IDC
Analyze the Future

WHITE PAPER

La sicurezza IT nelle PMI e la fine del supporto tecnico per Windows XP

Sponsored by: Microsoft Italia

Giancarlo Vercellino
February 2014

IDC OPINION

A livello internazionale la sofisticazione degli attacchi sta oltrepassando qualsiasi livello con la comparsa di nuovi attori nell'arena del cyber-crime e della cyber-war che sfruttano in modo sistematico le vulnerabilità software esposte da qualsiasi sistema operativo, industrializzando i processi di produzione di malware per attaccare gli interessi di qualsiasi impresa. Nonostante la grande attenzione della stampa specializzata e internazionale, lo sviluppo e la diffusione di una cultura aziendale legata alla sicurezza informatica ancora stenta a consolidarsi in alcuni comparti dell'economia, soprattutto nel segmento delle Piccole e Medie Imprese (PMI).

I consueti processi di aggiornamento del software e dei sistemi operativi sono lo strumento essenziale per garantire il mantenimento di base della sicurezza dei sistemi di qualsiasi impresa, ed è proprio in questa prospettiva più generale che occorre prestare grande attenzione alla data dell'8 aprile 2014 (End-of-Support Day, EoS Day), quando Microsoft terminerà ufficialmente il supporto sul sistema Windows XP: oltre tale data non saranno più disponibili né gli aggiornamenti automatici per la sicurezza né il download di Microsoft Security Essentials.

Il documento presenta la sintesi delle principali evidenze derivanti dall'indagine condotta da IDC approfondendo la percezione del rischio delle PMI all'approssimarsi dell'EoS Day. L'indagine ha coinvolto un campione di 850 PMI che rappresentano una parte fondamentale dell'economia nazionale e sono riconducibili quasi all'intero spettro industriale. Alcune delle principali evidenze osservate sono le seguenti:

- Windows XP è ancora profondamente radicato nel tessuto imprenditoriale italiano: il 23,8% delle imprese lavora con Windows XP per oltre l'80% del parco PC aziendali.
- Nonostante si ritengano informate sul tema della sicurezza informatica (oltre 86%), le PMI sottovalutano ampiamente le vulnerabilità software come fattore di rischio per la sicurezza, evidenziandolo soltanto in occasioni limitate (7,6%).
- Molto spesso le imprese sono prive di referenti interni cui attribuire la responsabilità della sicurezza informatica (44,1%) e destinano alla gestione del problema meno del 10% del loro budget IT (73,5%).
- L'indagine evidenzia come le PMI facciano ampio affidamento sul canale per comprendere al meglio i rischi alla sicurezza informatica, i partner e i fornitori di fiducia vengono evidenziati dal 52,2% delle imprese.

Viale Monza, 14 20127 Milan, Italy P.39.02.28457.1

TABLE OF CONTENTS

LIST OF FIGURES

METODOLOGIA

L'indagine è stata condotta tra dicembre 2013 e gennaio 2014 somministrando un questionario a 850 imprese con sede in Italia attraverso un campionamento casuale per quote. Lo studio ha coinvolto una ampia parte del tessuto imprenditoriale italiano (ambito cross-industry, esclusa Pubblica Amministrazione Centrale, Sanità e Istruzione) con riferimento al segmento di imprese con addetti compresi tra 6 e 499 (dunque un segmento prevalentemente formato da PMI, sebbene comprenda anche una porzione di imprese di grandi dimensioni). L'analisi ha portato all'estrapolazione del dato campionario rispetto a un universo di riferimento che consta di circa 446mila imprese secondo il modello statistico di IDC elaborato da fonti ISTAT (dato di riferimento per le percentuali a totale; le basi per le percentuali calcolate con riferimento alle classi dimensionali e settoriali sono diverse; allo stesso modo sono diverse le basi di riferimento per le estrapolazioni sui sottogruppi).

Lo strumento di indagine, composto da circa 16 domande di approfondimento sul tema della Sicurezza IT, sullo scenario di adozione di WinXP precedente all'EoS Day, sulla diffusione di tecnologie mobili e gli investimenti in sicurezza, è stato sviluppato in collaborazione con Microsoft Italia. Il questionario è stato somministrato a un campione che comprende sia quelle figure che danno centralità di rappresentanza aziendale al tema della gestione della sicurezza IT (ad esempio IT Manager, Direttori dei Sistemi Informativi) sia quelle figure che ricoprono de facto tale responsabilità pur afferendo ad altre funzioni aziendali (ad esempio, l'area tecnico-amministrativa, l'area organizzativa, etc.). Seguono le tabelle di sintesi che descrivono la distribuzione dei rispondenti rispetto ai settori industriali, alle classi dimensionali e al ruolo aziendale (Tab. 1-3):

TABELLA 1

Campione di riferimento dell'indagine, settore industriale, n=850

Settore	% nel campione
Commercio	20%
Finanza	20%
Industria	20%
Pubblica Amministrazione Locale	20%
Servizi & TCU	20%
Totale	100%

Fonte: IDC, 2014

TABELLA 2

Campione di riferimento dell'indagine, dimensione aziendale, n=850

Dimensione	% nel campione
Addetti 6 – 19	29,4%
Addetti 20 – 49	29,4%
Addetti 50 – 249	23,6%
Addetti 250 – 499	17,6%
Totale	100%

Fonte: IDC, 2014

TABELLA 3

Campione di riferimento dell'indagine, ruolo dei rispondenti, n=850

Ruolo aziendale	% nel campione
Area sistemi informativi/ informatici	70,4%
Area tecnico-amministrativa	12,4%
Titolare/ Amministratore/ Area direzionale	7,1%
Altri ruoli/ figure aziendali	10,1%
Totale	100%

Fonte: IDC, 2014

IN QUESTO DOCUMENTO

La sicurezza informatica nelle PMI

Sia gli osservatori promossi dai maggiori vendor della sicurezza sia gli osservatori promossi da centri ricerche indipendenti (es. il CERT presso la Carnegie Mellon University) concordano sempre più spesso nell'osservare che il grado di sofisticazione degli attacchi sta raggiungendo un livello ineguagliato con la comparsa di nuovi attori nell'arena del cyber crime e della cyber war: agenzie sovvenzionate da enti governativi (es. Comment Crew), organizzazioni criminali e associazioni di hacktivist (es. Anonymous) non soltanto stanno industrializzando il processo di produzione dei malware ma lo stanno anche ingegnerizzando per portarlo a un livello del tutto nuovo (ad esempio, si pensi al caso storico di Stuxnet oppure al caso più recente di Flame), sia dal punto di vista tecnologico sia dal punto di vista strategico:

