proofpoint

Europa e Medio Oriente

REPORT

State of the Phish 2024

Azioni pericolose, minacce reali e resilienza degli utenti nell'epoca della sicurezza informatica incentrata sulle persone

proofpoint.com/it

INTRODUZIONE

Spesso, le notizie da prima pagina si concentrano sulle ingegnose strategie di social engineering e sulle vulnerabilità zero-day utilizzate dai criminali informatici. Ma questi ultimi non devono sempre fare grandi sforzi. In base al sondaggio State of the Phish di quest'anno, il 71% dei lavoratori adulti ha ammesso di aver compiuto un'azione pericolosa, come riutilizzare o condividere una password, fare clic su link inviati da mittenti sconosciuti o divulgare credenziali a una fonte non affidabile. E il 96% lo fa sapendo di correre un rischio. Le persone sono un elemento fondamentale di qualsiasi strategia di difesa efficace, ma possono anche essere il più vulnerabile. Possono commettere errori, cadere vittima di truffe o semplicemente ignorare le best practice di sicurezza.

Il report globale 2024 si basa su un sondaggio globale condotto tra 7.500 lavoratori adulti e 1.050 professionisti dell'IT in 15 paesi, di cui otto in Europa e Medio Oriente. Include inoltre dati dei nostri prodotti e delle ricerche sulle minacce, oltre a informazioni provenienti da 183 milioni di simulazioni di attacchi di phishing inviati dai nostri clienti in un periodo di 12 mesi e oltre 24 milioni di email sospette segnalate dagli utenti dei nostri clienti nello stesso periodo. Per il secondo anno consecutivo, abbiamo anche redatto tre sintesi regionali che mettono in evidenza le sfumature e le differenze.

La maggior parte degli utenti in Europa e Medio Oriente non sa se la responsabilità della sicurezza sia una loro responsabilità o di qualcun altro. Questa mancanza di chiarezza può avere conseguenze disastrose. I nostri dati mostrano una stretta correlazione tra attitudini ed esiti nella regione.

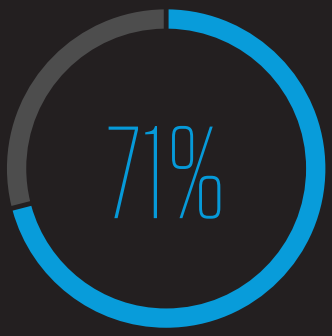
Ogni giorno, gli utenti nella regione presa in esame scelgono tra sicurezza e comodità. Questa sintesi regionale mostra che la maggior parte delle volte privilegiano la comodità. Nelle pagine seguenti analizzeremo più da vicino i comportamenti dei professionisti della sicurezza e degli utenti, nonché alcune delle principali tendenze in materia di minacce. Concluderemo con dei suggerimenti che aiuteranno gli utenti a modificare il loro comportamento e a cominciare a privilegiare la sicurezza.

SOMMARIO

Principali risultati: mondo

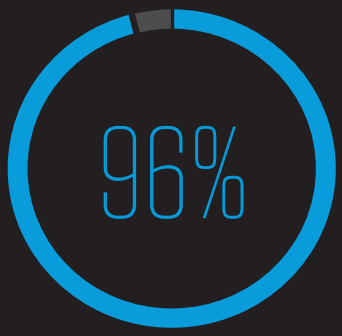
Oltre 1 milione

di attacchi viene lanciato con il framework di elusione dell'autenticazione a più fattori EvilProxy ogni mese, ma l'89% dei professionisti della sicurezza ritiene ancora che l'autenticazione a più fattori offra una protezione completa contro il takeover degli account



di utenti ha compiuto un'azione pericolosa

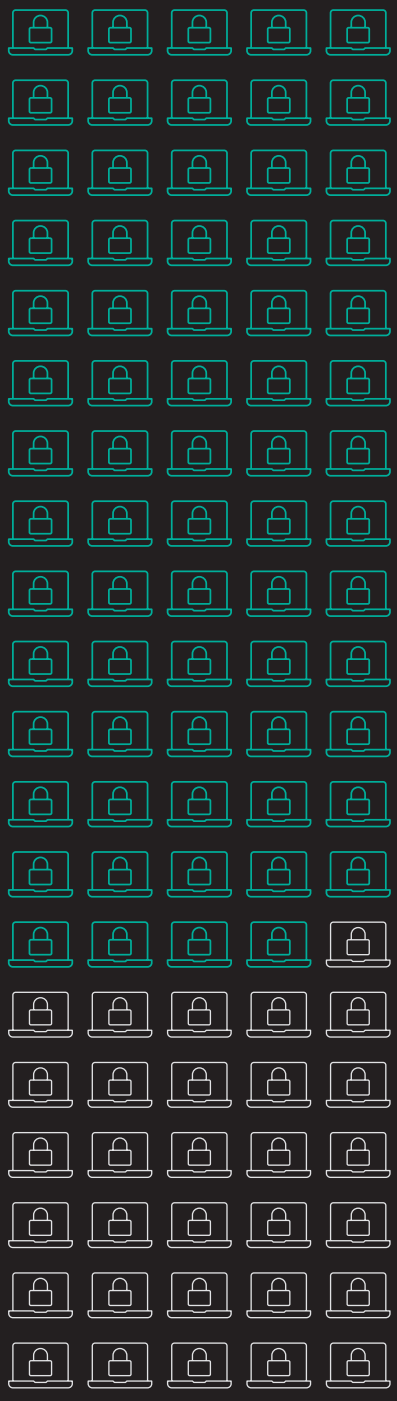
e



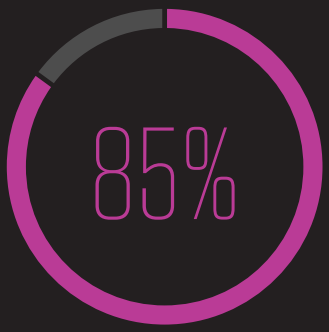
di loro l'ha fatto sapendo di correre un rischio.

