Datacenter & Cloud Security Survey 2018

Novembre 2018

A cura di: Elena Vaciago,

Associate Research Manager, The Innovation Group

Questa Ricerca è stata realizzata con la Sponsorship della società di Cybersecurity

Bitdefender®

The Innovation Group
Innovating business and organizations through ICT

Executive Summary /1

Datacenter & Cloud Security Survey: la Digital Transformation richiede un ripensamento della sicurezza cyber.

Le aziende stanno oggi affrontando numerose criticità per far fronte alle nuove sfide di cybersecurity. Non solo gli attaccanti fanno evolvere continuamente le proprie tecniche di hacking: sono anche le infrastrutture ICT delle aziende che si modificano, in un percorso di trasformazione del datacenter verso i nuovi modelli software-defined, verso un maggiore utilizzo del cloud e una maggiore presenza di ambienti virtuali, ibridi e convergenti. Come emerge dalla "***Datacenter & Cloud Security Survey***" di The Innovation Group, che tra luglio e ottobre 2018 ha riguardato un campione di 70 aziende medio grandi, dei diversi settori, analizzando nello specifico le risposte di Manager IT e della Sicurezza ICT, la consapevolezza dell'importanza di preservare la sicurezza delle infrastrutture (dalla rete, al data center, agli endpoint, device mobile, le applicazioni web) è molto elevata.

È fondamentale però ripensare la propria strategia di difesa, per potersi avvantaggiare in modo sicuro delle nuove opportunità legate alla trasformazione digitale in corso. **Quali sono oggi le nuove sfide e le minacce più importanti da considerare?**

Al primo posto le aziende posizionano il tema degli attacchi avanzati, che sono in grado di evadere le misure tradizionali di sicurezza e avere impatti molto gravi per il business. Al secondo posto, il fatto che un utilizzo sempre più spinto del cloud comporta nuovi rischi, alcuni ancora sconosciuti, e in terza battuta, la necessità di tenere sotto controllo una superfice più ampia – con un numero maggiore di device e ambienti eterogenei – e quindi un'accresciuta complessità sul fronte della gestione.

Executive Summary /2

Proprio in risposta al tema della complessità di gestione, tra le principali qualità di una soluzione di security i rispondenti apprezzano la possibilità di integrare la soluzione in modo agevole (57% delle risposte); inoltre, cercano soluzioni nuove a minacce avanzate (48% delle risposte); affidabilità della soluzione (43%); gestione unificata (39%); offerta di sicurezza integrata nel cloud (36%). Il discorso del ROI (return of investment) non viene visto come prioritario, data l'attuale difficoltà di misurare questo investimento (20%). Anche la protezione degli ambienti virtuali non è vista come prioritaria: si assume (a torto) che questi ambienti siano solidi dal punto di vista della sicurezza (20%).

Trasformazione digitale significa anche maggiori criticità di sicurezza per gli Endpoint (PC, Tablet).

I vettori d'attacco per colpire questi device sono molteplici, la sicurezza deve quindi riguardare numerosi aspetti e possibili minacce: si va dal furto di credenziali e al Phishing (considerati i principali rischi cyber per questi device, 77% e 72% delle risposte) allo sfruttamento di vulnerabilità note (51%), attacchi tramite browser (43%), infezioni da altri device che entrano in contatto con l'Endpoint (32%). Rispondendo alla domanda successiva, che chiede quali incidenti hanno riguardato gli Endpoint nell'ultimo anno, il 65% degli intervistati ammette di averne subiti, in prevalenza dei primi due tipi, Phishing e Furto di credenziali.

Il tema del cloud, anche se oggi si osserva un'adozione ancora parziale di questi ambienti, può rappresentare un problema: dall'indagine si evince infatti che le aziende cominciano ad avere incidenti informatici anche per ambienti di Private cloud (9% degli intervistati li hanno subiti nell'ultimo anno), Public cloud (9%) e Hybrid cloud (12%).

Executive Summary /3

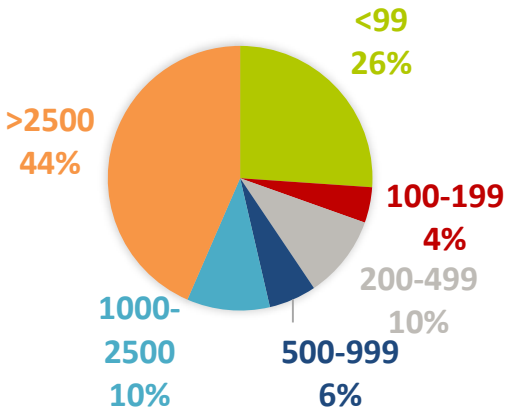
La consapevolezza sui problemi del cloud è un ambito che andrà monitorato nei prossimi anni, perché ancora poco maturo. Al momento, con riferimento alle possibili minacce avvertite per il cloud, ai primi posti si conferma il tema dell'accesso (80% delle risposte), che può avvenire da parte di estranei o di device usati dagli utenti senza un controllo dell'azienda. Si hanno poi problematiche di mancanza di visibilità, e quindi di compliance/mancanza di controllo su aspetti gestiti dal provider (come la localizzazione dei dati). Problematiche come la configurazione errata o i downtime sono indicate da una minoranza di aziende. C'è nel complesso una percezione positiva sulla capacità dei cloud provider di rispondere alle più comuni minacce cyber.

Sezioni della Survey

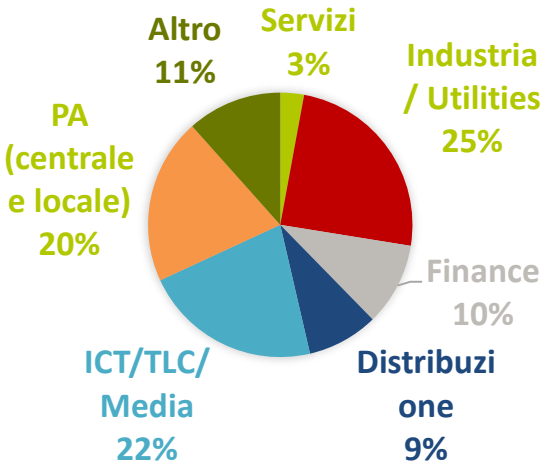
1. *Caratteristiche del Campione della Survey*
2. *Proteggere il Datacenter che cambia*
3. *Quali sono i requisiti di sicurezza prioritari per Datacenter e Cloud*
4. *Proteggere gli Endpoint dell'azienda*
5. *Protezione degli ambienti Cloud*

Caratteristiche del Campione /1

DIMENSIONE DELL'AZIENDA



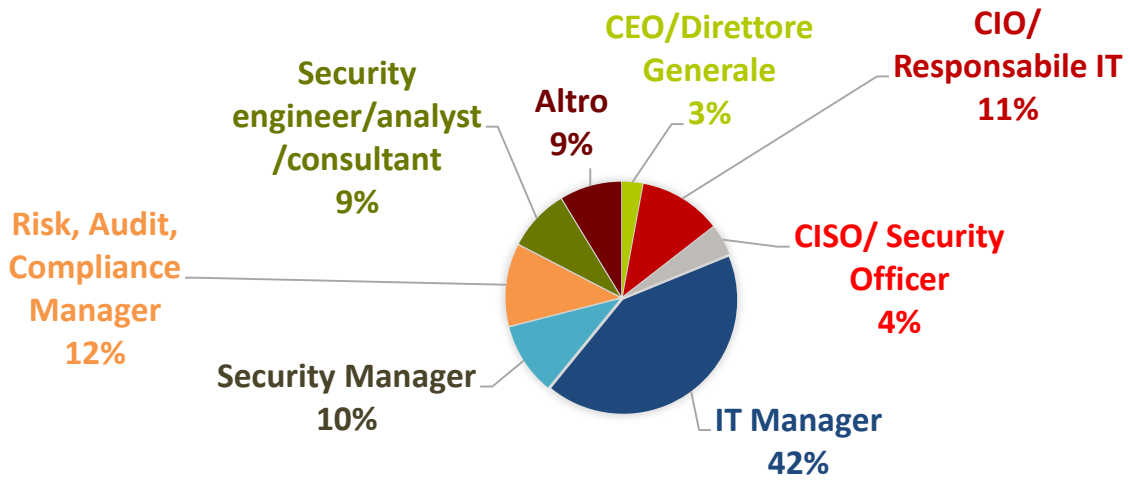
SETTORE DELL'AZIENDA



Il campione della survey, condotta da The Innovation Group tra luglio e ottobre 2018, comprende 70 aziende italiane dei diversi settori di mercato, con una prevalenza di aziende medio grandi (i tre quarti hanno oltre 100 dipendenti)

