Prima Giornata del Triveneto
5 ottobre 2018

GIORNATE del TRIVENETO

Associazione dei Dottori Commercialisti e degli Esperti Contabili delle Tre Venezie

POLITECNICO MILANO 1863

SCHOOL OF MANAGEMENT

OSSERVATORI.NET digital innovation

UBIQUE - il grande occhio del sesto potere. Privacy, Cybersecurity e Big Data

ASSOCIAZIONE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI DELLE TRE VENEZIE

Osservatorio Information Security & Privacy

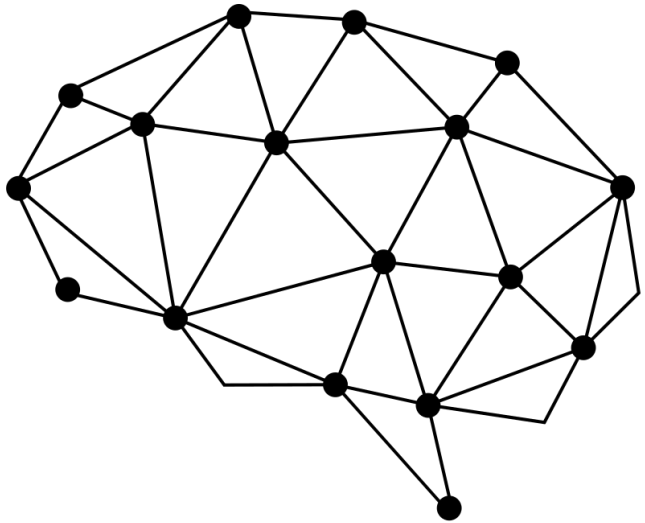
5 ottobre 2018

Nel 2017…


CORRIERE DELLA SERA
Attacco hacker in tutto il mondo
Colpiti 75 Paesi, anche l'Italia
Chiesti riscatti di 300 dollari a pc
The Guardian
'Petya' ransomware attack: what is it and how can it be stopped?
il POST
I dati di 143 milioni di clienti di Equifax sono stati rubati in un attacco hacker
la Repubblica.it
Uber, rubati i dati di milioni di clienti: la multinazionale ha taciuto e pagato un riscatto
WIRED
Meltdown e Spectre sono solo all'inizio.

2018

OSSERVATORI.NET digital innovation



Cambridge Analytica

2018

prestare il consenso solo ad alcuni utilizzi Clicca qui. Cliccando in un punto qualsiasi dello schermo, effettuando un'azione di scroll o chiudendo all'uso di tutti i cookie OK

MENU la Repubblica.it

Economia & Finanza con Bloomberg Seguici su

HOME MACROECONOMIA FINANZA LAVORO DIRITTI E CONSUMI AFFARI&FINANZA OSSERVA ITALIA CALCOLATORI

Marchionne malato da un anno, Fca non sapeva nulla. L'avvocato: "Vince il diritto alla privacy"

La famiglia conferma le parole dell'ospedale di Zurigo. Abbiamo chiesto al giuslavorista se si tratti di un caso in cui la privacy entra in collisione con l'interesse societario

di WALTER GALBIATI

26 Luglio 2018

L'ospedale di Zurigo ha comunicato che Marchionne era malato da un anno. Fca ha però sostenuto di non saperne nulla. Abbiamo chiesto a Vittorio Pomarici, giuslavorista, partner dello studio BonelliErede, se si tratti di un caso dove la privacy entra in collisione con l'interesse societario.

Il manager poteva non dire nulla alla sua azienda?

«Ciascuno ha diritto alla propria privacy, un diritto ancora più forte quando si parla di salute. Poteva

(agf)

TOP VIDEO

DAL WEB

Newsl

Venture

NAVIGA HOME RICERCA

24 ORE MONDO

ABBONATI ACCEDI

EUROPA USA AMERICHE MEDIO ORIENTE ASIA E OCEANIA RAPPORTO PAESE AMERICA E ASIA24

IBERIA

Ogni giorno come fosse il primo. Scopri di più

Accise benzina, primo taglio in manovra: ecco quanto costa ogni cent in meno

Scuola, più inglese in classe ma con scarsi risultati

La nuova flat tax per i professionisti, ecco a chi converrà

Senza shopping di domenica 400 milioni in meno ai lavoratori

IL CALO DEGLI UTENTI IN EUROPA

Facebook e Twitter contro l'Europa sui dati flop: «Colpa del Gdpr»

di Alberto Magnani | 27 luglio 2018

IBERIA

E' per momenti come questi che ci impegniamo per essere ancora i più puntuali

Analisi Clusit dei principali attacchi a livello globale

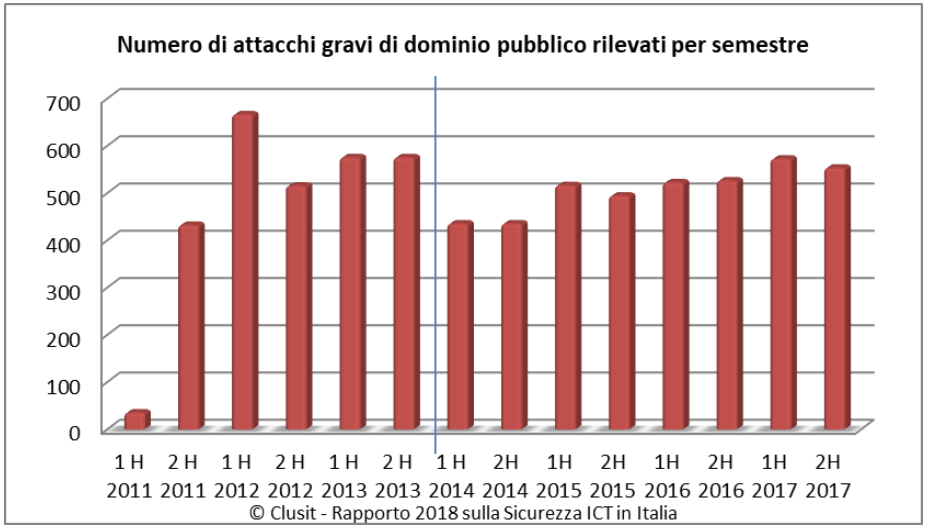
Quali sono i numeri del campione ?

In media negli ultimi 84 mesi abbiamo analizzato e classificato 83 attacchi gravi di dominio pubblico al mese (94 al mese nel 2017)

- **6.865** attacchi gravi analizzati dal gennaio 2011 al dicembre 2017.

