MICROSYS

30 ANNI

DIARIO 2022

Diario di un anno: 2022

Cari lettori e care lettrici,
anche quest'anno è passato con il suo carico di drammi terribili, responsabilità degli uomini, dei loro egoismi, della loro sete di potere e prevaricazione.

Credo che un fondo di tristezza e di sconforto non ci possa lasciare durante queste feste.

Non resta, nel nostro piccolo, che fare quello che possiamo nel quotidiano: non mancare mai alle nostre responsabilità e ai nostri doveri, al primo posto quelli sociali.

In alcune situazioni voi tutti avete delle posizioni importanti da cui dipende la qualità di vita di molte persone, in altri casi la responsabilità è solo quella di non parcheggiare in un posto riservato ad un disabile. Ecco, se ognuno di noi, in ogni momento, ricordasse di non essere egocentrico e prevaricatore e non accampasse scuse con sé stesso per perdonarsi comportamenti scorretti, il mondo sarebbe migliore.
Con questa riflessione ingenua, un po' sciocca e banale, non mi resta che augurarvi un Buon Natale e un sereno Anno Nuovo, con tutto il cuore.

Spero che la lettura dei Controcorrente sia un momento che vi regali una risata e un sorriso.

Microsys ha compiuto 30 anni e per 30 anni abbiamo mantenuto la rotta, facendo crescere una azienda responsabile, non solo attenta alla "bottom line".

I prossimi 30 anni saranno un nuovo viaggio dove Microsys cercherà di mantenere sempre fede al suo motto "Attenti, concreti e appassionati" per il nostro lavoro e per il nostro modo di viverlo.

Alessandra Galdabini

CONTRO CORRENTE

6_ Il pollo di coccio

9_ Le minacce

12_ Un UCAS tra le montagne

15_ Chatbot e motori di ricerca

16_ Gli stupefacenti

22_ Un fatto triste

24_ La fantasia del ladro

26_ The “art” of computer programming?

IL POLLO DI COCCIO

PHISHING, SI RIESCE A DIFENDERSI?

Qualche tempo fa ci è capitato di vedere un report interno sui risultati di una campagna di phishing fatta da un cliente: su 671 utenti presi di mira dalla campagna ben 119 si sono fatti pescare. Chiaramente troppi.

Ma quel che è peggio è che i 671 erano un'estrazione (da più di 9.000) di quelli che si erano fatti pescare nelle precedenti campagne. E questi erano stati oggetto di un'attività di formazione. Che apparentemente è servita poco.

La nostra prima reazione è stata di liquidare la cosa commentandola con un istintivo, romanesco e un po' presuntuoso "ma questi so' de coccio".

Ma poi ci abbiamo riflettuto.

Prima di tutto però vediamo cosa sono il "phishing" e la campagna di phishing. Il problema l'abbiamo discusso più di una volta: una mail falsa che invita l'utente ad andare su un sito per risolvere un qualche problema, ad esempio potrebbe dire "il tuo conto in banca è in pericolo!!! Fai click qui per risolvere il problema". Se il malcapitato fosse anche un po' pollo e seguisse il link, si troverebbe sul sito di una banca (sicuramente falso, e che potrebbe o no sembrare quello della sua banca). Se casualmente si trattasse della sua banca allora quell'utente potrebbe anche provare a fare login, e se lo facesse starebbe raccontando a qualche malintenzionato la propria user e password. Per questo tutte le banche utilizzano meccanismi di autenticazione a doppio fattore (il messaggino col numero, o altra roba del genere) in modo da rendere la sola password insufficiente per attivare l'accesso.
La campagna di phishing, nel contesto di questa discussione, è invece un'attività compiuta dai sistemi informativi, che deliberatamente mandano false mail di phishing (quindi sono false mail false, il che sia chiaro che non le rende vere ma caso mai veramente false!), cercando di stanare i polli.
Per poi dargli un'amichevole tirata d'orecchie, farli partecipare a una qualche attività di formazione (ce la immaginiamo come le riunioni degli alcolisti anonimi "io da dieci giorni non ci casco" e tutti che applaudono) e con questo evitare che i polli siano ancora polli con le vere mail false...

Ora chiaramente ci aspettiamo che qualcuno ci caschi, ma uno su sei è assolutamente troppo, ed è tantissimo se si pensa che sono quelli che erano già stati beccati e in teoria istruiti sul problema e sui rischi che ne derivano.

Dicevamo che la prima reazione è stata di pensare che il problema fossero gli utenti.
Ma teniamo presente che: sono sicuramente utenti con cultura nella media, anzi probabilmente superiore alla media, sono persone attive abituate a usare strumenti informatici, sono informate di quello che gli succede intorno. Inoltre, non ci sono tensioni o contenziosi con l'azienda o con i sistemi informativi che possono aver causato un comportamento deliberatamente poco collaborativo.

Quindi il dare la colpa ai soliti utenti potrebbe essere un po' superficiale e precipitoso. E comunque gli utenti sono come sono, non possiamo pretendere di averli come piacciono a noi, siamo noi a dover capire come spiegare loro cosa ci serve e magari ottenere che ci aiutino.

Teniamo presente che il problema è serio: se sei persone su cento ci cascano, allora se un malintenzionato riuscisse a procurarsi ad esempio 100 indirizzi mail della nostra azienda, avrebbe la certezza di trovare almeno un pollo (quasi, la probabilità è del 99.8%).

Ma, tornando al problema originale, come mai così tanti ci sono cascati sia al primo giro che al secondo? E soprattutto, cosa si potrebbe fare per evitarlo?

Il problema evidentemente è nella formazione e nell'informazione, sia prima che dopo la campagna.

Prima di tutto forse dovremmo semplificare quello che chiediamo agli utenti, ed evitare di chiedere loro di giudicare se il messaggio è

legittimo. Invece di spiegare che le mail potrebbero essere malevole, che in qualche caso seguendo un link in una mail si potrebbe cadere vittime di una truffa e dare gli elementi per distinguere, forse dovremmo dire che non si deve mai seguire un link in una mail. Mai. Senza distinzioni o precisazioni. Il che, seppur un po' estremo, è probabilmente la cosa che dovremmo effettivamente fare tutti.
Già, perché anche i migliori ci cascano. Solo che tipicamente non lo vogliono ammettere.

Poi sarebbe ora che si rinunciasse a mandare link nei messaggi di posta, e nei casi dove la si vuole usare per validare ad esempio un indirizzo, ci si limitasse ad inviare un codice, come si fa già in molti casi per l'autenticazione a doppio fattore. Se nessun mittente legittimo inviasse messaggi contenenti link, quelli illegittimi salterebbero all'occhio perché li contengono!

Una terza cosa è la comunicazione in generale, i media. Ci siano casi, nemmeno pochi soprattutto dopo log4j (*), dove effettivamente gli hacker entrano nelle reti private sfruttando buchi nella rete di protezione. Ma sono più frequenti i casi dove il tutto inizia con un utente che abbocca a una mail di phishing. Forse dovremmo smettere di dire ad esempio "gli hacker sono entrati nella rete della regione xyz" o altre cose del genere, ma dire cose come "un utente pollo, della regione xyz, si è fatto fregare da un hacker", evidenziando il fatto che ad aprire la porta è stato un utente...

Ps: per una discussione più approfondita sul phishing, sulle tecniche usate per ingannare il destinatario e su possibili difese si può guardare Phishing.org. Non concordiamo con parte di quanto suggerito per difendersi, e nemmeno su alcune caratterizzazioni delle mail di phishing, ma nell'insieme è certamente istruttivo.

