Cybersecurity, è il momento!

Un momento critico: da un lato si moltiplicano gli **attacchi informatici** (WannaCry, Petya, ransomware, ecc.), dall'altro aumentano **responsabilità, normative e sanzioni**. Come fare?

Attiva Incontra, Padova, 21 Settembre 2017

Primo Bonacina
Managing Partner
PBS – Primo Bonacina Services

www.primobonacina.com

PBS Digital Actionable Measurable

Parliamo di **Cybersecurity**

Sicurezza informatica

Da Wikipedia, l'enciclopedia libera.

> **Questa voce o sezione sull'argomento informatica è priva o carente di note e riferimenti bibliografici puntuali.**
> **Commento**: *solo l'ultima sezione ha delle note*
>
> Sebbene vi siano una bibliografia e/o dei collegamenti esterni, manca la contestualizzazione delle fonti con note a piè di pagina o altri riferimenti precisi che indichino puntualmente la provenienza delle informazioni. Puoi migliorare questa voce citando le fonti più precisamente. Segui i suggerimenti del progetto di riferimento.

Con il termine **sicurezza informatica** si intende quel ramo dell'informatica che si occupa delle analisi delle minacce, delle vulnerabilità e del rischio associato agli asset informatici, al fine di proteggerli da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti di impatto superiore ad una determinata soglia di tollerabilità (es. economico, reputazionale, politico-sociale, ecc...).

Navy Cyber Defense Operations Command, unità che controlla le attività non autorizzate nei sistemi informativi della United States Navy

Il termine è spesso sostituito con il neologismo **cybersecurity**, che rappresenta una sottoclasse del più ampio concetto di *information security*[1]. Per cybersecurity si intende infatti quell'ambito dell'information security prettamente ed esclusivamente dipendente dalla tecnologia informatica. Nell'utilizzare il termine *cybersecurity* si vuole intendere, in particolare, un approccio mirato ad enfatizzare non tanto le *misure di prevenzione* (ovvero quelle misure che agiscono riducendo la probabilità di accadimento di una minaccia), ma soprattutto le *misure di protezione* (ovvero quelle misure che agiscono riducendo la gravità del danno realizzato da una minaccia).

L’espansione della superficie di attacco

Figura 1 Le principali fonti di preoccupazione degli esperti della sicurezza in merito agli attacchi informatici

Dispositivi mobili	Dati nel cloud pubblico	Infrastruttura cloud	Comportamento dell’utente (che, ad esempio, fa clic su link dannosi nelle e-mail o nei siti Web)
58%	57%	57%	57%

Percentuale di esperti della sicurezza che ritiene queste categorie molto o estremamente impegnative

Il comportamento degli hacker

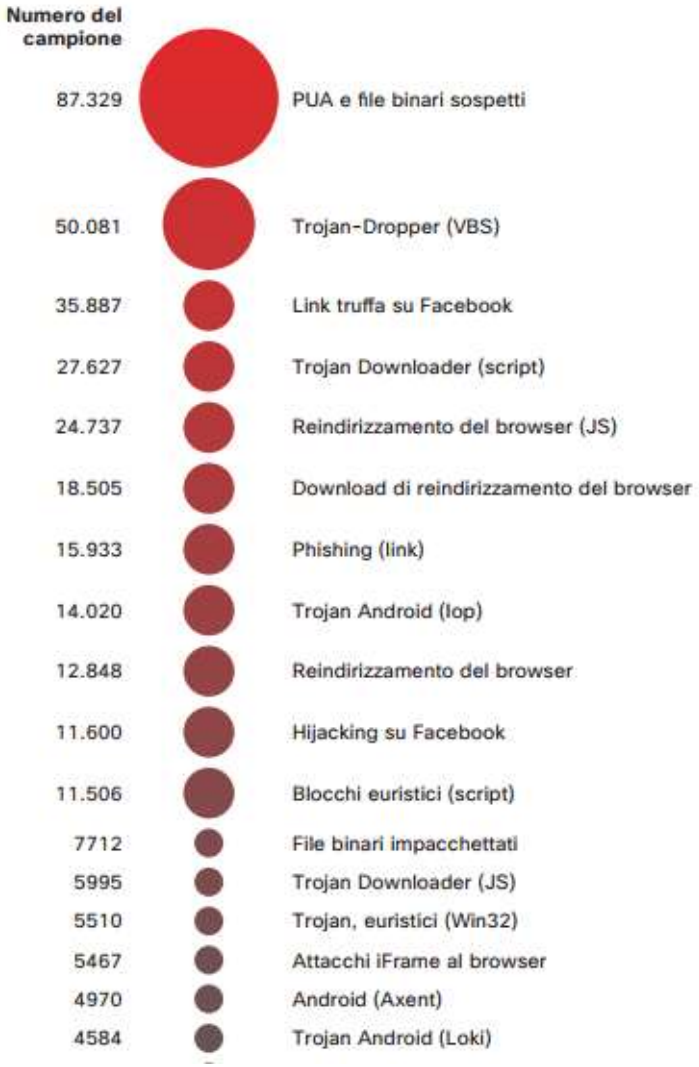
Metodi di attacco tramite Web: le minacce con la "coda corta" consentono ai criminali informatici di gettare le basi per le campagne

La ricognizione è, ovviamente, una fase fondamentale del lancio di attacchi informatici, durante la quale gli autori vanno alla ricerca di infrastrutture Internet vulnerabili o di punti deboli delle reti che consentano loro di ottenere l'accesso ai computer degli utenti e, in ultima analisi, di infiltrarsi nelle aziende.

I file binari di Windows sospetti e le applicazioni potenzialmente indesiderate (PUA) si stagliano inequivocabilmente in cima alla classifica dei metodi di attacco tramite Web per il 2016 (**vedere la figura 2**). I file binari di Windows sospetti veicolano minacce quali spyware e adware, mentre le estensioni dannose per i browser sono un esempio di PUA.

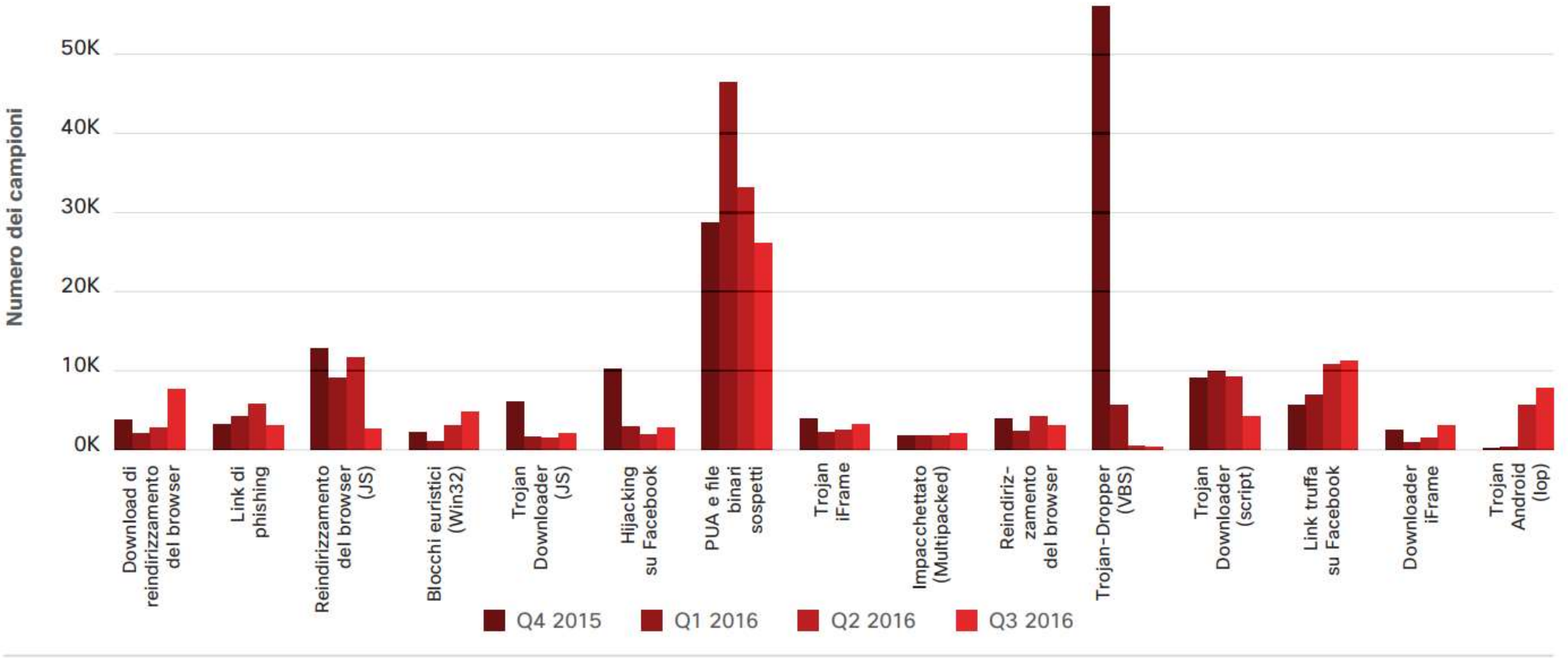
Le truffe su Facebook, costituite da false offerte e contenuti multimediali associati a finti sondaggi si sono classificati al terzo posto. La costante prevalenza delle truffe su Facebook nelle nostre classifiche annuali e semestrali relative ai casi di malware osservati più di frequente evidenzia il ruolo fondamentale del social engineering in molti attacchi informatici. Facebook dispone di circa 1,8 miliardi di utenti attivi al mese in tutto il mondo[4] ed è il terreno di caccia ideale per i criminali informatici e altri attori intenzionati a truffare gli utenti. Una notizia positiva è costituita dal recente annuncio dell'azienda di provvedimenti che verranno assunti per eliminare le notizie false e gli hoax. I critici ipotizzano che questi contenuti possano avere influito sul voto in occasione delle elezioni presidenziali del 2016 negli Stati Uniti.[5]