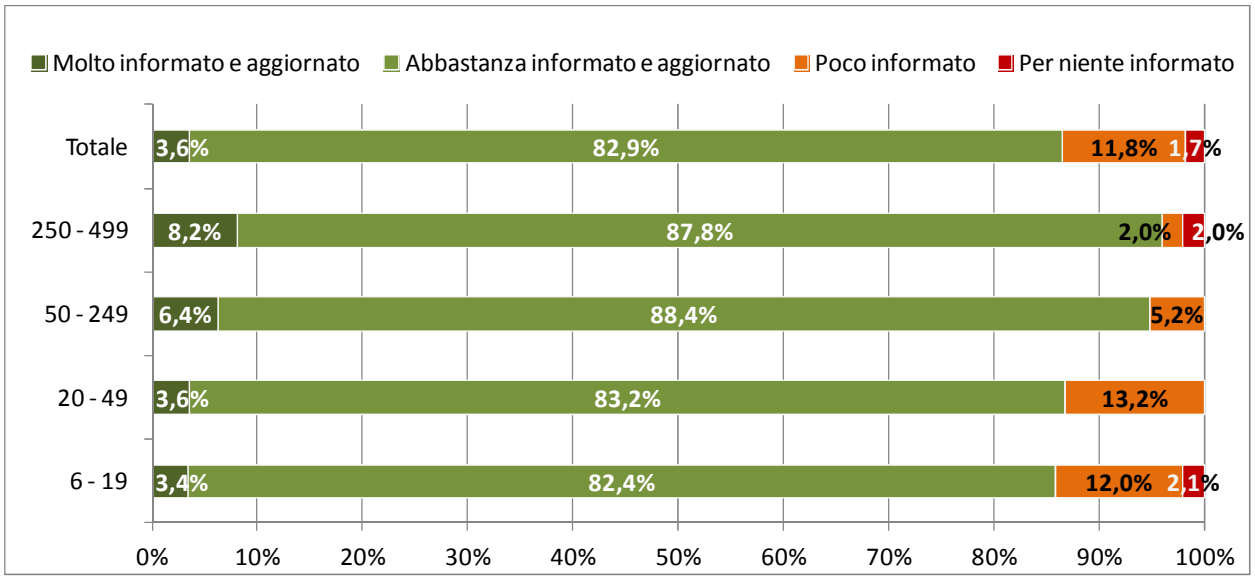
soprattutto negli ultimi tre anni, con il moltiplicarsi di attacchi eclatanti a livello globale (dalle minacce di Operation Aurora fino a Night Dragon e LURID), il tema della sicurezza informatica si è posto al centro dell'opinione pubblica mondiale.

Nonostante la grande attenzione della stampa specializzata e internazionale, lo sviluppo e la diffusione di una cultura aziendale legata alla sicurezza informatica ancora stenta a consolidarsi in alcuni comparti dell'economia, soprattutto nel segmento delle Piccole e Media Imprese (PMI). L'evidenza crescente dei rischi cui sono sottoposte le imprese di qualsiasi dimensione, soprattutto sul tema della vulnerabilità del software, sembra non incidere in misura sostanziale sulle policy di aggiornamento dei sistemi delle PMI, che ancora lavorano con sistemi che per quanto stabili ed efficienti dal punto di vista operativo di fatto risultano ampiamente superati dal punto di vista della sicurezza.

L'indagine ha approfondito una lista ampia e articolata di tematiche per comprendere la percezione della sicurezza IT nel segmento di imprese individuato nel campione di riferimento e comprendente una ampia parte delle PMI italiane, indagando il livello di consapevolezza rispetto al problema della sicurezza informatica, i canali di informazione attraverso i quali le imprese acquisiscono la nozione delle potenziali minacce e delle misure da intraprendere per difendersi, i veicoli di attacco attraverso i quali si percepisce la maggiore criticità in termini di rischio, il livello di organizzazione aziendale per gestire la sicurezza in modo strutturato, la presenza di programmi di informazione e sensibilizzazione per promuovere la diffusione di una cultura della sicurezza IT in azienda.

FIGURA 1

La conoscenza del tema della sicurezza per classe di addetti



Fonte: IDC, 2014 (n=850, dato totale estrapolato all'universo di riferimento; basi diverse per le classi dimensionali)

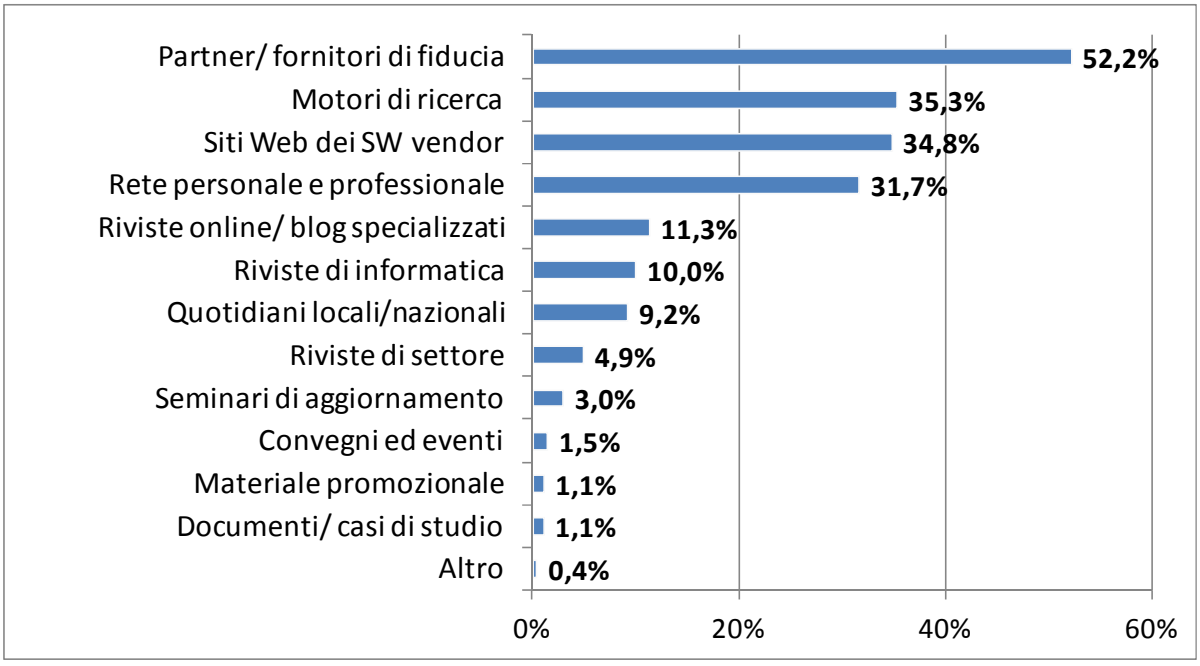
Dall'analisi dei risultati principali del survey, IDC stima che oltre l'86% delle imprese ritengano di disporre di un adeguato livello di conoscenza del tema della sicurezza

informatica (Fig. 1): le maggiori incertezze prevalgono nelle classi sotto i 50 addetti, dove emergono dubbi rilevanti rispetto al dominio del tematica, mentre sopra i 50 addetti le imprese raggiungono un livello di strutturazione tale per cui ritengono di dominare il problema senza incertezza a livello organizzativo. Osservando il dato per settori industriali emerge una maggiore attenzione da parte della Finanza e del Commercio: quando la sicurezza dei sistemi informativi può compromettere il core business aziendale la problematica viene interiorizzata nelle aziende in modo fisiologico.

Approfondendo l'indagine sui canali che determinano l'assimilazione delle problematiche della sicurezza (Fig. 2) appare evidente come il segmento esaminato faccia ampia affidamento sugli attori del canale per comprendere al meglio i rischi relativi alla sicurezza informatica: i partner e i fornitori di fiducia sono evidenziati al 52,2% con una variabilità assai limitata tra le classi dimensionali, mentre a livello di settori si osserva una maggiore predisposizione da parte dell'Industria rispetto agli altri comparti esaminati. Il carattere fiduciario del rapporto prevale nettamente su altri canali di informazione, come ad esempio la rete personale/ professionale (31,7%) mettendo in evidenza il valore saliente della relazione nell'affrontare un tema complesso e sensibile come la sicurezza informatica.

