Beveiliging van patiëntendata op de pc van de huisarts – een praktijkverbeterend project

Karel Anseeuw, Vrije Universiteit Brussel

Promotor: Prof. Dr. Dirk Devroey

Master of Family Medicine

Masterproef Huisartsgeneeskunde

Dankwoord

Hierbij wil ik alle mensen bedanken die mij geholpen hebben bij dit praktijk-verbeterend project. Bijzondere dank gaat uit naar mijn collega huisartsen en secretaresses in mijn opleidings-praktijk, zonder jullie medewerking was dit niet gelukt. Ook mijn Vriendin Eline Beckers wil ik bedanken voor de steun tijdens het schrijven en het proeflezen.

Anseeuw Karel

Inhoudsopgave

Abstract..... 3

Inleiding..... 4

Methode..... 6

Vragenlijst..... 6

Observaties in de praktijk..... 11

Resultaten..... 13

Vragen aan de artsen, secretaresses en systeembeheerder..... 13

Bevindingen beveiligingsrisico's in de praktijk..... 26

Identificatie zwakke punten 28

Perceptie..... 28

Fysieke beveiliging..... 27

Computerhygiëne – Software-matige beveiliging 30

Paswoordgebruik..... 32

Voorstellen tot verandering 34

Evaluatie verbeteringen 37

Conclusie..... 41

Discussie..... 42

Referenties..... 44

Bijlagen..... 44

Goedkeuring Ethische commissie..... 44

Protocol..... 46

Vragenlijst voorgelegd aan de artsen, secretaresses en systeembeheerder..... 48

Richtlijnen meegegeven aan de artsen, secretaresses en systeembeheerder..... 51

Abstract

Beveiliging van patiëntendata op de pc van de huisarts – een praktijkverbeterend project

Haio: Karel Anseeuw – Vrije Universiteit Brussel

Promotor: Prof. Dr. Dirk Devroey

Praktijkopleider: Dr. Philippe Thoné

Context:

De laatste 10 jaar heeft er een gestage digitalisering van de huisartsgeneeskunde plaats gevonden. Praktisch alle patiënten wordt nu digitaal opgeslagen. Deze nieuwe vorm van opslag breng naast de vele voordelen ook nieuwe verantwoordelijkheden met zich mee als de huisarts dit op een correcte en veilige manier wil doen.

Onderzoeksvraag:

Is het mogelijk om d.m.v. praktijkrichtlijnen de beveiliging van elektronisch opgeslagen patiëntendata te verbeteren?

P: 6 huisartsen werkzaam in de praktijk waar ik HAIO was voor de periode 2013-2015
I: Het opstellen en toepassen van richtlijnen met als doel de beveiliging van de elektronisch opgeslagen patiëntendata.
C: Er wordt een vergelijking gemaakt met de beveiliging van de elektronische patiëntendata voor en na het toepassen van opgestelde praktijkrichtlijnen met betrekking tot computerbeveiliging. Er was geen controlegroep.
O: De outcome is een antwoord op de vraag of een betere beveiliging van elektronische patiëntendata bekomen kan worden door het toepassen van hiervoor specifiek opgestelde praktijkrichtlijnen.

Methode:
De status van de computer-beveiliging in de praktijk werd nagegaan door observaties en een vragenlijst die werd ingevuld door de artsen, secretaresses en systeembeheerder van de praktijk. Op basis van de de naar voorgekomen pijnpunten werden richtlijnen opgesteld voor de artsen, secretaresses en systeembeheerder. De toepassing van deze richtlijnen en hun effect op de computerbeveiliging werd vervolgens gecontroleerd.

Resultaten:
Er werd een ernstige verbetering in de beveiliging van de elektronisch opgeslagen patiëntendata vastgesteld door het toepassen van de richtlijnen. Wel zijn er nog verschillende verbeterpunten vastgesteld.

Conclusie:
Het is mogelijk om d.m.v. praktijkrichtlijnen de beveiliging van elektronisch opgeslagen patiëntendata te verbeteren.

E-mail: anseeuw.karel@gmail.com

ICPC-code: computerbeveiliging kent geen ICPC code

I Inleiding

De laatste 10 jaar heeft er een gestage digitalisering van de huisartsgeneeskunde plaats gevonden. Papieren fiches zijn een zeldzaamheid geworden en praktisch alle patiënteninformatie wordt digitaal opgeslagen. Dankzij de voortdurende ontwikkeling van EMD-software kan de huisarts nu met meer efficiëntie en meer 'evidence based' praktijk voeren.

De overheid speelt hier een belangrijke stuwende rol door de telematicapremie die artsen jaarlijks ontvangen bij gebruik van gehomologeerde software. Ook voorziet zij met het ehealth-platform in een stevige basis waarop onderlinge elektronische dienstverlening en informatie-uitwisseling door andere partijen verder uitgebouwd kunnen worden. De achterliggende technologie voor dit platform werd reeds beproefd in de kruispuntbank van de sociale zekerheid die bekroond werd door de Verenigde Naties en de Europese Unie.[1] Dankzij het ehealth-platform wordt de digitale informatie-stroom van en naar de huisarts afdoende beschermd. Een keten is echter zo sterk als zijn zwakste schakel. En daar knelt vaak het schoentje zoals in mijn vorige masterproef 'Hoe is het gesteld met de beveiliging van de huisarts-pc?' naar voor kwam.[2]

Uit dit onderzoek bleek dat bij een groot deel van de onderzochte huisartsen de beveiliging van de pc in het kabinet ondermaats is. De vertrouwelijke patiënten-informatie opgeslagen op de harde schijven van de pc's van de huisarts is vaak erg slecht beveiligd, een pijnpunt dat niet enkel voorkomt bij huisartsen, maar ook in ziekenhuizen en bij andere partijen die omgaan met medische informatie. Dit werd pijnlijk duidelijk door de Koppen XL reportage over ethisch hacken waarin te zien was hoe makkelijk vertrouwelijke patiënten-informatie bij een huisarts en een universitair ziekenhuis gehackt kan worden.[3] Ook de kraak van de website van Mensura door de hacker 'Rex Mundi' waarbij naam, e-mailadres, rijksregisternummer en medische informatie van 1000 Belgen online werden gezet is hier een pijnlijke illustratie van.[4]

Naast het beveiligen van de informatie-stroom van en naar de huisarts moet ook de nodige aandacht besteed worden aan het beveiligen van de computer-apparatuur van de huisarts. Deze laatste wordt door de vorderende informatisering van zijn praktijk geconfronteerd met nieuwe uitdagingen omtrent de opslag van digitale patiënteninformatie. Als beheerder van de medische dossiers is hij verantwoordelijk voor een veilige opslag van deze data, maar uit mijn vorige masterproef blijkt echter dat huisartsen vaak niet over voldoende kennis beschikken om in een goede computer-beveiliging te voorzien.

Naast mijn studies geneeskunde ben ik sterk geïnteresseerd in informatica. Bij aanvang van mijn HAIO-jaren kwam mijn informatica kennis vaak van pas bij het oplossen van kleine computerproblemen in de praktijk waar ik werk. De artsen in de groepspraktijk stonden erg open voor verbeteringen en volgden de tips die ik hen meegaf i.v.m. veilig computer-gebruik op.

Toen ik de artsen polste over een eventueel praktijk-verbeterend project gericht op de beveiliging van de patiënten-informatie op de harde schijven van de computers in de praktijk werd dit met veel enthousiasme onthaald. Al snel kwam ik met een voorstel waarbij ik de computer-infrastructuur van de praktijk onder de loep zou nemen. In een tweede fase zou ik veranderingen introduceren d.m.v. praktijkrichtlijnen met als bedoeling de vastgestelde zwakheden te verhelpen. In een laatste fase zouden deze veranderingen op hun beurt ook geëvalueerd worden.

Ik wil met dit onderzoek nagaan of het mogelijk is de beveiliging van patiëntendata opgeslagen op de computers in de huisartspraktijk te verbeteren door het opstellen en toepassen van praktijkrichtlijnen rond computerbeveiliging.

De onderzoeksvraag luidt: **Is het mogelijk om d.m.v. praktijkrichtlijnen de beveiliging van elektronisch opgeslagen patiëntendata te verbeteren?**

II Methode

In een eerste deel van mijn onderzoek evalueerde ik de huidige status van de computer-beveiliging in de praktijk waar ik werk. Enerzijds liet ik de artsen, secretaresses en systeembeheerder een vragenlijst invullen. Anderzijds maakte ik een evaluatie van de computer-beveiliging in mijn praktijk door te controleren of de in mijn masterproef naar voor gekomen pijnpunten ook aanwezig zijn in mijn huidige praktijk d.m.v. een observatie van de computerinfrastructuur tijdens de periode dat ik als HAIO werkte in de praktijk.

1. Vragenlijst

Zoals eerder naar voor kwam in mijn masterproef is er geen geschikte gevalideerde vragenlijst over dit onderwerp specifiek voor huisartsen voor handen. Er bestaan wel vragenlijsten met als doelgroep apothekers maar deze zijn niet toepasbaar op de setting van mijn eerder en huidig onderzoek.[5] Naast deze enquête voor apothekers werden ook vragenlijsten gevonden i.v.m. de informatica-beveiliging in bedrijven, deze werden ook niet geschikt bevonden.[6] Om bovenstaande redenen werd besloten zelf een vragenlijst op te stellen die de verschillende aspecten van de computer-beveiliging in onze groepspraktijk bevraagt. Deze vragen zijn in verschillende categorieën in te delen.

1.1 Perceptie

In een eerste vragenreeks werd de perceptie van de huisartsen, secretaresses en informatica-beheerder bevraagd. Het is de bedoeling om d.m.v. deze categorie vragen te onderzoeken of er discrepanties zijn tussen wat de artsen, secretaresses en informatica-beheerder denken en de realiteit in de praktijk. *Zo werd aan de artsen gevraagd hoe ze de beveiliging van de computers in de praktijk inschatten en of ze die beter of slechter vinden dan die van andere praktijken. Wat vinden ze over hun eigen informatica-kennis? Zouden ze graag meer informatie ontvangen i.v.m. computer-beveiliging en vinden ze dat ze genoeg worden geïnformeerd over computer-beveiliging door de overheid en vakvereniging? Ook werd de artsen gevraagd of ze van mening zijn dat er bepaalde verplichtingen zouden moeten zijn naar artsen toe i.v.m. informatica-beveiliging? Zijn de artsen in de praktijk van mening dat ze voldoende inspanning leveren om voor een goede computer-beveiliging te zorgen? Hoe schatten ze hun score op het vlak van computer-beveiliging in vergelijking met andere collega's in? Hoe belangrijk vinden ze de beveiliging van de pc's in hun praktijk in het kader van een goede patiëntenzorg?*

De *secretaresses* werden dezelfde vragen gesteld waarbij vragen die niet van toepassing zijn weggelaten werden en extra vragen specifiek voor hen toegevoegd werden.

Aan de *systeembeheerder* werden volgende vragen gesteld: *Vindt hij dat de informatica-systemen in de praktijk voldoende beveiligd zijn? Is hij van mening dat hij voldoende tijd en middelen krijgt om in een goede beveiliging van de praktijk-computers te voorzien? Is hij van mening dat er in de praktijk hardware-matige en/of software-matige veranderingen nodig zijn om de computer-beveiliging in de praktijk te verbeteren? Vindt hij dat de dokters en secretaresses in de praktijk hun gedrag i.v.m. computer-beveiliging zouden moeten aanpassen om in een goede beveiliging van het ict-systeem in de praktijk te voorzien? Is hij er van overtuigd dat de artsen/secretaresses een goede computer-beveiliging belangrijk vinden? Denkt hij dat de artsen/secretaresses openstaan voor veranderingen die de beveiliging van de informatica ten goede zouden komen?*

1.2 Fysieke beveiliging van de pc

In dit stuk van de vragenlijst werd de fysieke beveiliging van de pc bevraagd. Hiermee wordt zowel bescherming van de fysieke toegang tot de informatica-structuur als bescherming tegen stroomuitval en kortsluiting bedoeld. Eerst worden de vragen aan de werknemers van de praktijk (artsen+secretaresses) overlopen om daarna de vragen aan de informatica-beheerder te overlopen.

