CENSIS

IISFA
ASSOCIAZIONE ITALIANA
DIGITAL FORENSICS

2° RAPPORTO CENSIS - IISFA

IL VALORE DELLA CYBERSECURITY IN ITALIA

LA SICUREZZA INFORMATICA GARANZIA DI BENESSERE E LIBERTÀ

SINTESI DEI PRINCIPALI RISULTATI

Roma, 19 luglio 2023

ASSOCOMUNICATORI
ASSOCIAZIONE NAZIONALE COMUNICATORI D'IMPRESA

ital communications
A STRATEGIC COMMUNICATION AGENCY

2° RAPPORTO CENSIS - IISFA

IL VALORE DELLA CYBERSECURITY IN ITALIA

LA SICUREZZA INFORMATICA GARANZIA DI BENESSERE E LIBERTÀ

SINTESI DEI PRINCIPALI RISULTATI

Roma, 19 luglio 2023

Indice

1. La sicurezza informatica garanzia di benessere e libertà 1
2. Prime reazioni al cyber risk 2
3. Cresce il cybercrime 2
4. Digital mismatch 5
5. Cronaca di minacce informatiche quotidiane 6
6. L'impatto emotivo del *cyber risk* 8
7. Resta fluttuante la conoscenza della *cybersecurity* 9
8. Pratiche di sicurezza più ricorrenti 9
9. Comparto aziende 13

1. LA SICUREZZA INFORMATICA GARANZIA DI BENESSERE E LIBERTÀ

Nel mondo attuale, attraversato dalla transizione digitale e dove l'essere connesso alla rete non è più solo una scelta, ma una necessità per poter contribuire ai processi di creazione del valore e per poter esercitare i propri diritti di cittadinanza, la dimensione della sicurezza informatica e della salvaguardia dei dati personali ha oramai assunto una sua acclarata e indiscutibile centralità.

Da tempo, infatti, l'Unione Europea ha indicato la cybersicurezza come una priorità della propria agenda digitale, declinando una strategia pluriennale al riguardo. L'Italia da parte sua, in attuazione delle riforme previste dal Piano Nazionale di Ripresa e Resilienza (PNRR), ha istituito dal 2021 l'Agenzia per la Cybersicurezza Nazionale. Come da più parti sottolineato la sua costituzione ha segnato l'avvio del processo di istituzionalizzazione della *Cybersecurity* a livello nazionale e lo scorso anno, nell'adempimento delle sue funzioni, l'Agenzia ha provveduto a presentare la *Strategia Nazionale di Cybersicurezza 2022-2026,* volta a pianificare, coordinare e attuare misure per rendere il Paese più sicuro e resiliente.

Accanto all'istituzionalizzazione di una *cybersecurity* nazionale è quantomai opportuna la promozione di una consapevolezza sociale sui rischi collegati all'insicurezza informatica. Questi ultimi, se non contrastati, espandono pericolosamente il perimetro della vulnerabilità sociale ed economica dell'intero "sistema Paese" ai diversi livelli e nei diversi ambiti istituzionali e produttivi, perché in un mondo sempre più interconnesso i danni causati a un nodo del sistema si ripercuotono inevitabilmente sui nodi limitrofi con effetti a catena.

È sulla spinta di questa avvertita urgenza che il Censis insieme a IISFA (Associazione Italiana Digital Forensics), ha inteso produrre il presente *Rapporto Censis - IISFA sul valore della Cybersecurity*, giunto alla sua seconda edizione, per continuare la narrazione di una dimensione che, seppure in misura diversa, è divenuta ormai strutturale nell'esistenza di ogni individuo, così da coglierne i mutamenti, anche alla luce dell'intensificarsi degli attacchi offensivi di pirateria informatica contro obiettivi privati e pubblici, e da alimentare così il dibattito pubblico per il consolidamento di una *cyber resilience* nazionale.

2. PRIME REAZIONI AL CYBER RISK

L'incremento degli attacchi informatici, insieme con il progressivo ampliamento dello spettro del *cyber risk,* sta producendo i loro effetti sulle condotte di vita degli italiani.