Figura 2 Malware più comuni



Una svolta alla fase di ricognizione degli attacchi Web: più minacce hanno per obiettivo browser e plug-in vulnerabili

Figura 3 Il malware più comune, Q4 2015–Q3 2016

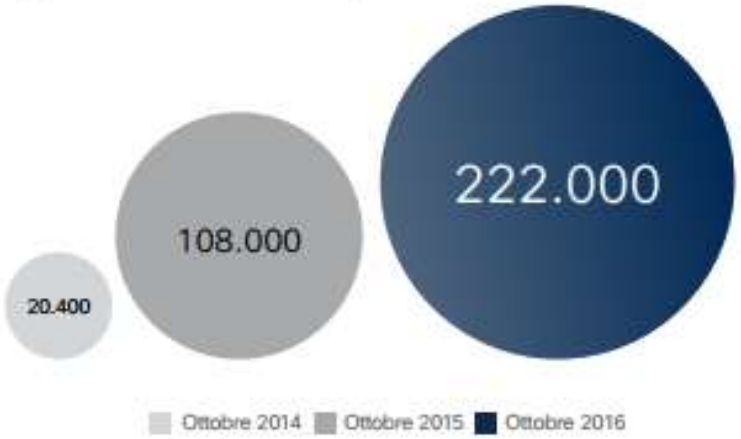


Sicurezza delle **applicazioni**: come gestire il rischio delle connessioni in seguito al boom delle app

Figura 4 Crescita esponenziale delle applicazioni cloud connesse di terze parti nel 2016

Fonte: Cisco CloudLock

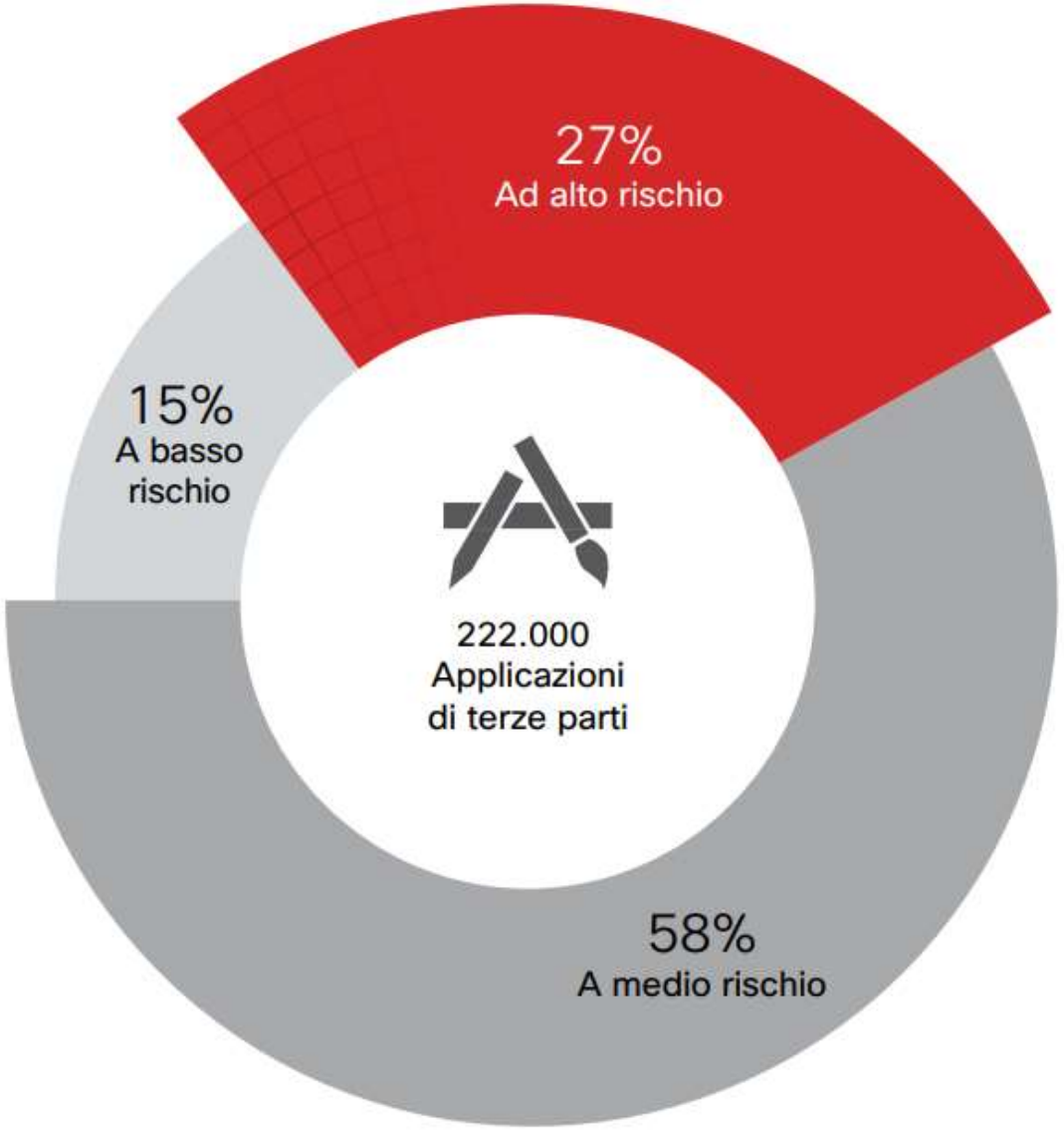
Figura 5 Confronto anno per anno della crescita delle applicazioni cloud di terze parti



Fonte: Cisco CloudLock

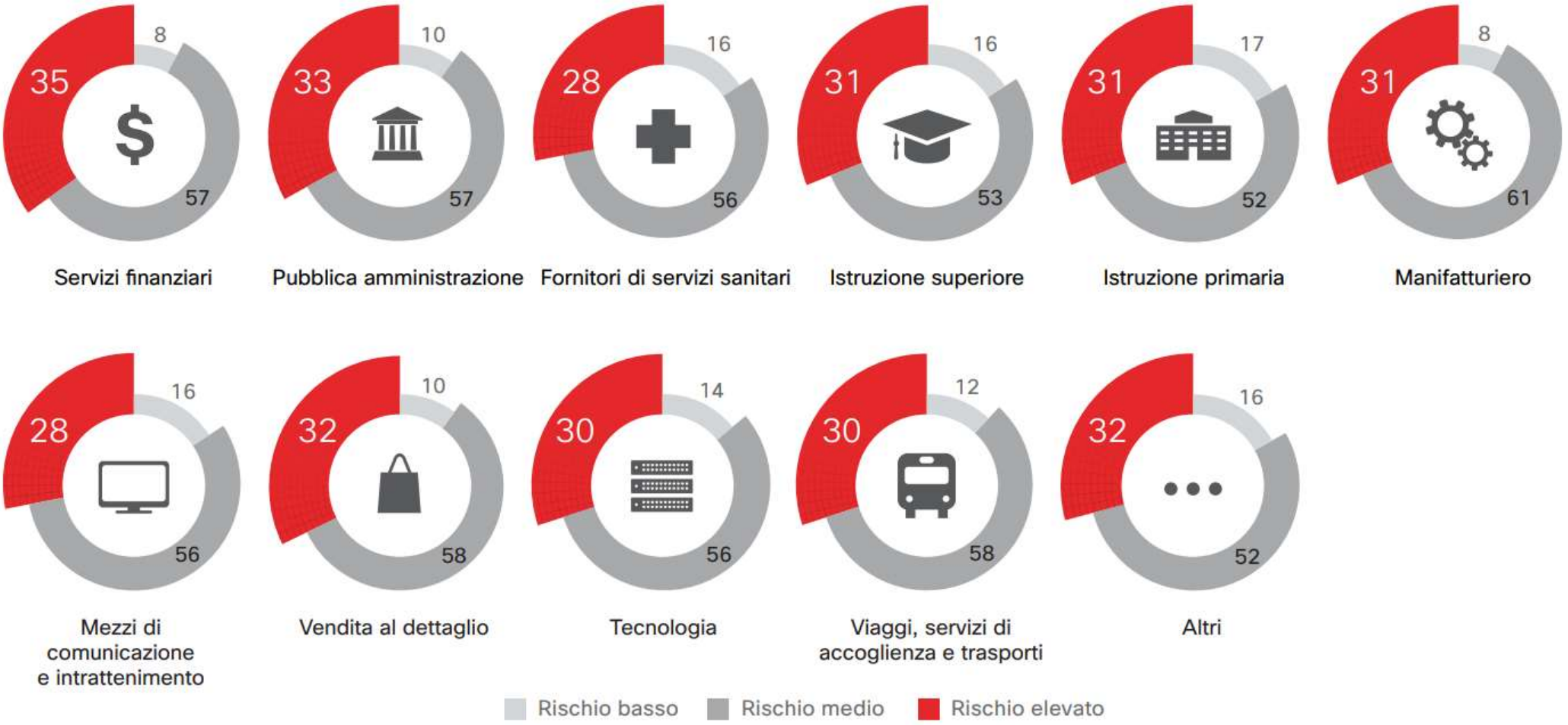
Classificazione delle applicazioni più rischiose

Figura 6 Applicazioni di terze parti classificate ad alto rischio



Tutte le aziende, indipendentemente da dimensioni, settore o area geografica, presentano una quantità uniforme di applicazioni a rischio

