KASPERSKY lab

QUALIFIKATIONSDEFIZIT IN DER CYBERSICHERHEIT – EINE TICKENDE ZEITBOMBE

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW

Gedanken zu diesem Thema von Eugene Kaspersky

„Wir leben in einem Zeitalter, in dem der geschäftliche und der öffentliche Sektor mit immer raffinierteren Sicherheitsbedrohungen zu kämpfen haben. In allen diesen Bereichen, von Unternehmen bis hin zu wichtigen öffentlichen Infrastrukturbetreibern und Finanzdienstleistern, wird allgemein anerkannt, dass nicht genügend Mitarbeiter mit den erforderlichen Qualifikationen vorhanden sind, um der Cyberkriminalität Einhalt zu gebieten.

Während sich Arbeitgeber bemühen, die immer größere Bedrohung durch Cyberkriminalität zu bekämpfen, um massive Störungen des öffentlichen und privaten Lebens abzuwenden, könnten technisch versierte junge Leute das immer größer werdende Qualifikationsdefizit wettmachen.

Kaspersky Lab hat sich die Aufgabe gesetzt, zur Lösung dieses Problems beizutragen. Dafür haben wir unter anderem eine Studie in Auftrag gegeben, um die Gründe für diesen Fachkräftemangel genauer zu beleuchten. Wir wollten einerseits herausfinden, inwieweit junge Leute Cybersicherheit als Berufsoption sehen, und andererseits die potenziellen wirtschaftlichen und sozialen Auswirkungen eines auch in Zukunft wachsenden Fachkräftemangels untersuchen.

Die Ergebnisse des Berichts sind äußerst bemerkenswert. Es zeigt sich, dass die heutige junge Generation online hochgradig kompetent ist. Sie legt gegenüber Cyber-Hackern eine gewisse Neugier an den Tag und will Möglichkeiten finden, ihre Fähigkeiten zu nutzen.

Die Studie weist aber auch darauf hin, dass die Cybersicherheitsbranche dagegen nicht wirklich in der Lage ist, diese Generation anzusprechen und ihr einen klaren Weg aufzuzeigen, Arbeitsplätze zu finden, die eigenen Fähigkeiten zu erweitern und der Gesellschaft nützliche Dienste zu erweisen. Stattdessen werden viele eher in Versuchung geführt, ihr Können auf der „Dunklen Seite“ einzusetzen, Cyberkriminalität also nicht zu verhindern, sondern zu initiieren.

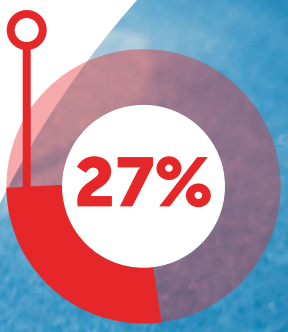
Da immer häufiger durch Teenager durchgeführte Cyberattacken bekannt werden, muss mehr getan werden, um Berufe im Bereich Cybersicherheit für junge Leute attraktiv zu machen und ihre Fähigkeiten zum Guten zu nutzen. Wir müssen die Interessen und Talente dieser neuen Generation in die richtige Richtung leiten, bevor es zu spät ist und der Mangel an qualifizierten Fachkräften noch ausgeprägter wird.“

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

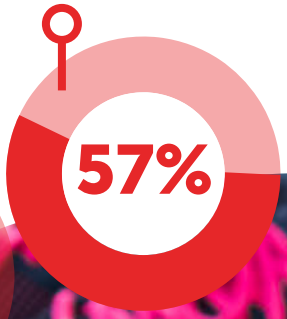
WICHTIGSTE ERKENNTNISSE

Etwa ein Viertel (27 Prozent) hat eine Karriere im Bereich Cybersicherheit in Betracht gezogen, wobei viele Befragte (47 Prozent) dies als gute Möglichkeit sehen, ihr Talent einzusetzen. Andere geben aber zu, sich lieber mit eher fragwürdigen Aktivitäten zu beschäftigen und ihre Fähigkeiten aus Spaß (17 Prozent), für geheime Aktivitäten (16 Prozent) und zur finanziellen Bereicherung (11 Prozent) zu nutzen.



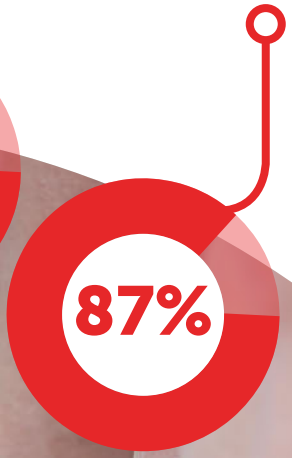
23 Prozent der 18-Jährigen kennen jemanden, der sich mit Cyberaktivitäten (also Hacking) befasst, die möglicherweise illegal sind.