** Recentemente è stata esposta una anomalia in una libreria Java che ha reso facilmente attaccabili una grande quantità di siti e di apparati: Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability - Microsoft Security Blog.*

LE MINACCE

GIRANO IN RETE, INVISIBILI COME GLI SQUALI. POI OGNI TANTO AFFIORANO.

Qualche settimana fa Sonicwall ha pubblicato il "2022 Sonicwall Cyber Threat Report", un interessante documento di analisi sui malware che i firewall hanno incrociato lo scorso anno. Sono 66 pagine piuttosto dense che vale la pena leggere se si è interessati all'argomento.
Non vogliamo togliervi il piacere della lettura, ma vorremmo riprendere alcune delle conclusioni del report, quelle che ci hanno più colpito.

Partiamo dal "2021 in review", che non è nemmeno nel documento, ma nel sito da cui lo si scarica (link sopra). Non è tanto la scala temporale e il numero di eventi a preoccuparci, ma un riscatto, pagato, da 4.4 milioni di dollari. E probabilmente c'è un secondo riscatto, quello di Colonial Pipeline, che qui non è citato ma che si dice sia stato pagato (sembra poi che il gruppo responsabile si sia pentito, su questo abbiamo qualche dubbio).
È chiaro che a fare l'hacker e il distributore di ramsomware si possono fare molti soldi, e non sembra essere nemmeno tanto difficile. E quindi dobbiamo dormire preoccupati, o almeno preoccuparci prima di andare a dormire.

Una prima cosa: è facile puntare il dito contro quelli che pagano il riscatto, perché così facendo peggiorano la situazione. Però è meno facile decidere di non pagare se ti hanno reso inaccessibili i dati e cancellato i backup. Quindi bisogna comunque essere in grado di ripristinare i dati. Dobbiamo considerare l'evento ramsomware come possibile, proprio come il disastro fisico. Con una differenza, il backup geografico non serve. Serve un backup che non si possa cancellare. Nel senso che non possiamo cancellarlo nemmeno noi. Perché dobbiamo ipotizzare che l'hacker ci freghi le credenziali, e agisca con la nostra autorità. Per questo Azure Backup tiene i dati per 14 giorni anche quando li si cancella, e manda all'amministratore una mail, tanto per stare dalla parte della ragione.

Pare che gli hacker abbiano inventato la tripla estorsione (o doppia nei casi fortunati). In sostanza, infettano un poveraccio con un ramsomware, e gli estorcono un riscatto per ridargli accesso ai dati. Poi lo ricattano una seconda volta per non rendergli pubblici i dati. Poi ricattano le persone coinvolte nei dati, per non pubblicare i loro dati personali. È successo in Finlandia a un gruppo di cliniche di psicoterapia. Hanno ricattato prima le cliniche, due volte, poi i pazienti per non pubblicare le note delle sedute.
Come osserva il report di Sonicwall, il fatto è che pagare il riscatto non garantisce assolutamente nulla. E il fatto che l'interlocutore sia per definizione ladro, dovrebbe dirci quanto ci si possa fidare.

Una nuova tecnica di phishing, basata sulla più vecchia tecnologia di comunicazione, è emersa in USA: ti mandano un pacco (fisico, vero), che fa finta di essere un regalo da Amazon (vi è mai capitato di chiedervi "ma questo chi me lo manda?", se avete parenti lontani sicuramente sì). Oppure potrebbe essere una busta proveniente dal ministero della salute. Dentro c'è una chiavetta USB, un falso buono omaggio e una lettera che spiega la falsa missione della chiavetta. E dentro la chiavetta USB il vero regalo...
La difesa è possibile: configurare il pc/laptop/tablet in modo che non esegua nulla da supporti rimuovibili. E non avere autorità amministrative.

Un'altra novità, non tanto diffusa ma interessante nel concetto, è il ladro di criptovalute: una app android che si fa dare il permesso di accedere al sistema e poi accede al cripto-portafoglio per prelevare i bitcoin e trasferirli all'hacker. Grazie alla non tracciabilità della criptovaluta i ladri sono al sicuro e il malcapitato è senza difesa. Ironico il nome dell'app, "Trust: Crypto & Bitcoin Wallet". Ci auguriamo che sia sparita dallo store, ma il fatto che ci sia stata è più che sufficiente. In questo specifico caso la difesa è facile, basta non possedere criptovalute.

Sempre riguardo alle criptovalute, pare che nel 2021 ci siano stati più di 20 attacchi a piattaforme di scambio di cripto valute in cui i ladri si sono appropriati di più di 10 milioni di dollari. E in quattro di questi casi il bottino ha superato i 100 milioni. Ancora una volta, perché speculare in criptovalute, quando si può divertirsi di più giocando al videopoker nel bar sotto casa? Almeno in questo caso i soldi non vanno all'estero.

Ultima considerazione, la lista delle vulnerabilità zero-day (*). Su 11 casi, 2 sono su Apple, 2 su Google Chrome, 2 Microsoft, e 1 per WordPress, Pulse, Adobe, Kaseya, Apache.
L'ultima, Apache Log4J, è molto insidiosa in quanto consente a chiunque di accedere remotamente ai sistemi vulnerabili, senza credenziali e senza necessità di utilizzare tool complessi. E per di più quella vulnerabilità è presente in tantissimi sistemi ed apparati.
Morale: non è più vero (ed è un bel po' che non è vero) che i sistemi più vulnerabili sono quelli Microsoft...

** Zero-day: sono vulnerabilità che vengono scoperte e sfruttate dagli hacker prima che sia disponibile una patch. Normalmente quando una vulnerabilità viene scoperta il ricercatore che la trova informa privatamente il produttore (e spesso per questo viene pagato). Il produttore crea la patch e la pubblica, prima che si sappia quale è il problema. Gli hacker studiando la patch possono scoprire quale era la vulnerabilità, e quindi provare ad attaccare i sistemi non aggiornati. Ma la patch arriva prima dell'hacker.*
Se però è l'hacker a trovare la vulnerabilità allora non avviserà il produttore, e l'attacco avverrà senza preavviso, e senza patch disponibile: zero-day.

UN UCAS TRA LE MONTAGNE

L'UFFICIO COMPLICAZIONI AFFARI SEMPLICI, OVVERO L'ETERNA LOTTA TRA GLI ITALIANI E I LORO BUROCRATI

Siamo più o meno tutti d'accordo sul fatto che l'Italia è tra i paesi più liberi del mondo. Noi pensiamo addirittura della galassia, perché il nostro è l'unico paese dove nei fatti i cittadini sono liberi di non rispettare le leggi. È una lotta continua tra noi e il burocrate, dove quest'ultimo inventa complicazioni assurde in qualunque cosa si debba fare, convinto che l'unica missione del cittadino sia quella di fregare i burocrati, non di vivere la sua vita.
E quindi tutto è inutilmente complicato, anche cose banali, come usare uno Skipass.

Recentemente abbiamo avuto la fortuna di poterci concedere una breve pausa tra le montagne (non tanto) innevate. Come prima cosa, armati di assicurazione e Green pass "rafforzato" abbiamo chiesto di acquistare lo Skipass per tutto il (breve) periodo.

Dopo aver emesso l'oggetto e raccolto il pagamento, la signora allo sportello ci dice: prima di usarlo dovete attivarlo, è una cosa un poco complicata, se volete vi aiuto io. Avete 20 minuti?
Abbiamo pensato di aver capito male, "come 20 minuti, per attivare uno Skipass?" e lei "eh sì, sa c'è da scaricare un'app, è un poco complicato".

