



Heeft u nog zicht op uw bedrijfsgegevens?

Organisaties delen meer en meer gegevens met elkaar. Gedreven door de mogelijkheden die de techniek biedt, is data veel mobieler geworden dan een aantal jaren geleden. Door de mogelijkheden van het internet, kunnen gegevens onderling gekoppeld worden. Medewerkers werken niet langer op één vaste lokatie, maar werken thuis, op kantoor, in de trein, etc. McAfee heeft deze maand een onderzoeksrapport uitgebracht, waarin de dreigingen m.b.t. dataverlies en compromittatie van data worden beschreven. McAfee heeft het onderzoek uitgevoerd onder 300 kantoormedewerkers in de Verenigde Staten, uit organisaties met tenminste 200 medewerkers. Meer dan 2/3 van deze medewerkers werken in organisaties met meer dan 1000 medewerkers. Conclusie van McAfee is dat, ondanks de vele maatregelen die in deze organisaties zijn getroffen om data te beschermen, er nog steeds grote risico's zijn m.b.t. verlies of compromittatie van data ten gevolge van het gedrag van deze medewerkers. De volgende percentages uit het onderzoek spreken voor zich:

- 21% geeft toe confidentiële of gevoelige documenten bij de printer te laten liggen;
- 26% vernietigt geen confidentiële of gevoelige documenten, wanneer niet meer nodig;
- 23% gebruikt (privé) WEBmail om bedrijfsgegevens naar buiten te brengen;
- 22% leent mobiele gegevensdragers (o.a. USB-sticks) uit aan collega's;

Ruim de helft (55%) van de respondenten gebruikt een draagbaar medium om confidentiële of anderszins gevoelige informatie mee te kunnen nemen buiten de organisatie. Een draagbaar medium is in dit geval:

- een laptop (41%)
- een USB memory stick (22%)
- een CD-ROM (13%)
- mobiele telefoon of blackberry (3%)



Bij gevoelige informatie moet worden gedacht aan:

- klantgegevens (48%)
- financiële gegevens van de organisatie (36%)
- gegevens over medewerkers (31%)
- officiële stukken (contracten e.d.) 28%



Dat de ondervraagde medewerkers slordig met de informatie en informatiedragers omgaan blijkt wel uit het feit dat 17% een draagbaar medium wel eens achterlaat in een openbare ruimte, 17% wel eens een informatiedrager uit een tas of zak heeft laten vallen en 8% wel eens slachtoffer geweest is van diefstal van een dergelijk medium.

Anno 2007 staat informatie niet meer veilig centraal opgeborgen in een organisatie, maar wordt verspreid via (WEB)mail, USB sticks, PDA's, laptops etc. Op deze manier is een organisatie erg afhankelijk geworden van het beveiligingsbewust gedrag van haar medewerkers. Meer en meer leidt een te weinig restrictief beleid ten aanzien van het (mobiel) gebruik van bedrijfsgegevens in combinatie met het slordig gedrag van medewerkers tot ernstige incidenten.

Gelet op de strengere wetgeving op het gebied van compliancy, zoals de Sarbanes-Oxley act, kan dit slordige gedrag van medewerkers, de organisatie serieus in de problemen brengen.

Organisaties doen er verstandig aan om behalve de aandacht voor dreigingen vanuit de "boze buitenwereld" meer aandacht te gaan besteden aan de beveiliging van mobiele data. Dit kan een combinatie van technische en organisatorische maatregelen zijn. Technisch kan worden afgedwongen dat data bijvoorbeeld niet op USB sticks kan worden gecopieerd, of alleen op specifieke devices, waarbij de data encrypted is.

Het rapport is te downloaden in pdf op <http://www.mcafee.com/us/>

Nieuws op assutools.com

Opmerkelijk nieuws is dat het aantal zombie PC's (PC's die door de introductie van een trojan horse bestuurd kunnen worden door een internet crimineel) in maart scherp is gestegen van 400.000 begin maart tot 1.200.000 deze week. Lees meer op <http://www.assutools.com/news/recent.htm>.

Verder een uitgebreider artikel over code injection:

<http://www.assutools.com/news/strategies/code-injection.htm>

Actueel

ABN/AMRO doelwit van malware aanval

ABN Amro klanten hebben op 22 maart 2007 een nepmailtje ontvangen met de mededeling dat ABN AMRO overging naar SSL 3.0. Dit vanwege een vermeend lek in SSL 2.0.

Aan de klanten werd verteld dat men de bijgevoegde executable moet starten om toch te kunnen blijven werken.

Het nep emailtje is in zeer slecht Nederlands in te zien op de site van ABN/AMRO.

De executable bevat Trojan Spy W32/Agent.QY, een variant van de Banker familie, Trojan-Spy.Win32.Banker.cmb. Dit zijn keyboard loggers.

Hoewel de email, die uit naam van support@abnamro.nl is verstuurd, niet bepaald professioneel is te noemen, zijn er helaas toch altijd weer slachtoffers.

Een bank zal nooit executables aan klanten verspreiden via email.

Een ander opvallend punt uit dit emailtje is dat gesproken wordt over de update naar SSL 3.0. Het is inderdaad al langer bekend dat SSL 2.0 niet veilig is en aangenomen zou mogen worden dat ABN AMRO al langer op SSL 3.0 is overgestapt.

Alleen de oudere versies van de Internetbrowsers ondersteunen geen SSL 3.0.

Bronnen:

https://www.abnamro.nl/nl/overabnamro/internetcrimineeliteit.html?pos=lb_20070321_nepsite

<http://www.waarschuwingsdienst.nl/>