatto da lui.

Ma cosa "ha fatto realmente" Antony? Ha scaricato quasi 10 Gb di documenti tecnici, a cui poteva accedere legittimamente, poco prima di dare le dimissioni per fondare Otto. Questo di per sé non è illegittimo, ma è ovvio che in quei pochi giorni sarebbe stato impossibile per Antony lavorare su un simile volume di dati. Quindi è ragionevole sospettare che il motivo per scaricarli fosse di copiarli. Ma è una ragionevole deduzione.
Poi, dopo molti mesi, è spuntato (per un errore di un fornitore Uber) un documento interno Uber con parte del progetto del lidar (Lidar - Wikipedia, un radar basato su laser al posto della radio) ed era identico a quello di Google. Questa è stata la "pistola fumante" che ha spinto Google a fare causa.
Questa storia non ci interessa tanto per la vicenda di Anthony, sul quale non vogliamo emettere giudizi non informati, ma per i risvolti tecnici che ne emergono. Come mai nemmeno Google ha saputo prevenire una cosa del genere?

Qualche tempo fa un cliente ci ha esposto essenzialmente lo stesso problema. Temeva, "era sicuro", che un ex dipendente se ne fosse andato con i disegni di un componente molto speciale e molto brevettato. Che è poi spuntato molto simile dalla concorrenza. E ci chiedeva cosa fare per evitare che la cosa si ripetesse.
La risposta non è semplice. Anzi, è semplice se si risponde "non si può", e probabilmente ci si azzecca. Perché il fatto è che se qualcuno ha legittimamente accesso a un documento, è praticamente impossibile evitare che ne faccia una copia, soprattutto se questo qualcuno è determinato e in malafede. Tant'è vero che nemmeno Google ha evitato che succedesse, con i documenti di un progetto molto importante, molto costoso, molto in vista e di conseguenza supponiamo molto protetto.
Ma Google aveva gli audit log, da cui ha potuto dimostrare che erano stati scaricati i documenti e quindi a posteriori ha potuto dimostrare (quasi) di aver subito un furto. Ma non ha potuto evitarlo.

Con Office 365, OneDrive e SharePoint si possono produrre gli audit log, con la lista degli accessi, e possono generare allarmi quando troppi documenti vengono condivisi o scaricati in un breve intervallo di tempo. Ma nessuna di queste funzionalità può impedire che si compia il fatto, nel migliore dei casi si verrà avvisati mentre succede, o poco dopo. Ma se il malandrino è attento non farà nemmeno scattare l'allarme.

E quindi?
Non possiamo impedire la copia, ma possiamo rendere il furto un po' più difficile, e evitare che la diffusione di informazioni riservate avvenga incidentalmente. Purtroppo la cosa fondamentale è avere collaboratori di cui ci si può fidare: se poi si scopre che ci hanno tradito allora i primi a sbagliare siamo stati noi, i sistemi possono fare qualcosa per proteggerci, ma il rischio rimane comunque.

Alcune delle cose che possiamo fare sono:
- Avere i log degli accessi, ai documenti e alla rete, per poter eventualmente usarli per capire cosa è successo.
- Limitare i diritti di accesso ai soli documenti necessari a eseguire i propri compiti
- In casi estremi limitare il diritto di accedere ad archivi storici senza

una giustificazione. Consentire l'accesso solamente dopo un processo approvativo.
- Usare gli strumenti di DLP(*) (data loss prevention), in particolare identificare come riservati i documenti da proteggere e imporre politiche di accesso più restrittive su questi documenti.
- Attivare Azure Information Protection(**) e applicare politiche che impediscano l'uso di strumenti che consentirebbero di aggirarlo.
- Utilizzare *conditional access* per consentire l'accesso ai dati aziendali solamente da dispositivi aziendali
- Controllare i dispositivi tramite Intune in modo da garantire che la configurazione corrisponda ai nostri requisiti
- Utilizzare Bitlocker in modo che in caso di perdita o furto di un portatile i dati non siano accessibili.

Dobbiamo tenere presente che anche il più sofisticato e rigoroso apparato di sicurezza non può impedire che un tecnico acceda a documenti con cui lavora normalmente. Perché appunto è previsto che lo faccia. Quello che vorremmo è che gli si impedisca di farne un uso improprio, ma di fatto questo è praticamente impossibile: come si può ad esempio assicurarsi che non fotografi lo schermo, o che banalmente prenda appunti a mano, o che utilizzi una microcamera per scorrere tutto un documento o un progetto, ecc.?

Un altro aiuto è meno tecnologico, ma altrettanto o più importante. I processi aziendali devono prevedere rigorose procedure di dismissione del personale che potrebbero (se opportuno e legale) limitare il perimetro delle informazioni accessibili a un dipendente dimissionario e alzare il livello di allerta su eventi che lo coinvolgano. In extremis si potrebbe persino ipotizzare un istantaneo blocco del diritto di accedere ai dati dal momento delle dimissioni. Ovviamente questo avrà un impatto economico, e diventa quindi una questione di ROI. Sempre in seguito alle dimissioni si può prevedere un'analisi degli accessi sia nel periodo immediatamente precedente, che durante il preavviso, che possa evidenziare eventuali anomalie e costituire anche una azione deterrente. Tutte queste cose non sono certo risolutive, ma possono fare differenza.

