Nederlandse Vereniging voor Arbeids- en Bedrijfsgeneeskunde nvab

De bedrijfsarts en het gebruik van bedrijfsgeneeskundige informatiesystemen

In de dagelijkse praktijk blijkt er door bedrijfsartsen met diverse automatiseringssystemen te worden gewerkt. Aspecten als doelmatigheid, privacy en kwaliteit moeten dan voldoende gewaarborgd zijn.

De NVAB richt zich op de totstandkoming van een betere informatievoorziening rondom en voor de patiënt/cliënt met behulp van ICT. Het uiteindelijke doel is het bereiken van een hogere doelmatigheid en kwaliteit van ICT in de bedrijfsgeneeskundige zorg. Daarom ontwikkelde de NVAB een programma van eisen waaraan een bedrijfsgeneeskundig informatiesysteem (BIS) moet voldoen. De NVAB gaat deze typekwalificatie in de toekomst ook toetsen.

Vooruitlopend op het toetsen van verschillende BIS-en aan het volledige programma van eisen gaat de NVAB in dit document in op de beveiliging van bedrijfsgeneeskundige informatiesystemen.

Hoe weet een bedrijfsarts dat het systeem goed beveiligd is en wat kan een bedrijfsarts zelf bijdragen aan de beveiliging van medische gegevens?
Hoe weet een bedrijfsarts dat het systeem bij bijvoorbeeld de arbodienst of een klant veilig is?
De eisen voor beveiliging en privacy van systemen in de zorg zijn vastgelegd in NEN-norm 7510 (www.nen7510.org). NEN heeft een brochure uitgebracht met de belangrijkste informatie. De volledige norm en het bijbehorende praktijkboek kunt u – tegen betaling – bestellen via www.nen7510.org.

Het is echter niet nodig dat de bedrijfsarts zelf de software toetst of test. De arbodienst, de klant of de softwareleverancier (wanneer bedrijfsarts zelf een systeem aanschaft) moet aan de bedrijfsarts, via specificaties, kunnen aantonen dat het systeem voldoet aan de gestelde eisen volgens NEN 7510.

In 2001 heeft de KNMG een brochure gepubliceerd over de privacy en omgaan met patiëntgegevens waarin ook handige en praktische informatie staat over dit onderwerp.

Hoe kan een bedrijfsarts zelf zo veilig mogelijk omgaan met computers, laptops, USB-sticks, bedrijfsgeneeskundige informatiesystemen?
De NVAB heeft een aantal adviezen en tips voor bedrijfsartsen verzameld. Het gaat om tips voor wachtwoordbeveiliging en om uw computer en netwerk veilig te houden.

NVAB, 10 mei 2012

Tien tips voor een betere wachtwoordbeveiliging

(bron: http://www.bestedownloads.nl/tips/10-tips-voor-betere-wachtwoordbeveiliging)

Wachtwoorden moeten gevoelige informatie beschermen. Ze zijn de sleutel om websites waar u lid van bent te kunnen bezoeken. Het is makkelijk voor te stellen wat voor vervelende zaken er kunnen gebeuren als een onbevoegde uw wachtwoord ontdekt. Hier wat tips om dat minder gemakkelijk te maken.

