Security & GDPR: belangrijker dan ooit

Organisaties moeten investeren in een sterke beveiligingscultuur – juist nu steeds meer bedrijven hun werknemers massaal thuis laten werken is dat belangrijker dan ooit tevoren. Michel Schaalje (Cisco Nederland), Jasper Wenselaar (Micro Focus) en Hendrik Flierman (G DATA CyberDefense) geven hun visie op de ontwikkelingen.

Michel Schaalje, *Directeur Security Cisco Nederland*

1

Welk security-aspect wordt door bedrijven het meest onderschat als bedrijven medewerkers thuis laten werken?

ZeroTrust, ofwel vertrouw niet op enkel gebruikersnaam en wachtwoord. Doe een extra validatie, zoals Multifactor Authenticatie.

2

Wat onderschatten medewerkers zélf vooral op gebied van security bij thuiswerken?

Confidentiële informatie op eigen systemen opslaan. Denk goed na over de informatie die je bij je bedrijf weg haalt, en waar je deze vervolgens plaatst. Je eigen omgeving, of die van sommige clouddiensten, voldoen waarschijnlijk niet aan de securityregels die bij je organisatie gehanteerd dienen te worden. Meestal is de medewerker daar ook niet voldoende van op de hoogte.

3

Welke innovatie of technologie (voorbeelden: cloud, secure access, wifi, etc.) profiteert het meest van het toegenomen thuiswerken?

Cloudsecurity en daarmee ook Secure Remote Access (bijvoorbeeld VPN) profiteren uiteraard van het thuiswerken. Cloudsecurity zorgt voor effectieve en schaalbare security voor medewerkers, ongeacht waar de medewerkers werken. Uiteraard enkel mits juist toegepast. Het mooie van goede cloudsecurity is dat het medewerkers ook van deze beveiliging kunnen genieten op het moment dat ze toch weer terug naar kantoor gaan. Medewerkers krijgen dus overal de juiste bescherming.

Michel Schaalje

Jasper Wenselaar, *Partner Business Manager Micro Focus*

1

Welk security-aspect wordt door bedrijven het meest onderschat als bedrijven medewerkers thuis laten werken?

Datasecurity.

2

Wat onderschatten medewerkers zélf vooral op gebied van security bij thuiswerken?

Het veilig stellen en beschermen van bedrijfsdata (zowel IP als privacy data). Thuiswerken brengt andere risico's met zich mee die een gevaar kunnen vormen voor de data die medewerkers gebruiken/verwerken.

3

Welke innovatie of technologie (voorbeelden: cloud, secure access, wifi, etc.) profiteert het meest van het toegenomen thuiswerken?

Secure Access Management; nu er meer thuis gewerkt wordt, zien we dat de vraag naar secure access management in relatie tot thuiswerken toeneemt.

Jasper Wenselaar

Hendrik Flierman, *Global Sales Director van G DATA CyberDefense*

1

Welk security-aspect wordt door bedrijven het meest onderschat als bedrijven medewerkers thuis laten werken?

Het grootste probleem bij het beveiligen van organisatie ligt nog altijd bij de mens. Medewerkers kunnen onbewust een mailtje met een gevaarlijke link of bestand openen dat een virus bevat. Daarnaast gebruiken medewerkers soms hun apparaten, zowel zakelijk als privé, om contact te maken met het bedrijfsnetwerk. Juist nu zoveel werknemers buiten de veilige schil van het kantoor moeten werken, is aandacht voor cyberawareness nog meer van belang.

2

Wat onderschatten medewerkers zélf vooral op gebied van security bij thuiswerken?

Mensen zijn al snel gemakzuchtig. Als een apparaat of oplossing beter werkt, of sneller is, kiezen ze er al snel voor om het te gebruiken. Dit is alleen niet altijd veilig. Het is daarom verstandig dat medewerkers alleen de tools gebruiken van de organisatie waar ze voor werken. Als werknemers ervoor kiezen om applicaties te gebruiken die niet zijn goedgekeurd door de IT-afdeling, dan is de kans groot dat gevoelige bedrijfsgegevens onbedoeld worden blootgesteld aan de kans op misbruik. In andere gevallen worden gegevens willens en wetens buiten beveiligde bedrijfsapplicaties om opgeslagen en uitgewisseld. Ook hiermee wordt de kans op datalekken aanzienlijk vergroot.

3

Welke innovatie of technologie (voorbeelden: cloud, secure access, wifi, etc.) profiteert het meest van het toegenomen thuiswerken?

Ik denk dat met name tools en platforms om te videobellen en te chatten een enorme vlucht hebben genomen dankzij Covid-19. Ook hier kleven de nodige cyberrisico's aan. Met name de gratis varianten verdienen meestal geld aan gegevens. Hierdoor zijn ze niet altijd even privacyvriendelijk. In het algemeen geldt: als je voor een dienst betaalt is deze vaak privacyvriendelijker. Ik adviseer werknemers dan ook om alleen gebruik te maken van de diensten en apps die door je werk beschikbaar zijn gesteld. Voor organisaties is het belangrijk om de risico's van het gebruik zorgvuldig in te schatten. Denk aan bijvoorbeeld het gebruik van encryptie en de overeenkomst voor verwerking van alle data.

Hendrik Flierman