L'APPROFONDIMENTO

CyberSecurity as a Service e Managed Security Services: quali vantaggi per Pmi e PA

L'outsourcing della gestione della sicurezza digitale è ormai quasi un obbligo per PMI ed enti pubblici. Ma la scelta va ponderata con la massima attenzione. Ecco vantaggi e rischi

9 minuti fa

Marco R. A. Bozzetti
Presidente AIPSI - Associazione Italiana Professionisti Sicurezza Informatica

Security Solutions - Global Security - Online Security - House Security

Per le PMI e le piccole organizzazione delle PA, ma in molti casi anche per le medio grandi organizzazioni, la terziarizzazione della gestione della sicurezza digitale è ormai **quasi un obbligo**, per poter realizzare e gestire misure di sicurezza adeguate. Ma tale outsourcing deve essere realizzato con particolare attenzione, con scelte giuste ed oculate. Terziarizzare non significa demandare in toto ad altri, e non pensarci più: occorre sistematicamente verificare e controllare. Il Fornitore, anche il migliore, fa i suoi affari, non quelli del Cliente. **Sicuramente la sicurezza digitale richiede impegno e costa, ma quanto costa la non sicurezza**

Argomenti

A Agid Agenzia per l'Italia Digitale | C cloud

Canali

Mercati digitali | S Sicurezza digitale

digitale?

Esaminiamo la questione a 360 gradi, partendo proprio dalla necessaria comprensione dei due termini chiave: **Managed Security Services, MSS, e CyberSecurity as a Service, CSaaS.**

"Colao: "Il 95% delle PA è facile preda hacker", ma il Governo non sa ancora come rimediare"

Indice degli argomenti

Managed Security Services

Managed Security Services, MSS, è il termine inglese per indicare la gestione terziarizzata dei servizi di sicurezza digitale. La terziarizzazione di questi servizi, brevemente elencati nel seguito, può essere totale o parziale, ed erogata da uno o più consulenti, o da una o più aziende specializzate. Può inoltre essere svolta con strumenti informatici inseriti all'interno del Sistema Informativo stesso, o esterni, di proprietà dei e/o utilizzati dalle terze parti coinvolte.

CyberSecurity as a Service

CyberSecurity as a Service, CSaaS, fa riferimento ai servizi di sicurezza digitale erogati in cloud, e che possono essere gestiti direttamente da chi si occupa della sicurezza digitale del Sistema Informativo "cliente", o da altre terze parti, quali consulenti e società che li gestiscono in nome e per conto dei responsabili del Sistema Informativo del cliente.

Il CSaaS è quindi un sottoinsieme del più generale MSS.

La sicurezza delle informazioni

La sicurezza digitale, chiamata anche sicurezza ICT o sicurezza informatica o cybersecurity (pur se questi termini hanno differenze semantiche), è l'insieme di strumenti tecnici ed organizzativi per la protezione delle informazioni trattate dai Sistemi Informativi (nel seguito SI), ossia acquisite,

Articoli correlati

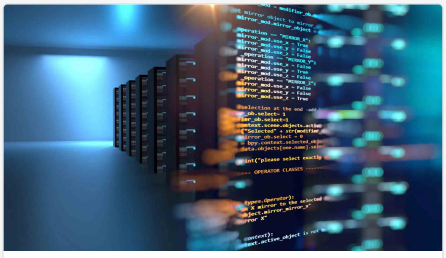
IL PUNTO

Cyber security, come va la strategia italiana: cosa abbiamo fatto e cosa resta da fare

02 Set 2021

di **Luisa Franchina e Matteo Taraborelli**

Condividi



PA DIGITALE

Cloud: roadmap e prospettive alla luce della nuova strategia nazionale

01 Ott 2021

di **Lorenzo Principali e Domenico Salerno**

Condividi

comunicate, archiviate, processate, in termini di:

- **integrità** è la proprietà dell'informazione di non essere alterabile; o poter verificare se è stata alterata
- **disponibilità** è la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti autorizzati;
- **confidenzialità** è la proprietà dell'informazione di essere nota solo a chi ne ha il diritto di accedervi
- Per le informazioni e i sistemi connessi **in rete,** ed oggi lo sono quasi tutti con Internet, le esigenze di sicurezza includono anche:
- **autenticità**, ossia la certezza da parte del destinatario dell'identità del mittente
- **non ripudio**, ossia il mittente o il destinatario di un messaggio non ne possono negare l'invio o la ricezione.

La sicurezza delle informazioni con le caratteristiche sopra evidenziate richiede la sicurezza digitale dell'intero SI che le tratta, e che si articola nella sua sicurezza fisica[1] (protezione dell'hardware e degli ambienti in cui sono posti ed operanti i sistemi ICT), logica (protezione in particolare del software, sia di base che applicativo, e dei dati trattati) ed organizzativa (riguarda gli aspetti organizzativi della assegnazione-suddivisione dei ruoli e dei compiti, delle procedure organizzative, del rispetto delle varie norme e leggi in vigore, etc.).

Indipendentemente dal settore merceologico e dalle dimensioni (come numero di dipendenti) ogni azienda ed ente pubblico supporta la quasi totalità delle attività e dei processi interni tramite le applicazioni del suo SI, che ne deve **garantire la continuità operativa** (business continuity), **l'integrità** e la **consistenza** dei dati trattati, il rispetto delle varie leggi e normative italiane ed europee: le leggi sul crimine informatico, sulla privacy, sulla responsabilità amministrativa (L. 231), e quelle specifiche per determinati settori e per le infrastrutture critiche.