Sentiment e comportamenti ne sono influenzati: aumenta la preoccupazione rispetto all'attuale situazione di crisi, di cui l'alea digitale è elemento ricorrente; si teme per la violazione della propria privacy e l'integrità dei propri dati personali; in alcuni casi connessioni e transazioni online sono addirittura ridotte in via precauzionale.

Ma al *cyber risk* gli italiani stanno reagendo. Per quanto il concetto di cybersicurezza debba trovare ancora un suo consolidato posizionamento nell'opinione pubblica tra chi dichiara di conoscerne significato e conseguente declinazione fattuale nella società e chi dichiara di averne una cognizione vaga o, persino, di non averne alcuna, i dati sulle quotidiane misure di sicurezza delineano un certo orientamento rispetto all'adozione di posture difensive. All'interno del corpo sociale si stanno sviluppando, come risposta dal basso al rischio percepito, anticorpi di protezione, di cui talvolta gli individui non sembrano avere una piena consapevolezza e per questo ancora parzialmente sottotraccia. Più forte è, inoltre, la risposta tra quelli che hanno già avuto diretta esperienza di attacchi malevoli.

È quantomai opportuno, allora, mettere a valore questa reazione sociale e a partire da ciò promuovere una maggiore consapevolezza collettiva al riguardo, che includa anche quei gruppi che per condizione sociale, culturale o anagrafica, oltre a essere più a rischio di *digital divide*, rappresentano le componenti più deboli di tutto l'ecosistema digitale.

3. CRESCE IL CYBERCRIME

Nel 2022 gli attacchi informatici ad infrastrutture sono più che raddoppiati rispetto all'anno precedente, incrementandosi del 138%. Tra il 2012 e il 2021, nell'arco di quasi dieci anni, i reati informatici denunciati all'Autorità giudiziaria dalle Forze di Polizia sono raddoppiati (+155,2%) in controtendenza con l'andamento totale dei reati (-25,4%) (tab.1). Sono

Milano e Roma a guidare la classifica delle prime 10 Province per numero di reati informatici denunciati (rispettivamente 24.077 e 21.637). È, però, Torino a primeggiare per numero di reati in rapporto alla popolazione con 7,8 reati ogni mille abitanti (tab.2). Sempre nel 2022, le attività cibernetiche ostili condotte contro assetti informatici rilevanti per la sicurezza nazionale hanno interessato nel 56% dei casi infrastrutture informatiche di soggetti privati (+32% rispetto al 2021) e per il 43% obiettivi pubblici (-26% rispetto al 2021). Tra gli attori ostili prevalgono i gruppi criminali (47%, +33% rispetto al 2021), seguiti da attori statuali o sponsorizzati da Stati (26%, +3%) e, a distanza, dagli *hacktivisti* (8%, -15%). (fig.1)

Tab. 1 - Reati informatici denunciati all'Autorità giudiziaria dalle Forze di polizia ([1]), 2012-2021 *(v.a. e var. %)*

Anno	Reati informatici	Totale reati
2012	124.113	2.818.834
2013	150.035	2.892.155
2014	144.107	2.812.936
2015	154.867	2.687.249
2016	162.292	2.487.389
2017	174.743	2.429.795
2018	202.387	2.371.806
2019	228.254	2.301.912
2020	267.565	1.900.624
2021	316.716	2.104.114
Var.%		
2019-2021	38,8	-8,6
2020-2021	18,4	10,7
2012-2021	155,2	-25,4

(1) Sono considerati, oltre ai delitti denunciati all'Autorità giudiziaria da Polizia di Stato, Arma dei carabinieri e Guardia di finanza che alimentavano il modello cartaceo 165 in uso fino all'anno 2003, anche quelli denunciati dal Corpo forestale dello Stato, dalla Polizia penitenziaria, dalla Direzione Investigativa Antimafia e da altri uffici (Servizio Interpol, Guardia costiera, Polizia venatoria ed altre Polizie locali)

