proofpoint.

REPORT

Europa e Medio Oriente

2023 State of The Phish

Un'analisi approfondita sulla sensibilizzazione degli utenti, le vulnerabilità e la resilienza

proofpoint.com/it

UN'INDAGINE CONDOTTA FRA:

7.500

lavoratori aduli in 15 paesi

1.050

professionisti della sicurezza informatica in questi stessi paesi

E BASATA SU:

135 milioni

di simulazioni di attacchi di phishing inviati dai nostri clienti in un periodo di 12 mesi

18 milioni

di email segnalate dagli utenti dei nostri clienti in un periodo di 12 mesi

2022: un anno all'insegna della creatività dei criminali informatici

Ogni anno, i criminali informatici sviluppano nuovi schemi per ingannare le vittime e aggirare le difese. E il 2022 non ha fatto eccezione. Le aziende hanno implementato nuovi controlli di sicurezza e i criminali informatici hanno risposto di conseguenza.

I criminali informatici hanno aggiunto al loro arsenale tecniche complesse come gli attacchi tramite telefono e l'elusione dell'autenticazione a più fattori (MFA). Sconosciute alla maggior parte degli utenti, queste tecniche offrono ai criminali informatici un nuovo vantaggio. A fronte di una tale diffusione, i CISO e i team della sicurezza delle informazioni sono stati molto impegnati.

Giunto alla sua nona edizione, il nostro report annuale *State of The Phish* si basa sui dati raccolti da un'indagine condotta in 15 paesi per valutare la sensibilizzazione degli utenti, la resilienza e le vulnerabilità. Il report mette a confronto il livello di comprensione degli attacchi informatici e delle tattiche di difesa comuni. Inoltre, analizza come le lacune nella conoscenza e le pratiche insufficienti in materia di sicurezza informatica favoriscono lo sviluppo del panorama delle minacce. La maggior parte degli attacchi prende di mira le persone prima che i sistemi. Per questo motivo, la sezione finale di questo report esamina le pratiche di formazione sulla sicurezza e mette l'accento sulle opportunità di creare e sostenere una cultura basata sulla sicurezza a tutti i livelli.

Oltre al report principale, quest'anno abbiamo sviluppato delle sintesi regionali per determinare come le sfumature locali possano influenzare le lacune in materia di sensibilizzazione. Questa sintesi regionale include i dati relativi a **Emirati Arabi Uniti, Francia, Germania, Italia, Paesi Bassi, Regno Unito, Spagna e Svezia**. I dati provengono da un sondaggio condotto su 4.000 lavoratori adulti e 650 professionisti della sicurezza informatica.

SOMMARIO

Principali risultati a livello mondiale

44%

degli intervistati ritiene che un'email sia sicura quando include un marchio familiare

300.000-400.000

tentativi di attacchi tramite telefono ogni giorno nel 2022, con un picco di 600.000 al giorno ad agosto

1/3

degli intervistati ha intrapreso un'azione pericolosa (come fare clic su link o scaricare malware) a fronte di un attacco

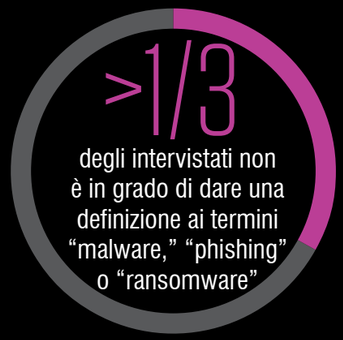
aumento delle perdite finanziarie dirette causate dagli attacchi di phishing

30 milioni

di messaggi pericolosi inviati nel 2022 hanno coinvolto il marchio o i prodotti Microsoft

>1 su 10

percentuale di minacce bloccate in seguito alla segnalazione di un utente



degli intervistati non è in grado di dare una definizione ai termini "malware," "phishing" o "ransomware"

Manca anche la comprensione di concetti di base

SOLO 35%

delle aziende effettua simulazioni di attacchi di phishing

64% delle aziende infettate dal ransomware ha pagato un riscatto

90% delle aziende colpite dal ransomware possedeva una polizza assicurativa contro i rischi informatici

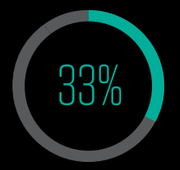
65% delle aziende ha segnalato almeno una perdita di dati di origine interna

SOLO 56%

delle aziende con un programma di sensibilizzazione alla sicurezza forma tutti i suoi collaboratori

dei professionisti della sicurezza considera la sicurezza una priorità assoluta nella loro azienda

ma



dei collaboratori ammette che la sicurezza informatica non è una delle loro priorità sul posto di lavoro

94%

delle aziende svedesi sono risultate le più a rischio di subire un attacco di phishing riuscito

ma...