Pc's en ander informatica hardware die toegankelijk zijn voor onbevoegden kunnen relatief makkelijk worden meegenomen. De data op de harde schijven in deze apparaten kan vervolgens worden geanalyseerd.[7] Niet geëncrypteerde informatie op deze schijven is erg makkelijk uit te lezen, geëncrypteerde informatie (bvb de patiëntengegevens opgeslagen in de database van de medische software) kan achterhaald worden d.m.v. 'brute-force'[a] technieken indien geen gebruik gemaakt werd van een goed paswoord. Ook Windows paswoorden kunnen achterhaald worden met beschikbare software.[8] Hiermee kan een kwaadwillend persoon zich vervolgens toegang verschaffen tot de andere systemen in de praktijk. *Om bovenstaande reden werd gevraagd aan de artsen en secretaresses of zij bij het verlaten van hun werkruimte (waar hun pc staat) deze afsluiten.*

Indien de pc's in de praktijkruimte niet voldoende afgeschermd zijn en deze bovendien niet afgemeld zijn uit Windows en de medische software, kan een kwaadwillend persoon zich direct toegang verschaffen tot de pc om patiëntengegevens te consulteren, te kopiëren of aan te passen. Ook het installeren van malware - zoals een keylogger[b]- is op dit moment erg makkelijk. *Om deze reden werd aan de werknemers van de praktijk (artsen + secretaresses) gevraagd of zij hun pc afmelden bij het verlaten van de ruimte waar hun pc zich bevindt.*

Externe opslagmedia (usb-stick/cd-rom/externe harde schijf) worden door malware frequent gebruikt als vector om computer-systemen te besmetten. Vaak gebeurt dit zonder dat de gebruiker het beseft. De recentelijk blootgelegde zwakheden in het usb protocol tonen bovendien aan dat het niet volstaat om een besmette usb-stick te wissen om de malware te verwijderen.[9] Het gebruik van externe opslagmedia die ook op andere (mogelijk besmette) systemen worden gebruikt is daarom zeker af te raden op een computer systeem waar vertrouwelijke (patiënten-)data op wordt bewaard. *Om deze reden werd gevraagd aan de werknemers van de praktijk of zij soms opslagmedia die buiten de praktijk worden gebruikt (bvb. voor privé-gebruik) aansluiten op de pc's in de praktijk?*

Computer-apparatuur heeft elektriciteit nodig om te werken. Buiten het feit dat een stroomonderbreking er voor zorgt dat de computers en servers in de praktijk uitvallen kan deze ook tot dataverlies leiden. Dit kan gaan van verlies van documenten die op dat moment weggeschreven worden naar de harde schijf tot zelfs verlies van gegevens die al weggeschreven waren[10]. Plots stroomverlies kan vermeden worden door het plaatsen van een UPS (uninterruptible power supply). Dit is een toestel dat bij uitval van het regulier stroomnet d.m.v. een ingebouwde batterij de aangekoppelde toestellen lang genoeg van stroom blijft voorzien om deze op een veilige manier af te sluiten zodat data-verlies vermeden kan worden. *Aangezien de aanwezigheid van een UPS essentieel is voor de veiligheid van de data op de informatica-infrastructuur werd aan de systeembeheerder gevraagd of een dergelijk toestel aanwezig is in de praktijk.*

Naast het wegvallen van de stroom kan een plotse stroompiek (bv. bliksem-inslag, slecht functionerende ballast van een TL-lamp) ook desastreuze gevolgen hebben. Dit kan gaan van het stuk gaan van de voedingen, over het doorbranden van het moederbord tot het demagnetiseren van de harde schijven met hiermee gepaard gaand data-verlies. *De aanwezigheid van een stroompiek-beveiliging werd eveneens bevraagd.*

---

a Bij een 'brute-force' aanval worden alle mogelijke opties uitgeprobeerd totdat er een werkend paswoord wordt gevonden.

b Een 'keylogger' is een programma dat alle toetsaanslagen registreert. Op deze manier kunnen paswoorden en logins verzameld worden.

Een essentieel onderdeel van een goede beveiliging van de patiëntendata op de computer-infrastructuur in de praktijk is het nemen van back-ups. Bij rampspoed kan d.m.v. deze back-ups de verloren data gerecupereerd worden. *Om deze reden werd bevraagd of er back-ups genomen worden van de data in de praktijk?* Het nemen van back-ups volstaat niet om de data te beschermen. Hoe frequenter deze back-ups genomen worden, hoe recenter de data op deze back-ups en dus hoe minder data-verlies er is. *Om deze reden werd nagevraagd hoe frequent er back-ups worden genomen in de praktijk.* Bij sommige gevallen van rampspoed zoals brand of overstroming is het mogelijk dat alle data aanwezig in de praktijk-ruimte getroffen wordt. Het is daarom van belang dat de back-ups bewaard (bv. externe harde schijven die elke avond worden meegenomen) of gemaakt worden op een plaats buiten de praktijk. *Om deze reden werd bevraagd op welk medium de back-ups worden genomen en of deze zich ook buiten de praktijk bevinden.*

Vandaag de dag wordt bijna alle computer-apparatuur aangesloten op het internet. Bij de computer-apparatuur van de praktijk is dit ook het geval. Door het veelvuldig gebruik van allerlei online informatiebronnen en services is internet in de praktijk onmisbaar geworden. Dit betekent wel dat alle data die op deze verbonden apparatuur staat afdoende dient te worden afgeschermd opdat onbevoegden zich hier geen toegang toe kunnen verschaffen. Hiervoor wordt best een hardware firewall gebruikt. Dit is a.h.w. een aparte computer die tussen het internet en het intranet van de praktijk hangt. Hij heeft als enige taak ongeoorloofde verbindingen te blokkeren en bevoegde verbindingen door te laten. *Er werd gekeken of er in de praktijk gebruik gemaakt wordt van een firewall.* Net zoals software op een pc regelmatig moet worden bijgewerkt met de nieuwste beveiligingsupdates is dit ook het geval met de firmware op de firewall. Elke dag worden er nieuwe manieren gevonden om de software van de firewall te omzeilen. Het is dus essentieel dat de firmware van de firewall zo snel mogelijk wordt bijgewerkt met beschikbare updates. *Om deze reden werd aan de systeembeheerder gevraagd hoe vaak hij de firmware op de firewall bijwerkt?*

1.3 Softwarematige beveiliging/ computerhygiëne

In dit stuk van de vragenlijst werd de software-matige beveiliging van de pc bevraagd. Voor de gebruiker is dit vooral de manier waarop hij met de computers omgaat, voor de administrator is dit vooral de manier waarop hij bepaalde software, met als doel de beveiliging van de pc, implementeert.

1.3.1 Computerhygiëne

Hiermee wordt de manier waarop de artsen en secretaresses omgaan met de softwarematige beveiliging op de pc bedoeld.

In de huisartsenpraktijk wordt veel gecommuniceerd met collega artsen. Dit kan via de klassieke manieren gebeuren zoals briefwisseling, telefonie en fax. Meer en meer wordt ook gebruik gemaakt van digitale communicatie. Dit kan via Medibridge, Hector al dan niet via het nieuwe ehealth-platform. Daarnaast wordt voor communicatie tussen huisartsen onderling (al dan niet van dezelfde groepspraktijk) soms ook gebruik gemaakt van email.

Medibridge en Hector die gebruik kunnen maken van het nieuwe ehealth-box platform zijn geschikt voor het uitwisselen van gevoelige patiënten-info. De informatie wordt via deze kanalen versleuteld en de identiteit van zender en ontvanger staat vast. Het is de bedoeling dat in de nabije toekomst elke arts met het ehealth-platform zal werken.

Bij klassieke email zijn deze beveiligingen niet voorhanden. Zo kan een kwaadwillend persoon berichten onderscheppen en meelezen. Ook kunnen bij email-verkeer berichten worden verstuurd in naam van iemand anders.[11] Dit probleem kan worden opgelost door gebruik te maken van encryptie.

Om bovenstaande redenen werd gevraagd aan de artsen of zij met collega artsen informatie over patiënten via email uitwissellen. Evenals werd gevraagd of dit email verkeer geëncrypteerd wordt. Ook werd aan de artsen gevraagd of ze reeds gebruiken maken van het ehealth-platform?

Ook al is de hardware- en softwarematige beveiliging in orde, dan kan een kwaadwillend persoon nog altijd aan confidentiële patiënteninformatie geraken door zgn. 'social engineering'[a] toe te passen. Hierbij gaat men een persoon die toegang heeft tot gevoelige gegevens er van overtuigen deze door te spelen, door zich voor te doen als een bevoegd persoon. *Om deze reden werd de werknemers van de praktijk gevraagd of ze telefonisch, per fax of via email patiënten-informatie doorgeven aan derden van wie ze de identiteit niet verifiëren.*

Een erg belangrijk onderdeel van de beveiliging van de informatica in de praktijk hangt af van paswoorden. Niet enkel de paswoorden zelf zijn van belang. Ook de manier waarop ze tot stand komen, hoe frequent ze vernieuwd worden, voor welke diensten ze worden gebruikt en hoe ze worden afgeschermd voor derden is van belang. Aan de artsen en secretaresses werden verschillende vragen gesteld i.v.m. hun wachtwoorden en de manier waarop ze deze gebruiken.

Volgens het SANS technology Insititute[12] moet een paswoord aan een aantal eigenschappen voldoen om een veilig paswoord te zijn. Zo moet een paswoord voldoende lang zijn. Korte paswoorden kunnen relatief makkelijk achterhaald worden door simpelweg alle mogelijke combinaties te proberen (dit wordt brute-forcing genoemd). Bij gebruik van langere paswoorden wordt dit een stuk moeilijker en tijdrovender. Daarom raadt het SANS technology institute aan om geen paswoorden korter dan 12 symbolen te gebruiken. *We vroegen aan de werknemers van de praktijk of hun paswoorden korter waren dan 12 symbolen?*

Net zoals het aan te raden is een voldoende lang paswoord te gebruiken is het ook aangewezen om cijfers, letters en/of leestekens te gebruiken. Dit maakt het erg moeilijk om het paswoord te kraken met een brute-force attack. *Om deze redenen werd de artsen en secretaresses gevraagd of hun paswoorden bestaan uit een combinatie van letters en leestekens, letters en cijfers, leestekens en cijfers of letters, leestekens en cijfers.*

Eveneens volgens de richtlijnen van het SANS technology Institute[12] zou elk paswoord minimaal om de 6 maand moeten worden veranderd. *Om deze reden werd aan de werknemers van de praktijk gevraagd of ze hun paswoorden regelmatig veranderen met een minimum van 1x per half jaar.* Bij verschillende diensten (bv. Medisch labo) krijg je wanneer je je aanmeldt een eerste wachtwoord dat je zelf dient te veranderen nadat je de eerste maal bent ingelogd. Deze verandering wordt meestal aangemoedigd door de leverancier van de diensten. In de praktijk gebeurt het echter vaak dat gebruikers nalaten dit te doen. *Om deze reden werd nagevraagd of de werknemers van de praktijk dit standaard wachtwoord veranderen zoals gevraagd door de leverancier?*

Een aantal frequent voorkomende fouten zorgen er voor dat een paswoord makkelijk te raden is, bv. een paswoord gebruiken dat gelijk is aan de gebruikersnaam. A*an de artsen en secretaresses werd gevraagd of ze gebruik maken van een paswoord dat gelijk is aan de gebruikersnaam voor die toepassing?*

Ook het hergebruik van paswoorden voor verschillende toepassingen is nefast voor de veiligheid. Dit kan er toe leiden dat wanneer het paswoord voor één toepassing gekraakt wordt al de andere toepassingen waarvoor dit paswoord wordt gebruikt onbeschermd zijn. *Om deze reden werd nagevraagd of de werknemers in de praktijk hun paswoorden hergebruiken voor verschillende toepassingen?*

Een andere gemaakte fout is een paswoord gebruiken dat (gedeeltelijk) uit de naam van een familielid of een huisdier bestaat. Deze paswoorden zijn erg kwetsbaar voor social-engineering.[13] *Om deze reden werd nagevraagd of dit het geval was met de paswoorden gebruikt in de praktijk?*

a Met 'Social Engineering' wordt die techniek bedoelt waarbij de hacker zich voordoet als iemand anders om zich zo informatie verschaffen waar hij anders geen toegang toe heeft.

Ook werd nagevraagd of sommige van de paswoorden gebruikt door de artsen en secretaresses (gedeeltelijk) zijn opgebouwd uit woord(en) die terug te vinden zijn in een woorden boek en/of deze (gedeeltelijk) bestaan uit een opeenvolgende reeks van letters/tekens (bvb 123456789, abcdefg,...)? Indien dit het geval is,is het namelijk mogelijk het wachtwoord te achterhalen d.m.v. een 'dictionary attack'[a].

Zoals hierboven beschreven is de manier waarop een paswoord samengesteld wordt erg belangrijk. Een sterk paswoord is echter van weinig nut als het ergens makkelijk te lezen is.[12] Net zoals een paswoord niet mag worden opgeschreven mag het ook niet gedeeld worden met anderen aangezien het strikt persoonlijk is. Het gebeurt echter dat deze regels -vaak om praktische redenen- niet opgevolgd worden.[12] *Om deze redenen werd aan de werknemers van de praktijk gevraagd of ze ergens hun paswoorden hebben opgeschreven of hebben gedeeld met derden? Ook werd aan de systeembeheerder gevraagd of hij de paswoorden voor het medisch programma van de artsen kent en of hij toegang heeft tot de patiëntengegevens op de pc?*

Er werd aan de werknemers van de praktijk gevraagd of ze van mening zijn dat hun paswoorden moeilijk te raden zijn? Hiermee wordt nagegaan of er een discrepantie is tussen wat de werknemers van de prakijk denken en de realiteit.

Als afsluiter van deze categorie werd er gevraagd aan de artsen en secretaresses of ze graag informatie hadden ontvangen over hoe ze een veilig paswoord kunnen kiezen? Dit om na te gaan of er een vraag is naar informatie hierover.

1.3.2 Softwarematige beveiliging

In deze categorie werden de vragen over softwarematige beveiliging besproken.
Eén van de voornaamste bedreigingen voor computer-apparatuur is malware. Hiermee wordt kwaadaardige software zoals virussen, worms, trojans, adware en spyware bedoeld die de bedoeling heeft gevoelige informatie te verzamelen, toegang te krijgen tot private computersystemen of computersystemen te verstoren in het algemeen. Voor een adequate computer-beveiliging is het essentieel dat alle computers en servers uitgerust zijn met antivirus-software opdat infectie door malware vermeden, bestreden en gedetecteerd kan worden. Om deze reden werd volgende vraag gesteld: *Zijn de computers in de praktijk beschermd tegen malware d.m.v. een antivirus-programma?*

Aangezien er continu nieuwe malware geschreven wordt is het erg belangrijk dat antivirus-software regelmatig updates ontvangt zodat deze de nieuwe malware kan herkennen en de computers hiertegen kan beschermen. *Er werd gevraagd of de anti-virus software automatisch updates ontvangt?*

Meestal scant deze software elke dag automatisch oppervlakkig naar virussen. Zo worden de data in het werkgeheugen, alle geopende bestanden en alle geopende mappen gescand op aanwezigheid van malware. Bepaalde gesofisticeerde malware zoals rootkits kunnen zich vaak onder de radar houden door zich diep in de bestandenstructuur te nestelen of zich onzichtbaar te maken voor de antivirus-software. Soms kan een handmatige diepe scan van het systeem hier soelaas brengen. *Om deze reden werd gevraagd aan de administrator of hij regelmatig handmatige scans deed van het systeem?*

Praktisch alle medische software voor huisartsen is enkel beschikbaar voor het Microsoft Windows besturingssysteem. Onderzoek toont aan dat recentere versies van Microsoft Windows beter de pc waarop ze draaien beschermen tegen malware en andere bedreigingen.[14,15] Als beste scoort Windows 8.1 die over verschillende nieuwe beveiligingsmechanismen beschikt. Deze wordt gevolgd door Windows 7, Windows Vista en Windows XP. Deze laatste wordt niet meer ondersteund door Microsoft sinds april 2014.

a Een 'dictionary attack' of woordenlijstaanval is een techniek waarbij een aanvaller probeert een paswoord te achterhalen door het aftoetsen van een samengestelde lijst van mogelijkheden (bv. een woordenboek). Dit is een meer gerichte vorm dan een 'brute-force' aanval waardoor er een belangrijke tijdswinst kan behaald worden. Als het paswoord niet in de lijst staat zal het paswoord niet achterhaald kunnen worden en is een 'brute-force' aanval de enige overblijvende optie.

