Der Weg aus dem Fachkräftemangel

Eine Umfrage zum weltweiten Mangel an Fachkräften für Cyber-Sicherheit

Aufgrund des weltweiten Mangels an geschulten und qualifizierten Fachkräften für Cyber-Sicherheit wird die ohnehin schon schwierige Abwehr der in Raffinesse und Zahlen zunehmenden Bedrohungen zusätzlich erschwert. Das Center for Strategic and International Studies (CSIS) führte eine Umfrage dazu durch, wie groß der Mangel an Cyber-Sicherheitsexperten in acht Ländern (Australien, Deutschland, Frankreich, Großbritannien, Israel, Japan, Mexiko und USA) tatsächlich ist. Dazu wurden Entscheidungsträger im IT-Bereich aus dem privaten sowie öffentlichen Sektor befragt, wobei der Schwerpunkt auf vier fachkräftebezogenen Cyber-Sicherheitsbereichen lag: Sicherheitsausgaben, Schulungsprogramme, Mitarbeiterdynamik und gesetzliche Richtlinien. Mithilfe der Umfrageergebnisse können Unternehmen und Regierungen einen stabilen und zukunftsfähigen Mitarbeiterstamm aufbauen, der über die erforderlichen Kompetenzen verfügt. Die Umfrage liefert zudem mehrere konkrete Empfehlungen dazu, wie der aktuelle Mangel an Cyber-Sicherheitsmitarbeitern behoben und die allgemeine Cyber-Sicherheit weltweit verbessert werden kann.

Die wichtigsten Erkenntnisse

- Der Mangel an Cyber-Sicherheitsexperten betrifft praktisch alle Bereiche. Laut der CSIS-Umfrage sehen 82 Prozent der Befragten einen Mangel an Cyber-Sicherheitskompetenzen in ihrem Unternehmen. Die geringe Zahl von und gleichzeitig hohe Nachfrage nach Cyber-Sicherheitsexperten hat die Gehälter nach oben getrieben. In den USA liegt das Gehalt im Cyber-Sicherheitsbereich fast 10 Prozent höher als bei anderen IT-Jobs.
- Aufgrund fehlender Kompetenzen sind Unternehmen anfälliger für Angriffe. Diese Aussage wurde von 71 Prozent der Umfrageteilnehmer bestätigt, wobei 25 Prozent angaben, dass unzureichendes Cyber-Sicherheitspersonal letztlich zu Datenverlust oder -diebstahl sowie Rufschädigungen geführt hat.
- Bestimmte Kompetenzen werden stark nachgefragt. Die in allen acht Ländern am stärksten nachgefragten Kompetenzen sind Eindringungserkennung, Entwicklung sicherer Software sowie Angriffsverhinderung.

- Praktische Schulungen sind die beste Möglichkeit, sich Cyber-Sicherheitskompetenzen anzueignen. Etwa 50 Prozent der befragten Entscheidungsträger erwarten als Mindestvoraussetzung für die Einstellung einen Bachelor-Abschluss in einem relevanten technischen Bereich. Dennoch sind viele Umfrageteilnehmer der Meinung, dass Erfahrung, Hacking-Wettbewerbe und professionelle Zertifizierungen mehr zum Erwerb von Cyber-Sicherheitskompetenzen beitragen als ein Hochschulabschluss.
- Technologie kann den Fachkräftemangel teilweise kompensieren. Etwa 90 Prozent der Befragten sind der Meinung, dass Sicherheitstechnologie vorhandene Lücken schließen kann, und 55 Prozent glauben, dass die Weiterentwicklung von Cyber-Sicherheitslösungen in fünf Jahren so weit sein wird, dass diese Lösungen die Anforderungen ihrer Unternehmen erfüllen. Unternehmen lagern außerdem Sicherheitsfunktionen sowie Prozesse aus, für die sich eine Automatisierung anbietet.
- Regierungen investieren nicht genug in Cyber-Sicherheit. Laut 76 Prozent der Umfrageteilnehmer investieren ihre Regierungen nicht genug in Programme, mit denen Cyber-Sicherheitsexperten aufgebaut werden. Zudem glauben sie, dass die in ihrem Land geltenden Gesetze und Vorschriften im Bereich Cyber-Sicherheit ungeeignet sind.