66 milioni

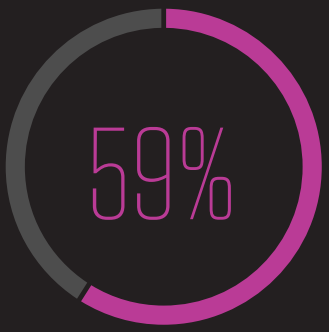
di attacchi BEC sono stati rilevati e bloccati in media ogni mese da Proofpoint.



69% delle aziende è stato infettato dal ransomware.



dei professionisti della sicurezza ha affermato che la maggior parte dei collaboratori sa di essere responsabile della sicurezza, ma



degli utenti non era sicuro o ha affermato di non esserne affatto responsabile.

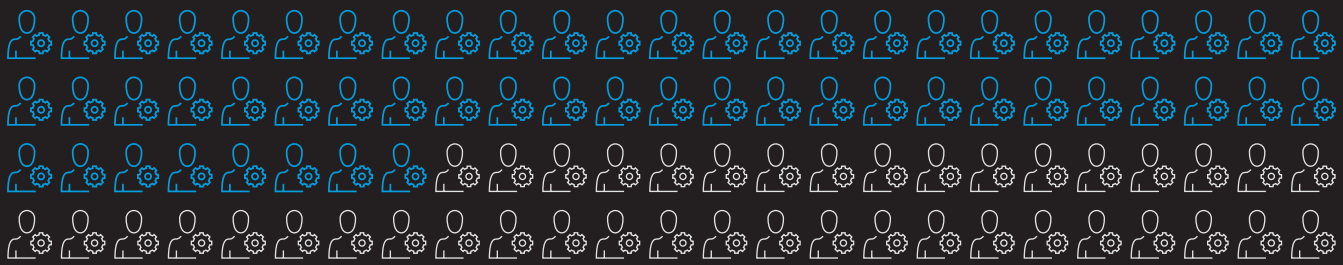
10 milioni

di messaggi TOAD vengono inviati ogni mese

Microsoft continua ad essere il marchio più abusato, con

68 milioni

di messaggi dannosi associati al marchio o ai suoi prodotti



58% degli utenti che ha compiuto azioni pericolose ha assunto comportamenti che li avrebbero resi vulnerabili alle tattiche di social engineering comuni.

Focus su Europa e Medio Oriente

Il report State of The Phish di quest'anno è stato condotto tra 7.500 lavoratori adulti e 1.050 professionisti dell'IT in 15 paesi. Questa sintesi si focalizza sui seguenti Paesi:

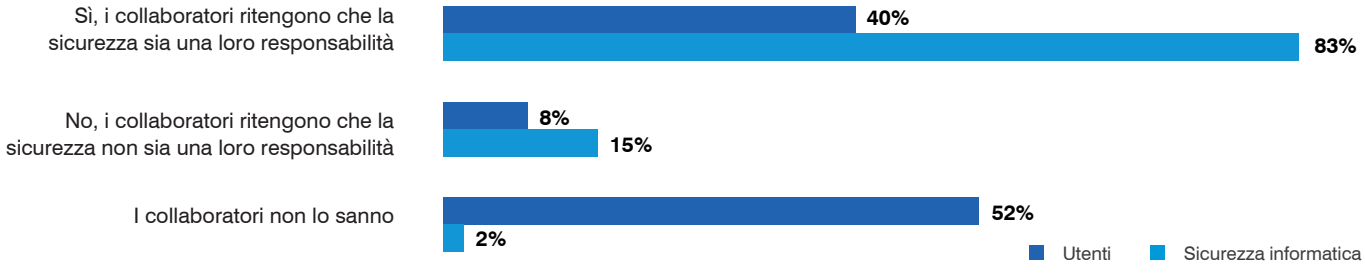
- Francia
- Germania
- Italia
- Paesi Bassi
- Spagna
- Svezia
- Regno Unito
- Emirati Arabi Uniti

Data l'ampia gamma di lingue, culture e livelli di maturità digitale, abbiamo riscontrato variazioni significative tra le varie regioni e tra gli otto Paesi coperti in questa sintesi. La regione è diversificata dal punto di vista geografico, culturale ed economico. Ma per almeno un aspetto la regione mostra una certa uniformità. Gli utenti nella regione sono stati i più numerosi (76%) ad ammettere di aver compiuto un'azione pericolosa rispetto alla media globale (71%). Tuttavia, la percentuale di persone che ha dichiarato di sapere che l'azione intrapresa comportava dei rischi è stata del 95%, ovvero solo 1 punto percentuale in meno rispetto al dato globale.

