La cyber-criminalità contro il commercio in Italia

Report 2017

INTELLEGit
Turning science into intelligence

UNIVERSITÀ DEGLI STUDI DI TRENTO

CONFCOMMERCIO
IMPRESE PER L'ITALIA

La cyber-criminalità contro il commercio in Italia
Report 2017

Supervisione scientifica
Andrea Di Nicola
Giuseppe Espa

Autori
Andrea Di Nicola
Gabriele Baratto
Alessandro Giglioni
Andrea Nicolamarino

Hanno collaborato
Roberta Carraro, Ylenia Giordani, Elisa Martini, Erica Marturana, Silvia Semenzin, Giorgio Sinisi, Valentina Piol e Giuseppe Vitto

Progetto grafico e impaginazione
Damiano Salvetti

ISBN 978-88-94891-01-0

Intellegit
Salita dei Molini 2
38123, Trento
www.intellegit.it

Questo report è redatto da Intellegit, start up sulla sicurezza dell'Università degli Studi di Trento. Gli autori sono responsabili delle analisi e dei risultati esposti nel presente report.

Trento, novembre 2017

Indice


01

Introduzione

Questo report è redatto per Confcommercio da Intellegit, start up sulla sicurezza dell'Università degli Studi di Trento.

Le minacce legate alla cyber-criminalità sono in continua evoluzione e destinate a crescere in un mondo sempre più digitalizzato e connesso: secondo l'ultimo rapporto Clusit (I° semestre 2017), nell'anno passato oltre il 50% delle organizzazioni pubbliche e private del mondo è stata vittima di almeno un tentativo di attacco informatico. Il settore del commercio non fa eccezione: per fare solo un esempio, stando ad uno studio del *Center for Strategic and International Studies*, nel solo 2013 i commercianti del Regno Unito hanno subito perdite per oltre 850 milioni di dollari.

Nonostante ciò, fino ad oggi, il tema dei rischi e dei costi della cyber-criminalità per i commercianti italiani è stato poco analizzato, se non addirittura trascurato.

Questo lavoro parte proprio dal bisogno di colmare questa lacuna dando una risposta alle seguenti domande:

1. Quali sono le principali cyber-minacce per i commercianti?
2. Qual è la situazione della cyber-criminalità a danno dei commercianti oggi in Italia? Esistono differenze tra Nord, Centro e Sud?
3. Qual è il livello di sicurezza dei siti internet usati dai commercianti?
4. Quali sono i costi che la cyber-criminalità arreca ai commercianti in Italia?

Per rispondere a queste domande, Intellegit ha realizzato (*ad hoc* per Confcommercio) un sondaggio sulla cyber-criminalità somministrato ai commercianti in tre città campione (Milano, Roma e Bari); ha valutato attraverso una serie di controlli non intrusivi il livello di sicurezza dei siti internet dei commercianti aventi sede nelle tre città campione; ha creato e applicato una metodologia per stimare i costi della cyber-criminalità per il commercio.

I risultati di questo sforzo, presentati nelle quattro sezioni di cui si compone questo report, sono utili non solo per identificare e comprendere meglio i rischi connessi alla cyber-criminalità, ma anche per gestirli meglio, alla ricerca di soluzioni basate sulla conoscenza che consentano di proteggere i commercianti e i loro clienti. La visione, che coincide con la missione di Intellegit, è trasformare capacità analitica e scienza in azione strategica per la sicurezza del sistema Paese.

Andrea Di Nicola

Socio fondatore e membro del CdA di Intellegit
Coordinatore di eCrime — Facoltà di Giurisprudenza,
Università degli Studi di Trento

Executive summary

1. Cyber-minacce contro il commercio: in particolare malware, attacchi DoS, black hat hacking e phishing

Le cyber-minacce sono in continua evoluzione e destinate a crescere in un mondo sempre più connesso e digitalizzato e questa tendenza non risparmia nessun settore. Quelle più frequenti per i commercianti possono essere divise in due macro categorie: attacchi contro gli strumenti informatici dell'attività commerciale (in particolar modo *malware*, attacchi DoS e *black hat hacking*) e attacchi contro l'attività commerciale attraverso strumenti informatici (specialmente le frodi tramite email di *phishing*).

2. Commercianti a rischio, ma solo uno su due conosce le minacce

Dai risultati di un sondaggio (realizzato *ad hoc* da Intellegit per Confcommercio) ai commercianti in 3 città campione (Milano, Roma e Bari) è emerso che il 96,3% delle attività commerciali a rischio cyber-criminalità, facendo uso di un qualche tipo di strumento informatico. Quasi un commerciante su due, però, non conosce le minacce: i meno consapevoli a Bari (47% non consapevole), situazione leggermente migliore a Roma (43%) e Milano (41%).

3. Misure di protezione: non ci si protegge a sufficienza contro i ransomware e pochissimi si assicurano

La misura di protezione contro la cyber-criminalità più utilizzata dai commercianti è costituita dai software antivirus e firewall (91,6% a Milano, 89,4% a Roma, 92,6% Bari). La meno utilizzata le coperture assicurative per i danni dovuti a cyber-attacchi (8,4% a Milano, 10,6% a Roma, 7,4% a Bari). I commercianti sono particolarmente esposti ai rischi legati ai *ransomware* (meno della metà crea con regolarità copie di backup dei file utilizzati per l'attività) e alle truffe tramite email di *phishing* (a Milano, ad esempio, più di un commerciante su cinque dichiara di non fare attenzione ai messaggi di posta elettronica sospetti).

4. In media 7 commercianti su 100 sono stati vittime di un cyber-attacco: svetta Milano, con 12 ogni 100

In media il 6,9% dei commercianti (del campione nelle tre città considerate) è stato vittima di un cyber-attacco negli ultimi 12 mesi. La situazione, però, è diversa da città a città. A Milano sono stati ben il 12% gli esercizi commerciali ad aver subito un episodio di cyber-criminalità, la metà di questi più di una volta (a dimostrazione del fatto che alcuni commercianti sono più esposti alle cyber-minacce). Percentuali più basse a Roma e a Bari, dove a subire un cyber-attacco sono stati rispettivamente il 4% e il 3%. In generale, sulla base dei risultati del sondaggio di Intellegit e dell'indagine Confcommercio-GFK, è possibile stimare (in modo logico) che in Italia siano stati più di 250.000 gli esercizi commerciali vittime di cyber-criminalità negli ultimi 12 mesi (novembre 2016 - ottobre 2017).