Vier Dimensionen des Mangels an Fachkräften für Cyber-Sicherheit

Ausgaben für Cyber-Sicherheit

Laut Schätzungen liegen die Gesamtausgaben für Cyber-Sicherheit in den nächsten vier bis fünf Jahren bei mehr als 100 Milliarden US-Dollar.[1] Die größten Investoren in und Nutzer von Cyber-Sicherheitstechnologien sind die US-Regierung und Finanzdienstleister, die gleichzeitig die Hauptziele von Angreifern sind. Durch die starke Investition in Cyber-Sicherheit können diese beiden Sektoren den Fachkräftemangel besser ausgleichen und bessere empfohlene Vorgehensweisen bei der Schulung und Einstellung von Mitarbeitern durchsetzen.

Ausbildung und Schulungen

Der CSIS-Bericht weist darauf hin, dass akademische Abschlüsse zwar eine Mindestvoraussetzung für eine Stelle im Cyber-Sicherheitsbereich sind, die meisten Entscheidungsträger jedoch glauben, dass praktische Erfahrungen unschlagbar sind: Nur 23 Prozent der Befragten sind der Meinung, dass die Ausbildung die Studenten auf die Realitäten der Branche vorbereitet. Wie die Umfrage zeigt, stehen die USA und Großbritannien bei Investitionen in die Cyber-Sicherheitsausbildung an erster Stelle, Mexiko, Frankreich und Japan an letzter. Mehr als 75 Prozent der Umfrageteilnehmer sehen professionelle Zertifizierungen als effektiven Nachweis für Kompetenzen, und 40 Prozent sind der Meinung, dass Hacking-Wettbewerbe die beste Möglichkeit sind, sich entsprechendes Fachwissen anzueignen.

Mitarbeiterdynamik

Mit welchen Einstellungsstrategien werden Cyber-Sicherheitsexperten am besten angeworben und gehalten? An erster Stelle steht das Gehalt, gefolgt von Schulungen, dem Ruf der IT-Abteilung sowie Aufstiegschancen. Fast 50 Prozent der Umfrageteilnehmer gaben an, dass fehlende Schulungen oder Förderung von Zertifizierungsprogrammen häufige Gründe dafür sind, dass Mitarbeiter das Unternehmen verlassen. Da der Aufbau eines starken Cyber-Sicherheitsteams häufig längere Zeit in Anspruch nimmt, setzen Unternehmen verstärkt auf Technologien, um vorhandene Lücken zu schließen. Etwa 90 Prozent der Befragten glauben, dass die Weiterentwicklungen der Cyber-Sicherheitslösungen den Fachkräftemangel kompensieren könnten. Alternativ werden bestimmte Sicherheitsfunktionen häufig ausgelagert. Dazu zählen die Risikobewertung und -vermeidung, Netzwerküberwachung und Zugangskontrolle sowie die Reparatur kompromittierter Systeme. Mehr als 60 Prozent der Umfrageteilnehmer lagern zumindest einige ihrer Cyber-Sicherheitsaufgaben aus.

Gesetzliche Richtlinien
In vielen Ländern (Australien, Großbritannien, Israel, USA) wird der Fachkräftemangel zunehmend angegangen. In den meisten Ländern existieren zudem Richtlinien, die die Ausbildung im Bereich Cyber-Sicherheit verbessern sollen. Dennoch sind mehr als 75 Prozent der Befragten der Meinungen, dass ihre Regierungen nicht in genug in die Ausbildung von Cyber-Sicherheits-fachkräften investieren. Ebenso viele sagen, dass die Gesetze und Vorschriften zur Verbesserung der Cyber-Sicherheit in ihrem Land unzureichend sind.

