Luiss Business School

GENNAIO 2022

Il Sole 24 ORE Radiocor

DigitEconomy.24 – CYBERSECURITY AL CENTRO DEGLI INTERESSI

L'INTERVISTA ALL'AMMINISTRATORE DELEGATO DELLA SOCIETÀ

«Santagata (Telsy): «Pronti a una campagna di M&A, guardiamo a società di diritto italiano»

Crescita organica e inorganica, acquisizioni allo studio, preferibilmente in Italia, raddoppio dell'occupazione nei prossimi anni, nuovi servizi. Si apre un 2022 sfidante per Telsy, azienda della cybersicurezza su cui il governo può esercitare il golden power, dal 2000 dentro il gruppo Tim, guidata da Eugenio Santagata, ex ceo di Cy4gate. «L'assetto di Telsy – racconta Santagata a DigitEconomy.24, report del Sole 24 Ore e della Luiss Business School società già strategica di per sé, può avere una crescita fortissima. Siamo riusciti a registrare un incremento del 45% in volume nel 2021 e una crescita importante sia in valore

↑ **Eugenio Santagata**, amministratore delegato di Telsy (gruppo Tim)

sia in marginalità. La sfida vera è iniziare il 2022 con una macchina che si può cimentare già in una gara da Formula 1, con tutto ciò che serve». Il contesto offre varie opportunità: il mercato della cybersecurity in Italia, infatti, «vale circa 2 miliardi e, anche se è difficile reperire i dati, visto che ogni giorno un pezzo di economia digitale in più diventa cybersecurity, di anno in anno il tasso di crescita composto va dal 14 al 16%, sia sulla cybersecurity sia sulla criptografia». La cybersecurity «va dunque pensata a monte, non a valle, e Tim l'ha integrata in maniera corretta. Telsy, nell'ambito del gruppo, è in grado di intercettare questo tipo di crescita, in particolare nel prossimo triennio. Peraltro, questa è la mission che il gruppo Tim affida a Telsy e che io

>> *continua a pag. 4*

IL RAPPORTO 2021 DI NTT SUGLI ATTACCHI INFORMATICI

«Il settore finanziario il più colpito, segue la manifattura»

Il settore finanziario è al top della classifica, ma sono sempre più bersaglio degli attacchi informatici anche i comparti del manifatturiero e della sanità. È il quadro che si compone guardando le statistiche del Global Threat Intelligence Report del 2021 realizzato dal gruppo giapponese Ntt. Gli attacchi al comparto finanziario passano dal 17% nel 2018 al 23% nel 2020; il manifatturiero, che era al sesto posto in classifica nel 2018, si piazza al secondo posto nel 2020 con il 22%; la sanità passa dal 7 al 17% dell'anno scorso. «Nel corso degli ultimi anni, gli attacchi informatici - spiega Dolman Aradori, vicepresidente e Head of Security di Ntt Italia - sono aumentati. Ne è cresciuto il numero e soprattutto se ne sono diversificati i target: se pure ancora oggi la finanza è il settore più colpito, nel

Industry	2018	2019	2020
Finance	#1 – 17%	#2 – 15%	#1 – 23%
Manufacturing	#6 – 7%	#5 – 7%	#2 – 22%
Healthcare	#7 – 7%	#6 – 7%	#3 – 17%
Business and professional services	#3 – 12%	#7 – 7%	#4 – 10%
Education	#4 – 11%	#4 – 10%	#5 – 6 %

↑ Percentuale del volume di attacco per settore nel 2018-2019-2020

>> *continua a pag. 3*

IL PUNTO

«Fastweb e Consorzio Italia Cloud avanti nella gara per la Nuvola di Stato»

↑ **Antonio Baldassarra,** ceo di Seeweb e consigliere di Consorzio Italia Cloud

«Fastweb, che è in cordata con Engineering, e il Consorzio Italia Cloud andranno avanti nella gara per la "Nuvola di Stato", nonostante la scelta da parte del governo per il modello presentato da Tim, Cdp, Sogei e Leonardo. «Dopo l'espressione di gradimento per la soluzione tecnologica di Tim, adesso - ha detto l'amministratore delegato di Fastweb, Alberto Calcagno, in occasione della conferenza stampa per aggiornare i target del gruppo - sarà costruito un bando e di nuovo ci sarà la possibilità per tutti, compresa Fastweb, di poter presentare un'offerta. Noi eravamo molto sicuri e ab-