5. Più di un episodio di cyber-criminalità su due non viene denunciato

In media solo il 44,4% degli episodi di cyber-criminalità è stato denunciato alle autorità competenti. Esistono però differenze tra città. A Bari i commercianti hanno riportato tutti i casi di cyber-criminalità subiti alle forze dell'ordine. A Milano, al contrario, viene denunciato un episodio su tre, mentre a Roma solo uno su quattro.

6. La metà dei siti internet dei commercianti è poco o per nulla sicura

Un'analisi di vulnerabilità condotta da Intellegit su un campione di siti web di esercizi commerciali aventi sede in tre città campione (Milano, Roma e Bari) ha evidenziato come un sito su due sia poco o per nulla sicuro (48% del totale del campione) e quindi molto esposto ad attacchi da parte dei cyber-criminali. La maggior frequenza di siti internet molto vulnerabili riguarda esercizi commerciali aventi sede a Bari (61%, contro il 43% di Milano e il 40% di Roma).

7. Sicurezza dei siti che usano CMS: uno su tre è molto vulnerabile

Una delle falle più sfruttate dai cyber-criminali per attaccare un sito internet riguarda le vulnerabilità dei CMS (*Content Management System*) quando questi non vengono utilizzati nella loro versione più aggiornata (e per questo più sicura). L'analisi ha evidenziato che un sito su tre dei commercianti che fanno uso di CMS (il 34,2%) è un bersaglio particolarmente vulnerabile ad eventi di cyber-criminalità dal momento che utilizza una versione arretrata e obsoleta.

8. Tre tipologie di costi arrecati dalla cyber-criminalità: di protezione, diretti e indiretti

I costi arrecati dalla cyber-criminalità al commercio in Italia sono di tre tipologie: di protezione (sostenuti dai commercianti per dotarsi di sistemi di sicurezza contro le cyber-minacce), diretti (perdite monetarie subite da un commerciante nel caso sia stato vittima di un cyber-attacco) e indiretti (quantificazione monetaria di una serie di danni immateriali cui un commerciante può incorrere come conseguenza di un episodio di cyber-criminalità).

9. Nell'ultimo anno i commercianti hanno speso quasi 900 milioni per proteggersi dalla cyber-criminalità: nonostante ciò le perdite dirette hanno superato gli 850 milioni e sono stati spesi più di 50 milioni per risolvere i problemi

Intellegit ha sviluppato una metodologia (che utilizza i risultati del sondaggio sulla cyber-criminalità somministrato ai commercianti in tre città campione e dell'indagine 2017 Confcommercio-GFK Italia sui fenomeni criminali, incrociandoli con dati MISE e ISTAT) per stimare in modo logico quali sono stati i costi arrecati dalla cyber-criminalità al commercio in Italia negli ultimi 12 mesi (novembre 2016 - ottobre 2017).
In totale, i costi di protezione stimati sostenuti dai commercianti nel periodo considerato dall'analisi ammontano a 885.600.000 euro. Nonostante ciò, le perdite dirette subite sono state di oltre 854.000.000 euro. Tra i possibili costi indiretti, infine, è stato possibile calcolare il valore monetario delle ore che i commercianti che hanno subito un cyber-attacco hanno perso per risolvere il problema, che supera i 54.460.000 euro.

10. Nell'ultimo anno la cyber-criminalità è costata ai commercianti quasi due miliardi di euro

In totale, negli ultimi 12 mesi (novembre 2016 - ottobre 2017) la cyber-criminalità ha arrecato ai commercianti italiani costi che sfiorano i due miliardi di euro (ovvero pari a circa 1.800.000.000 euro). Questa stima è sicuramente per difetto dal momento che non include le perdite indirette diverse dalle ore di lavoro impiegate per risolvere il problema.


02

Cyber-minacce contro il commercio

Internet e nuove tecnologie: nuove opportunità, nuovi pericoli

L'avvento di **internet** e delle **nuove tecnologie** ha comportato notevoli cambiamenti nel mondo in cui viviamo modificando in modo profondo la vita di tutti i giorni.

La società dell'informazione offre oggi grandi **opportunità** ad individui, imprese e operatori economici, compresi i commercianti. Si pensi alle potenzialità del commercio elettronico, alla possibilità di promuovere la propria attività in rete o ancora all'avvento di nuovi e veloci metodi di pagamento virtuali e telematici.

Allo stesso tempo, però, la esociety ha creato nuovi **pericoli**, legati a quella che viene definita cyber-criminalità: tutti quei reati che possono essere commessi a danno degli strumenti informatici dell'attività commerciale o comunque perpetrati a suo danno attraverso strumenti informatici.

Le **cyber-minacce** per i commercianti, a conferma di una tendenza globale che non risparmia nessun settore, sono in continua evoluzione e destinate a crescere in un mondo sempre più connesso e digitalizzato. Un solo esempio: secondo l'ultimo Rapporto Clusit (I° semestre 2017) tra il 2016 e la prima metà del 2017 i crimini informatici contro i bersagli appartenenti alla categoria "ricettività" (ovvero strutture alberghiere, residence, ecc.) sono aumentati del 16%.

I **potenziali danni** a cui possono andare incontro i commercianti in caso di episodi di cyber-criminalità sono tutt'altro che trascurabili. Oltre a perdite economiche dirette, si può incorrere in danni reputazionali e di immagine, fino ad arrivare a possibili profili di responsabilità giuridica (nel caso, ad esempio, di furto di informazioni sensibili dei clienti quando non si riesca a dimostrare di aver adottato tutte le cautele necessarie per prevenire l'evento).

Ma quali sono oggi le **principali cyber-minacce** per i commercianti?

Le principali cyber-minacce per i commercianti

Le cyber-minacce più frequenti per i commercianti possono essere divise in due macro categorie:

1. attacchi contro gli strumenti informatici dell'attività commerciale. Le principali minacce per i commercianti in questa categoria sono ***malware***, **attacchi DoS** e ***black hat hacking***.

2. attacchi contro l'attività commerciale attraverso strumenti informatici. Le principali minacce per i commercianti in questa categoria sono le email di ***phishing***.