I dati del SI costituiscono un reale bene (asset), e come tale valorizzabile nel conto economico/ bilancio.

La necessità di una efficace e reale sicurezza digitale

La necessità di una efficace e reale sicurezza digitale è dovuta soprattutto alla possibilità di subire attacchi digitali sia dall'interno della propria struttura, sia dall'esterno e online via Internet. Attacchi causati da un lato dalle vulnerabilità tecniche dei vari elementi costituenti il Sistema Informativo, dall'altro dalle vulnerabilità delle persone utenti dello stesso e dell'organizzazione dell'azienda/ente (per approfondimenti si rimanda ai **Rapporti annuali** dell'Osservatorio Attacchi Digitali, OAD, di AIPSI curato

dall'autore).

La sicurezza digitale deve essere considerata come una caratteristica globale ed integrata al SI, e come un processo continuo e dinamico che evolve nel tempo sia per l'innovazione tecnologica sia per l'evoluzione del business e dell'organizzazine dell'azienda/ente, sia per i nuovi possibili e sempre piu sofisticati cyber attacchi. Tenendo conto poi delle ultime normative, dovrebbe inoltre essere by default**,** ossia progettata come prerequisito al normale funzionamento dei sistemi ICT, e by design, ossia con le misure, strumenti e tecniche da usare individuate e considerate fin dalla iniziale fase di progettazione, in modo che possano essere realmente funzionali ed integrate col SI che devono proteggere.

Questa introduzione evidenzia la **complessità e l'interdisciplinarietà della sicurezza digitale**, che risulta veramente "ostica" da gestire e governare per gran parte dei decisori di vertice, in particolare per le piccole e piccolissime strutture (ma talvolta anche per quelle ben più grandi).

La pandemia Covid con il lockdown e la conseguente necessità, di colpo, di ampliare l'uso dei servizi online via Internet e del lavoro da remoto online, il così detto smart working, ha creato **seri problemi d**ata la non idoneità delle misure di sicurezza in essere soprattutto nelle PMI e nelle piccolissime organizzazioni.

I tipici servizi della gestione operativa della sicurezza digitale

La fig. 1 mostra le principali fasi del processo continuo per la sicurezza digitale.

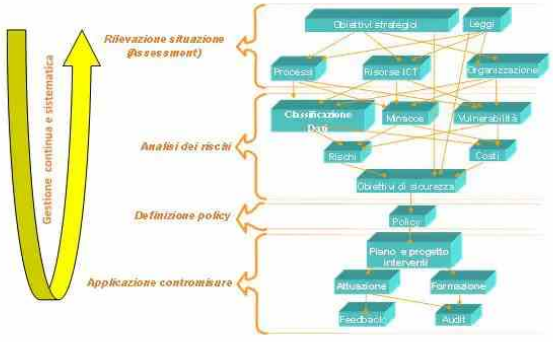


Fig. 1 (Fonte: dal volume "Sicurezza Digitale" di M.R. A. Bozzetti e F. Zambon)

La fig. 2 schematizza le funzioni del framework NIST[2], anch'esse ricorsive, per ciascuna delle quali vengono dettagliate le misure di sicurezza digitale ed i relativi standard e best practice di riferimento: per i **dettagli** si rimanda a nist.gov/cyberframework/framework). Questo framework è adottato da AgID[3] come guida per le Pubbliche Amministrazioni (PA)

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Fig. 2 (Fonte: NIST)

Senza entrare nei dettagli delle varie misure tecniche ed organizzative, i principali servizi per la gestione operativa della sicurezza digitale di un SI che rientrano in una logica MSS/CSaaS includono:

- la rilevazione automatica di tutte le risorse hardware e software presenti nel SI, inclusi i vari dispositivi anche mobili degli utenti finali;
- l'analisi automatica e periodica delle vulnerabilità dei sistemi in produzione;
- il monitoraggio continuo del funzionamento e delle prestazioni dell'intero SI;
- la gestione dell'identificazione, autenticazione ed autorizzazioni degli utenti;
- la raccolta e l'analisi dei log degli utenti e delle segnalazioni (alarm, warning, …) dei sistemi;
- la gestione dei vari strumenti di sicurezza quali firewall, firewall applicativi, IPS/IDS, anti malware, crittografia dei dati e delle comunicazioni, etc.;
- la gestione degli aggiornamenti software, delle patch/fix, etc.;
- l'helpdesk con trouble ticketing;
- la gestione dei problemi e degli incidenti sul SI;
- la gestione dei backup e del rispristino da backup;
- il Disaster Recovery (DR) con messa a disposizione delle risorse ICT alternative da attivare in caso di disastro;
- la gestione del SOC, Security Operation Centre.

