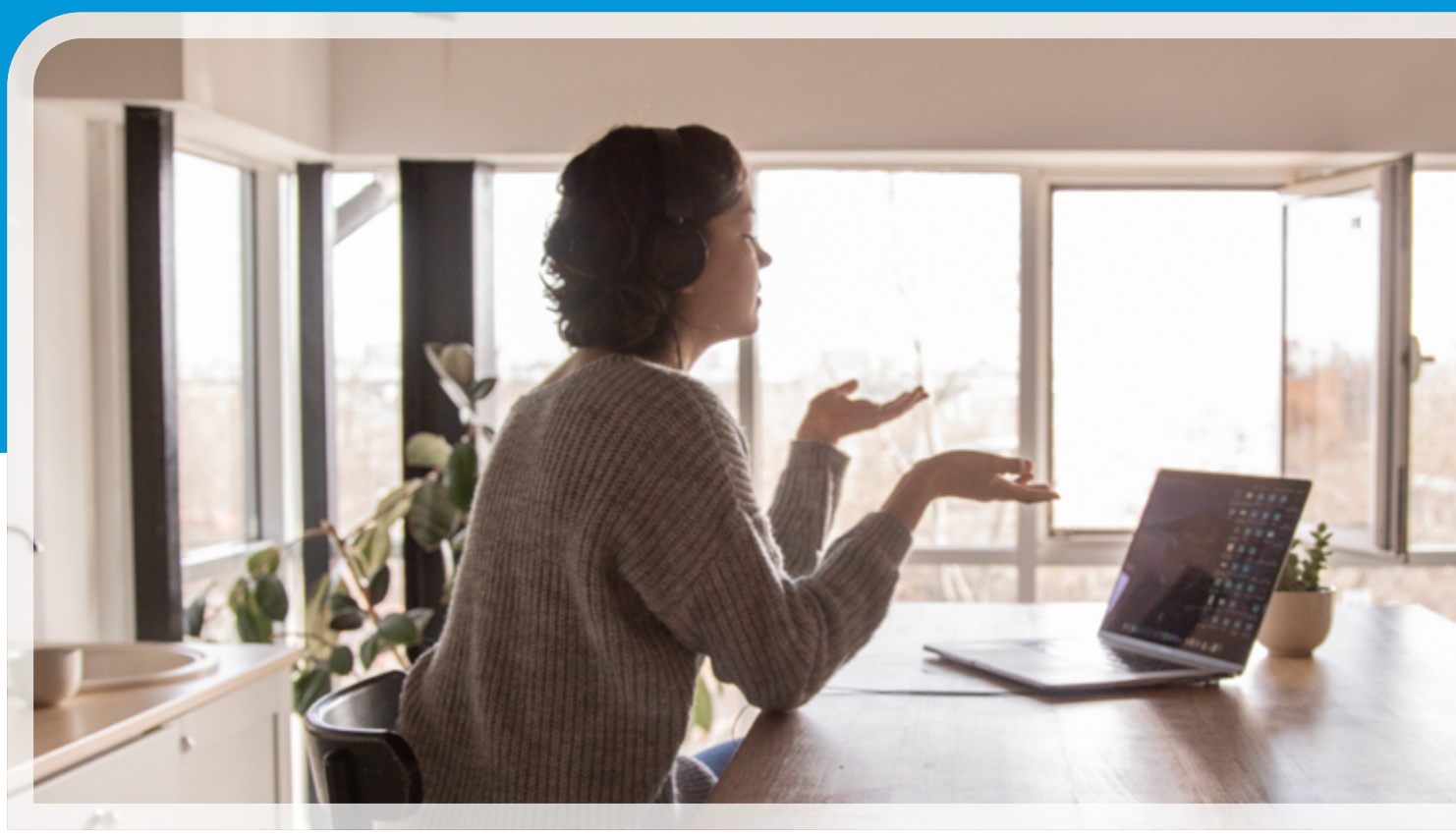

MODERNE SECURITY ALS SOM VAN BEWUSTWORDING EN EXPERTISE

Veel Nederlandse medewerkers gaan uitermate slordig om met hun digitale veiligheid. Dat is één van de conclusies uit het rapport Veilig Online 2020 van het ministerie van Economische Zaken en Klimaat. Dat mag met recht verontrustend worden genoemd in het zakelijke landschap van vandaag. Het is essentieel dat organisaties maatregelen nemen om het risiconiveau te verlagen.

Bewustzijn security ver onder de maat

Uit het rapport komt naar voren dat veel Nederlandse medewerkers het niet zo nauw nemen met hun online veiligheid. Ruim zestig procent gebruikt nog altijd een zwak wachtwoord en denkt er niet aan dit regelmatig te updaten. Ook links in e-mails worden in de helft van de gevallen niet gecontroleerd voordat erop wordt geklikt. Het niet opvolgen van dit soort basismaatregelen maakt alle overige securitymaatregelen een stuk minder effectief; een absolute doodzonde anno 2020.

De mens als zwakste schakel

Het gebrek aan bewustzijn rondom veilig werken is koren op de molen van de cybercrimineel. Deze richt zijn pijlen dan ook steeds vaker op de mens, in plaats van op de techniek. Cybercriminelen azen op onwetendheid van de medewerker om toegang te krijgen tot het bedrijfsnetwerk. Dat kan al snel uitmonden in desastreuze gevolgen voor de productiviteit, de bereikbaarheid, het imago én de financiële positie van de organisatie.

Thuiswerken verhoogt risico

De transitie naar thuiswerken vergroot de risico's van het gebrek aan securitybewustzijn nog eens. Bij thuiswerken vormen zakelijke en privé-IT vaak één geheel. Een voorbeeld is de cloudwerkplek, die toegankelijk is via de privé en mogelijk minder goed beveiligde modem. Wellicht gebruiken medewerkers hun zakelijke device thuis sneller voor privézaken, zoals het doorsturen van mailtjes of het gebruik van bepaalde apps of websites. Ook dat kan allerlei ellende in de hand werken.

Kennisverbetering noodzakelijk

De conclusie die aan deze trend kan worden verbonden is even logisch als simpel: medewerkers zouden zich bewuster moeten zijn van de risico's van onveilig werken en cybercrime in het algemeen. Een manier om dat te bereiken is via trainingen. Door medewerkers te wijzen op het groeiende aantal dreigingen - en ze te trainen op herkenning daarvan - kan veel ellende al worden voorkomen.

Uitbesteden van security

Security is en blijft echter een samenwerking tussen mens en technologie. Hoe intensiever dit verbond, hoe sterker de dataveiligheid. Security in eigen beheer houden is tegenwoordig echter geen sinecure. Computacenter biedt u daarin ondersteuning door security van uw (inter)nationale vestigingen over te nemen en doorlopend up-to-date te houden. Hiermee profiteert u van hoogwaardige en gecertificeerde security op het snijvlak van gebruiksgemak, toekomstbestendigheid en innovatie.

> Het niet opvolgen van basismaatregelen maakt alle overige securitymaatregelen minder effectief.

Bart Brunink
Manager Professional Solutions

Computacenter

Postbus 300, 1180 AH Amstelveen
nl.sales@computacenter.com
+31 (0)88 4358222

www.computacenter.com/nl