Caratteristiche del Campione /2

RISPONDENTI ALLA SURVEY



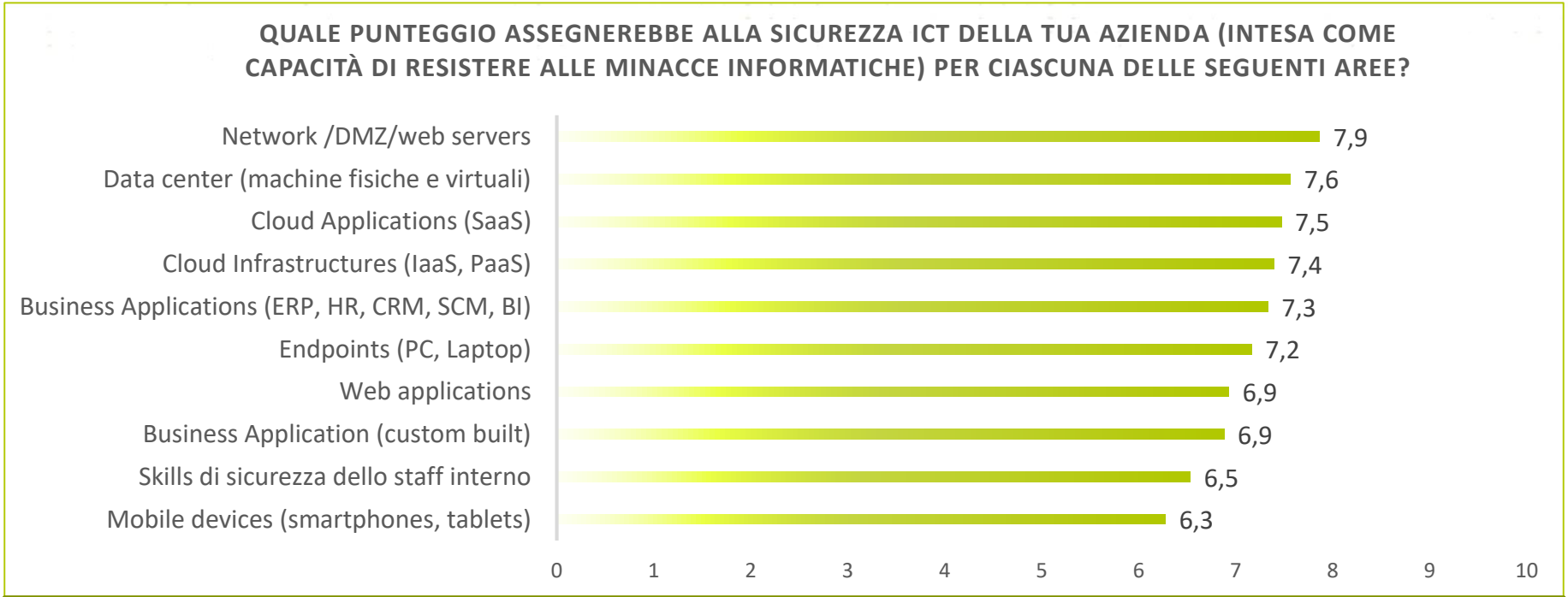
I rispondenti fanno principalmente riferimento all'area ICT delle aziende (53% delle risposte) e a seguire della sicurezza ICT (23% delle risposte), ma una componente di rispondenti fa riferimento all'area risk/audit/compliance (12%) e in minima parte all'alta direzione (3%)

Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 70 aziende italiane

Sezioni della Survey

1. *Caratteristiche del Campione della Survey*
2. *Proteggere il Datacenter che cambia*
3. *Quali sono i requisiti di sicurezza prioritari per Datacenter e Cloud*
4. *Proteggere gli Endpoint dell'azienda*
5. *Protezione degli ambienti Cloud*

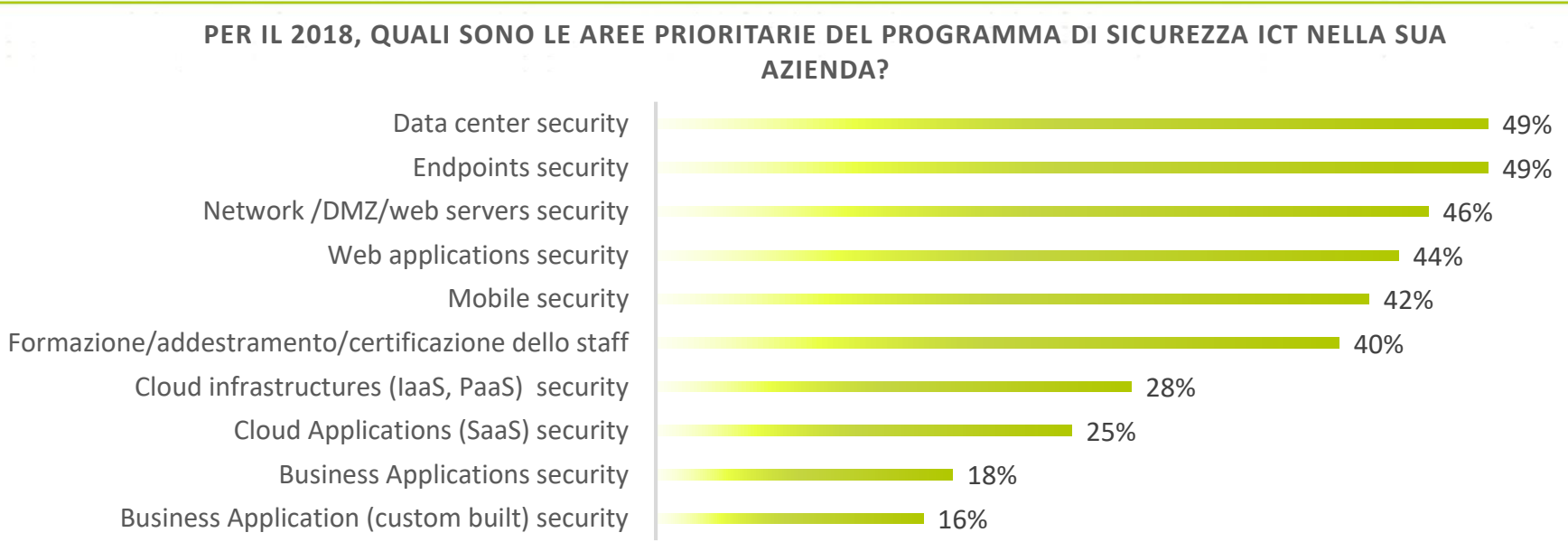
Per le infrastrutture di rete e Datacenter la percezione di sicurezza è buona



Il Network e il Datacenter sono gli ambiti considerati maggiormente sicuri in azienda: anche gli ambienti cloud ottengono valutazioni molto alte, nonostante vedremo che non sono esenti da problemi di sicurezza. Agli ultimi posti invece le applicazioni web e custom, gli skill, il mobile

Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 70 aziende italiane

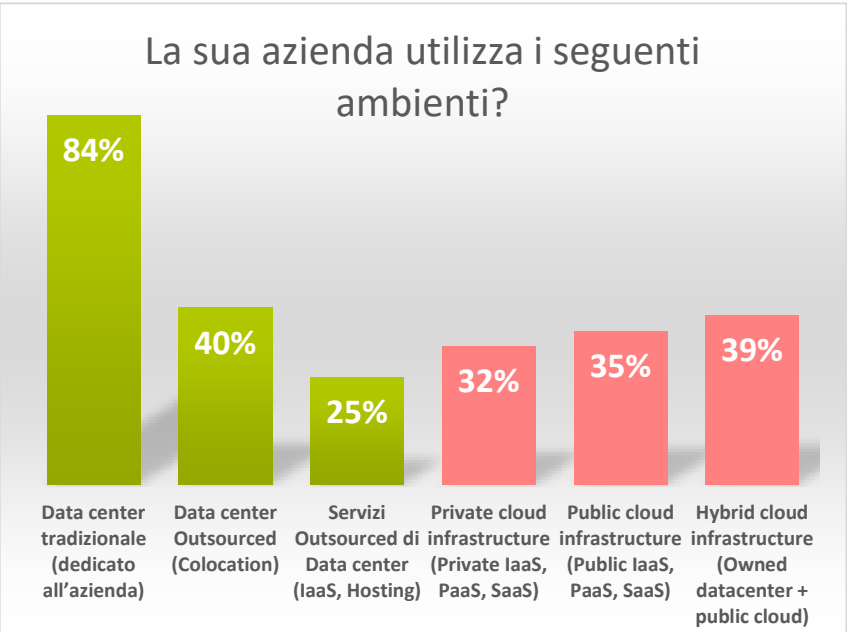
Il Datacenter e gli Endpoint ambiti prioritari sul fronte della sicurezza



La sicurezza delle infrastrutture di Datacenter è oggi al primo posto negli obiettivi di protezione cyber delle aziende. Il Datacenter, gli endpoint, la rete e le applicazioni web, il mobile, sono gli ambiti prioritari. Quello che però preoccupa maggiormente è vedere che due aspetti sono tuttora sottovalutati: da un lato la sicurezza applicativa, dall'altro lato, il cloud. Per le applicazioni non ci sono scuse, anche considerando le nuove richieste normative, come ad esempio il *Privacy-by-design* arrivato con il nuovo Regolamento UE sulla Privacy (GDPR). Per il cloud va osservato che l'adozione di questi ambienti è ancora parziale, ma di sicuro i rischi associati sono sottostimati.

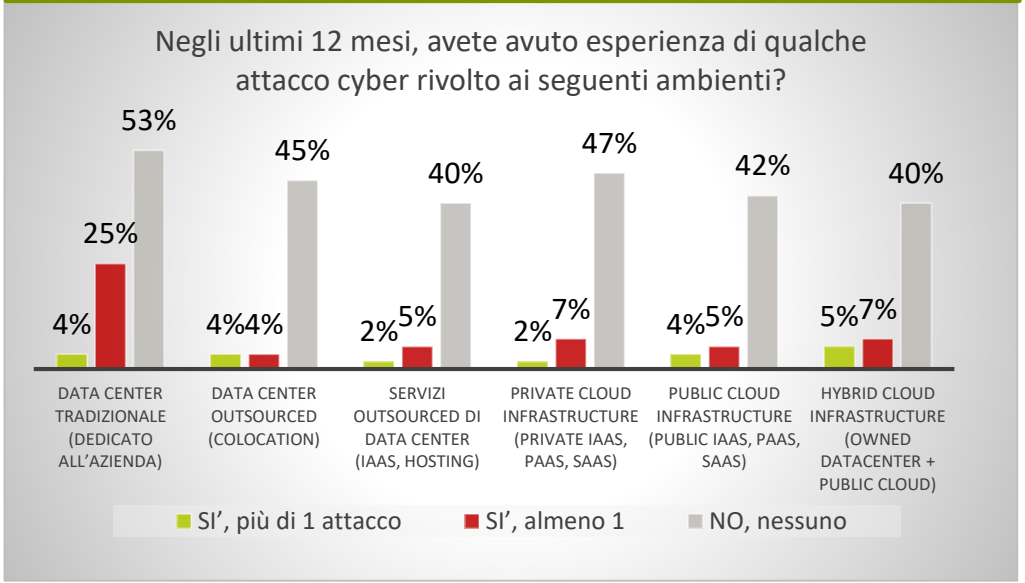
Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 70 aziende italiane

Gli ambienti da proteggere sono molteplici e tutti oggetto di attacchi cyber



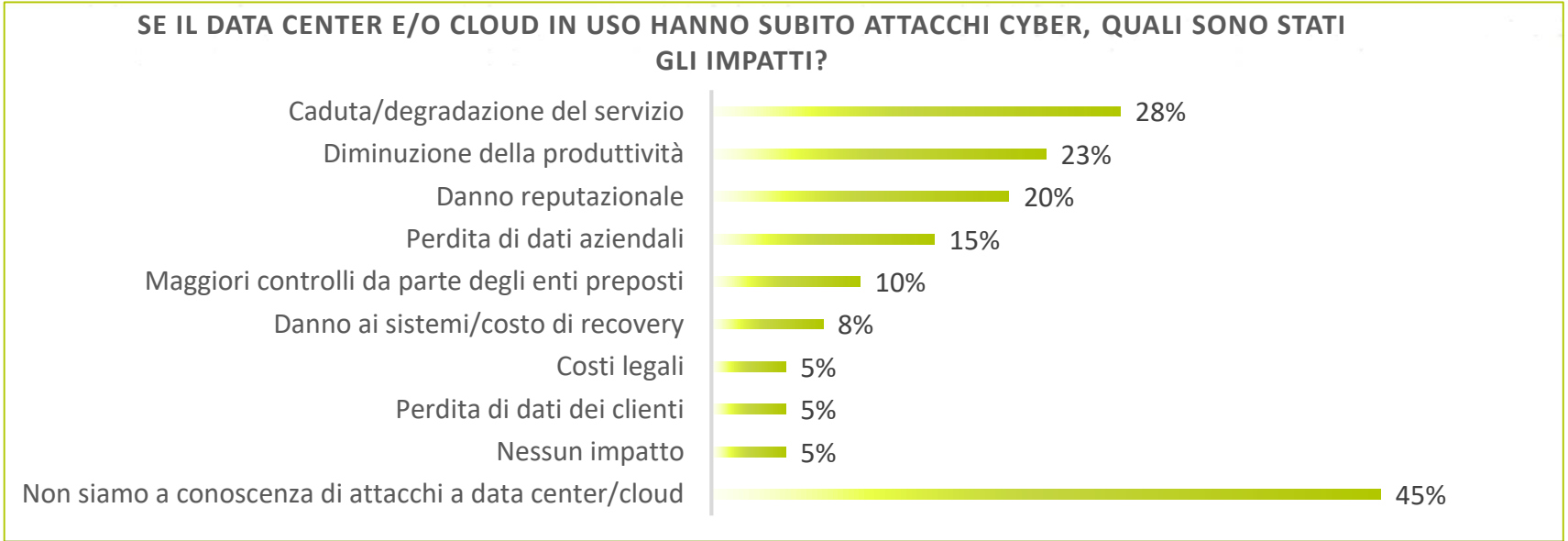
Nonostante prevalga tuttora tra le aziende italiane l'utilizzo di infrastrutture tradizionali, l'adozione del cloud, nella forma di Private, Public e Hybrid cloud, è in crescita. Serve quindi ripensare le politiche di security per questi ambienti

Fatto importante, si comincia ad osservare incidenti anche per ambienti Private cloud (9%), Public cloud (9%) e Hybrid cloud (12%). Questo risultato si ha nonostante l'adozione del cloud sia ancora parziale. Con riferimento al Datacenter, gli attacchi sono stati osservati nel 29% dei casi: in realtà da survey internazionali si evince che gli attacchi ai Datacenter sono in numero superiore