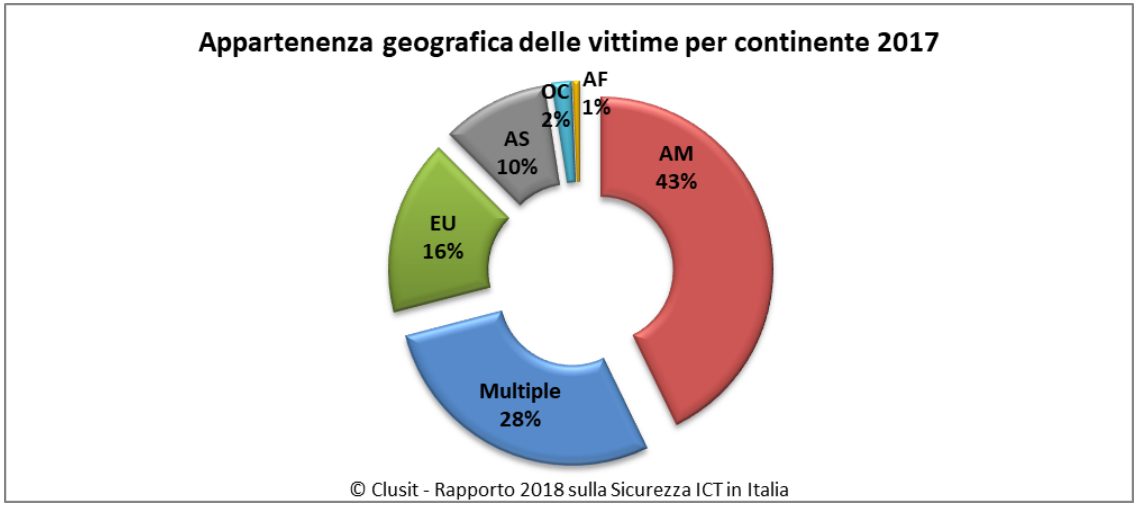
- 469 nel 2011
- 1.183 nel 2012
- 1.154 nel 2013

- 873 nel 2014 (*)
- 1.012 nel 2015
- 1.050 nel 2016
- **1.127 nel 2017**



(*) Nel 2014 il numero assoluto di attacchi gravi che abbiamo registrato è diminuito perché abbiamo reso più restrittivi i criteri di classificazione per allinearli al livello crescente di minaccia. Con i criteri precedenti sarebbe aumentato di circa il 10%. Nel 2015, pur applicando i nuovi criteri, la crescita rispetto al 2014 è pari al 14% Y/Y. Nel 2016 la crescita è del 3,75% Y/Y (circa +20% rispetto al 2014). Nel 2017, la crescita rispetto al 2014 è del 30%.

Distribuzione geografica vittime



Rispetto al 2016, nel 2017 diminuiscono leggermente le vittime di area americana (dal 53% al 43%), mentre rimangono invariati gli attacchi noti verso realtà basate in Europa (16%) e diminuiscono quelli contro bersagli in Asia (dal 16% al 10%).

La categoria "Multinational" cresce sostanzialmente (dall'11% del 2016 al **28%** del 2017, era il 9% nel 2015), ad indicare la tendenza a colpire in modo trasversale bersagli sempre più importanti, di natura transnazionale.

Tipologia e distribuzione degli attaccanti

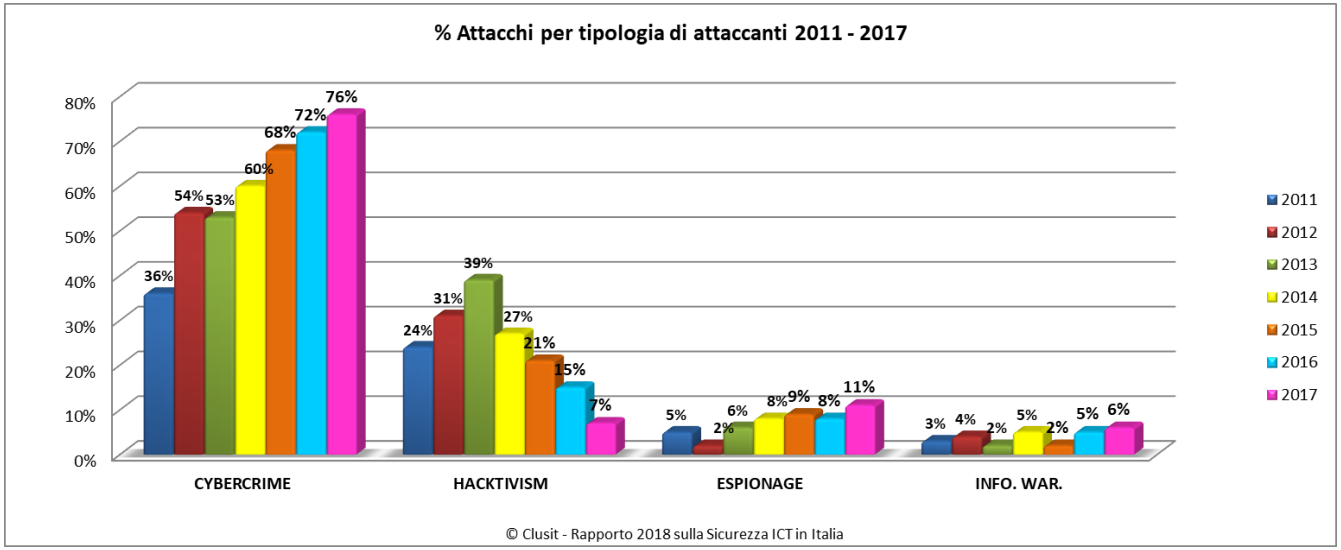
ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	Variazioni 2017 su 2016	Trend 2017
Cybercrime	526	684	751	857	14,11%	↑
Hacktivism	236	209	161	79	-50,93%	↓
Espionage / Sabotage	69	96	88	129	46,59%	↑
Information Warfare	42	23	50	62	24,00%	↑
TOTALE	**873**	**1.012**	**1.050**	**1.127**	**+7,33%**	↗

In termini assoluti, nel 2017 le categorie “Cybercrime”, “Cyber Espionage” e “Information Warfare” fanno registrare il numero di attacchi più elevato degli ultimi 7 anni.

Dal campione emerge chiaramente che, con l’esclusione delle attività riferibili ad attacchi della categoria “Hacktivism” che diminuisce sensibilmente (-50%) rispetto al 2016), nel 2017 gli attacchi gravi compiuti per finalità “Cybercrime” sono in aumento (+14%), così come quelli riferibili ad attività di “Information warfare” (+24%), mentre crescono sensibilmente gli attacchi del gruppo “Cyber Espionage” (46%).