FIGURA 2

Canali di informazione sul tema della sicurezza



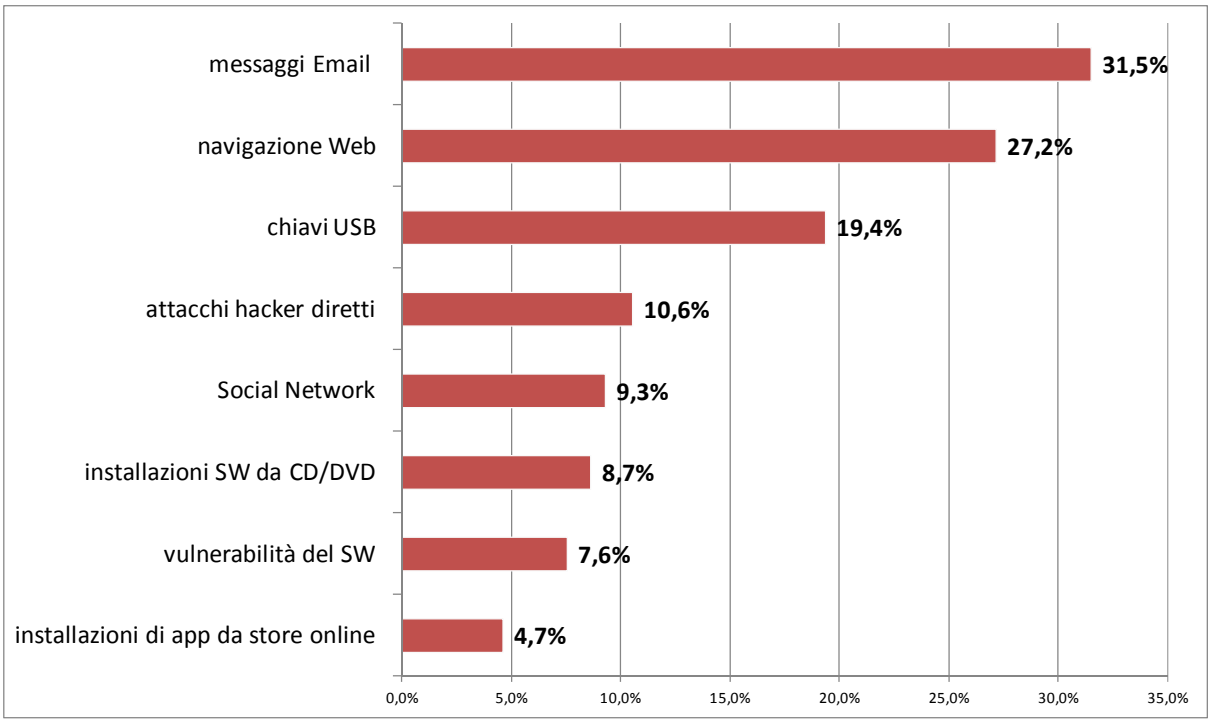
Fonte: IDC, 2014 (sottoinsieme del campione n=850, "solo se informati"; domanda a risposta multipla; dato estrapolato al sottoinsieme dell'universo di riferimento)

Una parte importante del mercato fa affidamento al Web per recuperare le informazioni essenziali per gestire il problema, sebbene anche in questo caso il tema dell'autorevolezza delle fonti sia comunque evidente (Sito Web dei Vendor della sicurezza 34,8%). Se non sorprende il dato assai basso relativo alla convegnistica, ai

casi studio e ai seminari di aggiornamento, che nel complesso appaiono come strumenti di comunicazione e di informazione che caratterizzano più propriamente il segmento Large Enterprise, appare senza dubbio allarmante l'impiego limitato delle riviste specialistiche, con un dato che oscilla tra il 4,9% e l'11,3%: in base a questi risultati diviene più che ragionevole chiedersi su quali basi le imprese ritengano di avere una buona conoscenza del tema della sicurezza come evidenziato nelle figure precedenti.

FIGURA 3

Fattori di rischio percepito rispetto a diversi veicoli di attacco



Fonte: IDC, 2014 (n=850, frequenza risposte rischio percepito >=7 in una scala da 1 a 10, dato totale estrapolato all'universo di riferimento; domanda a risposta multipla)

Al campione è stato chiesto di evidenziare su una scala da 1 a 10 la gravità del rischio percepito rispetto a diversi veicoli di attacco (Fig. 3). La maggior parte delle imprese ha messo in evidenza i fattori di rischio più comunemente conosciuti (messaggi email 31,5%, navigazione web 27,2%) come se le problematiche della sicurezza IT fossero rimaste sostanzialmente inalterate nell'ultimo decennio senza alcun cambiamento di sorta.

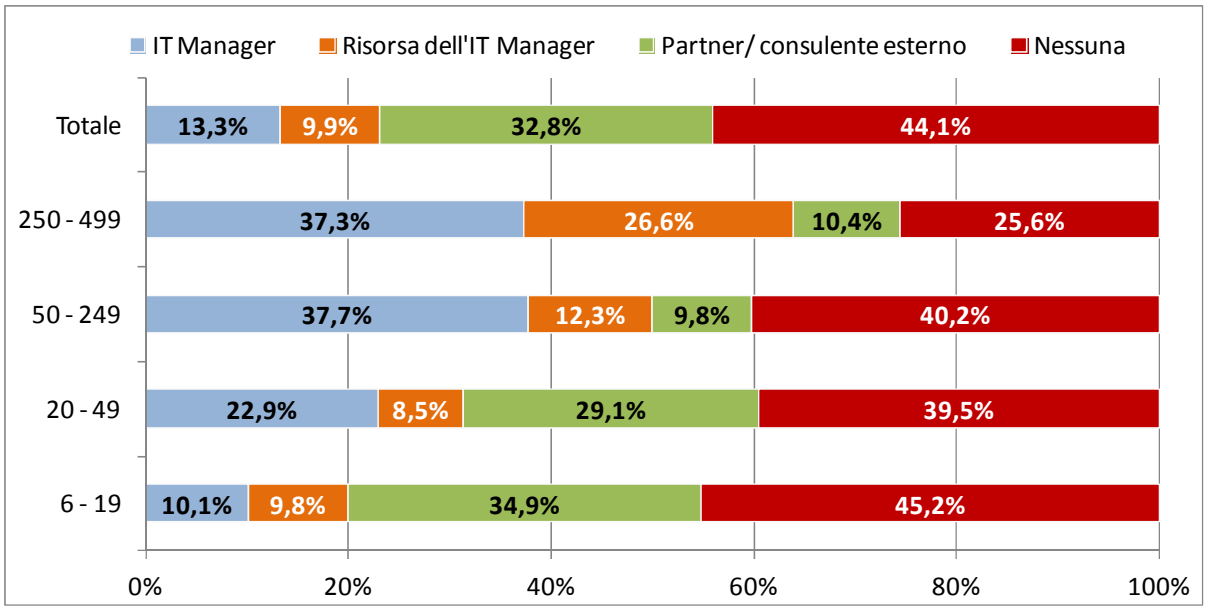
Risultano ampiamente sottostimati i fattori di rischio emergente, con particolare riferimento ai social network (9,3%) e alle installazioni di app da store online (4,7%). Interpretando il dato, abbastanza basso, relativo alla percezione dei rischi legati alla vulnerabilità software in relazione al tema dell'EoS Day di Windows XP si comprende la rilevanza dell'indagine nel suo impianto complessivo: la maggior parte del segmento PMI di fatto trascura in modo importante l'esposizione al rischio di attacchi derivanti da malware ed exploit zero-day che vanno sistematicamente ad incidere nel

corso del tempo sui punti deboli di qualsiasi sistema operativo. IDC stima che soltanto il 7,6% delle imprese comprende il rischio derivante dalle vulnerabilità software, esprimendo una visione complessiva della sicurezza informatica che è ormai del tutto superata dagli eventi.

