Veel cybersecurityproblemen bij bedrijven die deel uitmaken van het portfolio van private equity-partijen

Onderzoek BlueVoyant toont de aandachtsgebieden voor het verminderen van cyberrisico's aan

Release date Nov. 24, 2022, 03:24 am EDT
Amsterdam, NL

Toonaangevend leverancier van cybersecurity diensten BlueVoyant heeft onderzoek gedaan naar de cybersecurityrisico's onder 780 bedrijven die deel uitmaken van het portfolio van private equity-bedrijven. Hieruit blijkt dat het IT-beheer bij deze doelgroep een belangrijk punt van zorg is en dat een groot aantal veel steken laat vallen op het gebied van cybersecurity. Ruim zeventig procent van alle kritieke kwetsbaarheden in systemen die verbonden zijn met het internet was het gevolg van gebrekkige cyberhygiëne. Dit maakt de onderzochte bedrijven kwetsbaar voor cyberincidenten.

Gebrekkige cyberhygiëne
Bijna een vijfde (19%) van de onderzochte bedrijven wordt aan cyberrisico's blootgesteld via 'zero tolerance findings'. Dit detecteerde BlueVoyant binnen haar publiek toegankelijke systemen verbonden met het internet. Zero tolerance staat bekend als een kritieke kwetsbaarheid waar cybercriminelen makkelijk misbruik van kunnen maken en die vaak ten grondslag ligt aan succesvolle ransomware-aanvallen. Misbruik van deze kwetsbaarheid kan leiden tot gegevensverlies en downtime van diensten. Met als gevolg verlies van klantenvertrouwen en financiële schade.

Samenwerking belangrijk voor risicoreductie
Private equity-bedrijven moeten dus alert blijven. "Bij private equity portfoliobedrijven blijft er sprake

van een sterk uiteenlopend beveiligingsniveau. Cybersecurity wordt nog niet overal erkend als een groot bedrijfsrisico en wordt daarmee soms over het hoofd gezien”, aldus Vincent Turner, Directeur Nederland bij BlueVoyant. “Ons onderzoek wijst op de noodzaak om daar prioriteit aan toe te kennen. Private equity-bedrijven moeten proactief blijven samenwerken met de bedrijven in hun portfolio aan het terugdringen van hun cyberrisico’s en de kosten die met cyberincidenten gepaard gaan. Verder is het belangrijk om een programma voor risicoreductie op te zetten dat cyberrisico’s op prioriteit indeelt en het aanvalsoppervlak van portfoliobedrijven continu en realtime analyseert op kwetsbaarheden.”

Contact

- BlueVoyant

The full press release with contact information can be viewed online at:
https://amaxwire.com/short/10468

Amaxwire prioritizes transparent and sincere sources, we do not allow opaque clients. Our editors carefully try to remove false and misleading content. If you, as a user, see something that we have missed, please bring it to our attention.

See our editorial guidelines for more information.
© 2024 Amaxwire All rights reserved.