A livello nazionale, l'86% degli intervistati degli Emirati Arabi Uniti ha ammesso di aver compiuto un'azione pericolosa, la percentuale più elevata tra tutti i Paesi partecipanti al sondaggio. Le aziende degli Emirati Arabi Uniti hanno anche riportato il numero più elevato di attacchi di spear-phishing andati a buon fine, mostrando uno stretto collegamento tra sensibilizzazione degli utenti e livello di sicurezza. Tuttavia, gli Emirati Arabi Uniti hanno registrato il numero più elevato di utenti (62%) che considerano la sicurezza una loro responsabilità rispetto alla media globale (41%).

Gli utenti in Svezia sono stati i meno numerosi ad affermare che la sicurezza sia una loro responsabilità. Ciò è in linea con il numero superiore alla media di utenti che intraprendono azioni pericolose (82%) in Svezia.

Responsabilità in materia di sicurezza (Europa e Medio Oriente)

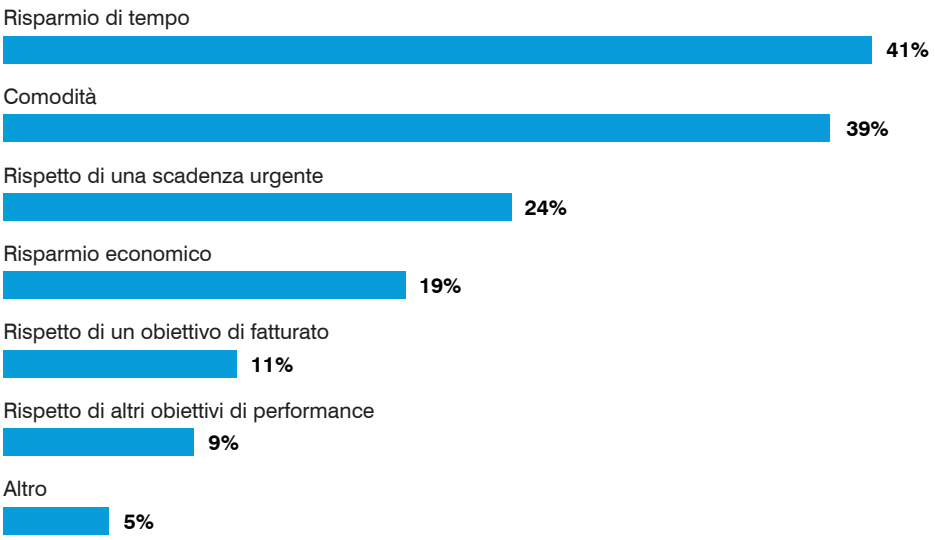


I professionisti della sicurezza nella regione considerano il riutilizzo delle password il comportamento più a rischio. Sfortunatamente, la condivisione e il riutilizzo delle password sono il secondo comportamento più comune tra gli utenti. Ma ci sono alcune buone notizie per i team della sicurezza: l'accesso a siti web inopportuni è l'unica altra azione tra le loro prime cinque ad apparire anche tra i comportamenti più adottati dagli utenti.

Posizione	Comportamenti a rischio (secondo i professionisti della sicurezza)	Comportamenti a rischio (secondo gli utenti)
1	Riutilizzo o condivisione delle password	Utilizzo di dispositivi professionali per attività personali
2	Clic su un link o download di allegati provenienti da uno sconosciuto	Riutilizzo o condivisione delle password
3	Caricamento di dati sensibili su cloud di terze parti non approvato	Collegamento in un luogo pubblico senza utilizzare la VPN
4	Divulgazione di credenziali d'accesso a fonti non affidabili	Risposta a un messaggio (email o SMS) inviato da uno sconosciuto
5	Accesso a siti web inappropriati	Accesso a siti web inappropriati

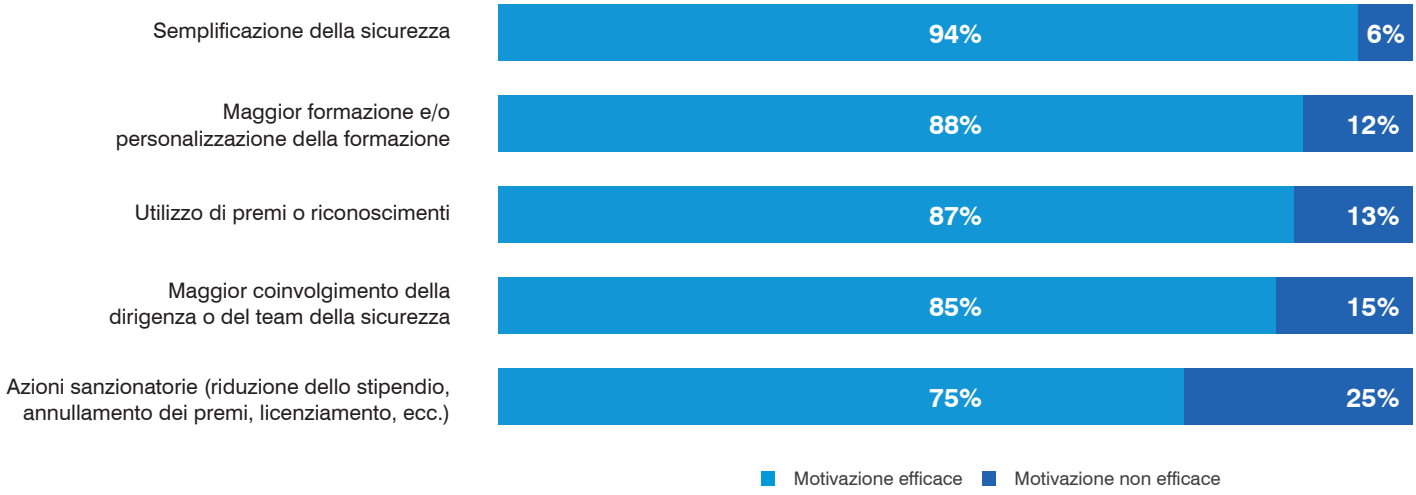
Ma perché gli utenti compiono azioni pericolose? Il risparmio di tempo è stata la risposta più comune, seguita a ruota dalla comodità. Nel Regno Unito, la comodità è in prima posizione e il risparmio di tempo al secondo posto, con un maggior numero di intervistati britannici che cita la comodità più di chiunque altro.