Va sottolineato che, rispetto al passato, oggi risulta più difficile distinguere nettamente tra queste due ultime categorie: sommando gli attacchi di entrambe, nel 2017 si assiste ad un aumento del 38% rispetto all’anno precedente (191 contro 138).

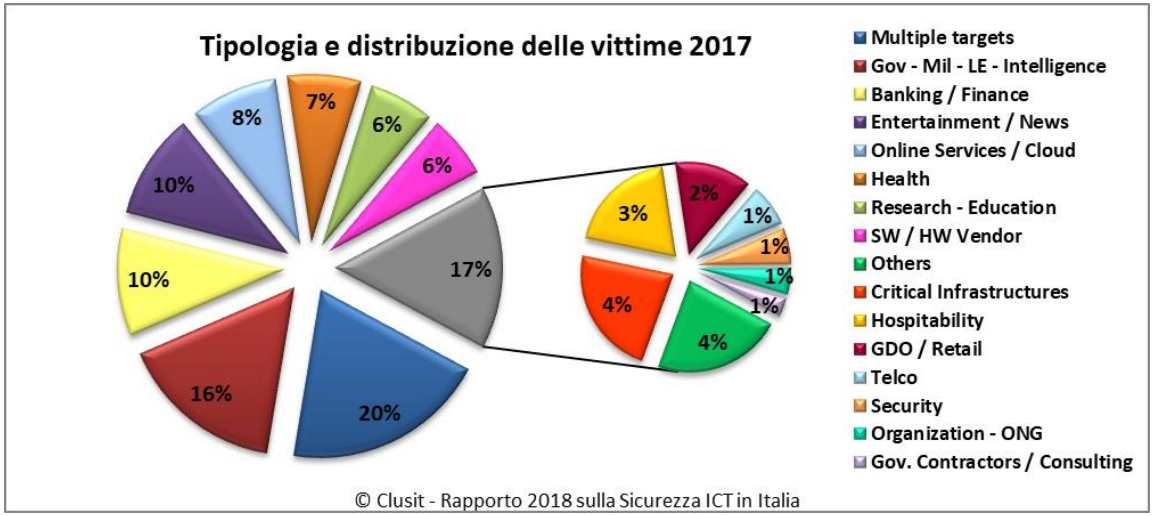
Tipologia e distribuzione degli attaccanti (7 anni)



Il Cybercrime passa dal 72% al **76**% del totale, mentre l'Hacktivism diminuisce di 32 punti percentuali rispetto al suo picco del 2013, passando da oltre un terzo a meno di un decimo dei casi analizzati.

Per quanto riguarda le attività di Espionage, rispetto alla percentuale degli attacchi gravi registrati nel 2016 la quota di attacchi nel 2017 è in aumento dal 8 all'11%, mentre l'Information Warfare risulta essere in crescita (nonostante la scarsità di informazioni pubbliche in merito), dal 5% al 6%.

Distribuzione vittime nel mondo (2017)

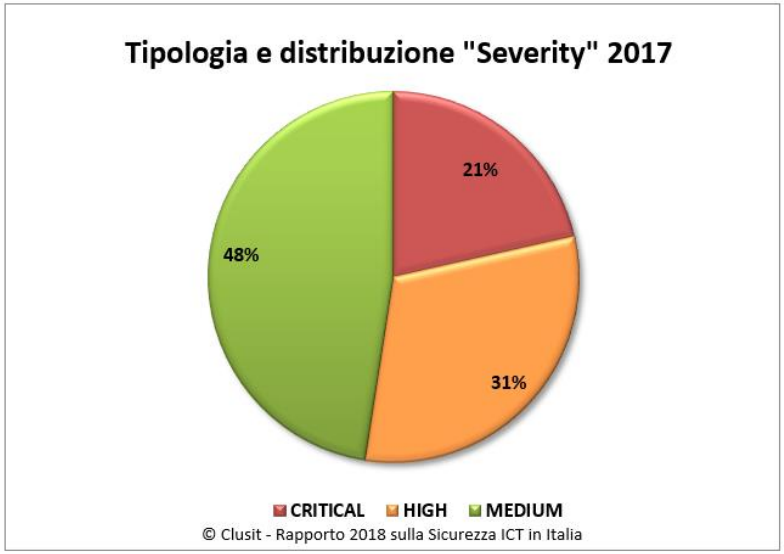


Nel 2017 al primo posto assoluto balza la categoria “Multiple Targets” (20%), superando per la prima volta il settore “Gov”, in diminuzione al 16%, che fin dal 2011 è sempre stato al primo posto nel nostro studio. Rispetto al 2016, nel 2017 “Banking/Finance” sale al terzo posto (10%) insieme a “Entertainment/News” (10%), seguiti da “Online Services / Cloud” (8%) e “Health” (7%). Salgono al 6% “Software/Hardware Vendor” e “Research/Education”, mentre la categoria “Others” (anche a causa dell’introduzione della nuova categoria “Multiple Targets”), scende al 4%.

Distribuzione vittime nel mondo (2017)

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	Variazioni 2017 su 2016	Trend 2017
Institutions: Gov - Mil - LEAs - Intelligence	213	223	220	179	-18,64%	↓
Others	172	51	38	40	5,26%	↗
Entertainment / News	77	138	131	115	-12,21%	↘
Online Services / Cloud	103	187	179	95	-46,93%	↓
Research - Education	54	82	55	71	29,09%	↑
Banking / Finance	50	64	105	117	11,43%	↑
Software / Hardware Vendor	44	55	56	68	21,43%	↑
Telco	18	18	14	13	-7,14%	↘
Gov. Contractors / Consulting	13	8	7	6	-14,29%	↘
Security Industry	2	3	0	11	-	↗
Religion	7	5	6	0	-	↓
Health	32	36	73	80	9,59%	↑
Chemical	5	2	0	0	-	→
Critical Infrastructures	13	33	38	40	5,26%	↗
Automotive	3	5	4	4	-	→
Org / ONG	47	46	13	8	-38,46%	↓
Multiple Targets	-	-	49	222	353,06%	↑
GDO / Retail	20	17	29	24	-17,24%	↘
Hospitability	-	39	33	34	3,03%	↗