Malware

I *malware* sono dei software malevoli che hanno il solo scopo di arrecare un danno ad un dispositivo (computer, smartphone, tablet, ecc.), ad una rete o ad un sistema informatico in generale. Il bersaglio dell'attacco viene di norma infettato da file e documenti allegati in email di *phishing* o scaricando software e applicazioni da fonti non sicure e sconosciute. Più raramente, i *malware* si diffondono tramite vulnerabilità di sistema o siti internet a loro volta infettati. Ne esistono moltissimi tipi (virus, *trojan*, *adware*, *worms*, ecc.), ognuno con specifiche finalità: le minacce maggiori per i commercianti sono oggi costituite dai *ransomware* e dagli *spyware*.

Ransomware

I *ransomware* (considerati da Europol come la principale cyber-minaccia del 2017) sono dei *malware* che, dopo aver infettato un dispositivo informatico (ad esempio un computer, un tablet o uno smartphone), rendono **inaccessibili** all'utente (perché criptati) **tutti i file** in esso salvati. Il cyber-criminale che ha infettato il dispositivo è solitamente l'unico in grado di decriptare e sbloccare i file: a tal fine, richiede all'utente il **pagamento di un riscatto** da effettuarsi tramite forme di pagamento online (spesso utilizzando delle criptovalute, come il bitcoin), bonifico bancario o servizi voucher.

I rischi concreti per i commercianti legati ai *ransomware* possono variare da settore a settore. A gennaio del 2017, ad esempio, un *ransomware* ha bloccato il dispositivo che gestiva l'aggiornamento delle chiavi elettroniche delle camere di un albergo in Austria. Per riuscire a sbloccare la situazione in tempi brevi e garantire la continuità del business, il direttore dell'albergo è stato costretto a cedere al ricatto pagando la somma richiesta dal cyber-criminale (1.500 euro). Il disagio è durato circa un giorno, generando perdite non solo economiche ma anche (e soprattutto) reputazionali.

In generale, i *ransomware* sono particolarmente pericolosi per tutti quei commercianti che non creano con regolarità copie di backup (in altri dispositivi, in memorie esterne o usando servizi cloud) dei file che utilizzano nell'ambito della propria attività: essere attaccati da uno di questi *malware*, infatti, significa non essere più in grado di accedere a quei documenti, spesso nemmeno a seguito del pagamento del riscatto.

Spyware

Gli *spyware* sono *malware* che, dopo aver infettato un dispositivo informatico, **raccolgono di nascosto** e **senza autorizzazione** informazioni relative all'utente o in possesso dello stesso. Ne esistono di varie tipologie: alcuni sono finalizzati a rubare password, credenziali di accesso o numero delle carte di credito, altri consentono al cyber-criminale di accedere ai documenti contenuti nel dispositivo o di leggere i messaggi di posta, altri ancora di poter registrare le conversazioni oppure attivare di nascosto le webcam.

Gli *spyware* possono essere molto pericolosi per le attività commerciali per svariati motivi. Ad esempio, un cyber-criminale potrebbe usare un *malware* di questo tipo per rubare informazioni sensibili e segrete

riguardanti i prodotti venduti, i servizi erogati, le procedure e le strategie commerciali seguite, ecc. e rivenderli ad un concorrente.

Nel caso l'attività di spionaggio del criminale riguardi i dati dei clienti (ad esempio gli indirizzi email o altri contatti personali detenuti per ragioni di marketing) e il commerciante non riesca a dimostrare di aver adottato tutte le cautele necessarie per evitare l'evento, potrebbero anche aprirsi pesanti profili di responsabilità giuridica.

Denial of Service (DoS)

I DoS - *Denial of Service* (in italiano, "negazione del servizio") sono attacchi informatici che hanno l'obiettivo di creare un **disservizio** (totale o parziale) rendendo irraggiungibile un sistema informatico e negando, quindi, agli utenti le possibilità di accedere al servizio collegato a quel sistema. Uno degli esempi più comuni di questo tipo di attacchi è l'invio di un elevato numero di richieste di accesso verso un sito internet in modo da sovraccaricarlo, bloccarlo e, di conseguenza, renderlo **inaccessibile**.

Oltre agli indubbi danni reputazionali e di immagine, le perdite per i commercianti a seguito di un attacco DoS possono essere molto significative nel caso di beni o servizi forniti avvalendosi di sistemi online (siti di ecommerce, servizi di online ticketing per compagnie di trasporto, servizi di online booking per alberghi e ristoranti, ecc.). Ai danni per il mancato guadagno durante l'attacco (spesso non trascurabili a causa del tempo necessario per mitigarne o eliminarne gli effetti) vanno aggiunti quelli nel medio-lungo periodo dovuti alla perdita dei quei clienti che non si fideranno più a fornire i propri dati personali ad un sito o ad un sistema che è già stato oggetto di un attacco informatico.

Black hat hacking

Con il termine *black hat hacking* si intende l'insieme delle attività poste in essere dai cyber-criminali per **violare la sicurezza** di un dispositivo o di un sistema informatico per guadagno personale o per arrecare un danno al bersaglio dell'attacco.

Accesso abusivo

Con il termine accesso abusivo ci si riferisce a tutte quelle attività in cui un **soggetto non autorizzato** si introduce, solitamente sfruttando delle falle nelle misure di protezione, in un dispositivo, un sistema o una rete. Le motivazioni possono essere diverse a seconda dell'attacco ma solitamente l'accesso è finalizzato al **danneggiamento** del dispositivo/sistema/rete o al **furto/modifica/distruzione** dei dati e delle informazioni in esso contenuti.

I rischi concreti per i commercianti legati ad un accesso abusivo da parte di un malintenzionato variano da caso a caso e dipendono dalle finalità dell'attacco. Ad esempio, una catena di alberghi ha subito nel marzo del 2017 un attacco informatico grazie al quale i criminali sono riusciti a rubare nomi, cognomi, numeri di carta di credito e di telefono di tutti i clienti registrati nel loro sistema. Si trattava del terzo attacco andato a buon fine

contro quella catena in meno di due anni. Le perdite, in questi casi, sono considerevoli. Sempre più commercianti, infatti, registrano e gestiscono un gran numero di informazioni (anche sensibili) relative ai loro clienti, quali contatti personali, codici bancari, ecc. Un accesso non autorizzato finalizzato al furto di queste informazioni andato a buon fine espone l'attività commerciali a diversi profili di responsabilità giuridica oltre che a notevoli perdite reputazionali e di immagine.

Defacing

Il *defacing* (chiamato anche *website defacement*) è l'attività attraverso cui un cyber-criminale **modifica** senza alcuna autorizzazione una o più pagine di un **sito internet** oppure lo sostituisce completamente con un altro.