L'attuale situazione della sicurezza digitale nelle piccole strutture private

In Italia la stragrande maggioranza delle imprese private è di piccole e piccolissime dimensioni, come indicato dai più recenti dati ISTAT (2011) riportati nella fig. 3

ISTAT: Imprese private per numero dipendenti	ISTAT Numero imprese	% sul totale ISTAT
< 10	4.149.572	94,80%

11-49	199.340	**4,55%**
50-249	24.288	**0,55%**
>250	4.179	**0,10%**
Complessivo	**4.377.379**	100%

Fig. 3 (elaborazione su dati ISTAT)

Quasi il 95% delle aziende italiane ha meno di 10 dipendenti. Andando ad esaminare la ripartizione per settore merceologico Ateco, sempre dai più recenti dati ISTAT, si è estratta la tabella di fig. 4 che evidenzia i settori merceologici con più di 300.000 aziende tra quelle con <10 dipendenti. Al primo posto si posiziona il "Commercio all'ingrosso e al dettaglio", al secondo le "Attività professionali, scientifiche e tecniche". Le aziende dei 5 settori selezionati, con il maggior numero di piccole e piccolissime aziende, rappresentano nel loro insieme il 65% circa di tutte le aziende italiane ed anche di tutte le PMI. Il numero totale dei dipendenti (2021) delle aziende italiane è calcolato dall'ISAT in circa 17 milioni e mezzo (17.438.078).

Numero aziende ISTAT per settori merceologici selezionati	< 10 dipendenti	11-49 dipendenti	50-249 dipendenti	Totale PMI	% PMI su tot . aziende	% aziende <10 dipendenti su tot. PMI	% aziende <10 dipendenti su complessivo aziende
C: Manifatturiere	302.152	59.674	9.162	370.988	8,48%	6,91%	6,90%
F: Costruzioni	466.567	19.375	1.236	487.178	11,13%	10,67%	10,66%
G: Commercio all'ingrosso e al dettaglio	1.027.992	37.198	3.130	1.068.320	24,41%	23,51%	23,49%
I: Servizi di alloggio e di ristorazione	305.764	28.145	1.087	334.996	7,65%	6,99%	6,99%
M: Attività professionali, scientifiche e tecniche	740.776	8.230	948	749.954	17,13%	16,94%	16,92%
					68,80%	**65,02%**	**64,95%**
Numero complessivo aziende ISTAT	**4.377.379**						
Numero totale PMI	**4.373.200**						

Fig. 4 (elaborazione su dati ISTAT)

In termini di informatizzazione, e quindi anche di livello di sicurezza digitale, le PMI italiane, pur migliorate negli ultimi anni, non sono ancora a livelli soddisfacenti ed in linea con le nazioni più "digitali" e quindi più competitive sui mercati a livello mondiale. La spesa in ICT è prevalente per le aziende grandi e grandissime, come evidenzia chiaramente la fig. 5, tratta dal recente Rapporto Assintel 2021, elaborato da IDC.

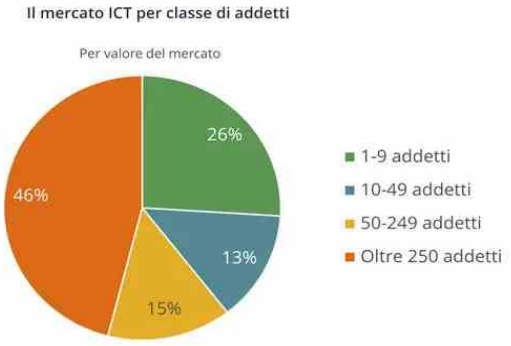


Fig. 5 (Fonte: Rapporto Assintel 2021)

Anche ISTAT ha effettuato nel 2021 **un'indagine** sullo stato dell'ICT nelle aziende italiane, considerando solo le aziende con più di 10 dipendenti e prendendo a riferimento l'indice europeo **DII, Digital Intensity Index** 2021: è un indice costruito a livello di macrodati che misura l'utilizzo da parte delle imprese di 12 diverse tecnologie digitali elencate nella tabella di fig. 6. Si noti come questo indice sia molto orientato alla connettività e alla vendita online, ma non consideri affatto la sicurezza digitale!

1. Imprese che hanno la percentuale di addetti connessi superiore al 50%
2. Imprese che utilizzano ERP per condividere informazioni tra diverse funzioni aziendali
3. Imprese che si connettono a Internet in banda larga fissa a velocità di download >= 30 Mbit/s
4. Imprese che hanno vendite via web maggiori dell'1% dei ricavi e vendite via web verso consumatori privati (B2C) superiori al 10% del totale delle vendite via web
5. Imprese con utilizzano almeno un IoT
6. Imprese che hanno almeno un social media
7. Imprese che utilizzano CRM
8. Imprese che acquistano servizi cloud di livello intermedio o sofisticato
9. Imprese che utilizzano almeno una tecnologia IA
10. Imprese che acquistano servizi cloud computing
11. Imprese con il valore delle vendite online >=1% dei ricavi totali
12. Imprese che utilizzano almeno due social media

Fig.6 (Fonte: Unione Europea)

In base all'indice DII, la fig. 7 mostra il livello di digitalizzazione delle aziende italiane con più di 10 dipendenti.

L'indice DII individua quattro intensità digitali in funzione del numero di attività svolte dalle imprese, facendo riferimento alle 12 attività elencate nella fig.6: fino a 3 attività (livello molto basso), da 4 a 6 (livello basso), da 7 a 9 (livello alto), da 10 a 12 (livello molto alto). Il "livello base" di digitalizzazione del DII è raggiunto quando l'impresa svolge almeno 4 delle 12 attività digitali considerate.