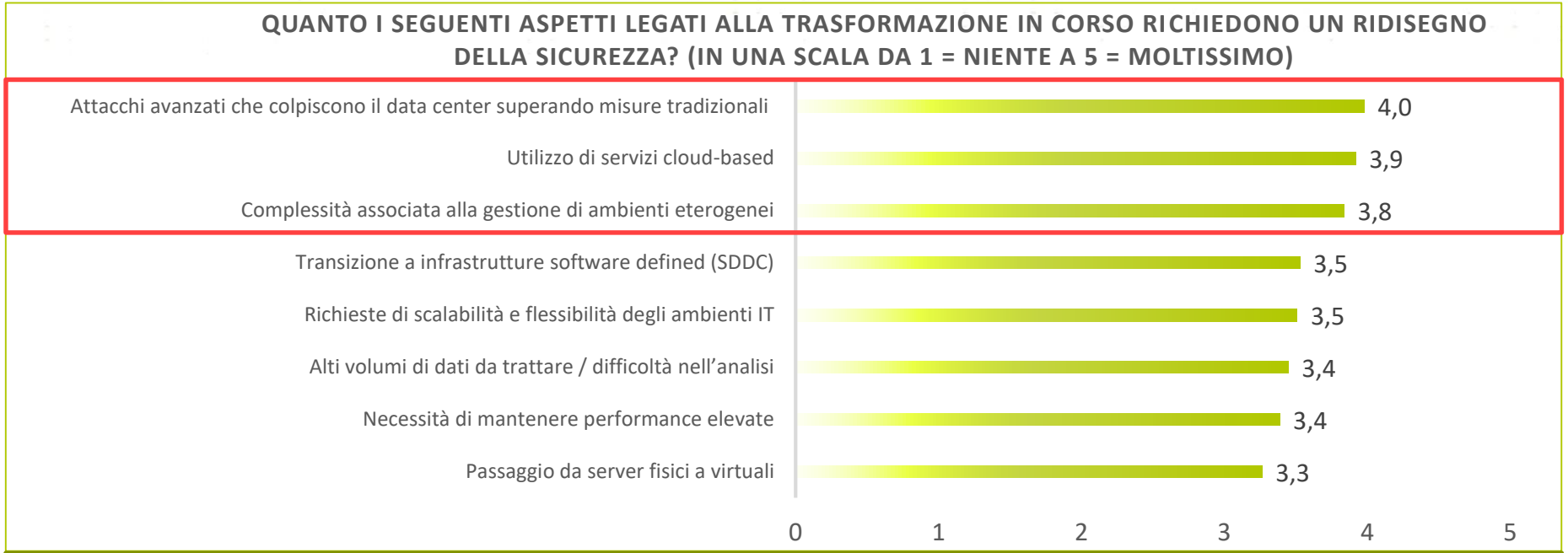
Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 57 aziende italiane

Quali sono le principali conseguenze degli attacchi informatici?



Circa una metà delle aziende afferma di aver subito impatti negativi dall'evenienza di incidenti cyber. L'altra metà, o non ha osservato incidenti (ma questo non significa che non ci siano stati) oppure, in un numero molto limitato di casi (5%) è riuscita a superare l'incidente senza alcun impatto: questo numero in prospettiva dovrebbe crescere, dimostrando così la *Cyber Resilience* delle aziende.
Guardando alle conseguenze negative più diffuse, al primo posto la **caduta/degradazione del servizio**, che può in alcuni casi (pensiamo ad un attacco ransomware che colpisce un'azienda manifatturiera o un operatore di servizi essenziali), avere conseguenze economiche o sulla reputazione del brand molto gravi. Si osservano anche incidenti con **perdita di dati**, aziendali o dei clienti

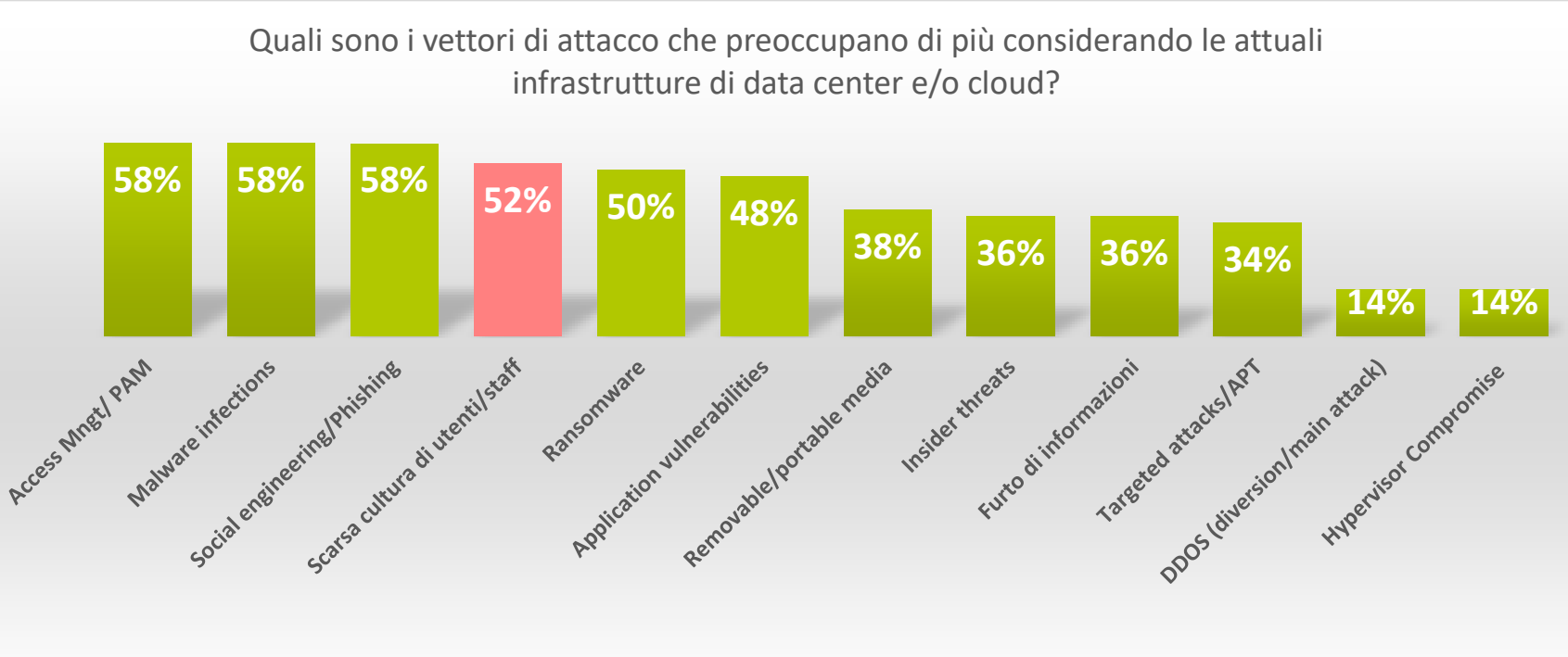
La trasformazione digitale ha un forte impatto sulla sicurezza delle infrastrutture



La trasformazione digitale in corso comporta nuove sfide di cybersecurity: quelle più temute dalle aziende sono gli **attacchi avanzati**, che possono evadere le misure tradizionali di sicurezza e avere impatti molto gravi per il business. Al secondo posto, il fatto che un utilizzo sempre più spinto del **cloud** comporta nuovi rischi, alcuni ancora sconosciuti, e in terza battuta, la necessità di tenere sotto controllo una superfice molto più ampia – un numero di device e ambienti eterogenei maggiori – quindi un'accresciuta **complessità sul fronte della gestione**

Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 51 aziende italiane

Tra i principali vettori di attacco figurano anche le persone



Tra le minacce alla sicurezza delle infrastrutture figura anche la mancanza di cultura sia degli utenti, sia anche dello staff IT, che manca in alcuni casi di una conoscenza specifica su accorgimenti per la sicurezza delle infrastrutture (ad esempio, i nuovi ambienti virtuali)