Solo il 18%

delle aziende svedesi forma gli utenti che sanno essere presi di mira

Focus su Europa e Medio Oriente

Come prevedibile, data la diversità in termini di lingue, culture e livelli di maturità digitale abbiamo registrato variazioni significative tra i 15 paesi coinvolti nell'indagine per il report *State of The Phish*. E questo vale anche per gli otto paesi oggetto di questa sintesi.

Di tutte le regioni coinvolte nell'indagine, l'EMEA (Europa, Medio Oriente e Africa) è probabilmente la più diversificata. Questo immenso territorio geografico, che abbraccia sia l'emisfero settentrionale che quello meridionale, comprende culture, politiche ed economie molto diverse tra loro. Come molti altri luoghi nel 2022, i paesi della regione EMEA hanno registrato cambiamenti geopolitici e un acuirsi dei conflitti. Non sorprende che ciò si sia riflesso nel panorama della sicurezza informatica.

Con una percentuale del 94%, le aziende svedesi sono quelle che sono risultate le più a rischio di subire un attacco di phishing riuscito tra tutti i Paesi presi in esame per questo report. Naturalmente, questi dati anomali possono essere il risultato di diversi fattori. Una potenziale spiegazione potrebbe essere la scarsa importanza attribuita alla formazione di sensibilizzazione alla sicurezza informatica del paese: solo il 18% delle aziende svedesi forma gli utenti che sanno essere presi di mira, una percentuale inferiore a quella di tutti gli altri Paesi presi in esame. È anche possibile che i tassi di segnalazione siano più elevati. La Svezia è all'avanguardia nella sicurezza dei dati fin dagli anni '70, avendo approvato una delle prime leggi europee sulla privacy digitale. Pertanto, potrebbe essere culturalmente più accettabile ammettere le violazioni di sicurezza, il che si traduce in segnalazioni più accurate.

Questo abbiamo incluso l'Italia per la prima volta e i risultati sono sorprendenti. Tra tutti i 15 Paesi presi in esame, le aziende italiane sono risultate le meno a rischio di essere prese di mira da un'ampia gamma di minacce. Solo il 47% ha perso dati o proprietà intellettuale a causa di un attacco esterno (rispetto al 69% della media globale). Rispetto a altri paesi coinvolti in questo report, le aziende italiane sono risultate le meno a rischio di subire un attacco di phishing (79%). Questi risultati possono indicare un ritardo o un'immaturità nei confronti delle normative sulla segnalazione degli incidenti di sicurezza. Potrebbero anche riflettere una cultura meno attenta alla trasparenza e alla trasparenza delle informazioni.

Considerando altre categorie di attacchi informatici, abbiamo rilevato che la violazione dell'email aziendale (BEC, Business Email Compromise) si sta diffondendo rapidamente. Paesi Bassi e Svezia hanno registrato il tasso di attacchi più elevato con il 92% (rispetto alla media globale del 75%). Il numero di incidenti è aumentato più rapidamente in Germania e in Spagna, con un incremento medio del 16,5% rispetto all'anno precedente. L'evoluzione della lingua può giocare un ruolo determinante nell'aumento degli attacchi BEC. In passato, la maggior parte delle email BEC era scritta in inglese. Recentemente, però, abbiamo notato un aumento delle email BEC scritte in tedesco, spagnolo, sloveno e altre lingue. Ciò è in linea con la crescente sofisticatezza degli attacchi.

I Paesi Bassi si contraddistinguono come il paese più colpito dagli attacchi informatici condotti da utenti interni (86% rispetto alla media globale dell'66%) e da criminali informatici esterni (84% rispetto al 68%). Ma la formazione sembra essere efficace. I collaboratori olandesi sono i meno propensi a rivelare informazioni personali o le proprie password.

PARLIAMO DI TERMINOLOGIA:

Manca la piena comprensione anche di concetti di base: oltre un terzo degli utenti non è in grado di dare una definizione ai termini "malware", "phishing" e "ransomware"

40%

degli utenti sa cos'è il ransomware, un aumento di 9 punti percentuali rispetto al 2019, l'incremento maggiore tra i termini menzionati

29% e 30%

degli utenti conosce, rispettivamente, i termini relativamente nuovi "SMiShing" e "vishing"