A seguito di questo tipo di attacchi un commerciante può subire danni di immagine anche molto seri. Un ristorante di Udine, ad esempio, è stato recentemente vittima di un attacco da parte di alcuni fondamentalisti islamici che hanno inserito nella homepage del sito internet scritte jihadiste e immagini raccapriccianti, causando al ristoratore un indubbio danno reputazionale oltre alle perdite, sia monetarie che di tempo, per ripristinare il sito.

Phishing

Il *phishing* è un tentativo di **truffa online** con la quale un cyber-criminale invia messaggi di posta elettronica fingendosi qualcun altro (talvolta molto accurati e convincenti) con il fine ultimo di ingannare il destinatario e **rubare dati e/o informazioni** sensibili oppure infettare il dispositivo.

Nel primo caso, i messaggi di posta elettronica inviati dal criminale imitano il contenuto e l'aspetto delle email di organizzazioni legittime e conosciute (quali ad esempio banche, servizi postali o siti di ecommerce) e hanno all'apparenza l'obiettivo di informare di presunti problemi riscontrati con l'account personale dell'utente. Al fine di risolvere il problema, viene chiesto all'utente di cliccare su di un link e di inserire nella pagina internet collegata (anche questa creata ad arte dal criminale) alcuni dati (ad esempio credenziali di accesso, dettagli della carta di credito): in questo modo, le informazioni inserite dall'utente vengono rubate dal criminale.

Nel caso di messaggi *phishing* finalizzati ad **infettare il dispositivo**, il cyber-criminale solitamente si finge un fornitore, un collega, un cliente o una ditta di autotrasporti. Nel messaggio si chiede all'utente di scaricare un allegato (ad esempio una bolletta, una fattura, o una nota di accredito) o di cliccare in un link presente nella mail (ad esempio per controllare il tracking di un pacco). Il dispositivo viene infettato appena l'utente cerca di aprire il file scaricato nel suo dispositivo.

Alla luce del modus operandi dei cyber-criminali e a causa delle sempre maggior digitalizzazione delle interazioni con fornitori, colleghi e clienti, i commercianti risultano essere un obiettivo particolarmente sensibile per gli attacchi di *phishing*. Ad esempio, il recente attacco *ransomware* "WannaCry" che ha bloccato i dispositivi informatici, tra gli altri, di centinaia commercianti in vari settori in tutto il mondo veniva diffuso principalmente attraverso mail di *phishing*.

03

Cyber-criminalità contro il commercio: tre città a confronto

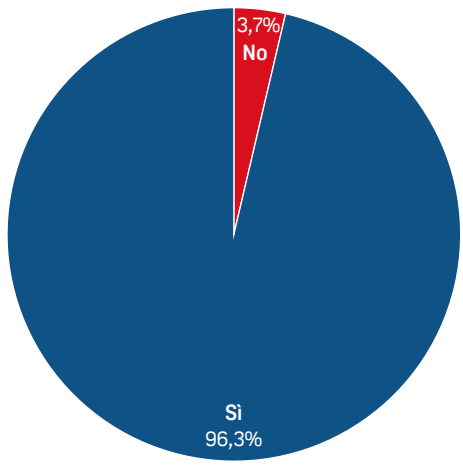
In questa sezione si illustrano i risultati di un sondaggio sulla cyber-criminalità somministrato ai commercianti in tre città campione (Milano, Roma e Bari)[1], condotto con l'obiettivo di ottenere una prima fotografia del fenomeno in Italia, capendo se e quali differenze esistano tra città del Nord, del Centro e del Sud.

Utilizzo di strumenti informatici da parte dei commercianti

Il 96,3% è a rischio cyber-criminalità

Oggi la quasi totalità dei commercianti (**96,3%** in media) fa uso di strumenti informatici per realizzare, facilitare o promuovere la propria attività. In testa Roma (**99%**), seguita da Milano (**96%**) e Bari (**94%**). Quasi tutti i commercianti, di conseguenza, sono potenzialmente esposti alle cyber-minacce. Il dato medio delle tre città è leggermente superiore a quello **nazionale** rilevato nell'indagine 2017 Confcommercio-GFK Italia sui fenomeni criminali (**84%**): questo è probabilmente dovuto al fatto che la percentuale di commercianti che fa uso di strumenti informatici è più alta nelle città rispetto che in altre zone del territorio.

Figura 1. Utilizzo di strumenti informatici da parte dei commercianti in tre città campione (Milano, Roma e Bari). Valori percentuali (n=300)



Fonte: sondaggio Intellegit per Confcommercio, 2017

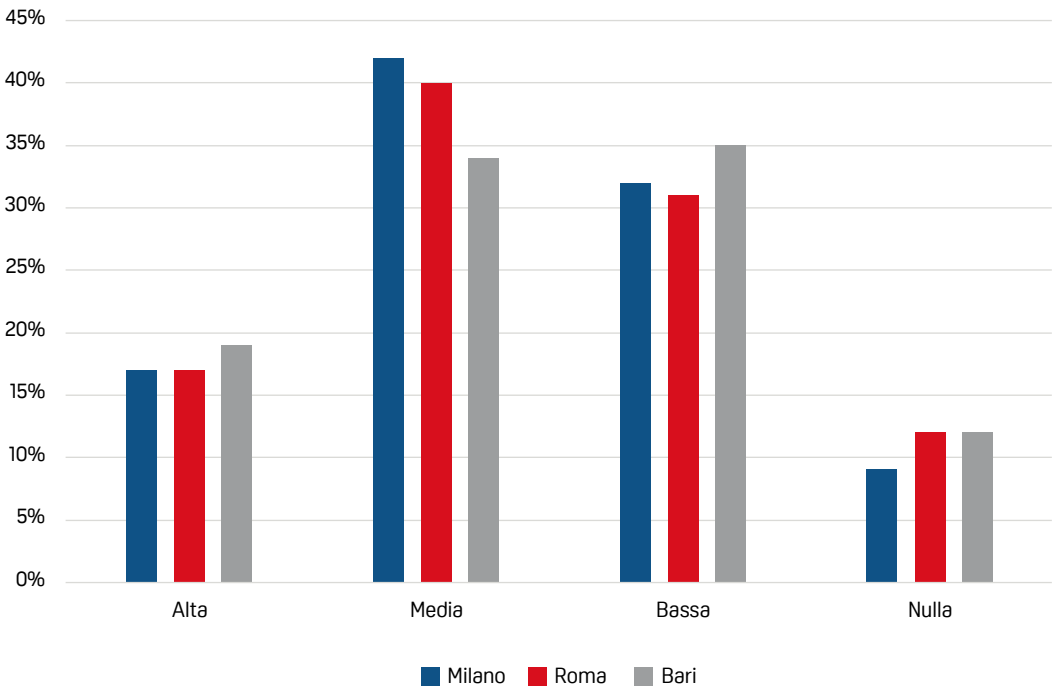
[1] Il sondaggio (realizzato *ad hoc* da Intellegit per Confcommercio) è stato somministrato a 100 attività commerciali, cercando di coprire il maggior numero di categorie possibili, in ciascuna delle tre città campione (Milano, Roma e Bari), in due modalità alternative: *web survey* o intervista *face-to-face*.