Dit betekent dat er voor nieuw ontdekte veiligheidslekken geen patches meer worden gemaakt en verspreid via updates. Het gebruik van een dergelijk systeem is een ernstige bedreiging voor de computer-veiligheid. Ook voor het besturingssysteem dat draait op de achterliggende servers die vaak gebruikt worden in groepspraktijken geldt hoe recenter de versie hoe meer de focus ligt op de bescherming tegen malware en en andere bedreigingen. *Om bovenstaande redenen werd nagevraagd welke besturingssystemen -op zowel de pc's als de server- worden gebruikt in de praktijk?*

Naar analogie met de updates die anti-virus software ontvangt, ontvangt een besturingssysteem ook updates. Hiermee worden nieuw ontdekte beveiligingslekken gedicht. In dit voortdurend kat en muis spel tussen ontwikkelaars en hackers komt het er op aan zo snel mogelijk de nieuwste patches te installeren. Om deze reden is het aangeraden in Windows automatisch deze updates te laten installeren van zodra ze beschikbaar zijn. *Er werd nagevraagd of dit op de systemen in de praktijk zo ingesteld is?*

Naast de antivirus-software en het besturingssysteem is het ook erg belangrijk de andere software regelmatig te updaten. Vaak wordt gebruik gemaakt van bugs in pdf-readers, office en andere veelgebruikte desktop-software om d.m.v. een exploit de computer waarop deze software draait te infecteren met malware. Ook hier komt het er op aan zo snel mogelijk de patch tegen deze exploits te installeren d.m.v. updates. *Om deze reden werd gevraagd aan de administrator of ook deze software regelmatig updates krijgt?*

Naast bovenstaande manieren kan een infectie van een computer systeem ook gebeuren door het handmatig installeren van besmette software. Een veelgebruikt kanaal voor het binnenloodsen van malware is gepirateerde software. Deze software die uit illegale bron wordt gedownload is vaak voorzien -zonder dat de gebruiker dit opmerkt- van malware. Bij installatie van deze software of bijgevoegde cracks[a] wordt op de achtergrond malware geïnstalleerd. *Omdat het gebruik van deze illegale software grote risico's met zich meebrengt werd de administrator gevraagd of er op de pc's software wordt gebruikt waar geen licentie voor betaald werd?*

Ook bij een pc die goed beveiligd is tegen virtuele bedreigingen bestaat het risico dat een kwaadwillend persoon de computer, server, nas of de harde schijven aanwezig in deze apparaten meeneemt. Een handige tool om te vermijden dat bij een dergelijke diefstal vertrouwelijke patiëntengegevens in handen vallen van een onbevoegde is het gebruik van encryptie. D.m.v. deze techniek worden alle gegevens versleuteld met een wiskundige formule waarna deze enkel nog uit te lezen zijn door personen die in het bezit zijn van de decryptiesleutel. Een kwaadwillend persoon die bv. door diefstal van de harde schijven de ruwe data in handen krijgt zal deze hierdoor niet kunnen uitlezen. Het gebruik van encryptie zorgt voor een goede bescherming van patiëntendata en heeft zeker zijn plaats in de huisartspraktijk. *Om deze reden werd bevraagd of in de praktijk ook gebruik wordt gemaakt van deze techniek op de verschillende computers, server en NAS[b]?*

1.4 Vragen i.v.m. preventieve maatregelen rond computer-beveiliging

Het is de taak van een systeembeheerder om pro-actief bezig te zijn met computer-beveiliging. Zo zou regelmatig een audit moeten gebeuren van de computer-beveiliging om eventuele gaten op te sporen. *Om deze reden werd gevraagd of er audits van de computer-beveiliging gedaan worden?*

Een ander pro-actieve maatregel is het opstellen van richtlijnen voor de artsen en secretaresses van de praktijk. *Om deze reden werd gevraagd of er een beleid is inzake veilig gebruik van de computers en meer specifiek een beleid naar veilig paswoord-gebruik.*

---

a Een 'crack' is een stukje software dat de kopieerbeveiliging omzeilt waardoor het mogelijk wordt software waarvoor je geen geldige licentie-sleutel hebt tocht te gebruiken.

b Een 'NAS' of network attached storage is een server waarop de backups worden opgeslagen.

2. Observaties in de praktijk

Naast de hierboven besproken vragenlijst werd de huidige situatie in mijn praktijk op het vlak van computer-beveiliging eveneens geëvalueerd d.m.v. observaties die ik deed tijdens de afgelopen periode als haio in mijn praktijk. Hiervoor heb ik gebruik gemaakt van de in mijn masterproef naar voor gekomen pijnpunten als leidraad.

III Resultaten

In dit deel worden de resultaten van de bevraging van de artsen, secretaresses en systeembeheerder besproken. Ook de bevindingen i.v.m. de computer-beveiliging, gedaan tijdens de afgelopen tijd die ik als haio in de praktijk doorbracht, worden besproken.

1. Vragen aan de dokters

1.1 Deel Perceptie

1. Hoe schat u de beveiliging van de computers in de praktijk in? (5 antwoordmogelijkheden van erg slecht tot erg goed)



De artsen hebben allen een verschillende inschatting over de veiligheid van de computers in de praktijk. Deze varieert van heel slecht over neutraal tot heel goed. Er is dus geen consensus onder artsen.

2. Hoe schat u uw kennis over informatica in het algemeen in? (5 antwoordmogelijkheden van erg slecht tot erg goed)



Eén van de vijf artsen schat zijn kennis als zeer slecht in. Twee van de vijf artsen schatten hun kennis als slecht in en twee artsen schatten hun kennis als neutraal. Uit deze antwoorden kan besloten worden dat de artsen in de praktijk hun kennis neutraal tot slecht inschatten.

3. Vindt u dat u genoeg wordt geïnformeerd door de overheid inzake computer-beveiliging?



Het overgrote deel van de artsen in de praktijk vindt dat de overheid tekort schiet i.v.m. het informeren van artsen over computer-beveiliging.

4. Vindt u dat u genoeg wordt geïnformeerd door uw vakvereniging inzake computer-beveiliging?



Het overgrote deel van de artsen in de praktijk vindt dat hun vakvereniging tekort schiet i.v.m. het informeren van artsen over computer-beveiliging.

5. Indien deze makkelijk beschikbaar was zou u dan graag meer informatie krijgen over een goede beveiliging van uw pc?



n = 5

Alle artsen in de praktijk zouden graag meer informatie krijgen over computer-beveiliging.

6. Vindt u het de taak van de huisarts om zich bezig te houden met computer-beveiliging?



n = 5

Slechts 2/5e van de ondervraagde artsen is van mening dat het de taak van de huisarts is zich bezig te houden met een goede computer-beveiliging.

7. Vindt u dat er bepaalde verplichtingen omtrent computer-beveiliging zouden moeten worden gesteld aan huisartsen?



n = 5

Het overgrote deel van de artsen vindt dat er bepaalde verplichtingen omtrent computer beveiliging zouden moeten gesteld worden.

8. Bent u van mening dat de beveiliging van de computers in uw praktijk beter is dan bij de gemiddelde huisartspraktijk?



n = 5

Een kleine meerderheid van de huisartsen is van mening dat de beveiliging in de praktijk beter is dan die bij collega-praktijken.

9. Bent u van mening dat u het nodige doet om een goede beveiliging van de computers in uw praktijk te verzekeren?



n = 5

Een kleine meerderheid van de huisartsen is van mening dat ze voldoende doen om een goede computer-beveiliging te garanderen.

10. Hoe goed scoort u volgens uzelf op het vlak van computer-beveiliging in vergelijking met uw collega's in de praktijk?



n = 5

Alle artsen in de praktijk zijn van mening dat hun kennis over computer-beveiliging even goed is dan die van hun collega-artsen.

11. Hoe belangrijk vindt u de beveiliging van de pc's in uw praktijk in het kader van een goede patiëntenzorg? (5 antwoordmogelijkheden van erg onbelangrijk tot heel belangrijk)



n = 5

Twee van de vijf artsen vinden de beveiliging van de pc's belangrijk in het kader van een goede patiëntenzorg, één noch belangrijk noch onbelangrijk en twee erg belangrijk. Evenveel artsen hechten hier minder als meer belang aan. De artsen hebben allen een verschillende inschatting over de veiligheid van de computers in de praktijk. Deze varieert van heel slecht over neutraal tot heel goed. Er is dus geen consensus onder de artsen.

1.2 Deel Fysieke beveiliging

1. Zet u uw pc uit of meldt u zich af uit Windows als u uw kabinet verlaat (korte periodes om naar het toilet te gaan of een nieuwe patiënt te halen uitgesloten)?



Iets minder dan de helft van de artsen sluit zijn pc niet af of meldt zich niet af uit Windows. Dit betekent dat iedereen die zich fysiek toegang kan verschaffen tot deze pc's ook alle gegevens (inclusief de patiëntendata via het medisch programma) kan consulteren, bewerken of verwijderen. Dit houdt vanzelfsprekend een ernstig veiligheidsrisico in.

2. Sluit u uw kabinet af als u het verlaat? (korte periodes om naar het toilet te gaan of een nieuwe patiënt te halen uitgesloten).



Meer dan de helft van de artsen geeft aan zijn kabinet niet af te sluiten. Dit houdt een veiligheidsrisico in aangezien een kwaadwillende zich hierdoor makkelijk fysieke toegang kan verschaffen. Hiermee kan hij makkelijk aan de pc's. Als deze afgesloten of uitgelogd zijn kan hij enkel aan de ruwe data op de harde schijven, als deze aanstaan en ingelogd zijn heeft hij onbeperkte toegang tot alle data op de computer evenals de patiëntendata via de medische programma's.

3. Sluit u soms opslagmedia (usb-stick/cd-rom/externe harde schijf) die u ook buiten de praktijk gebruikt aan op uw praktijk-pc? (bv usb stick die u ook gebruikt voor privé-gebruik)?



Meer dan de helft van de artsen geeft aan opslagmedia te gebruiken die ook buiten de praktijk worden gebruikt. Dit vormt een ernstig risico aangezien heel wat malware deze opslagmedia als vector gebruikt.

1.3 Deel Computerhygiëne

1. Communiceert u met uw collega-artsen (binnen en buiten de praktijk) over patiënten-dossiers via email?



Zestig procent van de huisartsen geeft aan over patiënten-dossiers te communiceren via email. Verdere navraag en verduidelijking bracht naar voor dat alle artsen in de praktijk reeds over patiënten communiceerden via email. Aangezien alle artsen tegenwoordig over een ehealth-box beschikken om beveiligd te communiceren, is het email-protocol, die de tekst onversleuteld verstuurd en waar bij geen zekerheid is van de identiteit van zender en ontvanger, een inferieure manier om dergelijke gevoelige informatie te versturen.

2. Wordt dit email-verkeer geëncrypteerd?



Geen enkele arts maakt gebruik van encryptie om zijn email berichten te versleutelen. Dit betekent dat de tekst in de verstuurde emails kan worden gelezen als deze mails worden uitgelezen.

3. Gebruikt u uw ehealth-box om te communiceren met collega artsen over patiëntendossiers?



Geen enkele arts maakt gebruik van zijn ehealth-box om te communiceren met collega artsen over patiëntendossiers. Zij laten de op dit moment meest veilige manier om te communiceren volledig links liggen.

4. Gebruikt u uw pc ook voor niet praktijk gerelateerde zaken?



De meerderheid van de artsen geeft aan zijn pc niet enkel te gebruiken voor praktijk gerelateerde zaken. Dit houdt in dat de pc aan meer gevaren wordt blootgesteld.

5. Geeft u telefonisch/per fax/via email informatie over patiënten door aan derden zonder dat u deze kent (bv een voor u onbekende collega die om informatie vraagt over een patiënt).



Meer dan de helft van de artsen geeft aan dat ze informatie doorgeven aan derden zonder dat ze de persoon kennen en ze zijn identiteit kunnen verifiëren. Dit betekent dat een kwaadwillend persoon zich d.m.v. social-engineering makkelijk vertrouwelijke patiënten-informatie kan verschaffen bij deze dokters.

6. Sommige van mijn paswoorden zijn gelijk aan mijn gebruikersnaam?



Meer dan de helft geeft aan dat zij voor sommige toepassingen een wachtwoord gebruiken dat gelijk is aan hun gebruikersnaam. Alle artsen gebruiken voor de medische software Windoc echter een wachtwoord dat gelijk is aan hun gebruikersnaam, en men kan dus aanmen dat het werkelijke antwoord in alle gevallen 'ja' is. Dit is een ernstige fout op het vlak van paswoordveiligheid.

7. Ik gebruik hetzelfde paswoord voor verschillende toepassingen?



Meer dan de helft geeft aan zijn/haar paswoord te hergebruiken voor verschillende toepassingen. Dit vormt een veiligheidsrisico aangezien bij het kraken van een wachtwoord van één enkele applicatie bijgevolg verschillende applicaties onbeschermd zijn.