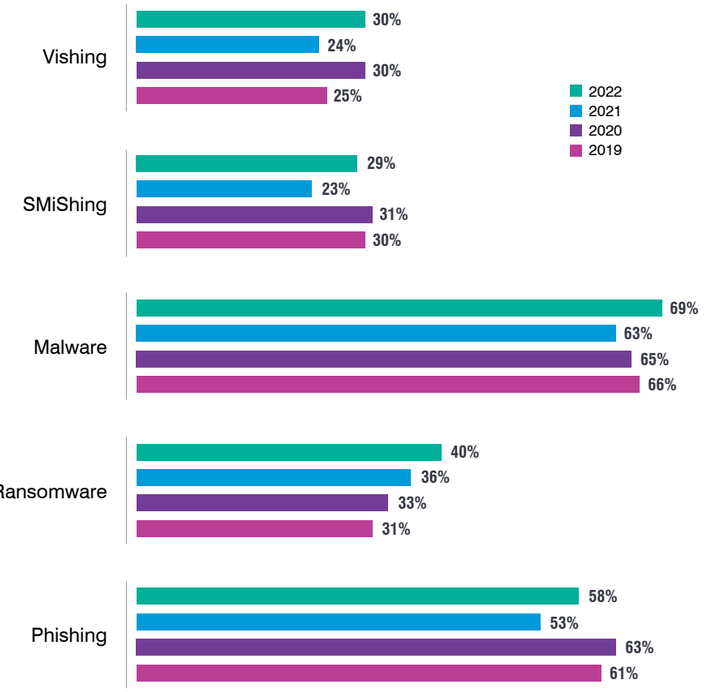
58%

degli utenti sa cos'è il phishing, un incremento di 5 punti percentuali rispetto all'anno scorso ma un calo di 3 punti rispetto al 2019

Sensibilizzazione alla sicurezza: cifre e opportunità

In tutti i 15 Paesi presi in esame, emerge uno schema simile per quanto riguarda la conoscenza dei termini di sicurezza di base da parte degli utenti finali. Le minacce più comuni, come il phishing, il ransomware e il malware, esistono da anni, ma le persone non capiscono ancora bene ciò che rappresentano. E c'è ancora meno consapevolezza di minacce più recenti come lo SMiShing (phishing via SMS) e il vishing (phishing vocale). Purtroppo, i nostri dati mostrano pochi cambiamenti rispetto all'anno precedente.

La comprensione degli utenti è cambiata poco rispetto all'anno precedente



IL PRINCIPIO DI INDETERMINAZIONE:

69%

degli utenti nei Paesi Bassi sa cos'è il phishing, la percentuale più elevata tra gli otto paesi che abbiamo intervistato in questa regione

45%

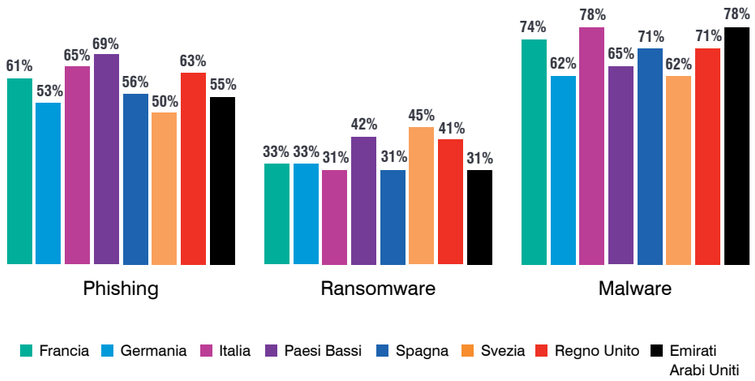
degli svedesi intervistati conosce il ransomware, superando gli altri sette paesi.

78%

degli utenti in Italia e negli Emirati Arabi Uniti sa cos'è il malware, le percentuali più elevate di consapevolezza tra gli otto paesi in questa regione

Emergono diverse differenze degne di nota quando si mettono a confronto le conoscenze degli utenti relativamente alle tre minacce più comuni. Gli intervistati svedesi e tedeschi sono risultati i meno capaci a fornire una definizione di "malware" o "phishing". Per contro, gli intervistati in Italia e Emirati Arabi Uniti sono i stati i migliori nel definire il termine "malware" ma hanno ottenuto risultati inferiori alla media nella definizione del termine "ransomware".

Conoscenza delle minacce comuni (accuratezza)



Queste differenze potrebbero essere spiegate dal fatto che meno del 50% delle aziende di Europa e Medio Oriente fanno formazione su questi argomenti. Le medie europee sono ammontate al 37% per il phishing, 34% per il ransomware, 40% per il malware e 27% per gli attacchi BEC.