>> *continua a pag. 3*

«Entro il 2022 un'acquisizione nella cybersecurity, su Hwg ci siamo ritirati ma resta interesse»

↑ La sede di Lutech

↑ **Tullio Pirovano,** ad di Lutech

Un'acquisizione nel settore della cybersecurity entro l'anno e un numero significativo e importante di acquisizioni in generale, considerati anche gli altri campi. Sono gli obiettivi di Lutech, gruppo Ict da circa 500 milioni di euro, per il 2022, come spiega l'amministratore delegato Tullio Pirovano a DigitEconomy.24 (report del Sole 24 Ore Radiocor e della Luiss Business School). Nella cybersecurity in particolare, una volta constatato che Hwg, azienda per cui Lutech ha presentato un'offerta, ha fatto altre scelte strategiche, Pirovano conferma comunque l'interesse a collaborare. Confermato anche il target di raggiungere un miliardo di ricavi entro il 2024-25 (obiettivo «impegnativo ma fattibile»), attraverso crescita organica e operazioni straordinarie. Poi c'è l'opzione quotazione: una volta arrivati al miliardo di ricavi, «riteniamo di poter essere un soggetto interessante per gli scambi e attrarre investitori istituzionali importanti».

La cybersecurity è un settore che suscita molto interesse, che ruolo ha all'interno del vostro business?

La cybersecurity è sicuramente una delle aree strategiche su cui Lutech sta puntando con maggiore determinazione. Noi abbiamo un posizionamento storico, con un volume di affari aggregato di circa 40 milioni di euro e un'ampia offerta che va dalla progettazione e realizzazione di soluzioni complesse fino a servizi di consulenza e al Soc (Security operations center) di ultima generazione, un investimento molto importante fatto 3 anni fa e ubicato nella nostra nuova sede. L'obiettivo è quello di essere uno dei principali player nel panorama Ict italiano, crescendo organicamente, ma anche attraverso operazioni di M&A, portando in Lutech nuove competenze e professionalità. In sintesi, siamo alla ricerca di persone e realtà che vogliano condividere con noi un percorso di crescita. E per noi la cybersecurity è un elemento centrale della nostra offerta.

Pensate di chiudere a breve qualche acquisizione nella cybersecurity?

Penso che entro l'anno ne chiuderemo almeno una.

Restate interessati ad Hwg per cui avete presentato un'offerta?

Lutech ha fatto un'offerta molto interessante non solo economica ma anche di progetto, un'offerta, secondo me, unica e distintiva. Ma ci siamo ritirati perché abbiamo capito che Hwg non è più interessata al deal avendo fatto altre scelte strategiche. Con loro stiamo collaborando e continueremo a farlo, non è detto che non ci si incontri nuovamente in futuro.

Farete una divisione ad hoc per la cybersecurity?

Il nostro è un obiettivo di gruppo, avere una società separata, oppure optare per una practice all'interno del gruppo con una propria identità, è una decisione che prenderemo sulla base anche di considerazioni contingenti.

Oltre a quelle nella cybersecurity che tipo di altre acquisizioni state valutando?

Sul fronte delle acquisizioni abbiamo un track record notevole con una macchina di M&A molto collaudata. Ci sono le premesse per mettere in campo nel 2022 un numero significativo, importante di acquisizioni. Per noi si articolano principalmente su due filoni: l'acquiring nei settori dove Lutech è già presente, con l'obiettivo di migliorare il nostro posizionamento in un'area specifica, ad esempio nel mondo dei big data, del cloud, riguardo alle competenze verticali di industry, come nel comparto del manufacturing dove nello scorso novembre abbiamo completato quattro acquisizioni. Proprio nel manufacturing abbiamo una pipeline di operazioni, alcune delle quali si completeranno entro il 2022. Per noi quello dell'acquiring è un modo molto efficace per portare a bordo competenze e acquisire un pool di risorse specializzate che possano trovare in Lutech opportunità di crescita. Un altro filone strategico riguarda le operazioni più significative, di tipo trasformative che permettono di accelerare la crescita. Sono operazioni complesse che richiedono un'analisi più profonda rispetto alle precedenti. Anche su questo fronte stiamo lavorando molto. L'obiettivo principale è in Italia, visto che Lutech vuole diventare uno dei primi operatori Ict nel nostro Paese, ma qualora vi fossero opportunità all'estero che possano permetterci di rafforzare e offrire crescita e sviluppo, le valuteremo. All'estero guardiamo soprattutto operazioni riguardanti aziende il cui sviluppo può essere governato dall'Italia, in modo sinergico.