Motivi per cui gli utenti compiono azioni pericolose



Gli utenti in Europa e Medio Oriente spiegano chiaramente perché compiono azioni pericolose. Ma cosa li motiverebbe ad anteporre la sicurezza? Come a livello globale, la maggior parte ha menzionato la semplificazione della sicurezza come la motivazione più efficace e le azioni sanzionatorie come le meno motivanti.

Strategie per rendere la sicurezza una priorità per gli utenti



78%

delle aziende tedesche ha subito un attacco TOAD, ma solo il

21%

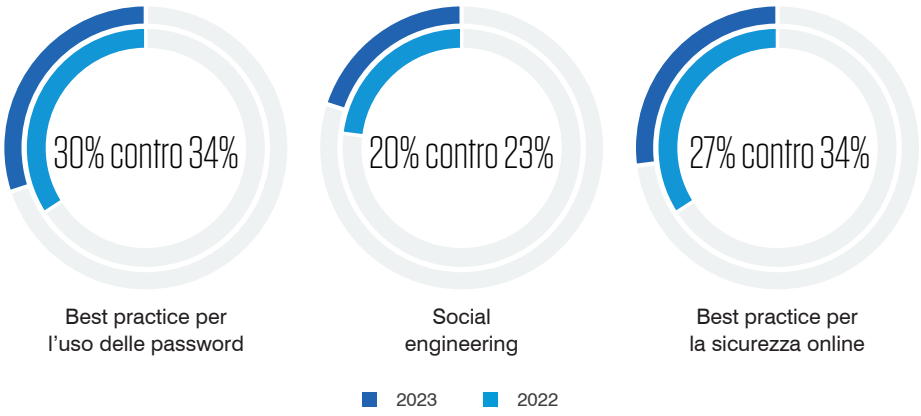
lo utilizza come tema per la formazione.

Possibilità di miglioramento

Il 95% delle aziende nella regione utilizza già la threat intelligence per creare i propri programmi di formazione e di sensibilizzazione alla sicurezza informatica. Ma ci sono lacune significative. Sebbene la maggior parte delle aziende abbia dichiarato di essere stata colpita da attacchi tramite telefonate (TOAD, Telephone-Oriented Attack Delivery), meno di un terzo lo utilizza come tema per la formazione. In Germania, il 78% delle aziende ha subito attacchi TOAD, ma solo il 21% li utilizza come tema della formazione, uno dei divari più ampi tra attacchi quotidiani e argomenti della formazione.

Complessivamente, viene dedicato più tempo alla formazione di sensibilizzazione alla sicurezza informatica nella regione. La Spagna ha registrato l'incremento maggiore, con un aumento del 120% del numero di aziende che vi dedicano tre o più ore all'anno.

Tuttavia, la percentuale di aziende che propongono questi temi di formazione fondamentali sembra essere in calo:



Queste sono tutte nozioni di sicurezza fondamentali. Se meno utenti sanno come configurare password sicure, evitare esche comuni e navigare sul web in modo sicuro, i criminali informatici ne approfitteranno di sicuro.