Für mehr als die Hälfte (57 Prozent) der Personen unter 25 Jahren ist Hacking eine „beeindruckende" Fähigkeit.



Drei Viertel (73 Prozent) der befragten Unternehmen stimmten zu, dass es schwierig ist, genügend IT-Sicherheitsexperten zu finden.

87 Prozent der Unternehmen glauben, dass es wichtig ist, dass junge Menschen dem Cyber-Sicherheitskrieg beitreten.



Einleitung

Unternehmen sind sich bewusst, dass es nicht darum geht, ob sie zukünftig einem Cyberangriff ausgesetzt sein werden, sondern wann. Daher sorgen sich Führungskräfte zunehmend darum, was zum Schutz ihrer Organisation getan wird, und ob Cybersicherheit inzwischen ein anerkannter Wachstumsbereich in den Unternehmen ist. Ein Problem liegt dabei in dem Umstand, dass der Pool qualifizierter Fachkräfte in diesem Bereich nicht mit den Anforderungen der Unternehmen Schritt halten kann.

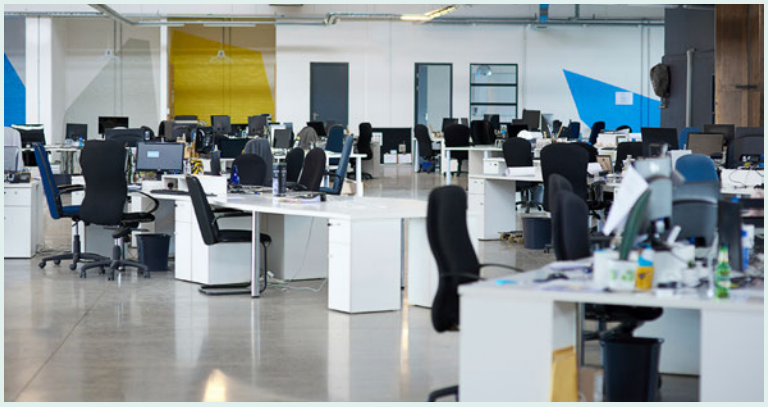
Laut Prognosen wird die weltweite Nachfrage nach Cybersicherheitsexperten das Angebot bis zum Ende des Jahrzehnts um ein Drittel übersteigen. Die neueste Global-Workforce-Umfrage von Frost and Sullivan prognostiziert, dass nach aktuellen Trends bis ins Jahr 2020 im Bereich Sicherheit ein Defizit von 1,5 Millionen Fachkräften bestehen wird. Es müssen dringend neue Prioritäten gesetzt werden, um den Fachkräftemangel zu beheben, bevor es zu spät ist.

Die weltweite Nachfrage nach Cybersicherheitsexperten wird voraussichtlich das Personalangebot bis zum Ende des Jahrzehnts um ein Drittel übersteigen...

Tut die Branche genug, um Berufe im Bereich Cybersicherheit für junge Leute attraktiv zu machen? Sollten sich Arbeitgeber mehr engagieren, um die Interessen und Talente der jungen Generation auf diesem Gebiet in die richtige Richtung zu leiten? Oder liegt es eher an den Bildungseinrichtungen, Studenten besser auf den digitalen Arbeitsmarkt vorzubereiten?

Um dies näher zu beleuchten, hat Kaspersky Lab eine Studie[1] unter fast 12.000 Anwendern und IT-Fachleute in den USA und Europa (Großbritannien, Deutschland, Frankreich, Italien, Spanien und den Niederlanden) durchgeführt. Wir wollten herausfinden, wie sich das wachsende Qualifikationsdefizit beheben lässt und wer die Verantwortung für die Behebung übernehmen soll.

Die Ergebnisse zeigen, dass der Fachkräftemangel nur durch gemeinsame Anstrengungen der Branche und der Bildungseinrichtungen behoben werden kann, wenn wir Berufe im Bereich Cybersicherheit für junge Leute attraktiv machen wollen. Diese Generation ist mehr mit Technologie vertraut als jede andere. Wenn dieses Talent nicht in die richtige Richtung geleitet wird, besteht die Gefahr, dass begabte junge Leute in Versuchung geraten, es eher für kriminelle Zwecke einzusetzen. Die junge Generation muss besser über die beruflichen Chancen im Bereich Cybersicherheit informiert und ermutigt werden, ihre Fähigkeiten zum Nutzen der Gesellschaft einzusetzen. Durch eine Kombination aus theoretischem und praktischem Lernen (also in Lehreinrichtungen und im Beruf) können wir dieses Talent fördern und mehr jungen Leuten Anreize für diese Berufe bieten, bevor das Qualifikationsdefizit noch ausgeprägter wird.