Quanto all'obiettivo annunciato di raggiungere un miliardo di ricavi entro il 2024 siete sulla buona strada?

Stiamo andando bene, abbiamo un 2021 in linea con i nostri obiettivi. Chiuderemo l'anno scorso, annualizzando le operazioni di acquisizione effettuate, con ricavi vicini ai 500 milioni di euro. Vediamo l'obiettivo del miliardo di ricavi da raggiungere entro il 2024-25 impegnativo ma fattibile.

E poi valuterete la Borsa?

Se ci saranno le condizioni, a quel punto Lutech può essere un soggetto interessante con tutte le carte in regola per aspirare a fare una quotazione importante su un mercato importante. Riteniamo, infatti, che, per poter essere un soggetto interessante per gli scambi e attrarre investitori istituzionali importanti, si debba arrivare intorno a un miliardo di ricavi. ■

«Il nostro Paese ha una capacità di reazione agli attacchi informatici ancora bassa»

↑ **Dolman Aradori**, Vp, responsabile security di Ntt Data Italia

nostro Global Threat Intelligence Report 2021 emerge con chiarezza che anche la sanità e il comparto manifatturiero sono ormai bersagli primari». L'incremento nei settori manifatturiero e sanitario, prosegue il manager, si lega al fatto che le aziende appartenenti a questi settori per lo più non hanno un approccio strutturato alla problematica, mancando di efficaci strutture di controllo e processi di gestione. E soprattutto spesso presentano un parco macchine obsoleto e quindi più esposto a vulnerabilità anche già note da tempo. Si consideri che il tipico meccanismo del ransomware, per esempio, è quello di "attaccare" senza un target specifico e, quindi, aziende che hanno infrastrutture vulnerabili sono quelle più esposte e che più facilmente vengono "bucate". Un altro aspetto da considerare sono le informazioni che trattano: brevetti e proprietà intellettuale nel caso manifatturiero e dati personali per quanto riguarda la sanità.

Le statistiche di Ntt Data si basano su 1.350 interviste online a technology e business decision-maker in grandi organizzazioni in 15 settori e 21 Paesi (in America, Europa, Medio Oriente e Africa, Asia, Australia e Nuova Zelanda), inclusi 1.046 professionisti It e di sicurezza informatica. I dati si riferiscono agli attacchi globali tra il primo gennaio 2020 e il 31 dicembre 2020. «A livello mondo, l'Italia – prosegue Aradori - non è il principale target mentre Usa, India, Giappone e Germania sono tipicamente tra i più colpiti. Il diffondersi di malware aspecifici ha però incrementato il numero di incidenti informatici anche nella nostra nazione». Purtroppo, commenta Aradori, «la capacità di rilevazione e reazione in Italia è ancora bassa, in quanto la piccola e media azienda non può avere internamente la struttura necessaria per fare questo lavoro e il ricorso a fornitori di servizi specialistici di sicurezza gestita sono in questo momento in diffusione. Non si è pensato di lavorare in forma preventiva alla problematica, ma spesso si tende ad agire nel momento in cui si è già subito un attacco o aziende dello stesso settore lo hanno sperimentato».

La causa dell'incremento degli attacchi è da rinvenire nel sempre maggiore utilizzo degli strumenti digitali. Smart working, adozione del cloud, maggiore offerta di servizi digitali, informatizzazione dei processi produttivi hanno incrementato la superficie di attacco e messo in luce vulnerabilità sia tecniche sia organizzative delle aziende, sottolineando come il grado di maturità con cui il tema della cybersecurity è affrontato sia ancora oggi molto diverso in relazione al settore di appartenenza. «Sono sempre di più le imprese che spostano online gran parte dei propri dati e dei propri processi, ma manca il più delle volte – commenta il vicepresidente - un contestuale rafforzamento delle misure di cybersecurity. Le aziende sono ormai mature per la transizione digitale, ma non per la messa in sicurezza di quel che caricano online: è per questo che diventa fondamentale affidarsi a player competenti». Un altro fenomeno, conclude il vicepresidente «generato da questa rapida crescita della minaccia informatica è la carenza di personale che abbia le competenze necessarie sia dal punto di vista operativo che gestionale per affrontare il problema; in conseguenza di ciò, temi come sensibilizzazione di dipendenti ed utenti finali, formazione, disponibilità di servizi gestiti e collaborazione pubblico e privato in materia di cybersecurity diventano temi sempre più rilevanti e di strettissima attualità». ■