Effettivamente non siamo proprio giovanissimi, e quindi abbiamo pensato che precedenti clienti della nostra età fossero tanto lenti ad usare il telefonino da fare in 20 minuti quello che ovviamente non poteva richiederne più di un paio. Noi però siamo nonni, sì, ma informatici. Non ci facciamo certo intimidire da un'app. Per cui abbiamo dato per scontato che noi l'avremmo saputo fare in pochi istanti, e magari senza bisogno di aiuto. Nonni presuntuosi che pensano di saperla lunga.

Il primo passo, download e install dell'app procede senza intoppi. In pochi istanti siamo operativi.

Lanciamo l'app, che immediatamente ci informa che dobbiamo disabilitare il battery manager, altrimenti l'app potrebbe non funzionare in background. E della mia batteria non vi importa nulla? E perché l'app per validare lo Skipass deve essere attiva in background? Infatti non abbiamo disabilitato nulla e abbiamo accuratamente spento l'app e sugli sci funzionavano benissimo. Anzi abbiamo avuto l'impressione che con l'app attiva rallentassero un po'.

Gestita la faccenda della batteria ci vengono chiesti un indirizzo mail, una password (nuova, specifica, nessun sso...) e successivamente un nome, cognome, data di nascita, genere (obbligatorio, ma posso dire "non te lo voglio dire"). Non è chiaro perché per usare questa app si debbano dare queste informazioni. Magari servono?

Finita la parte anagrafica dobbiamo caricare lo Skipass sull'app. Puoi usare NFR (near field radio, in sostanza la tecnologia contactless delle carte di credito e appunto dello Skipass). Metti lo Skipass a contatto col telefono e l'app dice "hai NFR disabilitato". Ovviamente non è così, e il telefono ha vibrato, quindi ha parlato con lo Skipass. Non importa, la signora non si scompone, anzi dice "è normale" e procede a digitare il numero dello Skipass. Che guarda caso conosce tutte le informazioni che abbiamo appena inserito. Magari l'intento è appunto di incrociare le info? No, non devono corrispondere, l'abbiamo verificato.

A questo punto devi dare il Green pass all'app e farlo corrispondere allo Skipass. Scegli uno Skipass che hai caricato e poi leggi con la telecamera il QR code. Oppure se l'hai memorizzato sul telefono lo cerchi tra i tuoi file.

Poi in un passo successivo dici all'app di validare il Green pass, e a questo punto presumiamo che l'app interroghi i sistemi centrali, o periferici, o chissà dove, e incroci i dati dello Skipass con quelli del Green pass, per assicurarsi che corrispondano, ma no, anche se non corrispondono va bene lo stesso, l'abbiamo verificato. Alla fine della procedura il Green pass è validato e lo Skipass è buono.
Per 24 ore.
Sì, il giorno dopo devi rifare la validazione, perché il Green pass nel frattempo potrebbe essere scaduto o essere stato invalidato da un test positivo.

In effetti ci sono voluti almeno 15 minuti.

Ora, ci chiediamo:

- Perché abbiamo dovuto inserire informazioni anagrafiche che non servivano? Teniamo presente che digitare su un telefonino non è il nostro passatempo preferito.
- Perché non limitare al massimo le richieste di informazioni?
- Per quale motivo al caricamento del QR code il sistema non l'ha validato al volo?
- Perché non ha provveduto a rivalidarlo automaticamente ogni 24 ore fino a un eventuale fallimento?
- Perché usare un'app quando si sarebbe potuto leggere il QR code al momento della vendita e validarlo centralmente ogni mattina utilizzando gli stessi sistemi che gestiscono lo Skipass, senza chiedere informazioni aggiuntive?
- Se proprio vogliamo farci del male e usare una app, perché non farne una dove metto un numero di Skipass, leggo un QR code e voilà lo Skipass è attivo e si attiva automaticamente ogni mattina?

La risposta è più o meno sempre la stessa. Siamo fissati con le app, siamo fissati con la raccolta di dati inutili, siamo convinti che tutti cercheranno di barare per cui complicando tutto facilitiamo la vita a chi appunto vuole barare, non coltiviamo l'amore per la semplicità e l'eleganza nelle soluzioni tecnologiche, non possiamo memorizzare nulla, perché non lo vuole il garante, anzi no, i dati dello Skipass li memorizziamo, ma il QR code no, quello non si può.

CHATBOT E MOTORI DI RICERCA

LORO DIVENTANO SEMPRE PIÙ INTELLIGENTI, E NOI SEMPRE PIÙ STUPIDI?

Chatbot, da chat+(ro)bot, quindi in italiano potremmo tradurlo con "robot che parla". Gli manca però il numero della smorfia, ci dovremo accontentare del 48, per approssimazione.
Il bot del chatbot in verità non sarebbe un vero robot. È un'entità virtuale, che capita di incontrare navigando internet, e che interagisce con l'utente in linguaggio naturale, scritto o vocale.
Erano onnipresenti, praticamente chiunque avesse un sito si sentiva obbligato ad avere un chatbot. Ma poi molti si sono resi conto che se accetti che ti facciano qualunque domanda devi anche essere in grado di produrre qualunque risposta, o almeno produrre una risposta pertinente la maggior parte delle volte.
Mentre in realtà nella maggior parte dei casi le risposte disponibili erano pre-confezionate, e poche. Pochissime.
Come nel negozio online di jeans, a cui abbiamo chiesto "dove è coltivato il cotone dei vostri jeans?" e lui ha proposto di rispondere a "Come faccio a verificare che i miei jeans xxxxx siano proprio quelli originali e autentici?". Bah, come bot ci pare piuttosto inutile.

Ma in realtà il chatbot funziona, e pure bene. Il problema non è il bot, o la sintesi vocale, o la comprensione della lingua parlata. Quelle sono tutte cose che l'intelligenza artificiale ora sa fare benissimo. Il fatto è che poi dietro al coso che capisce e parla serve una base di conoscenza da cui pescare le risposte.

E quindi ovviamente il miglior candidato per un chatbot è il motore di ricerca. Di questo si preoccupava il MIT Technology Review qualche mese fa (Chatbots could one day replace search engines. Here's why that's a terrible idea. | MIT Technology Review).

La cosa è molto semplice: invece di cercare un documento che contenga un'informazione che risponde a una mia domanda, faccio direttamente la domanda al motore di ricerca.

Anni fa per scoprire quando è nato Napoleone saremmo andati su Google e avremmo digitato “Napoleone Buonaparte”. Dalla lista dei risultati avremmo selezionato un articolo dall’aria promettente, ad esempio Wikipedia o la Treccani, e nell’articolo avremmo cercato la data di nascita.
Oggi se scrivo o dico “Quando è nato Napoleone” Google risponde direttamente “15 agosto 1769”, e se scrivo “dove è nato Napoleone” mi risponde Ajaccio, senza batter ciglio (perché non ha le ciglia).
Ma attenzione: Google non sa niente di Napoleone, non ha capito la domanda, e nemmeno la risposta. Google ha capito la sintassi, ha estratto dalla domanda quali erano le informazioni richieste, ha cercato nei suoi database (quindi su internet) la risposta e l’ha presentata. E non ci ha mostrato la sorgente, e meno ancora ci ha permesso di sceglierla.

Se dico “hey gugu, quanto fa 7 per 8?” o se chiedo quando è nato Napoleone, la risposta dovrebbe essere una, e le sorgenti non sono un problema. Molto diverso sarebbe se chiedessi ad esempio “come si è originato il COVID-19”. Se ci provate oggi, con Google, Bing o Yahoo otterrete una lista di siti. Se provate a dire al vostro telefono “hey gugu come si è originato il COVID-19?” Google risponde citando sì la sorgente (*), ma ovviamente senza darvi possibilità di scegliere.