Figura 8 Distribuzione di applicazioni a basso, medio e alto rischio per settore

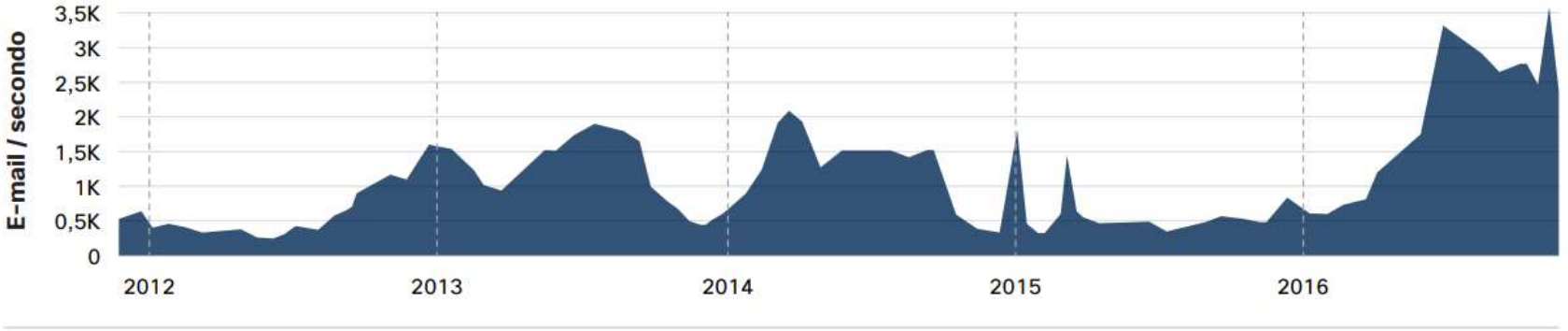


L’indagine ha rilevato che il 75% delle aziende è interessata da infezioni Adware

Figura 12 Percentuale di aziende colpite da infezioni da adware

La quantità complessiva di **spam** è in aumento, così come la percentuale degli allegati dannosi, #1

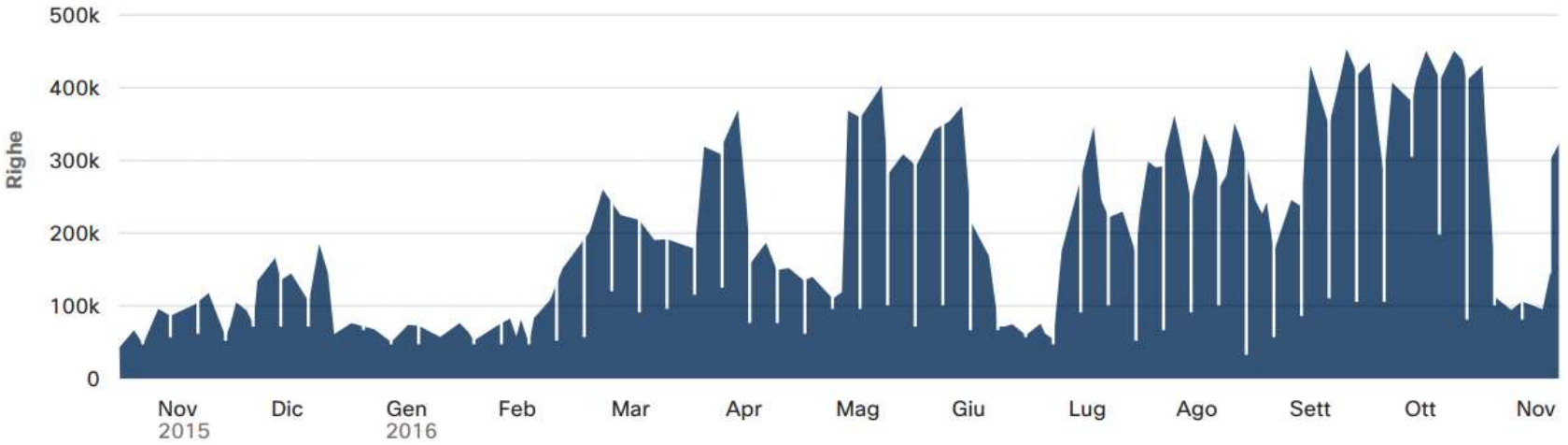
Figura 15 Volume totale di spam



Fonte: CBL

SCBL = Spam Cop Block List

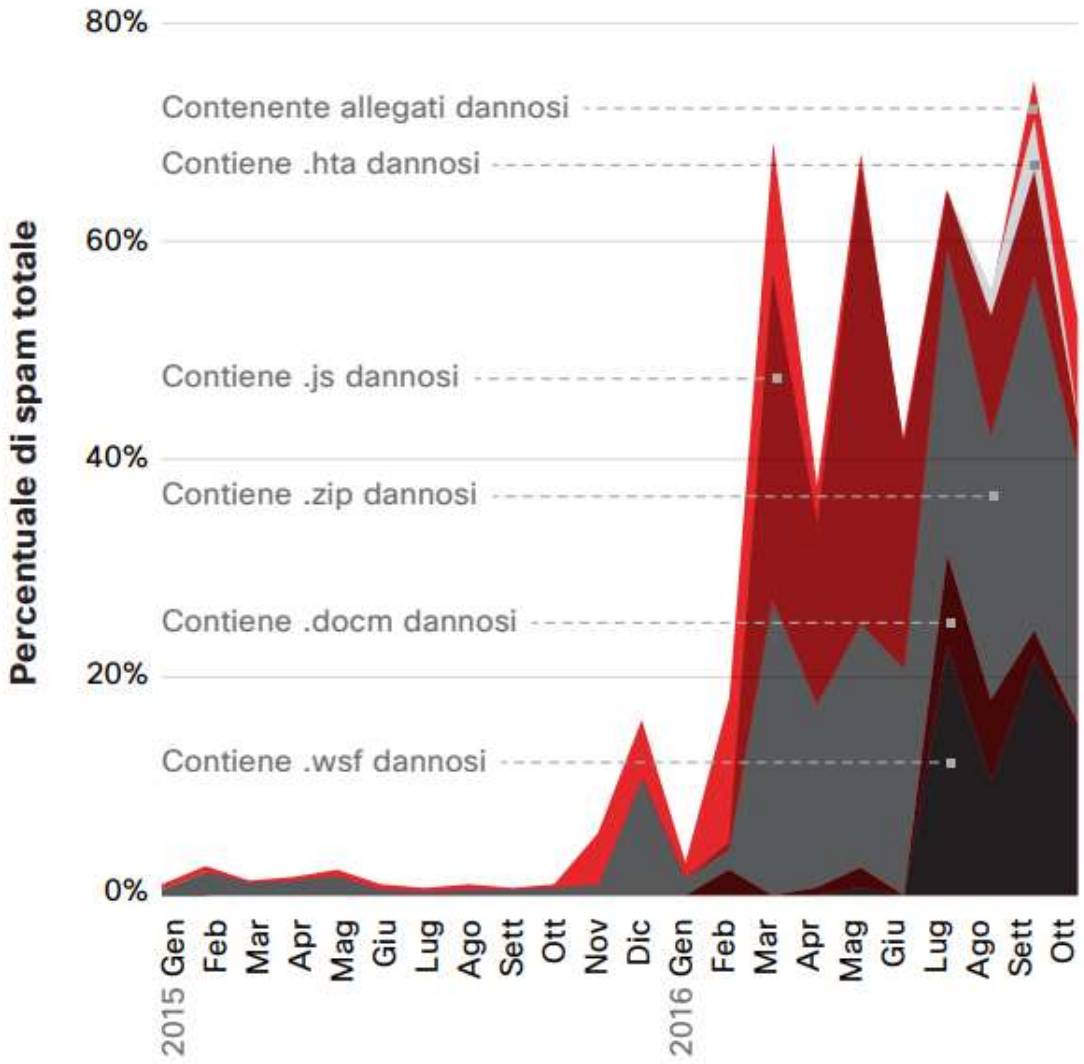
Figura 16 Volume complessivo di SCBL



Fonte: SpamCop

La quantità complessiva di spam è in aumento, così come la percentuale degli allegati dannosi, #2

Figura 17 Percentuale di spam totale contenente allegati dannosi



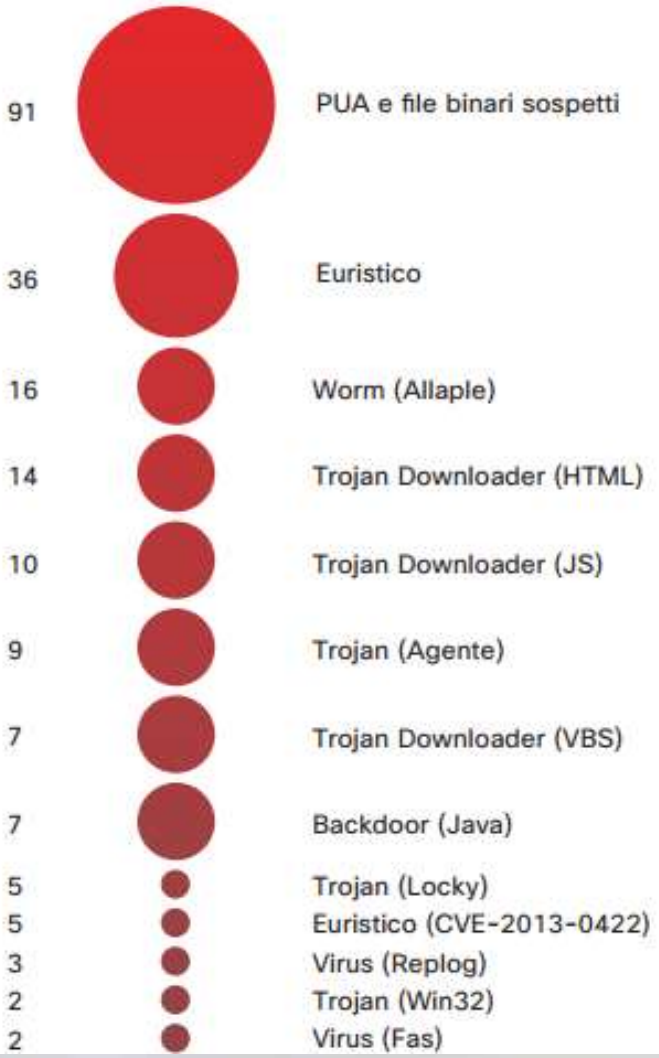
Una volta posizionatasi, la **minaccia installa una backdoor** sul sistema dell'obiettivo, fornendo agli hacker un accesso costante

Metodi di attacco Web: una panoramica sulla "coda lunga" svela le minacce che gli utenti possono evitare con facilità

La cosiddetta coda lunga del panorama dei metodi di attacco Web (**figura 20**) presenta una raccolta di malware che generano volumi inferiori impiegati in una fase successiva della catena di attacco: l'installazione. In questa fase, la minaccia che è giunta a destinazione (un trojan bancario, un virus, un downloader o un exploit di altro tipo) installa una backdoor nel sistema oggetto di attacco, garantendo agli hacker un accesso permanente e, insieme, l'opportunità di esfiltrare dati, lanciare attacchi ransomware e compiere altri misfatti.