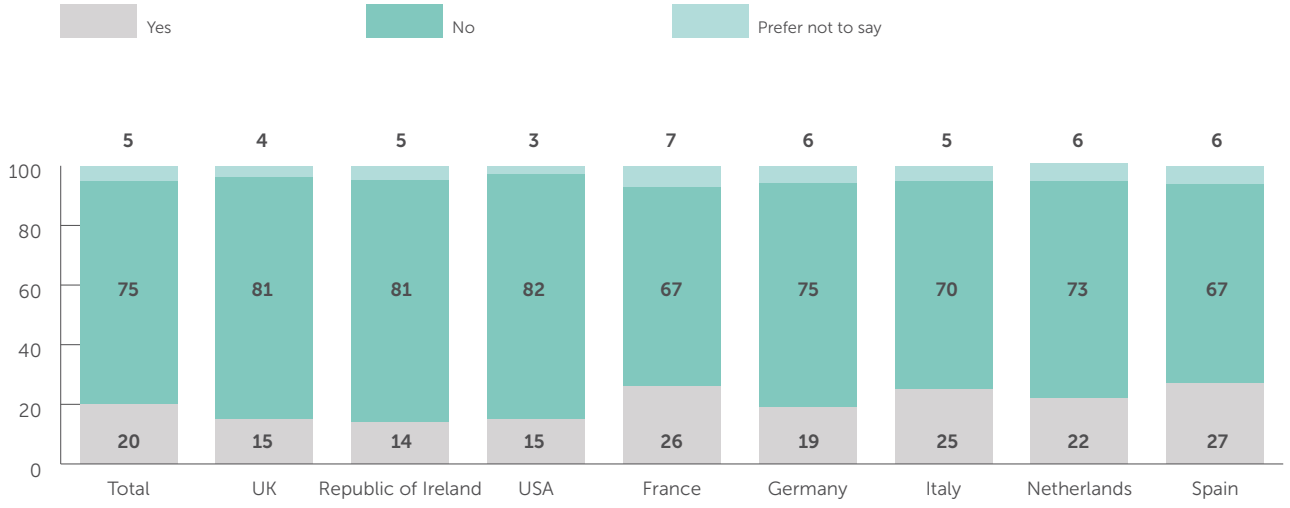
Ergebnisse der Studie

Junge Leute werden in Versuchung geführt, die Cyberkriminalität zu verschlimmern, statt sie zu verhindern

Die heutigen jungen Leute sind äußerst talentiert, aber auch sehr leicht zu beeinflussen. Oft beginnen sie gerade ein neues Kapitel in ihrem Leben – sie fangen an zu studieren, ziehen von zu Hause aus oder starten einen neuen Job. Sie sind mit der digitalen Welt aufgewachsen und gehen voll und ganz in ihr auf. Gleichzeitig sind sie aber bereits an großflächige Cyberangriffe gewöhnt.

Wir stellten fest, dass 23 Prozent der 18-Jährigen jemanden kennen, der sich mit Cyberaktivitäten (zum Beispiel Hacking) befasst, die möglicherweise illegal sind. Solche Aktivitäten zeigen sich stärker bei Studenten (24 Prozent) und denen, die bereits einen Abschluss haben und berufstätig sind (23 Prozent). Im Vergleich dazu kennen nur 15 Prozent der arbeitslosen Schulabgänger jemanden, der sich mit möglicherweise illegalen Cyberaktivitäten beschäftigt.

Kennen Sie jemanden, von dem Sie wissen, dass sich diese Person mit illegalen Cyberaktivitäten (z.B. Hacking) befasst?



Ihre Bedenken sind nur geringfügig höher als ihre Neugier, und sie hegen sogar eine gewisse Anerkennung für diese Art von Kriminalität. Fast die Hälfte (47 Prozent) der jungen Leute unter 25 ist „beeindruckt", wenn sie hört, dass Hacker ein Unternehmen angegriffen haben, und ein Drittel (33 Prozent) interessiert sich dafür, wie dies im Einzelnen vor sich ging. Weiterhin haben wir festgestellt, dass die Bedenken zur Cyberkriminalität mit steigendem Alter zunehmen. 40 Prozent der jungen Leute im Alter von 21 bis 25 Jahren gaben an, dass sie sich Sorgen um die möglichen Auswirkungen machen und wie das betroffene Unternehmen wohl reagieren wird. Unter den 16-Jährigen Umfrageteilnehmern waren es lediglich 36 Prozent.

Es ist erschreckend, dass Hacking für mehr als die Hälfte (57 Prozent) der Personen unter 25 Jahren eine „beeindruckende" Fähigkeit ist. Eine erhebliche Anzahl würde ihre Fähigkeiten aus Spaß (17 Prozent), für geheime Aktivitäten (16 Prozent) und zur finanziellen Bereicherung (11 Prozent) nutzen.