CLASSI DI ADDETTI	Imprese per livello di digitalizzazione (%)				Imprese con *livello base* [1] di digitalizzazione (%)	Addetti delle imprese con *livello base* di digitalizzazione (%)
	molto basso	basso	alto	molto alto		
10-49	41,6	41,0	15,8	1,6	58,4	61,3
50-99	24,9	44,3	26,6	4,2	75,1	74,4
100-249	20,3	36,8	36,7	6,2	79,7	80,1
250 e più	12,2	26,2	41,7	19,9	87,8	93,2

Fig. 7 (elaborazione su dati ISTAT)

Si evidenzia come l'82,6% delle aziende molto piccole italiane, con <10 dipendenti, nel 2021 avevano un livello di digitalizzazione basso o molto basso, secondo la metrica DII, ma con un livello di base quasi al 60%. Nel complesso le aziende PMI di dimensioni più grandi avevano un livello migliore e in crescita col crescere dei dipendenti: comunque in una posizione

migliore della media europea per il livello di base per le PMI che si attesta al 54%.

Dall'indagine ISTAT 2021 sull'ICT nelle imprese emerge un solo dato che in qualche misura fa riferimento ai servizi CSaaS in cloud, riportato nella fig. 8: per classi di addetti, la % di chi acquista servizi in cloud, e tra questi la % di chi ha in cloud applicazioni software di sicurezza digitale.

CLASSI DI ADDETTI	Imprese che acquistano servizi di cloud computing in %	Applicazioni software di sicurezza in CLOUD (es. programma antivirus, controllo di accesso alla rete) in %
10-49	58,7	41,2
50-99	69,9	50,0
100-249	73,6	53,3
250 e più	83,0	59,7

Fig. 8 (elaborazione su dati ISTAT)

Più della metà delle PMI con più di 10 dipendenti utilizza software di cyber sicurezza in cloud: probabilmente una parte lo gestisce direttamente, ma un'altra parte lo fa sicuramente gestire da terze parte specializzate e dedicate a queste attività., utilizza quindi servizi CSaaS.

Nel PNRR[4] nell'ambito della Missione 1 il M1C2 per la Digitalizzazione, innovazione e competitività del sistema produttivo prevede 30,57 Mldi suddivisi in cinque diversi interventi. Nessuno di questi richiama esplicitamente la sicurezza digitale, che sarà "embedded" nei vari progetti che si faranno in questo contesto.

L'attuale situazione della sicurezza digitale nelle piccole organizzazioni pubbliche

La situazione per le PA, alla data, è simile a quella delle imprese private, con problemi analoghi nella sicurezza digitale sin particolare nelle piccole organizzazioni, ma con minori informazioni disponibili e con difficoltà nell'ottenerle, soprattutto in merito alla sicurezza digitale. Si hanno a disposizione meno indagini e meno dati, rispetto alle aziende private, ed è generalmente più difficile ottenerli, anche per la complessità e l'articolazione dell'intera PA italiana, che pure ha un numero molto inferiore di dipendenti: al 1° gennaio 2021 la PA italiana contava 3,2 milioni di dipendenti. Per comprendere e ben considerare la situazione della sicurezza digitale nella PA, e nelle sue strutture più piccole, occorre aver presente la sua intera struttura, dato che varie indagini fanno riferimento alla PA, ma ne considerano ed analizzano solo alcune sue parti. La PA italiana è costituita , in accordo con l'art. 1 comma 2 del d.lgs 30 marzo 2001 n. 165

(https://www.gazzettaufficiale.it/eli/id/2001/05/09/001G0219/sg) da:

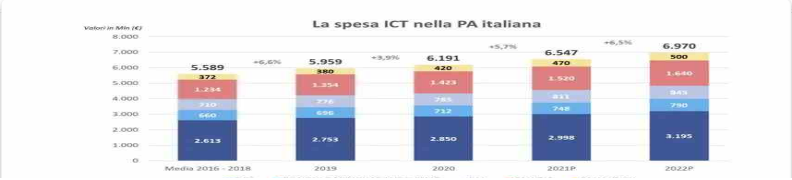
- Presidenza del Consiglio dei ministri, i ministeri e le loro articolazioni centrali e locali, le istituzioni scolastiche, le agenzie[5] e le aziende autonome[6];
- le autorità amministrative indipendenti, che sono Enti pubblici con personalità giuridica: attualmente sono solo l'Amministrazione degli archivi notarili ed i Monopoli di Stato ;
- le regioni, le province, le città metropolitane, i comuni e gli altri enti territoriali locali quali ad esempio comunità montane, le comunità isolane, le unioni di comuni e i consorzi fra enti territoriali;
- gli altri enti pubblici, nazionali e locali, tra cui le istituzioni universitarie, gli enti pubblici di ricerca, le camere di commercio, industria, artigianato e agricoltura e gli enti che compongono il Servizio Sanitario Nazionale.

Nel complesso le strutture organizzative della PA sono **nell'ordine di 55.000**, e di queste (2021):

- Comuni: 7.904
- Province e Citta Metropolitane: 80 province, 14 città metropolitane e 6 liberi consorzi comunali in Sicilia) 2 province autonome in Trentino-Alto Adige
- Regioni: 20 di cui 5 a statuto speciale
- Scuole pubbliche: **40.749**
- Università pubbliche: 67
- USL del Servizio Sanitario Nazionale[7](SSN): 650

AgID realizza un Piano Triennale per l'informatica nella PA, arrivato ora con **l'aggiornamento** 2021-23, ed effettua sulle spese e sull'attuazione dei vari progetti dei controlli su circa il 50% della PA, Difesa esclusa. La fig. 9 sintetizza la spesa in ICT sempre in crescita tra il 2016 ed il 2022 (previsione). Si noti che nella voce "Education" sono incluse scuole, università e centri di ricerca pubblici: questo comparto ha una previsione di crescita superiore ai trend del passato. Nella Sanità è inclusa la sanità regionale.