Fonte: elaborazione Censis su dati Ministero dell'Interno

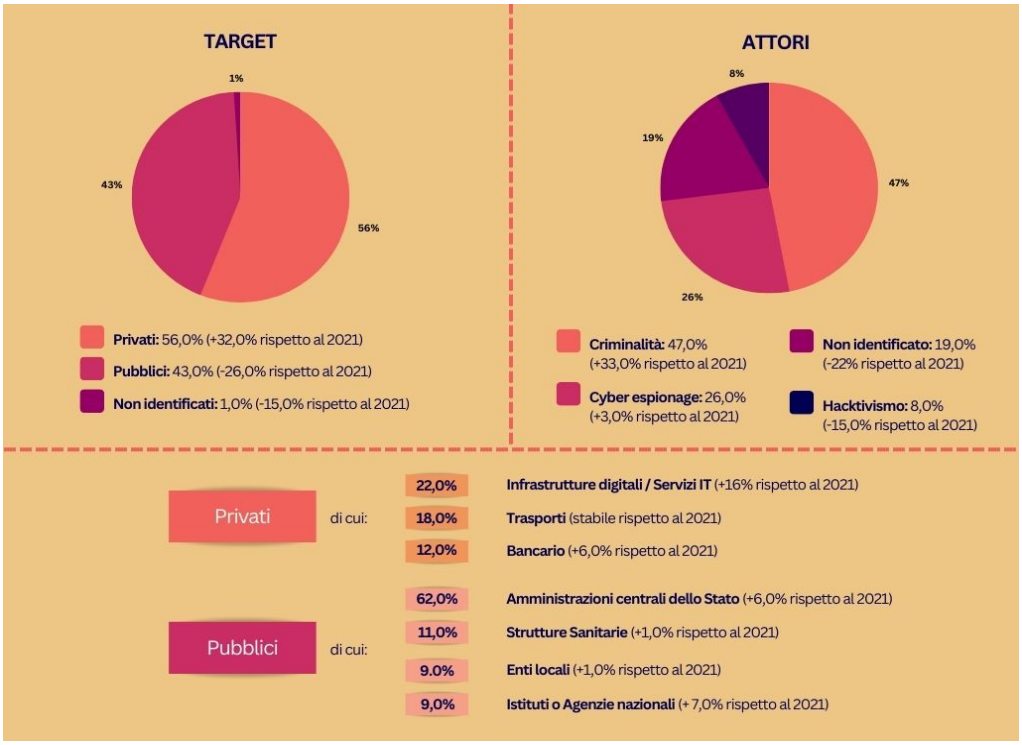
Tab. 2 - Prime 10 Province (*) per numero di reati informatici denunciati all'Autorità giudiziaria dalle Forze di polizia 2021 *(v.a., val. per 1.000 abitanti e val. %)*

Province	Totale reati informatici			Val. % popolazione sul totale Italia
	v.a.	per 1.000 abitanti	% sul totale	
Milano	24.077	7,5	7,6	5,4
Roma	21.637	5,1	6,8	7,1
Torino	17.165	7,8	5,4	3,7
Napoli	16.016	5,4	5,1	5,1
Brescia	8.323	6,6	2,6	2,1
Palermo	6.253	5,2	2,0	2,0
Firenze	6.063	6,1	1,9	1,7
Bari	5.891	4,8	1,9	2,1
Bologna	5.833	5,8	1,8	1,7
Venezia	5.519	6,6	1,7	1,4
Totale 10 province	116.777	6,1	36,9	32,4
Totale reati informatici	316.716	5,4	100,0	100,0

(*) Relativo a 92 province (la regione Sardegna è ripartita nelle quattro vecchie Province: Sassari, Cagliari, Oristano e Nuoro) e 14 Città Metropolitane

Fonte: elaborazione Censis su dati Ministero dell'Interno

Fig. 1 - Attività cibernetiche ostili contro assetti informatici rilevanti per la sicurezza nazionale, 2022



Fonte: elaborazione Censis su dati della Presidenza del Consiglio dei Ministri – Sistema di informazione per la sicurezza della Repubblica