Un altro aspetto messo in evidenza dall'indagine è la carenza a livello organizzativo (Fig. 4): il 44,1% delle imprese non dispongono di alcuna struttura per la gestione della sicurezza informatica e sono prive di referenti interni cui attribuire tale responsabilità. In questo scenario di concreta destrutturazione, il ruolo dei partner/ consulenti esterni (32,8%) risalta in modo particolare per colmare carenze e lacune che altrimenti sarebbero del tutto insanabili: infatti, soprattutto le imprese di dimensioni più modeste si avvalgono in misura sostanziale del contributo di consulenti esterni (34,9%), mentre le imprese di maggiori dimensioni dispongono di figure strutturate legate al dipartimento IT (IT Manager o risorse afferenti all'IT Manager nel 63,9% dei casi per le imprese tra 250 e 499 addetti).

FIGURA 4

La figura responsabile della sicurezza informatica per classe di addetti



Fonte: IDC, 2014 (n=850, dato totale estrapolato all'universo di riferimento; basi diverse per le classi dimensionali)

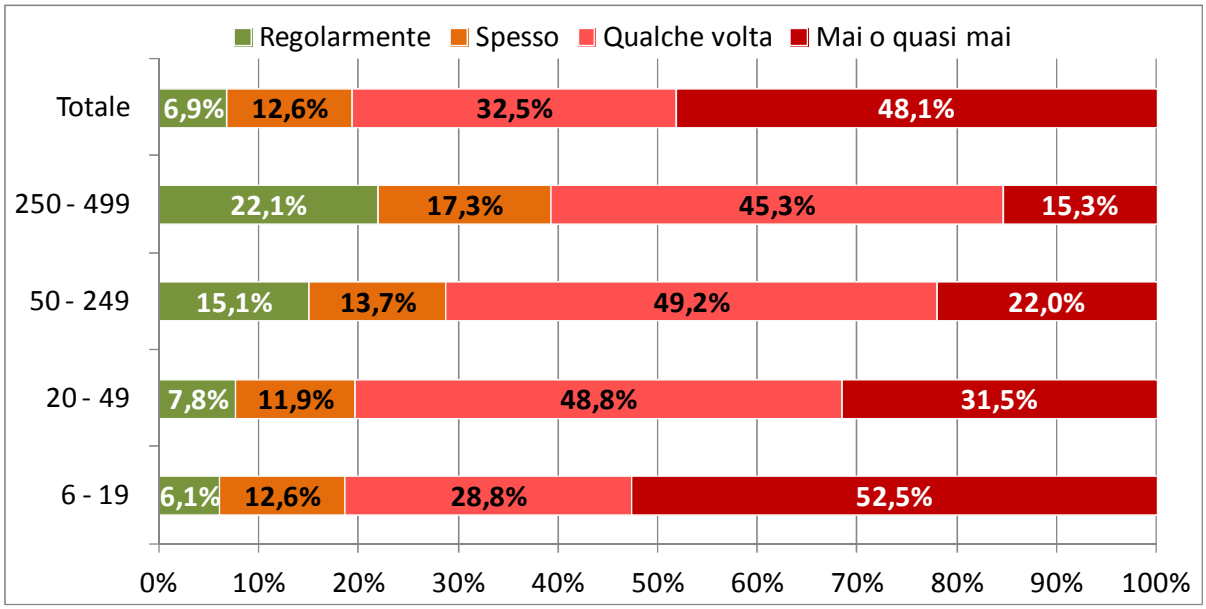
Considerando un simile scenario organizzativo, qualsiasi strategia per lo sviluppo di una cultura della sicurezza informatica rischia di confrontarsi con l'assenza quasi totale, soprattutto nelle imprese di dimensioni più limitate, di interlocutori aziendali capaci di farsi carico non soltanto dell'implementazione di policy o soluzioni specifiche, ma perfino di una più semplice azione di sensibilizzazione della cultura aziendale. Infatti, la frequenza di iniziative specifiche di formazione per la sicurezza informatica (Fig. 5) è del tutto nulla nel 48,1% delle imprese, con un evidente effetto di correlazione con la dimensione aziendale (nelle imprese con meno di 20 addetti si arriva al 52,5%). A una analisi per settore industriale emergono differenze meno

significative: nei settori caratterizzati da una notevole intensità di informazione, come Servizi & TCU, prevale una maggiore attenzione al tema delle iniziative di sensibilizzazione mentre in altri comparti, come il Commercio, la distanza appare lontanissima.

Dunque, la (presunta) conoscenza dei problemi relativi alla sicurezza informatica, così come evidenziato nella Fig. 1, si confronta con una realtà che appare ben diversa: la percezione effettiva dei rischi informatici sembra fondata su uno scenario che è quello del decennio passato, i canali di informazione e aggiornamento sono limitati e ampiamente basati su esperti esterni, il livello di organizzazione aziendale per gestire il problema è pressoché elementare. In questo scenario di grande fragilità della sicurezza informatica delle PMI si introduce una ulteriore variabile che rende ancora più complesso il quadro generale e che risulta pericolosamente sottovalutato da molte imprese: la fine del supporto tecnico su Windows XP.

FIGURA 5

La frequenza delle iniziative di sensibilizzazione sulla sicurezza per classe di addetti



Fonte: IDC, 2014 (n=850, dato totale estrapolato all'universo di riferimento; basi diverse per le classi dimensionali)

Lo scenario di adozione di WinXP precedente all'EoS Day

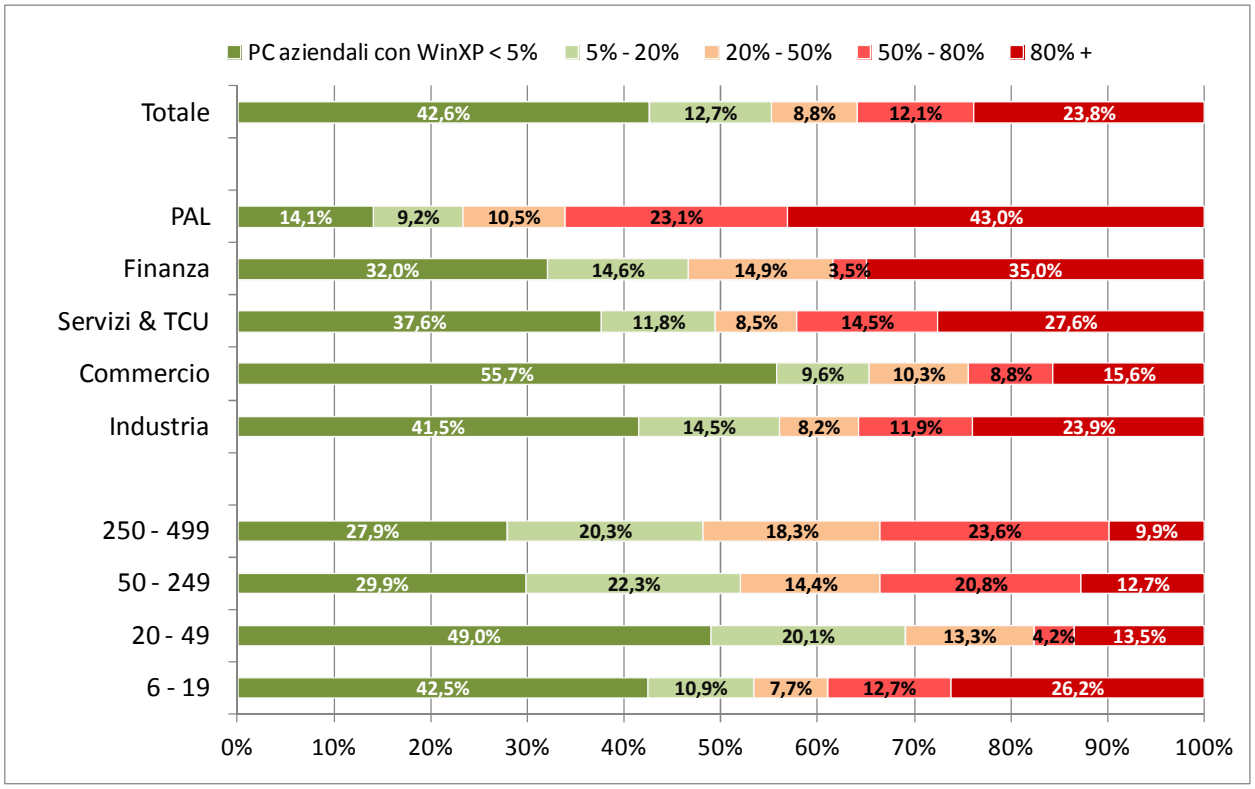
Come largamente anticipato attraverso i media e i mezzi di informazione, dopo oltre un decennio, l'8 aprile 2014 (EoS Day) Microsoft terminerà ufficialmente il supporto sul sistema Windows XP: oltre tale data non saranno più disponibili né gli aggiornamenti automatici sulla sicurezza né il download di Microsoft Security Essentials. Coloro che avranno già installato Microsoft Security Essentials continueranno a ricevere aggiornamenti per le signature anti-malware per un periodo