La fig. 10 fornisce delle indicazioni sulla spesa in cybersecurity, e mostra la ripartizione % delle principali aree di intervento: queste % evidenziano che il focus è soprattutto sulla protezione delle infrastrutture ICT, oltre che sul Disater Recovery, ma è limitato sulle attività proattive e preventive, sulla governance e sulla protezione degli applicativi. Le applicazioni sono quelle che trattano e gestiscono i dati, che rappresentano l'asset principale dell'intero SI. E proprio qui ho il valore minimo di spesa?



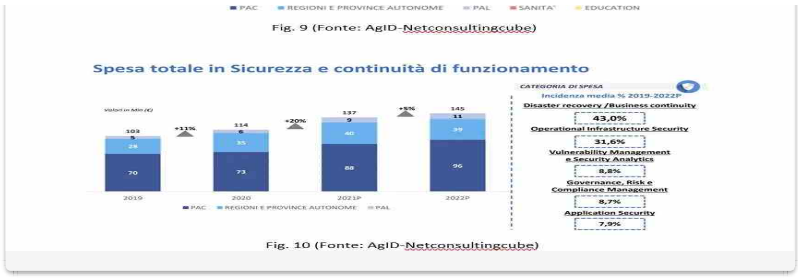


Fig. 9 (Fonte: AgID-Netconsultingcube)

Fig. 10 (Fonte: AgID-Netconsultingcube)

In termini di livelli di digitalizzazione la PA, sia PAC ma soprattutto PAL, necessita di significativi miglioramenti, soprattutto per quanto riguarda la sicurezza digitale. Il Ministro Colao, agli inizi del 2021, ha affermato che "il 95% della PA è facile preda di hacker", si veda. E tale affermazione è suffragata da varie indagini: ne vengono considerate due effettuate da o in collaborazione con AgID. La prima si riferisce al livello di sicurezza digitale dei siti web delle PA, con focus particolare sull'uso di HTTPS e sul corretto e tempestivo aggiornamento del software del web e dei vari plugin (CMS, Content Management System). AgID ha effettuato due indagini su questo tema, una nel 2020 ed una nel **2021**. Quest'ultima ha rilevato che :

- La situazione lato HTTPS è migliorata tra 2020 e 2021, e solo il 2% delle PA rispondenti non ha ancora in produzione il protocollo sicuro https;
- La situazione lato CMS tra le due rilevazioni è complessivamente peggiorata. Pur con le difficoltà illustrate nel documento per la verifica della sicurezza dei CMS, il numero di CMS aggiornati all'ultima versione disponibile, inclusi i plugin, sono passati dal **13,7%** del totale nel 2020 all'**8,3%** nel 2021, con un calo del **52. WordPress si rivela il CMS più usato**: viene usato **due volte** tanto il suo concorrente più prossimo, **Joomla**, e **cinque volte tanto** il terzo classificato **Drupal**.

La seconda indagine di AgID, effettuata in collaborazione con Netconsultingcube, è "La spesa ICT nella PA italiana". Fa riferimento solo ad un campione ristretto di PA[8], con l'esclusione di scuole, università, difesa, etc, ma fornisce interessanti **dati** sulla cybersecurity.

Dal documento emerge che la spesa per la sicurezza informatica è prevista per progetti ad hoc ripartiti tra :

- Amministrazioni centrali: 16 progetti – valore complessivo di circa 95 milioni di euro;
- Regioni e Province Autonome: 8 progetti – valore complessivo 40 milioni di euro;
- Amministrazioni locali: 3 progetti – valore 730 mila euro.

Un valore complessivo veramente basso, a giudizio dell'autore, anche se molta sicurezza digitale è sicuramente inclusa, embedded, negli altri progetti e difficilmente può essere valutata a se stante.

CONFERENZA DELLE REGIONI E DELLE PROVINCE AUTONOME
Agenda Digitale.eu
www.agendadigitale.eu
Utenti unici: 4.145
Rassegna del 30/03/2022
Notizia del: 30/03/2022
Foglio:11/17

Ai fini di MSS/CSaaS, di particolare interesse la rilevazione su questo campione delle modalità di "governo" della cybersecurity, mostrata nella fig. 11.

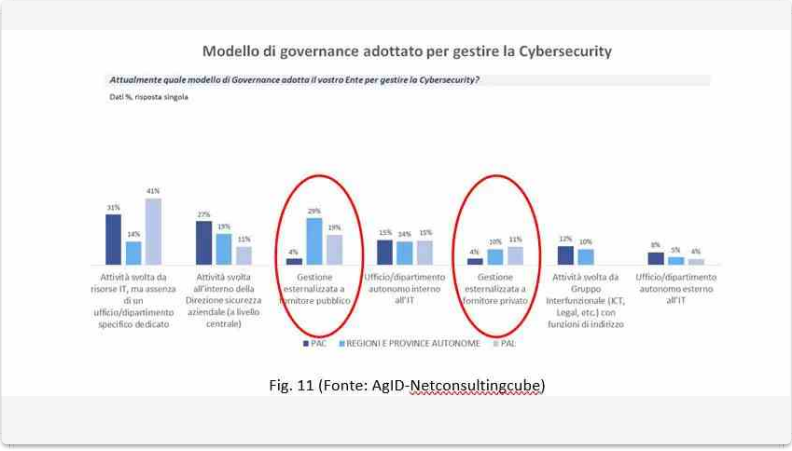


Fig. 11 (Fonte: AgID-Netconsultingcube)

La figura evidenzia come la terziarizzazione per la cybersecurity e la sua gestione-governo sia più diffusa nelle PAL e Regioni, sia con fornitore pubblico o privato: con il primo arriviamo al 52%, con il secondo al 25%. Per quanto riguarda il SOC, Security Operation Centre, nelle PA, nelle organizzazioni che già lo hanno prevale una gestione totalmente esterna, seguita da una gestione interna e ibrida. La presenza di un SOC interno ricorre con maggior frequenza nelle PAC ma anche nelle Regioni e nelle Province autonome.

