

IL GAP DI COMPETENZE NELLA CYBERSECURITY: UNA BOMBA A OROLOGERIA



**FUTUREPROOFING
CYBERSECURITY**

INVESTING IN TODAY'S TALENT
TO SECURE TOMORROW

Il commento di Eugene Kaspersky

“Viviamo in un’era in cui le aziende del settore pubblico e privato affrontano minacce sempre più sofisticate. Imprese, Infrastrutture critiche nazionali e servizi finanziari hanno ampiamente accettato il fatto che se le organizzazioni non hanno dipendenti con le competenze necessarie per combattere i cyber criminali, combatteranno una guerra persa in partenza.

I giovani con competenze in campo tecnologico potranno colmare queste lacune se i datori di lavoro cercheranno di combattere le crescenti minacce del cyber crimine ed evitare che vengano rovinate vite pubbliche e private.

Le preoccupazioni per la carenza di competenze informatiche, unite a un profondo desiderio di affrontare il problema, hanno portato Kaspersky Lab a commissionare uno studio per cominciare a capire meglio la questione. Volevamo scoprire come i giovani vedono una possibile carriera nella cyber sicurezza e, nel caso in cui il gap di competenze continui a crescere, scoprire le potenziali implicazioni per le imprese e la società nel suo complesso.

I risultati di questo report sono sorprendenti: i giovani di oggi sono altamente competenti online. Sono particolarmente interessati agli attacchi informatici su larga scala e cercano il modo di mettere in pratica le loro competenze.

Tuttavia, lo studio indica anche che il settore della cybersecurity non riesce ad attrarre l’attenzione di questa generazione e a fornire ai giovani un percorso chiaro per trovare lavoro, affinare le competenze e servire la società. Al contrario, molti sono tentati di utilizzare le proprie competenze nel ‘lato oscuro’, impegnandosi nello sviluppo di minacce informatiche piuttosto che nella loro prevenzione.

Con l’aumento della frequenza e della notorietà dei cyber attacchi condotti da adolescenti, si dovrebbe fare di più per incoraggiare i giovani a intraprendere una carriera nella sicurezza informatica e utilizzare le proprie competenze per il bene. Abbiamo bisogno di canalizzare gli interessi della nuova generazione verso la giusta direzione, prima che sia troppo tardi e che il gap di competenze diventi ancora più ampio”



**FUTUREPROOFING
CYBERSECURITY**

RISULTATI PRINCIPALI

Uno su quattro (27%) ha preso in considerazione una carriera nella cybersecurity, considerata da molti (47%) un buon uso del proprio talento. Altri invece hanno ammesso di essere inclini a prendere parte ad attività più discutibili, come l'utilizzo delle proprie competenze per divertimento (17%), attività segrete (16%) e profitti finanziari (11%)

Il 23% delle persone sotto i 18 anni conosce qualcuno impegnato in attività informatiche probabilmente illegali (come l'hacking)

Più della metà delle persone sotto i 25 anni (57%) considera l'hacking una competenza "notevole"

Tre aziende su quattro (73%) hanno affermato che è difficile trovare sufficienti professionisti nel settore della sicurezza IT

L'87% delle aziende ritiene che sia importante che i giovani si uniscano alla guerra per la sicurezza informatica



Introduzione

Le organizzazioni si stanno rendendo conto che non è una questione di **se** un attacco informatico accadrà, ma di **quando**. Questo ha portato i dirigenti a interessarsi maggiormente a ciò che viene fatto per proteggere le loro organizzazioni e, di conseguenza, supportare lo sviluppo della sicurezza informatica. Il problema sta nel fatto che il pool di talenti nella cybersecurity non sta crescendo allo stesso modo.

Si prevede che la domanda globale di esperti di sicurezza informatica supererà l'offerta di un terzo prima della fine del decennio. La recente Global Workforce Survey condotta da Frost & Sullivan ha previsto, sulla base delle tendenze attuali, una carenza di 1,5 milioni di professionisti della sicurezza informatica entro il 2020. Le priorità devono quindi spostarsi rapidamente eliminando, prima che sia troppo tardi, questo gap di competenze nella cybersecurity.

Il settore sta facendo tutto il possibile per incoraggiare di più i giovani a intraprendere una carriera nella cybersecurity? I datori di lavoro dovrebbero fare di più per riuscire a canalizzare gli interessi e il talento dei giovani verso questo settore? O forse gli istituti di istruzione dovrebbero preparare al meglio gli studenti con competenze informatiche più avanzate?