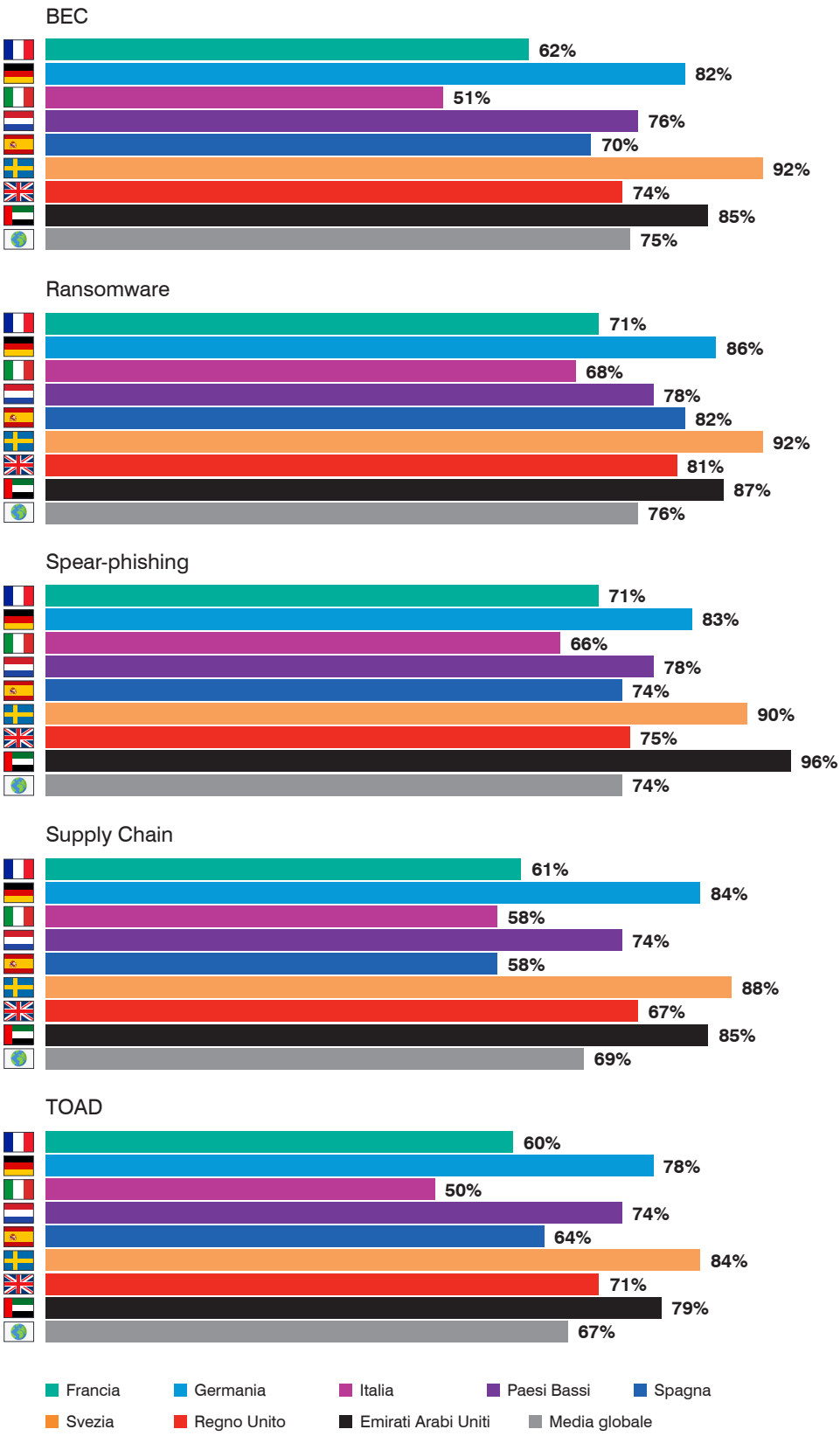
Panorama delle minacce in Europa e Medio Oriente

Lo scorso anno il panorama delle minacce regionale ha seguito le tendenze globali. Le violazioni dell'email aziendale (BEC, Business Email Compromise) hanno subito un calo a livello mondiale, ma i Paesi non anglofoni hanno registrato un aumento. Ciò potrebbe essere legato all'aumento degli strumenti di intelligenza artificiale generativa come ChatGPT, che possono essere utilizzati per scrivere email ingannevoli convincenti in diverse lingue. Tendenze simili sono state osservate in altri Paesi non anglofoni in tutto il mondo. Complessivamente, il 75% delle aziende ha osservato almeno un attacco di phishing andato a buon fine, in calo rispetto all'88% del 2022.

Nella regione gli attacchi TOAD sono stati lievemente superiori (70%) rispetto alla media globale (67%). L'84% delle aziende svedesi ha subito un attacco TOAD, il livello più elevato nella regione.

Come a livello globale, le aziende in Europa e Medio Oriente hanno segnalato un aumento delle conseguenze negative a seguito di attacchi andati a buon fine. Le sanzioni finanziarie sono aumentate del 122%, una percentuale leggermente inferiore rispetto al dato globale, che potrebbe indicare che multe per il GDPR siano già state pagate nel corso degli anni precedenti.

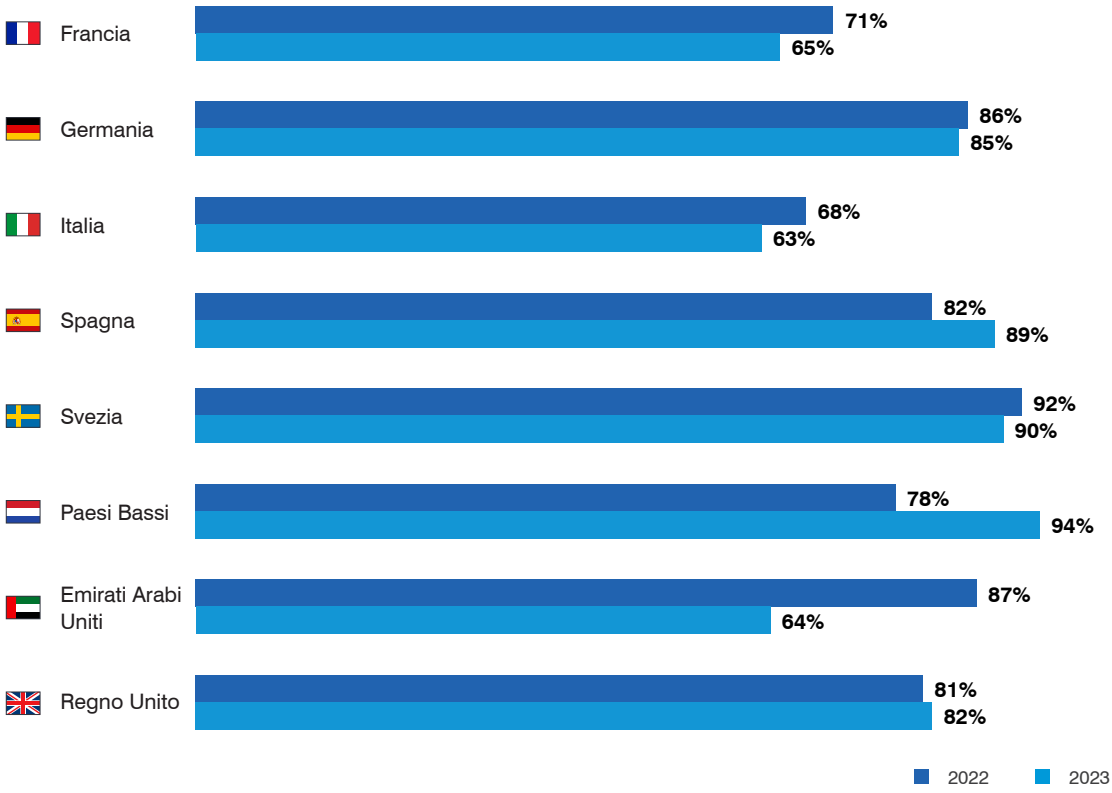
Percentuale di aziende colpite da attacchi mirati