Cyber-minacce e livello di consapevolezza dei commercianti

Quasi un commerciante su due non conosce i rischi

Quasi la metà dei commercianti nelle tre città campione ha dichiarato di avere una consapevolezza **bassa** o **nulla** riguardo ai rischi legati alla cyber-criminalità. Poco rilevante la differenza tra le città esaminate: i meno consapevoli a **Bari (47%)**, situazione leggermente migliore a **Roma (43%)** e **Milano (41%)**. I rischi legati alla cyber-criminalità sono tanto maggiori quanto non conosciuti e, per questo, sottovalutati.

Figura 2. Consapevolezza dei commercianti riguardo ai rischi legati alla cyber-criminalità. Confronto tra tre città campione (Milano, Roma e Bari). Valori percentuali (n=300)



Fonte: sondaggio Intellegit per Confcommercio, 2017

Sistemi di protezione contro la cyber-criminalità

Non ci si protegge a sufficienza contro i ransomware. Quasi nessuno si assicura

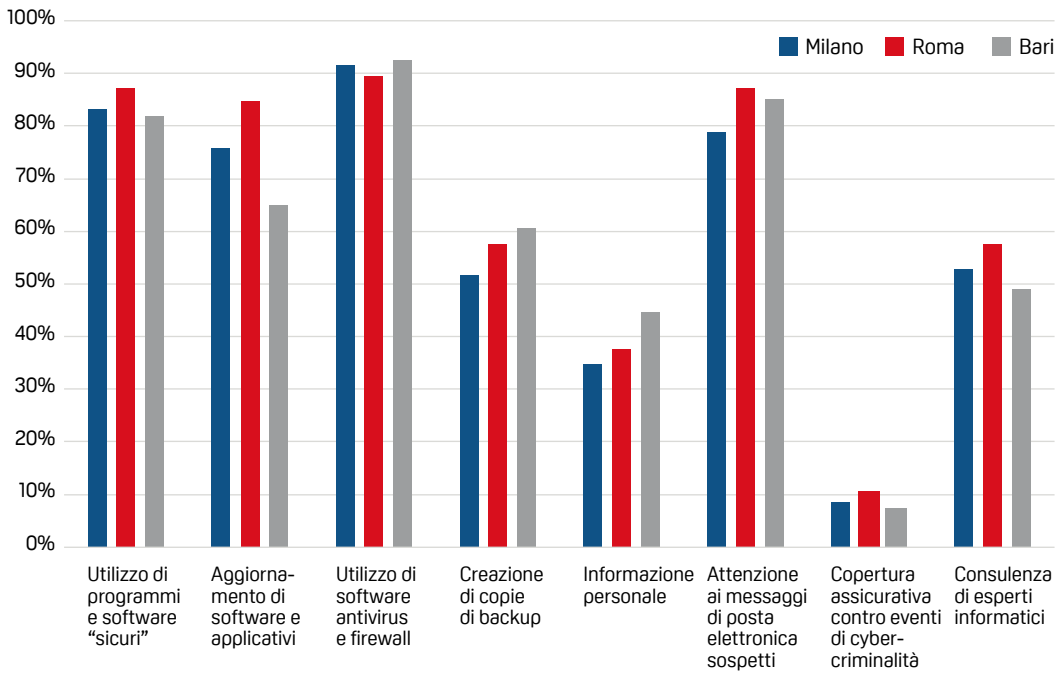
Non esistono grandi differenze tra le città campione per quanto riguarda le misure di sicurezza adottate dai commercianti per mettersi al riparo dai rischi legati alla cyber-criminalità.

La misura **più utilizzata** è costituita dai **software antivirus** e **firewall** (91,6% a Milano, 89,4% a Roma, 92,6% Bari). La **meno utilizzata** le **coperture assicurative** per i danni dovuti a cyber-attacchi (8,4% a Milano, 10,6% a Roma, 7,4% a Bari).

Secondo il sondaggio i commercianti sono particolarmente **esposti** ai rischi legati ai ***ransomware***, una delle principali cyber-minacce del 2017: sono, infatti, ancora molti quelli che non creano copie di **backup** dei file utilizzati nell'attività commerciale (48,4% a Milano, 42,4% a Roma, 39,4% a Bari).

Gli esercizi commerciali sono particolarmente esposti, inoltre, al rischio ***phishing***. A Milano più di un commerciante su cinque dichiara di non fare attenzione ai messaggi di posta elettronica sospetti (21,1%). Situazione leggermente migliore a Roma (12,9%) e Bari (14,9%).

Figura 3. Strumenti di protezione contro la cyber-criminalità utilizzati dai commercianti. Confronto tra tre città campione (Milano, Roma e Bari). Valori percentuali (n=300)



Fonte: sondaggio Intellegit per Confcommercio, 2017

Episodi di cyber-criminalità contro i commercianti

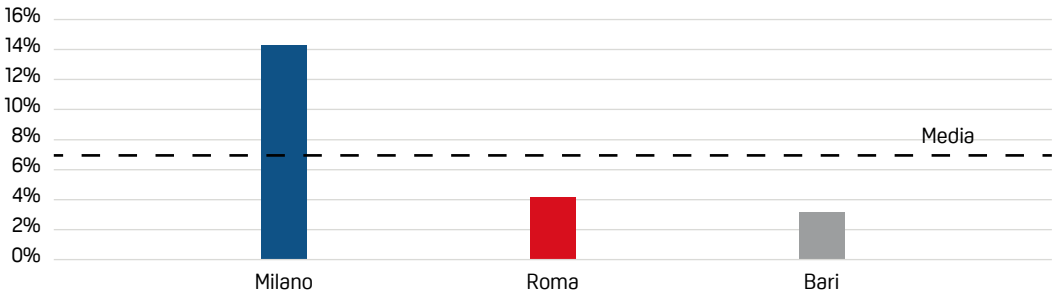
In media 7 commercianti su 100 sono stati vittime di un cyber-attacco: svetta Milano, con 12 ogni 100