biamo lavorato molto sulla nostra proposta. Daremo il massimo per portare a casa la gara». Avanti nella selezione anche il Consorzio Italia Cloud che aveva presentato manifestazione di interesse, ma non aveva poi partecipato alla seconda fase con un'offerta, come invece fatto dalla cordata di Tim, da Fastweb-Engineering e da Almaviva-Aruba. Il Consorzio, annuncia Antonio Baldassarra a DigitEconomy.24 (report del Sole 24 Ore Radiocor e della Luiss Business School), resta comunque interessato alla gara che partirà una volta pubblicato il bando.

«Abbiamo deciso nei mesi scorsi – precisa Baldassarra - di non presentare per il polo strategico nazionale una nostra proposta specifica, ma resta l'obiettivo di partecipare alla gara che sarà fatta sul capitolato messo a punto dalla cordata con Tim, stiamo lavorando in un'ottica federata pubblico-privata». Allo stesso tempo il Consorzio Italia Cloud, composto da sei aziende più Insiel, la in house che progetta, realizza e gestisce servizi informatici per conto della Regione Friuli-Venezia-Giulia, «lavora a un diverso scenario. Parteciperemo alla gara, ma ci candidiamo allo stesso tempo a essere un fornitore alternativo completamente compliant con le linee guida della cybersecurity dettate dall'Agenzia nazionale».

A far decidere il Consorzio verso questa doppia scelta, spiega Baldassarra, ha contribuito anche la constatazione che l'adesione al polo nazionale strategico del cloud per le Pa non è obbligatoria. Come spiegato in un convegno del Garr di qualche settimana fa da Paolo De Rosa, Cto del dipartimento per la Trasformazione digitale, «il cloud nazionale non è un 'trattamento sanitario obbligatorio' per nessuna Pubblica amministrazione».

Il Consorzio Italia Cloud, ad oggi formato oltre che da Insiel e Seeweb, da Sourcesense, Infordata, Babylon Cloud, Eht e Netaliall, è, inoltre, alle battute finali per chiudere le trattative con altri due enti pubblici. «Siamo in fase avanzata, forse le chiuderemo a fine mese. Inoltre, valutiamo l'ingresso nel nostro consorzio di altri tre soggetti privati», aggiunge il ceo di Seeweb. Riguardo alle linee guida richieste dall'Agenzia per cybersicurezza nazionale, elemento necessario per un'offerta di cloud alternativa al Polo, «Insiel si era già adeguata, alcuni data center di soggetti privati compreso il nostro hanno fatto la stessa cosa, ora – conclude Baldassarra - si tratterà di mettere a punto un'offerta che rispetti in maniera precisa i dettati dell'agenzia». ■

«Prevediamo una crescita che ci porterà a più che raddoppiare la nostra forza lavoro»

stesso sono stato chiamato a implementare. Nel piano di gruppo, prevediamo una crescita molto forte di Telsy, puntiamo a una crescita migliore del mercato, o almeno in linea. Il nostro tratto distintivo consiste nella possibilità di integrare le due anime, la sicurezza delle comunicazioni e la sicurezza informatica».

Da un lato, prosegue l'amministratore delegato, «proseguiremo con la crescita organica, ma al contempo pensiamo a crescere a livello inorganico: il 2021 è stato l'anno in cui abbiamo posto le basi per una campagna di M&A, nell'ottica non tanto di affrontare le acquisizioni tout court, ma di identificare i soggetti nel piano industriale da poter integrare». Telsy è alla ricerca di elementi che possano coesistere, anche di tipo tecnologico: «in Italia ad oggi l'80% delle aziende che dicono di fare cybersecurity sono erogatrici di servizi, non hanno una tecnologia propria, mentre per Telsy è fondamentale avere la tecnologia in casa. Attualmente stiamo studiando acquisizioni che annunceremo al momento opportuno. Guardiamo prevalentemente a soggetti di diritto italiano; d'altronde ci sono elementi di sistema, tra questi il perimetro di sicurezza cibernetica di cui Telsy fa parte, alla luce dei quali l'italianità diventa un fattore importante».