Ransomware

Il ransomware rimane una minaccia grave per le aziende della regione; il numero di attacchi e infezioni è aumentato nel corso dello scorso anno. Tuttavia, i dettagli variano in funzione del Paese.

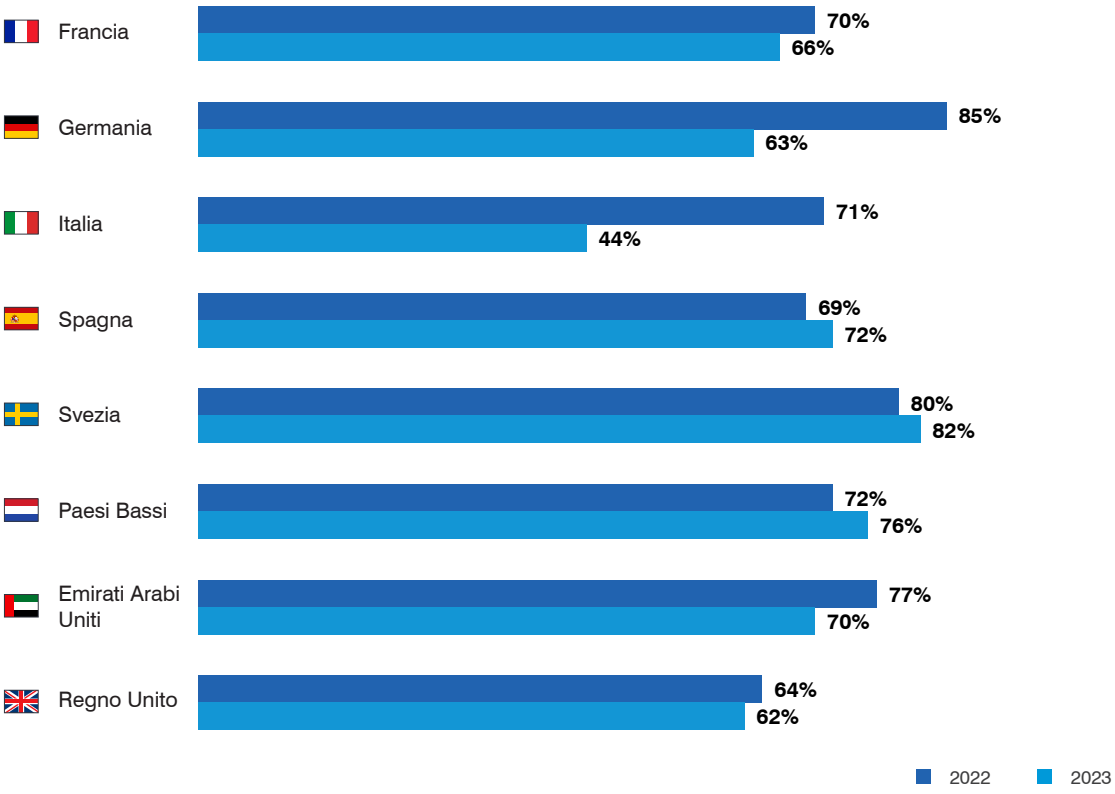
Attacchi ransomware via email



Le aziende italiane, per esempio, hanno segnalato il maggior incremento del numero di infezioni di ransomware andate a buon fine, passando dal 44% nel 2022 al 71% nel 2023, nonostante affrontino lo stesso volume di attacchi delle aziende di tutti gli altri Paesi. Ciò ha spinto le autorità italiane a emanare un'allerta a giugno sul crescente numero di attacchi ransomware che sfruttano un bug VMware.

La Svezia ha subito lo stesso livello di attacchi ransomware nel mondo, con il 92% delle sue aziende prese di mira. Ciò può essere legato al fatto che, in un precedente sondaggio, il 74% degli intervistati svedesi ha menzionato il furto delle credenziali di accesso come la causa principale delle violazioni dei dati. Dare priorità alla protezione contro questi attacchi può ridurre la possibilità di attività secondarie, come la distribuzione di ransomware.

