

E-accounting en security

Erwin Vercammen
Accountant – Belastingconsulent

E-accounting behelst niet enkel het gebruik van computers, programma's en elektronica, maar heeft ook betrekking op de er noodzakelijk mee gepaard gaande beveiliging. Onze dagelijkse auditactiviteiten leren immers dat problemen niet altijd het gevolg zijn van frauduleuze of corrupte praktijken, maar ook kunnen voortvloeien uit onschuldige foutieve of onvakkundige handelingen. Deze problemen kunnen resulteren in een verlaagde productiviteit. Het hoeft dan ook geen betoog dat storingen in de werking van het informaticasysteem een doorn in het oog zijn voor menig kantoor. Tegen de achtergrond van dit laatste vonden wij het dan ook passend om hierna een licht te werpen op de beveiligingsproblematiek.

Beveiliging situeert zich op diverse vlakken die door de gebruiker moeten worden erkend en gerespecteerd.

Vooreerst verdient de *toegangsbeveiliging op het niveau van de verbinding* een bijzondere aandacht. Wanneer we gebruik maken van een ASP-omgeving wordt niet enkel de back-upfunctie, maar ook de toegangscontrole en andere beveiliging door de ASP-provider van ons overgenomen. Een dankbare outsourcing. Vergeet hierbij evenwel niet dat u zelf de toegang tot uw persoonlijke pc en/of uw netwerk moet organiseren. Vele confraters doen hiervoor terecht een beroep op een externe firma. In dit verband is het belangrijk om een contract op te stellen waarin niet enkel een aantal activiteiten worden beschreven, maar waarin ook een resultaatsverbintenis wordt aangegaan. Uiteraard zal er hierbij sprake zijn van "normaal gebruik" en van handelen "naar best vermogen", waardoor nog altijd geen 100 % beveiliging wordt gegarandeerd.

Het verdient aanbeveling om een hardware-firewall te installeren. Dat is een toestel, voorzien van software, dat de toegang via internet (ADSL of kabel) regelt alvorens de informatie op uw computer(s) toekomt.

Daarnaast is het noodzakelijk om een software-firewall te installeren, die met meer accurate en up-to-date informatie inbreuken op uw systeem belet.

De toegangsrechten op het niveau van de mappen en bestanden zijn aangelegenheden die binnen ieder kantoor moet worden geregeld, eventueel in samenspraak met een netwerkverantwoordelijke. Ook dat kan u uitbesteden.

Zelf kan u erop toezien dat de instellingen via de eigenschappen van bestanden worden geregeld. Dat kan via de tabkaart "Delen" of "Delen van bestanden". Moeilijk is dat niet en na enig experimenteren kan u zelf, via een andere computer in uw netwerk, nagaan of er voldoende rechten werden toegekend.

De grootste bedreigingen worden echter gevormd door de dagelijkse spammail en virussen die het professionele leven van accountants en belastingconsulenten verstoren. Vaak leiden zij ook tot de nodige paniek en irritatie. Uiteraard is dat terecht! Een massa bedreigingen komen op ons af. Hieronder worden er enkele omschreven.

- *Spam* is ongewenste e-mail die in bulk wordt verzonden.
- *Malware* is elke vorm van kwaadaardige of schadelijke software.
- *Spyware* is elke vorm van software die gebruik maakt van uw internetverbinding om gegevens te verzamelen en te verzenden.

- *Adware* is software die advertenties vertoont op uw scherm en eventueel gebruik maakt van uw internetverbinding om gegevens door te sturen.
- *Browser hijacker* is kwaadaardige software die instellingen aan uw internet browser verandert, zoals de startpagina, de balken met icoontjes enz.
- *Phishing* is een criminele vorm van identiteitsdiefstal via elektronische weg. Dit kan via advertenties of e-mails van internationale banken e.d.m.
- *Trojaanse Paarden* zijn kleine bestandjes die met e-mails of gratis programma's op je harde schijf terecht komen, of die er rechtstreeks op worden geschreven door hackers en zich "nestelen" om zich vervolgens verder te verspreiden. Ze kunnen data of programmabestanden aantasten of er delen van vernietigen.
- *Virussen* zijn programma's die op uw vaste schijf worden geïnstalleerd en zichzelf verzenden met kwaadaardige bedoelingen, zoals bijvoorbeeld bestanden of delen van bestanden vernietigen of onbruikbaar maken;
- Een *hacker* is iemand die ongewild, en soms met criminele bedoelingen, toegang tot uw computer "neemt".

Voor een gedetailleerde omschrijving en de bestrijding van deze verschillende boosdoeners, moeten wij u doorverwijzen naar gespecialiseerde ondernemingen en vakliteratuur. Het is in dit verband essentieel dat binnen uw kantoor de nodige acties worden ondernomen om elke vorm van bedreiging af te wenden. Daarvoor zal u verschillende software moeten aanschaffen, die – indien mogelijk – kan worden gebundeld aangezien beveiligingssoftware niet zelden conflicten veroorzaakt. Een goede voorlichting is dan ook noodzakelijk.

Het is eveneens belangrijk om de organisatie van de backups te onderwerpen aan een kritische blik. Het kan en mag niet mogelijk zijn om bestanden te back-uppen die besmet (kunnen) zijn met virussen, trojans, malware e.d. Ook in dat opzicht zal u derhalve de nodige omzichtigheid aan de dag moeten leggen.

Ten slotte wensen wij erop te wijzen dat de volgende principes worden gehuldigd in het kader van computerbeveiliging, nl.:

- de moeilijkst te beveiligen locatie is de laatste meter;
- de moeilijkst te beveiligen apparatuur is de mobiele apparatuur.

Het eerste principe duidt op de afstand van ons geheugen of onze handen tot de pc zelf. We kunnen immers elke vorm van beveiliging ongedaan maken door ze zelf te omzeilen of te neutraliseren. Het verdient aanbeveling hiermee rekening te houden bij de installatie en het onderhoud van uw beveiligingsprogramma's.

Ook uw naaste medewerkers kunnen soms ongewenst malware toelaten tot uw systeem door via diskettes, USB memory-sticks enz. programma's of data te kopiëren naar uw systeem. Zorg dus voor goede afspraken i.v.m. het gebruik van externe geheugens, alsook van de connectie via kabel of WIFI (wireless internet) door laptops, PDA's, smartphones enz. Hierin schuilen immers grote besmettingshaarden.

Onlangs opende minister Marc Verwilghen nog een praktische website die alle wapens aanreikt om de gevaren en bedreigingen van het internet in de kiem te smoren, m.n. <http://www.spamsquad.be>. We kunnen u enkel aanraden om deze site eens uitgebreid te raadplegen.

Besluit

Er bestaan diverse mogelijkheden om gratis online scanning te organiseren inzake antivirus, antispyware enz.

Het is in ieder geval raadzaam om een goed antivirus/antispywareprogramma te installeren en regelmatig uw vaste en variabele schijven te laten controleren.

Het is extreem belangrijk dat u voorzichtig bent en niet willekeurig allerlei dubieuze websites bezoekt, onbekende software downloadt en installeert, of verdachte mails opent en bekijkt. Uiteindelijk vloeien de meeste besmettingen nog steeds voort uit eigen handelen...

Veel succes! ●