Un'ultima osservazione: possiamo legittimamente ritenere che un collaboratore che se ne va non debba portarsi via documenti riservati. Ma non possiamo pretendere che non si porti via la testa. Quella è sua e quello che ha imparato lavorando con noi diventa anche suo patrimonio, la distinzione tra copiare e appoggiarsi sulla propria esperienza non è poi così netta. Certo, se mi faccio una copia di qualcosa risparmio un po' di fatica, e non è giusto. Ma alla fine probabilmente il risultato cambia poco, e l'unica protezione efficace è il brevetto.

* Purtroppo molte delle protezioni di Microsoft 365 sono più efficaci su documenti Office. Questo perché in realtà la protezione è frutto di una collaborazione tra il client (il prodotto Office, ad esempio Word) ed il server (ad esempio SharePoint). Ad esempio se un documento non può essere stampato, è il client che deve rifiutarsi di stamparlo, il server non può impedirlo. Quindi la protezione di documenti non Office dipenderà anche dal prodotto con cui quel documento è creato.

** Un insieme di strumenti di Office 365 che consentono di associare limiti di utilizzo ai documenti, per cui il documento è leggibile solo da persone autorizzate ed è protetto da specifiche azioni (esempio: non inoltrare, non stampare, ...), indipendentemente da dove si trova. Quindi per esempio anche una copia spedita per mail rimane protetta.

ANCORA L'ALGORITMO

CON LA MAIUSCOLA, UNA BRUTTA BESTIA

Pare che Facebook non rispetti le leggi USA per le pari opportunità di genere.
Almeno, così dice il MIT Technology Review: Facebook's ad algorithms are still excluding women from seeing jobs.
A quanto pare alcuni ricercatori hanno comprato spazio pubblicitario in Facebook e hanno pubblicato annunci di ricerca personale per due diversi lavori che statisticamente hanno una distribuzione asimmetrica rispetto al genere. E incredibilmente l'Algoritmo(*) ha scelto di far vedere l'annuncio prevalentemente a persone del genere che maggiormente era rappresentato per quel tipo di lavoro. Cosa vietatissima perché non si può selezionare personale in base al genere (e, ci auguriamo, nemmeno in base a qualsiasi altra caratteristica fisica).

Proviamo a estremizzare giusto per capire meglio il ragionamento, l'Algoritmo e il problema: supponiamo di voler mettere un annuncio di ricerca personale, ad esempio per trasportatori di pianoforti a coda (quelli che li portano su e giù dalle scale con delle cinghie). Anzi, fingiamo di dover fermare per strada possibili candidati per dargli un ipotetico volantino di selezione candidati. Supponendo di non voler sprecare volantini, a chi lo daremmo? Attenzione, perché qui è nascosto un dettaglio importante: se attacco una pubblicità al muro, la legge chi la legge. Se metto un volantino in mano ai passanti, e mi do come obiettivo di non sprecare volantini, devo scegliere a chi darlo. L'annuncio su Facebook è l'equivalente virtuale del volantino, e l'Algoritmo ci sostituisce nel selezionare i candidati più plausibili. Ma posso scegliere i più plausibili e contemporaneamente ignorare il genere?
Proviamo a omettere il fattore genere, e comunque a voler evitare lo spreco di volantini: potremmo ad esempio dare i volantini a persone (di ogni genere) dall'aspetto forzuto, e di altezza sopra la media? Forse sì, ma di che genere sarebbero i candidati? Sicuramente non 50/50 maschi/femmine...

Il fatto è che noi stiamo chiedendo all'Algoritmo di fare cose che sono in contrasto tra loro: indovinare chi potrebbe essere interessato, ma produrre un risultato dove maschi e femmine hanno rappresentanza equivalente. Non ha senso se oggi quello stesso lavoro lo fanno prevalentemente rappresentanti di uno dei generi.

Se l'algoritmo basa le proprie decisioni sulla precedente esperienza, e se questa esperienza ci dice che un certo tipo di persone saranno più interessate di altre, non ci pare che ci sia via di scampo: è inevitabile che, pur trascurando il genere, si finisca per escludere le persone che tipicamente quel lavoro non lo fanno. Non saranno escluse in quanto di uno specifico sesso, ma banalmente perché hanno caratteristiche d'insieme che le rendono candidati meno plausibili.

Ma è anche perfettamente comprensibile il nostro desiderio di avere un comportamento differente. In realtà perché siamo schizofrenici: da una parte parliamo in modo politically correct: parità di tutto per tutti, nessuna discriminazione. Dall'altra parte la statistica (o il machine learning se preferissimo chiamarla così) mette a nudo il fatto che ci comportiamo in altro modo, e quindi istruisce l'Algoritmo a fare lo stesso.

La soluzione: banale. Non serve cambiare l'Algoritmo. Basta **TOGLIERLO**.

* L'Algoritmo, con la maiuscola. Un animale mitico che decide su varie cose sulla base di criteri opachi, non condivisi e probabilmente non compresi nemmeno dal suo creatore. Decide ad esempio quali pubblicità vedremo, quali film ci piacciono, qual è la nostra capacità di ripagare un prestito, chi ci piace e cosa dirci par farci votare in un modo piuttosto che in un altro.