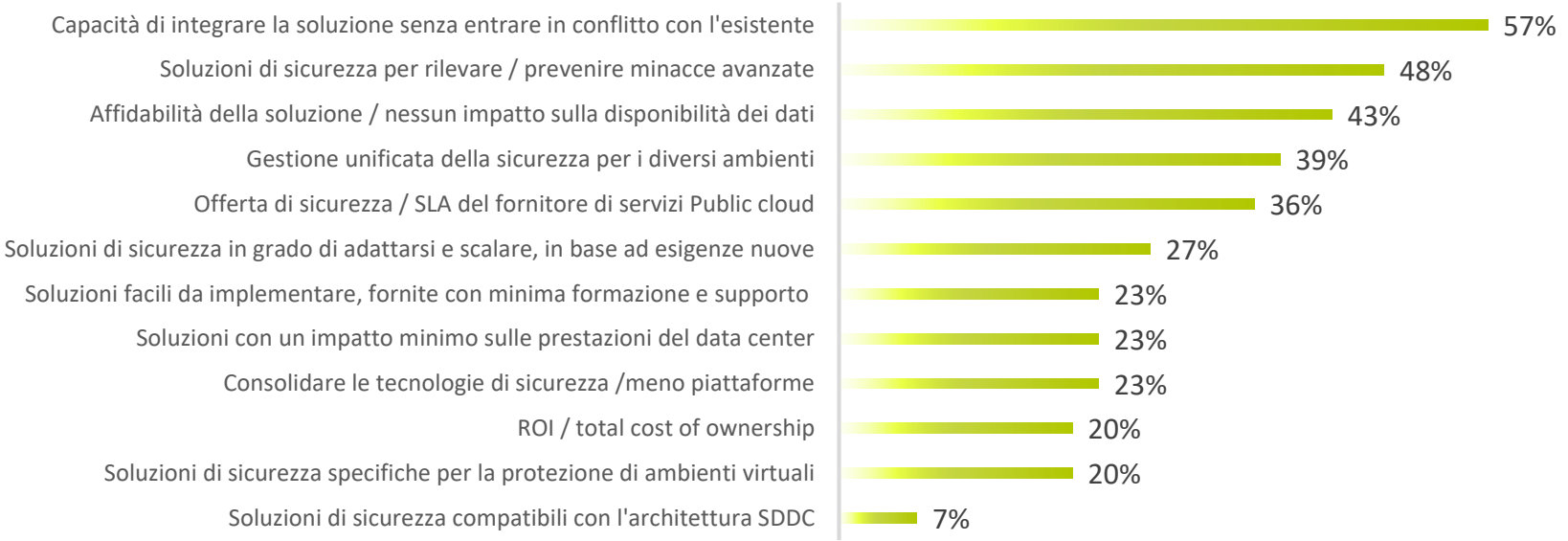
Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 50 aziende italiane

Sezioni della Survey

1. *Caratteristiche del Campione della Survey*
2. *Proteggere il Datacenter che cambia*
3. *Quali sono i requisiti di sicurezza prioritari per Datacenter e Cloud*
4. *Proteggere gli Endpoint dell'azienda*
5. *Protezione degli ambienti Cloud*

I requisiti che deve avere un'offerta di sicurezza per il Datacenter

CONSIDERANDO I REQUISITI DI SICUREZZA DEL DATA CENTER/CLOUD DELLA SUA AZIENDA, QUALI ELEMENTI SONO PRIORITARI?

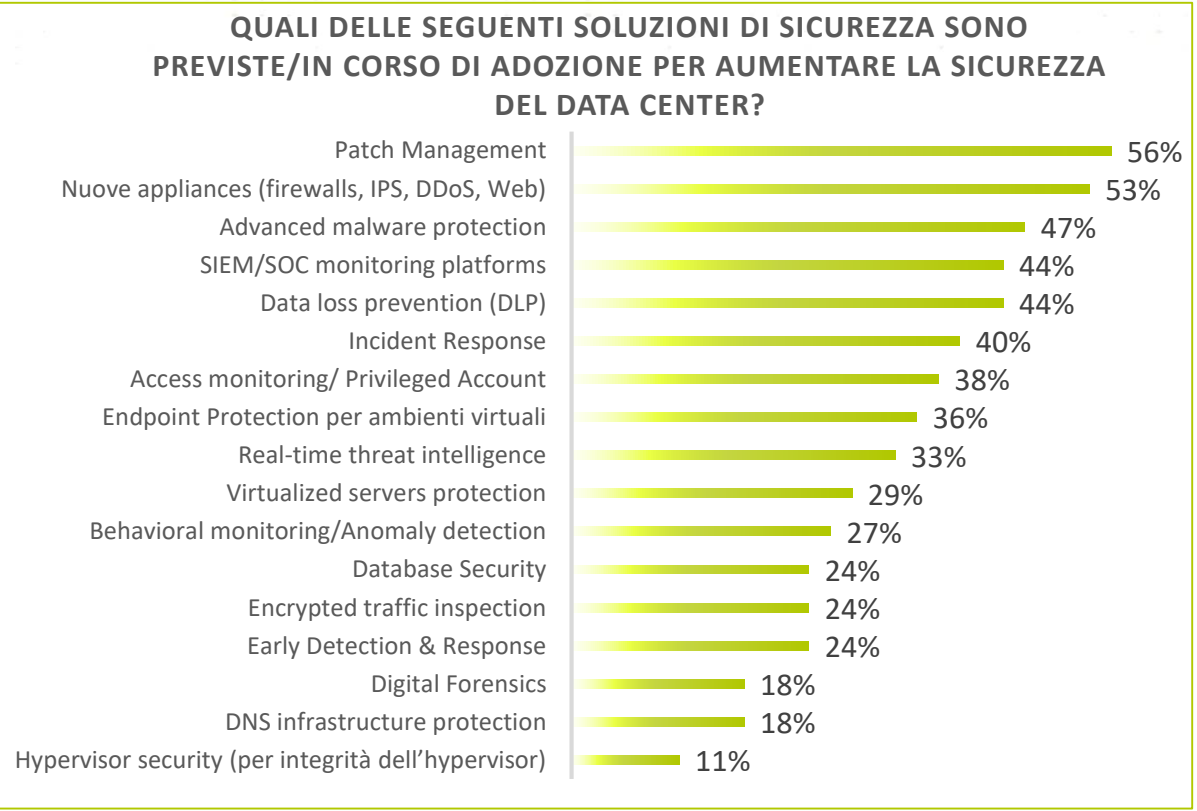


Proprio per un discorso di accresciuta complessità di gestione, tra le principali qualità di una soluzione di security i rispondenti apprezzano la possibilità di integrare la soluzione in modo agevole; inoltre, cercano risposte nuove a minacce avanzate; affidabilità della soluzione; gestione unificata; offerta di sicurezza integrata nel cloud. Il discorso del ROI non viene visto come prioritario, data l'attuale difficoltà di misura di questo investimento. Anche la protezione degli ambienti virtuali non è vista come prioritaria – si assume che questi ambienti siano solidi dal punto di vista della sicurezza

Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 44 aziende italiane

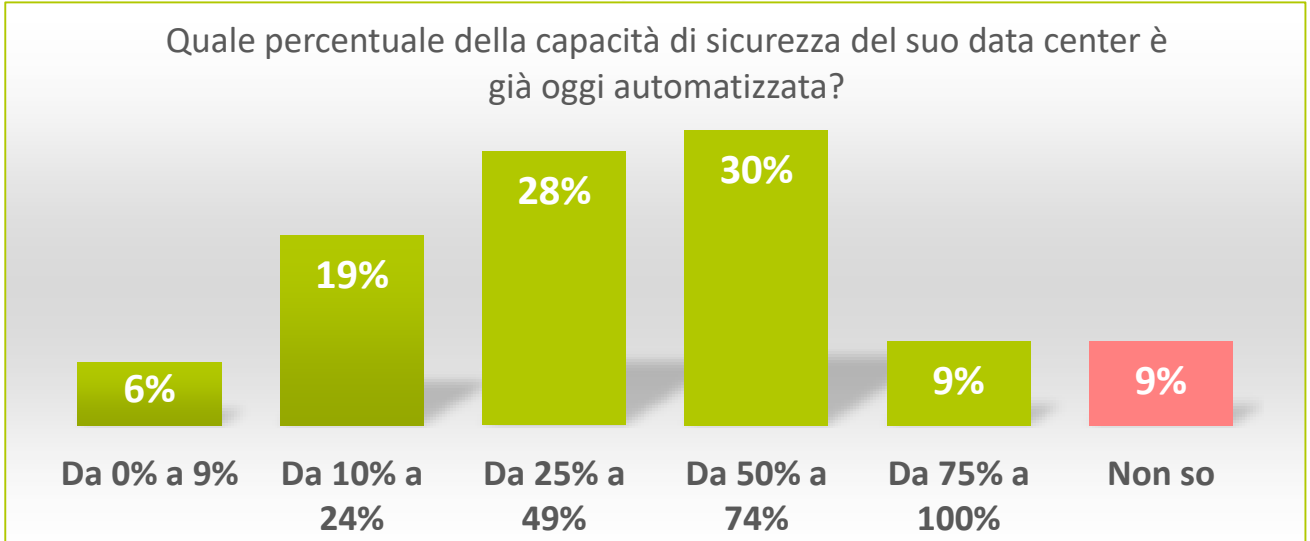
Le aree su cui le aziende andranno a investire maggiormente: Patch Management, nuove appliances e Advanced Malware Protection

Le aziende sono chiamate oggi a dotarsi di numerosi strumenti per tenere sotto controllo i rischi associati al Datacenter in evoluzione. Oltre al rinnovo di appliance dedicate alla sicurezza (come possono essere i firewall, sistemi IPS, DDoS o web filtering) l'indagine mette in evidenza una forte attenzione, molto superiore al passato, per soluzioni che abilitino un più efficace Patch Management. E' questa infatti un'area di debolezza che ha comportato negli ultimi anni una forte esposizione (pensiamo ad esempio alla diffusione dei ransomware Wannacry e NotPetya). Anche la Advanced Malware Protection è un ambito che registra forte interesse, proprio perché il timore è oggi che nuove tecniche di hacking, nuovi malware e attacchi avanzati, superino le difese attuali. Al quarto posto, in crescita rispetto a precedenti rilevazioni, il tema del SOC e del monitoraggio come misura per intercettare gli attacchi



Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 45 aziende italiane

L’automazione nella gestione della sicurezza è sempre più pervasiva



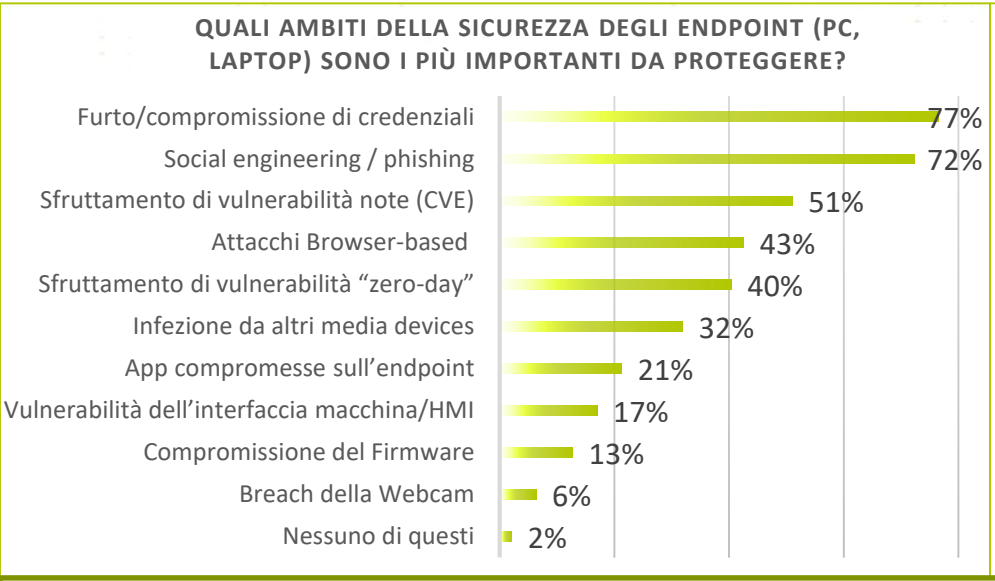
Il tema dell’automazione nella gestione della sicurezza, oggi realizzabile anche con tecniche avanzate di AI/Machine Learning, vede le aziende del campione piuttosto preparate, con un 39% dei rispondenti che addirittura affermano che l’automazione ha superato il 50% delle attività di security nel Datacenter

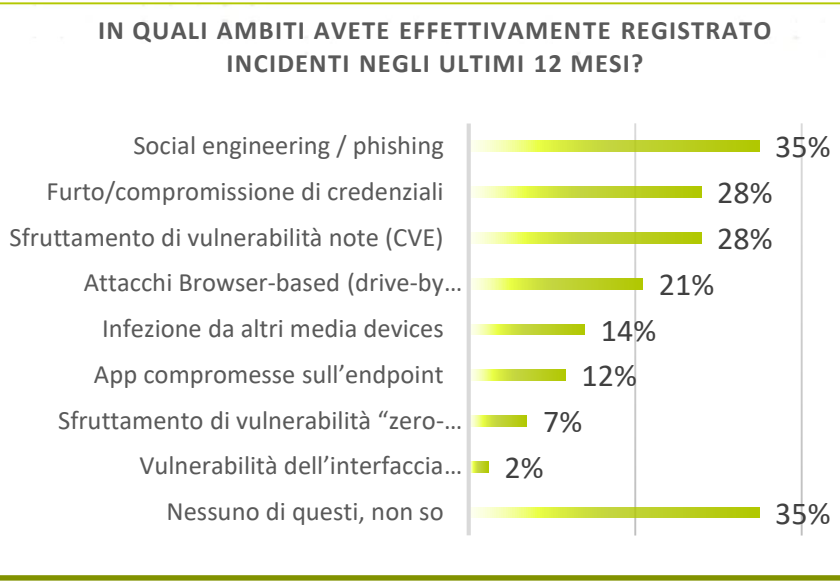
Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 47 aziende italiane

Sezioni della Survey

1. *Caratteristiche del Campione della Survey*
2. *Proteggere il Datacenter che cambia*
3. *Quali sono i requisiti di sicurezza prioritari per Datacenter e Cloud*
4. *Proteggere gli Endpoint dell'azienda*
5. *Protezione degli ambienti Cloud*