1. Het lijkt een open deur, maar gebruik geen makkelijk te raden wachtwoorden zoals uw geboortedatum, de naam van uw partner of uw huisdier. Gebruik dus liever geen wachtwoorden die te maken hebben met uw privéleven. U hebt een wachtwoord nodig dat niet gemakkelijk te raden is, maar dat voor uzelf wel makkelijk te onthouden is.
2. Gebruik een combinatie van kleine en hoofdletters en symbolen en getallen om het moeilijker te maken het wachtwoord te raden. Sommige websites staan het gebruik van symbolen niet toe, dus die zijn niet altijd te gebruiken. De meeste websites gebruiken wachtwoorden als case sensitive (hoofdlettergevoelig) dus hoofdletters gebruiken is dan een goed idee.
3. Maak een wachtwoord langer dan 8 karakters. Hoe langer het wachtwoord, hoe moeilijker het te raden valt.
4. Nog zo'n open deur. Gebruik een verschillend wachtwoord voor elk programma of website. Mocht uw wachtwoord in onbevoegde handen vallen, dan zijn tenminste andere accounts of websites nog wel beschermd.
5. Verander wachtwoorden regelmatig, als dit al niet door de website van bijvoorbeeld een bank geëist wordt. Minimaal éénmaal per jaar is verstandig.
6. Schrijf wachtwoorden nergens op. Je weet nooit wie er in uw laden of ergens anders snuffelt. Sla uw wachtwoorden ook niet op in uw PDA. Dat is net zo onveilig als een stukje papier. Wat u wel kunt doen is uw wachtwoorden op een beveiligde USB-stick opslaan (zie het gratis Cryptainer). Er zijn passwordmanagers die wachtwoorden versleuteld opslaan. Wanneer u met een USB-stick werkt, gebruik dan een programma dat de bestandsinhoud verbergt. Dat is dubbel veilig. U kunt ook gebruik maken van een programma als Roboform. Dit programma slaat wachtwoorden ook beveiligd op en vult ze bovendien automatisch in op websites die u bezoekt. Hoeft u helemaal niets te onthouden. De Roboform bestanden kunt u ook op een USB-stick opslaan. Kijk voor wachtwoordmanagers en Roboform hier.
7. Deel nooit uw wachtwoord aan iemand anders mee. Is het toch nodig om het te doen, verander het dan onmiddellijk daarna.
8. Gebruik geen woorden die in het woordenboek staan. Er zijn password-cracking programma's die naar deze woorden zoeken om een wachtwoord te kraken. Een goede tip is om zelf wachtwoorden samen te stellen die eenvoudig te onthouden zijn. Stel u reist elke dag per trein naar uw werk. U bedenkt de volgende wachtwoordzin: "Ik reis elke dag met de trein van 9 uur 45 Neemt dan van elk woord de eerste letter + de cijfers. Uw wachtwoord wordt dan: iredmdtv9u45. U kunt ook nog kleine en grote letters husselen. Het wachtwoord is dan bijvoorbeeld: IrEdMdTv9U45.
9. Gebruik natuurlijk nooit als wachtwoord "wachtwoord" of "geen". Zelfs niet "WachtWoorD"!
10. Tot slot, als u een email ontvangt of iemand belt u met de mededeling dat ze van uw bank of uw creditcardmaatschappij of van PayPal of welk bedrijf dan ook waar u een wachtwoord bij hebt zijn, geef ze NOOIT uw wachtwoord of PIN welk verhaal ze ook vertellen. Dit zijn gewoon oplichters.

Tien tips om uw pc veilig te houden

(bron: http://www.gratissoftwaresite.nl/Top-tien-geboden-om-je-pc-veilig-te-houden?page=5)

In de jaren negentig had bijna niemand beveiligingssoftware op zijn Windows-pc. Toen kwamen de virussen en raakte iedereen ervan overtuigd dat je een virusscanner nodig had. Zo'n tien jaar terug begon de spyware-plaag, waarna anti-spyware en firewalls tot het collectieve bewustzijn van de pc-gebruikers doordrongen. Maar tegenwoordig lukt het zelfs niet meer om met bovengenoemde beveiligingssoftware alle malware af te stoppen. Het kraken en misbruiken van computers is big business geworden voor internet criminelen, die bankrekeningen plunderen en pc's in zogeheten botnets gebruiken om op grote schaal schadelijke acties uit te voeren.
Wat te doen om krakers en andere internet-misbruikers buiten de deur te houden? Deze tien tips zijn van belang om een pc veilig te houden.
Essentiële beveiligingssoftware is op een Windows-pc zeker nodig. Maar ook op een Mac is een virusscanner geen overbodige luxe meer.

1. Gebruik een (gratis) virusscanner.
   Zorg dat de virusscanner up-to-date is! Een betaalde virusscanner waarvan het abonnement verlopen is, is zinloos. Dan maar beter een gratis anti-virus applicatie downloaden.
2. Gebruik een (gratis) firewall.
   Er is geen aparte firewall nodig als u alle meldingen lastig vindt. Het is ook prima als de ingebouwde Windows Firewall aanstaat (Configuratiescherm | Beveiliging).
3. Gebruik (gratis) anti-spyware software.
   Als extra beveiliging kan het handig zijn om af en toe handmatig te scannen met een on demand malware-verwijderaar. Gebruik echter niet meerdere realtime (altijd draaiende) virusscanners of spyware-verwijderaars. Dat is onnodig en vertraagt de pc.
   Altijd updaten!
   De sleutel tot pc-beveiliging (voor zowel Windows, Mac OS X en zelfs Linux) is en blijft: houd alle software up-to-date. Beveiliging is namelijk een continu proces dat nooit ophoudt.
4. Update uw browser.
   Zorg dat u altijd de laatste versie van uw browser hebt. De meeste aanvallen vinden nu via internet plaats en de eerste verdedigingslinie is een browser zonder gaten. Sla dus nooit een browser update over! Google Chrome wordt automatisch geüpdated, dus daar hoef je niks voor te doen. Internet Explorer wordt via Windows Update geüpdated (de laatste versie voor Windows XP is IE8 en voor Vista en Windows 7 is dat momenteel IE9). Firefox en Opera updaten ook automatisch, maar maken daar nog wel melding van. Als u een heel oude versie van de browser hebt dan moet u naar Windows Update gaan (IE6, IE7) of handmatig de laatste versie downloaden (Firefox, Opera, Safari).
5. Update uw browser plugins.
   Internet criminelen maken tegenwoordig heel veel gebruik van lekken in browser plugins als Java, Flash en Adobe Reader. Laat dus de automatische updaters van deze plugins in de systeembalk aanstaan en sla geen update over! Java kan zelfs misschien beter verwijderd worden van uw pc.
6. Update alle software op je pc.
   Sla nooit Windows Updates over. Automatische Updates van Microsoft komen elke tweede dinsdag van de maand binnen. Hiermee wordt alle Microsoft-software automatisch geüpdated. Andere software kunt u zelf op updates controleren door bijvoorbeeld Secunia PSI. Ook Mac OS X en Linux krijgen automatisch beveiligingsupdates.
7. Gebruik gezond verstand.
   Internet is net als het echte leven: de meeste mensen zijn wel vriendelijk, maar er zijn ook veel kwaadwillenden.