UFBP / UFTP ???

UN AIUTINO: NON È UNA VARIANTE DI FTP

Un cliente, vittima di ramsomware, diceva “dicono che mi hanno bucato il firewall”. Abbiamo risposto che non credevamo che fosse successo. E abbiamo pensato che dire che gli avevano “bucato” il firewall sarebbe stato come dire che gli avevano “scassinato” una serratura che era stata lasciata aperta. E il buco era aperto per necessità, non per distrazione.

Tanto, ma proprio tanto tempo fa, siamo stati a una conferenza Microsoft a Barcellona. Lì, tra le molte presentazioni interessanti ne abbiamo vista una di un esperto di sicurezza, che ci ha colpito per almeno due motivi:

- Diceva cose intelligenti, e l’intelligenza è merce rara
- Aveva senso dell’umorismo, cosa non frequente tra gli esperti di sicurezza, che si prendono molto sul serio perché sono sempre sotto attacco.

In quella presentazione, tra le varie cose abbiamo sentito questo nuovo (allora) acronimo, UFTP. Oggi lo si può trovare come UFBP ma il significato è esattamente lo stesso: Universal Firewall Traversal (oppure Bypass) Protocol.

Il problema è noto: far passare dai firewall protocolli specifici di un’applicazione può essere difficile, se non impossibile. Non perché sia tecnicamente difficile da fare, ma perché i responsabili del firewall non lo vogliono fare. E poi non è nemmeno detto che ci sia un responsabile a cui chiedere. Se ad esempio sono ospite da un cliente o in un albergo, non solo probabilmente non posso chiedere che facciano qualcosa di specifico per me, ma appunto non so nemmeno a chi chiedere. E poi, chi gestisce il firewall non può stare lì a rispondere a ogni tipo di richiesta, altrimenti alla fine più che con un firewall si troverà con una fetta di groviera.

E quindi a un certo punto qualcuno ha osservato che HTTP/HTTPS (i protocolli del web) sono quasi sempre aperti, sono il passpartout dei firewall. E che quindi la cosa più semplice da fare era di usare HTTP come vettore, una specie di cavallo di Troia informatico, per trasportare protocolli che con HTTP non hanno nulla a che fare. Ed ecco che HTTP è diventato, per scherzo, UFBP, il protocollo passpartout da usare per passare dai firewall.
Oggi ci sono tantissime cose che “fingono” di essere HTTP: ad esempio terminal server, molte VPN, i protocolli di sincronizzazione di Exchange. E sempre su HTTP passano cose che con il World Wide Web hanno poco, anzi nulla a che fare, come ad esempio i web services, che hanno dentro la parola web, ma sono delle API.

E indubbiamente questo modo di comunicare su internet ha semplificato un sacco di cose, ma ha un prezzo.

Per capire meglio il problema vorremmo fare un’analogia. Supponiamo che un ipotetico censore voglia controllare tutte le comunicazioni che passano in un certo canale. Ora, trattandosi di un censore ignorante (del resto, fa il censore), questo signore conosce solo l’Italiano, e quindi decide di imporre che su quel canale si comunichi esclusivamente in lingua Italiana.
E, come dicono da queste parti, “fatta la legge, trovato l’inganno”. Consideriamo il messaggio sotto:
Questo è un messaggio in italiano. Lettera acca, lettera e, elle, elle, lettera o, spazio, v doppia, lettera o, erre ,elle, di, punto. Fine del messaggio.
Crediamo si possa dire che questo messaggio:

- È in Italiano
- Rispetta la lettera della legge
- Non ne rispetta l’intento
- Contiene un messaggio non in italiano.
- È mostruosamente inefficiente
- Per capirlo serve sapere l’inglese

Usare HTTP per trasmettere roba che in realtà non è HTTP ha più o meno gli inconvenienti dell’esempio, anche se non così estremi. Ad esempio active-sync trasmette tutti i contenuti codificati Base64, in modo che siano sempre solo testo. Così facendo si buttano 2 bit ogni 8, cioè si spreca il 25% della banda. Inoltre far passare di tutto per HTTP limita la capacità del firewall di distinguere e bloccare gli abusi. Ad esempio è improbabile che un firewall sappia entrare nel merito di una connessione Mapi over HTTP per bloccarla se non corretta.

Un esempio di questo problema è l'episodio di marzo 2021, quando tutti di corsa hanno dovuto aggiornare i server Exchange accessibili da Internet perché Hafnium, un gruppo di hacker, stava sfruttando una qualche debolezza di Exchange per entrare nei server e da lì nelle reti. A tutt'oggi non ci risulta esista un firewall che protegga un server privo delle patch. Al massimo rivelano i malware che i pirati iniettano nei server dopo che l'attacco è avvenuto con successo.
L'uso sistematico di HTTP per gran parte delle comunicazioni ha comunque un importante vantaggio: standardizza e mette a fattor comune tutte le parti presenti in tutti i protocolli come ad esempio l'autenticazione. E così facendo semplifichiamo l'implementazione e aumentiamo la sicurezza.