Viele von ihnen sind schon ziemlich versiert darin, die Grenzen zu verwischen. Beispielsweise ist ein Drittel der Personen unter 25 (31 Prozent) in der Lage, die eigene IP-Adresse zu verbergen. Und da sich nur die Hälfte (50 Prozent) dieser Personen am Kampf gegen die Cyberkriminalität beteiligen würde, sind junge Leute offensichtlich nicht genügend an diesem Bereich interessiert.

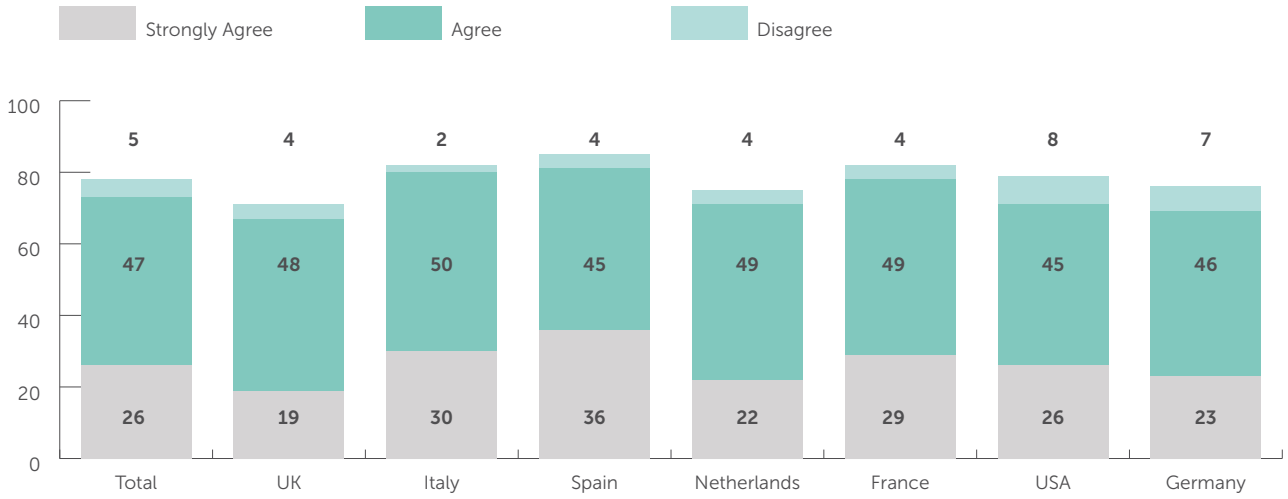
Unternehmen brauchen junge Leute im Kampf gegen die Cyberkriminalität

Das Qualifikationsdefizit im Bereich Cybersicherheit wird immer größer. Daher müssen junge IT-Enthusiasten eingestellt werden, um neu zu schaffende Positionen zu übernehmen. Diese Personengruppe verfügt über das grundlegende Wissen und den erforderlichen Wissensdurst, aber viele Arbeitgeber lenken die Interessen und Talente dieser jungen Leute nicht in die richtige Richtung.

Die überwältigende Mehrheit der Branchenexperten (93 Prozent) erkennt, dass die Branche sich im Hinblick auf die aktuelle und die zukünftige Bedrohungslandschaft weiterentwickeln muss, und 87 Prozent glauben, dass es wichtig ist, dass junge Menschen dem Cyber-Sicherheitskrieg beitreten.

Die Herausforderungen liegen darin, dass es in vielen Unternehmen keine Stellen für Berufsanfänger im Bereich Cybersicherheit gibt, dass die Unternehmen die meisten Beförderungen nur intern vornehmen (72 Prozent), dass interne Schulungen nur nach Bedarf angeboten werden, und dass bei Neueinstellungen in der Regel nach erfahrenen Sicherheitsexperten extern gesucht wird (53 Prozent).

Dans quelle mesure êtes-vous d'accord avec l'affirmation suivante : « Il est difficile de trouver suffisamment de professionnels en sécurité IT à recruter » ?