Le Forze Armate hanno un elevato utilizzo, e quindi spesa, nell'ICT e nella sua sicurezza, sia nell'ambito dei loro SI e delle loro reti, sia "embedded" nei loro sistemi d'arma. Il "Documento Programmatico Pluriennale della Difesa" () prevede in particolare specifici progetti sulla cybersecurity, dal potenziamento dei sistemi con Intelligenza Artificiale al "Defence Cloud" e al miglioramento del MDL, Multi Data Link, con una spesa pluriennale di quasi 600 milioni di euro.

"La Difesa italiana si rafforza nel cyberspazio: obiettivi e strategia"

Nel PNRR, nell'ambito della Missione 1 il M1C1 per la Digitalizzazione, innovazione e sicurezza nella PA sono previsti 11,15 miliardi e la cyber sicurezza è nel titolo: essa è prevista nella parte Digitalizzazione con l'Investimento 1.5 di €. Tale investimento fa riferimento al "Perimetro di Sicurezza Nazionale Cibernetica" e è articolato in quattro principali aree: il rafforzamento della front-line per la gestione degli alert e degli eventi a rischio verso la PA e le imprese di interesse nazionale; il potenziamento delle capacità tecniche di valutazione e audit continuo della sicurezza digitale degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale a livello

nazionali; l'immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il paese da minacce cibernetiche; potenziamento e rafforzamento gli asset e le unità cyber incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.

Il mercato previsto in Italia per MSS/CSaaS

Alla data ben pochi i dati di riferimento specifici ed attendibili per l'Italia. L'ultimo rapporto "Il Digitale in Italia 2021" di Anitec-Assinform, curato da Netconsultingcube, riporta dei dettagli per la crescita del mercato della cybersecurity nei prossimi anni, ed riportati nella fig. 12. La voce MSS e Cloud della figura fa in pratica riferimento ai servizi MSS/CSaaS , ed evidenzia per essi la più alta % del TCMA, Tasso di Crescita Medio Annuo, pari ad un aumento del 15,4%

Fig. 12 (Fonte: Anitec-Assinform Netconsultingcube)

Questo tipo di mercato esiste anche in Italia e sta crescendo, e le piccole imprese, pubbliche e private potrebbero o dovrebbero utilizzarlo. Ma come e a quali condizioni? Cerchiamo di approfondirlo nel prossimo ed ultimo paragrafo.

Terziarizzare la gestione della sicurezza digitale per le piccole strutture private e pubbliche

Dai paragrafi precedenti emerge una situazione per la sicurezza digitale in crescente miglioramento, ma ancora con molto da fare per raggiungere i livelli di sicurezza necessari per una Italia realmente competitiva in mondo sempre più digitale: e questo vale in particolare per le piccole e piccolissime organizzazioni, sia private che pubbliche, che costituiscono, con il loro enorme numero, l'asse portante dell'economia del paese.

Queste strutture "piccole", salo rari casi, non hanno e non possono avere le risorse finanziarie e le competenze interne per gestire "on premise" e con le proprie forze la dinamica complessità della moderna sicurezza digitale per

Agenda Digitale.eu
www.agendadigitale.eu
Utenti unici: 4.145
Rassegna del 30/03/2022
Notizia del: 30/03/2022
Foglio:13/17

poter realmente proteggere il proprio business e le proprie attività. Non possono quindi che terziarizzare a chi professionalmente ha tali competenze e capacità: questo da un lato ha un costo, e dall'altro la necessità di controllare che la/le terze parti coinvolte operino correttamente

"Come posso fidarmi di una terza parte che non so e posso controllare", "Il dato è mio e me lo gestisco io …", "Non posso dare a terzi le mie informazioni più riservate e confidenziali ..". Queste sono le tipiche affermazioni dubitative che l'imprenditore e/o il top manager hanno in mente quando considerano la terziarizzazione dell'ICT. Ed in questo spesso si confondono, e si usano come sinonimi, due termini che hanno un ben diverso signifcato: la gestione operativa del SI e della sicurezza digitale, indicata anche con il termine "management", ed il governo, "governance". La **gestione operativa**, lo dice il nome, è operativa: pianifica, sviluppa, esegue e monitora le attività seguendo le direttive strategiche emesse dall'organismo di governance. Quest'ultimo definisce La **governance è strategica:** definisce gli obiettivi da perseguire in linea con le necessità del business e/o delle attività dell'azienda/ente, fissando priorità, assegnando compiti e responsabilità, e verificando che la gestione operativa operi come richiesto ed ottenga i risultati attesi.