Si accompagna al piano di crescita dell'azienda anche il progetto di incremento dell'occupazione: «dal mio ingresso, lo scorso aprile, siamo cresciuti notevolmente e continueremo a farlo: prevediamo, infatti, una crescita esponenziale che ci porterà a più che raddoppiare in pochi anni la nostra forza lavoro». In quest'ottica «trovare le competenze è sfidante. In Italia sono stati fatti passi in avanti, ma vi è sempre una sana lotta per i talenti. Sono molto ricercati i coders, in grado di realizzare codici avanzati rispetto ai sistemi di cybersecurity. La sfida è sempre complessa, ma meno problematica e più gestibile rispetto a 3-4 anni fa, grazie alle sinergie crescenti tra industria e università. Si parla di più, ci sono progetti di ricerca cofinanziati».

Per il modello di business di Telsy «il punto chiave è la convergenza crescente tra criptografia e mondo del digitale, l'ambito in cui si muove tutto ciò che oggi è cybersecurity. L'azienda ha realizzato algoritmi di criptografia, realizzati da criptografi e da ingegneri con specializzazioni particolari, per proteggere i dati sia quando sono a riposo sia quando viaggiano. La convergenza si declina poi in vari modi, noi abbiamo cercato di coglierla sul piano tecnologico e industriale. Nell'ambito della criptografia ci sono tante applicazioni nate per usi di difesa e governativi che stanno trovando applicazione nel mercato corporate e civile, ad esempio le app di instant messaging proprietarie, che vengono fornite e prodotte da Telsy».

> *Trovare le competenze è sfidante. In Italia passi in avanti, ma vi è sempre una sana lotta per i talenti*

Guardando più in particolare ai prodotti, l'azienda immetterà sul mercato nei primi mesi del 2022 «sistemi di video conference sicuri, app di instant messaging proprietarie (quale alternativa ai più noti ma meno sicuri WhatsApp, Signal, etc.). Offriamo competenze distintive nella ricerca e soluzione di vulnerabilità in sistemi di connettività come i dispositivi IoT, chipset, router, piattaforme It usate per gestire chiamate, sistemi Scada (si pensi alle esigenze di mercato di aziende come Olivetti, crescenti richieste di implementazione di una 'sicurezza by design' e competenze chiave in ambito cloud, con particolare riferimento a Noovle). A tali competenze si aggiungono servizi e prodotti di monitoring, di analisi del traffico dati e scoperta di anomalie, threat intelligence, su cui stiamo investendo molto, al fine di prevenire e predire problematiche cyber, open source intelligence, decision intelligence e mobile security. Insomma, un cyber e crypto hub a 360° unico nel suo genere in seno alla struttura industriale ed alla cultura digitale di Tim».

Oltre a fornire soluzioni crypto ai partner storici, Telsy «guarda, in piena e forte sinergia con la forza vendite da Tim, ai clienti large e allo small e medium business. La nostra offerta è stata infatti arricchita per tutte le linee di business. Per la parte crypto abbiamo sviluppato soluzioni di varia natura, spaziando da prodotti per la sicurezza delle comunicazioni telefoniche, videoconference e messaggistica istantanea (come Pillow, Antares e InTouch), a prodotti per la sicurezza dei server (come Musa), cifranti (come Hypnos e BFT) e jammer ultrasonici (come Atmo). Sul lato cyber abbiamo sviluppato Omnia, una piattaforma integrata di cybersecurity che sfrutta la combinazione delle sue componenti per fornire funzionalità estremamente specializzate, unitamente alle nostre altre soluzioni per Soar, Edr, Apt detection e mobile security».

> *Immetteremo sul mercato sistemi di video conference sicuri e app di instant messaging proprietarie*

Grande rilevanza acquista, infine, il tema del quantum computing: quest'anno Telsy, ricorda Santagata, ha acquisito circa il 20% di Quantum Telecomunication Italy, società italiana leader nella tecnologia Qkd (Quantum key distribution). «Integrando le competenze di QTI con il know how di Telsy stiamo sviluppando delle soluzioni future-proof di crittografia post-quantum, ovvero prodotti che – conclude il ceo - siano resistenti ad attacchi portati tramite computer quantistici». ■