limitato senza comunque alcuna garanzia sulla protezione complessiva del sistema operativo Windows XP.

Oltre ad approfondire la percezione della sicurezza informatica da parte del segmento esaminato, nella seconda parte dell'indagine si è cercato di evidenziare lo scenario di adozione di Windows XP antecedente all'EoS Day, determinando l'ampiezza del parco installato su Windows XP, la conoscenza del termine di scadenza, la disponibilità di piani di aggiornamento del parco macchine entro tale termine, le motivazioni per rimanere operativi su Windows XP affrontando i rischi di vulnerabilità del software, raccogliendo attraverso un complesso di elementi che consentono di presagire un ulteriore indebolimento della sicurezza informatica delle PMI.

FIGURA 6

La base installata di PC aziendali con Windows XP, per settore e classe di addetti



Fonte: IDC, 2014 (n=850, dato totale estrapolato all'universo di riferimento; basi diverse per le classi settoriali/ dimensionali)

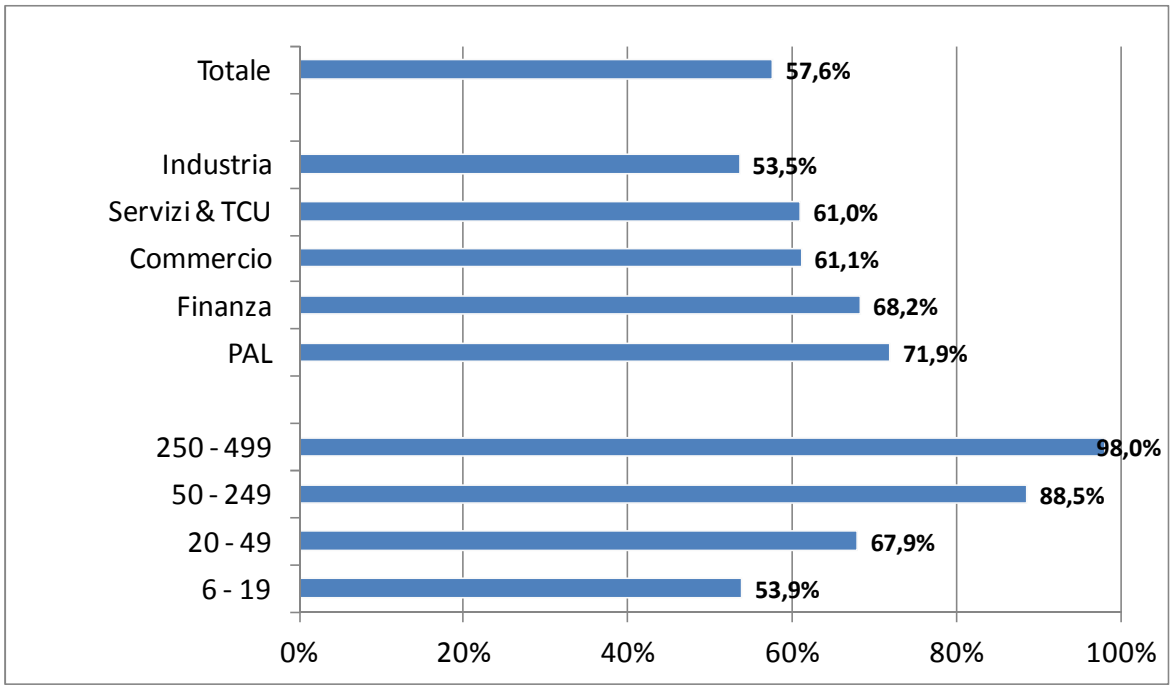
Dall'indagine emerge quanto il sistema operativo Windows XP sia ancora profondamente radicato nel tessuto imprenditoriale italiano: nel segmento esaminato dalla ricerca IDC, il 35,9% delle imprese dispone di un parco PC aziendali che per oltre il 50% lavora ancora stabilmente su Windows XP, nel caso del 23,8% delle imprese il parco macchine aziendali basato su XP sale a oltre l'80% (Fig. 6). Approfondendo l'analisi per classe addetti, si osserva una evidente correlazione del fenomeno rispetto a fattori dimensionali: salvo rare eccezioni, le imprese di maggiori dimensioni si sono già ampiamente svincolate da Windows XP, mentre le imprese di

modeste dimensioni fanno ancora largo affidamento su questo sistema operativo (più dell'80% dei PC nel 26,2% delle imprese nella classe tra 6 e 19 addetti). L'interpretazione del dato a livello settoriale mette in evidenza una sostanziale dipendenza della PAL (43%) e della Finanza (35%); le ragioni sono senza dubbio diverse: da una parte la carenza di disponibilità per gli investimenti nella pubblica amministrazione, dall'altra la persistenza di un legacy sviluppato ad-hoc per rispondere alle esigenze del settore finanziario in molte occasioni diventa un ostacolo al rinnovo dei sistemi.

Il profondo radicamento di Windows XP nel segmento delle PMI, maturato in oltre un decennio di successo commerciale, rappresenta lo scenario in cui andare a contestualizzare l'atteggiamento del mercato rispetto all'EoS Day. Nel corso degli ultimi mesi Microsoft ha già sviluppato una campagna di comunicazione che andrà ulteriormente intensificandosi nelle prossime settimane per informare dei rischi, e delle opportunità, che deriveranno dalla fine del supporto su Windows XP. Dall'indagine (Fig. 7) emerge con chiarezza che una parte importante del mercato ha già ricevuto notizia dell'imminente discontinuità del supporto su Windows XP (57,6%): come ovvio il fattore dimensionale incide sensibilmente rispetto all'attenzione prestata a queste scadenze, maggiormente accentuata nelle realtà di maggiori dimensioni.