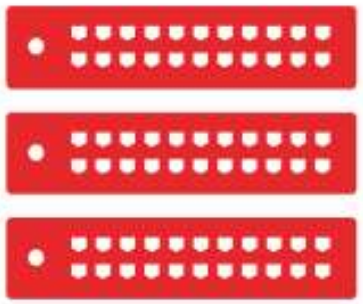
Le minacce elencate nella **figura 20** sono esempi di firme individuate nei 50 tipi di malware osservati più di frequente. La coda lunga dei metodi di attacco Web è, sostanzialmente, un'istantanea delle minacce che lavorano silenziosamente all'interno dei computer e dei sistemi in seguito a un attacco condotto con successo. Molte di queste infezioni sono state diffuse inizialmente dall'incontro con adware dannoso o dall'esposizione a una truffa basata sul phishing ben architettata: queste sono situazioni che gli utenti spesso possono evitare facilmente o correggere rapidamente.

Figura 20 Campione di malware a più basso volume osservato



Lanciando attacchi ai software dei server, si può possono acquisire il controllo di più risorse di rete o spostarsi su risorse fondamentali per le aziende, #1

Figura 40 Analisi dettagliata delle vulnerabilità client-server, 2015-2016



Vulnerabilità del server
(da 2332 a 3142)

▲34%

Vulnerabilità del client
(da 2300 a 2106)

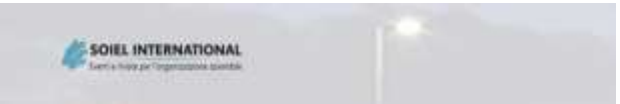
▼8%

Vulnerabilità della rete
(da 501 a 396)

▼20%

Fonte: National Vulnerability Database

Lanciando attacchi ai software dei server, si può possono acquisire il controllo di più risorse di rete o spostarsi su risorse fondamentali per le aziende, #2



CERT nazionale Italia
COMPUTER EMERGENCY RESPONSE TEAM

MINISTERO DELLO SVILUPPO ECONOMICO

Link Utili FAQ Glossario

Home Chi siamo News Bollettini Documenti Contatti

Ricerca:

Home » News » Avviso relativo a vulnerabilità critiche in prodotti Microsoft sfruttabili in attacchi reali

INFORMAZIONI - VULNERABILITÀ

AVVISO RELATIVO A VULNERABILITÀ CRITICHE IN PRODOTTI MICROSOFT SFRUTTABILI IN ATTACCHI REALI

microsoft remote code execution mercoledì, 14 giugno 2017

Nella giornata del 13 giugno 2017 **Microsoft** ha emesso un avviso relativo ad aggiornamenti di sicurezza critici, alcuni nuovi ed altri pubblicati nell'arco dell'ultimo decennio, che riguardano vulnerabilità ad alto rischio che si ritiene possano essere sfruttabili in attacchi reali. Se sfruttate con successo, le più gravi tra queste vulnerabilità possono causare l'esecuzione di codice arbitrario da remoto.

Si raccomanda ai gestori e agli utenti di sistemi e prodotti Microsoft di prendere visione del Microsoft Security Advisory 4025685.

Gli utenti che hanno abilitato per le proprie piattaforme gli aggiornamenti automatici dovrebbero risultare già protetti. I gestori di sistemi più vecchi o per i quali gli aggiornamenti vengono installati manualmente debbono applicare al più presto gli aggiornamenti necessari, previa opportuna verifica.

Dettagli degli aggiornamenti contenuti nell'avviso di Microsoft:

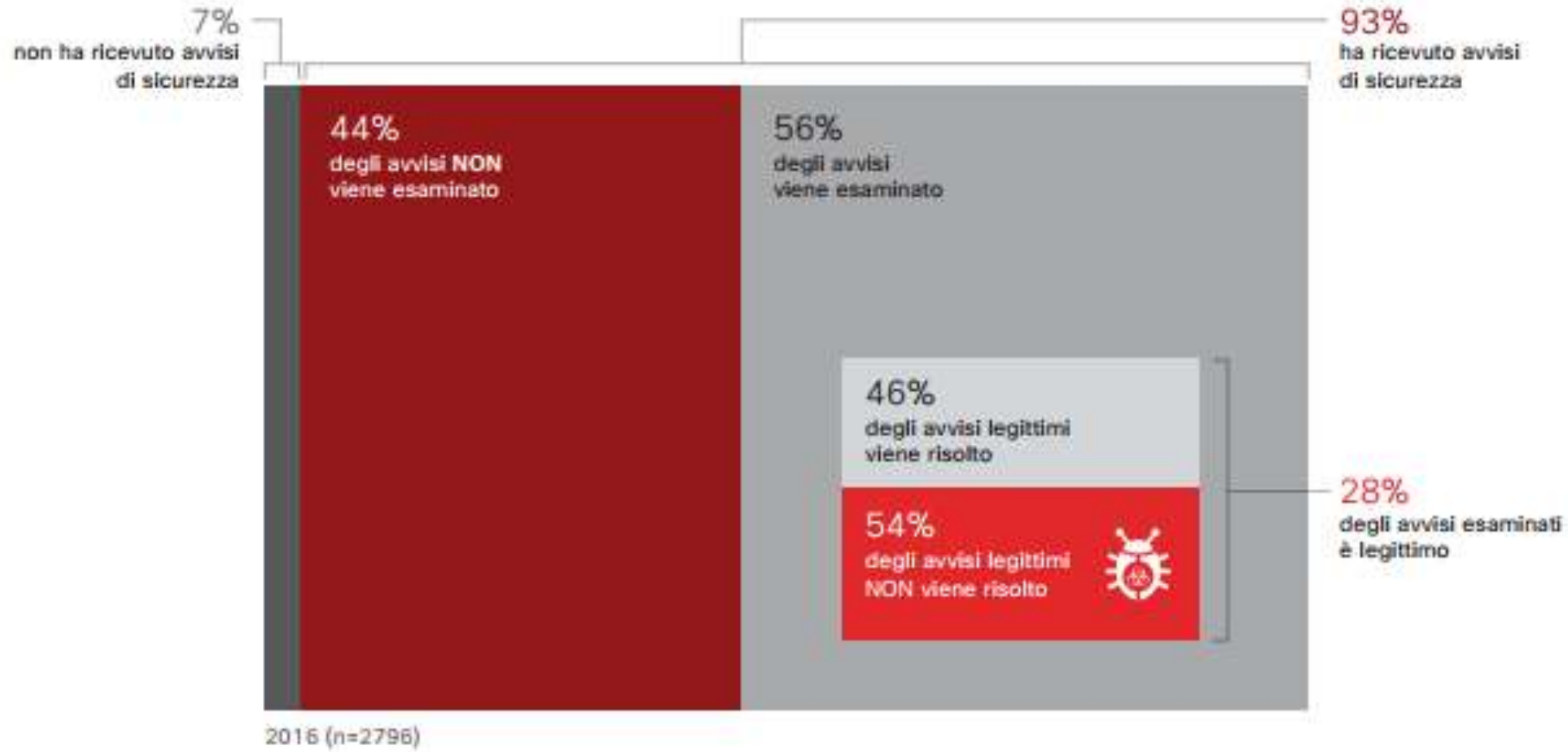
- [Critico] **Vulnerability in Server Service Could Allow Remote Code Execution** (MS08-067): questo aggiornamento di sicurezza risolve una vulnerabilità nel **servizio Server** sui sistemi Windows. Questa vulnerabilità può consentire l'esecuzione di codice in modalità remota se il sistema affetto riceve una richiesta RPC appositamente predisposta. Un attaccante potrebbe sfruttare questa vulnerabilità sui sistemi **Microsoft Windows XP** e **Windows Server 2003** per eseguire codice arbitrario senza autenticazione. Si ritiene che questa vulnerabilità possa essere utilizzata per realizzare un exploit con caratteristiche di worm.