Negli ultimi 12 mesi (ovvero a partire da novembre 2016), a **Milano** il **12%** degli esercizi commerciali ha subito almeno un episodio di cyber-criminalità. Di questi, **la metà** ha subito **più di un attacco** (multivittimizzazione). Ciò dimostra che alcuni commercianti sono più esposti alle cyber-minacce. Gli episodi hanno riguardato il furto di informazioni e di denaro online, l'accesso abusivo ai sistemi informatici, le truffe tramite email phishing, l'infezione da parte di *malware* e il vandalismo a danno del sito internet (*defacing*). A **Roma** sono il **4%**, invece, i commercianti che hanno subito cyber-attacchi (infezioni da *malware* e truffe tramite email di *phishing*). Anche in questo caso, **3 commercianti su 4** tra quelli che sono stati vittime di episodi di cyber-criminalità hanno subito **più di un attacco**. Situazione diversa **Bari**, città in cui i commercianti che sono stati vittime di cyber-criminalità (il **3%**) hanno subito soltanto un episodio.

Il dato di Milano (12%) supera in modo significativo il dato medio relativo alle tre città oggetto di sondaggio (**6,9%**). Ma perché? Tra i possibili motivi, il fatto che Milano sia la città in cui si è registrata la **maggior consapevolezza** riguardo ai rischi legati alla cyber-criminalità: i commercianti, dunque, potrebbero rendersi maggiormente conto degli attacchi rispetto alle altre città analizzate. Allo stesso tempo, però, i commercianti di Milano si sono dimostrati **poco attenti** verso i messaggi di posta elettronica sospetti, principale tramite delle truffe e delle infezioni tramite email di *phishing*.

Il dato medio delle tre città (6,9%) risulta essere più basso di quello **nazionale** rilevato nell'indagine 2017 Confcommercio-GFK Italia sui fenomeni criminali (**19%**): probabilmente la somministrazione del sondaggio face-to face nelle tre città ha consentito di chiarire meglio agli intervistati che non dovevano essere presi in considerazione i cyber attacchi subiti a danno degli strumenti informatici diversi da quelli utilizzati nell'attività commerciale. In generale, sulla base dei risultati del sondaggio e dell'indagine Confcommercio-GFK, è possibile stimare (in modo logico) che in Italia siano stati **più di 250.000** gli **esercizi commerciali vittime** di **cyber-criminalità** negli ultimi 12 mesi (novembre 2016 - ottobre 2017).

Figura 4. Commercianti vittime di episodi di cyber-criminalità. Periodo novembre 2016 - ottobre 2017. Confronto tra tre città campione (Milano, Roma e Bari). Valori percentuali (n=274)[2]



Fonte: sondaggio Intellegit per Confcommercio, 2017

[2] Dei 300 commercianti intervistati: 11 non hanno risposto in quanto non utilizzano nessuno strumento informatico nella loro attività mentre 15, pur utilizzando strumenti informatici, non hanno saputo o voluto fornire una risposta.

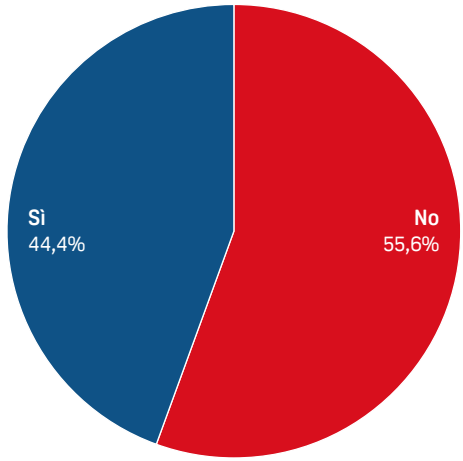
Denunce degli episodi di cyber-criminalità

Più della metà dei casi non vengono riportati alle forze dell'ordine

In media solo il **44,4%** degli episodi di cyber-criminalità è stato **denunciato** alle autorità competenti. Esistono però differenze tra città. A **Bari** i commercianti hanno riportato alle forze dell'ordine tutti i casi di cyber-criminalità subiti. A **Milano**, al contrario, viene denunciato un episodio su tre, mentre a **Roma** solo uno su quattro.

Questo risultato conferma che per una corretta misurazione del fenomeno sono necessarie indagini campionarie di vittimizzazione, essendo molti gli episodi non registrati nelle statistiche ufficiali (il cosiddetto "numero oscuro").

Figura 5. Denuncia alle forze dell'ordine dell'ultimo episodio di cyber-criminalità subito in tre città campione (Milano, Roma e Bari). Periodo novembre 2016 - ottobre 2017. Valori percentuali (n=18)[3]



Fonte: sondaggio Intellegit per Confcommercio, 2017

[3] Dei 19 commercianti che hanno dichiarato di aver subito almeno un episodio di cyber-criminalità negli ultimi 12 mesi (novembre 2016 - ottobre 2017), 1 non ha saputo o voluto fornire una risposta.

04

La sicurezza dei siti internet dei commercianti

Vetrine virtuali, problemi reali

Nella società dell'informazione i **siti internet** costituiscono, in particolar modo per le attività commerciali, delle vere e proprie vetrine virtuali. Essi infatti, in alcuni casi, sono un'estensione del locale fisico dell'attività (in particolare nei casi in cui internet rappresenta uno strumento per ottenere ulteriore visibilità), in altri lo sostituiscono completamente o quasi, perché l'esercizio commerciale fa affidamento in modo esclusivo o almeno preponderante sull'ecommerce.

Come si è visto, i siti web delle attività commerciali possono diventare il **bersaglio** di cyber-criminalità. Nel caso di attacchi DoS, ad esempio, è possibile che i servizi erogati dal sito bersagliato vengano interrotti. Qualora invece si verifichi un *defacing*, ad essere alterato e stravolto è l'aspetto e il modo in cui il sito si presenta agli utenti. In entrambe le situazioni si va incontro ad un danno economico e reputazionale considerevole.

Ma quanto sono vulnerabili a questi eventi di cyber-criminalità i siti online di cui si avvalgono i commercianti? Qual è il loro **grado di sicurezza**?