FIGURA 7

La conoscenza del termine del supporto su Windows XP, per settore e classe di addetti



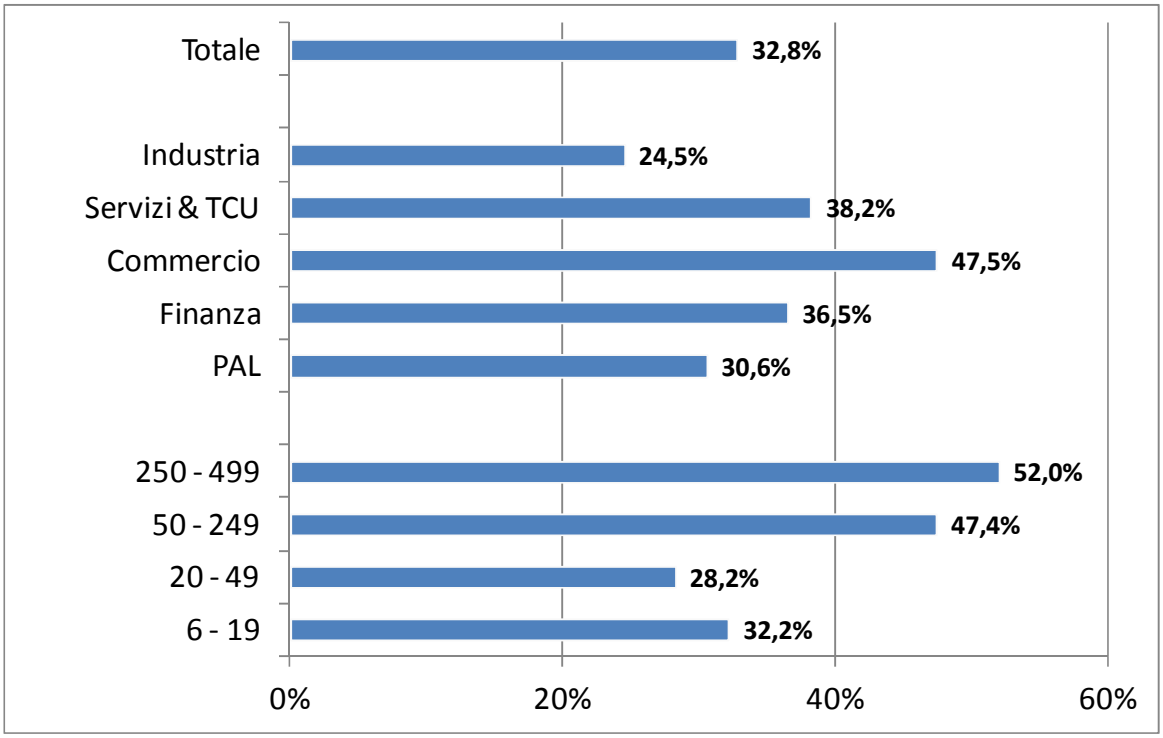
Fonte: IDC, 2014 (n=850, dato totale estrapolato all'universo di riferimento; basi diverse per le classi dimensionali/ settoriali)

Dalla conoscenza dell'EoS Day non discende necessariamente una puntuale pianificazione per gestire l'avvicendamento dei sistemi entro il termine previsto (Fig. 8): soltanto il 32,8% delle imprese con un parco di PC su Windows XP superiore al

20% ha in programma di aggiornare le proprie macchine entro la scadenza del supporto, un dato che mette in evidenza come una ampia parte delle imprese stia pericolosamente sottovalutando il carattere sistemico dei rischi legati alla sicurezza informatica (il tipico ragionamento della PMI: sono troppo piccola per essere un bersaglio di qualche interesse … senza però rendersi conto che i propri PC possono diventare strumento per portare attacchi su altri bersagli oppure senza considerare che la disponibilità di strumenti di hacking è ormai alla portata di qualsiasi individuo, anche senza competenze tecniche avanzate).

FIGURA 8

Piano di aggiornamento dei PC con Windows XP pre-EoS Day, per settore e classe di addetti



Fonte: IDC, 2014 (sottoinsieme del campione n=850, solo se WinXP > 20% dei PC aziendali; dato totale estrapolato al sottoinsieme dell'universo di riferimento, basi diverse per le classi dimensionali/ settoriali)

Le imprese di maggiori dimensioni hanno senza dubbio maggiore percezione dei rischi economici legati alla sicurezza informatica e dunque prestano grande attenzione al tema dell'aggiornamento dei sistemi prima della scadenza dell'8 aprile 2014 (52% nella classe 250-499 addetti). A un esame del dato per settore si osserva invece come la PAL (30,6%) e l'Industria (24,5%) siano i settori meno orientati a gestire l'aggiornamento dei sistemi prima dell'EoS Day, mentre il Commercio esprime il maggiore dinamismo sotto questo punto di vista (47,5%). In settori come l'Industria, la Finanza e la PAL, dove il livello di informazione è alto, il parco installato su Windows XP considerevole, e allo stesso tempo la pianificazione degli aggiornamenti abbastanza limitata, IDC ritiene che in molti casi si venga a determinare quella

nozione illusoria di sicurezza che è stata disegnata nella sezione precedente dell'indagine.

Un breve approfondimento dei dati a livello geografico

Sebbene la ricerca non si sia focalizzata nell'approfondimento delle dinamiche a livello territoriale, con le informazioni raccolte attraverso il questionario è stato possibile trarre alcune considerazioni generali sulla forma assunta dai fenomeni esaminati a livello di macro aggregazione geografica e alcune aree locali (con una precisione della misura inferiore rispetto a una interpretazione basata esclusivamente sulle dimensioni di campionamento).

Se si approfondisce a livello territoriale il dato relativo alla base installata di Windows XP antecedente all'EoS Day, si osserva che la maggiore attestazione si trova nel Sud e nelle Isole (33,7% delle imprese dell'area ha una base installata superiore all'80% delle macchine), seguita dal Centro (30,7%), dal Nord Est (18,6%) e dal Nord Ovest (18,5%). In regioni come la Lombardia, lo stesso dato scende al 17,3%, mentre in regioni come la Puglia il dato sale al 54,1%.

Illustrando secondo la medesima lente di ingrandimento il dato relativo ai piani di aggiornamento delle macchine prima dell'EoS Day, il Nord Ovest si evidenzia come l'area che guida il processo di rinnovamento dei sistemi (44% delle imprese prevede di aggiornare prima della scadenza), seguito dal Nord Est (36,4%), dal Sud e dalle Isole (22,7%), mentre il Centro appare in ritardo (14,8%). In regioni come la Lombardia, lo stesso dato sale al 50,2%, mentre in regioni come la Puglia il dato scende all'8,7%.

Le nuove tecnologie e gli investimenti in sicurezza

Nel momento in cui una pletora di nuovi dispositivi raggiunge i sistemi informativi delle imprese, la gestione della sicurezza informatica diventa un processo che richiede necessariamente un approccio integrato e una strategia complessiva, non soltanto nella gestione degli aggiornamenti delle varie applicazioni ma soprattutto in una gestione razionale della varietà del ciclo di vita di differenti prodotti, non tutti necessariamente allo stesso grado di maturazione e sviluppo, per evitare di esporre i sistemi a possibili attacchi. Pur comprendendo la grande complessità del problema della vulnerabilità software quando si considerano le interazioni tra sistemi diversi, nella terza parte dell'indagine si è cercato di raccogliere almeno a livello generale alcuni elementi per valutare come la percezione della sicurezza delle PMI stia evolvendo nell'incontro con i nuovi dispositivi mobili, ad esempio i tablet, che si stanno spingendo sempre più in profondità anche in ambito aziendale.