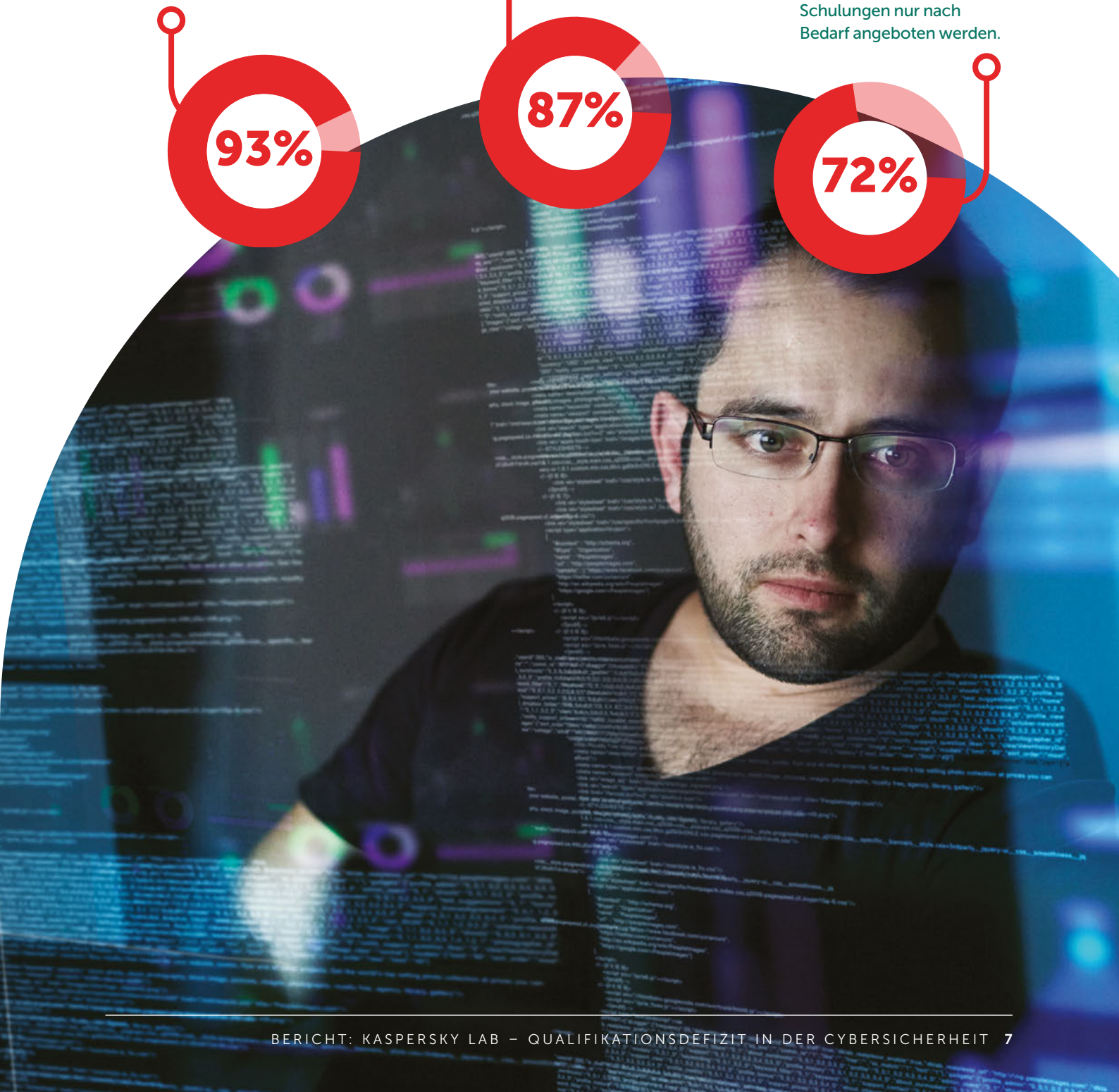
Wie bei jeder Fachrichtung im IT-Bereich entwickeln sich die Sicherheitskenntnisse immer über einen gewissen Zeitraum hinweg. Mitarbeiter steigen in einer Position ein, die ihren Fähigkeiten entspricht, lernen dann in der Praxis und durchlaufen entsprechende Schulungen. Da aber fast drei Viertel (73 Prozent) der Unternehmen Schwierigkeiten haben, ausreichend qualifizierte IT-Fachkräfte einzustellen, ist es vielleicht an der Zeit, die herkömmlichen beruflichen Einstiegsmöglichkeiten in die Cybersicherheit zu überdenken.

WICHTIGSTE ERKENNTNISSE

Die überwältigende Mehrheit der Branchenexperten (93 Prozent) erkennt, dass die Branche sich im Hinblick auf die aktuelle und die zukünftige Bedrohungslandschaft weiterentwickeln muss.

87 Prozent der Unternehmen glauben, dass es wichtig ist, dass junge Menschen dem Cyber-Sicherheitskrieg beitreten.

Die Herausforderungen liegen darin, dass es in vielen Unternehmen keine Stellen für Berufsanfänger im Bereich Cybersicherheit gibt, dass die Unternehmen die meisten Beförderungen nur intern vornehmen (72 Prozent), und dass interne Schulungen nur nach Bedarf angeboten werden.