FORMAZIONI TEMATICHE:

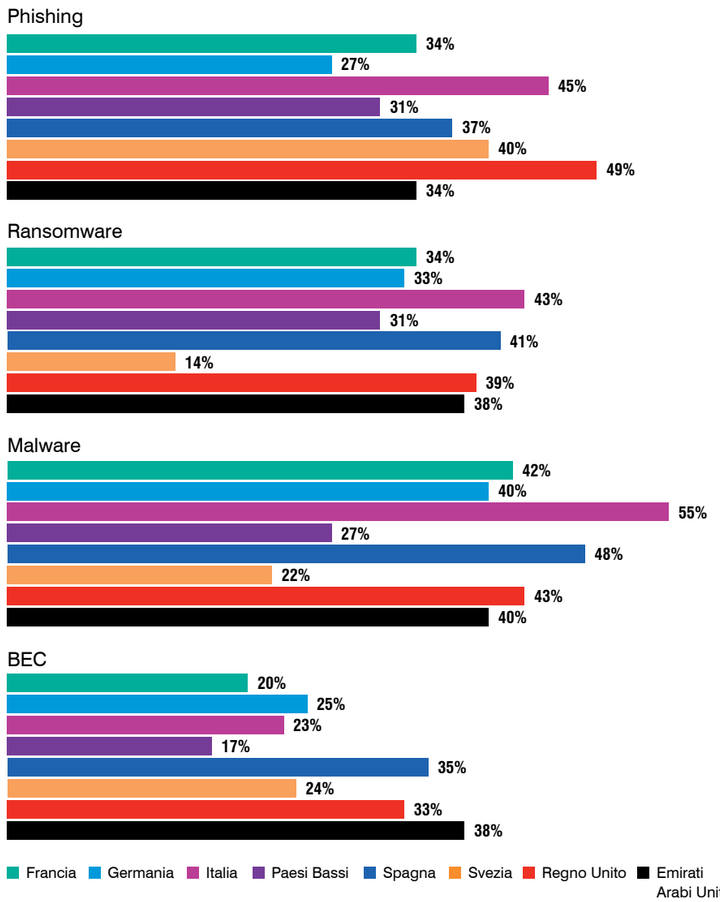
55%

delle aziende italiane educa gli utenti a riconoscere il malware, la percentuale più elevata per un argomento in tutti i paesi della regione

14%

delle aziende svedesi forma gli utenti sul ransomware, la percentuale più bassa per un argomento in tutti i paesi della regione

Argomenti affrontati nei programmi di formazione e sensibilizzazione alla sicurezza



Se la maggior parte delle aziende dispone di un programma di sensibilizzazione alla sicurezza, non tutti i collaboratori all'interno di queste aziende ricevono formazione. Un dato che spicca è quello delle aziende degli Emirati Arabi Uniti: il 64% forma tutti i collaboratori e il 52% gli utenti notoriamente presi di mira. Inoltre, il 74% delle aziende degli Emirati Arabi Uniti forma i collaboratori su argomenti di sicurezza che li riguardano esplicitamente, un dato superiore a quello degli altri 14 paesi.

SENSIBILIZZAZIONE PER TUTTI:

64%

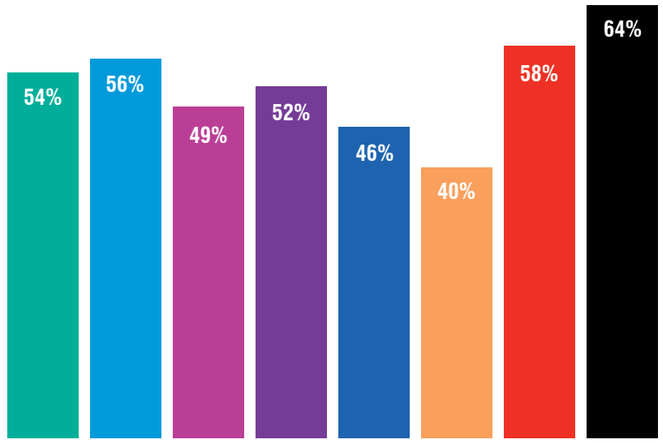
dei datori di lavoro negli Emirati Arabi Uniti ha formato tutti i collaboratori dell'azienda, la percentuale più elevata tra i paesi coinvolti nell'indagine in Europa e Medio Oriente

40%

delle aziende svedesi ha fatto lo stesso, la percentuale più bassa tra i paesi coinvolti in questa regione

I CISO britannici sembrano fare un buon lavoro nel rendere la sicurezza una priorità per le loro aziende. I collaboratori britannici sono quelli più inclini ad avere fiducia nel loro team IT e ad affermare che la sicurezza informatica è una priorità della loro azienda. Questa convinzione potrebbe essere dovuta alla formazione: le aziende britanniche sono a pari merito con gli Emirati Arabi Uniti per quanto riguarda i tassi più alti di formazione per gli utenti che sanno essere presi di mira (52%).