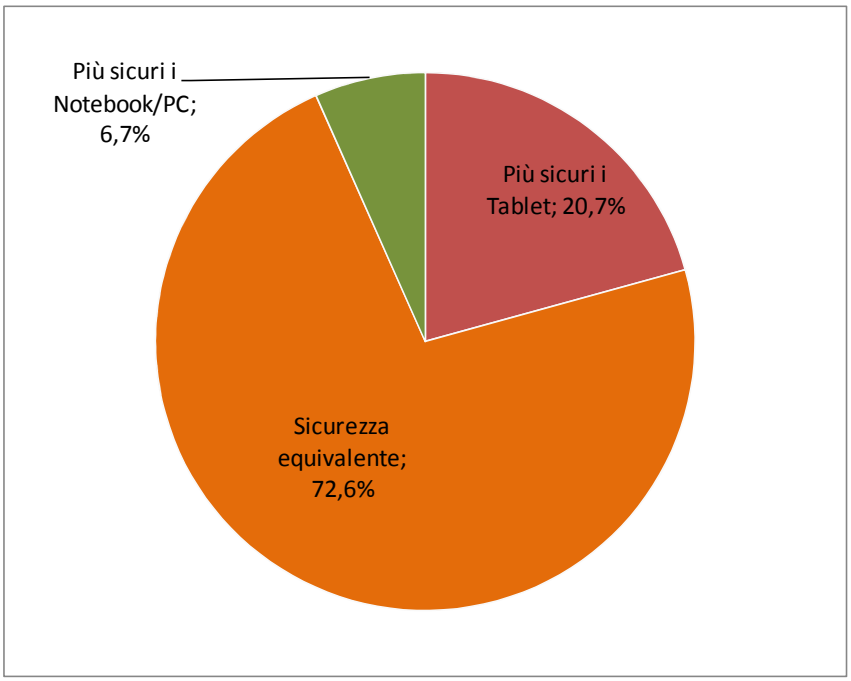
Nel perimetro di campionamento analizzato nel corso della ricerca e costituito in larga misura da PMI e da una parte di grande impresa, l'indagine evidenzia un notevole livello di diffusione (21,6%) dei tablet con sistema operativo Android, IoS e Windows: l'impiego dei nuovi dispositivi in azienda per la gestione delle attività di base di desktop automation e la vendita è un fatto consolidato in un numero sempre

maggiore di imprese. L'adozione dei tablet dipende chiaramente da fattori dimensionali (nella classe tra 50 e 249 addetti si arriva a un tasso di adozione del 47,4%, mentre nella classe tra 6 e 19 addetti non supera il 18,3%) e dipende anche in misura rilevante da logiche specifiche del settore (nei Servizi si arriva fino al 29,5%, mentre nella PAL non si raggiunge neanche il 5%).

Nel corso dell'indagine si è chiesto di confrontare il livello di sicurezza percepito rispetto ai tablet con quello relativo ai tradizionali Notebook/ PC con risultati nel complesso abbastanza sorprendenti (Fig. 9): nonostante la stampa specializzata e diversi osservatori della sicurezza informatica da diversi anni mettano in evidenza l'intrinseca vulnerabilità dei tablet, soprattutto di sistemi aperti come Android, presentando una ampia aneddotica di attacchi che hanno coinvolto tali sistemi negli ultimi anni, il segmento di mercato coinvolto nella ricerca ritiene i rischi che si corrono impiegando i nuovi dispositivi in larga misura del tutto equivalenti ai Notebook/ PC (72,6%). Tali valutazioni sono del tutto coerenti con la cultura complessiva della sicurezza espressa dal segmento PMI, come evidenziato nella prima sezione della ricerca, in particolare con riferimento ai fattori di rischio percepito (Fig. 3), dove soltanto il 4,7% delle imprese evidenzia un rischio specifico riconducibile all'installazione di applicazioni dagli store online. Nel nuovo ambiente IT che viene configurandosi attorno a dispositivi sempre nuovi e nuovi sistemi operativi, le PMI rischiano concretamente di confrontarsi con problematiche di sicurezza che non riescono ancora a percepire chiaramente, esponendosi a rischi economici che vanno dalla sottrazione di informazioni sensibili fino al fermo dei sistemi.

FIGURA 9

La percezione della sicurezza dei dispositivi mobili

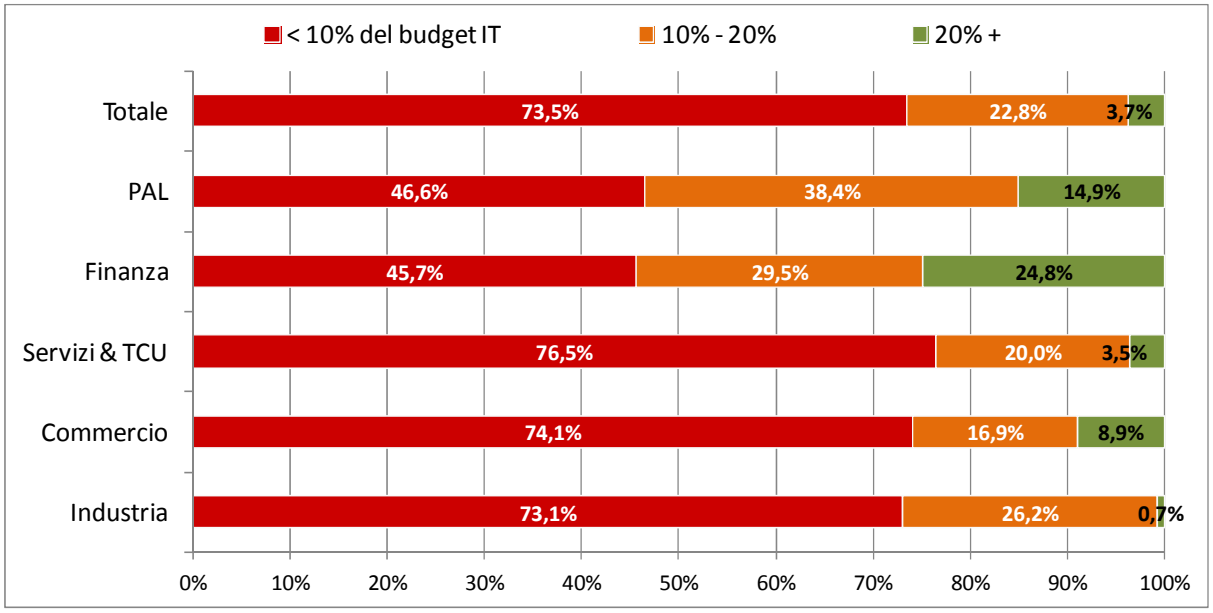


Fonte: IDC, 2014 (sottoinsieme del campione n=850, "solo se utilizzano almeno un tablet"; dato estrapolato al sottoinsieme dell'universo di riferimento)

Nonostante la complessità dei rischi degli scenari emergenti, la necessità di tutelare la propria azienda perseguendo una strategia di investimento specifico nella sicurezza informatica deve ancora fare molta strada nelle PMI. La ristrettezza dei budget disponibili per le infrastrutture informatiche, in parte determinata da fattori esogeni come la pressione generale della crisi economica sulle imprese, in parte determinata da fattori culturali endogeni come evidenziato nella prima sezione della ricerca, di fatto impone un vincolo insuperabile alle potenzialità di espansione della spesa per la sicurezza informatica, soprattutto per le PMI (Fig. 10).