Valutazione degli impatti (“Severity”) 2017



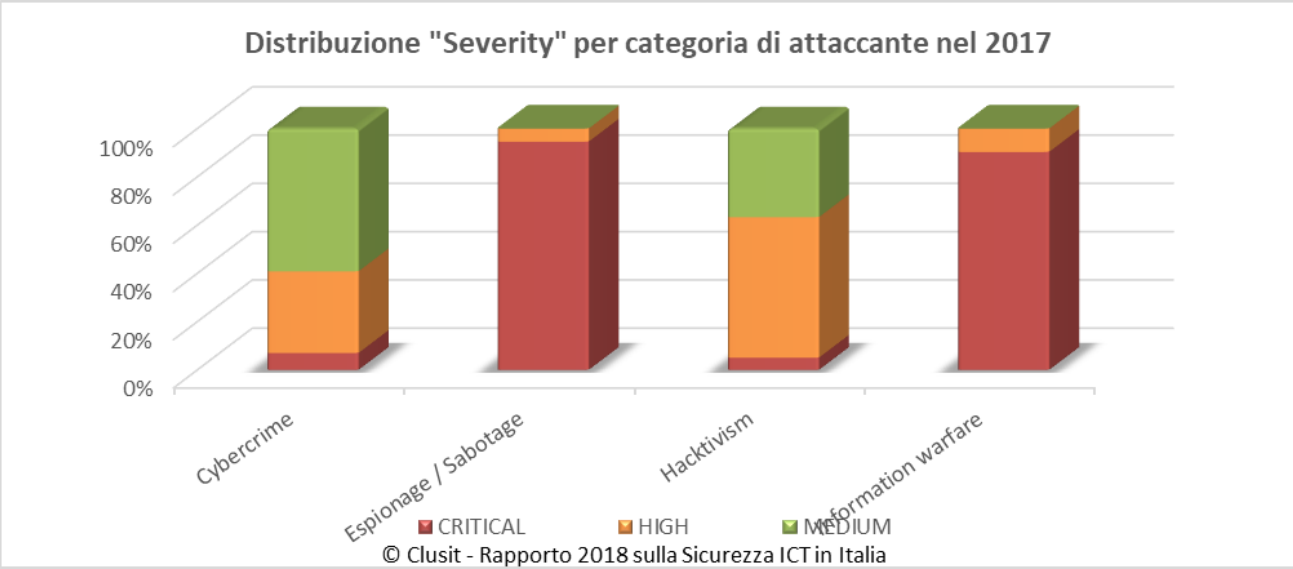
Per la prima volta quest’anno abbiamo definito tre categorie o livelli di impatto (considerato che stiamo comunque analizzando un campione di attacchi già tutti definiti come “gravi”): Medio, Alto e Critico.

Le variabili che contribuiscono a comporre la valutazione dell’impatto per ogni singolo attacco analizzato sono molteplici, ed includono: impatto geopolitico, sociale, economico (diretto e indiretto), di immagine e di costo/opportunità per le vittime.

Gli attacchi con impatto “Medio” rappresentano nel nostro campione quasi la metà del totale (**48%**), quelli di livello “Alto” un terzo (**31%**) e quelli di livello “Critico” un quinto (**21%**).

Raggruppando i dati per le consuete categorie (Attaccanti, Vittime e Tecniche di attacco) emergono ulteriori elementi di interesse.

Cyber Crime = tanti incidenti di basso impatto
Spionaggio Industriale = pochi incidenti ad alto impatto

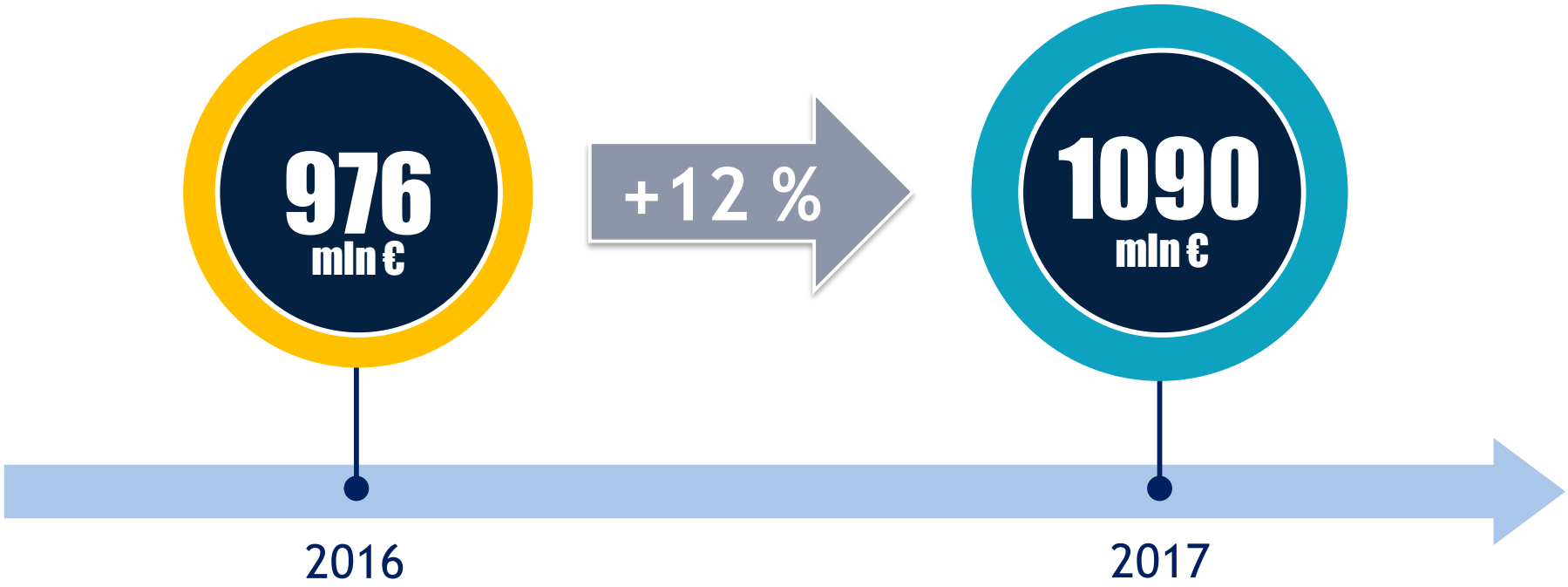


Trends 2018

- «Salto quantico" (soprattutto per Espionage e State sponsored attacks / Information Warfare): siamo in territorio inesplorato
- Phishing (via mail, IM e Social) ancora in crescita
- Malware per piattaforme Mobile sempre più diffuso e sofisticato
- Internet of Things troppo insicuro, rischi sistemici crescenti
- Discesa in campo degli Stati e aumento della (cyber) tensione
- Cyber crime sempre più aggressivo e organizzato