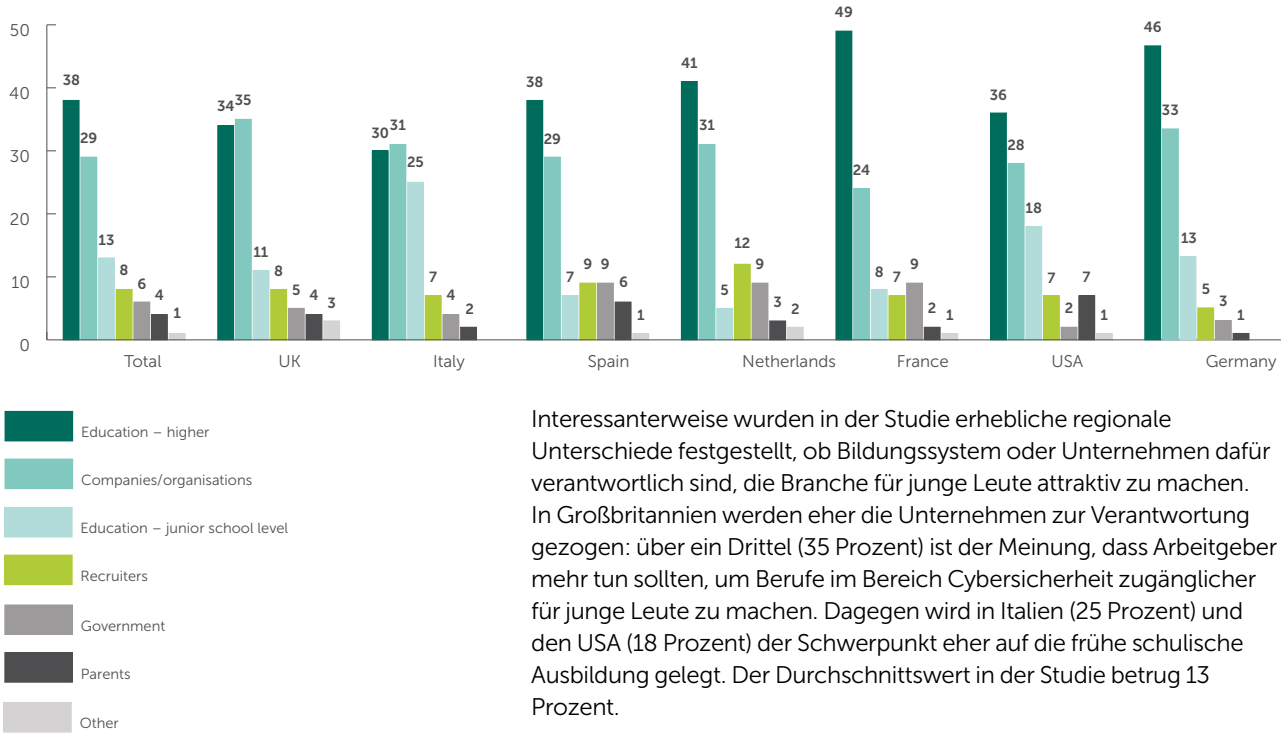


Arbeitgeber oder Bildungssystem – wo liegt die Verantwortung?

Es ist eine wichtige Frage, wer für die Einbindung der nächsten Generation in den Kampf gegen die Cyberkriminalität verantwortlich ist, denn die Herausforderung ist groß. Wir brauchen einen Plan, der die offensichtlichen Interessen junger Leute berücksichtigt, bevor sich intelligente und wissbegierige Menschen von der Cybersicherheit abwenden und sich mithilfe ihrer Fähigkeiten kriminell bereichern.

Nach Ansicht der IT-Branche spielt das Bildungssystem eine entscheidende Rolle dabei, diese jungen Talente in entsprechende Berufe zu bringen und ihnen die erforderlichen Qualifikationen an die Hand zu geben. Unsere Studie ergab, dass fast zwei Drittel der IT-Fachleute (62 Prozent) der Meinung sind, dass es in erster Linie in der Verantwortung der Bildungseinrichtungen liegt, zukünftige Generationen von Cybersicherheitsexperten auf ihre Aufgaben vorzubereiten. Die Branche spielt natürlich auch eine klare Rolle beim Schutz ihrer eigenen Zukunft, so dass 27 Prozent der Befragten die Verantwortung eher bei den Unternehmen sehen.

Wer sollte für die Förderung junger Talente in den Beruf hauptverantwortlich sein?



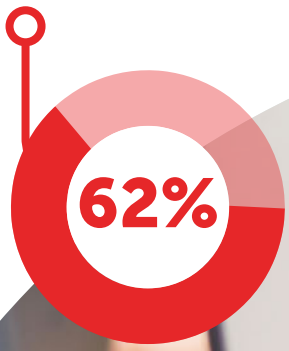
Interessanterweise wurden in der Studie erhebliche regionale Unterschiede festgestellt, ob Bildungssystem oder Unternehmen dafür verantwortlich sind, die Branche für junge Leute attraktiv zu machen. In Großbritannien werden eher die Unternehmen zur Verantwortung gezogen: über ein Drittel (35 Prozent) ist der Meinung, dass Arbeitgeber mehr tun sollten, um Berufe im Bereich Cybersicherheit zugänglicher für junge Leute zu machen. Dagegen wird in Italien (25 Prozent) und den USA (18 Prozent) der Schwerpunkt eher auf die frühe schulische Ausbildung gelegt. Der Durchschnittswert in der Studie betrug 13 Prozent.

