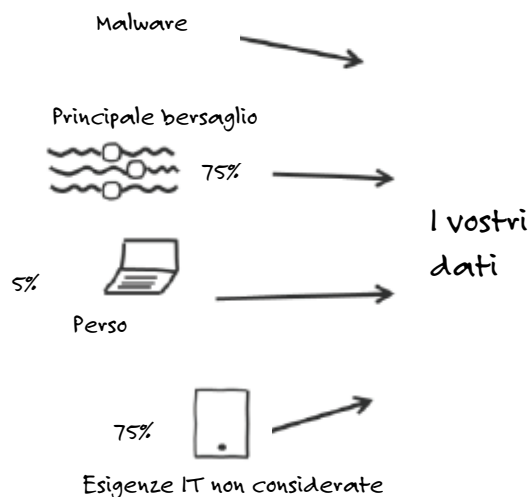


*Eliminare le falle nell'approccio  
alla sicurezza*

**KASPERSKY** lab

## Come risultano protetti i vostri dati contro gli attacchi di hacker e cybercriminali?

Da una ricerca condotta lo scorso anno dall'unità di analisi di Verizon Communications Inc., è emerso che il 77% delle violazioni dei dati prese in considerazione ha interessato aziende con un massimo di 1.000 dipendenti.<sup>1</sup>



Tuttavia, l'85% dei titolari di piccole aziende ritiene poco probabile il verificarsi di una violazione dei dati e, per quanto la cosa possa sembrare preoccupante, molti di loro non implementano affatto misure di sicurezza finalizzate a proteggere i dati di clienti e dipendenti.<sup>2</sup>

Il rischio di minacce malware sta aumentando in maniera esponenziale. I cybercriminali stanno sferrando attacchi ad aziende come la vostra anche sfruttando nuovi vettori, oltre a quelli già utilizzati. Il principale bersaglio dei cybercriminali di oggi è rappresentato dalle vulnerabilità non ancora corrette presenti nel codice delle applicazioni, che possono essere sfruttate attraverso il malware.

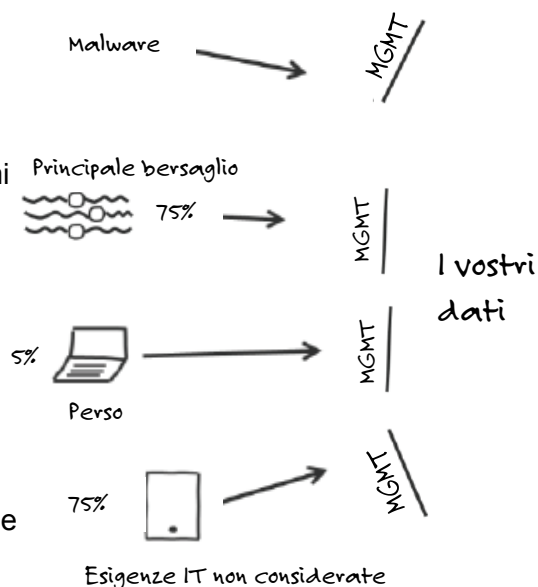
Di fatto, il 75% di tutte le vulnerabilità soggette ad attacchi è presente in applicazioni PDF, IE e Java.

D'altro canto, le aziende devono supportare una forza lavoro sempre più mobile e grandi volumi di dati disseminati su laptop, smartphone, tablet e altri dispositivi portabili. Tali dati, inoltre, non sono sicuri come potreste pensare. In base a una ricerca condotta da Intel, il 5-10% di tutti i laptop verrà smarrito o rubato nel corso del proprio ciclo di vita utile e il 75% dei dipendenti ha scelto i dispositivi mobili senza prendere minimamente in considerazione le esigenze relative alla gestione o alla sicurezza dell'IT.<sup>3</sup>

### Come gestite tutti questi vettori di minaccia?

Sicuramente avrete già acquistato un'efficace soluzione antivirus che funge da base per la vostra strategia di protezione. Tuttavia, per gestire tutti questi nuovi vettori, avrete bisogno anche di un soluzione di gestione dei sistemi in grado di correggere le vulnerabilità presenti nelle vostre applicazioni, nonché di uno strumento di crittografia che vi consenta di proteggere i dati dei laptop e di uno strumento per la gestione dei dispositivi mobili che ne assicuri la protezione. Tutto ciò si traduce in quattro, o forse anche più, processi di valutazione e in altrettante console di gestione, oltre che nell'esigenza di gestire un'ampia serie di criteri. Inoltre, subirete un inevitabile calo del livello di efficienza della vostra attività e dovrete incrementare tanto le iniziative di formazione che l'attività di supporto, con un inevitabile aumento dei costi da sostenere.

Il fattore più importante, nonostante tutti questi strumenti a vostra disposizione, è che continuerete ad avere un problema di sicurezza.