8. Sommige van mijn paswoorden zijn korter dan twaalf symbolen?



De grote meerderheid van de artsen gebruikt één of meerdere paswoorden die korter zijn dan twaalf symbolen. Deze wachtwoorden zijn te kort om een goede beveiliging te bieden tegen brute-force aanvallen en kunnen bijgevolg dus relatief makkelijk achterhaald worden.

9. Mijn paswoorden bestaan uit een combinatie van letters en cijfers/ letters en leestekens/ cijfers en leestekens/ letters, cijfers en leestekens?



Meer dan de helft van de artsen gebruikt paswoorden die opgebouwd zijn uit een combinatie van letters en cijfers/ letters of leestekens/ cijfers of leestekens/ letters, cijfers en leestekens. Dit maakt het moeilijker het wachtwoord te achterhalen d.m.v. brute-forcing of een dictionary-attack.

10. Andere mensen kennen één/ meerdere van uw paswoorden?



Bijna alle dokters geven aan dat andere mensen één of meerdere van hun paswoorden kennen. Bovendien ken ik als haio van elke dokter minimaal één paswoord. Er kan dus gesteld worden dat het antwoord voor alle dokters positief is. Een paswoord mag enkel door de gebruiker gekend zijn om een goede veiligheid te garanderen.

11. Mijn paswoord(en) staat(n) ergens opgeschreven zodat ik ze makkelijk kan lezen (bvb post-it op pc)?



Eén dokter geeft aan dat zijn/haar paswoorden staan opgeschreven. Vanzelfsprekend is dit een groot veiligheidsrisico.

12. Is 1 van volgende stellingen van toepassing op u?
Mijn paswoord is/ bestaat gedeeltelijk uit
- naam van familielid/huisdier
- een bestaand woord dat in het woordenboek terug te vinden is
- een opeenvolgende reeks van letters of tekens (bvb 123456789, abcdefg,...)



De grote meerderheid van de artsen geeft aan dat één of meer van bovenstaande stellingen van toepassing zijn op zijn/haar paswoord. Dit betekent dat hun paswoorden relatief eenvoudig te achterhalen zijn d.m.v. dictionary-attacks en social-engineering.

13. Ik verander mijn paswoord(en) regelmatig (min. 1x om de 6 maand)?



Slechts 1 arts in de praktijk geeft aan regelmatig zijn/haar paswoorden te veranderen. Het regelmatig veranderen van het paswoord is 1 van de basisprincipes van een goed paswoordgebruik.

14. Ik denk dat mijn paswoorden makkelijk te raden zijn?



Het overgrote deel van de artsen is van mening dat zijn/haar paswoorden niet makkelijk te raden zijn. Afgaand op de antwoorden hierboven is dit denkbeeld een illusie.

15. Ik zou graag meer informatie ontvangen over hoe ik een goed paswoord maak?



Iets minder dan de helft van de artsen geeft aan graag informatie te ontvangen i.v.m. een goed

paswoordgebruik. Meer dan de helft van de artsen is hier niet in geïnteresseerd.

16. Als u zich inschrijft voor een bepaalde dienst (bvb het online raadplegen van labo uitslagen) dan krijgt u een standaard paswoord. Verandert u dit standaard paswoord na ontvangst?



n = 5

Op deze vraag antwoorden alle artsen positief. Ze scoren hiermee goed op het vlak van paswoordbeveiliging. Het actief aansporen van de artsen om hun paswoord te veranderen door deze diensten lijkt zijn effect te hebben.

2. Vragen aan de secretaresses

2.1 Deel Perceptie

1. Hoe schat u de beveiliging van de computers in de praktijk in? (5 antwoordmogelijkheden van erg slecht tot erg goed)



n = 2

De secretaresses schatten de computerveiligheid in de praktijk in van neutraal tot slecht. Volgens hen is er dus zeker ruimte voor verbetering.

2. Hoe schat u uw kennis over informatica in het algemeen in? (5 antwoordmogelijkheden van erg slecht tot erg goed)



n=2

De secretaresses schatten hun kennis i.v.m. informatica in van neutraal tot slecht.

3. Vindt u het de taak van de huisarts om zich bezig te houden met computer-beveiliging?



n = 2

Alle secretaresses in de praktijk zijn van mening dat huisartsen een verantwoordelijkheid hebben i.v.m. computer-beveiliging.

4. Vindt u dat er bepaalde verplichtingen omtrent computer-beveiliging zouden moeten worden gesteld aan huisartsen?



n = 2

Alle secretaresses in de praktijk zijn van mening dat er aan de huisartsen bepaalde verplichtingen moeten opgelegd worden i.v.m. computer-beveiliging.

5. Bent u van mening dat de beveiliging van de computers in uw praktijk beter is dan bij de gemiddelde huisartspraktijk?



n=2

De meningen zijn verdeeld.

6. Bent u van mening dat u het nodige doet om een goede beveiliging van de computers in uw praktijk te verzekeren?



n = 2

Beide secretaresses zijn er van overtuigd dat zij het nodige doen om een goede beveiliging van de computers te garanderen.

7. Hoe goed scoort u volgens uzelf op het vlak van computer-beveiliging in vergelijking met uw collega's in de praktijk?



n = 2

De ene secretaresse schat haar score even goed als haar collega in. De andere schat die slechter in.

8. Hoe belangrijk vindt u de beveiliging van de pc's in uw praktijk in het kader van een goede patiëntenzorg? (5 antwoordmogelijkheden van erg onbelangrijk tot heel erg belangrijk)



n = 2

Beide secretaresses vinden de beveiliging van de pc's in de praktijk erg belangrijk in het kader van een goede patiëntenzorg.

2.2 Deel Fysieke beveiliging

1. Zet u uw pc uit of meldt u zich af uit Windows als u uw bureau verlaat (korte periodes om naar het toilet te gaan uitgesloten).



n = 2

Eén van de twee secretaressen geeft aan dat zij de pc niet af sluit of zich afmeldt uit Windows. Dit betekent dat iedereen die zich fysiek toegang kan verschaffen tot deze pc ook alle gegevens (inclusief de patiëntendata via het medisch programma) kan consulteren, bewerken of verwijderen. Dit houdt vanzelfsprekend een ernstig veiligheidsrisico in.

2. Sluit u de schuifdeur die naar de balie leidt af als u de pc verlaat? (korte periodes om naar het toilet te gaan uitgesloten).



n = 2

Eén van de twee secretaressen geeft aan de balie niet af te sluiten. Dit houdt een veiligheidsrisico in aangezien een kwaadwillende zich hierdoor makkelijk fysieke toegang tot de pc kan verschaffen. Als deze afgesloten of uitgelogd is kan hij enkel aan de ruwe data op de harde schijven, als deze aanstaat en ingelogd is heeft hij onbeperkte toegang tot alle data op de computer evenals de patiëntendata via de medische programma's.

3. Sluit u soms opslagmedia (usb-stick/cd-rom/externe harde schijf) die u ook buiten de praktijk gebruikt aan op uw praktijk-pc? (bv usb stick die u ook gebruikt voor privé-gebruik)





n = 2

Beide secretaresses geven aan dat ze geen opslagmedia van buiten de praktijk gebruiken. Ze scoren hier mee beter dan de artsen op het vlak van computer-beveiliging.

2.3 Deel Computerhygiëne

1. Communiceert u met uw collega secretaresses of andere artsen (binnen en buiten de praktijk) over patiënten-dossiers via email?



n = 2

Beide secretaressen geven aan nooit via email te communiceren over patiënten. Hiermee scoren ze beter op vlak van computer-beveiliging dan de artsen in de praktijk.

2. Gebruikt u uw praktijk-pc voor niet praktijk gerelateerde zaken?



n = 2

Beide secretaresses geven aan hun pc enkel te gebruiken voor praktijkgerelateerde zaken. Hiermee scoren ze beter op vlak van computer-beveiliging dan de artsen.

3. Geeft u telefonisch/per fax/via email informatie door aan derden zonder dat u deze kent (bv een voor u onbekende collega die om informatie vraagt over een patiënt)?



n = 2

Beide secretaresses geven aan informatie te verstrekken aan derden zonder dat ze deze kennen en zijn identiteit kunnen verifiëren. Dit betekent dat een kwaadwillend persoon zich d.m.v. social-engineering makkelijk vertrouwelijke patiënten-informatie kan verschaffen bij deze secretaresses.

4. Sommige van mijn paswoorden zijn gelijk aan mijn login?



n = 2

Alle secretaresses geven aan dat zij voor geen enkele toepassing een wachtwoord gebruiken dat gelijk is aan hun login. Alle secretaresses gebruiken voor de medische software windoc en het telefoonsysteem echter een wachtwoord dat gelijk is aan hun usernaam, er kan dus aangenomen worden dat het werkelijke antwoord voor beide secretaresses ja is. Dit is een ernstige fout op het vlak van paswoordveiligheid.

5. Ik gebruik hetzelfde paswoord voor verschillende toepassingen?



n = 2

De helft van de secretaresses geeft aan voor verschillende toepassingen hetzelfde paswoord te gebruiken. Dit vormt een veiligheidsrisico aangezien er bij het kraken van dit wachtwoord van één enkele applicatie er bijgevolg verschillende applicaties onbeschermd zijn.

6. Sommige van mijn paswoorden zijn korter dan twaalf symbolen?



n = 2

Beide secretaresses geven aan dat ze paswoorden gebruiken die korter zijn dan twaalf

symbolen. Deze wachtwoorden zijn te kort om een goede beveiliging te bieden tegen brute-force aanvallen en kunnen bijgevolg relatief makkelijk achterhaald worden.

7. Mijn paswoorden bestaan uit een combinatie van letters en cijfers/ letters en leestekens/ cijfers en leestekens/ letters, cijfers en leestekens



Beide secretaressen geven aan dat hun paswoorden uit een combinatie van letters en cijfers/ letters en leestekens/ cijfers en leestekens/ letters, cijfers en leestekens bestaan. Dit maakt het moeilijker het wachtwoord te achterhalen d.m.v. brute forcing.

8. Andere mensen kennen één/meerdere van uw paswoorden?



Eén van de secretaressen geeft aan dat ander mensen één of meerdere van haar paswoorden kennen. Ik ken als HAIO minimaal één paswoord van beide secretaresses. Er kan dus gesteld worden dat het antwoord voor alle secretaresses positief is. Een paswoord mag enkel door de gebruiker gekend zijn om een goede veiligheid te garanderen.

9. Mijn paswoord(en) staat(n) ergens opgeschreven zodat ik ze makkelijk kan lezen (bvb post-it op pc)?



Beide secretaresses geven aan dat ze hun paswoorden nergens opgeschreven hebben. Dit klopt niet, er hangt namelijk een post-it met een paswoord voor de secretaresses achter de balie. Hiermee kan gesteld worden dat het antwoord op deze vraag positief is. Vanzelfsprekend is dit een groot veiligheidsrisico.

10. Mijn paswoord is/ bestaat gedeeltelijk uit
- naam van familielid/huisdier
- een bestaand woord dat in het woordenboek terug te vinden is
- een opeenvolgende reeks van letters of van tekens (bvb 123456789, abcdefg,...)



Eén secretaresse geeft aan dat één van bovenstaande stellingen van toepassing is op haar paswoorden. Dit betekent dat deze paswoorden relatief eenvoudig te achterhalen zijn d.m.v. dictionary-attacks en social-engineering.

11. Ik verander mijn paswoord(en) regelmatig (min. 1x om de 6 maand)?



Beide secretaresses geven aan dat ze hun paswoorden niet regelmatig veranderen. Het regelmatig veranderen van het paswoord is één van de basisprincipes van een goed paswoordgebruik.

12. Ik denk dat mijn paswoorden makkelijk te raden zijn?



Beide secretaresses zijn van mening dat hun paswoorden niet makkelijk te raden zijn. Afgaande op de antwoorden hierboven is dit voor één van de secretaresses eerder een illusie.

13. Ik zou graag meer informatie ontvangen over hoe ik een goed paswoord maak.



Eén secretaresse geeft aan dat ze graag informatie zou ontvangen over het opstellen van een goed paswoord. De andere geeft aan hier niet in geïnteresseerd te zijn.

14. Als u zich inschrijft voor een bepaalde dienst (bvb het online kunnen raadplegen van labo uitslagen) dan krijgt u een standaard paswoord. Verandert u dit standaard paswoord na ontvangst?



Op deze vraag antwoorden alle secretaresses positief. Ze scoren hiermee goed op het vlak van paswoordbeveiliging. Het actief aansporen van de gebruiker om hun paswoord te veranderen door deze diensten lijkt zijn effect te hebben.

3. Vragen aan de systeembeheerder

3.1 Deel Perceptie

1. Bent u van mening dat de informatica-systemen in de praktijk goed beveiligd zijn? (5 antwoordmogelijkheden van erg slecht tot erg goed)



De systeembeheerder is van mening dat de systemen goed beveiligd zijn, maar dat er nog ruimte voor verbetering is.

2. Bent u van mening dat u voldoende middelen en tijd ter beschikking krijgt om in een goede beveiliging van het ict-systeem in de praktijk te voorzien?



Op deze vraag wordt positief geantwoord.

3. Bent u van mening dat er hardware-matige veranderingen in de praktijk nodig zijn om de computer-beveiliging te verbeteren?



Op deze vraag wordt negatief geantwoord.

4. Bent u van mening dat er software-matige veranderingen in de praktijk nodig zijn om de computer-beveiliging te verbeteren? Indien Ja welke?



Op deze vraag antwoordde de systeembeheerder positief. Hij is dus van mening dat er software-matige aanpassingen dienen te gebeuren in de praktijk om de computerveiligheid te garanderen. Zoals hieronder ook besproken bij het stuk "vaststellingen" geeft de admin aan dat er op dit moment nog een pc met Windows XP gebruikt wordt. Microsoft brengt geen veiligheidsupdates

meer uit voor dit besturingssysteem. Nieuw gevonden exploits worden dus niet meer verholpen en kunnen dus worden uitgebuit door hackers. Dit is een ernstige bedreiging voor de computer-beveiliging.