Il risultato di tutto questo è che il ruolo del firewall è cambiato. Non entra più tanto nel merito della "conversazione" che passa, perché non la può comprendere, ma cerca in quello che passa le "firme" del contenuto malevolo, in un modo simile agli antivirus. Un po' come se il censore dell'esempio cercasse la parola "hello" e bloccasse messaggi che la contenessero, non perché ne capisse il significato ma perché gli è stato detto essere pericolosa.
Ma tra antivirus e firewall c'è un'importante differenza: l'antivirus ha modo di vedere il malware nella sua forma finale, quella che il sistema sta per eseguire, mentre il firewall ne vede una forma transitoria, potenzialmente alterata dai vincoli imposti dal mezzo trasmissivo, quindi il firewall potrebbe essere meno efficace. In compenso il firewall le cose le vede prima che arrivino, e può quindi bloccarle prima che diventino pericolose.

Quindi: se HTTP serve a trasmettere di tutto, e non solo a trasferire ipertesti, allora forse potremmo cambiarlo di nome (UFBP?), e soprattutto adattarlo e renderlo il più possibile d'uso generale, rimuovendo limiti che avrebbero senso se si trattasse solo di HTML, e magari aggiungendo meccanismi per minimizzare l'uso di banda, facilitare la trasmissione di contenuti binari, aumentare la sicurezza. Insomma, definiamo un nuovo protocollo.

E il buon, vecchio HTTP lo teniamo per le pagine web...

L'INDIGESTIONE DI BISCOTTI

'STI BISCOTTI HANNO VERAMENTE SCOCCIATO (E PIÙ CHE BISCOTTI SONO CROCCANTINI DA CANE, DI QUELLI ECONOMICI)

Ormai non si riesce a entrare in un sito senza sentirsi chiedere se accettiamo i cookie (i biscotti in inglese). Se li accettiamo allora va tutto bene. Se non li accettiamo allora forse non funzionerà nulla, forse funzionerà qualcosa, forse non cambierà niente. Raramente i siti spiegano in modo comprensibile perché usano cookie e cosa succederebbe se non volessimo lasciarglieli usare.

Quindi proviamo a dire la nostra.

Innanzitutto non si tratta di biscotti, fisici o virtuali. Almeno, per noi il biscotto è una roba buona, questi invece sono una fregatura. Un nome più proprio sarebbe qualcosa come "traccia" oppure "memo". Il cookie è un piccolo file, che il server deposita nel nostro pc quando navighiamo il sito.
Lo scopo originale del cookie è di consentire al sito di riconoscere la sessione, perché in realtà http si dimentica tutto da una pagina all'altra. Senza il cookie il sito avrebbe la memoria di un pesce rosso, si dimenticherebbe di noi nel tempo in cui passiamo da una pagina all'altra. E il biscotto è la sua pillola di fosforo (*).
Quindi senza un cookie (o qualcosa di simile) si potrebbe navigare un sito, ma non sarebbe possibile ad esempio fare login e poi navigarlo sempre come la stessa persona. Il server non potrebbe sapere che siamo sempre noi quando cambiamo pagina. Il che ovviamente renderebbe irrealizzabile qualunque sito dove è necessario mantenere una memoria della visita.

Il problema è proprio nella memoria. I cookie sono un sistema perfetto per tracciare la navigazione, anche di un utente anonimo. Ad esempio, navigate su un sito di e-commerce e guardate pannolini, poi entrate su un giornale online e compaiono pubblicità di prodotti per bambini? E come facevano a sapere che avete bambini piccoli? Un cookie ha

fatto la spia! (ma non ha detto chi eravate, solo che eravate lo stesso che prima cercava pannolini).

Il fatto di poter usare i cookie persistenti (che sono biscotti a lunga conservazione, non scadono dopo che esco dal sito) per ricordare dove è stato un visitatore ha consentito usi di marketing e statistica che non hanno nulla a che fare con l'intento tecnico originale dello strumento. È un po' come se, quando andiamo in giro per negozi, i commessi ci attaccassero degli adesivi sulla schiena, senza dircelo, così poi tutti possono sapere dove siamo stati, se sanno riconoscere gli adesivi. E noi fessi, entrando in un negozio siamo contenti perché ci ricevono dicendo "vedo che è già stato da noi..."
E ormai il "vero sito" sente l'obbligo di raccogliere informazioni anche se non gli servono, un po' come il "vero uomo", che può appunto fare solo cose da uomo vero... (**)
Teniamo presente che stiamo parlando anche di utenti anonimi, che non hanno volontariamente inserito informazioni personali o anagrafiche o creato un account o che si siano fatti riconoscere in un qualsiasi modo. E che quindi non si aspettano di essere oggetto di una raccolta di informazioni e di una profilazione. Ma anche per gli utenti autenticati, il raccogliere ed elaborare dati su quello che hanno fatto navigando Internet non dovrebbe essere liberamente consentito.

E infatti non lo è, un po' perché in realtà il GDPR non lo permette, anche se in modo non proprio esplicito, e poi perché a un certo punto, ancora prima del GDPR il legislatore si è accorto di questo uso indiscriminato dei biscotti, e ha pensato di intervenire.

E qua non ci troviamo d'accordo col legislatore...