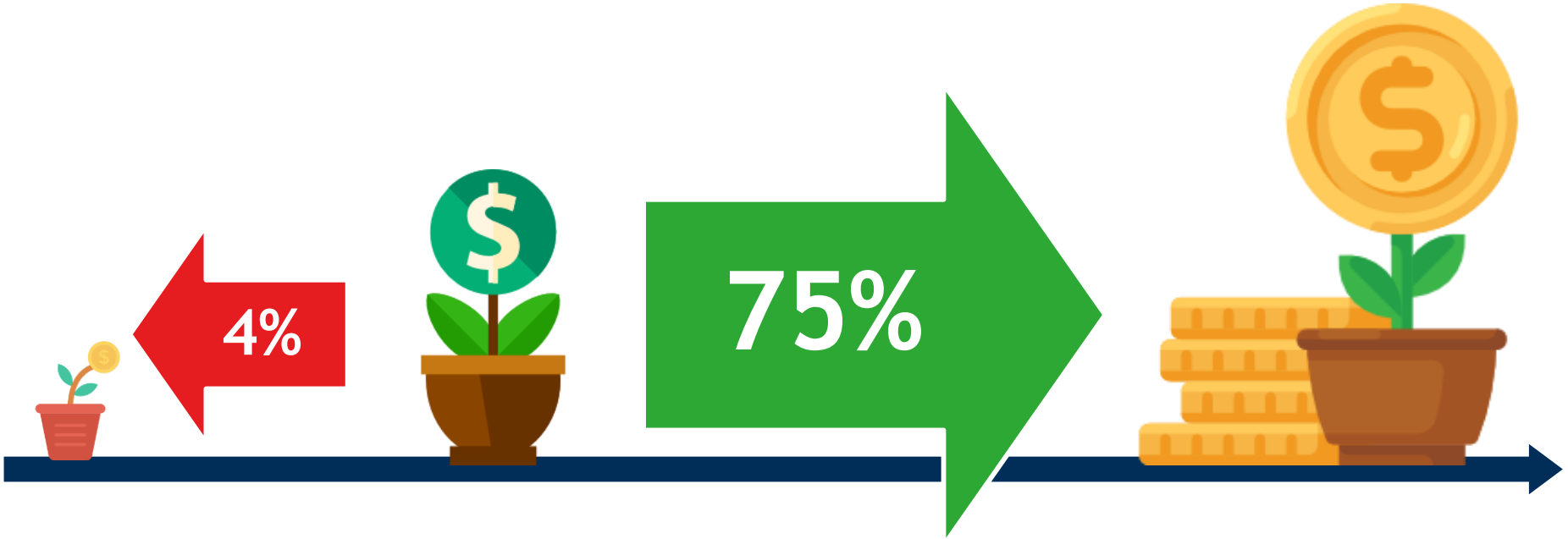
Il mercato Information Security 2017

OSSERVATORI.NET digital innovation



Campione: 1107 organizzazioni italiane

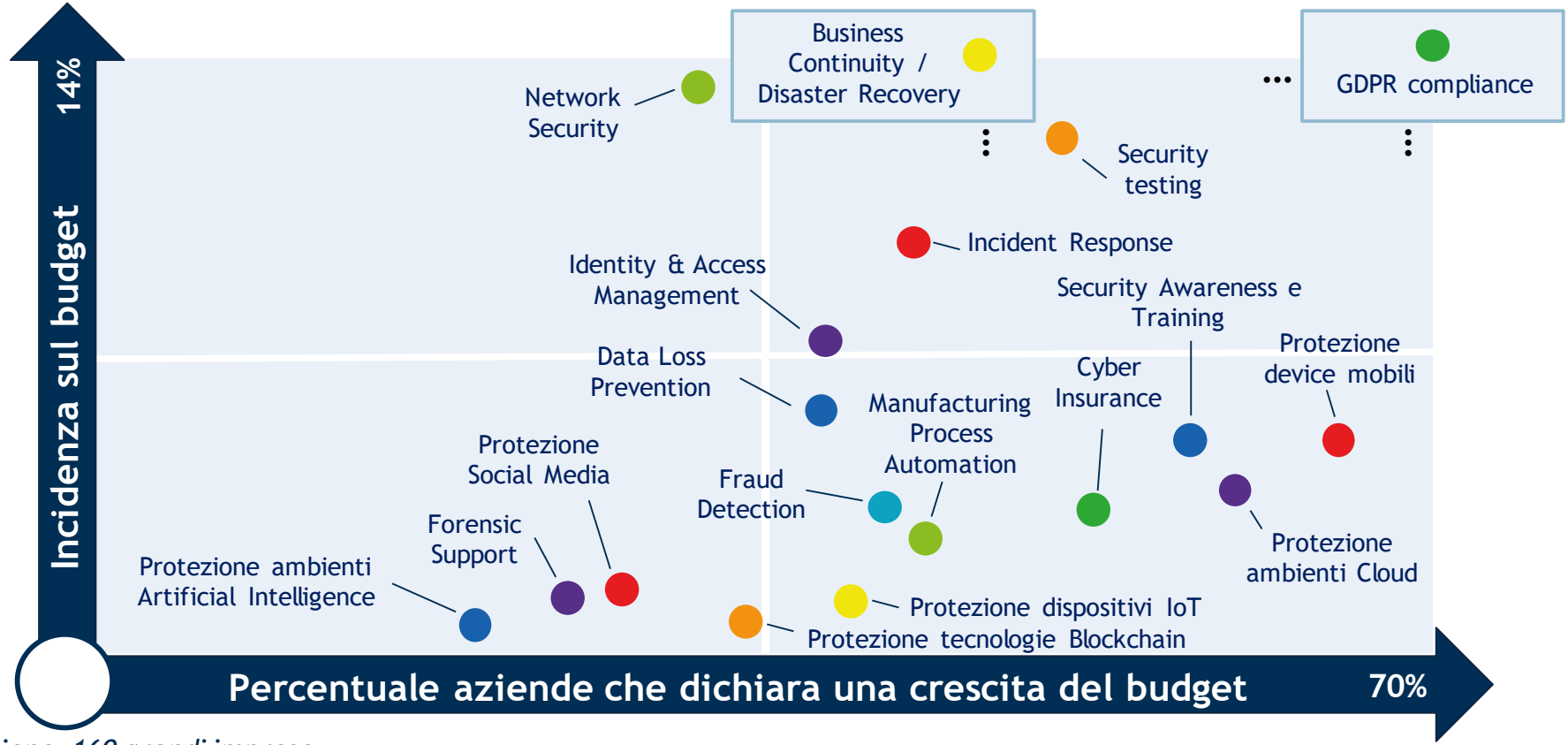
La crescita del budget



Campione: 160 grandi imprese

La scomposizione del mercato Information Security

OSSERVATORI.NET digital innovation



Campione: 160 grandi imprese

Le principali motivazioni di spesa delle PMI