5. Bent u van mening dat de dokters en secretaresse in de praktijk hun gedrag ivm. computer-beveiliging zouden moeten aanpassen om in een goede beveiliging van het ict-systeem in de praktijk te voorzien?



Hierop wordt positief geantwoord. Dit impliceert dat er veranderingen in het gedrag van de artsen en secretaresses i.v.m. computer-beveiliging nodig zijn om deze laatste te optimaliseren.

6. Bent u van mening dat de artsen/secretaresses in de praktijk een goede computer-beveiliging belangrijk vinden?



Op deze vraag wordt positief geantwoord.

7. Bent u van mening dat de artsen/secretaresses in de praktijk openstaan voor veranderingen die de beveiliging van de computers zouden verbeteren?



Op deze vraag wordt positief geantwoord.

3.2 Deel Fysieke beveiliging

1. Is er een UPS aanwezig in de praktijk?



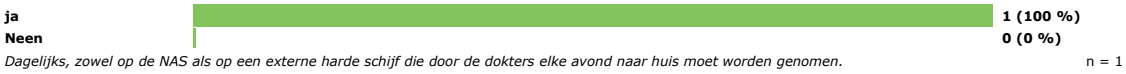
Op deze vraag wordt positief geantwoord. Er is een UPS aanwezig in de praktijk waardoor bij stroompanne de server met alle patiëntendata op een veilige manier kan afsluiten en dus data-verlies vermeden kan worden.

2. Is er een stroompiekbeveiliging aanwezig in de praktijk?



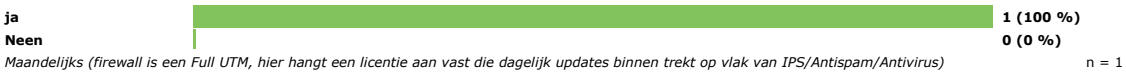
Een stroompiekbeveiliging beschermt het stroomnet tegen stroompieken in de praktijk waar ik als HAIO werk.

3. Worden back-ups gemaakt van de computergegevens? Hoe vaak? Op welke media?



De Administrator heeft er voor gezorgd dat er dagelijks back-ups worden gemaakt van de gegevens in de praktijk. Hierdoor is de data beschermd tegen verlies door rampspoed doordat er steeds kan teruggegrepen worden naar de back-up. De gegevens worden weggeschreven naar de NAS en een externe harde schijf. Het is de bedoeling dat de artsen deze laatste elke avond mee naar huis nemen zodat er zich steeds een kopie van de data buiten de praktijk bevindt. De artsen doen dit echter niet op dit moment.

4. Wordt er een hardware firewall gebruikt om het LAN-netwerk van de praktijk af te schermen? Hoe regelmatig wordt de firmware van deze firewall geüpdatet?



In de de praktijk waar ik HAIO ben is een hardware-firewall aanwezig. Dit toestel houdt kwaadwilligen tegen die zich toegang willen verschaffen tot de gegevens op de pc's. Elke maand krijgt deze firewall een firmware update opdat hij het netwerk kan beschermen tegen de meest recente bedreigingen.

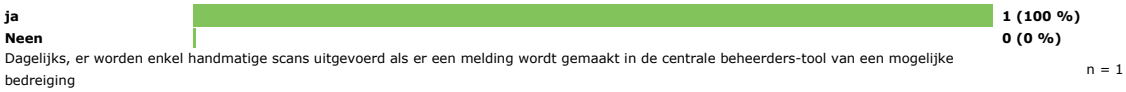
3.3 Deel Software-matige beveiliging

1. Wordt er een hardware-firewall gebruikt om het Lan-netwerk van de praktijk af te schermen? Hoe regelmatig wordt de firmware van deze firewall geüpdatet?



In de praktijk is een hardware-firewall aanwezig. Dit toestel houdt kwaadwilligen tegen zich toegang te verschaffen tot de gegevens op de pc's. Elke maand krijgt deze firewall een firmware update opdat hij het netwerk kan beschermen tegen de meest recente bedreigingen.

2. Zijn de computers in de praktijk beschermd tegen malware d.m.v. een antivirus-programma? Hoe vaak ontvangt deze automatisch updates van malware-definities? Hoe vaak voert u een handmatig scan van de systemen uit om malware te detecteren?



Uit het antwoord van de systeembeheerder valt af te leiden dat de computers in de praktijk over anti-virus software beschikken. Er wordt dagelijks automatisch een scan uitgevoerd. Eveneens worden dagelijks signaturen van de nieuwste malware bijgewerkt opdat de antivirus-software deze kan herkennen. Blijkbaar worden er enkel diepe handmatige scans uitgevoerd als er een melding is van een mogelijke bedreiging in de centrale beheerders-software.

2. Welke besturingssystemen worden in de praktijk gebruikt? Ontvangen al deze besturingssystemen automatische updates?



In de praktijk waar ik ben haio ben wordt van volgende besturingssystemen gebruik gemaakt: Windows Server 2008 op de server, Windows 7 op de pc's in de kabinetten, Windows Xp op de pc aan de balie. Het gebruik van Windows Xp houdt een beveiligingsrisico in. Microsoft brengt namelijk geen veiligheidsupdates meer uit voor dit besturingssysteem. Nieuw gevonden exploits worden dus niet meer verholpen en kunnen dus worden uitgebuit door hackers. De andere besturingssystemen ontvangen wel allemaal nog automatische updates.

3. Hoe vaak gebeurt er een update van de software op de pc? (bv java/adobe reader/…)

De meeste software zoals Adobe Reader wordt geüpdatet bij groot onderhoud van de pc's, dit gebeurt halfjaarlijks. Java vormt hier een uitzondering op aangezien de nieuwste versies vaak compatibiliteitsproblemen geven i.v.m. software die hier afhankelijk van is bvb banksoftware. Hier wordt dus de versie gebruikt waarmee de software goed werkt.

Uit bovenstaand antwoord valt op te maken dat de software op de pc's de nieuwste updates uitgesteld ontvangt. Dit houdt in dat eventuele ontdekte exploits in deze software langer beschikbaar blijven voor hackers en dus een veiligheidsrisico inhouden.

4. Wordt de data op de harde schijven van de pc's/server/NAS versleuteld(via bv Windows bitlocker, truecrypt, andere encryptie software)?



Er wordt in de praktijk geen gebruik gemaakt van encryptie. In geval van diefstal van computer, servers of NAS kan de ruwe data op de harde schijven van deze toestellen erg eenvoudig worden uitgelezen. Dit houdt een bedreiging voor de computer-beveiliging in de praktijk in.

3.4 Deel Preventie

Om praktische redenen werden in dit stuk ook vragen gesteld die onder de noemer software-matige beveiliging vallen.

1. Wordt er software gebruikt in de praktijk waar geen licentie voor werd betaald?



Er wordt in de praktijk geen gebruik gemaakt van gepirateerde software.

2. Worden er audits gedaan van de computer-beveiliging?



De systeembeheerder geeft aan dat hij in onze praktijk de computer-beveiliging onder de loep neemt om eventuele verbeteringen toe te passen.

3. Is er een beleid naar de gebruikers van de computer systemen toe inzake paswoord gebruik (specifieke regels en afspraken over de samenstelling en het gebruik van paswoorden)?



Volgens de administrator is er een beleid iv.m. paswoord gebruik. Zoals in het stuk bevindingen hieronder beschreven loopt dit beleid niet altijd even vlot en is er weinig controle op.

3. Is er een beleid naar de gebruikers van de computersystemen toe inzake veilig gebruik van de pc?



Volgens de administrator is er een beleid iv.m. veilig gebruik van de pc's. Zoals in het stuk bevindingen hieronder beschreven is dit echter weinig concreet.

4. Is er een beleid i.v.m. het regelmatig veranderen van de paswoorden?

Paswoord change policy is actief, maar eindgebruikers geven hun paswoorden soms door (wat niet echt de bedoeling is.)

Op deze vraag werd niet helemaal correct geantwoord. Wel kan men uit het antwoord afleiden dat er de wachtwoorden worden veranderd, de frequentie wordt echter niet gegeven. Ook stelt de beheerder vast dat er problemen zijn met de implementatie van deze paswoorden.

5. Hebt u als systeembeheerder toegang tot patiëntengegevens op de pc?



De systeembeheerder antwoordt negatief op deze vraag.

6. Kent u als systeembeheerder de paswoorden voor het medische programma van de dokters?





De systeembeheerder geeft aan deze paswoorden niet te weten.

2. Bevindingen beveiligingsrisico's in de praktijk

Naast bovenstaande vragen maakte ik ook gebruik van de bevindingen gedaan in de praktijk waar ik als HAIO werk om een beeld te krijgen van de computer-beveiliging in de praktijk.

2.1 Fysieke en hardwarematige beveiliging

1. De server, NAS en externe harde schijven zijn niet op een veilige locatie geplaatst. Ze bevinden zich in een niet afgesloten ruimte in een niet afgesloten kast. Iedereen die toegang heeft tot de wachtzaal in de praktijk kan makkelijk aan deze kast. Het risico bestaat dus dat iemand bovenstaande apparatuur meeneemt en zich zo toegang kan verschaffen tot de patiëntendata aanwezig op deze apparatuur.

2. De externe harde schijven met een extra back-up worden nooit meegenomen naar huis door de artsen zoals de bedoeling is. Hierdoor blijven alle back-ups dus in de praktijk aanwezig. Bij rampspoed zoals brand zal er dus geen enkele back-up beschikbaar zijn aangezien deze zich allemaal in de praktijk bevinden.

3. Er wordt in de pratijk gebruik gemaakt van Microsoft draadloze keyboards. Recentelijk werd bekend dat de beveiliging van deze apparaten erg slecht is.[16] Het is betrekkelijk eenvoudig om alle toetsaanslagen die gemaakt worden op deze apparaten uit te lezen. Dit betekent dat gebruikersnamen en wachtwoorden dus makkelijk te achterhalen zijn.

4. Bij de protocollering van labo's typen de secretaresses van de praktijk de handgeschreven notities van de artsen op de labo-uitslagen over in het elektronisch dossier. Eenmaal deze notities zijn ingebracht worden de afdrukken van de labo-uitslagen met de notities er op weggesmeten. Ze komen uiteindelijk terecht in de container waar al het te recycleren papier van de praktijk terechtkomt. Deze container bevindt zich buiten en is voor iedereen toegankelijk. De labo-uitslagen plus notities van de dokters die gevoelige patiënteninformatie bevatten zijn als dusdanig beschikbaar voor iedereen die ze uit deze container haalt.

2.2 Softwarematige beveiliging en computerhygiëne

1. Het bios[a] van de computers is niet beveiligd met een paswoord. Dit betekent dat iedereen met fysieke toegang tot de pc's de bios-instellingen kan veranderen. Zo kan er bv. een Linux distributie worden opgestart vanaf een USB-stick of dvd. Op deze manier kunnen erg makkelijk bestanden op de pc's worden aangepast. Hierdoor wordt het erg makkelijk om administrator rechten te krijgen op de pc's door bv. de 'Sticky keys attack'[b] of de admin wachtwoorden te achterhalen d.m.v. een hiervoor speciaal ontwikkelde software zoals Ophcrack[c] Ook kan men zich op deze wijze toegang verschaffen tot alle (patiënten-)data op de pc's als deze niet geëncrypteerd zijn (wat het geval is).

a 'bios': een acroniem voor **B**asic **I**nput/**O**utput **S**ystem, is een bibliotheek met een set basisinstructies voor de communicatie tussen het besturingssysteem en de hardware.

b 'Sticky keys'-aanval: Dit is een aanval waarbij door gebruik te maken van een zwakte in het Sticky keys hulpprogramma volledige beheerdersrechten verkregen worden. Hier wordt later verder op in gegaan.

c 'Ophcrack': Dit is een programma waarmee je d.m.v. beredeneerd gokken via Windows paswoorden kunt kraken.

2. 'Sticky Keys' en andere mogelijke aanvalsvectoren om administrator rechten te krijgen op de pc's zijn niet uitgeschakeld. Hierdoor kunnen d.m.v. het opstarten van een Linux distributie of door misbruik te maken van de Windows hersteloptie eenvoudig administrator toegangsrechten verkregen worden.

3. Patches voor beveiligingslekken aanwezig in software op de pc's zoals Java of Acrobat Reader worden slechts halfjaarlijks geïnstalleerd door de systeembeheerder. Hierdoor zijn de computers soms geruime periode kwetsbaar voor exploits in deze software.

4. De netwerkverbindingen zijn niet beveiligd d.m.v. Mac-adres[a] koppeling. Dit betekent dat een kwaadwillend persoon zijn laptop zonder meer kan aankoppelen op het netwerk d.m.v. de aanwezige netwerkkabels (in kabinetten, bureau secretaresse en serverkast) en zo de (patiënten)data op de pc's en server kan benaderen. Ook kan op deze manier erg makkelijk een "man in the middle attack" worden gedaan met een programma als Ettercap[b]. Hierbij kunnen gebruikersnamen en paswoorden worden onderschept.

5. Aangezien ik als HAIO niet beschik over de administrator wachtwoorden was het moeilijk deze te beoordelen op hun veiligheid. Er werd daarom gebruik gemaakt van het programma Ophcrack om te kijken of deze makkelijk te raden waren d.m.v. het gebruik van Rainbowtabellen[c]. Het administrator wachtwoord werd op deze wijze al erg snel achterhaald en bleek dus niet lang en moeilijk genoeg te zijn.