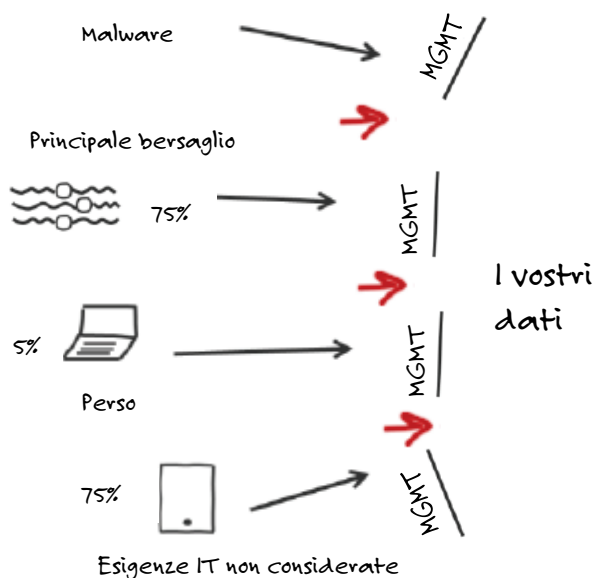


<sup>1</sup> Cybercriminals Sniff Out Vulnerable Firms, The Wall Street Journal, 5 luglio 2012

<sup>2</sup> Small Business Data Protection Survey, The Hartford

<sup>3</sup> Forrsights Workforce Employee Survey, 2° trimestre 2012, Forrester Research Inc., 2012

## Il vostro approccio di sicurezza complessivo continua a presentare falle:



- ✓ priorità non definite per le patch
- ✓ numerosi set di criteri da gestire
- ✓ numerosi sistemi non progettati per essere interoperabili

Di fatto, i professionisti della sicurezza IT dichiarano che una delle principali sfide che si ritrovano puntualmente ad affrontare è la mancanza di interoperabilità tra i sistemi di sicurezza.

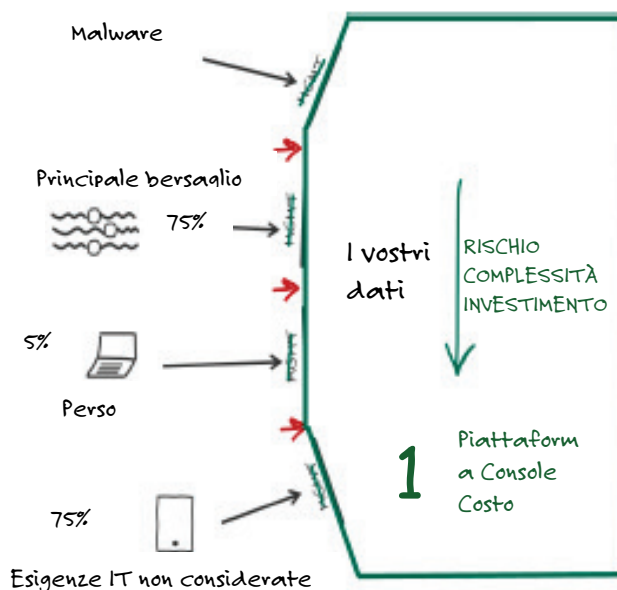
La principale sfida da affrontare al momento non è la carenza di strumenti disponibili, bensì il fatto che l'uso di strumenti separati contribuisce a rendere sempre più complicata l'implementazione dei vostri criteri di sicurezza. **Inoltre, la complessità è nemica della sicurezza.**

**Che ne pensate di poter ridurre il numero di strumenti da utilizzare e delle console da gestire, continuando ad usufruire del livello di sicurezza desiderato?**

Le soluzioni di Kaspersky vi offrono il livello di sicurezza necessario per risolvere le falle del vostro approccio di sicurezza, a fronte di meno strumenti da gestire.

Solo Kaspersky fornisce una **piattaforma completa e totalmente integrata** in grado di garantire una protezione anti-malware di livello impareggiabile, potenti strumenti di controllo delle applicazioni, tecnologia di gestione dei sistemi, funzionalità di crittografia e Mobile Device Management, tutti gestiti da un'**unica console e disponibili al costo di un unico prodotto**.

Non si tratta semplicemente di una serie di soluzioni riunite insieme per essere proposte sotto forma di "suite", bensì di una piattaforma realmente unificata che vi consente di identificare i potenziali rischi esistenti in tutti i vostri sistemi ed endpoint e di applicare costantemente i criteri in modo uniforme, permettendovi di allineare l'approccio di sicurezza agli obiettivi aziendali.



## **Un'unica piattaforma! Un'unica console! Un unico costo!**

Sarete pertanto in grado di ridurre i rischi per i vostri dati, la complessità degli strumenti di sicurezza utilizzati e l'entità degli investimenti da sostenere.

Quale può essere quindi la vostra prossima mossa?

### **Visitate il sito [www.kaspersky.it/beready](http://www.kaspersky.it/beready)**

- Guardate l'intero [video sulla storia di Kaspersky](#)
- Scoprite ulteriori informazioni sulla [piattaforma Kaspersky Endpoint Security](#)
- Contattate un rappresentante di vendita Kaspersky oggi stesso