Per scoprirlo, Kaspersky Lab ha condotto uno studio su oltre 12.000 consumatori e professionisti IT negli Stati Uniti e in Europa (Regno Unito, Germania, Francia, Italia, Spagna e Paesi Bassi)¹. L'obiettivo era scoprire come eliminare questo crescente gap di competenze e chi abbia il compito di farlo.

I risultati mostrano che, se vogliamo avvicinare i giovani a una carriera nella cybersecurity, il gap di competenze dovrà essere eliminato con un'azione combinata del settore e degli istituti di istruzione.

Questa generazione è più vicina alla tecnologia delle precedenti e il pericolo sta nel fatto che, se il talento tecnologico non viene canalizzato correttamente, i giovani potrebbero essere tentati di utilizzare le proprie competenze per intenti criminali. I giovani dovrebbero essere maggiormente informati delle opportunità di carriera che esistono nella cybersecurity e incoraggiati a sviluppare le proprie capacità per il bene della società. Attraverso una combinazione di istruzione e apprendimento sul posto di lavoro, è necessario coltivare e invogliare i giovani talenti alla professione prima che il gap si allarghi ulteriormente.

Si prevede che la domanda globale di esperti di sicurezza informatica supererà l'offerta di un terzo prima della fine del decennio...



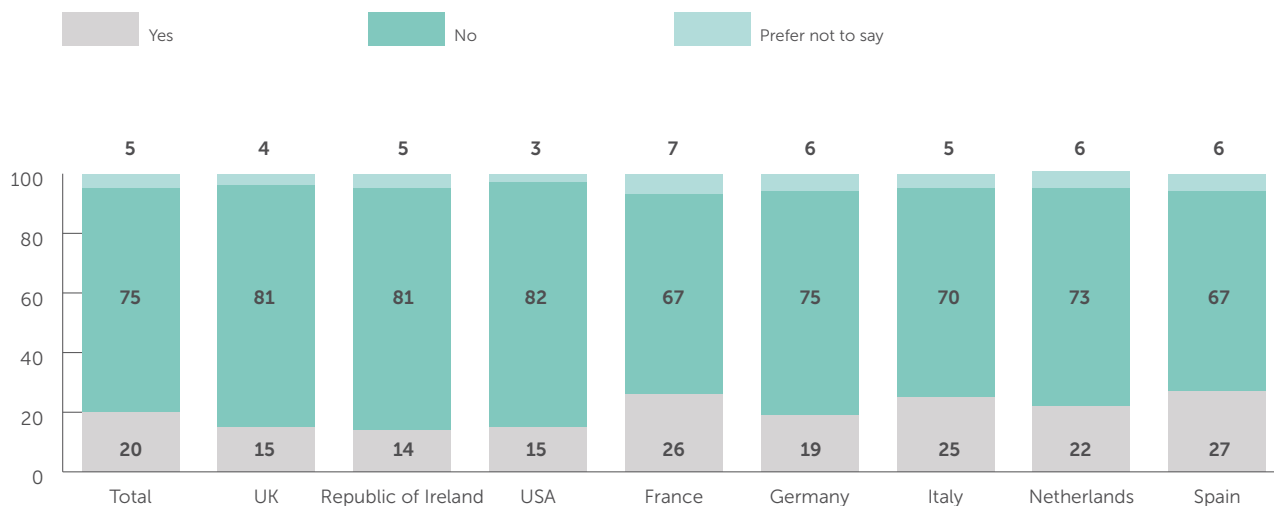
I risultati della ricerca

I giovani vengono tentati di intensificare il cyber crimine, anziché prevenirlo

I giovani di oggi sono altamente qualificati, ma anche altamente influenzabili sulla via da intraprendere nella vita, che si tratti della scelta del percorso di studi, di andare via di casa o di iniziare un nuovo lavoro. Essendo nativi digitali, sono completamente immersi nel mondo digitale e sono affascinati dagli attacchi informatici su larga scala.

Abbiamo scoperto che il 23% delle persone sotto i 18 anni conosce qualcuno impegnato in attività informatiche probabilmente illegali (ad esempio l'hacking). Queste attività sono più prevalenti tra i giovani universitari (24%) e tra quelli che hanno appena terminato gli studi e sono impiegati (23%) rispetto ai giovani disoccupati: solo il 15% di questi conosce qualcuno impegnato in attività informatiche che potrebbero essere illegali.