6. De printer aan de front-desk is benaderbaar via wifi. Dit signaal is beveiligd d.m.v. WPA2 encryptie. D.m.v. het gebruik van Wifite[d] kwam naar voor dat hier echter het standaard paswoord gebruikt wordt dat makkelijk te achterhalen is. Eenmaal dit wachtwoord achterhaald is kan men via deze printer het achterliggende netwerk met de pc's en server benaderen.

a Het Mac-adres (Media Acces Control) is een uniek identificatienummer dat aan een apparaat in een ethernetnetwerk is toegekend.

b 'Ettercap': dit is een programma dat kan worden gebruikt voor het hacken en beveiligen van een LAN (lokaal netwerk) zoals een thuisnetwerk. Het is vooral sterk in het uitvoeren van man-in-the-middle aanvallen, dus aanvallen waarbij informatie tussen twee communicerende partijen onderschept en eventueel aangepast wordt, zonder dat beide partijen daar weet van hebben.

c 'Rainbowtabellen': dit zijn tabellen die alle mogelijke oplossingen voor een bepaald wiskundig probleem bevatten. Hierdoor wordt het proces om een paswoord te kraken verkort aangezien reeds een groot deel van de wiskundige berekeningen nodig om het paswoord re kraken gemaakt zijn.

b 'Wifite': Dit is een programma dat volledig autonoom draadloze netwerken kan analyseren, manipuleren en wachtwoorden achterhalen.

Identificatie Zwakke punten

In dit stuk worden de zwakheden die naar voor kwamen uit de antwoorden en de bevindingen geëvalueerd.

1. Deel perceptie

1. De artsen en secretaresses schatten hun informatica-kennis van neutraal tot slecht in. Een goede basiskennis van informatica is een basisvereiste voor een goede computer-beveiliging. Door de artsen en secretaresse hun kennis omtrent informatica te verbeteren zou er een beter computer-beveiliging bekomen kunnen worden.

2. Bij de artsen is er een duidelijke vraag naar informatie. Zij zouden erg graag meer informatie i.v.m. computer-beveiliging krijgen en ze verwachten van de overheid en hun vakvereniging dat zij hen deze informatie verstrekken. De overheid en vakvereniging er toe aan zetten de artsen meer te informeren over computer-beveiliging is in het kader van dit onderzoek jammer genoeg niet mogelijk. Wel kan er gekeken worden of er reeds geschikte informatie beschikbaar is en of deze aan de artsen bezorgd kan worden.

3. In tegenstelling tot de secretaresses zijn slechts een minderheid van de artsen er van overtuigd dat het hun taak is zich bezig te houden met computer-beveiliging. Ook vind slechts een minderheid van de artsen een goede computer-beveiliging belangrijk in het kader van een goede patiëntenzorg.
   Door de artsen te informeren over het belang van een goede computer-beveiliging zou men hen ook van hun verantwoordelijkheid op dit gebied kunnen overtuigen.

4. Het overgrote deel van de artsen en beide secretaresses zijn van mening dat hun paswoorden niet makkelijk te raden zijn. Zoals hierboven beschreven is dit echter een illusie. Door de artsen en secretaresses hierop te wijzen en ze te leren hoe ze er voor kunnen zorgen dat hun paswoorden daadwerkelijk moeilijk te raden zijn zou de computer-beveiliging in de praktijk significant verbeteren.

5. De systeembeheerder is van mening dat er geen hardware-matige veranderingen nodig zijn in de praktijk om de computer-beveiliging te garanderen. Zoals hierboven beschreven zijn er wel degelijk een aantal wijzigingen nodig.
   Het informeren van de systeembeheerder van de huidige tekortkomingen zal hem er wellicht toe aanzetten deze aan te pakken.

6. De systeembeheerder vindt dat er veranderingen in het gedrag van artsen en secretaressen i.v.m. computer-beveiliging nodig zijn om deze laatste te optimaliseren. Verdere navraag naar de concrete veranderingen die volgens hem nodig zijn zou interessant zijn om eventueel andere zwakheden in de computer-beveiliging vast te stellen die niet door masterproef naar voor kwamen.

2. Deel Fysieke beveiliging

1. Zowel de helft van de secretaresses als meer dan de helft van de dokters geven aan dat ze hun pc niet uitzetten of afmelden als ze hun bureau of kabinet verlaten. Dit betekent dat iedereen die zich fysiek toegang kan verschaffen tot deze pc's patiënten-gegevens kan kopiëren, consulteren of verwijderen. Dit is een ernstig veiligheidsrisico in de praktijk. De artsen en secretaresses zouden er een gewoonte van moeten maken om hun pc uit te zetten of af te melden als ze deze achter laten.

2. Zowel de helft van de secretaresses en meer dan de helft van de artsen geven aan dat zij hun kabinet niet afsluiten als ze hun bureau of kabinet verlaten. Dit houdt een ernstig veiligheidsrisico in aangezien het hierdoor erg makkelijk wordt zich fysiek toegang te verschaffen tot deze computers. Als de pc's aangemeld zijn kan een kwaadwillende persoon zonder meer aan alle patiëntendata. Als pc's uit staan of afgemeld zijn kan hij de pc's of de harde schijven uit deze pc's meenemen om later de data uit te lezen. De artsen en secretaresses zouden er een gewoonte van moeten maken om hun kabinet af te sluiten als ze deze verlaten.

3. In tegenstelling tot de secretaresses gebruikt meer dan de helft van de artsen opslagmedia die ook buiten de praktijk worden gebruikt. Dit houdt een ernstig risico in aangezien heel wat malware deze opslagmedia als vector gebruikt. De artsen moeten ophouden met gebruik te maken van dergelijke opslagmedia om zo de computer-beveiliging te verbeteren.

4. De systeembeheerder heeft er voor gezorgd dat er dagelijks back-ups worden gemaakt. Deze back-ups gebeuren op een NAS server en een externe harde schijf. Het is de bedoeling dat de artsen deze laatste elke avond mee naar huis nemen zodat er zich ook steeds een back-up buiten de praktijk bevindt. Deze kan dan niet verloren gaan als er bv. brand uitbreekt in de praktijk. De artsen nemen deze externe harde schijf momenteel niet mee naar huis zoals de bedoeling is. Door er voor te zorgen dat de artsen alsnog elke avond een externe harde schijf meenemen naar huis, door de NAS buiten de praktijk te plaatsen of door een back-up in de cloud op te slaan zou er altijd een kopie van de gegevens beschikbaar zijn buiten praktijk.

5. De server en NAS staan in een kast waarvan de deur open staat. Hierdoor kan iedereen die dat wil zich erg makkelijk toegang tot deze apparatuur verschaffen. De fysieke beveiliging is hier onbestaande, wat er voor zorgt dat een kwaadwillend persoon erg makkelijk de server, de NAS of de harde schijven in deze apparaten kan meenemen. Deze kast is op dit moment niet afgesloten omdat er anders niet voldoende ventilatie is wat tot oververhitting van de apparatuur kan leiden. Door er voor te zorgen dat de server en NAS zich op een goed beveiligde plaats bevinden zal de computer-beveiliging verbeteren. Dit zou kunnen gebeuren door de huidig kast af te sluiten (waarbij ventilatie-gaten moeten worden voorzien) of de server en NAS op een andere locatie te plaatsen.

6. De draadloze keyboards gebruikt in de praktijk bevatten een beveiligingslek die het mogelijk maakt om alle ingevoerde karakters te registeren van op afstand. Dit betekent dat ook gebruikersnamen en paswoorden kunnen worden geregistreerd. Door deze keyboards te vervangen door exemplaren die niet kwetsbaar zijn voor dit soort aanvallen zou de computer-

beveiliging een stuk verbeterd kunnen worden.

7. Op dit moment wordt gevoelige patiënten-informatie zoals geprinte verslagen en labo-uitslagen niet vernietigd voor ze in de vuil-container terecht komen. Deze container is voor iedereen toegankelijk. Dit zorgt er voor dat elke persoon die zich toegang weet te verschaffen tot deze container beschikt over verschillende documenten die gevoelige patiënten-informatie bevatten. Het vernietigen van deze documenten d.m.v. een papier-versnipperaar zou een oplossing kunnen bieden.

3. Deel Computerhygiëne – Software-matige beveiliging

1. De digitale communicatie in de praktijk is een pijnpunt. Zo geven meer dan de helft van de artsen aan dat ze over patiënten-dossiers communiceren via email. Het email-protocol is niet geschikt om gevoelige informatie te versturen. De geschreven tekst wordt namelijk onversleuteld verstuurd. Dit betekent dat een persoon die deze communicatie kan onderscheppen met een 'packet-sniffer'[a] zoals bv. Wireshark deze berichten kan lezen. Dit kan voorkomen worden door dit mail-verkeer te encrypteren. De artsen in de praktijk geven echter aan dat ze hier geen gebruik van maken. Een ander pijnpunt bij email is het feit dat er geen verificatie van zender en ontvanger mogelijk is. Zo is het relatief eenvoudig om het afzender-adres van een mail te vervalsen. De ontvanger kan hierbij onmogelijk achterhalen dat de verzender niet de echte verzender is (een mooi voorbeeld hiervan zijn de verschillende phishing mails die we dagelijks ontvangen). Deze twee tekortkomingen van het e-mail protocol zorgen er voor dat dit communicatie middel bijzonder ongeschikt is voor het delen van gevoelige patiënten-informatie. Een veel geschikter middel is de ehealth-box, waar ondertussen elke arts over beschikt. Deze is gemaakt met vertrouwelijke communicatie, encryptie en verificatie van zender/ontvanger in het achterhoofd en is de op dit moment de meest geschikte manier voor artsen om te communiceren. Navraag bij de artsen bracht naar voor dat nog geen enkele arts hier gebruik van maakt. Een groot deel van de artsen wist niet hoe ze deze konden gebruiken in hun EMD software. Door de artsen het gebruik van de ehealth-box eigen te maken zou alle communicatie over patiënten-gegevens voldoende beveiligd kunnen verlopen. Voor de secretaresses is dit jammer genoeg niet mogelijk.

2. In tegenstelling tot de secretaresses geeft de meerderheid van de artsen aan zijn pc niet enkel te gebruiken voor praktijkgerelateerde zaken. Hierdoor worden de pc's aan meer gevaren blootgesteld dan nodig. Het zou de computerveiligheid verbeteren indien de artsen de pc's enkel gebruikten voor praktijkgerelateerde zaken.

3. Alle secretaresses en meer dan de helft van de artsen geven aan dat ze vertrouwelijke patiënten-informatie doorgeven aan derden via telefoon, fax of email zonder dat ze deze persoon kennen en zijn identiteit kunnen verifiëren. Dit betekent dat een kwaadwillend persoon d.m.v. 'social-engineering' makkelijk vertrouwelijke patiënteninformatie kan opvragen. Het gebruik van de

a Een 'Packet sniffer' is een programma dat gebruikt wordt om gegevens op een computernetwerk op te vangen en te analyseren.

hierboven reeds beschreven ehealth-box door de artsen kan het probleem van verificatie verhelpen. De secretaresses zouden het doorgeven van medische informatie aan de artsen kunnen overlaten of extra maatregelen moeten nemen om de identiteit van de verzoekende partij te kunnen verifiëren.

4. De systeembeheerder geeft aan dat hij enkel handmatig een diepe virus-scan doet als hij een melding krijgt van een mogelijke bedreiging in de centrale beheerders-software. Het op regelmatige basis proactief uitvoeren van deze diepe scans zou een betere computer-beveiliging met zich meebrengen. De systeembeheerder zou hiertoe moeten worden aangezet.

5. Op één van de pc's in de praktijk wordt nog altijd gebruik gemaakt van het besturingssysteem Windows XP. Microsoft levert niet langer ondersteuning en brengt geen veiligheidsupdates meer uit voor dit besturingssysteem. Nieuw gevonden beveiligingsgaten worden dus niet langer verholpen en kunnen dus worden uitgebuit door hackers om controle te krijgen over deze systemen. Zoals door de systeembeheerder zelf aangegeven houdt het gebruik van dit besturingssysteem een erg groot veiligheidsrisico in. Een upgrade van dit besturingssysteem naar een recentere versie zou dit gat in de computer-beveiliging dichten.

6. De software die op de pc's is geïnstalleerd ontvangt slechts halfjaarlijks updates. Dit betekent dat veiligheidslekken in deze software waar een patch voor bestaat soms meerder maanden aanwezig blijven op de computers. Deze veiligheidslekken kunnen worden uitgebuit door hackers en vormen een ernstige bedreiging voor de computer-beveiliging in de praktijk. Het zou wenselijk zijn dat deze updates sneller gebeuren door bv. één van de artsen of secretaresses de nodige rechten te geven om dit te doen.

7. De harde schijven in de server, NAS en pc's zijn niet geëncrypteerd. Dit betekent dat iedereen die zich toegang kan verschaffen tot deze schijven de hierop opgeslagen data kan uitlezen, vernietigen of bewerken. Dit kan zowel in de praktijk zelf gebeuren door het booten van bv. 'Kali linux'[a] of op een andere locatie in het geval de harde schijven meegenomen worden.
   Een erg efficiënte manier om dit tegen te gaan is het gebruik van encryptie. Hierbij wordt alle data op de schijven versleuteld waardoor deze niet meer leesbaar zijn door een persoon die niet over de decryptie-sleutel beschikt.
   Het toepassen van encryptie op de schijven in de server, NAS en pc's in de kabinetten is technisch makkelijk toepasbaar aangezien alle huidige besturingssystemen hierop voorzien zijn. Het zou een ernstige verbetering van de computer-beveiliging inhouden.

8. De systeembeheerder geeft aan dat er een beleid is i.v.m. computer-beveiliging. Wel zijn er geen concrete richtlijnen of een draaiboek. Ook is er weinig controle op dit beleid. Het zou een verbetering in de computer-beveiliging betekenen als er concrete richtlijnen beschikbaar zouden zijn voor de dokters en als deze gecontroleerd en opgevolgd zouden worden.

9. Bij het opstarten van de pc's is het mogelijk om instellingen in het bios te veranderen. Dit houdt een ernstig veiligheidsrisico in omdat op deze manier de opstart-instellingen zo kunnen worden gewijzigd dat de pc opstart vanaf een usb-stick of dvd-rom. Op deze manier kan een alternatief besturingssysteem worden opgestart zoals bv. 'Kali linux' waarmee verschillende aanvallen op de

a 'Kali Linux' is een linux distributie die kan worden opgestart vanaf een dvd of usb-stick en voorzien is van verschillende tools die gebruikt worden door hackers om systemen te kraken.

computers en de achterliggende hardware kunnen worden uitgevoerd. Het afschermen van het bios d.m.v. een extra wachtwoord zou een significante verbetering in de computer-beveiliging betekenen.