OSSERVATORI.NET digital innovation

TUTELA DEI DATI DEI CLIENTI

45%

ADEGUAMENTO ALLE NORMATIVE

19%

ATTACCHI INFORMATICI SUBITI

11%

TUTELA DELLA PROPRIETÀ INTELLETTUALE

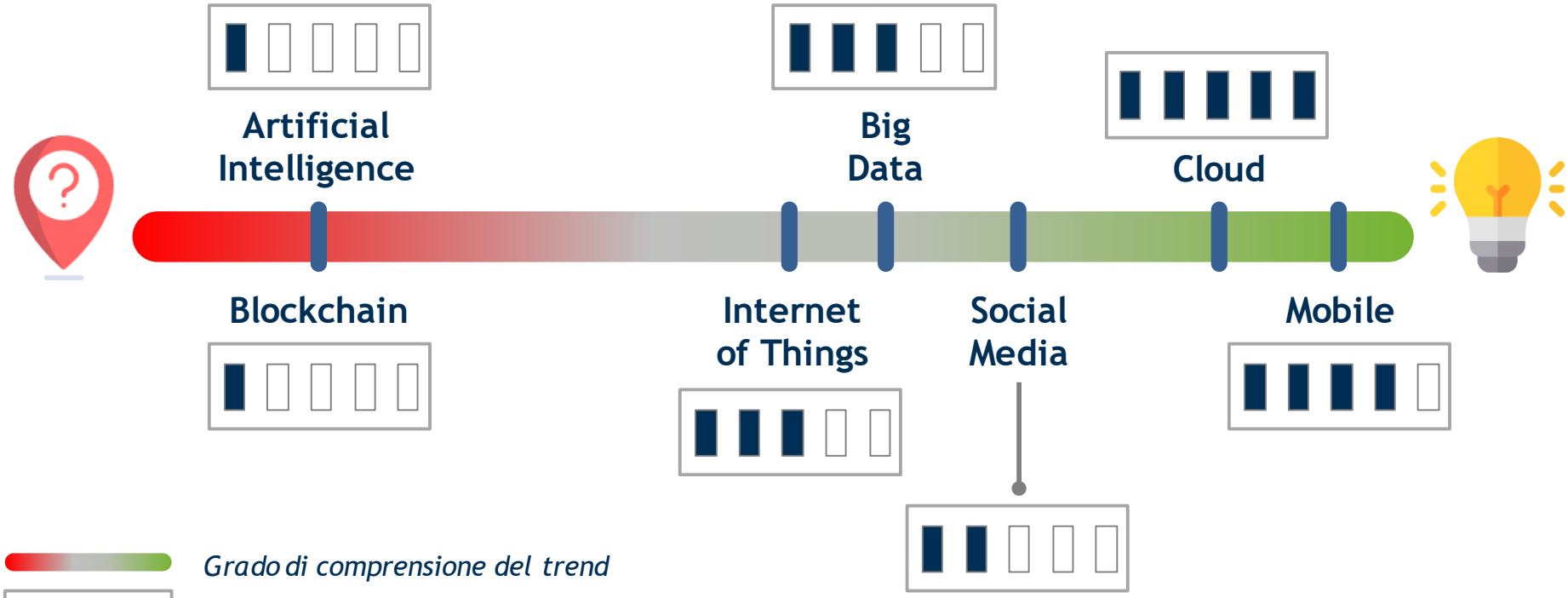
8%

PROTEZIONE DI AMBITI APPLICATIVI CORE

6%

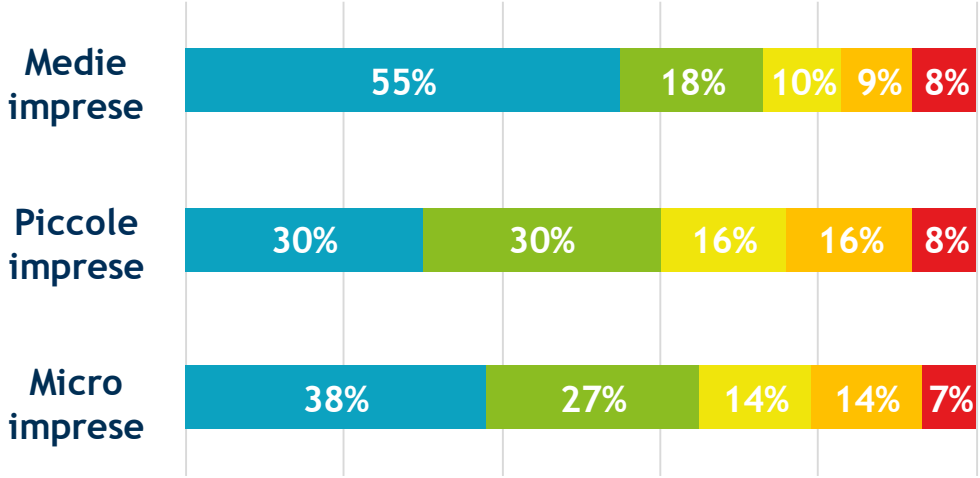
Dati ottenuti tramite un'elaborazione statistica di un campione di 947 micro, piccole e medie imprese (addetti compresi tra 2 e 249)