- Klik nooit zomaar op verdachte bijlagen of linkjes in mail of chat.
- Een oeroude tip die geldig blijft. Met name pdf-bijlagen en Office-bestanden kunnen vergiftigd zijn met schadelijke scripts. En gevaarlijke zip- en exe-bestanden waren ook nog altijd rond. Uitnodigende linkjes in de mail kunnen u naar schadelijke websites lokken die uw pc besmetten. Denk dus goed na voor u klikt!

8. Kijk goed uit wat u binnenhaalt met p2p- en bittorrent-programma's.
   Op deze netwerken (waarmee bestanden gedeeld worden) staat heel veel schadelijk materiaal.
9. Klik nooit op linkjes in e-mails die zogenaamd van de bank zijn.
   Banken zullen NOOIT via e-mail vragen of u wilt inloggen of uw gegevens wilt wijzigen. Gooi dit soort e-mailtjes (die vaak ook vol taalfouten zitten) direct weg. Als u internet bankiert, controleer dan in de adresbalk of de url begint met https (de s staat voor een beveiligde verbinding) en www. naamvanjouwbank.nl (nep-websites hebben vaak hele lange adressen met andere namen na de www).
10. Download (gratis) software alleen uit vertrouwde bron.
    Als u op zoek bent naar (gratis) software download dan niet zomaar alles van elke website. Er zijn veel websites die schadelijke software ter download aanbieden, dus bezoek alleen vertrouwde adressen (zoals GratisSoftware.nl, of MajorGeeks of FileHippo) of de officiële website van de producent.

Een tip die niet per se met beveiliging te maken heeft, maar wel handig is om onnodige werkbalken, veranderde zoekmachines en meer van dit soort ongein te voorkomen, is: let altijd goed op tijdens de installatie van software! Vaak wordt er onnodige extra software van derde partijen aangeboden tijdens de installatie. Lees dus alles goed en haal de vinkjes weg!
Op GratisSoftware.nl wordt altijd melding gemaakt van dit soort overbodige 'extraatjes' onder het kopje Installatie instructies.
Een bonustip is om over te stappen van Windows op een veiliger besturingssysteem zoals Ubuntu.

Meer lezen?

Hieronder vindt u enkele links naar relevante artikelen:

Hoe veilig is uw netwerk?
http://computertotaal.nl/software/25655-hoe-veilig-is-uw-netwerk.html
Uw netwerk is de achilleshiel van uw digitale bestaan. Hoe moet u het eigenlijk beveiligen? En hoe weet u dat uw netwerk nog veilig genoeg is? Weet u zeker of uw netwerk nog wel schoon is? Misschien zijn hackers al tijden op uw netwerk actief, zonder dat u dat weet. Door de beveiligingsinstellingen van uw netwerk regelmatig bij te werken, weet u zeker dat u veilig kunt computeren.

Veiliger computergebruik
http://computertotaal.nl/software/23245-veiliger-computergebruik.html
De meeste mensen zorgen er wel voor dat hun huis goed is beveiligd, maar zijn minder secuur als het om de toegang tot hun thuisnetwerk, computers en opgeslagen bestanden gaat. Als u alles goed dicht wilt timmeren, komt u er niet met de installatie van een enkel antivirusprogramma. Op deze pagina vindt u de tien belangrijkste veiligheidslekken, en hoe u ze kunt dichten.