Wenn es darum geht, dafür zu sorgen, dass junge Leute über die richtigen Qualifikationen verfügen, so wird die Verantwortung allgemein den höheren Bildungseinrichtungen (49 Prozent) sowie Unternehmen und Organisationen (27 Prozent) zugeschrieben. Wiederum zeichnen sich aber regionale Unterschiede ab. Beispielsweise liegen in den Niederlanden die Erwartungen an die Arbeitgeber höher (40 Prozent).

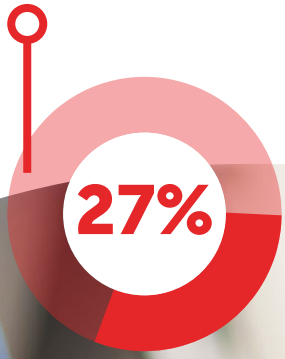
Natürlich begründen sich diese Unterschiede teilweise in den verschiedenen Bildungssystemen und länderspezifischen Prioritäten. Aber wir brauchen auf jeden Fall einen ganzheitlichen Ansatz bei Arbeitgebern und im Bildungswesen, um eine wissbegierige Tech-Generation mit den notwendigen Fähigkeiten auszustatten und diese weiterzuentwickeln.

WICHTIGSTE ERKENNTNISSE

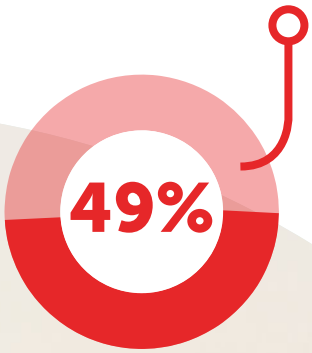
Unsere Studie ergab, dass fast zwei Drittel der IT-Fachleute (62 Prozent) der Meinung sind, dass es in erster Linie in der Verantwortung der Bildungseinrichtungen liegt, zukünftige Generationen von Cybersicherheitsexperten auf ihre Aufgaben vorzubereiten.



Die Industrie hat auch eine eindeutige Rolle, ihre eigene Zukunft zu schützen. 27 Prozent der Befragten sehen die Hauptverantwortung in den Unternehmen.



Wenn es darum geht, dafür zu sorgen, dass junge Leute über die richtigen Qualifikationen verfügen, so wird die Verantwortung allgemein den höheren Bildungseinrichtungen (49 Prozent) zugeschrieben.



Die Zukunft der Sicherheitsbranche sichern

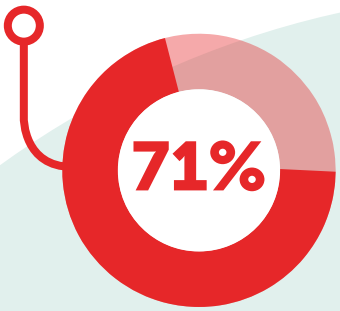
Da der zunehmende Fachkräftemangel im Bereich Cybersicherheit eine Zeitbombe ist, muss mehr getan werden, um junge Talente für diese Berufe zu interessieren und sie zu fördern.

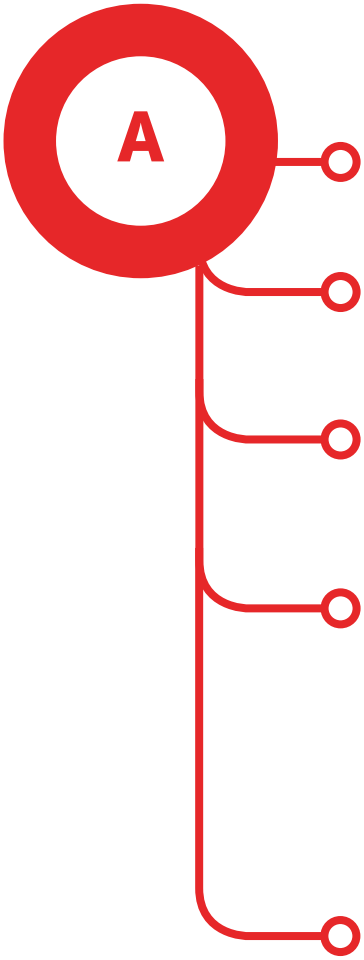
Wir müssen den Brancheneinstieg für diese begabten jungen Leute einfacher und attraktiver machen. In der Studie wurde festgestellt, dass drei Viertel der jungen Leute (71 Prozent) nicht wissen, ob es Möglichkeiten für (Hochschul-)Ausbildungs- oder Praktikantenprogramme im Bereich IT-Sicherheit gibt.