Conosci qualcuno impegnato in attività (come l'hacking) che potrebbero essere illegali?



La loro preoccupazione supera solo in maniera marginale la loro curiosità – e persino la loro stima – per queste tipologie di crimine. Poco meno della metà delle persone di età inferiore ai 25 anni (47%) è “colpita” dalla notizia di una società hackerata e un terzo (33%) si interessa al modo in cui è stato eseguito l’attacco. Abbiamo inoltre scoperto che la preoccupazione aumenta con l’età. Il 40% delle persone di età compresa tra i 21 e i 25 anni ha dichiarato di essere preoccupato dalla consistenza del danno inflitto e dalla risposta della società, contro il 36% delle persone di 16 anni.

Un dato allarmante è che più della metà delle persone sotto i 25 anni di età (57%) considera l’hacking una competenza “notevole”. Un numero significativo, invece, userebbe le proprie competenze per divertimento (17%), attività segrete (16%) e profitti finanziari (11%).

Molti sono già in grado di confondere le informazioni, con un terzo delle persone di età inferiore ai 25 anni (31%), ad esempio, capace di nascondere il proprio indirizzo IP. Con solo il 50% che parteciperebbe alla lotta contro il cyber crimine, risulta evidente una mancanza di impegno nei giovani nell’utilizzare le proprie competenze informatiche per combattere il crimine.

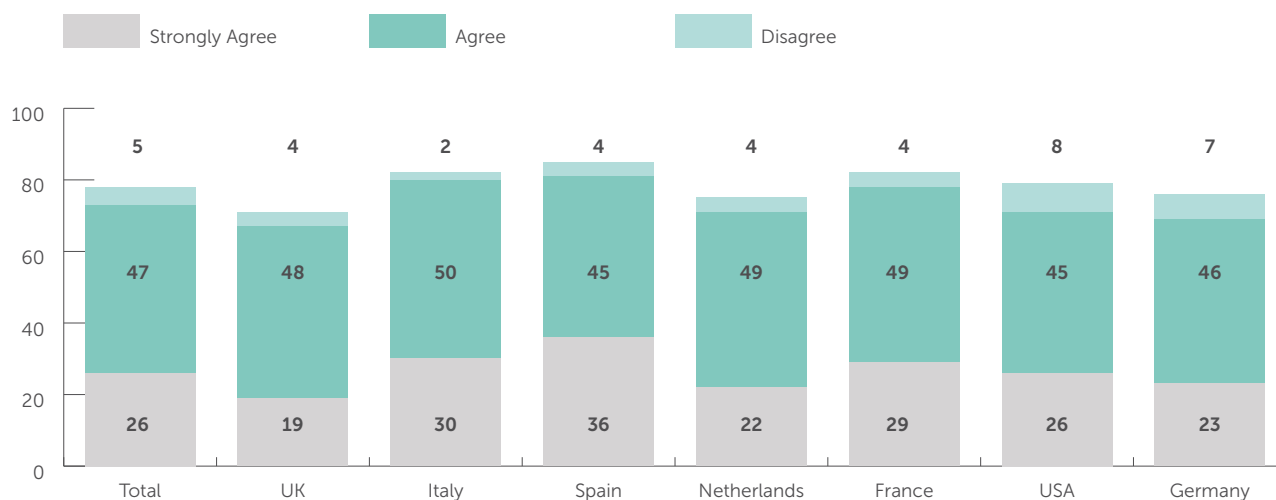
Le aziende hanno bisogno che i giovani aiutino a combattere il cyber crimine

Con l'emergere di un gap di competenze informatiche sempre più ampio, i giovani appassionati di informatica sono la chiave per la creazione di nuovi ruoli lavorativi sul fronte della cybersecurity. Questo gruppo ha le conoscenze di base e la voglia di imparare, ma i datori di lavoro non riescono a canalizzare l'interesse e il talento dei giovani verso questo settore.

Un numero enorme di professionisti del settore (93%) riconosce che la professione ha bisogno di evolversi insieme al panorama attuale e futuro e l'87% ritiene che sia importante che i giovani si uniscano alla guerra per la sicurezza informatica.