4. DIGITAL MISMATCH

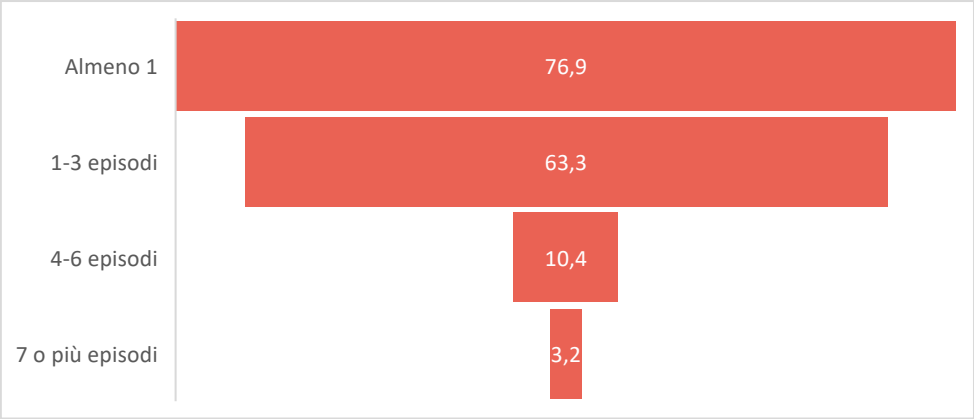
Se in media nel 2022 il 40% delle imprese ha dichiarato di avere difficoltà nella ricerca di lavoratori, nel caso dell'ICT (Information and Communications Technology) tale quota sale al 52%. Accanto al *software developer* o al *data engineer*, il *cybersecurity specialist* è indicato tra le figure emergenti più legate alla transizione digitale nelle previsioni di fabbisogni occupazionali e professionali a medio termine (2023-2027) per il settore dell'informatica e delle telecomunicazioni. Si amplia anche l'offerta universitaria: le lauree specifiche sul tema della *cybersecurity* a gennaio 2022 erano 13, un anno dopo sono 26, mentre sono 234 i corsi universitari in cui è presente l'insegnamento della *cybersecurity*. A giugno 2022, degli 837 corsi erogati

dall'Istruzione Tecnica Superiore, quelli dell'area tecnologica denominata Tecnologie dell'Informazione e della Comunicazione erano il 14% del totale e degli oltre 21.300 allievi, quelli aspiranti al titolo di tecnico superiore in campo ICT erano il 14,1%. Dei 13 ITS Academy censiti lo scorso anno e operanti nell'area ICT, 8 hanno almeno un corso sulla *cybersecurity* nella loro offerta formativa.

5. CRONACA DI MINACCE INFORMATICHE QUOTIDIANE

Nel corso dell'ultimo anno al 76,9% degli italiani è capitato di imbattersi almeno in una minaccia informatica, quota che raggiunge l'87,3% tra i 18-34enni. Il 63,3%, inoltre, è stato coinvolto in un numero di episodi compreso tra 1 e 3, mentre il 10,4% tra 4 e 6. *Smishing* e *phishing* sono di gran lunga le tecniche prevalentemente introdotte dai *cyber threat actor.* Il 60,9% del totale ha ricevuto un sms o un messaggio su WhatsApp con invito a cliccare su un link sospetto, con valori che arrivano al 70,7% tra i 18-34enni, mentre il 56% è stato bersaglio di e-mail ingannevoli che chiedevano informazioni sensibili, con mittente banche e/o aziende di cui sono clienti (67,2% dei 18-34enni). La richiesta di denaro o di prestiti da persone conosciute sul web è un inconveniente denunciato dal 15,9% degli intervistati e dal 19,7% dei 18-34enni. Una quota pressoché equivalente di individui (15,7%) ha poi avuto il proprio Pc/laptop infettato da un virus. Altre fattispecie meno ricorrenti, ma non per questo meno pericolose, riguardano i pagamenti online, la violazione della privacy e l'attacco alla sfera emotiva delle potenziali vittime. (tab.3).