A gestione operativa è quindi terziarizzabile, la governance no, è compito del top management attuarla, anche con l'aiuto di una idonea consulenza. Per una effettiva ed efficace realizzazione di un corretto "management" e "governance", i decisori, ossia il top management, devono avere idee chiare sul tema, e devono sape scegliere cosa fare, tenendo conto della loro realtà interna e di che cosa offre io mercato, in particolare sul loro territorio. I decisori nell'ambito delle piccole e piccolissime strutture, sia pubbliche che private, ritengono sovente (anche se non sempre lo ammettono) che l'ICT, e quindi un sistema informativo, soprattutto se di piccole dimensioni, con la sua sicurezza digitale sia di fatto una "**commodity**" e come tale debba essere negoziata ed acquista. Commodity è un termine inglese che indica un bene per cui c'è domanda ma che è offerto senza differenze qualitative sul mercato ed è fungibile, cioè il prodotto è lo stesso indipendentemente da chi lo produce, come per esempio il petrolio, i metalli, la telefonia, l'energia elettrica. L'energia elettrica, così come la telefonia, sono esempi calzanti: io non so, e non voglio sapere, cosa ci sia dietro ad una presa elettrica. Tutti i miei dispositivi elettrici hanno uno spina e seguono specifici standard che permettono di rendere compatibile la presa elettrica con la spina e le caratteristiche elettriche del mio dispositivo. Inserita la spina, tutto funziona. Analoga cosa per la telefonia. Nel mondo digitale odierno si è arrivati ad una forte standardizzazione, al prevalere sul mercato di pochi prodotti di riferimento e ad avere Internet ed il suo stack di protocolli come di fatto unico standard e mezzo universale di comunicazione multi-mediale. Qualsiasi impresa, anche di una sola persona, ha almeno un PC ed una connessione ad

Internet: tali infrastrutture ICT di base possono essere considerate una commodity, ma le applicazioni che sono sul PC e che interagiscono con il mondo di Internet sul web sono personalizzate sulle specifiche esigenze di quell'impresa e del suo business ed attività, così come tutti i dati trattati. E questa parte non è e non potrà essere considerata una commodity: ed è la parte che supporta e genera l'effettivo "valore" per l'impresa.

La terziarizzazione dell'operatività della sicurezza digitale può e deve essere terziarizzata, in particolare per le piccole strutture, ma a condizione che sia terziarizzata alle corrette condizioni tecniche, economiche e normative, che sia trasparente e controllabile: in una parola che sia un "**right-sourcing**", un giusto approvvigionamento.

L'outsourcing dell'ICT e ben noto e consolidato da tempo, ed ha ben note motivazioni finanziarie (da Capex a Opex), sulle competenze aggiornate dei fornitori, sulla flessibilità (sovente più teorica che pratica) dei contratti tra cliente e fornitore, sulla possibilità di cambiamenti migliorativi nei processi interni, con conseguenti possibili riduzioni del personale, almeno nelle grandi realtà (quelle piccole sono già da tempo ridotte all'osso ..).

Per avere successo con un outsourcing, e quindi anche nell'adozione di servizi MSS/CSaaS, debbono essere realmente soddisfatte alcune condizioni, il più delle volte però difficili per le piccole e piccolissime organizzazioni:

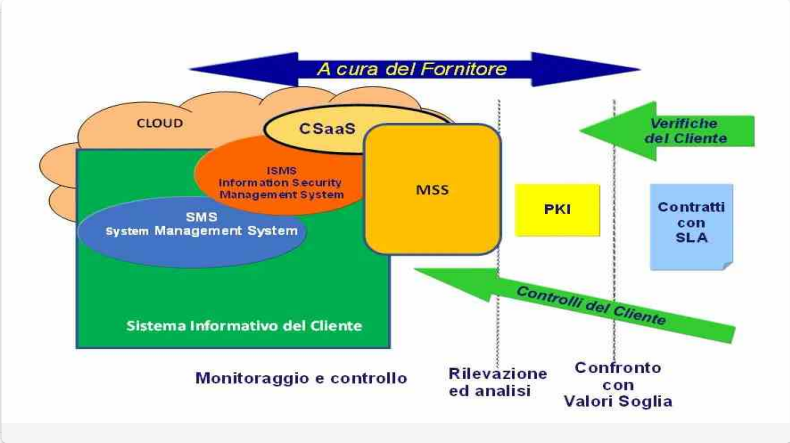
- Controfirmare un contratto con il fornitore con SLA[9] e KPI[10] ben definite, ed evitando clausole di forti vincoli tali da causare di fatto l'inamovibilità di quel fornitore, il così detto "locked in" ;
- Controllare periodicamente (o far controllare da un consulente terzo) l'effettivo rispetto delle SLA concordate;
- Controllare periodicamente (o far controllare da un consulente terzo) che il rapporto prezzi/prestazioni del fornitore sia in linea con quelli che offre il mercato.

La fig. 13 schematizza tale approccio e tale logica, e vale per aziende/enti di qualsiasi dimensione, come numero di dipendenti, e settore merceologico di appartenenza.

Il SI del cliente è raffigurato dal rettangolo verde, e concettualmente è dotato (o dovrebbe essere) di un sistema di monitoraggio e controllo, indicato nella figura come SMS, System Management System, ed al suo interno il sitema di monitoraggio e controllo della sicurezza digitale dell'intero SI, indicato come ISMS, Information Security Management System. L'intero SI o sue parti possono essere in cloud (o terziarizzate presso Terze Parti) , così come l'SMS e l'ISMS. Il CSaaS è totalmente in cloud, in interagisce e/o ingloba l'ISMS. I servizi MSS possono usare il cloud ed il CSaaS.