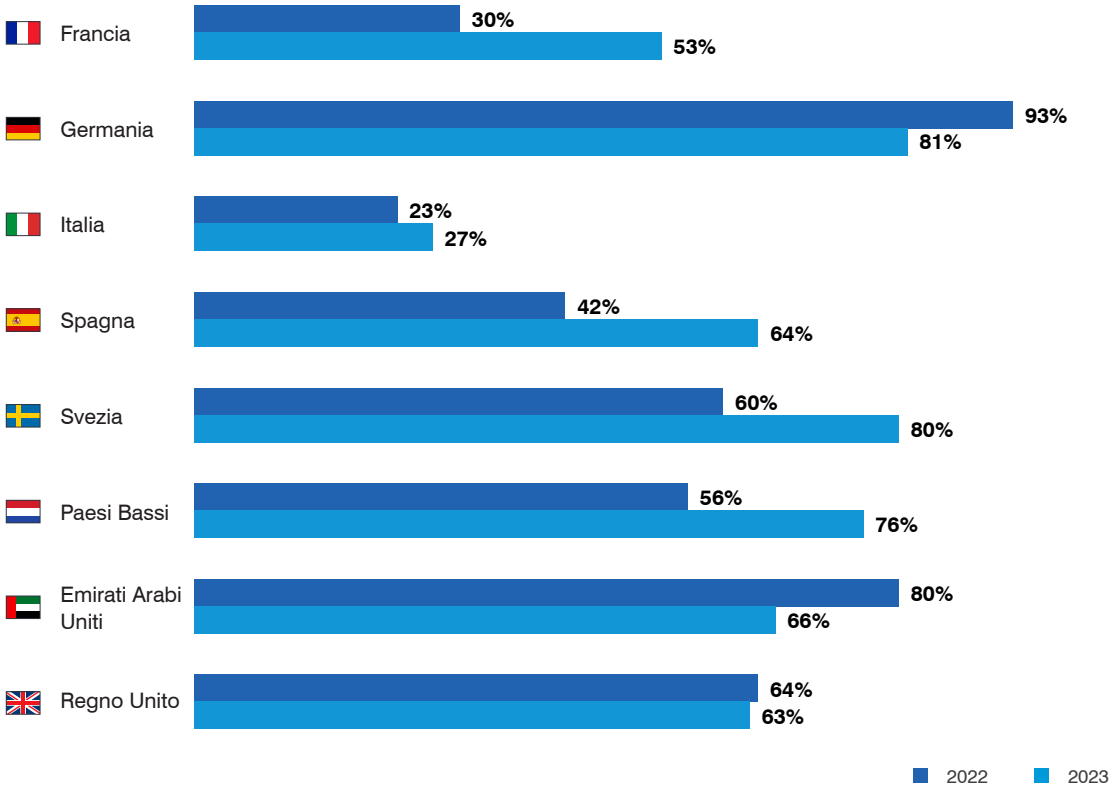
Infezioni ransomware



D'altro canto, solo tre Paesi - Germania, Emirati Arabi Uniti e Regno Unito - hanno mostrato una maggior propensione al pagamento. La Germania ha registrato anche la percentuale più elevata di aziende che hanno pagato un riscatto (93% rispetto alla media globale del 54%).

Questa strategia è sembrata funzionare per le aziende in Germania e Emirati Arabi Uniti, molte delle quali hanno recuperato i propri sistemi e dati dopo un solo pagamento. Il fatto che l'85% delle aziende tedesche abbia dichiarato di aver subito un'infezione di ransomware andata a buon fine, la percentuale più elevata nella regione, suggerisce un collegamento tra la loro volontà di pagare e l'intensità del targeting.

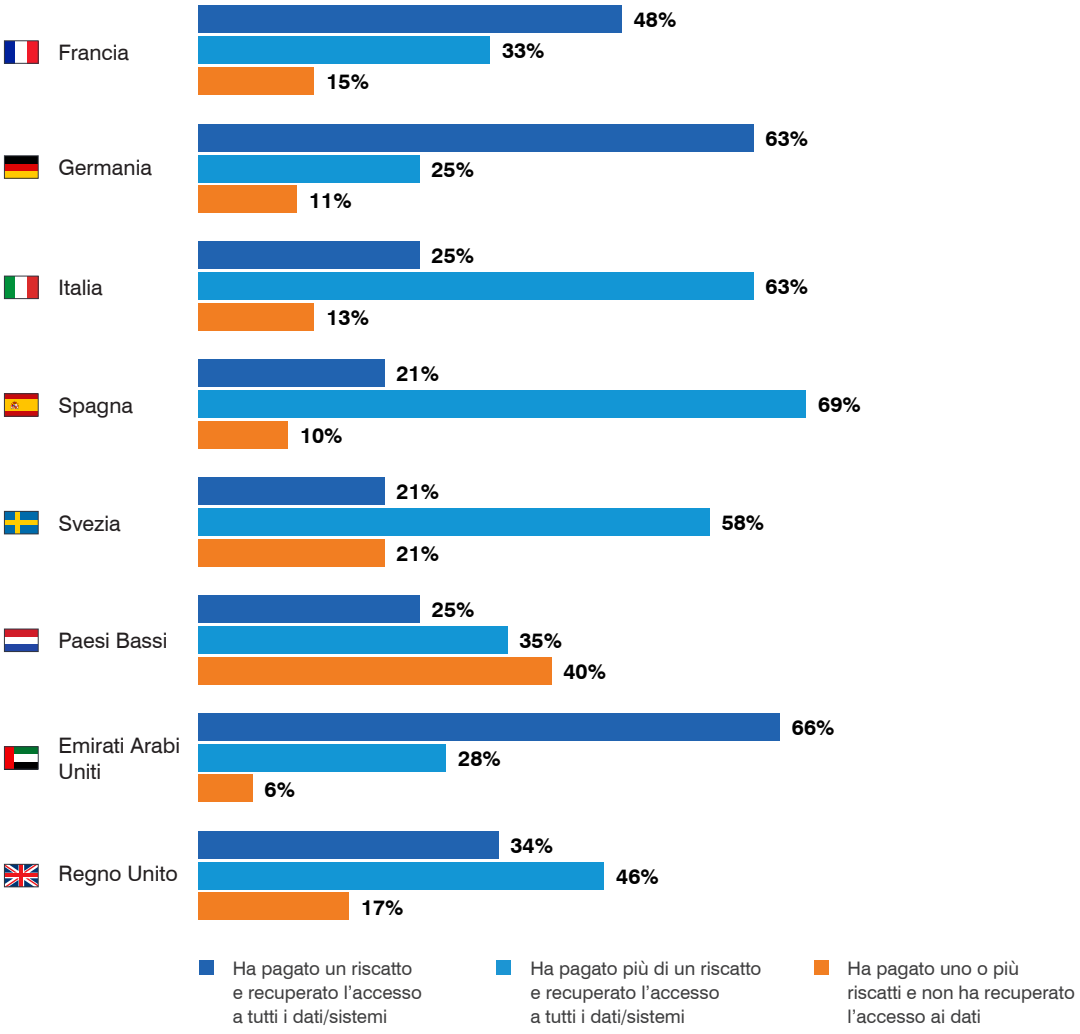
Percentuale di aziende che hanno pagato un riscatto



