Gescheiden door taal: Kaspersky-onderzoek toont aan dat Nederlandse bedrijven cybersecurity niet begrijpen

Uit onderzoek van Kaspersky blijkt dat C-level managers cyberaanvallen als een groter risico ervaart dan het verslechterende economische klimaat. Toch zijn ze niet in staat passende maatregelen te nemen door de verwarrende terminologie....

Release date Nov. 24, 2022, 05:37 am EDT
Utrecht, NL

Uit onderzoek van Kaspersky blijkt dat C-level managers cyberaanvallen als een groter risico ervaart dan het verslechterende economische klimaat. Toch zijn ze niet in staat passende maatregelen te nemen door de verwarrende terminologie en het jargon dat wordt gebruikt binnen de cybersecurity. Meer dan de helft (51%) van de ondervraagde Nederlandse C-level managers gelooft dat cybersecurityaanvallen een groter risico voor hun bedrijf zijn dan economische factoren (49%) en compliance (35%). Nog eens 45 procent van de C-level managers verklaren dat zij de taal die wordt gebruikt om deze cyberdreigingen te beschrijven als de grootste belemmering zien voor het begrip van hun managementteam.

Cybersecurity op de agenda
Alle Nederlandse C-level respondenten (100%) zijn zich bewust van de frequentie waarmee hun bedrijf wordt aangevallen door dreigingsactoren, blijkt uit het onderzoek van Kaspersky naar de taalbarrières die er bestaan op het gebied van cybersecurity. Ondanks dit bewustzijn verklaart 39 procent van de respondenten dat cybersecurity slechts soms een agendapunt was tijdens bestuursvergaderingen, terwijl iets meer dan de helft (56%) zegt dat cybersecurity altijd een agendapunt was.

De bevindingen suggereren ook dat hoe groter de organisatie, hoe groter de potentiële kloof met het algemene cybersecuritybewustzijn is. 10 procent van de C-level respondenten in bedrijven met 5000+ werknemers verklaren dat cybersecurity zelden een agendapunt is voor hun management- of bestuursvergaderingen ten opzichte van slechts 2,5 procent van de C-level in bedrijven tussen 2000-2999 werknemers.

Taal als belemmering
Een mogelijke kloof tussen C-level en hun vermogen om de implicaties van hun grootste risico echt te begrijpen, kan worden verklaard door hun problemen met de taal die wordt gebruikt om bedreigingen te beschrijven. Bijna de helft (45%) van alle beveiligings-, compliance- en risicospecialisten op C-level is van mening dat jargon en verwarrende industrietermen momenteel de grootste belemmering vormen voor het begrip van cybersecurity door C-level en, belangrijker nog, wat zij eraan moeten doen.

Om dit punt duidelijker te illustreren, verklaren de ondervraagden dat zij de basis cybersecuritytermen malware (47%), supply chain-aanvallen (48%) en Zero-Day exploit (50%) verwarrend vinden. Iets technischer taalgebruik, zoals 'YARA' en 'Suricata-regels', kent een vergelijkbare mate van verwarring: respectievelijk 50 procent en 49 procent van de respondenten geeft aan deze termen niet volledig te begrijpen.

"Acroniemen en jargon zijn vanzelfsprekend voor ingewijden, maar lijken vaak verwarrend voor anderen die geen directe ervaring hebben met het werken in cybersecurity. Onze bevindingen suggereren dat het onvermogen van het senior management om de aard van de bedreigingen waaraan ze voortdurend worden blootgesteld echt te begrijpen, betekent dat ze vaak niet worden beschouwd als een prioriteit voor de directie", legt Tim De Groot, General Manager Benelux en Nordics bij Kaspersky, uit. "Dit betekent in wezen dat hooggeplaatste C-level executives tijdig cruciale zakelijke beslissingen moeten nemen zonder een duidelijk beeld te hebben van hun eigen unieke dreigingslandschap en, nog belangrijker, zonder inzicht te hebben in het risico dat dit voor hun organisatie vormt. Hierdoor kunnen ze geen cybersecuritycultuur ontwikkelen op basis van best-practices, kennisdeling en uiteindelijk bruikbare informatie."

Methodologie
Kaspersky 'Separated by a common language: Is the C-Suite able to truly decipher and act upon the real threat of cyber-attacks?' volgt op een totaal van 1.800 interviews met C-level beslissers in grote ondernemingen van 1.000 of meer werknemers in 13 landen, waarvan 100 in Nederland. In het onderzoek werd de respondenten gevraagd naar de cybersecurity binnen hun organisatie, de maatregelen die zij hebben genomen om zich te beschermen en de belemmeringen waarmee zij als managementteam worden geconfronteerd.

Contact

- Kaspersky

Amaxwire

The full press release with contact information can be viewed online at:
https://amaxwire.com/short/10478

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.