Middleware: gli hacker individuano opportunità nel **software privo di patch**

Figura 41 Vulnerabilità riscontrate nelle librerie del middleware

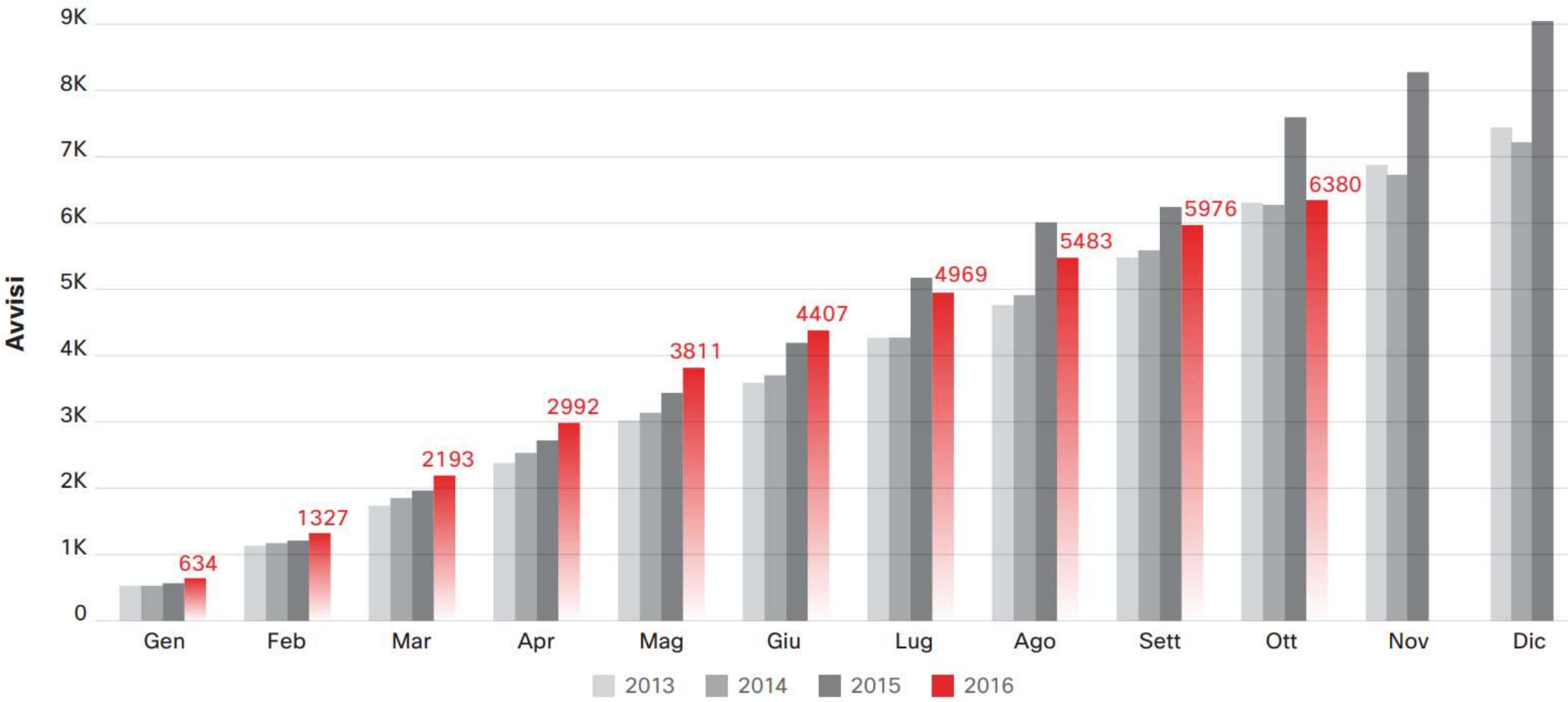
Quante volte siamo efficaci?

Figura 52 Percentuali di avvisi di sicurezza che non vengono analizzati o corretti

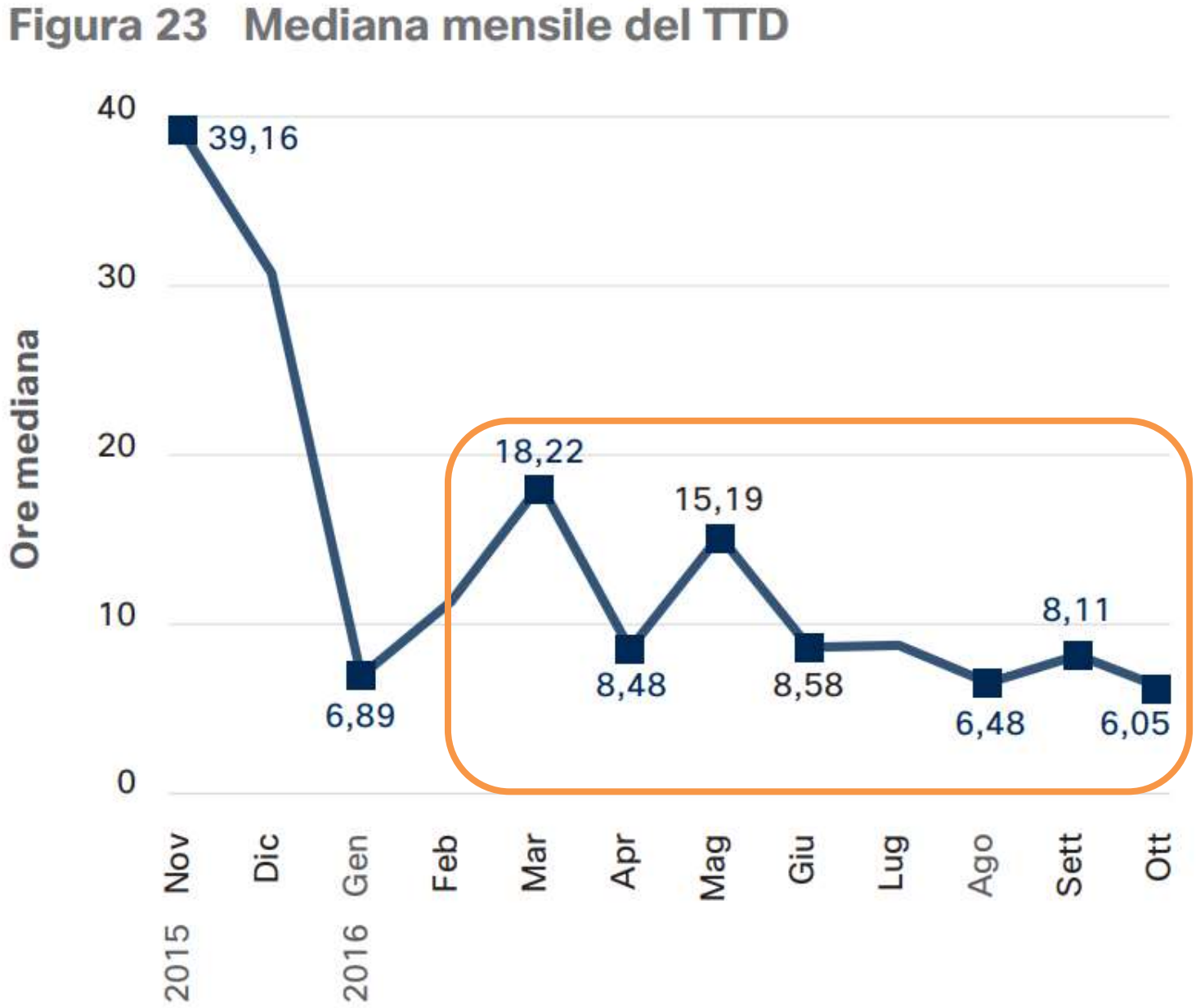


Qualche progresso: Vulnerabilità in declino nel 2016

Figura 37 Totale cumulativo annuo degli avvisi

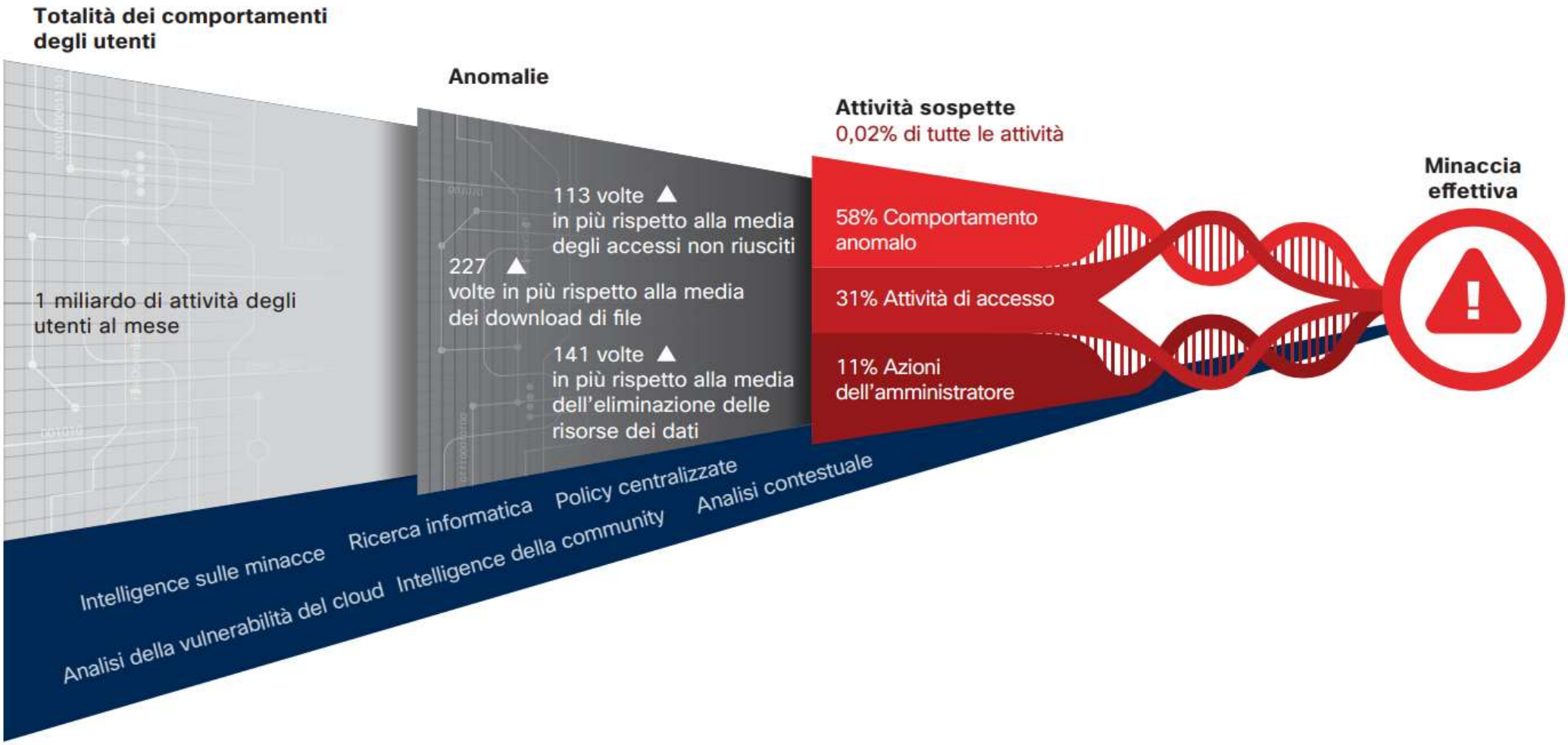


Tempi di rilevamento («Time To Detect»): metrica essenziale per misurare i nostri progressi sulla sicurezza