Fig. 2 – Minacce informatiche capitate agli italiani nell'ultimo anno *(val.%)*



Fonte: indagine Censis, 2023

Tab. 3 - Italiani che hanno subito minacce e truffe informatiche *(val.%)*

Nell'ultimo anno le è capitato di:	%
Ricevere un SMS o un messaggio su WhatsApp con invito a cliccare su un link sospetto/malevolo	60,9
Essere bersaglio di e-mail ingannevoli per truffarla, per convincerla a dare informazioni sensibili che la riguardano (ad esempio, con mittente banche e/o aziende di cui lei è cliente)	56,0
Ricevere richieste di denaro, prestiti da persone conosciute sul web	15,9
Avere il suo pc/laptop infettato da un virus	15,7
Essere truffato facendo acquisti on line su siti web fraudolenti o all'interno di piattaforme con annunci legittimi (per.es. Facebook, eBay, Instagram)	8,9
Avere conversazioni e/o frequentazioni con persone conosciute sul web scoprendo poi che avevano una falsa identità	8,8
Scoprire sui social account fake con il suo nome/identità/foto	8,5
Subire una violazione della privacy (ad esempio a causa di un furto di un *device*, di una copia di dati personali non autorizzata, condivisione di video, foto, non autorizzate da parte di altri ecc.)	8,2
Scoprire pagamenti di acquisti online fatti a suo nome e con la sua carta	6,6
Vedersi clonata carta di credito e/o bancomat	6,6

Fonte: indagine Censis, 2023

6. L'IMPATTO EMOTIVO DEL *CYBER RISK*

Il *cyber risk* ha un impatto sociale pervasivo, che arriva a colpire lo spazio vitale di ogni singolo individuo. Il numero crescente di attacchi informatici a enti e istituzioni dei mesi passati ha condizionato la sfera emotiva e i comportamenti degli italiani. Per il 62,9% di loro sono stati fonte di ulteriore preoccupazione rispetto all'attuale situazione di crisi; un'apprensione aggiuntiva che è maggiore tra le donne (64,4%) rispetto agli uomini (61,4%) e tra i più giovani (67,9% dei 18-34nni). I maggiori attacchi informatici, nel 53,2% della popolazione, hanno ingenerato la paura che i propri dati possano essere rubati e usati per altri scopi, quando ci si collega a Internet per svolgere attività online. Infine, per circa un quarto della stessa popolazione (24,4%), tale paura si traduce, in conseguenza della riduzione dei collegamenti alla Rete in un'autolimitazione precauzionale della propria esistenza digitale (30,8% dei 18-34enni). (tab.4).

Tab. 4 - Reazioni degli italiani al numero crescente di attacchi informatici a enti e istituzioni, per classi di età *(val.%)*

Il numero crescente di attacchi informatici a enti ed istituzioni verificatosi durante i mesi passati, quali delle seguenti situazioni le ha provocato?	18-34 anni	35-64 anni	65 anni e oltre	Totale
Ulteriore preoccupazione rispetto all'attuale situazione di crisi	67,9	65,6	54,2	62,9
Quando mi collego a internet per svolgere attività on line (per. es. acquisti, prenotazioni, operazioni con la banca) ho più paura che i miei dati personali siano rubati e usati per altre cose	66,3	59,4	32,5	53,2
Mi collego meno a internet per svolgere attività on line (per es. acquisti, prenotazioni, operazioni con la banca)	30,8	24,9	19,0	24,4

Fonte: indagine Censis, 2023

7. Resta fluttuante la conoscenza della *cybersecurity*

Il 28,8% degli italiani dichiara di sapere precisamente cosa si intende per cybersicurezza, una quota cresciuta di 4,5 punti percentuali in confronto al 2022 (quando erano il 24,3%). Più esperti sull'argomento sono gli uomini (35,4%), i laureati (40,5%) e i lavoratori autonomi (45,5%). Diminuiscono coloro i quali affermano di averne una conoscenza a grandi linee: dal 58,6% passano a quota 50,4% (-8,2% punti percentuali rispetto al 2022). Non diminuiscono, anzi crescono in numero, i cittadini che dichiarano, infine, di non conoscere il significato del termine, che dal 17,1% del 2022 salgono al 20,8% del 2023. Più ignari sono gli individui meno scolarizzati (53,9% con al massimo la licenza media) e i più anziani (51,8% con 65 anni e oltre). (tab.5).