Già il fatto che sia il motore di ricerca a selezionare la sorgente è quanto meno opinabile. Ma se questi sistemi evolvendo arrivassero al punto di poter rispondere verbalmente, corriamo il rischio di ricevere risposte apparentemente plausibili ma prese da sorgenti inaffidabili, o deliberatamente false.
Molti conosceranno il termine SEO (Search Engine Optimization). Si riferisce all’arte oscura di scrivere contenuti (e metadati) in modo tale da rendere più probabile la comparsa di una pagina per gli utenti che sono alla ricerca di un concetto, di una specifica informazione. In sostanza, se faccio “bene” la pagina aumento le probabilità che quella pagina sia scelta come risultato di una determinata ricerca. Il problema è proprio il “se faccio bene”. Qui non si intende se diciamo la verità, se siamo onesti. Anzi, è quasi il contrario: dobbiamo convincere il motore di ricerca che il nostro contenuto è quello più rilevante per un certo argomento. Quindi il rischio è che il motore finisca per dare più importanza a contenuti che si “vendono meglio” piuttosto che a quelli più autorevoli. E chi ci tiene a vendersi bene più di chi cerca di manipolare il motore di ricerca, per manipolare l’opinione pubblica?

In conclusione, il motore di ricerca troppo intelligente rischia di offuscarci la mente, ridurre la nostra capacità critica, e soprattutto renderci più vulnerabili a condizionamenti voluti da altri e ottenuti diffondendo notizie false o fuorvianti e ingannando i motori di ricerca.

La soluzione? Come dice Il MIT Technology review, forse il linguaggio naturale nei motori di ricerca non è poi un gran progresso. Più in generale occorre rendersi conto dello strapotere esercitato dal motore di ricerca che, senza averlo cercato, è finito per mettersi in mezzo tra noi e tutto internet (**).
Quindi dobbiamo imparare a dipendere meno da gugu, dobbiamo insegnare alle nuove generazioni che quello che trovo in rete non necessariamente è vero, e soprattutto insegnare come cercare e a giudicare le risposte (***).

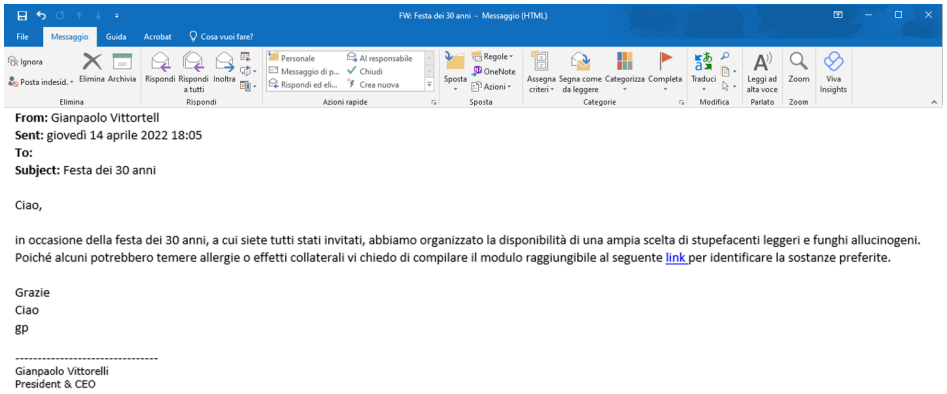
** Stranamente il comportamento cambia se si fa la domanda in inglese o in italiano. In inglese risponde parlando delle origini, e la sorgente è Wikipedia, in italiano si mette a parlare della trasmissione (che non era la domanda) e la sorgente è il ministero della salute. Inoltre le risposte in italiano cambiano se si chiede “come si è originato” piuttosto che “quali sono le origini”.*

*** Sull’esagerato uso del motore di ricerca ci sarebbe molto da dire. Noi abbiamo una collega che piuttosto che salvare una URL nei preferiti (quella del Microsoft Partner Center), fa una ricerca su Google tutte le volte, il che succede diverse volte al giorno, “perché faccio prima”.*

**** Sappiamo di un docente della facoltà di storia di Mc Gill (Montreal) che ha scritto un articolo falsissimo su Wikipedia, e subito assegnato ai suoi studenti una ricerca su quello stesso argomento, per poi chiarire a quelli che ci erano cascati copiando da Wikipedia che 1: le sorgenti sono importanti, 2: Wikipedia non è una sorgente affidabile 3: non si copia…*

GLI STUPEFACENTI

MAI FIDARSI DELLE APPARENZE



From: Gianpaolo Vittortell
Sent: giovedì 14 aprile 2022 18:05
To:
Subject: Festa dei 30 anni

Ciao,

in occasione della festa dei 30 anni, a cui siete tutti stati invitati, abbiamo organizzato la disponibilità di una ampia scelta di stupefacenti leggeri e funghi allucinogeni.
Poiché alcuni potrebbero temere allergie o effetti collaterali vi chiedo di compilare il modulo raggiungibile al seguente link per identificare la sostanze preferite.

Grazie
Ciao
gp

Gianpaolo Vittorelli
President & CEO

Questo il testo dell'inverosimile messaggio di phishing inviato da un sedicente AD a tutti i dipendenti di Microsys qualche settimana fa. Si trattava di una campagna di phishing, come quella di cui abbiamo parlato in precedenza: Il pollo di coccio.

Inverosimile?
Nemmeno tanto, almeno in base alle statistiche:
- Messaggi Inviati: 110
- Cliccato il link: 31
- Completato il download e abilitato le modifiche nel documento Word:13

Evidentemente molti l'hanno preso per vero.

Molti dei destinatari hanno però espresso dubbi sulla correttezza dell'operazione, obiettando che una vera campagna di phishing non avrebbe dovuto essere fatta con un messaggio come quello.

Prima di approfondire vogliamo però fare una distinzione tra phishing, l'invio massivo di un messaggio mail ingannevole, nella speranza che qualcuno ci caschi e che cascandoci riveli informazioni "rivendibili", e spear phishing, che è la stessa cosa, ma fatta verso un individuo specifico, usando un messaggio costruito ad arte per quel destinatario, sulla base di informazioni carpite ad altri o ricostruite ad esempio dai social.
Per una discussione su questo si può ad esempio riferirsi qui: What is Spear Phishing? Definition, Risks and More.

Il messaggio sopra va visto come un esempio di spear phishing, e l'elevato numero di persone che non l'hanno riconosciuto va visto proprio come indicazione della pericolosità di questo tipo di attacco. Che per l'hacker è molto più oneroso, perché deve documentarsi per creare un messaggio fatto a dovere, ma molto più pericoloso per la vittima.

Vediamo quindi le critiche mosse al messaggio:
- Mancava il banner "Mittente esterno" che in Microsys è presente in tutti i messaggi provenienti da mittenti esterni all'organizzazione: vero, ma una delle cose che possono succedere è che l'hacker entri nella mail di un collega e da lí mandi una mail alla vittima. Quindi l'assenza del banner non è garanzia di nulla.
- Era ovviamente riferito ad un evento reale (la festa effettivamente è programmata), mentre un estraneo non avrebbe parlato di una cosa così specifica: anche in questo caso, si tratta di spear phishing. Quindi è assolutamente possibile (anzi quasi sicuro) che l'argomento del messaggio abbia senso per il destinatario e che si parli di qualcosa che in qualche modo gli è familiare.
- Il tono, nel suo essere ironico o scherzoso, poteva certamente essere stata scritta dal vero AD: copiare lo stile di qualcuno può non essere facile, ma sappiamo di casi dove un messaggio di spear phishing riproduceva accuratamente lo stile del presunto mittente. Probabilmente l'hacker aveva acceduto a quella mailbox e usato la posta inviata per costruire un messaggio verosimile.