Il problema sta nel fatto che molti datori di lavoro non offrono ruoli entry-level nel campo della sicurezza informatica; la maggior parte (72%) promuove personale interno fornendo formazione se necessario e reclutando esternamente (53%) i professionisti senior della sicurezza.

Quanto sei d'accordo con l'affermazione: "È difficile trovare sufficienti professionisti di sicurezza IT da assumere"?



È importante riconoscere che, come per ogni disciplina all'interno del settore IT, le competenze sulla sicurezza si sviluppano nel corso del tempo, proprio come con le altre professioni. Le posizioni, infatti, vengono assegnate in maniera coerente al proprio livello di abilità, poi si impara e si riceve una formazione adeguata sul posto di lavoro. Ma con quasi tre quarti delle aziende (73%) con difficoltà nel reclutamento di professionisti IT opportunamente qualificati, è forse il momento di ripensare i percorsi tradizionali nella professione della sicurezza informatica?

RISULTATI PRINCIPALI

Un numero enorme di professionisti del settore (93%) riconosce che la professione ha bisogno di evolversi insieme al panorama attuale e futuro

93%

L'87% ritiene che sia importante che i giovani si uniscano alla guerra per la sicurezza informatica

87%

Il problema sta nel fatto che molti datori di lavoro non offrono ruoli entry-level nel campo della sicurezza informatica; la maggior parte (72%) promuove personale interno fornendo formazione se necessario

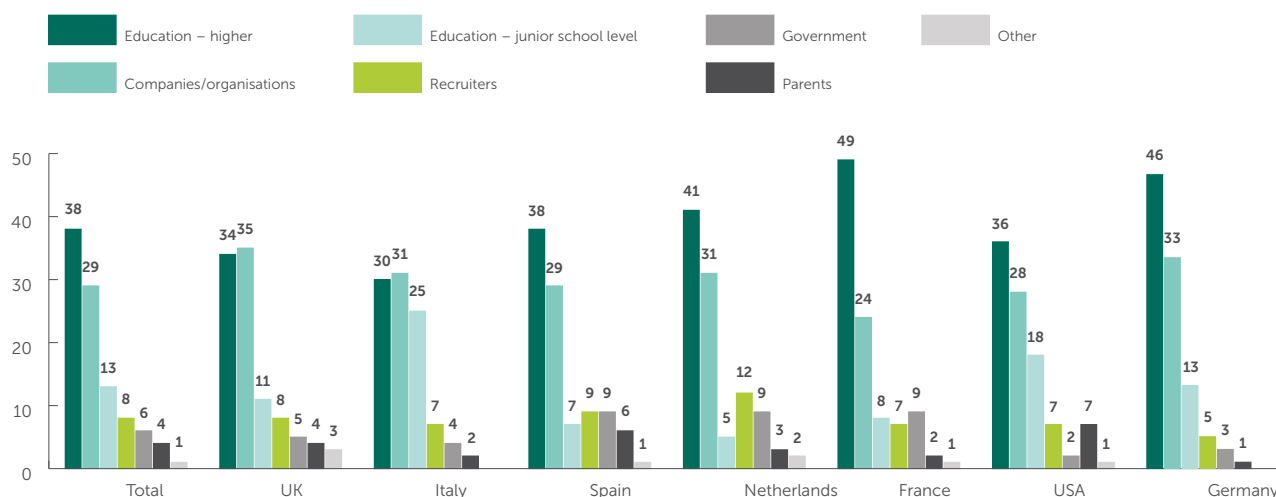
72%

La responsabilità è dei datori di lavoro o di chi forma i giovani?

La questione sul chi sia responsabile del reclutamento della prossima generazione di difensori informatici è importante in quanto appare evidente la portata della sfida. Abbiamo bisogno di un piano che si basi sugli interessi più evidenti, prima che le menti brillanti e curiose utilizzino le proprie competenze per un profitto criminale e voltino quindi le spalle alla sicurezza.

Secondo il settore IT, il sistema di istruzione ha un ruolo chiave da svolgere per incoraggiare i giovani talenti alla professione e per fornir loro i livelli di competenza necessari. La nostra ricerca ha rilevato che quasi due terzi dei professionisti IT (62%) ritiene che la preparazione delle future generazioni di professionisti nella cyber sicurezza sia una responsabilità degli istituti di istruzione. Anche il settore IT ha un ruolo fondamentale nella protezione del proprio futuro, con il 27% che attribuisce la responsabilità principale alle società.