Perché il legislatore, che in nessun caso può pensare a una soluzione semplice per un qualsiasi problema, ha ritenuto che la cosa da fare fosse di dire qualcosa come "non lo puoi fare senza permesso"(***). E il risultato ovvio è che ora ogni volta che entriamo in un sito ci sentiamo chiedere "posso usare i cookie?", spesso seguito da una serie di opzioni incomprensibili nel loro scopo e nei loro effetti. Oppure ci sono due sole opzioni "1- accetta tutto e non rompere", oppure "2 - perdi mezz'ora a leggere un'informativa e a decidere quali cookie ti piacciono e quali no". Certi siti particolarmente antipatici ti lasciano entrare ma dopo poco bloccano tutto fino a quando non rispondi, ma devi prima capire che ti stanno facendo una domanda che non puoi ignorare. Altri mettono un banner piccolo piccolo in alto, che facilmente non vedi e ignori, e quindi si applica, ahimè, il silenzio assenso. E così via.
La soluzione semplice, e secondo noi logica, sarebbe di dire che i cookie di sessione sono sempre permessi, quelli persistenti mai. E così si riuscirebbe a entrare nei siti senza dover litigare con l'informazione sui biscotti e si potrebbe uscirne senza il timore di avere qualche adesivo attaccato alla schiena.

* Per una spiegazione informale (ma un poco datata) sui cookie si veda ad esempio The History of Cookies and Their Effect on Privacy | Digital Trends: una discussione non tecnica su cosa sono e qualche considerazione su come vengono usati.

** I cookie sono più diffusi di quanto si possa sospettare. Per una discussione un po' complessa ma interessante per i numeri che riporta: www16_final.pdf (wisc.edu).

*** Provvedimento del Garante dell'8 maggio 2014: Individuazione delle modalità semplificate per l'informativa e... - Garante Privacy. E, sempre del garante Cookie - Garante Privacy una spiegazione semplificata di cosa sono e delle leggi che ne regolano l'utilizzo.

LE RISPOSTE CHE NON ABBIAMO DATO

ALCUNE RISPOSTE CHE NON ABBIAMO MAI OSATO INVIARE

La firma "pesante"

Gentile sig. qzy,

Ci hanno informato che avete espresso disappunto per il fatto che i vostri messaggi vengono sovente messi tra la mail spazzatura. Vi assicuriamo che questo in nessun modo rappresenta il nostro pensiero su di voi, anzi.
Il problema è invece causato dal fatto che ci inviate messaggi in formato html, con firme corredate da immagini (per un totale di diversi megabyte) che dirigono su molteplici siti di domini differenti dal mittente.
Questo mette in agitazione il nostro sistema antispam, che di conseguenza suggerisce ad Outlook di trattare il messaggio con cautela.

-

Non stampare questa mail

Gentile sig. xyz,

Ho appena ricevuto il suo cortese messaggio, corredato di un altrettanto cortese invito a non stampare il messaggio stesso.

In effetti concordo con voi: Outlook fa veramente un pessimo lavoro quando si tratta di stampare, per cui è certamente meglio evitare. Suppongo fosse questo il motivo del suggerimento e vi ringrazio per la premura. Se invece vi preoccupaste per gli alberi, non saprei. Forse ci sono modi più efficaci per risparmiare stampe inutili.

Mi sorge però un dubbio. Mi chiedete di restituire firmato in calce l'incarico al trattamento dati personali allegato al messaggio. Ora, a parte il fatto che in virtù dell'art. 29 del GDPR non sarebbe necessario che ci incaricaste, come faccio a firmare il vostro documento senza prima stamparlo?

-

Se l'hai ricevuta in errore, sono guai

Gentile sig. klz,

Pochi minuti addietro ho ricevuto un suo messaggio. Purtroppo nell'aprirlo mi è caduto l'occhio su un minaccioso disclaimer, che appunto minacciava gravi conseguenze se avendo ricevuto il messaggio per errore, in qualche modo avessi disatteso le vostre aspettative.
A questo punto ho ritenuto opportuno non leggere la missiva e informarla, affinché potesse verificare che il messaggio fosse realmente indirizzato a me, nel qual caso può inviarmelo senza le sopramenzionate minacce. Oppure, se me l'avesse mandato in errore le chiederei di inviarlo al destinatario corretto.

Tutto sommato solo lei sa a chi intende inviare...

-

Giusto per sorridere prima delle ferie.
Ma per carità, non stampate questo articolo.
Al massimo condividete il link, sempre che l'antispam ve lo permetta...

IL TABACCAIO

DI MALE IN PEGGIO

Il primo è stato il Guardian, in un articolo di una settimana fa. Poi la CNN il giorno dopo. E supponiamo che poi altri abbiano ripreso l'argomento. Durante la testimonianza al congresso del 5 ottobre, Frances Haugen ha raccontato che secondo uno studio fatto internamente da Facebook, si dedurrebbe, che Instagram è psicologicamente tossico in particolare per le giovani donne ("We make body image issues worse, for one in three teen girls,").
Una su tre!
Ovviamente Facebook (nella persona di Mark Zuckerberg) nega, anzi dice che i social network possono avere effetti benefici per la salute mentale.
La questione non è però limitata alle giovani. Basta guardarsi intorno per rendersi conto che i social possono essere usati per far credere a molti falsità che nessuna smentita riesce a far dimenticare, e che poi spingono le persone ad agire secondo l'agenda di qualcuno. È successo con le elezioni in molti paesi, con i vaccini, in Birmania (dove Facebook ha aiutato i militari a combattere i Rohingya), in Etiopia.