In compenso:
- Il nome del mittente era una storpiatura del vero AD: questo in generale non succederà. Tutto sommato un hacker come si deve non dovrebbe commettere errori di questo tipo. Ma potrebbe essere un modo per sfuggire alle protezioni dell'anti-malware.
- Il dominio mail del mittente era "@msis.it" mentre Microsys ha "@msys.it": questa è una tecnica utilizzata di frequente se l'hacker manda il messaggio dall'esterno, ed è quasi una scelta obbligata

per evitare che le protezioni identifichino il messaggio come malevolo. Ed è anche un indicatore sicuro del fatto che si tratta di un messaggio malevolo.
- Il link mandava a un sito che non era SharePoint ma www.sharepointin.com: e questo è il punto focale. Alla fine della fiera i messaggi di phishing hanno un solo scopo, spingere la vittima a seguire un link dove in qualche modo riveleranno informazioni importanti. E per farlo l'unico modo è di presentare un link balordo, che punta a un sito con un nome il più possibile simile a quello corretto.

Relativamente alla questione del banner mancante, ma in generale per tutte le misure di sicurezza, in tutti gli ambiti, è importante non presumere mai che una misura di sicurezza funzioni e quindi di poter abbassare la guardia, perché tanto c'è quella. Come se l'avere la cintura di sicurezza giustificasse l'uso del telefonino mentre si guida. Il banner serve ad attirare l'attenzione, ma la sua assenza non garantisce nulla.

Tornando alle mail di phishing, o a quelle di spear phishing, quale sarebbe una difesa efficace?
Come dicevamo nell'articolo sui polli, non è possibile basarsi sul buon senso e sperare di indentificare i messaggi falsi, perché prima o poi ne capiterà uno fatto abbastanza bene da passare i nostri controlli.
E poi c'è il problema della muscle memory, l'azione automatica, il dito che fa click prima che il cervello (se acceso) faccia in tempo a elaborare. Almeno due dei 31 cliccatori seriali hanno detto di aver seguito il link mentre facevano altro, uno in conf call, l'altro in piedi in treno, senza nemmeno pensare a quello che facevano.
Quindi serve una regola semplice: non si seguono i link nelle mail.

Alla quale dovremmo comunque consentire eccezioni, ammesse solo quando strettamente necessario e solo dopo aver attentamente esaminato la destinazione del collegamento. Il che è un po' il contrario di quello che abbiamo appena detto.
E tanto per peggiorare la cosa: sono anni che diciamo di non inviare copie di documenti nelle mail, ma di condividerli, come dire "salvali e manda un link", che quindi i colleghi devono poter seguire.
E poi ci sono le applicazioni, ad esempio i workflow approvativi, che inviano mail agli utenti che contengono link specifici.

Per questo in realtà non possiamo dare una regola integralista "non seguire MAI i link nelle mail", probabilmente ci bloccherebbe troppa roba.

E allora?

Per gli utenti collegati alla rete interna e per i documenti condivisi su una piattaforma con Single Sign On (come Office 365, SharePoint online, Onedrive), supponendo che tutto sia fatto come si deve, il sistema non chiede quasi mai la password, perché la sessione è già autenticata. Lo stesso può valere per le applicazioni interne, se esposte con il Web Application Proxy e se abilitate alla autenticazione Kerberos. Quindi il campanello di allarme deve scattare se dopo aver seguito un link ci vediamo chiedere una password.

In conclusione, se usiamo Office 365 e abbiamo tutto configurato per bene, possiamo dire:
Non seguire mai i link nelle mail, ma se devi controlla bene il link prima di fare click. Poi, se quando fai click ti vedi chiedere una password, spegni istantaneamente il pc, fai scattare l'allarme antincendio, scendi in strada, togli la corrente al palazzo, grida "al lupo!". E spera di cavartela.

UN FATTO TRISTE

LA GENTE SENZA SCRUPOLI HA VITA TROPPO FACILE?

Qualche mese fa, un giovane si è tolto la vita, in America.
Aveva 17 anni, andava al liceo. E fino all'ultimo non aveva motivi per un gesto simile. Poi è stato contattato da una coetanea, che gli ha mandato qualche foto intima. E gli ha chiesto di fare lo stesso. E lui l'ha fatto.

Solo che la coetanea non era quello che diceva di essere. Era un'organizzazione di ricattatori che gli ha estorto i pochi soldi che aveva messo da parte per l'università, altrimenti avrebbero pubblicato le sue foto. E poi, a furia di minacce, l'ha spinto al suicidio.

L'FBI dice che episodi come questo sono sempre più frequenti, che raramente vengono denunciati e che le vittime tipicamente sono giovani, a nostro parere forse un po' troppo abituati a contatti "social" con interlocutori mai visti in carne e ossa.

Chiaramente qui la tragedia è nella morte del giovane. Ma noi, come informatici, ci chiediamo se questo sempre più frequente uso delinquente della tecnologia possa essere limitato o evitato.
È chiaro che i colpevoli in questo caso sono i ricattatori. Pensare che in qualche modo internet in generale abbia una responsabilità sarebbe come dire che le strade sono in parte responsabili delle rapine, perché i rapinatori le usano per compiere il misfatto.
Ma la cultura del "su internet l'anonimato è sacro" insieme con una certa superficialità dei social sono sicuramente parte del problema.
Ci chiediamo: perché è così facile fare account falsi sui social?
E perché moltissimi account Twitter non dicono apertamente a chi appartengono, ma si nascondono dietro acronimi oscuri?
E poi, com'è che il 5% degli account Twitter sono falsi (ed Elon Musk dice che sono più di così), e nessuno nemmeno alza un sopracciglio?
E perché non è reato il consentire a qualcuno di fingere di essere qualcun altro in un social?

Evidentemente la risposta, forse superficiale, è che è troppo difficile verificare in modo serio, in remoto, l'identità di una persona che non puoi vedere e che necessariamente deve poter essere profilata automaticamente.

Però facciamo qualcosa di sicuramente più efficace ad esempio nel rilascio dei certificati SSL (quelli che servono per certificare l'identità di un sito), per non parlare dei meccanismi come lo SPID (Sistema Pubblico di Identità Digitale). E se lo può fare la Pubblica Amministrazione, allora lo possono fare pure i social.
Quindi perché non dire che i social, se non devono imporre un'identificazione certa della persona, almeno possono consigliarla e soprattutto possono evidenziare che una certa identità non è in realtà certificata?
Facebook e Twitter potrebbero ad esempio mettere una barra verde da qualche parte se l'identità è certa, e rossa se non lo è.
E i genitori potrebbero ad esempio bloccare ai figli ogni comunicazione con identità non certe, o almeno educarli in questo senso.
Certo, non sarebbe perfetto. Ma almeno staremmo facendo qualcosa, perché a noi pare che non si faccia assolutamente nulla. Continuiamo a dire che bisogna essere cauti, che non si devono accettare caramelle (virtuali) da estranei (virtuali), che non si devono seguire i link nelle mail, ecc. Insomma, continuiamo a scaricare la responsabilità sull'utente.
Ma non potremmo invece mettere un po' più di pressione su quelli che di fatto sono gli abilitatori di certi comportamenti? A partire dai social, con cui si guadagnano un sacco di soldi, e che noi pensiamo sarebbe il caso di responsabilizzare un poco di più.

Dicono che le ultime generazioni, quelle nate con i social, li usino quasi come l'unico mezzo per comunicare con i coetanei. Così mettiamo nelle mani di questi media un potere enorme, che aumenta ogni giorno. È assolutamente necessario regolamentarli e responsabilizzarli, prima che sia troppo tardi e che finiscano nelle mani delle persone sbagliate (sempre che non sia già troppo tardi).