FIGURA 10

La spesa IT destinata alla sicurezza nei prossimi 12 mesi per settore



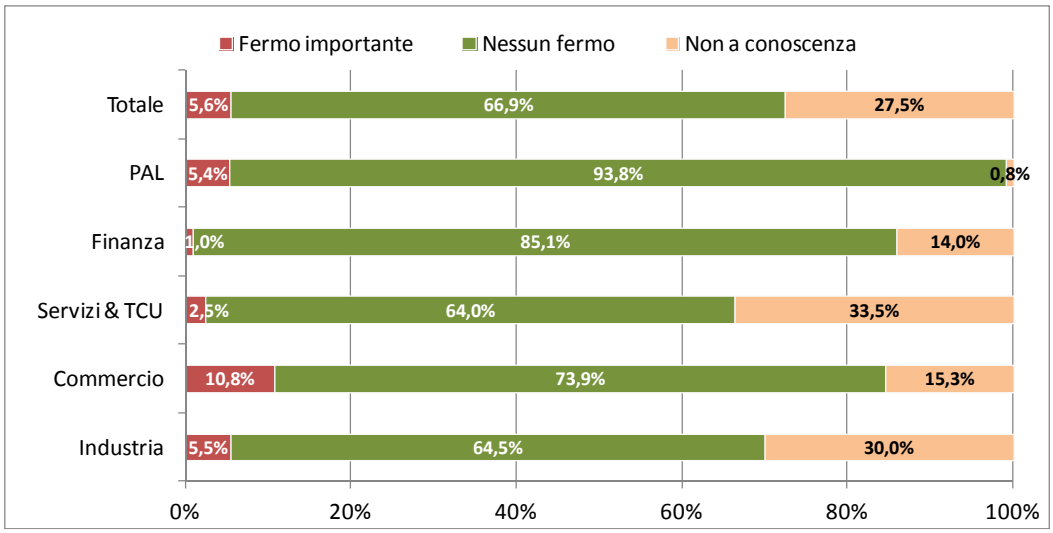
Fonte: IDC, 2014 (n=850, dato totale estrapolato all'universo di riferimento; basi diverse per le classi settoriali)

La maggior parte delle imprese (73,5%) destina soltanto una percentuale inferiore al 10% del proprio budget IT alla gestione della sicurezza, con risvolti diversi se si approfondisce il dato a livello settoriale: i settori che hanno ragioni politico-strategiche (PAL) oppure economico-finanziare (Finanza) per tutelare i propri interessi sono pronti a investire anche a due cifre nei prossimi dodici mesi, mentre altri comparti come i Servizi e il Commercio sono portati soltanto in rarissime occasioni a procedere a investimenti più significativi nella sicurezza informatica.

APPENDICE

FIGURA 11

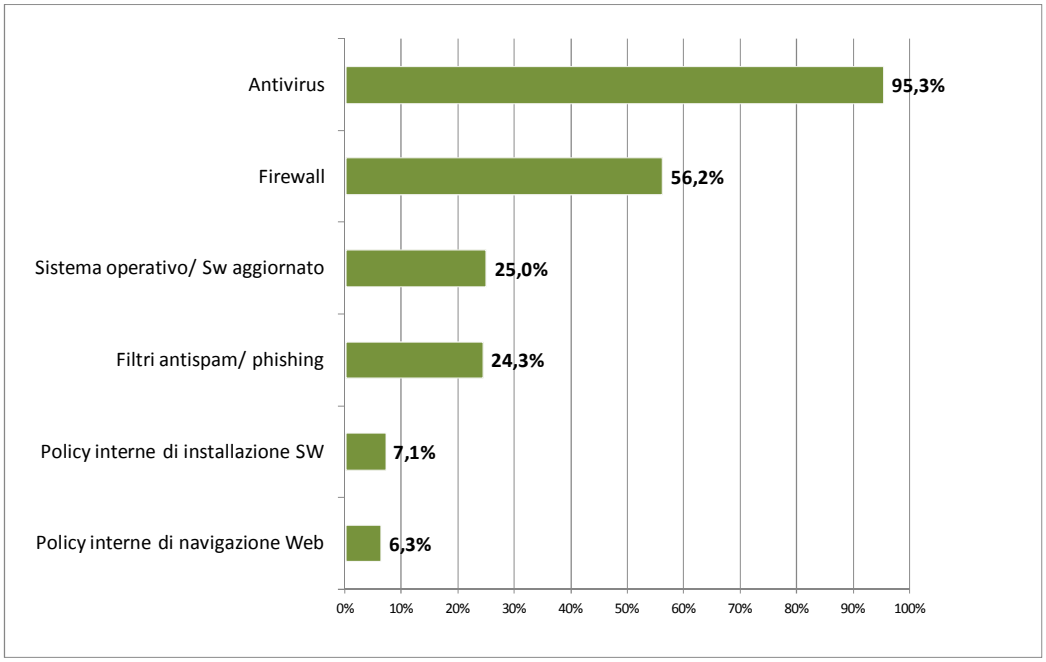
Esperienza di un fermo importante dei sistemi dovuto a minacce informatiche di varia natura, per settore



Fonte: IDC, 2014 (n=850, dato totale proiettato sull'universo di riferimento; basi diverse per le classi settoriali)

FIGURA 12

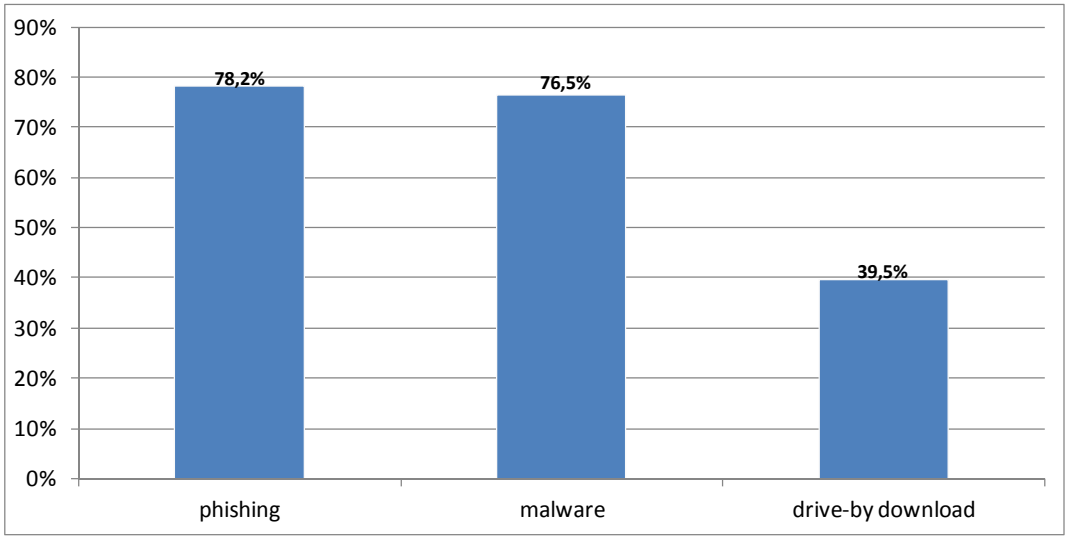
Percezione dell'utilità degli strumenti di protezione e prevenzione



Fonte: IDC, 2014 (n=850, dato totale proiettato sull'universo di riferimento; domanda a risposta multipla)

FIGURA 13

Conoscenza di termini tecnici



Fonte: IDC, 2014 (n=850, dato totale proiettato sull'universo di riferimento; domanda a risposte multiple)