Di chi dovrebbe essere la responsabilità di incoraggiare i giovani talenti alla professione?



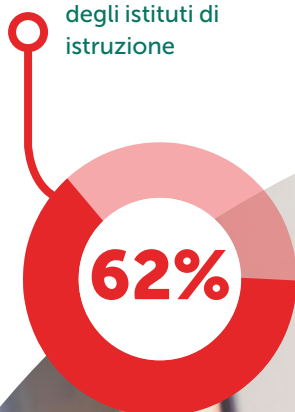
È interessante notare come la ricerca abbia rilevato significative differenze regionali alla domanda se l'educazione o il lavoro avesse il compito di incoraggiare i giovani a entrare nel settore. Le aziende sono considerate maggiormente responsabili nel Regno Unito, con più di un terzo dei datori di lavoro (35%) che afferma che si dovrebbe fare di più per aiutare i giovani a ricoprire ruoli nella sicurezza informatica. Al contrario, in Italia (25%) e negli Stati Uniti (18%) si attribuisce maggiore importanza al ruolo dell'educazione elementare, rispetto a una media del 13%.

Per quanto riguarda chi dovrebbe fornire le giuste competenze ai giovani, nel complesso si punta sull'istruzione superiore (49%), sulle società e sulle organizzazioni (27%). Ma, ancora una volta, ci troviamo di fronte a differenze geografiche, ad esempio, con più aspettative riposte nei datori di lavoro nei Paesi Bassi (40%).

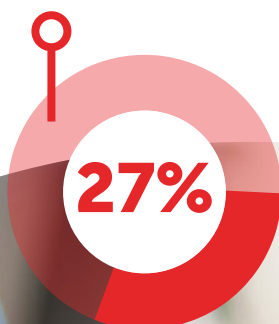
Chiaramente, le differenze sono legate ai diversi sistemi educativi e alle priorità del governo ma, in realtà, abbiamo bisogno di un approccio integrato tra datori di lavoro e istruzione per fornire e sviluppare le competenze di una generazione affamata di tecnologia.

RISULTATI PRINCIPALI

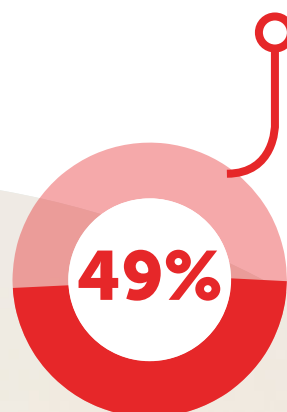
La nostra ricerca ha rilevato che quasi due terzi dei professionisti IT (62%) ritiene che la preparazione delle future generazioni di professionisti nella cyber sicurezza sia una responsabilità degli istituti di istruzione



Anche il settore IT ha un ruolo fondamentale nella protezione del proprio futuro, con il 27% che attribuisce la responsabilità principale alle società



Per quanto riguarda chi dovrebbe fornire le giuste competenze ai giovani, nel complesso si punta sull'istruzione superiore (49%)



Garantire il futuro del settore della sicurezza

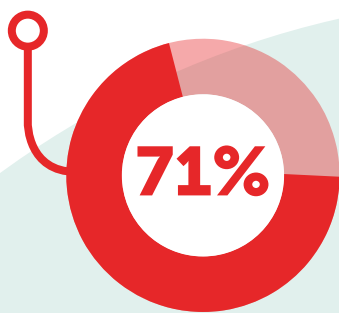
Molto resta da fare per nutrire e attrarre giovani talenti all'interno del settore, perché il crescente gap di competenze nella cyber sicurezza è una bomba a orologeria in attesa di esplodere.