E noi, utenti comuni, genitori, nonni, figli o amici: possiamo fare qualcosa?
Probabilmente serve poco, ma possiamo parlarne. Chissà mai che un giorno un qualche "influencer" si renda utile e influisca...

LA FANTASIA DEL LADRO

NELLA LOTTA TRA GUARDIE E LADRI, L'IDENTITÀ È UN PO' UN VASO DI COCCIO

Dicevamo, da quando hanno capito che si può usare "la rete" per rubare soldi veri, molti ladri devono essersi laureati in informatica. O forse è successo il contrario, molti informatici hanno preso la via del crimine.
Non importa, il fatto è che ogni giorno che passa qualcuno trova un nuovo modo per entrare da qualche parte (in senso informatico) e rubare. Soldi veri, non informazioni.

L'ultima trovata, da non sottovalutare, è di entrare in Azure (o Amazon Aws o Google Cloud), con un account carpito ad un amministratore. Ma non toccare quello che già c'è. Quello che fanno è usare quel cloud per creare macchine virtuali il più potenti possibile e usarle per fare crypto mining (*). Il conto chiaramente arriva al proprietario dello spazio cloud in questione, mentre gli eventuali bitcoin guadagnati se li tiene il ladro.

Molti forse pensavano che tutto sommato non fosse importante proteggere le credenziali di un ambiente cloud che non contenesse qualcosa di importante, ad esempio un ambiente di laboratorio, senza dati aziendali e senza applicazioni di produzione. Beh, dobbiamo ripensarci. Anche un ambiente vuoto o quasi, contiene qualcosa che ci possono rubare. E attenzione: non è detto che si tratti di pochi euro, anzi è sicuramente vero il contrario.

Cosa fare?
In generale la prima cosa da fare è ridurre la possibilità che un male intenzionato si appropri di credenziali amministrative. E se succedesse mettere in piedi strumenti per accorgersi e limitare i danni. Quindi:

1. Usare sempre mfa (autenticazione a più fattori).
2. Proteggere le identità con qualcosa come Identity Protection, e dare sempre seguito ad eventuali allarmi (sembra scontato, ma non lo è: serve un processo!).
3. Utilizzare conditional access, che permette di imporre condizioni specifiche per l'accesso di account "potenti", come ad esempio che arrivino da indirizzi ip predefiniti, o che non siano stati precedentemente oggetto di tentativi di accesso "strani".
4. Usare PIM (Privileged Identity Management) in modo da poter attivare un processo approvativo per l'attivazione e l'uso di credenziali privilegiate.
5. Ridurre il numero di account amministrativi.
6. Configurare uno o più budget di spesa con allarmi al superamento del budget.

Poi in generale si dovrebbe evitare di dare ruoli più ampi del necessario. E su questo tema occorre correggere una percezione: si limitano i diritti al minimo indispensabile non perché non ci si fidi di una persona, ma per limitare i rischi connessi alla possibilità che le credenziali di questa persona vengano compromesse. E siccome potrebbe anche capitare che la responsabilità di una azione malevola venga attribuita al proprietario dell'account, il limite è una protezione anche per lui.

Alla fine, la protezione delle identità è la cosa più importante. I firewall, le vpn, le password complesse, la DPI (deep packet inspection) ecc. nulla possono fare di fronte a un utente che dispone delle credenziali di accesso ed esegue operazioni legittime, come creare delle macchine virtuali.

Vale la pena di investire tempo e denaro nel proteggere le identità, perché siamo solo agli inizi...

** Crypto mining è un'attività che richiede elevate risorse informatiche (si tratta di risolvere un "problema") e che, quando produce un risultato, fa guadagnare bitcoin a chi ha trovato la soluzione.*
Analogamente a quanto succede ad esempio in una miniera di diamanti, dove devo scavare e setacciare una tonnellata di terra per trovare un grammo di diamanti, qui devo lavorare un sacco con una cpu per guadagnare un bitcoin. E analogamente a quanto capita con i diamanti, il valore di quello che trovo non ha alcuna relazione con la fatica che si fa a trovarlo, e nemmeno con il valore intrinseco di ciò che ho trovato. Il valore dipende solo da quanto gli altri desiderano avere quella pietra, o un bitcoin.
Avete l'impressione di non avere capito perché sembra non avere senso? Non è vero, avete capito. Solo che non ha senso.
Morale: trovare bitcoin costa caro, in corrente elettrica e in risorse informatiche. O non costa nulla se rubo le risorse con cui cercarlo.
E poi, per non perdere occasione di fare polemica, i diamanti, o l'oro, oltre a un valore estetico hanno anche un valore (non trascurabile) nell'industria. I Bitcoin invece non solo non servono a nulla, ma non sono nemmeno belli...

THE “ART” OF COMPUTER PROGRAMMING?

CONSIDERAZIONI SU ARTE E COMPUTER

Tempo fa i giornali ci hanno parlato di un ricercatore di Google (tal Blake Lemoine) che a un certo punto ha affermato pubblicamente che l’intelligenza artificiale su cui lavorava era “senziente”. Ammettiamo di aver dovuto cercare nel dizionario (ovvero appunto su Google) il significato di quella parola, che non avevamo mai sentito o usato, e che non abbiamo mai più avuto occasione di adoperare. Google dice che significa “dotato di sensi, di sensibilità”. Boh, non sappiamo bene come un programma (perché questo è un’intelligenza artificiale, è un programma molto complesso, con tanti dati) possa “sentire”. Ma tutto sommato tutto dipende dal significato che vogliamo dare alla parola “sentire”.

Recentemente ci è capitato di leggere un titolo, solo quello, di un articolo del MIT Tech Review che si chiedeva “di chi è l’arte prodotta da un computer?”. Ora, a noi pare che la questione non sia specifica dell’arte. La domanda “di chi è l’output di un computer” dovrebbe avere una solo risposta, indipendente dalla natura dell’output. Non che sia ovvia, beninteso.
Quello che ci ha colpito non è il dilemma sulla proprietà. Ma il fatto che si possa considerare “arte” l’output di un computer.
Ci è parso immediatamente evidente che la risposta debba essere negativa. No, un computer non può produrre arte. Ma poi ci siamo resi conto che in realtà non sapevamo perché no.

Abbiamo provato a cercare una definizione di arte. Ne abbiamo trovate numerose, spesso in contrasto tra loro. Da cui deduciamo che non esiste una definizione condivisa di arte. Il che è una delle definizioni che abbiamo trovato.

Ma molte avevano una cosa in comune, l’idea che si tratti di qualcosa fatto dall’uomo. Anche se nessuna giustificava questo vincolo. Ad esempio, è corretto dire che un fiore non è arte? O che un cielo stellato non lo è? A nostro parere sì, perché arte non è sinonimo di bello. E dire che il Creato sia arte suona un tantino presuntuoso.

E il computer? O l’intelligenza artificiale? Avete notato come spesso ci si riferisce alla IA (AI per gli anglofissati) come fosse una persona? Ora, la IA non è una persona e non è senziente. Anzi, è il contrario di senziente perché è deterministica (*).

E questa secondo noi è la distinzione: chiedete due volte ad un artista di fare la stessa cosa e farà due cose diverse, magari simili, ma diverse. E le differenze potrebbero, tra le altre cose, essere dovute allo stato d’animo dell’artista quando ha fatto quello che ha fatto. Date a un computer due volte gli stessi input e otterrete esattamente lo stesso risultato. Perché un computer non ha uno “stato d’animo”.
Quindi per noi un computer non può produrre arte, perché l’arte è l’espressione del sentimento di un artista.

Il che non impedisce che un computer possa produrre qualcosa di bello.