Percentuale di aziende che formano tutti i collaboratori nell'ambito del loro programma di sensibilizzazione alla sicurezza informatica



Con il 48%, le aziende spagnole sono le più numerose a eseguire delle simulazioni di attacchi di phishing (vedi grafici alla pagina successiva). Il Regno Unito si è distinto per aver attribuito un valore elevato al contatto personale, con il 45% della formazione di persona. All'interno della regione, le aziende britanniche sono le più propense a trattare il phishing (49%), ma molto meno propense a utilizzare simulazioni di attacchi di phishing (39%) rispetto alle aziende spagnole.

TIPI DI FORMAZIONE:

45%

delle aziende del Regno Unito ha offerto una formazione di persona, la percentuale più elevata di tutti i paesi intervistati in Europa e Medio Oriente

50% e 48%

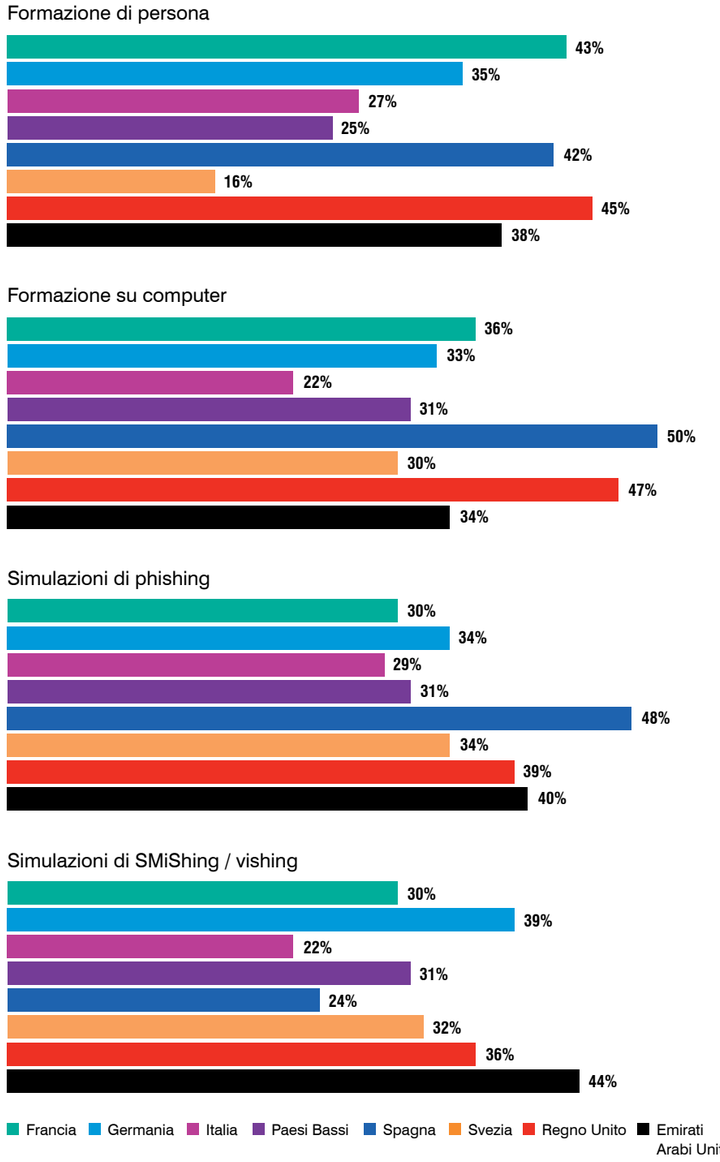
delle aziende spagnole ha offerto, rispettivamente, formazione su computer e ha eseguito simulazioni di attacchi di phishing, il che le distingue da altri paesi

44%

delle aziende degli Emirati Arabi Uniti ha effettuato simulazioni di attacchi di SMiShing e vishing, la percentuale più elevata in questa regione

Le cifre relative alla formazione in Svezia suggeriscono che le aziende non prendono abbastanza seriamente la sicurezza. Poche aziende fanno formazione di persona (16%). Le aziende svedesi sono anche le meno propense a formare tutti i loro collaboratori (40%). Questo dato è sorprendente se si considera che le infezioni ransomware sono più elevate in Svezia che in qualsiasi altro Paese preso in esame in questo report (82%).