Solo **l'automazione** può aiutare a orientarsi nel "rumore" degli avvisi di sicurezza e a concentrarsi sull'analisi delle minacce reali

Figura 9 Identificazione dei modelli di comportamento degli utenti attraverso l'automazione (processo)



Gli strumenti devono fornire una **visione olistica**: la mancata integrazione può aprire falle che i criminali utilizzano per lanciare attacchi

5+

Figura 51 Numero di fornitori e prodotti di sicurezza utilizzati dalle aziende

Numero di fornitori di sicurezza nell'ambiente di sicurezza
2016 (n=2850), grafico arrotondato al numero intero più vicino

1-5 fornitori	6-10 fornitori	11-20 fornitori	21-50 fornitori	Più di 50 fornitori
45%	29%	18%	7%	3%

Il 55% utilizza più di 5 fornitori

Numero di prodotti per la sicurezza nell'ambiente di sicurezza
2016 (n=2860), grafico arrotondato al numero intero più vicino

1-5 prodotti	6-10 prodotti	11-25 prodotti	26-50 prodotti	Più di 50 prodotti
35%	29%	21%	11%	6%

Il 65% utilizza più di 5 prodotti

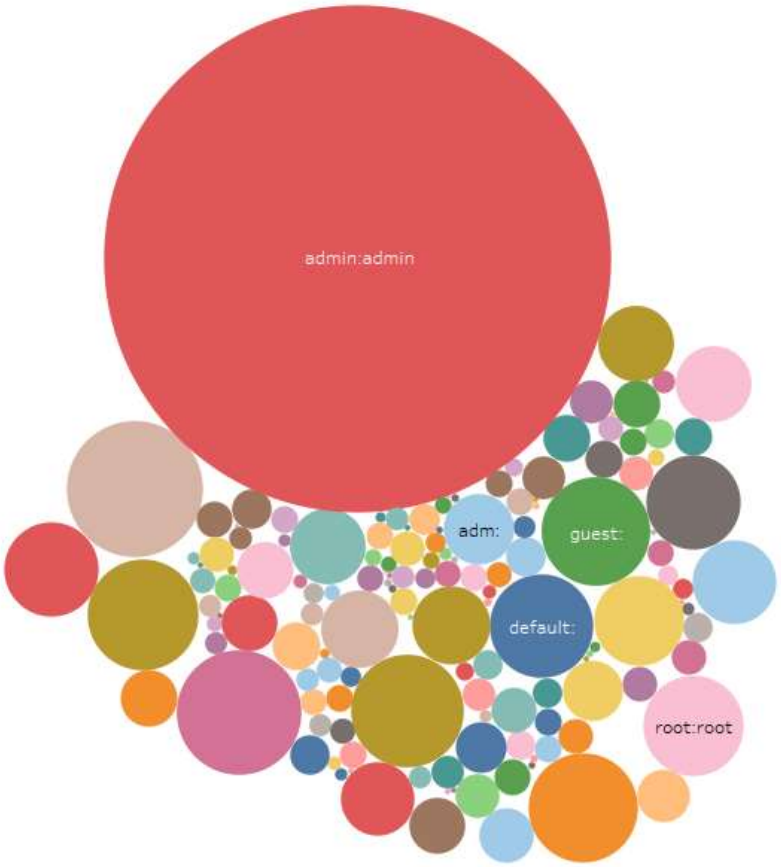
A volte basterebbe poco

Username Passwords Used in IOT Devices Visualisation

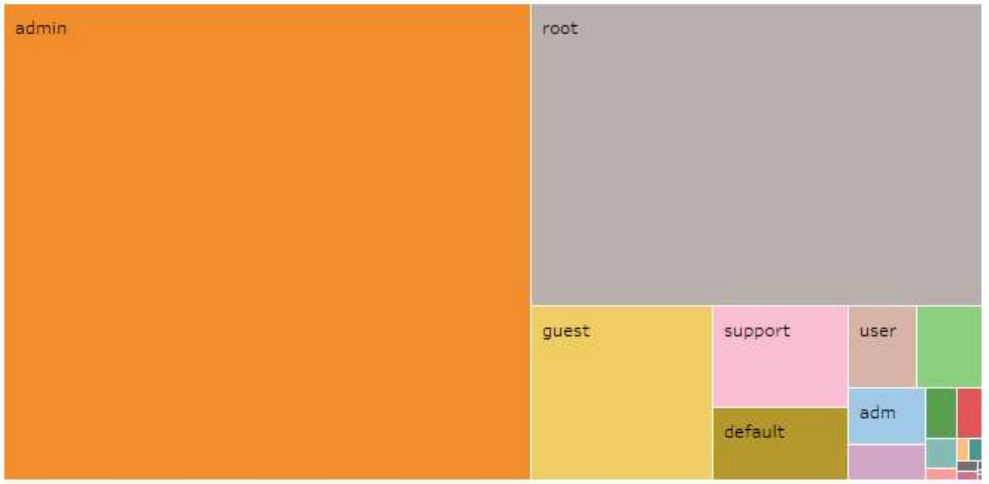
Recently about 33.000 Username/Password combinations from IOT devices have been released on Pastebin.
Read more at: https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse/
Created by @unbehandelt https://twitter.com/unbehandelt

Different Username/P..	142
Different Passwords	105
Different Users	19
Different IP	8.233
Number of Records	33.138

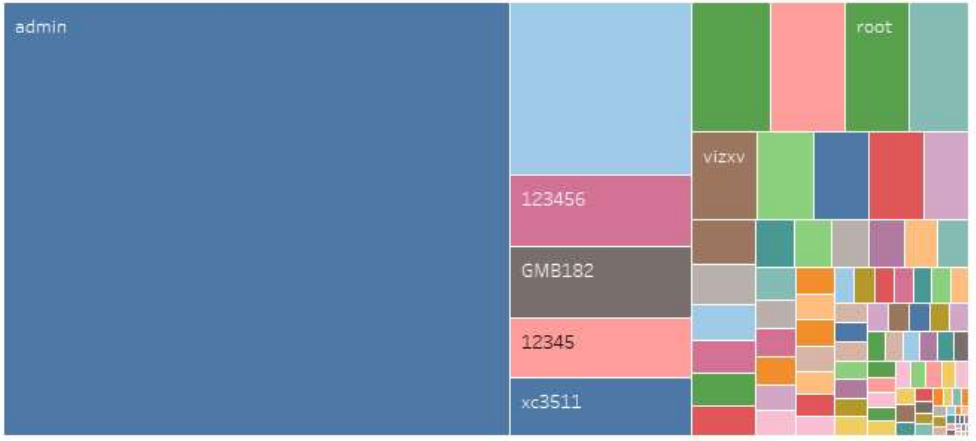
Different Username/Passwort Combinations Used



Different Usernames Used

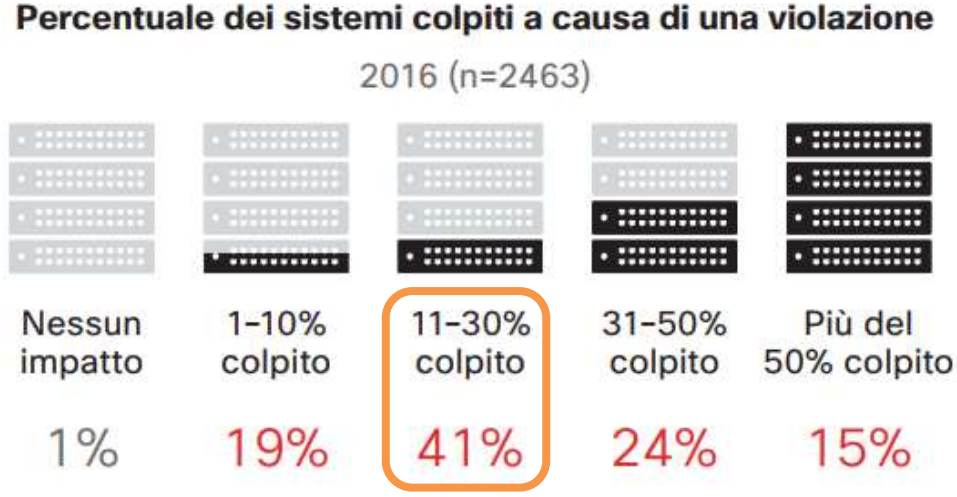


Different Passwords Used



L’impatto sul **business!**

Figura 53 Durata e dimensioni delle interruzioni causate da violazioni della sicurezza



L’impatto sul **business!**

Figura 56 Percentuale di opportunità di business perse a causa di un attacco

Figura 58 Percentuale di clienti persi dalle aziende a causa degli attacchi

42%
Ha riscontrato un numero notevole di opportunità perse
(n=625)

39%
Ha riscontrato una notevole perdita di clienti
(n=641)