** Deterministico: secondo la Treccani - “Effetto d.: effetto che proviene in modo univoco e quantitativamente definibile da cause chiaramente individuate”: Quindi date certe cause si ottiene uno specifico effetto, sempre. In effetti molti utenti di Windows potrebbero obiettare sulla affermazione che il pc con Windows sia deterministico, ma noi rimarremo fermamente convinti che lo sia.*

CASI DI BUSINESS

30_ Erion

30_ Gewiss

31_ Giacomini

31_ Rina

ERION

Erion, nasce nel 2020 dall'unione di Ecodom e Remedia, due Consorzi già esistenti nel settore della Raccolta di Rifiuti di Apparecchiature elettriche ed elettroniche (RAEE). La creazione di questa nuova realtà ha comportato un considerevole aumento nella mole di dati gestiti dall'azienda. Da qui, la necessità di introdurre nell'infrastruttura tecnologica aziendale una soluzione di Business Intelligence (BI), in grado di semplificare il monitoraggio delle attività e supportare i processi decisionali in diverse aree di business. Nella prima fase del progetto, sono state mappate le esigenze attraverso incontri specifici con stakeholder interni ed esterni al Consorzio.
L'introduzione della piattaforma di Business Intelligence ha portato benefici sensibili valutati sempre nell'ottica della soddisfazione dei Consorziati e dei Gestori dei Centri di Raccolta che costituiscono i principali beneficiari del servizio: ha permesso un miglior controllo della gestione operativa per prendere le decisioni aziendali in ottica predittiva.
Per il monitoraggio del budget è stata predisposta una reportistica aggregata del complesso insieme di costi e ricavi legati alle attività operative.

GEWISS

Gewiss S.p.A., società italiana del settore elettrotecnico, per favorire la mobilità e la flessibilità che si è consolidata negli ultimi anni, avvia il progetto di Comunicazione Unificata, che comprende l'integrazione tra la piattaforma di Microsoft Teams e la telefonia tradizionale.
Il progetto è iniziato in alcune sedi più piccole di Gewiss per poi estendersi a tutta l'azienda. Il dipartimento IT ha guidato l'adozione aziendale, sponsorizzata dai vertici della società stessa, consapevole dell'impatto che avrebbe portato una importante evoluzione sulla modalità di comunicazione e collaborazione aziendale su ogni singolo utente.
Entro aprile 2021 tutta la GEWISS ITALIA è stata migrata alla nuova soluzione UC (Comunicazione Unificata).
Uno dei principali vantaggi offerti dalla nuova soluzione è la grande semplificazione della gestione delle telefonate, che possono oggi essere ricevute in modo diretto dai singoli interessati, aumentando così la reperibilità delle persone. La soluzione, inoltre, si sposa bene con la domanda di flessibilità comunicativa degli utenti, che negli ultimi anni hanno aumentato moltissimo il ricorso a nuove modalità, pensiamo ad esempio alla videoconferenza, avendone compresi i vantaggi.

GIACOMINI

Giacomini S.p.A., Gruppo italiano che produce componenti per l'impiantistica idraulica, con lo scoppio della pandemia introduce lo Smart Working per parte dei lavoratori impiegati nella Ricerca e Sviluppo, nell'Amministrazione e nella forza vendite. Per supportare tutto ciò, l'azienda avvia la migrazione delle proprie utenze Microsoft in Cloud e sceglie la soluzione VDI (Virtual Desktop Infrastructure) di Azure per consentire alle persone non dotate di un PC aziendale di lavorare da casa utilizzando strumenti propri, in logica BYOD (Bring Your Own Device). Il Gruppo fa ampio utilizzo di Microsoft Teams che sta diventando il punto di riferimento per la gestione dei progetti e delle attività lavorative. Per rendere efficienteil processo di scambio di materiale e di documenti anche con i fornitori e le filiali presenti all'estero, Giacomini si sta affidando sempre più a SharePoint.
Giacomini ha modernizzato l'infrastruttura IT e ha svoltoun'attività per la messa in sicurezza e il monitoraggio continuo dei propri server e dei client, per la protezione avanzata dei dispositivi e della posta elettronica e per l'identificazione delle minacce sulle identità.

RINA

RINA, multinazionale di ispezione, certificazione e consulenza ingegneristica, per affrontare le conseguenze della pandemia Covid-19 decide di dotarsi di una piattaforma di eLearning a supporto delle attività della BU dedicata ai servizi di certificazione. L'obiettivo del progetto è stato inizialmente quello di garantire la continuità del business, passando rapidamente dalle fruizioni dei corsi in presenza all'erogazione online di un calendario molto ricco di corsi prenotati da differenti città italiane edestere. La scelta della soluzione LMS365 integrata a Office 365 e SharePoint, ha permesso una rapida fruizione in formato digitale dei corsi e la riorganizzazione e distribuzione attraverso una piattaforma intuitiva e di facile utilizzo sia per i docenti che per i partecipanti.
Il primo corso è stato erogato dopo 4 giorni dall'inizio del progetto: un vero successo. Lo staff ha imparato velocemente a caricare ed erogare corsi in videoconferenza e la piattaforma è risultata così efficace da ricevere subito l'apprezzamento interno su aspetti come sicurezza e privacy. Poiché RINA è presente in 3 diversi continenti, è stata apprezzata la scalabilità della soluzione, la possibilità di avere corsi multilingua, multialfabeto ed erogabili nei diversi fusi orari.

LE SOLUZIONI

34_ Modern Phone System 365

34_ Arxbc 365

35_ Keys Of The Kingdom 365

MODERN PHONE SYSTEM 365

Modern Phone System 365 è la soluzione, basata su Microsoft Teams, che garantisce l'adozione di un nuovo ambiente di lavoro con tutte le funzionalità per la collaborazione aziendale avanzata integrate con il centralino telefonico in Cloud.

Perché scegliere **Modern Phone System 365?**

- Migliora la produttività integrando il telefono con Microsoft Teams
- Facilita la comunicazione e la collaborazione
- Estende la comunicazione al di fuori dell'azienda
- Sei raggiungibile telefonicamente sempre e dovunque

KEYS OF THE KINGDOM 365

Keys of the Kingdom 365 è la soluzione basata sul modello ESAE di Microsoft per introdurre policy e configurazioni per gestire gli accessi delle credenziali privilegiate ai device (server e workstation) in Active Directory.

Perché scegliere Keys of the **Kingdom 365?**

- Riduzione della probabilità di successo delle tecniche di attacco definite da MITRE come Privilege Escalation e Lateral Movement.
- Introduzione di una nuova struttura di unità organizzative, gruppi e delegazioni.
- Gestione degli accessi privilegiati (PAM) basata su Azure Bastion e Azure Virtual Desktop o Azure WM come Privileged Access Workstation (PAW)

ARXBC 365

ArxBc365 è un briefing interattivo per la valutazione dell'integrazione di Microsoft Dynamics Business Central con Arxivar Next per estenderne le funzionalità con una moderna gestione documentale al fine di organizzare in modo semplice ed efficiente tutti i documenti.
Per le aziende italiane questa soluzione prevede una completa integrazione con il Sistema Fiscale di fatturazione elettronica e con l'archiviazione documentale a norma di legge.

Perché scegliere **ArxBC 365**?

- Identificare i documenti chiave nell'organizzazione
- Selezionare le proprietà principali per il documento che verrà utilizzato come ricerca chiave
- Determinare i flussi di lavoro che si prevede di implementare nella procedura di archiviazione
- Presentazione dell'integrazione per la Fatturazione Elettronica

TUTTE LE SOLUZIONI

CYBER DEFENSE 365

Cyber Defense 365, una suite di servizi per semplificare la protezione del sistema informativo aziendale, attraverso misure preventive costantemente verificate, riverificate ed aggiornate per minimizzare la superficie d'attacco.