Tab.5 - Italiani che dichiarano di sapere cosa si intende per cybersecurity *(val.%)*

	2023	*2022*
Sì, precisamente	28,8	*24,3*
Sì, a grandi linee	50,4	*58,6*
No	20,8	*17,1*
Totale	100,0	*100*

Fonte: indagine Censis, 2023

8. Pratiche di sicurezza più ricorrenti

Oltre 7 italiani su dieci utilizzano una password per il wi-fi di casa (75,2%); il 71,5% fa uso di password diverse in funzione dei servizi utilizzati (posta elettronica, home banking, profili social, piattaforme di intrattenimento, ecc.); il 70,8% consente l'aggiornamento periodico del sistema operativo e dei software di produttività del Pc di casa e il 74,6% per il Pc di lavoro; il 70,3% ha un antivirus installato e aggiornato sul Pc di casa e il 75% sul Pc di lavoro. I sistemi di autenticazione più complessi della password (autenticazione biometrica oppure OTP via sms) sono, invece, utilizzati dal 54% (tab.6). Il backup dei propri file è, invece, una pratica che accomuna il 59,5% degli

italiani e che avviene: per il 50,9% dei casi su dispositivi esterni per il 38,9% su cloud e per il 23% in locale. Per la salvaguardia del proprio cellulare, invece, il 77,1% consente gli aggiornamenti periodici del software di sistema, con valori che arrivano all'82,8% tra i laureati e all'84,5% tra i 18-34enni, mentre il 62,6% utilizza per accedere al proprio cellulare oltre alla password altri fattori (PIN, OTP, impronta digitale o riconoscimento facciale) (tab.7). A fronte del 58,8%, che si dichiara preoccupato della sicurezza dei propri dispositivi informatici e che prende anche delle precauzioni e del 27,1% che, nonostante sia preoccupato e affermi di non fare niente di concreto, i dati nel complesso sembrano evidenziare una realtà che va oltre la percezione che gli italiani hanno delle loro condotte in materia di prevenzione e tutela dal rischio. Su cinque misure di sicurezza con un maggiore gradiente di intenzionalità (regolare esecuzione del backup dei file, password diverse in funzione dei servizi utilizzati, sistemi di autenticazione più complessi della password, password per il wi-fi di casa, installazione e aggiornamento di un antivirus su Pc di casa e cellulare), quasi sei italiani su dieci (il 57,3%) ne adottano tra quattro e cinque, il 32,4% ne adotta cinque (fig.3).

Tab. 6 - Misure di sicurezza informatica utilizzate dagli italiani *(val.%)*

Tra le misure di sicurezza di seguito indicate quali utilizza?	Totale	Dispositivi di lavoro
Utilizza una password per il suo wi-fi di casa	75,2	
Fa uso di password diverse per i vari servizi che utilizza (posta elettronica, home banking, profili social, piattaforme di intrattenimento ecc.)	71,5	
Consente l'aggiornamento periodico del sistema operativo e dei software di produttività (es. Office) del PC di casa	70,8	*74,6*
Ha un antivirus installato e aggiornato sul suo PC di casa	70,3	*75,0*
Effettua di solito un backup dei suoi file	59,5	
Fa uso di una password complessa, con almeno 12 caratteri sia alfanumerici sia speciali, sul suo PC di casa	56,8	*64,5*
Utilizza sistemi di autenticazione più complessi della password per es. autenticazione biometrica con le impronte digitali o codice OTP via sms, ecc.	54,0	
Utilizza un firewall sul PC di casa	46,2	*59,6*