10. Op de pc's in de praktijk is het mogelijk om gebruik te maken van "Sticky Keys". Dit is een hulpprogramma in Windows dat bedoeld is voor mensen met een lichamelijk beperking. Het zorgt er voor dat de Shift, Ctrl , Alt of Windows knop ingedrukt blijven zonder dat er blijvend moet worden gedrukt op deze knoppen. Door vijf maal Shift in te drukken als u het aanmeld-venster in Windows voor u hebt wordt elk programma dat de naam "sethc.exe" draagt opgestart, dit bovendien met rechten. Een aanvaller kan door bv. het booten van 'Kali linux' het programma "cmd.exe" hernoemen naar "sethc.exe". Bij het 5 maal indrukken van de Shift key wordt dan niet het onschuldige programma sticky keys opgeroepen maar het hernoemde "cmd.exe" dat voor de command-line zorgt. Aangezien deze command-line met rechten draait heeft een aanvaller op dit moment volledige controle over de pc. Het uitzetten van deze functie en andere functies die op deze manier kunnen worden misbruikt zou er voor zorgen dat de hierboven beschreven aanval niet meer mogelijk is.

11. In de praktijk is het mogelijk om met om het even welke pc toegang te krijgen tot het netwerk als deze pc wordt ingeplugd in één van de netwerk-contactdozen in de kabinetten of in de switch die zich in de serverkast bevindt. Een kwaadwillend persoon die zich toegang weet te verschaffen tot deze contactdozen of de switch kan dus zijn laptop op het lokale netwerk aansluiten. Op dit moment zijn de pc's, server en NAS blootgesteld aan eventuele aanvallen via deze netwerkverbinding. De firewall wordt op deze manier volledig omzeild. Dit zou makkelijk kunnen verholpen worden d.m.v. 'Mac-adres' filtering. Bij deze techniek worden enkel vooraf toegelaten pc's toegelaten op het netwerk. Hiervoor wordt gebruik gemaakt van het Mac-adres van (de netwerk-kaarten van) de pc's die op het netwerk mogen. Iemand die op dat moment zijn niet toegelaten pc fysiek op het netwerk aansluit zal niet langer toegang hebben tot dit netwerk.

12. In de praktijk is de netwerk printer aan de front-desk benaderbaar via een wifi-verbinding die verder niet gebruikt wordt in de praktijk. Uit testen blijkt dat deze wifi-verbinding slecht beveiligd is. Hierdoor is via deze printer het achterliggende netwerk benaderbaar. Aangezien deze verbinding verder niet gebruikt wordt in de praktijk kan deze zonder hinder voor de werknemers gedeactiveerd worden. Dit zou er voor zou zorgen dat ze niet langer misbruikt kan worden.

4. Deel paswoordgebruik

Zowel bij de secretaresses, artsen als bij de systeembeheerder blijkt het paswoordgebruik problematisch.

1. Voor zowel alle artsen als secretaresses geldt dat zij voor sommige toepassingen in de praktijk een wachtwoord gebruiken dat identiek is aan de gebruikersnaam voor diezelfde toepassing. Dit houdt vanzelfsprekend een ernstig veiligheidsrisico in. Door er voor te zorgen dat er niet langer paswoorden gebruikt worden die gelijk zijn aan een gebruikersnaam kan de computerveiligheid ernstig verbeterd worden.

2. Meer dan de helft van de artsen en de helft van de secretaresses geven aan dat ze hun

paswoorden hergebruiken voor verschillende applicaties. Dit houdt een ernstig risico in aangezien bij het kraken van een wachtwoord van 1 enkele applicatie de andere applicaties waarvoor dit wachtwoord werd gebruikt ook niet langer veilig zijn. Het is in het kader van een goede wachtwoordveiligheid aangeraden voor elke applicatie een verschillend wachtwoord te gebruiken.

3. Beide secretaresses en de grote meerderheid van de artsen gebruiken een of meerder paswoorden die korter zijn dan twaalf symbolen. Deze wachtwoorden zijn te kort om een goede beveiliging te bieden tegen 'brute-force' aanvallen. Het vervangen van deze te korte paswoorden symbolen zou een significante verbetering van de computer-beveiliging met zich meebrengen.

4. In tegenstelling tot de secretaresses geven 2 van de 5 artsen aan dat ze gebruik maken van een paswoord dat niet uit een combinatie van letters, cijfers en/of leestekens bestaat. Dit zorgt er voor dat de paswoorden van deze artsen makkelijk te achterhalen zijn d.m.v. een 'brute-force' aanval. Het vervangen van deze paswoorden door paswoorden die wel uit een combinatie van letters, cijfers en/of leestekens bestaan zou een significante verbetering van de computer-beveiliging met zich meebrengen.

5. Voor alle dokters en secretaresses geldt dat andere mensen één of meerdere van hun paswoorden kennen. Vanzelfsprekend is dit erg slecht voor de computer-beveiliging. Het vervangen van deze paswoorden door paswoorden die niet door anderen gekend zijn zou een significante verbetering van de computer-beveiliging met zich meebrengen.

6. De grote meerderheid van de artsen en de helft van de secretaresses geven aan dat hun paswoord (gedeeltelijk) bestaat uit een naam van een familielid/huisdier, een woord dat terug te vinden is in het woordenboek of een opeenvolgende reeks van letters of cijfers. Dit maakt deze paswoorden erg kwetsbaar voor een 'dictionary attack' en 'social engineering'. Het vervangen van deze paswoorden door paswoorden waarop bovenstaande niet van toepassing is zou een significante verbetering van de computer-beveiliging met zich meebrengen.

7. Bij beide secretaresses en één dokter staan de paswoorden ergens opgeschreven zodat ze deze snel kunnen lezen. Vanzelfsprekend houdt dit een groot veiligheidsrisico in aangezien derden deze paswoorden ook kunnen lezen en gebruiken. Het zou de computer-beveiliging ten goede komen moesten deze neergeschreven wachtwoorden verwijderd worden.

8. Slechts één arts geeft aan regelmatig (minimum 1x per half jaar) zijn/haar paswoorden te veranderen. Bij de secretaresses is de toestand nog erger aangezien geen enkele secretaresse aangeeft dit te doen. Het regelmatig veranderen van de paswoorden is een essentieel onderdeel van een goede paswoordveiligheid. De artsen er toe aanzetten hun paswoorden minimaal halfjaarlijks te vervangen zou een significante verbetering in de computer-beveiliging betekenen.

Voorstellen tot verandering

In dit stuk wordt een overzicht gegeven van de veranderingen die zullen worden voorgesteld om de computer-beveiliging in de praktijk te verbeteren.

1. **Informatie:** Om verandering te kunnen brengen in de praktijk is het van belang dat de artsen en secretaresses op de hoogte zijn van wat er op dit moment fout loopt. Ook moeten ze worden ingelicht van het belang van een goede computer-beveiliging in het kader van het beschermen van vertrouwelijke patiënten-informatie. Bovendien kan verwacht worden dat de artsen en secretaresses beter zullen meewerken als ze begrijpen waarom hen gevraagd wordt bepaalde veranderingen toe te passen. Naast de artsen en secretaresses is het ook van belang dat de systeembeheerder op de hoogte wordt gebracht van de voorstellen tot verandering. Hij zal bij deze veranderingen in hoge mate betrokken zijn en het is dus ook aangewezen dat hij de redenen achter deze veranderingen kent.
2. **Pc's afmelden/uitzetten:** De artsen moeten er een goede gewoonte van maken hun pc's af te melden of uit te zetten als ze deze voor langere tijd verlaten. Dit zou deels geautomatiseerd kunnen worden door Windows automatisch te laten afmelden na een bepaalde periode, bv. 15 minuten.
3. **Kabinetten afsluiten:** De artsen moeten er een goede gewoonte van maken hun kabinetten af te sluiten als ze hun kabinetten voor langere tijd verlaten.
4. **USB-sticks:** USB-sticks die ook buiten de praktijk worden gebruikt mogen niet langer worden gebruikt voor praktijkdoeleinden.
5. **Back-ups:** De artsen moeten elke avond de externe harde schijf met extra back-up meenemen. Als alternatief kan er voor geëncrypteerde cloud back-ups worden gekozen.
6. **Serverkast:** De kast moet worden afgesloten. Om voldoende ventilatie te voorzien voor de apparatuur in deze kast zullen er ventilatie-gaten moeten voorzien worden. Als alternatief kan de server op een andere afgesloten plaats worden gezet.
7. **Keyboards:** De huidige keyboards moeten vervangen worden door veilige keyboards die niet kunnen worden uitgelezen vanop afstand.
8. **Versnipperaar:** Alle geprinte vertrouwelijke patiënten-informatie moet worden vernietigd in een versnipperaar voor deze in de afval container wordt gegooid.
9. **Encryptie communicatie/ Ehealth:** Communicatie over patiënten-dossiers dient bij voorkeur via de ehealth-box te gebeuren. Een alternatief is het encrypteren van het email verkeer. Om op een gebruiksvriendelijker manier te communiceren via het ehealth-box platform kan gebruik gemaakt worden van Cozo (Collaboratief Zorgplatform). Deze leveren via hun site www.cozo.be alle tools om te communiceren via de ehealth-box.
10. **Enkel praktijkgerelateerde activiteiten:** Activiteiten die niet praktijk gerelateerd zijn moeten

vermeden worden op de pc's in de praktijk.

11. **Verificatie van ontvangers van patiënten-informatie:** De identiteit van onbekende collega's die om patiënten-informatie verzoeken moet geverifieerd worden. Dit kan telefonisch door zelf de arts terug te bellen. Geschreven communicatie dient via de ehealth-box of geëncrypteerd via email te verlopen.

12. **Handmatige virus-scan:** Er moet meer frequent een uitgebreide virus-scan worden uitgevoerd door de systeembeheerder. Alternatief kan één van de artsen voldoende rechten worden gegeven zodat deze dit zelf kan doen.

13. **Vervanging Windows Xp:** De pc aan de front-desk moet voorzien worden van een nieuwer besturingssysteem dan het huidige Windows XP. In het geval er bepaalde applicaties op de pc Windows Xp vereisen en er geen alternatieven zijn kan er een virtuele machine worden gedraaid met Windows Xp. Deze virtuele machine mag niet over internet-toegang beschikken.

14. **Frequentere updates:** De software op de pc's dient frequenter te worden voorzien van updates. Dit kan gebeuren door de systeembeheerder of door een arts die hiervoor de rechten wordt toegekend.

15. **Encryptie van de harde schijven:** Alle harde schijven in de praktijk moeten worden geëncrypteerd. Op de server, externe harde schijven en de pc's kan "Windows Bitlocker-stationsversleuteling" worden gebruikt. Op de NAS dient een optie in het menu te worden geactiveerd zodat de harde schijven worden versleuteld.

16. **Draaiboek computer-beveiliging:** De beheerder dient het beleid i.v.m. computer-beveiliging concreet te maken d.m.v. een draaiboek

17. **Bios-lock:** De toegang tot het bios op de pc's moet worden afgeschermd d.m.v. een paswoord

18. **Uitzetten Sticky keys:** Sticky keys en andere hulpprogramma's die misbruikt kunnen worden door kwaadwilligen moeten worden gedeactiveerd.

19. **Mac-adres filtering:** Er moet Mac-adres filtering worden toegepast op het netwerk waardoor enkel pc's die gekend zijn verbinding kunnen maken.

20. **Uitzetten niet gebruikte wifi functionaliteit:** De draadloze functionaliteit van de printer aan de front-desk moet gedeactiveerd worden.

21. **Paswoord-beleid:** Er moet een paswoord-beleid komen waarbij de paswoorden voldoen aan volgende voorwaarden:

    - De gebruikersnaam en het paswoord mogen niet gelijk zijn
    - Een paswoord mag slechts voor 1 applicatie gebruikt worden
    - Een paswoord moet minimum 12 karakters lang zijn
    - Een paswoord moet minimaal uit een combinatie van letters en cijfers of letters en leestekens bestaan. Ideaal bestaat het paswoord uit een combinatie van zowel letters,

cijfers en leestekens.

- Een paswoord mag het volgende niet bevatten:
  - De naam van een familielid of huisdier
  - Opeenvolgende reeksen zoals bv abcde, 12345, …
  - Bestaande woorden die terug te vinden zijn in een woordenboek
- Een paswoord mag nergens worden opgeschreven
- Elk paswoord moet om het half jaar gewijzigd worden.

De systeembeheerder moet het toepassen van deze regels ondersteunen en controleren. Om dit proces gebruiksvriendelijker te maken kan eventueel gebruik gemaakt worden van een 'paswoord manager'[a] zoals LastPass in combinatie met 'two factor authentication'[b] zoals door 'Google authenticator voorzien.

Concrete uitwerking voorstellen

Tijdens een overleg waarbij alle artsen en secretaresses aanwezig waren werd een presentatie gegeven van de hierboven geformuleerde voorstellen. Er werd de artsen uitgelegd wat deze veranderingen precies inhouden en waarom ze ingevoerd werden. Daar waar nodig werd uitleg gegeven over de werking van bepaalde software.

De artsen en secretaresses kregen een overzicht van de veranderingen waarop duidelijk werd uitgelegd wat van hen verwacht werd.

Er werd hen duidelijk gemaakt dat de toepassing van deze veranderingen zou worden geëvalueerd over een periode van 3 maand. Dit d.m.v. steekproeven en een bevraging.

Samen met de artsen werd overlopen welke aankopen gedaan moeten worden om de voorstellen te kunnen opvolgen. Ook werd met er de aanpassingen die de systeembeheerder dient uit te voeren met hen doorgenomen.