Tipi di formazione



LA MINACCIA CHE VIENE DALL'INTERNO:

71%

delle aziende della regione EMEA ha subito una perdita di dati a causa di incidenti di origine interna

54%

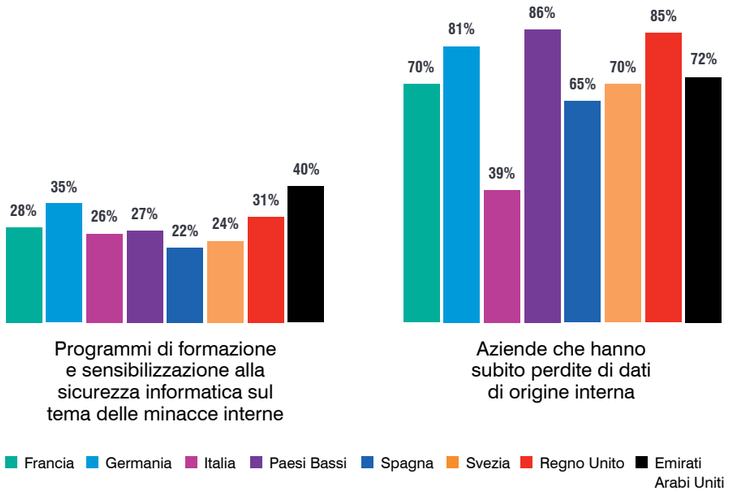
ha subito tre o più attacchi

Sensibilizzazione alla sicurezza informatica: minacce interne in evidenza

Quest'anno abbiamo ampliato la nostra indagine per riflettere la crescente influenza delle minacce interne, una categoria che va dal furto di dati da parte di utenti malintenzionati alla perdita di dati dovuta alla negligenza dei collaboratori e al furto di credenziali d'accesso.

In tutta la regione, il 71% delle aziende in media ha subito una perdita di dati a causa di minacce interne. È degno di nota lo scollamento tra l'elevato livello di attacchi e il basso livello medio di formazione sulla sicurezza, pari al 29%.

Rischi interni di fuga di dati



Le aziende tedesche sono risultate le più a rischio di subire frequenti attacchi di origine interna(18%) e i collaboratori tedeschi sono risultati anche i più propensi a portare con sé le informazioni di lavoro nel momento di lasciare il posto di lavoro. Questo potrebbe essere dovuto al fatto che i collaboratori tedeschi ritengono semplicemente che le informazioni appartengano a loro: solo il 35% delle aziende tedesche fa formazione sulle minacce interne. Se si confronta questo dato con quello delle aziende degli Emirati Arabi Uniti, sebbene solo il 4% di queste riferisce di frequenti attacchi di origine interna, il 40% forma i propri collaboratori. Questo potrebbe essere dovuto al fatto che i collaboratori degli Emirati Arabi Uniti sono stati i più propensi nella regione (29%) a rivelare accidentalmente informazioni personali o password di account a persone di cui non dovrebbero fidarsi.

VACANZE ROMANE:

il numero di aziende italiane che hanno subito attacchi mirati di vario tipo è inferiore a quello degli altri paesi presi in esame.

79%

è stato vittima di attacchi di phishing

51%

è stato preso di mira da un attacco BEC

63%

è stato preso di mira dal ransomware (solo gli Emirati Arabi Uniti hanno registrato una percentuale inferiore)