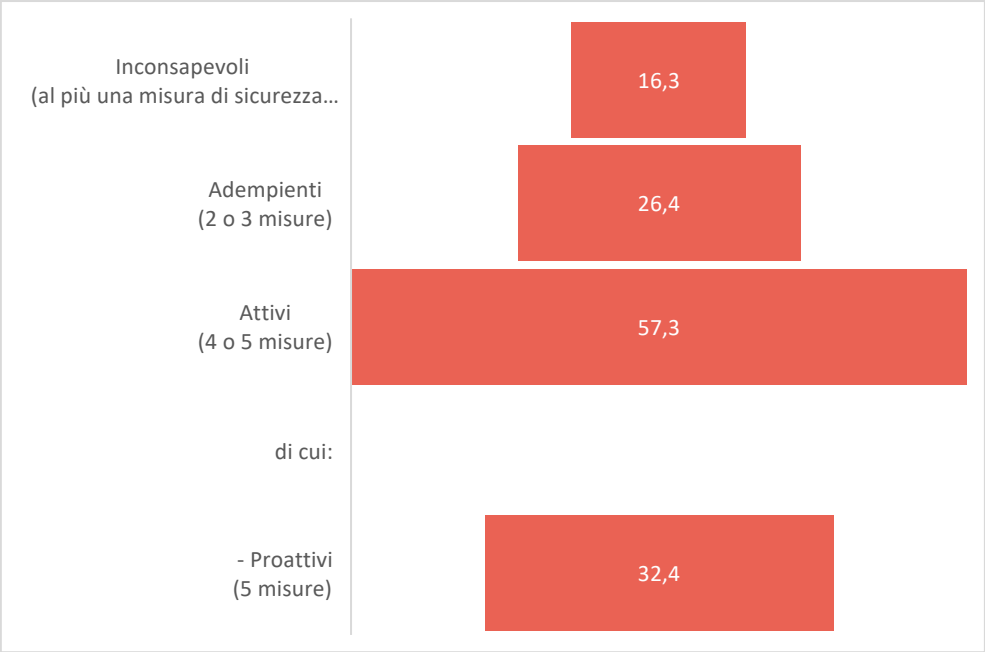
Fonte: indagine Censis, 2023

Tab. 7 - Misure di sicurezza applicate dagli italiani al proprio telefono cellulare, per classi di età *(val.%)*

	18-34 anni	35-64 anni	65 anni e oltre	Totale
Accede al cellulare con altri fattori utilizza oltre alla password (per es. PIN, codice OTP, impronta digitale o riconoscimento facciale)	79,7	72,2	32,6	62,6
Ha applicato un antivirus	51,7	55,6	28,5	47,2
Consente gli aggiornamenti periodici del software di sistema	84,5	90,1	48,2	77,1
Dispone di un sistema di cancellazione remota dei file in caso di furto o smarrimento	37,3	33,3	15,3	29,1
(solo se occupato) Dispone di cellulari distinti per uso privato e per lavoro	39,1	35,5	16,7	36,0
(solo per chi ha figli minorenni) Al cellulare dei suoi figli minorenni applica e le stesse misure di sicurezza del suo cellulare personale	29,7	44,3	0,0	36,8

Fonte: indagine Censis, 2023

Fig. 3 – Misure di sicurezza a maggiore intenzionalità adottate dagli italiani (*) *(val%)*



(*) Sono considerate le seguenti 5 misure:
- Fa uso di password diverse per i vari servizi che utilizza;
- Utilizza sistemi di autenticazione più complessi della password per es. autenticazione biometrica con le impronte digitali o codice OTP via sms, ecc.;
- Utilizza una Password per il suo WI-FI di casa;
- Ha un antivirus installato e aggiornato sul suo PC di casa e/o sul cellulare
- Effettua di solito un back up dei suoi file