In questa sezione del report si presentano i risultati di un'analisi volta a verificare il grado di vulnerabilità dei siti internet di 100 attività commerciali, per ognuna delle città prese in considerazione (ossia Milano, Roma e Bari)[4].

La sicurezza dei siti internet dei commercianti

La metà dei siti web è poco o per nulla sicura

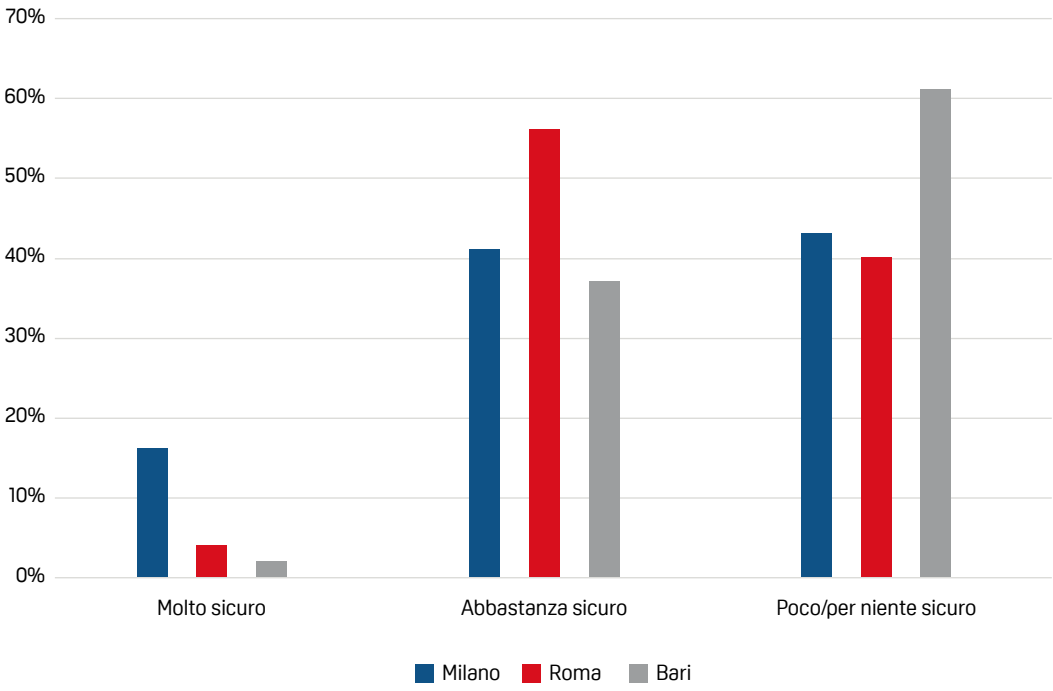
Per la valutazione Intellegit ha effettuato (utilizzando un software dedicato) una serie di controlli non intrusivi finalizzati alla verifica del grado di sicurezza dei 300 siti campione. A seguito delle analisi, i siti sono stati divisi in tre categorie, a seconda del numero e della tipologia di vulnerabilità presenti: molto sicuro, abbastanza sicuro e poco/per nulla sicuro (Figura 6).

Solo il **4,3%** dei siti è risultato essere **molto sicuro**, ovvero totalmente privo di vulnerabilità rilevanti. Esistono, però, profonde differenze tra città e città. Molto sicuro è il **16%** dei siti internet degli esercizi commerciali aventi sede a **Milano**, contro il **4%** di quelli a **Roma** e solo il **2%** di quelli a **Bari**.

Quasi un sito su due è risultato essere **poco** o per **nulla sicuro** (**48%** del totale del campione) e quindi molto esposto a possibili

[4] Il campione è formato da 100 siti di esercizi commerciali aventi sede in ciascuna delle tre città campione (Milano, Roma e Bari), scelti casualmente ma cercando di coprire il maggior numero di categorie commerciali.

Figura 6. Livello di sicurezza dei siti internet degli esercizi commerciali. Confronto tra tre città campione (Milano, Roma e Bari). Valori percentuali (n = 300)



Fonte: analisi Intellegit per Confcommercio, 2017

attacchi da parte dei cyber-criminali. La maggior frequenza di siti internet molto vulnerabili riguarda quelli di esercizi commerciali aventi sede a **Bari** (**61%**, contro il **43%** di Milano e il **40%** di Roma).

I rischi cui vanno incontro i commercianti con siti poco o per nulla sicuri variano a seconda della tipologia del sito. Un albergo con un sito internet poco sicuro, ad esempio, può essere più soggetto al dirottamento da parte di soggetti terzi dei pagamenti online e dei dati personali trasmessi dai clienti. Un bar o un ristorante invece possono essere colpiti da episodi di *defacing* (che andrebbe a danneggiare la visibilità che il sito internet conferisce a queste attività commerciali).

La parte restante del campione osservato (il **46%**) è costituita da siti internet **abbastanza sicuri**, ossia dotati di sistemi di sicurezza nella media anche se non completamente coperti contro alcuni episodi di cyber-criminalità particolarmente nocivi.

Sicurezza dei siti che utilizzano Content Management System

Pochi siti internet aggiornano regolarmente i CMS

I CMS (*Content Management System*, letteralmente "Sistema di Gestione dei Contenuti") sono dei programmi che consentono di gestire un sito internet in modo semplice e veloce, a livello sia di creazione di nuove

pagine sia di inserzione di contenuti di vario tipo, quali testi, immagini, video, musica, banner, link. Grazie alla loro versatilità e facilità di utilizzo, questi sistemi sono molto utilizzati nella creazione di siti internet per le attività commerciali.

Una delle falle che i cyber-criminali sfruttano maggiormente per attaccare un sito sono proprio le **vulnerabilità dei CMS**. Questo tipo di programmi sono, solitamente, molto dinamici e le società produttrici cercano costantemente di migliorarli, in modo da risolverne le criticità e renderli resistenti ad attacchi informatici. Per questo motivo è opportuno dotarsi della **versione più aggiornata** del CMS che si utilizza ogni qualvolta questa sia disponibile: per ridurre ulteriormente il rischio di cyber-criminalità.

A seguito di un'analisi non invasiva svolta su 300 siti internet di attività commerciali è emerso che uno su quattro (il **23,3%**) utilizza CMS. Tra questi, praticamente nessuno è aggiornato all'ultima versione rilasciata dalle rispettive società produttrici. In particolare è da evidenziare il fatto che il **34,2%** di questi siti utilizza una versione arretrata ed obsoleta del proprio CMS.