Cosa ne pensano i CISO

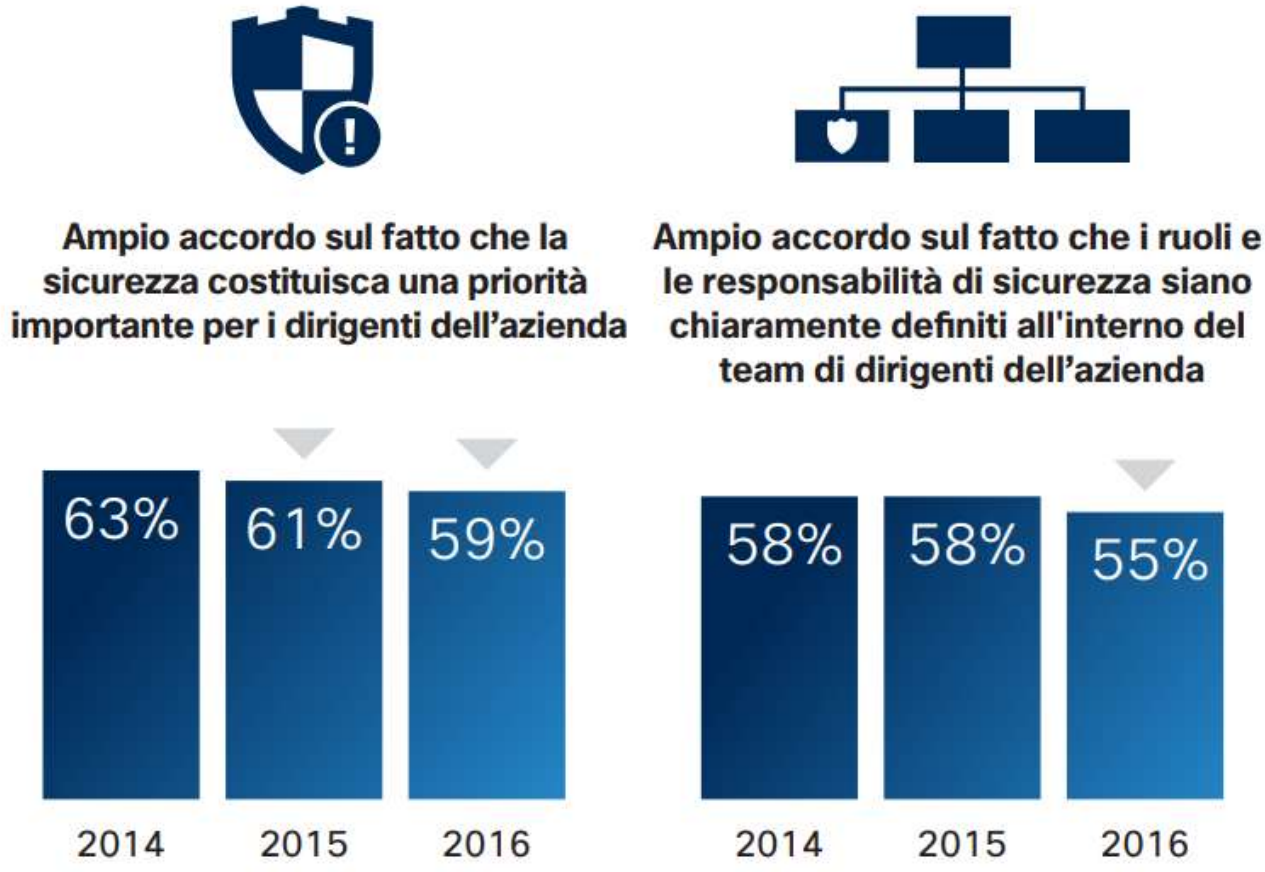
Figura 45 Percentuali di esperti della sicurezza che giudicano diversi strumenti di sicurezza estremamente efficaci

74%	71%
Ritiene di disporre di strumenti molto o estremamente efficaci contro minacce alla sicurezza note	Ritiene di disporre di strumenti molto o estremamente efficaci nel rilevare le anomalie di rete e nel difendere dinamicamente dalle variazioni delle minacce adattive

2016 (n=2912)

La sfida sta nell'ottenere il **sostegno del management** per adottare risposte efficaci

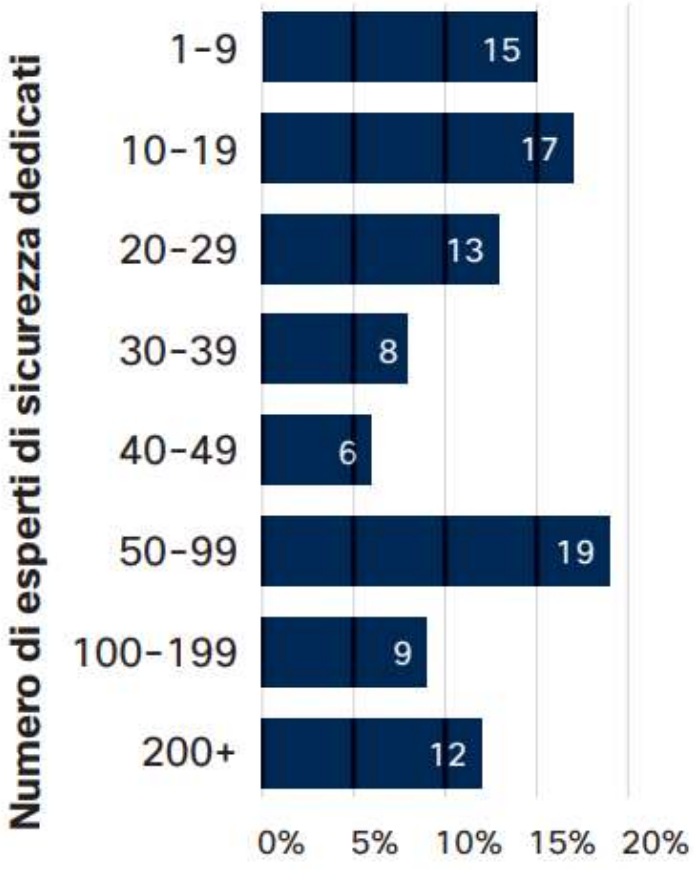
Figura 46 Percentuali di esperti della sicurezza che ritengono che la sicurezza sia di massima priorità a livello dirigenziale, 2014-2016



2014 (n=1738), 2015 (n=2432), 2016 (n=2912)

Le **grandi aziende** si sono comunque **strutturate**

Figura 48 Numero di esperti della sicurezza assunti dalle aziende

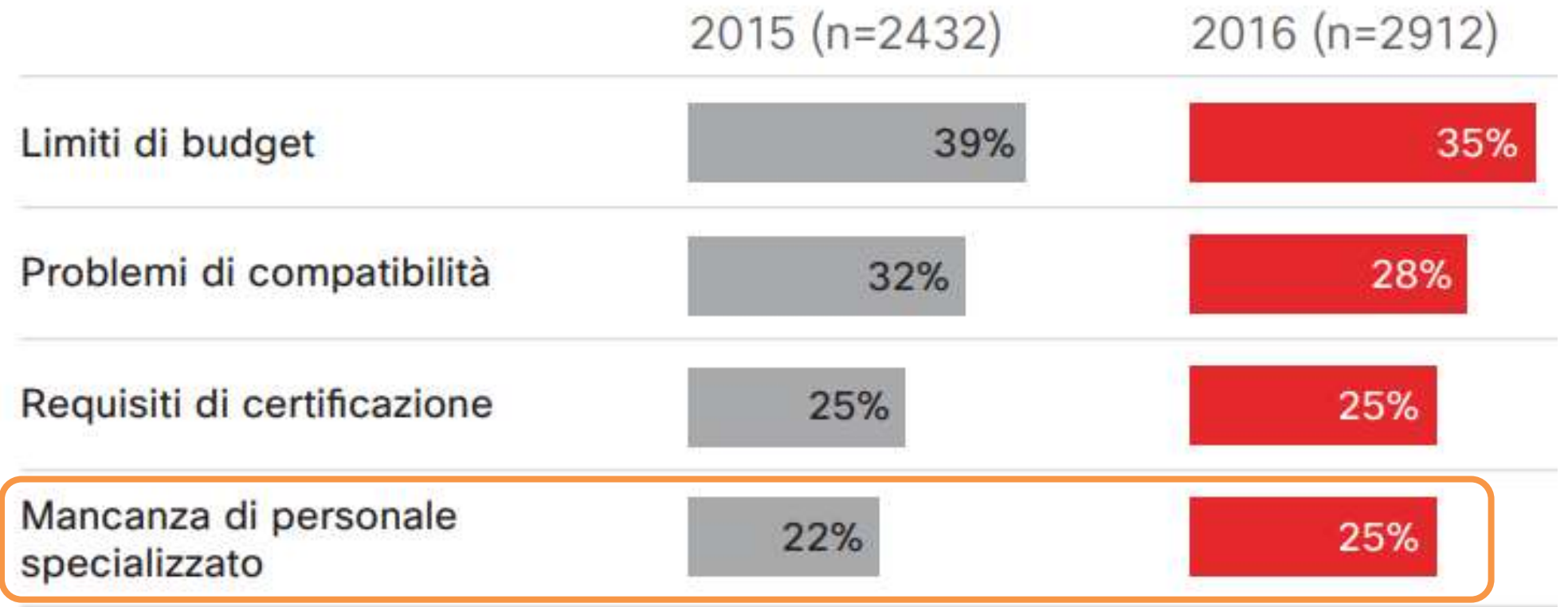


30 2014 | 25 2015 | 33 2016

Numero medio di esperti dedicati alla sicurezza

Limiti di tempo, risorse qualificate e fondi incidono sulla capacità di rispondere alle minacce

Figura 47 Maggiori ostacoli alla sicurezza



La «brutta bestia»: il cybersecurity skill gap

[WeLiveSecurity] Cybersecurity skills gap: It's big and it's bad for security

January 25, 2017 / Cybersecurity, Management, Recruiting, Technology, Top News

We have great expertise in supporting companies and candidates in their social recruiting and talent hunting journey, alleviating the "skill gap" issue. Our capabilities and problem-solving approach are proven by the appreciation of our many customers. Let's have a talk!