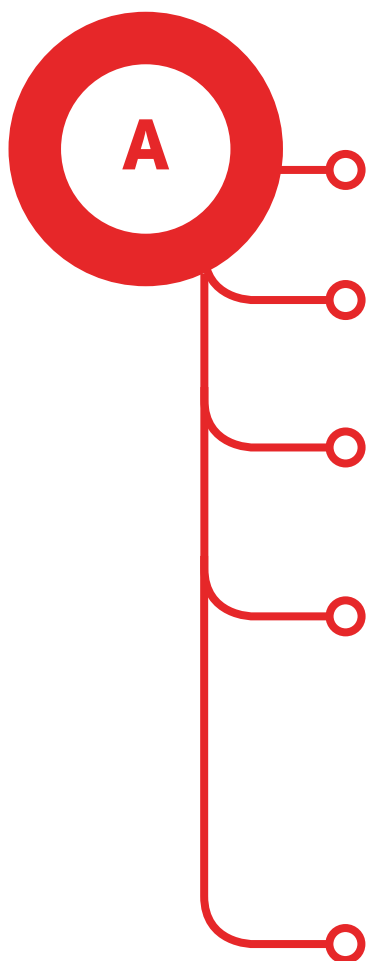
Dobbiamo rendere più facile e attraente agli occhi dei giovani qualificati un possibile futuro in questo settore. Abbiamo scoperto che quasi tre quarti dei giovani (71%) non sono a conoscenza di eventuali stage o opportunità per i laureati in sicurezza IT.

Sebbene le aziende sostengano che le nuove leve non hanno competenze pratiche di cybersecurity o l'esperienza necessaria, pochissimi attualmente offrono ruoli di base o stage che possono aiutare nello sviluppo del talento. Infatti, solo il 45% offre ruoli entry-level o percorsi di formazione.

Tre su dieci (30%) ammettono di non avere le risorse interne per istruire i laureati al ruolo di responsabili alla cybersecurity. E un dato allarmante è che solo un intervistato su cinque (20%) ritiene che un team dedicato alla sicurezza informatica sarà responsabile della sicurezza IT entro cinque anni, con la metà (50%) che crede che la responsabilità di affrontare il cyber crimine ricadrà sul team IT.

Abbiamo scoperto che quasi tre quarti dei giovani (71%) non sono a conoscenza di eventuali stage o opportunità per i laureati in sicurezza IT





Qual è la risposta?

Secondo Kaspersky Lab, questo report è l'inizio di un lungo viaggio verso l'eliminazione delle lacune in questo settore. Risolvere un problema di questa portata richiede sforzi coordinati tra aziende del settore, istruzione e governo.

Riteniamo che si dovrebbe fare di più per far sì che i datori di lavoro incoraggino i giovani a una carriera nella cybersecurity. Anche tra i professionisti della sicurezza IT, il 27% ammette che le organizzazioni debbano fare di più per offrire programmi di formazione e di specializzazione.

Le iniziative guidate dal settore possono aiutare a promuovere le carriere nella sicurezza informatica. Concorsi internazionali per studenti universitari e giovani professionisti, ad esempio, incoraggiano i giovani talenti ad utilizzare le proprie competenze per affrontare varie sfide di sicurezza informatica, dando loro un assaggio di come potrebbero essere utili per il settore e per la società in generale.

Lavorando a stretto contatto con le università, il nostro settore può essere determinante nello sviluppo del talento e nell'assicurarsi che gli insegnamenti teorici e pratici siano all'altezza delle aspettative e delle esigenze future. Dando consulenza sul materiale didattico, tenendo lezioni, mostrando le tecnologie e collaborando alla ricerca, il settore può contribuire a entusiasmare, coinvolgere e soprattutto illuminare e formare la prossima generazione di difensori informatici. Offrendo tirocini, stage e posizioni post-laurea sarà possibile rafforzare il rapporto tra settore e istruzione, facendo sì che preziose competenze non vadano perse quando più servono.

I risultati di questo report illustrano la portata della sfida che il settore deve affrontare, ma evidenziano anche alcune aree in cui può esserci progresso. Dobbiamo attuare questa procedura per disinnescare la bomba a orologeria di sicurezza informatica prima che sia troppo tardi.



-
- 1 Note sulla ricerca: Kaspersky Lab ha commissionato ad Arlington Research un'indagine su 2.120 professionisti IT in Regno Unito, Italia, Spagna, Paesi Bassi, Francia, Germania e Stati Uniti. Inoltre, Kaspersky Lab ha commissionato ad Arlington Research un'indagine su 11.531 giovani utenti, di età compresa tra i 16 e i 25 anni in Regno Unito, Irlanda, Stati Uniti, Francia, Germania, Italia, Paesi Bassi e Spagna. Entrambe le ricerche sono state concluse a luglio 2016.
-

KASPERSKY LAB

www.kaspersky.it



**FUTUREPROOFING
CYBERSECURITY**

INVESTING IN TODAY'S TALENT
TO SECURE TOMORROW