Un sito su tre di quelli che usano un CMS, dunque, è un bersaglio **particolarmente vulnerabile** ad eventi di cyber-criminalità.


05

I costi della cyber-criminalità per i commercianti

Calcolare i costi della cyber-criminalità

Intellegit, sulla base della letteratura scientifica e delle analisi criminologiche condotte in altri contesti nazionali ed internazionali, ha costruito per Confcommercio una **metodologia** per **stimare** (in modo logico) i **costi** arrecati dalla cyber-criminalità al commercio in Italia. Nel dettaglio, sono prese in considerazione tre tipologie di costi: quelli di **protezione**, quelli **diretti** e quelli **indiretti**.

Costi di protezione

Con il termine "costi di protezione" ci si riferisce a tutte quelle spese che i commercianti sostengono per dotarsi di **sistemi di sicurezza** contro le cyber-minacce, siano esse finalizzate a bloccare un tentativo di attacco oppure a mitigare/eliminare le conseguenze dannose di un attacco andato a buon fine. Sono considerati costi di protezione, ad esempio, quelli sostenuti per:

- installare adeguati software antivirus e firewall a protezione dei computer, degli smartphone e degli altri strumenti informatici utilizzati nell'ambito dell'attività commerciale;
- creare ed aggiornare copie di sicurezza (backup) dei documenti e degli altri file inerenti l'attività commerciale;
- informarsi o richiedere la consulenza di esperti sulle più adeguate ed efficaci misure di sicurezza da adottare per tutelare l'attività commerciale dai rischi legati alla cyber-criminalità;
- avvalersi di polizze assicurative a copertura dai danni arrecati da eventuali episodi di cyber-criminalità.

Costi diretti

Con il termine "costi diretti" ci si riferisce alle **perdite monetarie** subite da un commerciante nel caso in cui abbia subito un cyber-attacco. Sono costi diretti, a titolo d'esempio:

- il valore di un computer reso inutilizzabile in seguito ad un attacco *ransomware*;
- il denaro perso a seguito di una frode online (*phishing*);
- le perdite monetarie dovute ad un sistema irrimediabilmente danneggiato a causa di un cyber-attacco.

Costi indiretti

Per "costi indiretti" ci si riferisce alla quantificazione monetaria di una serie di **danni immateriali** in cui un commerciante può incorrere come conseguenza di un episodio di cyber-criminalità. Così sono costi indiretti:

- il tempo necessario (calcolato in ore di lavoro) per risolvere il problema derivante da un cyber-attacco, ovvero per ripristinare lo *status quo*;
- il danno reputazionale (ad esempio a seguito di un attacco al proprio sito internet o ad un attacco DoS);
- le perdite dovute all'impossibilità di esercitare la propria attività commerciale come conseguenza di un cyber-attacco.

Stima dei costi della cyber-criminalità contro i commercianti in Italia

Intellegit, sulla base dei risultati del sondaggio sulla cyber-criminalità somministrato ai commercianti in tre città campione (Milano, Roma e Bari) e dell'indagine 2017 Confcommercio-GFK Italia sui fenomeni criminali, dei dati MISE e ISTAT e di una metodologia elaborata *ad hoc* per Confcommercio, ha **stimato** (in modo logico) per la prima volta quali sono i **costi** arrecati dalla **cyber-criminalità** al **commercio** in Italia nei 12 mesi precedenti la pubblicazione di questo report (novembre 2016 - ottobre 2017).

Quasi 900 milioni spesi per proteggersi

In base ai risultati del sondaggio sulla cyber-criminalità somministrato ai commercianti in tre città campione, negli ultimi 12 mesi i commercianti hanno speso in media **590 euro ciascuno** per dotarsi di sistemi di protezione contro le cyber-minacce.

Questi costi variano molto a seconda del settore considerato: si passa da casi in cui le spese sono state nulle oppure molto basse (20-50 euro), ad altri in cui il singolo commerciante ha dichiarato di aver sostenuto spese superiori ai 1.500 euro (specialmente nel caso di strutture ricettive).
La spesa media varia molto anche da città a città: 715 euro a Milano, 665 euro a Roma, 340 euro a Bari.

In **totale**, i costi di protezione stimati sostenuti dai commercianti in Italia negli ultimi 12 mesi ammontano a **885.600.000 euro**.

Più di 850 milioni di perdite dirette

In base ai risultati dell'indagine 2017 Confcommercio-GFK Italia sui fenomeni criminali, i commercianti hanno subito a seguito di un cyber-attacco una perdita media diretta di circa **3.000 euro**. È possibile quindi stimare che in totale la cyber-criminalità negli ultimi 12 mesi abbia generato perdite dirette per i commercianti per oltre **854.000.000 euro**.

Il dato è in linea con i risultati di ricerche simili condotte al di fuori dell'Italia: ad esempio, secondo uno studio del Center for Strategic and International Studies, i commercianti del **Regno Unito** hanno subito nel solo 2013 perdite dirette che superano gli **850 milioni di dollari**.

Spesi più di 50 milioni per risolvere i problemi

Tra i possibili costi indiretti è stato possibile calcolare il **valore monetario** delle **ore** che i commercianti che hanno subito un cyber-attacco hanno perso per **risolvere il problema**. In media, i commercianti vittimizzati hanno impiegato circa **14 ore e mezza** per ripristinare la situazione precedente all'attacco (con poche differenze nelle tre città in cui è stato somministrato il sondaggio), per una perdita complessiva che supera i **54.460.000 euro**.

Non è stato possibile, invece, stimare gli altri costi indiretti, quali i costi reputazionali e le perdite derivanti dall'impossibilità di esercitare la propria attività commerciale come conseguenza di un cyber-attacco.

Nell'ultimo anno la cyber-criminalità è costata ai commercianti quasi due miliardi di euro

Negli ultimi **12 mesi** (novembre 2016 - ottobre 2017) la cyber-criminalità ha arrecato ai commercianti italiani costi che sfiorano i due miliardi di euro, ovvero pari a circa **1.800.000.000 euro**.

Questa stima è sicuramente per difetto dal momento che non include le perdite indirette diverse dalle ore lavorative impiegate per risolvere i problemi derivanti dal cyber-attacco.

Trento, novembre 2017

INTELLEGit

Turning science into intelligence

UNIVERSITÀ DEGLI STUDI
DI TRENTO

CONFCOMMERCIO

IMPRESE PER L'ITALIA