Unternehmen führen zwar an, dass Neueinsteiger nicht über die praktischen Erfahrungen bei der Cybersicherheit verfügen. Nur sehr wenige bieten aber aktuell Einsteiger-Positionen oder Praktikantenprogramme an, um Talente einzubinden. Zurzeit gibt es nur bei 45 Prozent der Unternehmen Stellen für Berufseinsteiger oder Trainee-Programme.

Knapp ein Drittel (30 Prozent) gibt zu, dass bei ihnen nicht die internen Ressourcen vorhanden sind, um Studienabgängern Stellen in der Cybersicherheit anzubieten. Anlass zur Sorge gibt auch, dass nur ein Fünftel (20 Prozent) der Befragten der Meinung waren, dass spezielle Cybersicherheitsteams in fünf Jahren für die IT-Sicherheit zuständig sein würden. Hälfte (50 Prozent) glaubt, der Kampf gegen die Cyberkriminalität würde dann in den Aufgabenbereich des allgemeinen IT-Teams fallen.

Nous avons constaté que près de trois quarts des jeunes (71%) ne sont pas informés des possibilités qui s'offrent à eux de poursuivre des études supérieures ou de réaliser des stages en sécurité informatique.





Und die Lösung ist?

Aus unserer Perspektive bei Kaspersky Lab ist dieser Bericht nur der erste Schritt, um dem Qualifikationsdefizit im Bereich Cybersicherheit entgegenzutreten. Ein Problem dieser Größenordnung erfordert gemeinsame Anstrengungen der Industrie, des Bildungswesens und der Behörden.

Wir sind der Ansicht, dass seitens der Arbeitgeber mehr getan werden muss, um jungen Leuten Anreize zu bieten, eine Laufbahn im Bereich Cybersicherheit einzuschlagen. Selbst unter IT-Sicherheitsexperten geben 27 Prozent zu, dass die Unternehmen mehr tun müssen, um Schulungen und Trainee-Programme anzubieten.

Von der Branche gestartete Initiativen können dabei helfen, eine Karriere im Bereich Cybersicherheit attraktiver zu machen. Internationale Wettbewerbe für Studenten und junge Leute dienen beispielsweise dazu, diese Talente zu fördern. Anhand anspruchsvoller Aufgaben im Bereich Cybersicherheit erhalten diese jungen Leute einen Vorgeschmack darauf, wie sie für die Branche und die Gesellschaft allgemein von Nutzen sein können.

Durch eine enge Kooperation mit Universitäten kann unsere Branche entscheidend dazu beitragen, dass fortlaufend Talente verfügbar sind, und sicherstellen, dass der theoretische und praktische Lernstoff den Erwartungen und zukünftigen Anforderungen entspricht. Die Branche kann durch Mitarbeit an Studienprogrammen, Entsenden von Gastrednern, Vorstellen neuer Technologien und Zusammenarbeit an Forschungsprojekten dafür sorgen, die nächste Generation von Experten für den Kampf gegen die Cyberkriminalität zu begeistern, einzubinden und vor allem aufzuklären und auszubilden. Programme für Praktikanten und Absolventen können helfen, die Beziehungen zwischen Unternehmen und dem Bildungssektor zu vertiefen, damit uns die wertvollen Talente, die wir so sehr benötigen, nicht entgehen.

Die Ergebnisse dieses Berichts verdeutlichen, welch großer Herausforderung die Branche gegenübersteht, zeigen aber auch Bereiche auf, in denen Fortschritte möglich sind. Wir müssen die hier aufgeführten Möglichkeiten unbedingt ausschöpfen, um die Cybersicherheits-Zeitbombe zu entschärfen, bevor sie explodiert.

1 Anmerkung zur Studie: Kaspersky Lab hat bei Arlington Research eine Studie beauftragt, die insgesamt 2.120 IT-Fachleute in Großbritannien, Italien, Spanien, den Niederlanden, Frankreich, Deutschland und den USA befragt. Darüber hinaus beauftragte Kaspersky Lab Arlington Research damit, 11.531 junge Anwender, im Alter von 16 bis 25 Jahren in Großbritannien, der Republik Irland, den USA, Frankreich, Deutschland, Italien, den Niederlanden und Spanien zu befragen. Beide Studien wurden im Juli 2016 abgeschlossen.

KASPERSKY LAB

Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK

www.kaspersky.co.uk

KASPERSKY lab

FUTUREPROOFING CYBERSECURITY

INVESTING IN TODAY'S TALENT TO SECURE TOMORROW