Secondo il Guardian tutto questo sarebbe analogo a quanto ha fatto l'industria del tabacco, che avendo fatto esaustive ricerche scientifiche nella speranza di dimostrare che il tabacco non faceva male, ha invece stabilito con certezza che era causa di tumori. E ovviamente ha cercato di nascondere sotto il tappeto ricerca e risultati, e continuato a sostenere che no, il tabacco non faceva male. In effetti a loro faceva benissimo.

No, Facebook e i produttori di tabacco in questo non sono simili. In confronto a Facebook, i produttori di tabacco sono dei pivelli.

Non c'è nulla da stupirsi quando, di fronte al denaro, qualcuno (azienda o persona) commette un reato. Fa parte della nostra natura, come il fatto di essere animali sociali. Il problema è che siamo un po' troppo animali, molto più degli animali veri.
Ma c'è una differenza importante tra chi vende roba che fa male alla salute e Facebook. I primi si limitano a far male al malcapitato (o autolesionista) consumatore. Ti piace il tabacco? Ecco. Ti piace l'alcol? Ecco. Ti piace scommettere? Si accomodi. Certo sono cinici e spesso bugiardi. Ma anche il cliente fa la sua parte.

Il social network è diverso, perché nella sua forsennata ricerca dell'utile a tutti i costi consente ad alcuni di diffondere un veleno che distrugge la vita di innocenti, mina la società, aiuta i delinquenti. Le vittime non sono solo persone che consapevolmente comprano qualcosa, ma anche tanti altri, che quella cosa forse nemmeno la usano.

Quello che ci stupisce non è l'ingordigia di Mark e compagni, ma l'inerzia di tutti noi, che in nome di una libertà che non ci serve, quella di poter scrivere qualunque idiozia su internet, ci rifiutiamo di regolamentare e limitare in modo serio queste piattaforme.
Se il direttore di un giornale è l'ultimo responsabile di ciò che pubblica, perché non può valere la stessa cosa per un social? Forse perché sarebbe impossibile controllare? Probabile, e in questo caso dobbiamo rinunciare al social. Non possiamo semplicemente consentire il danno.
E perché è così facile fare profili falsi sui social? Non si potrebbe multarli ogni volta che consentono a qualcuno di presentarsi per quello che non è? Ancora una volta: secondo noi non è importante che si possa fare il controllo. È importante attribuire la responsabilità, se poi è impossibile fare un social come Facebook stando alle regole che gli vogliamo imporre, allora Mark dovrà trovarsi un'altra occupazione, con buona pace di tutti.

Altra proposta: costringiamoli a fornire solo servizi a pagamento. Sarebbe analogo a quello che è successo con la televisione e la musica, che oggi in buona parte sono diventati streaming a pagamento. Questo eliminerebbe gran parte degli account falsi e ne aumenterebbe il costo, limitando un poco la possibilità di fare campagne basate su identità inesistenti.

CASI DI BUSINESS

CAAST

CAAST, azienda con una presenza ventennale nel mercato dei sistemi di tenuta, con il passaggio a realtà industriale emerge da un lato il bisogno di far evolvere i sistemi informativi da semplici esecutori di task a strumenti fondamentali per prendere decisioni di natura tattica e strategica e, dall'altro lato, di dotarsi di un sistema di supporto alle decisioni per il management. In questo quadro si inserisce il cambiamento del sistema ERP aziendale e la scelta di adottare la soluzione Microsoft Dynamics 365 Business Central con il supporto del partner Microsys. La scelta di adottare la soluzione Microsoft Dynamics 365 Business Central, è avvenuta in seguito a un'attenta attività di software selection attraverso cui sono stati valutati: interfaccia utente, copertura delle aree funzionali, innovazione, sviluppo verso il cloud e integrazione con i sistemi informativi già presenti in CAAST.
Il progetto di adozione della soluzione ERP Microsoft, ha contribuito in modo fondamentale a comprendere quali erano le inefficienze aziendali e ad evidenziare nuovi ambiti di miglioramento. Inoltre, contribuisce sempre più a migliorare l'efficienza e la capacità dell'azienda di generare flussi di cassa.

CASTELLO SGR

Castello SGR, società di gestione del risparmio indipendente, leader di mercato nella promozione e gestione di strumenti di investimento focalizzati sul settore Real Estate, consapevole sulle criticità in ambito cybersecurity decide di innalzare la sicurezza IT. Seguendo rigorosamente i passi della soluzione Cyber Defense 365 di Microsys, è stato definito un ampio programma di attività di presidio, di aggiornamento tecnologico e di controllo di configurazioni, su vari fronti: quello dei servizi cloud (la posta elettronica, la gestione di contenuti e della collaborazione), dei dispositivi mobile, sempre più utilizzati in Castello SGR (laptop, tablet e smartphone) tra cui anche sistemi di proprietà degli utenti, delle identità digitali e dei dati critici del business. L'esperienza di Castello SGR ha messo in luce come un corretto percorso di sicurezza, oltre a incrementare le capacità di difesa, monitoraggio e risposta, possa anche portare altri valori per l'impresa: una maggiore soddisfazione dei clienti e una semplificazione delle attività, indispensabile per evitare impatti sulla produttività delle persone, con un giusto bilancio tra sicurezza e praticità.

