

Bedrijven investeren jaarlijks ruim 92.000 euro voor bijscholing cybersecurityteams

02-04-2024 14:27



Meer dan 70 procent van de bedrijven wereldwijd betaalt jaarlijks ruim 92.000 euro (100.000 dollar) voor aanvullende training om de vaardigheden van hun cybersecuritymedewerkers up-to-date te houden, zo blijkt uit een recent onderzoek van Kaspersky. De ondervraagde bedrijven benadrukten echter ook dat er een gebrek is aan relevante cursussen die nieuwe uitdagende gebieden in de onderwijsmarkt behandelen, en verklaarden dat training niet altijd het verwachte resultaat oplevert.

In het recente onderzoek '[Het portret van de moderne informatiesecurityprofessional](#)' deed Kaspersky onderzoek naar het wereldwijde tekort aan cybersecuritypersoneel, de exacte redenen waarom bedrijven te weinig cybersecuritydeskundigen hebben en bracht het de manieren in kaart waarop bedrijven hun cybersecuritypersoneel evalueren en bijscholen.

Volgens het onderzoek investeren bedrijven wereldwijd aanzienlijke bedragen in het bijscholen van hun cybersecurityteams: 43 procent van de organisaties zegt gewoonlijk tussen de ruim 92.000 en 184.000 euro (\$100.000-\$200.000) per jaar te besteden aan informatiesecuritycursussen. 31 procent zegt zelfs meer dan 184.000 euro (\$200.000) te investeren in trainingsprogramma's. De overige 26 procent zegt gewoonlijk minder dan 92.000 te betalen voor opleidingsinitiatieven.

Verder blijkt uit het onderzoek dat meer dan een derde (37%) van de Europese cybersecurityprofessionals vinden dat bedrijfstrainingen niet genoeg zijn. Om concurrerend te blijven in de markt en kennis en vaardigheden up-to-date te houden, zijn ze bereid om met eigen geld te betalen voor aanvullende trainingen.

InfoSec-professionals merken echter ook op dat de onderwijsmarkt moeite heeft om de snel veranderende sector bij te houden en er niet in slaagt om de benodigde trainingsprogramma's op tijd te leveren. Uit het onderzoek blijkt dat de schaarste aan cursussen die nieuwe uitdagende gebieden behandelen het grootste probleem was voor degenen die op zoek zijn naar cybersecuritytraining. Het gaat hier om 52 procent van de Europese respondenten.

Misverstanden over de behoefte aan speciale opleidingsvereisten, zoals het kunnen coderen of vaardig zijn in gevorderde wiskunde, die niet van tevoren duidelijk werden gemaakt bij de pre-registratiefase was problematisch voor 51 procent van de Europese professionals. Nog eens 50 procent van de Europese respondenten verklaarde dat cursisten de neiging hadden om te vergeten wat ze hadden geleerd omdat ze geen gelegenheid hebben gehad om de nieuw verworven kennis toe te passen, waardoor de cursussen nutteloos voor hen waren.



"Met een voortdurend veranderend bedreigingslandschap moeten bedrijven de vaardigheden van hun cybersecuritypersoneel voortdurend verbeteren om goed voorbereid te zijn op geavanceerde cyberaanvallen. Het ontwikkelen van spraakmakende specialisten binnen bedrijven en het opbouwen van interne expertise kan een effectieve strategie zijn voor organisaties die ernaar streven om bestaande werknemers te behouden en hen professioneel te laten groeien. Dit in plaats van voortdurend op jacht te gaan naar nieuwe kandidaten en hun professionele achtergronden en praktische vaardigheden te controleren. Voor organisaties die worden bediend door Managed Service Providers is het ook belangrijk om intern een behoorlijk hoog expertiseniveau te handhaven en dezelfde taal te spreken wanneer ze de omvang van de services en de Service Level Agreement met hen bespreken," zegt Veniamin Levtsov, VP, Center of Corporate Business Expertise bij Kaspersky.