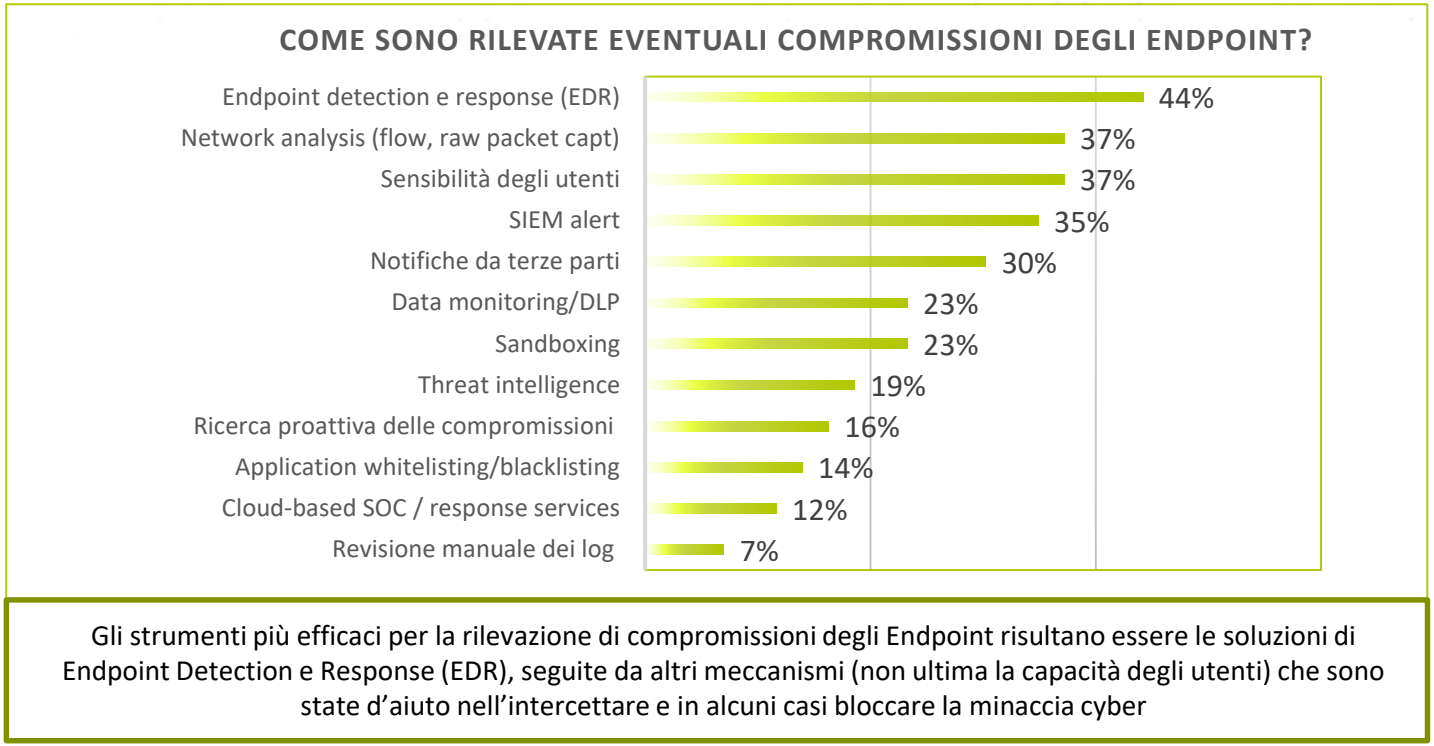
Gli Endpoint si confermano un anello debole, oggetto di frequenti attacchi cyber





Come riporta la figura, gli Endpoint (PC, Tablet) sono uno degli ambiti che richiedono una forte attenzione ad aspetti di cybersecurity. I vettori d'attacco per colpirli sono molteplici, e la sicurezza deve quindi riguardare numerosi aspetti e possibili minacce: si va dal furto di credenziali e al Phishing (considerati i principali rischi cyber per questi device, 77% e 72% delle risposte) allo sfruttamento di vulnerabilità note (51%), attacchi tramite browser (43%), infezioni da altri device che entrano in contatto con l'Endpoint (32%). Rispondendo alla domanda successiva, che chiedeva quali incidenti hanno riguardato gli Endpoint nell'ultimo anno, il 65% degli intervistati ammette di averne subiti, in prevalenza dei primi due tipi, Phishing e Furto di credenziali

Le aziende dispongono di numerosi strumenti per rilevare e bloccare le minacce



Gli strumenti più efficaci per la rilevazione di compromissioni degli Endpoint risultano essere le soluzioni di Endpoint Detection e Response (EDR), seguite da altri meccanismi (non ultima la capacità degli utenti) che sono state d'aiuto nell'intercettare e in alcuni casi bloccare la minaccia cyber

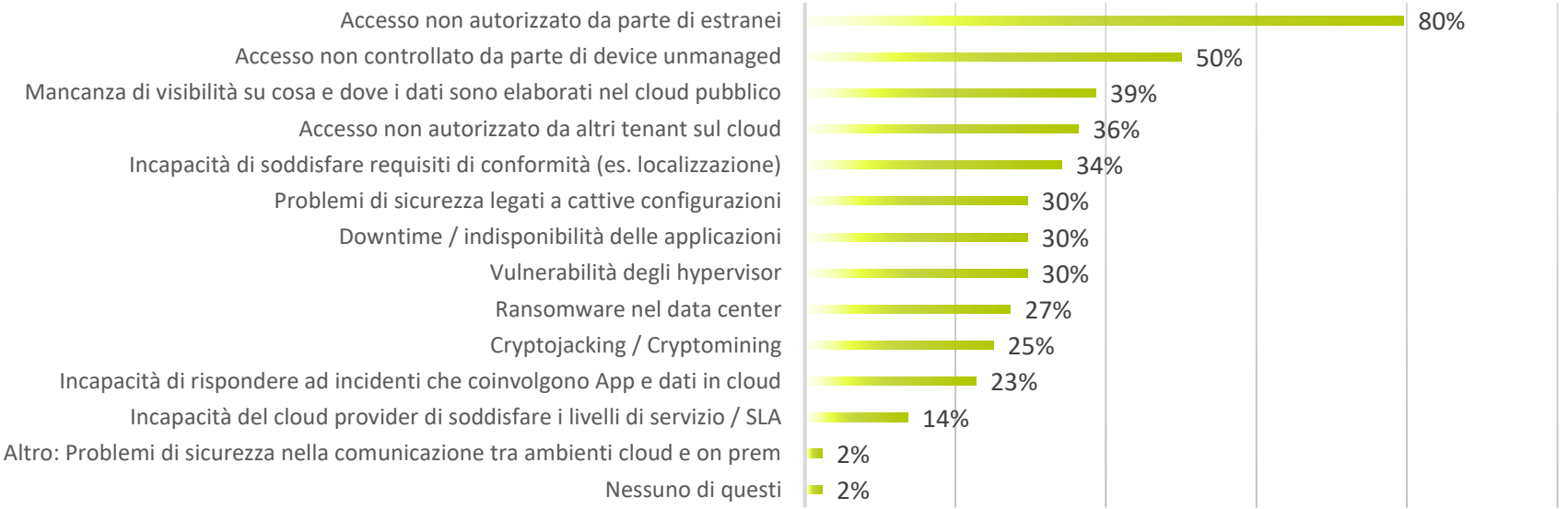
Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 43 aziende italiane

Sezioni della Survey

1. *Caratteristiche del Campione della Survey*
2. *Proteggere il Datacenter che cambia*
3. *Quali sono i requisiti di sicurezza prioritari per Datacenter e Cloud*
4. *Proteggere gli Endpoint dell'azienda*
5. *Protezione degli ambienti Cloud*

La sicurezza del cloud è ricollegata principalmente al tema del controllo accessi

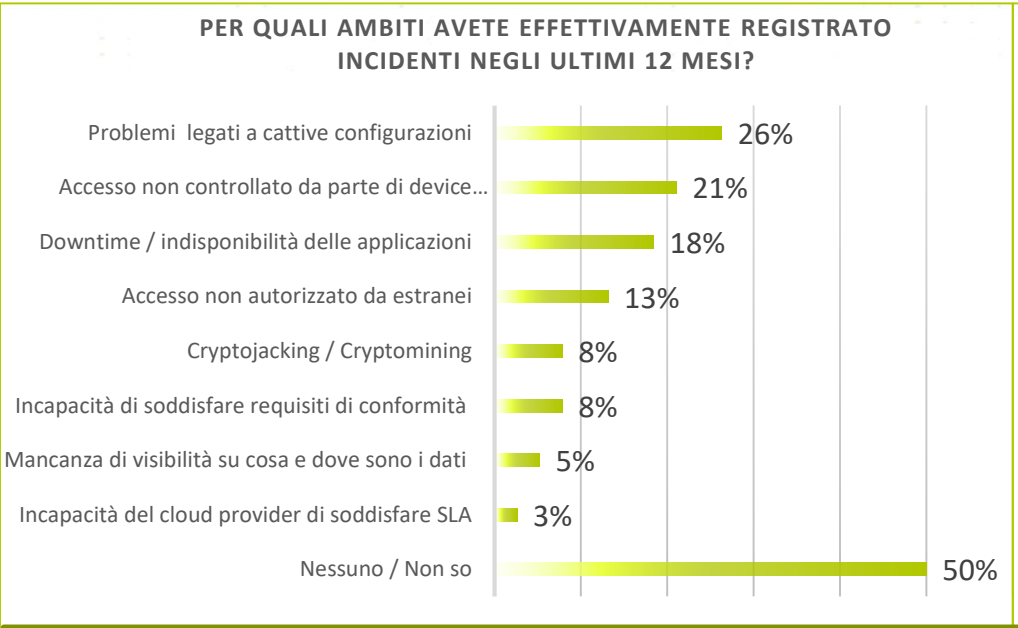
SECONDO LEI, QUALI AMBITI DELLA SICUREZZA DEL CLOUD SONO I PIÙ IMPORTANTI DA PROTEGGERE?