DEBEM

DEBEM, azienda specializzata nella progettazione, costruzione e produzione di pompe industriali, prima di adottare Dynamics NAV, i processi aziendali viaggiavano prevalentemente su carta e fogli excel, mentre il software gestionale veniva impiegato esclusivamente per fini contabili, l'inserimento di offerte e gli ordini. Grazie l'adozione del gestionale Dynamics NAV, con il supporto di Microsys, tutti i processi aziendali sono stati integrati e molti passaggi sono stati automatizzati. L'apporto del Partner Microsys è stato considerato di grande valore, sia per la presenza costante in azienda nella fase iniziale, sia poi per l'implementazione molto rapida del nuovo gestionale. La Direzione di DEBEM si pone l'obiettivo di trasformare un'azienda d'estrazione artigianale in una realtà industriale efficiente e sostenibile, in grado di riorganizzarsi e crescere con slancio, con una filosofia improntata a un'elevata efficienza. Disporre di una piattaforma integrata va nella direzione della logica di internazionalizzazione e aiuterà a raggiungere nuovi obiettivi, come l'adozione di un Lean Manufacturing che punti a rendere ancora più efficienti e integrati i processi di Procurement e Produzione.

ENERCOM

Il marketing di Enercom Luce e Gas, una delle maggiori aziende italiane private del settore energy, specializzata nella vendita di luce e gas a privati e aziende, si era posto l'obiettivo di analizzare la domanda di clienti e prospect per capire come ampliare la propria offerta e assistere al meglio i propri clienti. Enercom ha quindi ideato, con il supporto di Microsys, uno strumento informativo che potesse rispondere con semplicità ai clienti, indirizzandoli verso l'offerta più adeguata. È stato pensato un percorso che, partendo da una richiesta molto semplificata di alcune informazioni, e tramite un successivo algoritmo per la configurazione della migliore proposta, potesse indicare al prospect la migliore offerta Enercom, replicando in un Portale l'aspetto consulenziale che si offre di solito nei punti vendita. Oggi, grazie al nuovo strumento informativo, il Marketing e le Vendite di Enercom traggono vantaggio di una visione costantemente aggiornata e completa dei dati dei clienti grazie all'integrazione in cloud, dall'input nel Portale alla successiva sincronizzazione e automazione dei flussi verso i moduli Marketing e Sales di Microsoft Dynamics 365.

GEWISS

GEWISS, oggi la più importante azienda del settore elettrotecnico a capitale italiano, aveva la necessità di avvicinare maggiormente i dipendenti all'azienda, in particolare quanti attivi nelle sedi estere (500 su un totale di 1.600 risorse circa), migliorare la comunicazione interna e sviluppare la cultura di gruppo aziendale. Vi era quindi l'esigenza di realizzare una nuova piattaforma intranet aziendale facilmente accessibile, predisposta per una comunicazione efficace, facile da usare, sia nella navigazione, sia nella produzione e condivisione di contenuti. Per questo era necessario un vero salto tecnologico: GEWISS disponeva infatti di una precedente soluzione intranet non più in uso perché obsoleta e poco accessibile dall'esterno. Microsys fin dall'inizio suggerisce a GEWISS di sviluppare la GEWISS Intranet su SharePoint Online; una scelta che si è dimostrata vincente per i numerosi vantaggi apportati, come, per esempio, non dover gestire alcun sistema di back end per offrire un servizio intranet altamente disponibile. A oltre un anno dall'avvio della Intranet, il sistema è vivo, costantemente aggiornato e vi confluisce ogni comunicazione a partire da quelle del CEO a scendere.

LILT

La Lega Italiana per la Lotta contro i Tumori, LILT, è una organizzazione senza scopo di lucro, con sede a Roma, articolata in 106 Associazioni Provinciali. L'esigenza da cui è partito il nuovo sistema informativo di LILT basato sul gestionale Microsoft Dynamics NAV era quella di rendere più fluido il lavoro del medico, automatizzando la refertazione degli operatori sanitari in modo da liberare tempo da dedicare all'ascolto delle persone ed ai pazienti. Oggi con i referti in digitale il medico che effettua una visita di prevenzione oncologica può accedere allo storico degli esami del singolo paziente, alle precedenti prestazioni, effettuare analisi e confronti. Per quanto riguarda invece i volontari che operano nell'accettazione, a cui prima era richiesta una compilazione a mano di fogli di carta prestampati, oggi beneficiano di un sistema online che permette un notevole risparmio di tempo oltre che ridurre la possibilità d'errore. Il valore principale di Microsys, nello sviluppo del nuovo sistema informativo per LILT, è la capacito di saper integrare, in un ambiente molto complesso sia dal punto di vista tecnologico che di processo, le applicazioni per automatizzare le procedure.