Le aziende del Regno Unito non se la sono cavata altrettanto bene. In effetti, hanno registrato la percentuale più elevata di infezioni ripetute. Circa il 14% ha subito 10 o più infezioni, rispetto al 5% a livello globale. Ciò mostra che il pagamento del riscatto non garantisce l'immunità contro i futuri attacchi e potrebbe addirittura incoraggiarli.

Le aziende olandesi hanno registrato il minor numero di risultati positivi a seguito del pagamento. Il 40% ha dichiarato di non aver mai recuperato i dati, rispetto al 16% a livello globale. Ciò suggerisce che alcuni gruppi di ransomware potrebbero non rispettare le loro promesse o non essere sempre in grado di ripristinare i dati.

Risultati a seguito del pagamento di un riscatto



Una nota positiva è che i livelli di copertura per i contratti di assicurazione contro i rischi informatici sono migliorati, offrendo sgravi finanziari. L'unica eccezione è rappresentata dalla Francia, per cui la percentuale di aziende parzialmente o interamente coperte è scesa dall'87% nel 2022 al 76% nel 2023. Ciò è probabilmente dovuto al fatto che la più grande compagnia di assicurazioni francese ha annunciato che non coprirà più gli attacchi ransomware.

Raccomandazioni

I risultati del nostro sondaggio mostrano che gli utenti in Europa e Medio Oriente comprendono che il loro comportamento comporta dei rischi. Tuttavia, spesso ciò non è sufficiente per convincerli ad accordare la priorità alla sicurezza. Alcuni privilegiano la comodità o desiderano risparmiare tempo, mentre altri semplicemente non sanno se la sicurezza informatica è una loro responsabilità.

Per gli utenti che già comprendono che la sicurezza è una loro responsabilità

- Fornisci agli utenti strumenti che permettano loro di essere più proattivi. I tasti di segnalazione delle email permettono di segnalare facilmente i messaggi sospetti. Inoltre, le tecnologie di esortazione, come la visualizzazione di avvisi per le email sospette, possono spingere gli utenti ad agire. Prevedi anche di creare una rete di promotori e un sistema di ricompense per incoraggiare questi utenti a prendere a modello le best practice e a diventare sostenitori della segnalazione tra i loro colleghi che non sanno come comportarsi.

Per gli utenti che non sanno o pensano che la sicurezza non sia una loro responsabilità

- Proponi una formazione personalizzata e pertinente per ogni ruolo e responsabilità. Moltiplica le comunicazioni da parte della dirigenza e dei responsabili della sicurezza per informare meglio gli utenti in merito alle loro responsabilità e al loro impatto sull'azienda.

È inoltre importante proporre una formazione sulla sicurezza informatica e le funzionalità di prevenzione, rilevamento e risposta all'avanguardia. Soluzioni avanzate possono contribuire a trovare il giusto equilibrio tra controlli di sicurezza più rigorosi e produttività, riducendo il numero di minacce che gli utenti si trovano ad affrontare. Per esempio, l'implementazione di una soluzione di protezione dell'email efficace al 99,9% significa che la maggior parte degli utenti non dovrà mai decidere come reagire di fronte a un link sospetto.

Infine, collabora con le parti interessate aziendali e privilegia la facilità d'utilizzo quando si tratta di implementare le policy di sicurezza. Gli utenti saranno meno inclini a eludere i sistemi se la sicurezza è in linea con i loro obiettivi. E sono più propensi a utilizzare un controllo se è intuitivo e non richiede alcuna formazione.

PER SAPERNE DI PIÙ

Per scoprire come Proofpoint può fornirti informazioni sui rischi legati agli utenti e aiutarti a mitigarli con una strategia di sicurezza informatica incentrata sulle persone, visita il sito **www.proofpoint.com/it**

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui l'85% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.

proofpoint.

0402-001-05-01