Verdere beschermingsmaatregelen

Het nut en de voordelen van USB sticks behoeven geen verdere uitleg. Toch zorgt de 'plug & play' modus voor een beveiligingslek. Werknemers kunnen te pas en te onpas gevoelige data op hun USB stick plaatsen, met alle gevaren van dien. Met enkele ingrijpende en minder ingrijpende middelen kunt u de controle terug krijgen:

- De USB portal onbruikbaar maken in de BIOS. Een vrij radicale oplossing, vooral als uw werknemers wel gebruik willen maken van USB apparatuur. Het is vrij tijdrovend, vooral binnen grote organisaties.
- De Driver.cab file verwijderen. Met deze aanpak kunnen alleen beheerders nieuwe USB apparaten installeren. De beheerder verplaatst de Driver.cab file uit de Winnt\Driver Cache\i386 directory naar een locatie waar gebruikers niet kunnen komen. Het verwijderen van de Driver,cab file is een netwerk gerichte aanpak waarbij het systeem wel de mogelijkheid behoudt om USB apparaten te gebruiken, maar waarbij alleen de beheerders nieuwe systemen en apparaten kunnen installeren.
- Beveiligingssoftware installeren. Er bestaat een aantal software oplossingen die per USB apparaat de permissies controleren. Programma's als DeviceLock van Smartline geven controle door apparaten op de 'white list' te zetten, waardoor men gewoon gebuik kan blijven maken van bijboorbeeld de muis of keyboard. Met DeviceLock hoeft men geen hardware te verwijderen of te 'blocken'. Men kan met de software per gebruiker bepalen wat diegene wel of niet kan doen. Hiermee is bijvoorbeeld per groep te regelen wie wel en wie niet bij bepaalde informatie mag komen. Ook biedt de software bescherming tegen het per ongeluk of expres vernietigen of zoekraken van data en tegen virussen en trojans afkomstig van 'removable disks'. Nadeel van deze tool kan zijn dat iedere pc in het netwerk voorzien zal moeten zijn van deze software.

eigen personeel dat te pas en te onpas USB-sticks en dergelijke in hun computer kan pluggen.

Onwetendheid

Werknemers kunnen op verschillende manieren een gevaar voor uw organisatie vormen. Het bewust stelen van informatie wordt soms uitvergroot, terwijl een veel groter gevaar het onbewust op straat brengen van informatie is. Het is haast vanzelfsprekend dat werknemers niet zomaar een map met gevoelige klantgegevens mee naar huis mogen nemen. Toch loopt het personeel met dezelfde gegevens op een USB-stick vaak zo het pand uit. Een personeelslid dat regelmatig thuis of onderweg werkt, vormt een groot potentieel gevaar voor uw organisatie. Uw nietsvermoedende werknemer – vanzelfsprekend een harde werker die in het weekeinde thuis nog iets wil afronden of regelmatig onderweg werkt – neemt vaak zonder dat hij het weet voor soms wel honderdduizenden euro's aan gevoelige informatie mee het pand uit. Onbeveiligd, waardoor kostbare data op straat kunnen komen te liggen, en dat is niet bepaald in lijn met de bedrijfsvoorschriften of uw geheimhoudingsplicht richting klanten. De gevolgen kunnen desastreus zijn, zoals het verlies van belangrijke informatie, mogelijk verlies van klanten en reputatieschade.

'Onbewust lekken' is een groot gevaar

Ook de privé USB-stick kan een potentiële bom zijn voor de informatiebeveiliging. Het zou goed kunnen dat uw werknemer een eigen USB-stick gebruikt om er informatie van het werk op te zetten, bijvoorbeeld een presentatie of documenten om thuis verder te werken. Op zich is daar niets mis mee, totdat deze werknemer in alle onschuld zijn oude USB-stick aan iemand anders weggeeft of verkoopt zonder de informatie erop volledig te wissen.

Of wat te denken van de werknemer die collega's vakantiefoto's wil laten zien via een USB-stick, en zo een virus van zijn thuis-PC op de computer op het werk overbrengt?

Mobiel werken werpt haar vruchten af. USB-portals vergemakkelijken het mobiele werken. Om tot een betere, meer geïntegreerde IT-beveiliging te komen en uw werknemers bewust te maken van het gebruik van zulke USB-portals, doet u er echter goed aan het gebruik ervan te beheersen. Software als DeviceLock van SmartLine maakt het voor systeembeheerders en IT managers mogelijk het gebruik van USB-portals te auditeren, registeren, beveiligen en controleren.

Gebruik van USB vereist adequaat beheer

Door de recente persberichten rondom zoekgeraakte USB-sticks komt er steeds meer aandacht voor beveiligde apparaatjes. Hiervoor zijn diverse methoden, één ervan willen we u nog even noemen: de biometrisch beveiligde USB-stick. Bijvoorbeeld na herkenning van de vingerafdruk van de

→