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 di gestione oltre che per ratei e risconti. Inoltre la 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

VDI 365

Virtual Desktop Infrastructure 365, la soluzione di Microsys basata su tecnologia Microsoft Azure che ospita i desktop aziendali in remoto e consente agli utenti 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

CYBER DEFENCE 365

La protezione, l'analisi e le strategie di reazione all'interno di una corretta progettazione della sicurezza sono attività fondamentali e da non trascurare per il dipartimento IT. Una solida pianificazione delle misure di sicurezza può effettivamente contribuire a semplificare la protezione del sistema informativo aziendale, attraverso misure preventive costantemente verificate, ri-verificate e aggiornate per minimizzare la superficie d'attacco.

- Diffondere la cultura della sicurezza in azienda
- Aumentare la protezione delle identità e dati aziendali
- Aiutare a strutturare gli investimenti e il piano sulla sicurezza informatica

LEARNING 365

La formazione dei dipendenti è un fattore importante che dev'essere costruita tenendo anche in considerazione l'esigenza di ottimizzare e sincronizzare il percorso di formazione con le logiche aziendali, offrendo ai propri dipendenti una piattaforma di e-learning per un'esperienza di formazione al passo con i tempi: la parola chiave è flessibilità, in sintonia con i propri impegni.

- Piattaforma di e-learning per scegliere quando, dove e come frequentare i corsi
- Offrire più opportunità e percorsi formativi personalizzati
- Un unico ambiente per la creazione, gestione e controllo dello svolgimento dei programmi formativi

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

INCONTRI 2021

PILLOLE DI INNOVAZIONE

PROGETTI DI TRASFORMAZIONE DIGITALE

Incontri per diffondere il valore del digitale attraverso la narrazione dei progetti aziendali di successo e la voce delle persone che l'hanno guidato e reso possibile

TECH BITS

TECNOLOGIE E SOLUZIONI PER L'INNOVAZIONE

Incontri online per approfondire le tecnologie di Microsoft.

24 FEBBRAIO 2021

PILLOLE DI INNOVAZIONE

INCONTRO ON-LINE CON CA' ZAMPA

Insieme a Cà Zampa, la prima rete in Italia di centri veterinari che offrono tutti i servizi legati al benessere integrato dei pet, abbiamo presentato quanto sia importante adottare una piattaforma integrata per la gestione aziendale e la relazione con il cliente, che integri anche strumenti di marketing e che sia in grado di crescere insieme all'azienda.

23 GIUGNO 2021

PILLOLE DI INNOVAZIONE

INCONTRO ON-LINE CON ENERCOM

Insieme ad Enercom, una delle maggiori aziende italiane private del settore Energy & Utilities, abbiamo compreso come sfruttare le potenzialità di Microsoft Power Platform e della piattaforma Dynamics 365 per sviluppare la strategia di Phygital Marketing. La versatilità degli strumenti adottati permette al dipartimento Marketing di intercettare i diversi punti di contatto con i potenziali clienti ed indirizzare i dati nel processo di lead generation unificato, migliorando da un lato la Customer Experience e dall'altro il "win rate" della forza vendita.

14 APRILE 2021

TECH BITS

INCONTRO ON-LINE CON MIDA SOLUTIONS

Durante questo primo incontro del programma Tech Bits abbiamo presentato in collaborazione con Mida Solutions, i vantaggi di Microsoft Teams Phone Systems e Dynamics 365 integrati con la soluzione di Contact Center di Mida Solutions, per gestire in maniera centralizzata ed efficace la comunicazione con clienti e partner.

6 OTTOBRE 2021

TECH BITS

Benefici e potenzialità di Microsoft Power Platform: la piattaforma che semplifica, non più solo per gli sviluppatori ma anche per utenti, la creazione delle applicazioni.

LICENSING TRACK

SUGGERIMENTI E SOLUZIONI

Video registrazioni volte a condividere suggerimenti e soluzioni sulle modalità di adozione dei prodotti e dei servizi di Microsoft.

LUGLIO 2021

LICENSING TRACK

Nel primo evento registrato del programma Licensing Track, abbiamo condiviso suggerimenti e soluzioni sulle modalità di adozione dei prodotti e dei servizi di Microsoft:

- Cosa compro quando ho l'esigenza di prodotti e servizi cloud di Microsoft?
- Come posso acquistare le licenze dei prodotti e dei servizi di Microsoft?
- Cosa serve ai miei utenti per lavorare?

OTTOBRE 2021

LICENSING TRACK

Non si vedono, ma si usano: le CAL

Il concetto di CAL esiste da anni per i modelli di licenza Server con CAL, ma non è obsoleto, e anche nei sistemi Ibridi di oggi occorre ben valutare la necessità di coprire utenti e/o device con le CAL.

Purtroppo non tutti ne conoscono l'esistenza e ne comprendono dove è necessario applicarle, nella seconda puntata di Licensing Track sveliamo il mistero e "Uscimmo a riveder le stelle".

Milano | Via A. da Recanate, 1 - 20124 Milano | F. +39 02.303.707.70
Torino | P.za Luigi Lagrange, 1 - 10123 Torino | F. +39 011.45.46.013

T. +39 02.303.707.01 | info@msys.it

www.msys.it