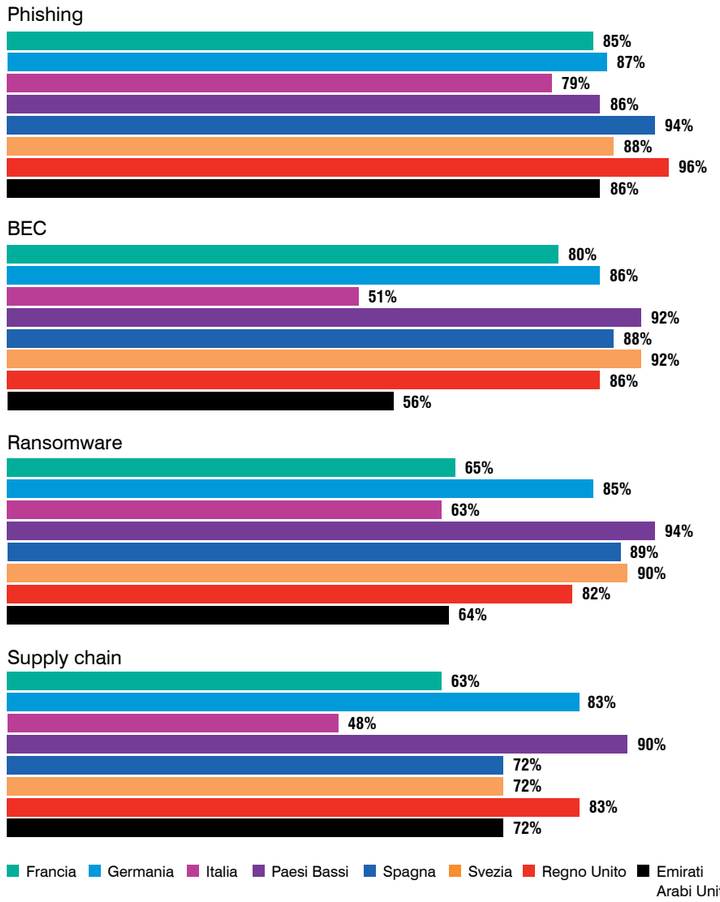
48%

ha subito attacchi alla supply chain

Tendenze del panorama delle minacce

Complessivamente, le aziende francesi si contraddistinguono collocandosi nella media della regine per tutti i tipi di attacchi mirati. Riteniamo che questi dati riflettano la maturità del Paese in materia di sicurezza informatica.

Percentuale di aziende colpita da attacchi mirati



PAGAMENTO DEI RISCATTI:

27%

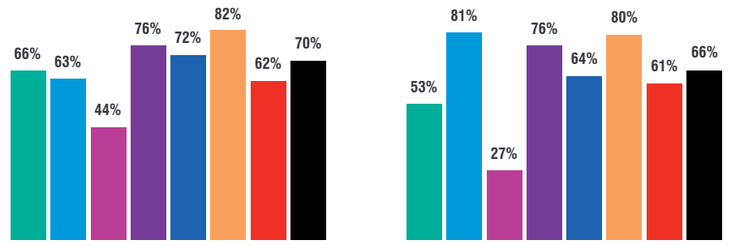
delle aziende italiane infettate dal ransomware ha pagato il riscatto richiesto dai criminali informatici, la percentuale più bassa tra i paesi coinvolti in questo report. Le aziende italiane sono risultate le meno a rischio di subire un'infezione (44%) e quelle con le minori possibilità di essere risarcite dalla propria assicurazione (56%).

Ransomware: le società di assicurazione aiutano le vittime

Il ransomware viene diffuso in una seconda fase, dopo la violazione iniziale. Cinque paesi della regione EMEA hanno mostrato un'elevata probabilità di infezione di ransomware.

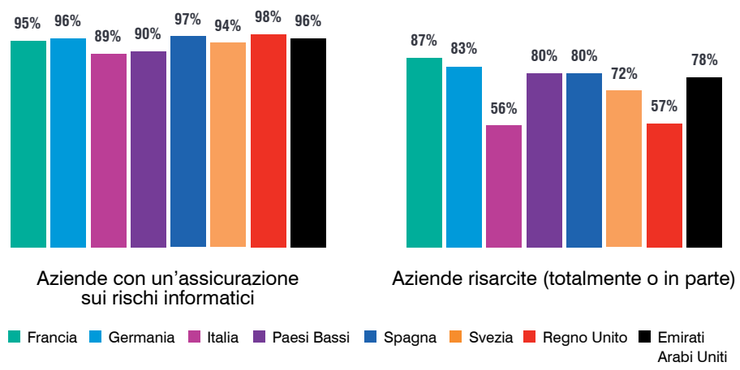
Tra tutti i paesi presi in esame, le aziende svedesi sono state quelle con la maggior probabilità di essere infettate dal ransomware (82%). La Svezia è uno dei paesi più connessi al mondo. E un pioniere nella digitalizzazione del settore pubblico e delle principali industrie. Queste cifre possono essere spiegate dal fatto che durante la pandemia molte aziende hanno trascurato la protezione contro le minacce informatiche.

Infezioni di ransomware e pagamenti



Mentre le aziende tedesche sono state le più propense a pagare il riscatto (81% rispetto a una media globale del 64%), le aziende del Regno Unito hanno sofferto complessivamente più degli altri 14 paesi. Non solo non sono riuscite a riottenere l'accesso ai propri dati dopo il pagamento (33% rispetto al 52%), ma nella maggior parte dei casi le loro richieste di indennizzo sono state negate (23% rispetto al 7%).

Infezioni di ransomware e pagamenti



Raccomandazioni

Date le importanti variazioni tra mercati e aziende, l'ideale è sviluppare un programma di sicurezza individuale che tenga conto delle minacce reali e dei rischi per gli utenti. Ma se non sei ancora arrivato a questo punto, il report State of The Phish di quest'anno raccomanda alcuni approcci utili.