DATA INTEGRATION FRAMEWORK 365

Data Integration Framework 365 è la soluzione che fornisce strumenti e funzionalità per facilitare l'integrazione e la comunicazione tra le piattaforme applicative presenti in azienda; aumenta la produttività e riduce l'impegno per lo sviluppo di nuove possibilità di integrazione a beneficio della standardizzazione dei sistemi applicativi.

LEARNING 365

Learning 365 è la soluzione di Microsys, basata sul prodotto SaaS LMS 365, per organizzare percorsi e attività di informazione e formazione online (e-learning). Grazie alla tecnologia di Microsoft.
Learning 365 offre la possibilità di pianificare la partecipazione alle attività proposte a partire dalle esigenze degli studenti, senza tralasciare gli aspetti di networking e collaborazione.

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 utenti di accedere in mobilità al proprio ambiente di lavoro.

LE NOSTRE APP

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, permette il ricevimento dei documenti passivi. Con una sinergia perfetta con la soluzione SDI 365 può essere gestita anche la fatturazione elettronica attiva.

DOC FINANCE 365

DocFinance 365, la soluzione di integrazione con il software DocFinance 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.

DOC TEMPLATE 365

Doc Template 365 è la soluzione Microsys per i documenti commerciali, un layout pulito, efficace ed estendibile, condiviso per tutti i documenti in uscita così da 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.

EXTRACONTABILE 365

Extracontabile 365, una soluzione completa e semplice per la contabilità analitica, è lo strumento proposto da Microsys per un efficace controllo di gestione oltre che per ratei e risconti. La soluzione integra inoltre le funzionalità per la generazione delle fatture da emettere e da ricevere.

SDI 365

SDI 365, l'estensione per l'estrazione delle fatture elettroniche, 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.

30 ANNI

40_ L’intervista

42_ L’evento

L'INTERVISTA

MAGGIO 2022
*INTERVISTA A **GIANPAOLO VITTORELLI**,*
AMMINISTRATORE DELEGATO, MICROSYS

Come nasce Microsys?

"Siamo partiti dal niente, ma questa è stata, per molti versi, la nostra fortuna. Alessandra collaborava con un'azienda che si occupava di soluzioni per IBM AS/400, mentre io ero un libero professionista. Avevo un'esperienza abbastanza unica sul mercato, perché avevo approfondito più di altri il tema dell'integrazione tra i Pc (che allora muovevano i primi passi) e il mainframe. Inoltre, Alessandra aveva una innegabile capacità di vendere il mio know-how ai suoi clienti. Insieme percepiamo le potenzialità di una sempre maggiore interoperabilità tra computer da scrivania e macchine centrali e, come si dice in questi casi, ci trovano al posto giusto nel momento giusto. Così, nel 1992 nasce Microsys, destinata, almeno nella prima fase della sua storia, ad accompagnare le aziende nella delicata transizione da mainframe ad architetture più agili. Per molti anni, abbiamo goduto di un innegabile vantaggio competitivo. Non solo avevamo le conoscenze e gli strumenti (lavoravamo ad esempio con un'azienda americana che sviluppava un software che permetteva di connettere Pc e mainframe), ma eravamo in grado di superare le convenzioni e la pessima comunicazione che veniva fatta in quegli anni sull'utilizzo delle nuove architetture".

Con l'avvento delle nuove architetture Cloud. Come cambia Microsys?

"Con l'avvento delle architetture cloud, Microsys diventa il partner ideale per "smontare" le architetture Pc/server, che nel frattempo avevano definitivamente sostituito i minicomputer e i mainframe, e portarle sulle nuvole. Una fase completamente nuova per noi, ma non sarà l'ultima. Penso che l'attuale tendenza ad andare in cloud subirà un rallentamento quando gli utenti si accorgeranno che la concentrazione dei dati in pochi data center e pochi fornitori non è la soluzione ideale. Mi aspetto prima o poi un ritorno della capacità computazionale e dello storage sulle scrivanie. Le mode cambiano e noi saremo pronti ad accompagnare i clienti anche in questo nuovo ciclo".

Microsys è una azienda che ha vissuto direttamente le evoluzioni tecnologiche. Quale sono i valori e la strategia adottata per supportare al meglio i clienti?

"Microsys è da sempre un'azienda fatta soprattutto di persone e di competenze. Non è tanto una scelta strategica, ma la volontà di dare più importanza al know-how che alla capacità di vendere. Ci sentiamo molto più consulenti che rivenditori di prodotti, ed è proprio per questo che sin dall'inizio abbiamo preferito lavorare con un solo vendor, cioè Microsoft.

Il fatto di essere mono-vendor è per Microsys un segno distintivo ma anche una garanzia, nei confronti dei clienti, che l'enfasi non è tanto sulla fornitura della soluzione più conveniente (per chi vende), ma sulla soluzione di un problema. La trasparenza per noi è fondamentale, il nostro cliente non penserà mai che stiamo cercando di piazzare una soluzione piuttosto che un'altra, ma si concentrerà insieme a noi sul progetto. Insomma, nel nostro essere cattivi venditori, siamo gente che parla chiaro e che va dritta al punto, conoscendo vita, morte e miracoli dei prodotti e non abdicando mai al nostro ruolo consulenziale nei confronti dei clienti, anche a costo di non appiattirci sui loro desiderata se non li riteniamo coerenti con l'obiettivo da raggiungere".

Se le chiedo di riassumere in poche parole Microsys?

Microsys è una società che oggi conta cento dipendenti abituati a sentirsi una famiglia e a lavorare con i clienti vestendo i panni del consulente più che del commerciale. Questa è Microsys, un'azienda che ha attraversato con coerenza 30 anni di storia dell'informatica tenendo la barra dritta su due direzioni parallele: trasparenza e competenza.

L'intervista è stata realizzata in occasione della stesura dell'artico "DAL FLOPPY AL CLOUD, LA FEDELTA' PAGA", pubblicato sul n°52 della rivista Technopolis.

Da 30 anni manteniamo la rotta. Attenti, concreti e appassionati

L'EVENTO

25 MAGGIO 2022
***TERRAZZA MARTINI**, MILANO*

Per festeggiare i nostri primi 30 anni, abbiamo deciso di organizzare una tavola rotonda intitolata "Dal mainframe alle nuvole, ma quanto siamo cambiati?" moderata da Emilio Mango, Direttore Responsabile, Technopolis e IctBusiness.

Tutto è nato dall'idea di parlare dell'evoluzione della tecnologia informatica senza parlare direttamente della tecnologia, ma dei cambiamenti che ha indotto e che ha consentito per la vita delle persone e delle aziende.

Abbiamo discusso infatti di come la tecnologia può supportare il business anche in condizioni di mercato sfavorevoli, di come può aiutare a far crescere un'azienda partendo da zero e di come può cambiare le relazioni tra colleghi e più in generale il modo in cui le persone comunicano.

Invitati ad Intervenire:

Alessandra Galdabini
2IC, Microsys

Alessandro Belloli
Direttore Generale, Avvenire

Annamaria Bottero
Direttore Divisione Customer Experience & Success, Microsoft Italia

Fabio Santini,
Direttore Divisione Global Partner Solutions, Microsoft Italia

Giovanna Salza,
Founder & CEO, Ca' Zampa

Michele Mariella,
Chief Information Officer, Maire Tecnimont

L'evento si è concluso con un Networking Cocktail, una splendida occasione per rivedere alcune delle persone che ci hanno accompagnato in questi 30 anni e alcune di quelle che, speriamo, ci accompagneranno per i prossimi 30.

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