Per i servizi CSaaS e MSS (così come per qualsiasi servizio terziarizzato/in cloud), deve essere stipulato un contratto tra il Fornitore (o anche più di uno) ed il Cliente, con specifiche SLA e relativi KPI.

SLA e KPI devono essere periodicamente verificati: il Fornitore dovrebbe fornire dei rapporti periodici sul soddisfacimento dei livelli di servizio, secondo quanto concordato nel contratto. Il Cliente dovrebbe verificare che tali rapporti siano veritieri e congruenti con quanto risulta effettivamente sul campo. In caso contrario o di ragionevoli sospetti di inadempienza, se la dovuta e motivata richiesta di controlli al Fornitore non dovesse avere esaurenti risposte, è bene che il Cliente effettui autonomi controlli, magari con l'aiuto di consulenti. Per poi, dati alla mano, fare eventuale causa legale al Fornitore.



Il problema di fondo, soprattutto per le realtà piccole e senza competenze specifiche in materia, e come scegliere il Fornitore giusto per le proprie esigenze. Il problema è il medesimo per la scelta di qualsiasi professionista su temi di non nostra diretta competenza e conoscenza: dal medico all'avvocato, dal notaio al

Commercialista e all'amministratore di condominio. Al di là del colpo di fortuna, i pochi criteri da seguire includono:

- Il passa parola con chi è già cliente di quel fornitore;
- La verifica presso le Associazioni di categoria e quelle specializzate nel settore ;
- La verifica del sito web del fornitore e le certificazioni che la sua azienda ed i suoi dipendenti hanno, in particolare in merito alla sicurezza digitale: al di là di quelle proprietarie sui prodotti, significative e vendor-neutral sono C/CISO, C/HFI, CompTIA, CSSP e le altre certificazioni (ICS)^2, eCF, Eucip, famiglia ISO 27000, ISACA (CISA, CISM, CRISC), ISO 20000, OSCP, SANS-GIAC, etc.;
- Le best practice e gli standard che segue, in particolare le misure minime e d il CAD per le PA: sul sito web del Fornitore ci dovrebbero essere le informazioni relative.

Note

1. La sicurezza fisica non riguarda solo i Data Center e le computer room decentrate, o l'accesso ad aree riservate al Sistema Informativo, ma anche i dispositivi d'utente, fissi e mobili, cui estranei non devono poter aver accesso, anche nel caso fossero persi o rubati. ↑
2. NIST, National Institute of Standards and Technology: fa parte del Dipartimento del Commercio USA. Promuove l'innovazione e la competitività industriale degli Stati Uniti basandosi sull'evoluzione scientifica, le tecnologie digitali, gli standard. ↑
3. AgID, Agenzia per l'Italia digitale (https://www.agid.gov.it/): è l'Agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. Ha il compito di coordinare le amministrazioni pubbliche nell'attuazione del Piano Triennale per l'informatica, favorendo la trasformazione digitale del Paese. ↑
4. PNRR, Piano Nazionale di Ripresa e Resilienza, si veda https://www.governo.it/sites/governo.it/files/PNRR.pdf ↑
5. Una Agenzia è distinta dall'organizzazione ministeriale, svolge una funzione pubblica ed è sottoposta a direzione o vigilanza da parte di un organo politico. Esempi: Agenzia delle Entrate, Agenzia del Demanio, AIFA, etc; nel nostro settore AgID e ACN. ↑
6. Una Azienda Autonoma è una organizzazione che parte dello Stato o di altro ente pubblico e che è normalmente priva di personalità giuridica, ma possiede caratteri che le conferiscono un certo grado di compiutezza e separatezza. Il suo compito è di fornire e gestire servizi di pubblico interesse. Testo unico delle leggi sull'ordinamento degli enti locali- D.Lgs. 18 agosto 2000, n. 267 (https://web.camera.it/parlam/leggi/deleghe/testi/00267dl.htm). Molte Aziende Autonome nel passato sono state privatizzate o trasformate in Ente pubblico economico o in Agenzia ↑
7. Il **Servizio sanitario nazionale** non è un'unica amministrazione, ma un insieme di enti ed organi che concorrono al raggiungimento degli obiettivi di tutela della salute dei cittadini. Lo compongono:
   - Organismi centrali dello stato: Ministero della Sanità, Consiglio Superiore di Sanità, Istituto Superiore di Sanità, Conferenza Stato-Regioni, Agenzia Italiana del Farmaco, Istituti Zooprofilattici Sperimentali, Agenzia nazionale per i servizi sanitari regionali.
   - Organismi regionali: assessorato alle attività sanitarie, Conferenza regionale permanente

- Organismi territoriali: Aziende Sanitarie Locali e Aziende Ospedaliere, Istituti di Ricovero e Cura a Carattere Scientifico

↑

8. la Rilevazione 2021 ha coinvolto un panel di soli 76 Enti della PA, con 26 PAC, 23 Regioni e Province autonome, 13 Città Metropolitane, 14 Comuni capoluogo delle Città Metropolitane, con un ragionevole bilanciamento tra PAC e PAL. ↑
9. SLA, Service Level Agreement: contratto che disciplina i rapporti tra cliente e fornitore. Il primo deve definire e documentare le proprie necessità ed i servizi richiesti, anche in termini prestazionali. Fornitore configura ed eroga tali servizi secondo i livelli concordati, e se ne assume la responsabilità. ↑
10. KPI, Key Performance Indicator: variabili misurabili che permettono di quantificare il livello di servizio erogato. ↑