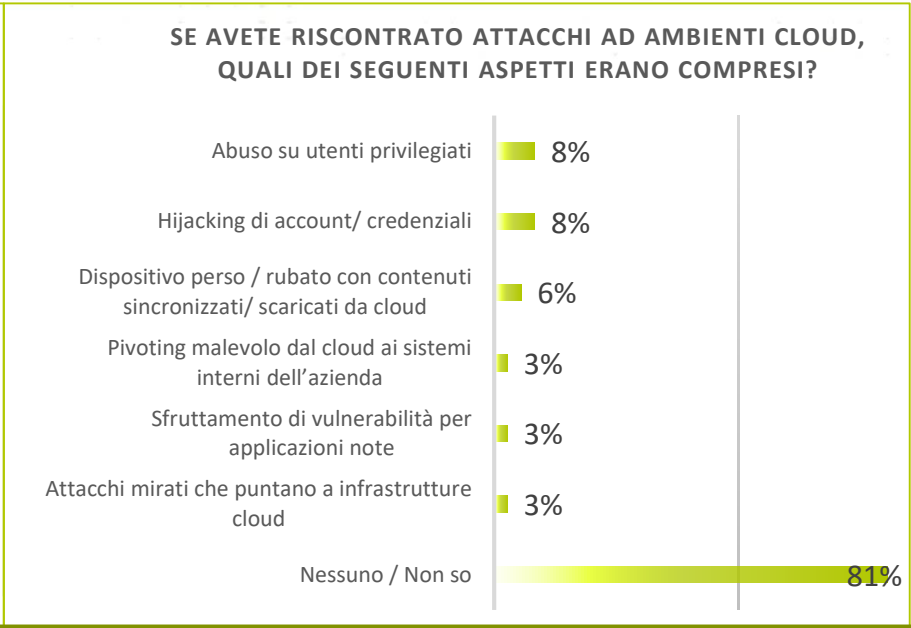


La consapevolezza sui problemi del cloud è un ambito che andrà monitorato nei prossimi anni. Al momento, con riferimento alle possibili minacce avvertite per il cloud, ai primi posti si conferma il tema dell'accesso, che può avvenire da parte di estranei o di device usati dagli utenti senza un controllo dell'azienda. Si hanno poi problematiche di mancanza di visibilità, e quindi di compliance/mancanza di controllo su aspetti gestiti dal provider (come la localizzazione dei dati). Problematiche come la configurazione errata o i downtime sono indicate da una minoranza di aziende.
C'è nel complesso una percezione positiva sulla capacità dei cloud provider di rispondere alle più comuni minacce cyber

Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 44 aziende italiane

Qualche problema con il cloud c'è ma ancora in misura molto limitata

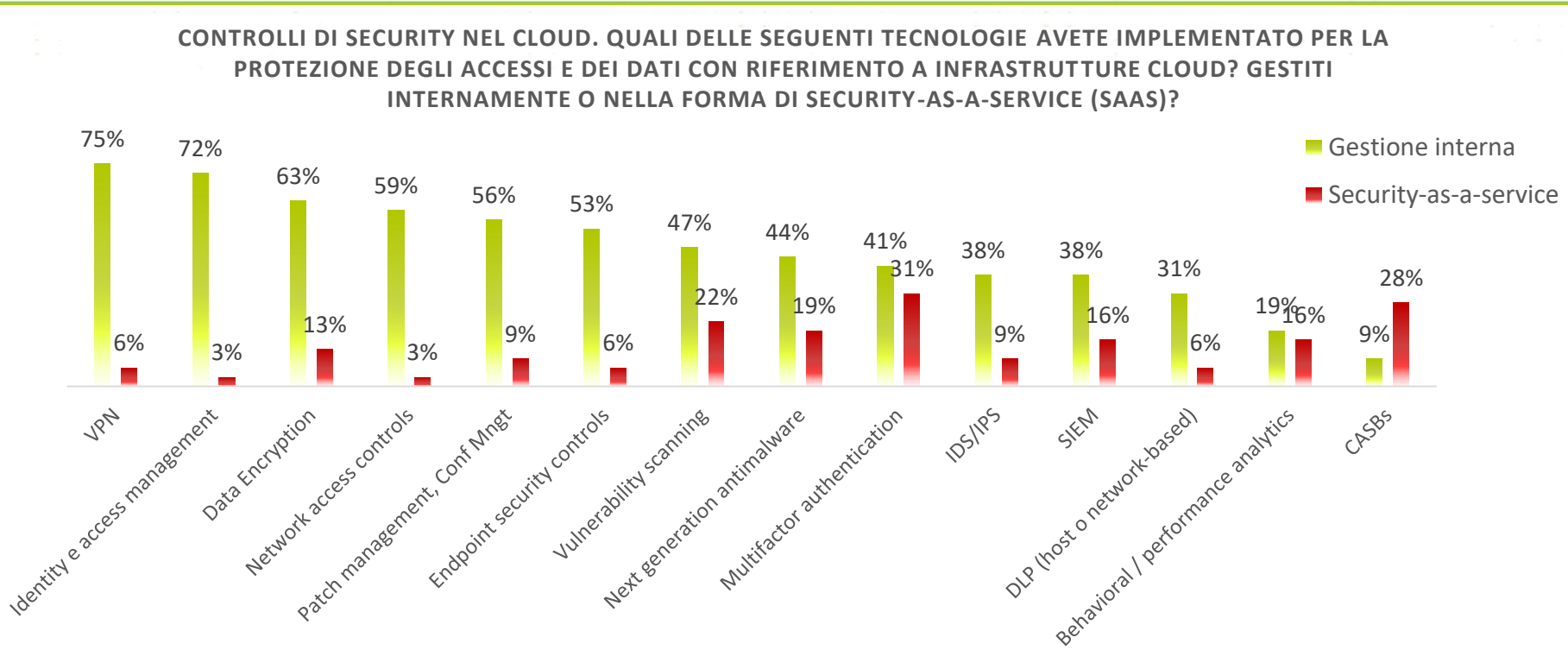




Gli ambienti cloud non sono esenti da problemi di sicurezza: come mostra la prima figura, questi sono principalmente da attribuire a cattive configurazioni e ad accessi non controllati: una buona percentuale di aziende però (il 50%) non ha osservato problemi nel proprio utilizzo del cloud.
Dove sono stati osservati dei veri e propri attacchi informatici ad ambienti cloud (solo da parte di poche aziende, il 19%) le compromissioni sono state in effetti legate all'utilizzo di account con privilegi, furto di credenziali, altri problemi (ma in misura molto limitata)

Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 38, N = 36 aziende italiane

Anche in tema di Cloud Security, si osserva l'adozione di una molteplicità di misure, in alcuni casi erogate da terze parti as-a-service



Le aziende del campione mostrano già un'attenzione alla sicurezza cloud, soprattutto sul fronte della rete, degli accessi, dell'encryption. Alcuni aspetti, come controlli sugli endpoint e antimalware, sono ancora poco diffusi. Si osserva per alcuni strumenti, come il CASB, una preferenza per servizi erogati online

Fonte: The Innovation Group, Datacenter Security 2018 Survey, Novembre 2018. N = 32 aziende italiane

The Innovation Group
via Palermo, 5, 20121 Milano – Italia
Tel. +39-02-87285500
Fax +39-02-87285519
Website: www.theinnovationgroup.it
E-mail: info@theinnovationgroup.it