Riduci la complessità ponendo le domande giuste.

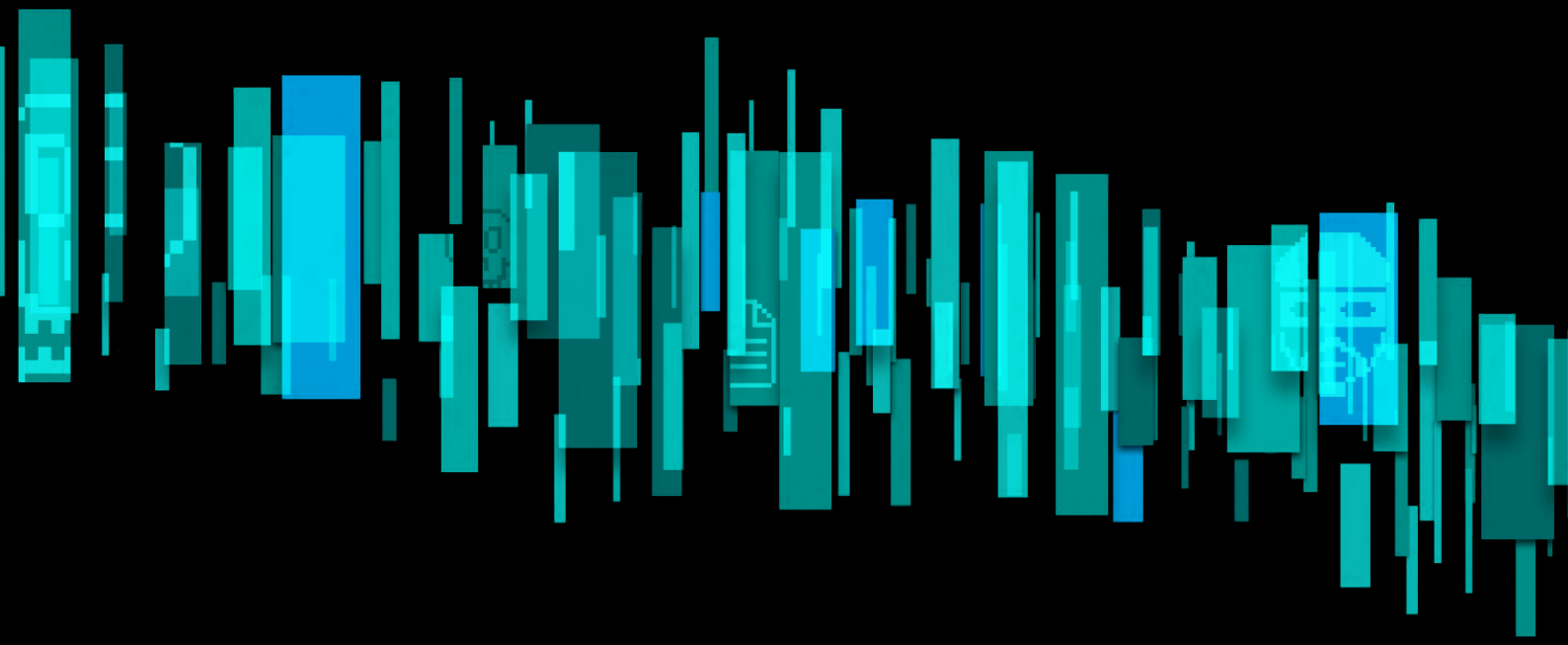
- Chi viene preso di mira dagli attacchi all'interno dell'azienda?
- Quali sono le attuali lacune nelle difese?
- Quali sono le mie priorità per limitare i rischi legati agli utenti?

Combina la threat intelligence con la formazione di sensibilizzazione alla sicurezza informatica in tutta l'azienda.

- Identifica gli utenti con le maggiori probabilità di essere attaccati e quelli che hanno la maggior probabilità di essere tratti in inganno.
- Collega i contenuti formativi con le minacce in circolazione.
- Insegna ai tuoi collaboratori a identificare il phishing utilizzando esche reali.

Crea una cultura della sicurezza informatica che vada oltre la formazione.

- La formazione è essenziale, ma non sufficiente.
- Una solida cultura della sicurezza informatica sul posto di lavoro incoraggerà gli utenti a considerare più seriamente la sicurezza delle informazioni nella loro vita personale.
- Valuta i parametri rilevanti e intraprendi azioni correttive appropriate ed eque.



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 **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 il 75% 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.

0400-013-05-01