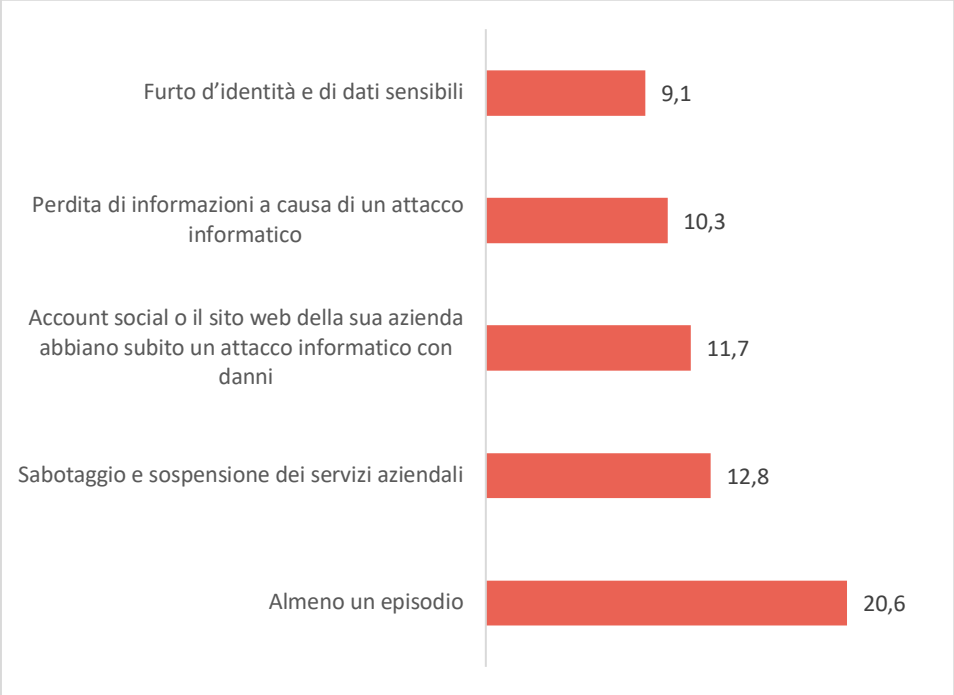
Fonte: indagine Censis, 2023

9. COMPARTO AZIENDE

Nel corso dell'ultimo anno il 20,6% degli occupati è stato testimone di almeno 1 problema informatico sul proprio luogo di lavoro e più nello specifico: il 12,8% ha sperimentato un sabotaggio e una sospensione dei servizi aziendali, l'11,7% un attacco informatico agli account social e al sito aziendale con danni conseguenti, il 10,3% una perdita di dati e informazioni a causa di un attacco informatico, infine il 9,1% un furto d'identità e di dati sensibili (fig.4). Nel 2022 le imprese italiane con 10 e più addetti che hanno

avuto un problema di sicurezza ICT sono state il 15,7%, (circa 30.000 unità in valore assoluto) (tab.8). Allo stesso tempo, il 55,4% degli stessi occupati è stato o sarà formato per contrastare o prevenire eventuali attacchi informatici di cui il 27,3% nell'ultimo anno e il 14,6% nei prossimi mesi e il 13,5% oltre un anno fa. A giugno 2022, le imprese antihacker hanno raggiunto la quota di 3.147, registrando un incremento del 5,4% rispetto al mese di settembre dell'anno precedente (tab.9).

Fig. 4 – Lavoratori la cui azienda ha subito nell'ultimo anno attacchi informatici *(val.%)*



Fonte: indagine Censis, 2023

Tab. 8 - Imprese che hanno avuto almeno un problema di sicurezza ICT (indisponibilità dei servizi ICT, distruzione o danneggiamento dei dati, divulgazione di dati riservati), per tipologia di danno e classe di addetto, 2022 *(val.%)*

	Classe di addetti				10 addetti e più
	10-49 addetti	50-99 addetti	100-249 addetti	250 addetti e più	
Divulgazione di dati riservati	0,8	1,7	2,6	4,3	1,0
Distruzione o danneggiamento dei dati	3,2	3,8	6,0	4,9	3,3
Indisponibilità dei servizi ICT	13,4	17,7	23,1	30,7	14,4
Divulgazione di dati riservati a causa di intrusioni, *pharming*, attacchi di phishing, azioni intenzionali dai propri addetti	0,5	1,2	1,9	2,9	0,6
Divulgazione di dati riservati a causa di azioni non intenzionali da parte dei propri addetti	0,4	1,2	1,0	2,3	0,5
Distruzione o danneggiamento dei dati a causa di infezione di software dannoso o intrusione non autorizzata	1,7	1,3	3,0	2,9	1,7
Distruzione o danneggiamento dei dati a causa di guasti hardware o software	2,1	2,9	3,7	3,2	2,3
Indisponibilità dei servizi ICT a causa di attacchi dall'esterno	2,9	2,6	5,7	7,8	3,1
Indisponibilità dei servizi ICT a causa di guasti hardware o software	12,1	16,3	20,5	27,1	13,0
Almeno un problema di sicurezza ICT	14,5	20,1	25,8	33,1	15,7
2019					*10,1*

Fonte: elaborazione Censis su dati Istat - Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese

Tab. 9 - Occupati che hanno avuto formazione specifica sulla cybersecurity nell'ultimo anno, per ripartizione geografica *(val.%)*

	Nord-Ovest	Nord-Est	Centro	Sud-Isole	Totale
Sì, nell'ultimo anno	29,4	30,2	27,4	22,6	27,3
Sì, più di un anno fa	10,8	9,3	22,6	13,6	13,5
No, ma è prevista nei prossimi mesi	15,3	18,2	9,6	14,3	14,6
No, mai	44,6	42,3	40,4	49,4	44,6
Totale	100,0	100,0	100,0	100,0	100,0

Fonte: indagine Censis, 2023