

Ondernemers schaffen de duurste 'firewalls' aan, stoppen alle papieren in een kast met een slot er op. Alleen vergeten ze dat werknemers vertrouwelijke informatie via hun USB-stick mee naar huis nemen. En die informatie ligt makkelijk op straat. 8 tips.

Tegenwoordig nemen werknemers tonnen aan informatie mee op een simpel, petieterig apparaatje, nauwelijks groter dan een kleine aansteker: de USB-stick of simpelweg insteekgeheugen. Het gemak dient de mens, want dankzij de gebruiksvriendelijkheid en de grote geheugencapaciteit, kunnen zij zich nog flexibeler verplaatsen van de ene werkplek naar de andere.

Er zijn ook gevaren van het gebruik van de geliefde USB-stick schuilen. Denk aan verlies of diefstal van gegevens, of juist in het verkrijgen van ongevraagde cadeautjes als de zogenaamde 'Trojan Horses' en andere enge virussen. De gevolgen zijn alleen niet altijd met een simpel antibioticumkuurtje op te lossen.

Wat als je hem verliest? Wie denkt dat de consequenties minimaal zijn als de gegevens toch al verwijderd zijn, komt bedrogen uit. Met kleine software programma's als R-studio is het mogelijk om de gewiste informatie binnen enkele minuten te herstellen. De gelukkige vinder met minder goede bedoelingen kan dus op eenvoudige wijze toegang krijgen tot gevoelige informatie. Diefstal? Daar is de stick eveneens niet tegen beschermd.

Daarnaast is het onschuldige staafje de ideale verspreider van virussen. Een virusscanner? Die heeft-ie niet. Noch heeft elke computer waar je gebruik van maakt zulke software. Het is dus een kwestie van een optelsommetje; het virus van de onbekende computer komt op de USB-stick.

8 tips om je geheugenstick veiliger gebruiken:

1. Wis de gegevens op uw USB-stick met een permanent verwijderprogramma of met een 'slow format'.
2. Wees selectief met het plaatsen van informatie op de USB-stick. Als je de stick in een andere computer steekt, zorg er dan voor dat er alleen informatie op de stick staat die anderen mogen zien.
3. Zorg voor een goede virusscanner op uw computer of notebook die ook daadwerkelijk actief controleert.
4. Wanneer er toch gevoelige data op een USB-stick staat, zorg dan in elk geval voor een 'ik-heb-wat-en-ik-weet-wat' beveiliging, bijvoorbeeld een smartcard en een pincode.

5. Voor mensen die werken vanaf een stick, kopieer de data elke avond (of elke ander acceptabele interval) naar een plek die (automatisch) er een backup wordt gemaakt.
6. USB sticks van andere mensen zijn natuurlijk om al bovenstaande redenen net zo gevaarlijk. Het liefst zou je ze weigeren van je computer/netwerk en er zijn dan ook veel organisaties die dat doen. Een oplossing in een grote it-omgeving, is het inrichten van een USB kopieer- en print station, dat los van het netwerk staat. In een kleine it-omgeving zijn er een aantal andere mogelijkheden. Denk hierbij aan een printer die rechtstreeks van de USB stick kan printen, waardoor deze niet in contact komt met de computer.
7. Je kunt de computers van uw werknemers eventueel blokkeren voor USB gebruik.
8. Monitor wie er grote hoeveelheden data van het netwerk kopieert. Hier zijn verschillende oplossingen voor, van simpel tot zeer geavanceerd.