

Kaspersky Lab



Martijn van Lom

Cybersecurity is een continu proces

Volgens general manager Martijn van Lom van Kaspersky Lab Benelux is databeveiliging een continu proces van informatie verzamelen en toetsen. Benchmarken is belangrijk om je inzicht te vergroten. Steeds meer brancheverenigingen pakken hun rol daarin op.

■ Cybersecurity ■ Internetbeveiliging ■ Datalekken ■ Hackers ■ Benchmarken

General manager Martijn van Lom is erg blij dat Kaspersky Lab is verkozen tot de beste dienstverlener in de categorie 'security'. "We roepen altijd dat databeveiliging op de bestuursagenda's moet komen. Daarom is het des te leuker dat wij juist in dit onderzoek onder zakelijke beslissers eerste zijn geworden."

Continu proces

Waar heeft Kaspersky Lab deze voor-

keurspositie aan te danken? Van Lom schrijft het toe aan het feit dat Kaspersky Lab vooral de laatste tijd veel energie heeft gestoken in het innoveren en toetsen van zijn producten. "We brengen alleen nieuwe releases uit op basis van innovatieve features, die weer een beter antwoord zijn op de cybercriminaliteit. Dat is een tak die continu evolueert. Het is zaak om mee te evolueren." Cybersecurity is niet een kwestie van een oplossing implementeren en dan

achteroverleunen. "Je moet er continu mee bezig zijn", vindt Van Lom. "Tegenwoordig is niet zozeer de vraag of je gehackt bent, maar wanneër je gehackt bent. Ga er maar gewoon van uit dat er een datahack is geweest; dat maakt je beveiliging alleen maar sterker. Het is de beste manier om intern naar je eigen organisatie te kijken, teneinde continu te evolueren."

'Ervan uitgaan dat er een datahack is geweest, maakt je beveiliging alleen maar sterker'

Ook is het volgens Van Lom belangrijk om te benchmarken, met name op het gebied van investeringen. "Het is best lastig om een budget tegenover cybersecurity te zetten. Het helpt als je weet welke investeringen binnen je branche worden gedaan, en waarin wordt geïnvesteerd. Brancheverenigingen kunnen op dit vlak een rol spelen, en ze pakken die ook steeds vaker op."

Brandoefening

Van Lom raadt bedrijven aan om met andere bedrijven over datasecurity te overleggen. "Zeker ook met bedrijven waar het een keer mis is gegaan. Het is waardevol om te weten hoe zij dat proces hebben doorlopen. Welke rollen erbij horen. Het is verder heel belangrijk om het bestuur van je bedrijf daarbij te betrekken. Oefen ook eens een cyberaanval, zodat je weet wat je moet doen, net als bij een ontruimingsoefening. Juist dan wordt duidelijk waar de zwakke schakels zitten. Zoek ook daar binnen je netwerk of je branche de samenwerking in."

Er bestaan tal van regels voor bedrijven op het gebied van veiligheid, voor brandoefeningen, bedrijfshulpverlening, ontruiming. Voor cybersecurity bestaan nog geen regels, maar het is wel aan te raden, vindt Van Lom. "Ik verwacht dat we in de toekomst behalve datalekken ook hacks zonder datalek zullen moeten melden bij de overheid."

