Bedrijfs-geheimen op straat

Hoe gevaarlijk is het gebruik van smartphones bij het nieuwe werken?

Steeds meer bedrijven in Nederland zien het nut in van **'het nieuwe werken'**. Slimme technische oplossingen maken het mogelijk om flexibeler om te gaan met werktijden en -locaties. Via smartphones zijn we altijd en overal bereikbaar, kunnen we e-mails beantwoorden en belangrijke bestanden verzenden. Maar hoe veilig is dit? Liggen er virussen op de loer en zijn de smartphonegebruikers of systeembeheerders wel voldoende ingespeeld op deze gevaren? Of ligt er juist meer gevaar in de nonchalance van de gebruiker?

PEAK-IT Magazine spreekt over deze thema's met de anti-virus-topconsultant Eddy Willems (zie foto). Willems is een bekende digitale veiligheidsexpert in België en ver daarbuiten. Volgens Willems is de virusdreiging voor smartphones op het moment nog te verwaarlozen: "De hoeveelheid virussen die in omloop zijn toont aan hoe minimaal het gevaar voor smartphones is. Ik zeg niet dat het gevaar niet bestaat, maar op het moment zijn er slechts 500 virussen voor smartphones ten opzichte van 40 miljoen voor de pc." Hij illustreert op heldere wijze waarom we ons hier niet al te druk over hoeven te maken. "Dat aantal van 500 virussen is vergelijkbaar met het aantal virussen dat in 1991 in omloop was voor pc's. In die tijd had ook nog niemand een virusscanner." Toch anderschat hij toekomstig gevaar niet. "De snelheid waarin virussen zich ontwikkelen is groter, dat is een feit. Het zou zeker zo kunnen zijn dat we volgend jaar al op een aantal zitten dat vergelijkbaar is met 1994 voor pc's. Dan zou er een behoorlijke sprong gemaakt zijn."

In de huid van de cybercrimineel

De reden dat er nog zo weinig virussen zijn, heeft volgens Willems te maken met de grote spreiding in besturingssystemen. "De markt is te verdeeld. Op het moment is er nog geen winnaar onder de operating systems. Symbian doet het goed, maar Iphone heeft met iOS ook een serieus stuk markt in handen. Dan heb je natuurlijk Android, Windows Mobile en het BlackBerry systeem. Zolang er geen partij is die, laten we zeggen meer dan 60% van de markt in handen heeft, loont het criminelen de moeite niet om hier malware voor te creëren." Om zijn uitspraak kracht bij te zetten stelt hij voor eens te kruipen in de huid van za'n cybercrimineel: "Als malwareschrijver wil je zoveel mogelijk geld verdienen en dus ga je op zoek naar het grootste publiek. Dan is het het makkelijkste om iets te maken voor een Windowsprogramma." Want al zijn de meeste computers tegenwoordig goed beveiligd, toch is het aantal Windows pc-gebruikers zo hoog, dat er voor cybercriminelen nog altijd meer succes mee te boeken valt. De virussen die wel gericht zijn op smartphones zijn tot nu toe vooral opgedoken in Aziatische landen en Rusland. Willems omschrijft om wat voor type virussen het gaat: "Dit is bijvoorbeeld malware die ervoor zorgt dat je telefoon automatisch belt naar dure buitenlandse nummers. Maar de kosten die gemaakt worden zijn ook weer niet zo gek hoog, za'n 10 à 20 euro per maand. Hierdoor valt het bijna niet op dat er meer geld dan normaal van je rekening wordt afgeschreven."

Controle op apps

De virusdreiging is dus laag, maar Willems ziet nog wel verbeterpunten wat betreft veiligheid en met name bij de controle op apps. "Er moet echt iets gedaan worden aan de applicatiekeuring. In veel apps die momenteel verkrijgbaar zijn, zitten codes die bedenkelijk zijn. Zo zijn er apps die gegevens over waar je je bevindt terugsturen naar een server, of gegevens over wie je belt. Er zijn gevallen bekend dat er effectief sms-gegevens worden opgeslagen. De gebruiker merkt daar niets van." Hoewel er ook wat apps betreft nog weinig alarmerends is gebeurd, is het geen prettig idee dat er misschien persoonlijke gegevens worden afgetapt. Daarom luidt Willems' advies om dit te voorkomen: "Uitkijken met het installeren van apps die nog maar kort op de markt zijn of apps die er wel leuk uitzien maar weinig nuttigs te bieden hebben." Veel gebruikers zien apps als leuk speelgoed, maar het is dus niet altijd zo onschuldig als het lijkt.

In veel apps die momenteel verkrijgbaar zijn, zitten codes die bedenkelijk zijn

De grootste bedreiging

Hoewel er nu nog weinig actie ondernomen hoeft te worden om virussen op smartphones te voorkomen, sluit Willems niet uit dat dit in de toekomst wel gebruikelijk zal zijn. "Als smartphones toegang hebben tot het bedrijfsnetwerk, is het belangrijk dat deze toestellen onder dezelfde beveiliging komen te staan." Op het moment is de analoge wereld echter een grotere bedreiging voor de bedrijfsdata op smartphones. "Er zijn anti-viruspakketten verkrijgbaar voor smartphones, maar eigenlijk komen deze altijd in combinatie met een anti-diefstalproduct. Een programma dat bijvoorbeeld ervoor zorgt dat het toestel een bericht uitzendt op het moment dat het gestolen of verloren is." Misschien is het beste advies om te voorkomen dat bedrijfsgegevens op straat belanden dan ook bewust om te gaan met je smartphone wanneer je deze ook voor je werk gebruikt. Niet laten slingeren of nonchalant opbergen waar iedere handige zakkenroller erbij kan. Iedereen kan zich vast nog herinneren hoe in 2006 een kapitein van de landmacht een memorystick met staatsgeheimen in een huurauto liet liggen. De informatie belandde zomaar op straat en daar kwam geen virus of hacker aan te pas.

www.anti-malware.info