I trend dell'innovazione digitale



Le PMI: i trend tecnologici e l'impatto sulla security

OSSERVATORI.NET digital innovation

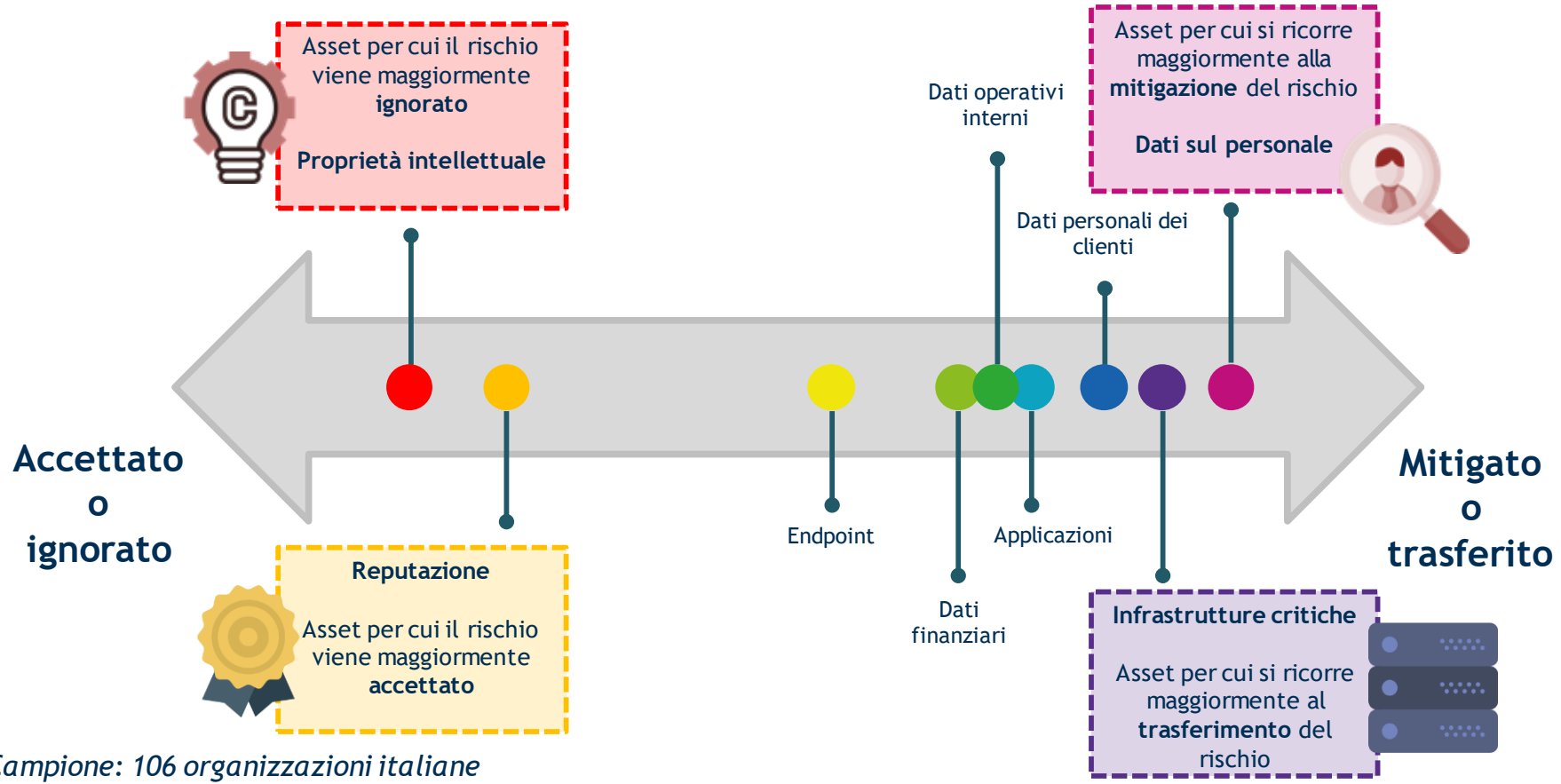


Principale trend che influenza le scelte di security:

- Cloud
- Big Data
- Social
- Mobile
- Internet of Things

Dati ottenuti tramite un'elaborazione statistica di un campione di 947 micro, piccole e medie imprese (addetti compresi tra 2 e 249)

Gli approcci per la gestione del rischio



Campione: 106 organizzazioni italiane

GDPR: l'orizzonte di pianificazione

OSSERVATORI.NET digital innovation

Campione: 160 grandi imprese

La crescita dell'organico

OSSERVATORI.NET digital innovation

Campione: 160 grandi imprese

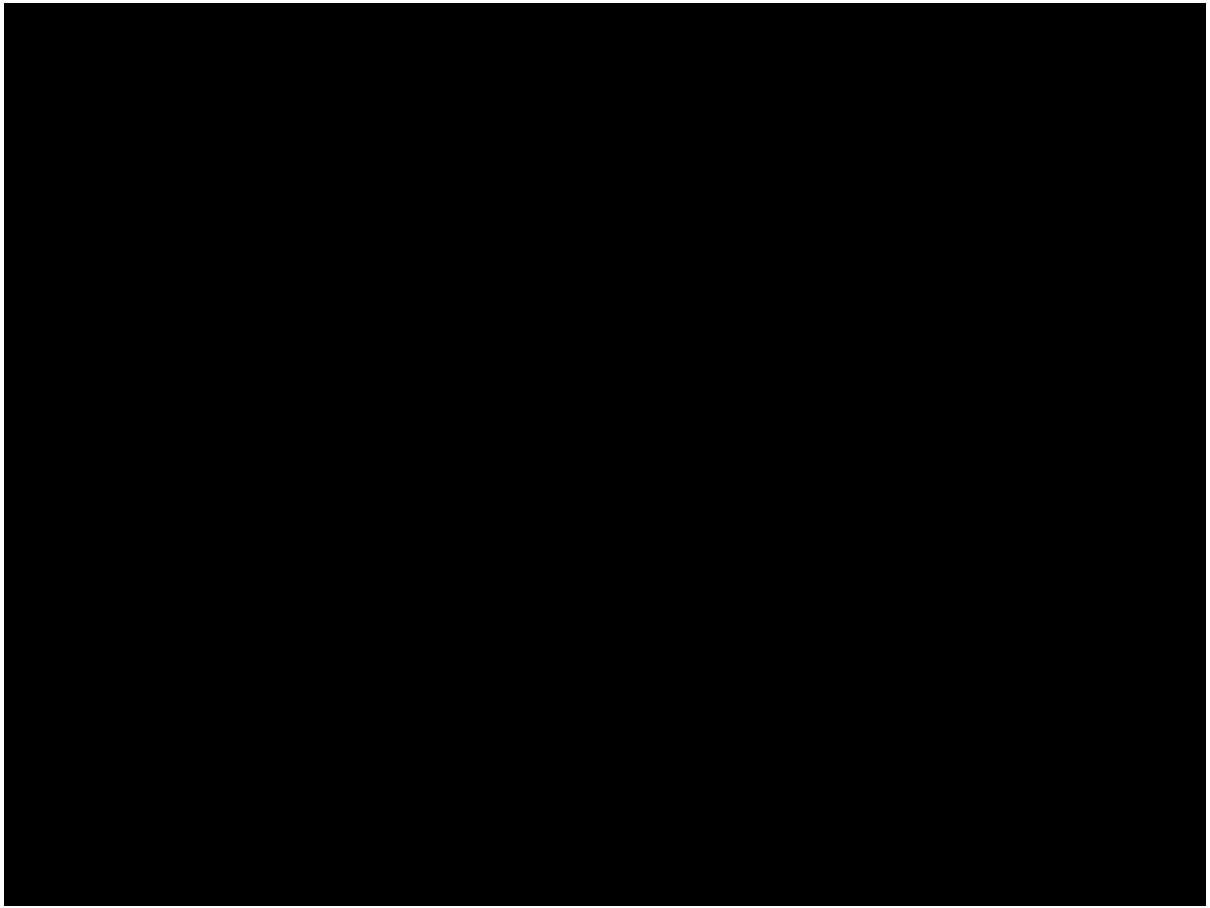
Ti sei mai chiesto…?