On this subject, here is an **article about the cybersecurity skill gap:** The cybersecurity skills gap, defined as a shortage of qualified people needed to fill open positions in IT security, is a phenomenon that I have researched quite extensively this year, and with good reason. You may have seen this recent headline:

"Donald Trump Advised to Train 100,000 Hackers to Protect the US"

I don't like the way that headline was worded, but I'm in agreement with the underlying point: the US President's Commission on Enhancing National Cybersecurity has strongly recommended that the country "should increase ... efforts on training security experts that would work for the country and not leave for the private sector, which has become a dramatic problem in the last few years" (Softpedia). And you may have seen other headlines, like this one from Forbes at the start of this year: "One Million Cybersecurity Job Openings In 2016". This is a problem that is negatively impacting governments, companies, non-profits, and even consumers (inadequate IT security staffing can lead to data breaches that expose your information).

Yes, the cybersecurity skills gap is *that* big

Having studied the numbers from multiple perspectives, I agree that the world is probably in need of one million more people with cybersecurity skills than are currently available to hire. The US alone needs something like 200,000 more people skilled in cybersecurity,

La Cybersecurity è un’opportunità per il canale?

I clienti cercano risorse qualificate in **outsourcing**, per sfruttare competenze non reperibili internamente, #1

Figura 60 Le aziende si affidano all'esternalizzazione

Servizi di sicurezza esternalizzati
2016 (n=2912)

Consulenza
51%

Reazione agli incidenti
45%

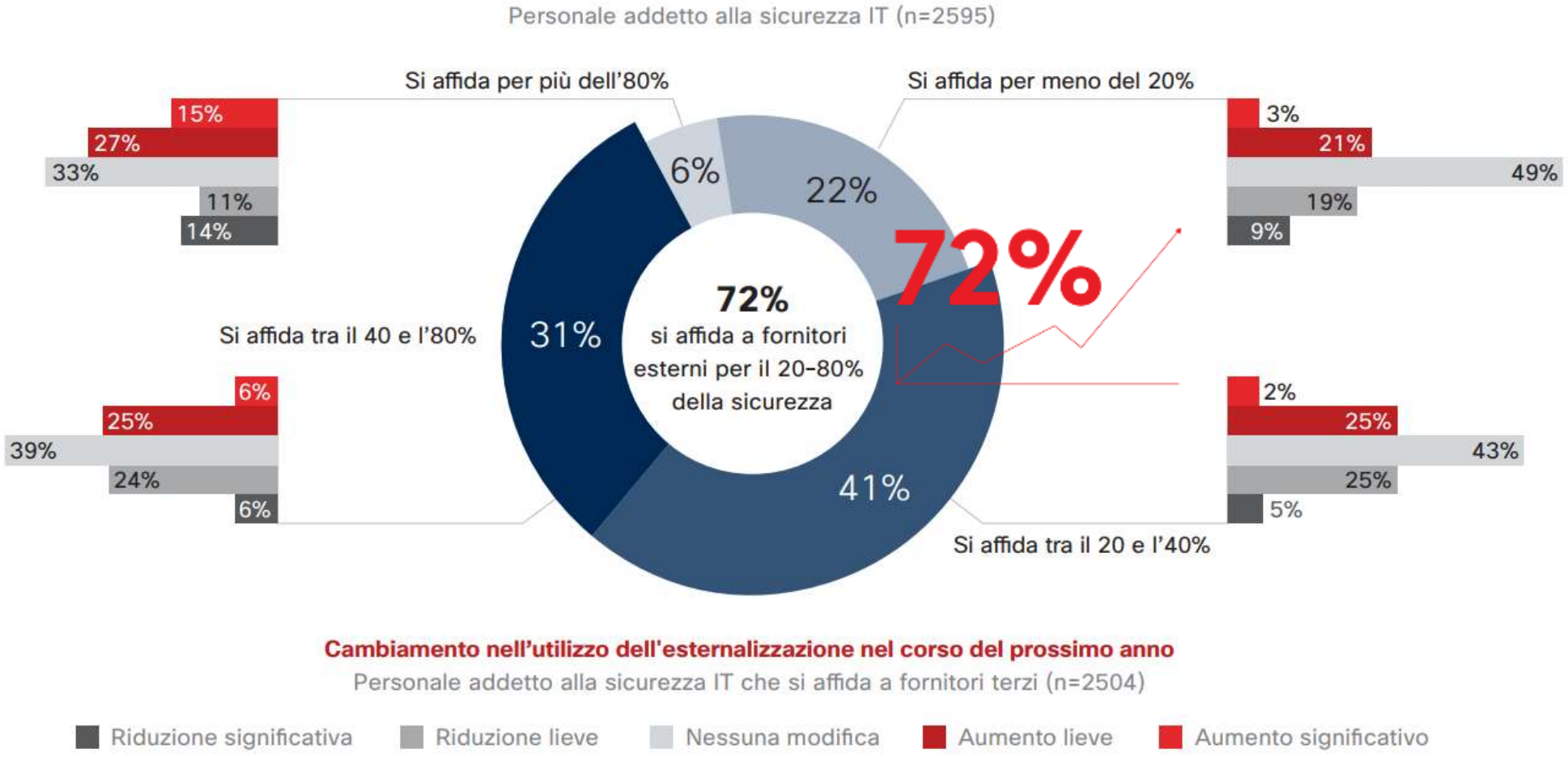
Motivo per cui i servizi vengono esternalizzati
2016 (n=2631)

Avere una maggiore efficienza dei costi
52%

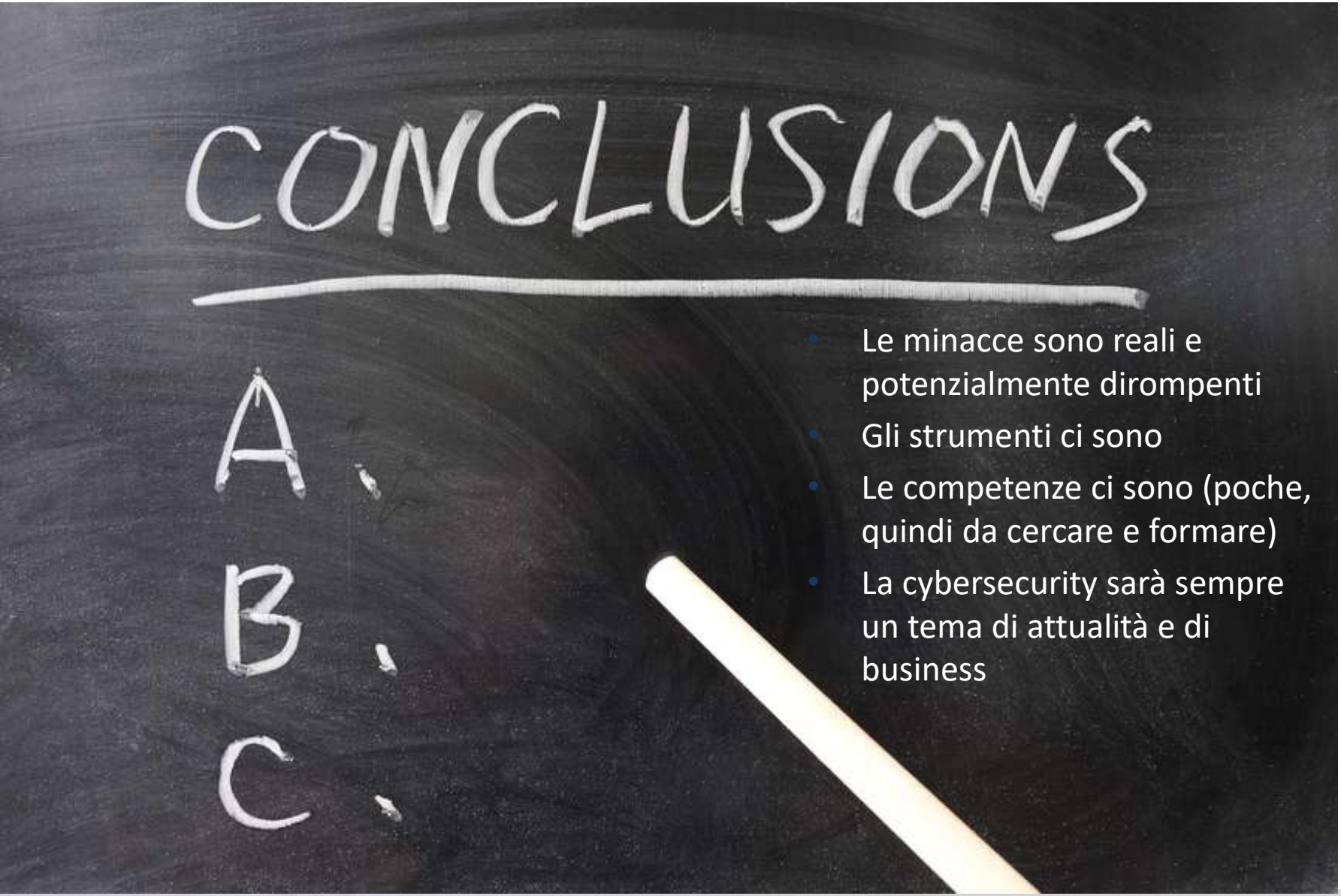
Ottenere analisi imparziali
48%

I clienti cercano risorse qualificate in **outsourcing**, per sfruttare competenze non reperibili internamente, #2

Figura 61 Percentuale con cui le aziende si affidano all'esternalizzazione



In conclusione



- Le minacce sono reali e potenzialmente dirompenti
- Gli strumenti ci sono
- Le competenze ci sono (poche, quindi da cercare e formare)
- La cybersecurity sarà sempre un tema di attualità e di business

Grazie e restiamo in contatto (www.primobonacina.com/)