Empfehlungen

Neue Mindestanforderungen für die Einstellung von Cyber-Sicherheitsfachkräften und Akzeptanz ungewöhnlicher Bildungswege
Die CSIS-Daten zeigen: Da in allen Ländern nur wenige Universitäten und Hochschulen Studiengänge zu Cyber-Sicherheit anbieten, sollten Personalentscheider professionellen Zertifizierungen und praktischen Erfahrungen einen höheren Wert beimessen als einschlägigen Studienabschlüssen. Universitäten und Hochschulen sollten ihre Studenten in praktischen Aspekten der Cyber-Sicherheit ausbilden und besondere Talente dabei unterstützen, ihre Fähigkeiten auszubauen. Solche Programme bieten Regierungen, dem privaten Sektor sowie Bildungseinrichtungen Möglichkeiten zur Zusammenarbeit, um die Ausbildung zu verbessern und studienbegleitende Praktika sowie Weiterbildungen anzubieten.

Diversität im Cyber-Sicherheitsbereich
Zahlreiche Umfragen zeigen, dass Frauen und Minderheiten in diesem Bereich unterrepräsentiert sind. Durch die strenge Einwanderungspolitik wird die Zahl der potenziellen hochqualifizierten Mitarbeiter zusätzlich verringert. Die Zahl der verfügbaren Cyber-Sicherheitsfachkräfte könnte in den USA und anderen Ländern mit ähnlichen Einwanderungsrichtlinien erheblich gesteigert werden, wenn mehr Arbeitsvisen ausgestellt und Minderheiten sowie Frauen berücksichtigt würden. Eine weitere Hürde bei der Einstellung neuer Cyber-Sicherheitsmitarbeiter besteht in dem schlechten Ruf, den IT-Experten mit Hacking-Erfahrung haben. Arbeitgeber sollten eine flexiblere Haltung bei der Einstellung neuer Mitarbeiter einnehmen, die in Hacking-Zwischenfälle verwickelt waren, da diese Erfahrungen und Fähigkeiten extrem nützlich sein können.

Mehr Möglichkeiten für externe Schulungen
Kontinuierliche Weiterbildungsprogramme sind sehr wichtig, um Cyber-Sicherheitsexperten im Unternehmen zu halten, da diese andernfalls zu anderen Arbeitgebern abwandern. Regierungen und der private Sektor sollten zusammenarbeiten, um die Schulungsmöglichkeiten für Studenten und Angestellte auszubauen, die ihre Kenntnisse erweitern möchten.

Anpassung der Kompetenzen an Automatisierung
Die CSIS-Umfrage zeigt, dass Unternehmen Cyber-Sicherheitsfunktionen automatisieren, um den Fachkräftemangel auszugleichen. Daher werden die Cyber-Sicherheitsmitarbeiter gezwungen, ihre Kompetenzen an diese neuen Prozesse anzupassen. Da Automatisierung mit verbesserter operativer Effizienz einhergeht, werden sich Cyber-Sicherheitsexperten mehr auf die Erkennung, Analyse und Behebung hochentwickelter Bedrohungen konzentrieren.

Datenerfassung und Definition einer Taxonomie
Wenn der private Sektor, Regierungen und Bildungseinrichtungen Daten zum Cyber-Sicherheits-Arbeitsmarkt und zu typischen Tätigkeitsbereichen sammeln, können sie eine allgemeine Taxonomie mit klar definierten Kompetenzen festlegen, die für alle Branchensektoren gelten.

Zusammenfassung

Ein stabiler Mitarbeiterstamm ist für effektive Sicherheit unabdingbar. Das gilt heute mehr als jemals zuvor. Der weltweite Mangel an Fachkräften für Cyber-Sicherheit kann durch die Einbeziehung von mehr talentierten IT-Experten behoben werden. Dazu bedarf es Verbesserungen in Bezug auf Ausbildung, Diversität am Arbeitsplatz, Weiterbildungsmöglichkeiten, Sicherheitstechnologie und Datenerfassung.

Den vollständigen Bericht finden Sie unter **mcafee.com/skillsshortage**.

1. http://www.forbes.com/sites/stevemorgan/2016/02/12/cybersecurity-market-outlook-for-2016-to-2020/#185c567a74a4

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com