Garante per la protezione dei dati personali

SEI UN RAGAZZO/A:

- Se sapessi che il vicino di casa o il tuo professore possono accedere al tuo profilo e al tuo diario on-line, scriveresti le stesse cose e nella stessa forma?
- Sei sicuro che le foto e le informazioni che pubblichi ti piaceranno anche tra qualche anno?
- Prima di caricare/postare la "foto ridicola" di un amico, ti sei chiesto se a te farebbe piacere trovarti nella stessa situazione?
- I membri dei gruppi ai quali sei iscritto possono leggere le informazioni riservate che posti sul tuo profilo?
- Sei sicuro che mostreresti "quella" foto con il tuo ex anche al tuo nuovo ragazzo/a?
- Vuoi veramente far sapere a chiunque dove ti trovi (si chiama geolocalizzazione) e chi stai incontrando in ogni momento della giornata?
- Prima di inviare, anche per gioco, un video sexy al tuo nuovo compagno, hai considerato che potrebbe essere condiviso con i suoi amici o con degli sconosciuti?

Dall’altra parte, potrebbe esserci CHIUNQUE!



«LEONI DA TASTIERA» - Lucarelli: ALICE

«LEONI DA TASTIERA» - Lucarelli: EMANUELE

Regole base

1

VITA DIGITALE – VITA REALE

- Non esiste più una separazione tra la vita “on-line” e quella “off-line”.
- Quello che scrivi e le immagini che pubblichi sui social network hanno quasi sempre un riflesso diretto sulla tua vita di tutti i giorni, e nei rapporti con amici, familiari, compagni di classe, colleghi di lavoro.
- L’effetto può non essere necessariamente immediato, ma ritardato nel tempo.

Regole base

2

PER SEMPRE… O QUASI

- Quando inserisci i tuoi dati personali su un sito di social network, ne perdi il controllo.
- I dati possono essere registrati da tutti i tuoi contatti e dai componenti dei gruppi cui hai aderito, rielaborati, diffusi, anche a distanza di anni.
- A volte, accettando di entrare in un social network, concedi al fornitore del servizio la licenza di usare senza limiti di tempo il materiale che inserisci on-line… le tue foto, le tue chat, i tuoi scritti, le tue opinioni.

Regole base

3

IL MITO DELL'ANONIMATO

- Non è poi così difficile risalire all'identità di coloro che pubblicano testi, immagini, video su Internet con l'intento di danneggiare l'immagine o la reputazione di un'altra persona.
- L'anonimato in rete può essere usato per necessità, ma mai per commettere reati: in questo caso le autorità competenti hanno molti strumenti per intervenire e scoprire il "colpevole".

Regole base

4

LA PRIVACY E IL RISPETTO DEGLI ALTRI

- Quando metti on-line la foto di un tuo amico o di un familiare, quando lo “tagghi” (inserisci, ad esempio, il suo nome e cognome su quella foto), domandati se stai violando la sua privacy.
- Nel dubbio chiedigli il consenso. Non lasciarti trascinare dagli hater, dai troll, nel gioco perverso dei gruppi “contro qualcuno”: la prossima volta potresti essere tu la vittima.

Regole base

5

NON SONO IO!

- Attenzione ai falsi profili.
- Basta la foto, il tuo nome e qualche informazione sulla tua vita per impadronirsi on-line della tua identità.
- Sono già molti i casi di attori, politici, personaggi pubblici, ma anche di gente comune, che hanno trovato su social network e blog la propria identità gestita da altri.

Regole base

6

DISATTIVAZIONE O CANCELLAZIONE?

- Se decidi di uscire da un social network spesso ti è permesso solo di “disattivare” il tuo profilo, non di “cancellarlo”.
- I dati, i materiali che hai messo on-line, potrebbero essere comunque conservati nei server, negli archivi informatici dell’azienda che offre il servizio.
- Leggi bene cosa prevedono le condizioni d'uso e le garanzie di privacy offerte nel contratto che accetti quando ti iscrivi.

Regole base

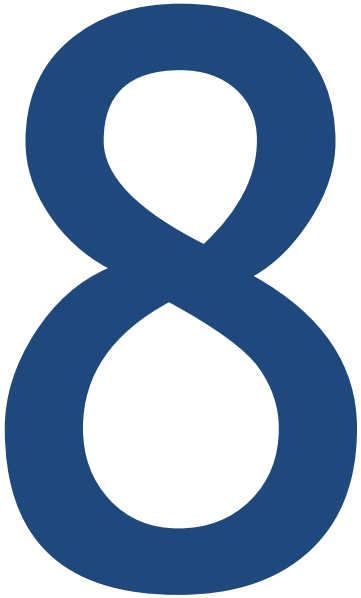
7

CHI PUÒ FARE COSA

- Rifletti bene prima di inserire on-line dati che non vuoi vengano diffusi o che possano essere usati a tuo danno.
- Segnala al Garante della privacy e alle altre autorità competenti le eventuali violazioni affinché possano intervenire a tua tutela.

RICORDA: il miglior difensore della tua privacy sei innanzitutto TU.

Regole base



LA LOGICA ECONOMICA: NIENTE È GRATIS

- Le aziende che gestiscono i social network generalmente si finanziano vendendo pubblicità mirate.
- Le informazioni raccolte su di te sono infatti usate per monitorare e prevedere i tuoi acquisti, le tue scelte, i tuoi comportamenti.

RICORDA: anche nel web, dietro l'offerta di un servizio "gratuito", si nasconde lo sfruttamento per molteplici scopi dei tuoi dati.

Regole base

9

CI SONO AMICI E AMICI

- Nelle amicizie esistono differenti livelli di relazione a seconda che ci si rapporti con amici stretti o semplici conoscenti, compagni di classe o professori, partner commerciali o datori di lavoro.
- Sui social network spesso poniamo tutti sullo stesso piano, rischiando di scrivere o mostrare la cosa sbagliata alla persona sbagliata.
- Impara a distinguere chi aggiungi alla tua rete di “amici” in base all’uso che ne fai.
- Se il social network a cui sei iscritto te lo consente, decidi quali tipi di informazioni possono essere consultate dai differenti tipi di amici.

POLITECNICO
MILANO 1863

SCHOOL OF MANAGEMENT

OSSERVATORI.NET
digital innovation

GRAZIE!

FAGGIOLI@MIP.POLIMI.IT