Met de systeembeheerder werden de veranderingen overlopen waarvoor hij verantwoordelijk is.

a Dit is een programma dat instaat voor het creëren van veilige paswoorden en het veilig bewaren er van. Een gebruiker van dit soort programma's hoeft in principe slechts één moeilijk paswoord te onthouden en (optioneel) gebruik te maken van 'Google Authenticator' om voor elke applicatie een verschillend veilig paswoord te hebben zonder deze allemaal te moeten memoriseren.

b 'Two factor authentication' betekent dat er naast het ingeven van een paswoord nog een tweede vorm van authenticatie nodig is alvorens toegang verleend wordt aan een bepaalde applicatie. Een voorbeeld hiervan is het ingeven van een door de cardreader gegeneerde pin-code bij online bankieren.

Evaluatie verbeteringen

Als afsluiter van dit praktijk-verbeterend project werd er een evaluatie gedaan van de doorgevoerde veranderingen. Er werd geëvalueerd hoe goed de artsen, secretaresses en administrator de richtlijnen hebben opgevolgd en welke problemen zich stelden.

1. Evaluatie eenvoudig controleerbare verbeter-punten

Onderstaande verbeterpunten werden zonder bevraging gecontroleerd.

1. **Pc's afmelden/uitzetten**
   Gedurende een periode van 1 maand werd dagelijks zowel voor aanvang van de consulten als tijdens de middag en na het beëindigen van de consulten gecontroleerd of de pc's waren afgemeld of uitgezet. Er werd voor deze momenten gekozen omdat er dan telkens geen artsen aanwezig zijn.
   Resultaat: Op elk controle-moment waren de pc's afgemeld of uitgezet. De aanpassing die werd ingevoerd om Windows automatisch te laten afmelden na een periode van 15 min inactiviteit blijkt erg succesvol.

2. **Kabinetten afsluiten:**
   Tijdens een periode van 1 maand werd dagelijks zowel voor aanvang van de consulten als tijdens de middag en na het beëindigen van de consulten gecontroleerd of de kabinetten afgesloten waren. Er werd voor deze momenten gekozen omdat er dan telkens geen artsen aanwezig zijn.
   Resultaat: Over de periode van 1 maand (90 controles) bleken de deuren slechts 5 maal niet gesloten.

3. **Back-ups:**
   Gedurende een periode van 1 maand werd dagelijks na het beëindigen van de consulten gecontroleerd of 1 van de artsen de externe harde schijf mee naar huis had genomen. Er werd hier niet gekozen voor het alternatief om te back-uppen in de cloud wegens de extra meerkost.
   Resultaat: Op elk controle-moment bleek de externe harde schijf meegenomen. Eén van de artsen heeft de taak op zich genomen om de externe harde schijf elke avond mee te nemen en doet dit ook consequent.

4. **Serverkast:**
   Tijdens een periode van 1 maand werd dagelijks na het beëindigen van de consulten gecontroleerd of de serverkast afgesloten was. Dit werd mogelijk gemaakt door het boren van ventilatie-gaten in de kast. Er werd niet voor het alternatief gekozen waarbij de server werd verplaatst wegens de extra werklast en kost die dit met zich zou brengen.
   Resultaat: Gedurende de gehele maand bleek de serverkast afgesloten.

5. **Keyboards:**
   Na de periode van 1 maand werd gecontroleerd of de kwetsbare keyboards vervangen werden.

Resultaat: De keyboards werden nog niet vervangen. Na de administrator hierover te hebben bevraagd bleek dat hij deze spoedig ging bestellen.

6. **Versnipperaar:**
   Tijdens een periode van 1 maand werd dagelijks na het beëindigen van de consulten gecontroleerd of alle geprinte documenten versnipperd werden en er dus geen vertrouwelijke patiënten-informatie in de afval-container terecht komt.
   Resultaat: Er werd een versnipperaar aangekocht en alle vertrouwelijke geprinte documenten worden nu vernietigd door de secretaresses.

7. **Vervanging Windows Xp:**
   Na de periode van 1 maand werd gecontroleerd of het besturingssysteem van de pc die Windows Xp draaide voorzien was van een moderner besturingssysteem.
   Resultaat: Het besturingssysteem van de pc werd vervangen door Windows 7.

8. **Draaiboek computer-beveiliging:**
   Na de periode van 1 maand werd gecontroleerd of er een draaiboek beschikbaar was.
   Resultaat: Dit draaiboek is nog niet beschikbaar. De systeembeheerder heeft dit nog niet samengesteld.

9. **Bios-lock:**
   Na de periode van 1 maand werd gecontroleerd of bij alle computers het bios afgeschermd is met een paswoord.
   Resultaat: De systeembeheerder heeft er voor gezorgd dat op alle computers het bios afgeschermd is met een paswoord.

10. **Uitzetten Sticky keys:**
    Na de periode van 1 maand werd gecontroleerd of bij alle computers de 'Sticky keys' en andere bij het inlogscherm te misbruiken hulpprogramma's werden uitgeschakeld.
    Resultaat: Sticky keys en ander programma's op het Windows inlog-scherm die kunnen misbruikt worden zijn gedeactiveerd.

11. **Mac-adres filtering:**
    Na de periode van 1 maand werd gecontroleerd of het mogelijk was met een vreemde laptop connectie te maken op het netwerk.
    Resultaat: Het is op dit moment nog altijd mogelijk om met een vreemde laptop connectie te maken met het netwerk. Bevraging van de beheerder bracht naar voor dat Mac-adres filtering niet mogelijk was met de huidige switch. De aankoop van een switch die dit wel kan zou besproken worden met de artsen, maar dit is tot op heden nog niet gebeurd.

12. **Uitzetten wifi functionaliteit printer front-desk:**
    Na de periode van 1 maand werd gecontroleerd of de wifi verbinding van de printer gedeactiveerd was.
    Resultaat: De wifi verbinding is niet langer beschikbaar.

2. Evaluatie overblijvende verbeterpunten

Onderstaande verbeterpunten konden moeilijk zonder ondervraging van de artsen en secretaresses geëvalueerd worden. Tijdens een bijeenkomst met alle artsen en secretaresses na een periode van 1 maand na het invoeren van de veranderingen, werden de aanwezigen ondervraagd over die veranderingen die enkel op deze wijze gecontroleerd kunnen worden. Ook voor de verbeterpunten die enkel kunnen worden gecontroleerd door ondervraging van de systeembeheerder werd een bijeenkomst met hem geregeld.

1. **USB-sticks:**
   De artsen en secretaresses werden gevraagd of ze in de afgelopen maand nog gebruik hadden gemaakt van een usb-stick die ze ook buiten de praktijk gebruiken.
   Resultaat: Zowel de artsen als secretaresses geven aan niet langer USB-sticks te gebruiken die ook buiten de praktijk worden gebruikt.

2. **Encryptie communicatie/ ehealth-box:**
   De artsen en secretaresses werden gevraagd of ze in de afgelopen maand nog onversleutelde e-mails met patiënten-informatie verstuurd hadden. Eveneens werd hen gevraagd of ze gebruik hadden gemaakt van de ehealth-box.
   Resultaat: Alle artsen maken ondertussen gebruik van de ehealth-box via het platform van Cozo (www.cozo.be) om patiënten-informatie te versturen. Twee van de 5 artsen gaven aan nog gebruik gemaakt te hebben van e-mail.
   De secretaresses versturen niet langer patiënten-informatie, ze laten dit over aan de artsen.

3. **Enkel praktijk-gerelateerde zaken:**
   De artsen en secretaresses werden gevraagd of ze in de afgelopen maand hun pc nog hadden gebruikt voor niet praktijk-gerelateerde zaken.
   Resultaat: De secretaresses geven aan dit niet te doen. De artsen geven, buiten het raadplegen van enkele nieuwssites, aan de computer enkel te gebruiken voor praktijk gerelateerde zaken.

4. **Verificatie van ontvangers van patiënten-informatie**
   De secretaresses werden gevraagd of ze in de afgelopen maand steeds hadden geverifieerd of de dokter naar wie ze patiënten-informatie doorspeelden effectief was wie hij vertelde te zijn.
   De artsen werd gevraagd of ze gebruik hadden gemaakt van de e-healthbox om zo de ontvanger te kunnen verifieren.
   Resultaat: De secretaresses geven niet langer patiënten-informatie door aan derden, ze laten dit over aan de artsen. De artsen geven aan enkel nog patiënten-informatie via het ehealth-box platform te sturen.

5. **Handmatige virus-scan**
   De systeembeheerder werd gevraagd of hij de afgelopen periode maandelijks een handmatig diepe virus-scan had uitgevoerd.
   Resultaat: De systeembeheerder gaf aan dat hij dit gedaan had en dit maandelijks zou blijven uitvoeren.

6. **Frequentere updates**

   De systeembeheerder werd gevraagd of hij de afgelopen maand de software op de pc's geüpdatet had.

   Resultaat: De systeembeheerder gaf aan dat dit het geval was en dat vanaf nu de updates maandelijks zouden worden toegepast door hem.

7. **Encryptie harde schijven**

   De systeembeheerder werd gevraagd of de harde schijven van de server, pc's, NAS en externe harde schijven ondertussen van encryptie werden voorzien.

   Resultaat: Dit blijkt nog niet het geval te zijn. Blijkbaar is dit moeilijker dan initieel gedacht en zou er hiervoor een upgrade van de server en computers nodig zijn om een vlotte werking toe te laten. Encryptie zal dus enkel worden toegepast bij een nog door te voeren upgrade van de computer-apparatuur in de praktijk.

8. **Paswoord-beleid**

   De artsen en secretaresses werden gevraagd of

   - ze nog gebruik maakten van een paswoord dat gelijk is aan de username

     Resultaat: Dit is niet langer het geval.

   - ze nog paswoorden hergebruiken voor verschillende applicaties

     Resultaat: Dit is niet langer het geval.

   - ze nog paswoorden gebruiken die korter zijn dan 12 karakters

     Resultaat: Dit is niet langer het geval

   - ze nog paswoorden gebruiken die niet een combinatie van *letters en cijfers* of *letters en leestekens* bestaan.

     Resultaat: Dit is niet langer het geval

   - ze nog paswoorden gebruiken die het volgende bevatten:

     - De naam van een familielid of huisdier
     - Opeenvolgende reeksen zoals bv abcde, 12345, …
     - Bestaande woorden die terug te vinden zijn in een woordenboek

     Resultaat: Dit is niet langer het geval

   - ze hun paswoorden ergens opschrijven

     Resultaat: Dit is niet langer het geval

   - ze hun paswoorden minimaal halfjaarlijks zullen vervangen

     Resultaat: Zowel artsen als secretaresses gaven aan dit te zullen doen in de toekomst.

IV Conclusie

Er werden d.m.v. de opgestelde vragenlijst en observaties verschillende pijnpunten in de beveiliging van de elektronisch opgeslagen patiëntendata vastgesteld. Aan de hand van deze zwakheden werden praktijkrichtlijnen opgesteld. Deze werden goed opgevolgd door de artsen, secretaresses en systeembeheerder. Er is echter wel nog ruimte voor verbetering.
De toepassing van deze praktijkrichtlijnen heeft er voor gezorgd dat de beveiliging van de elektronisch opgeslagen patiëntendata er op vooruitging. De onderzoeksvraag **"Is het mogelijk d.m.v. praktijkrichtlijnen de beveiliging van elektronisch opgeslagen patiëntendata te verbeteren?"** kan men bij deze dan ook positief beantwoorden.

V Discussie

Over het algemeen kan gesteld worden dat de voorgestelde verbeteringen goed werden opgevolgd door de artsen, secretaresses en systeembeheerder. Dit was enkel mogelijk doordat zij goed geïnformeerd waren over de noodzaak van de veranderingen. Hierdoor waren zij erg gemotiveerd om mee te werken, wat er voor heeft gezorgd dat er nu op een veiligere manier wordt omgegaan met de patiënten-data opgeslagen in de praktijk. Hiermee lijkt de doelstelling van dit praktijk-verbeterend project te zijn gehaald. Wel blijven er nog een aantal pijnpunten over die verdere aandacht vereisen. Zo moet er nog werk worden gemaakt van een draaiboek, moeten de keyboards nog vervangen worden en dient er nog meer op het afsluiten van de kabinetten te worden gelet. Encryptie van de harde schijven en Mac-adres filtering bleken op dit moment jammer genoeg nog niet mogelijk wegens beperkingen in de huidige hardware. Wil men deze verbeter-punten alsnog realiseren dan zal men de hardware hiervoor nodig moeten upgraden.

Wat opvalt is dat het relatief makkelijk was gedragingen van de artsen en secretaresses te veranderen, maar dat veranderingen die gekoppeld zijn aan nieuwe hardware minder vlot gebeurden. Een verklaring kan zijn dat de systeembeheerder meer tijd nodig heeft om deze laatste te implementeren. Tijdens deze masterproef kwam naar voor dat de artsen en secretaresses de juiste intenties hebben i.v.m. computer-beveiliging. Het zal er voor hen vooral op aankomen de doorgevoerde verandering aan te houden wil men verder in een optimale computer-beveiliging voorzien. De systeembeheerder zal hierbij een ondersteunende en controlerende functie te vervullen hebben.

Ook kwam naar voor dat er bij de artsen een vraag naar informatie is, maar dat zij vaak niet goed weten waar die te vinden is. Een beroepsvereniging zoals Domus Medica en ook de overheid zouden hier een belangrijke rol in kunnen spelen. Eveneens zou het volgens mij een goed idee zijn moesten artsen tijdens hun opleiding ook een notie van computer-beveiliging meekrijgen aangezien het goed beveiligen van vertrouwelijke patiënten-data deel uitmaakt van een goede patiënten-zorg.

Zoals bij aanvang van dit onderzoek bleek, zijn er echter geen richtlijnen, artikels of handboeken gericht op de huisarts-setting beschikbaar. Ook na afronding van dit onderzoek bleken deze niet voorhanden. Dit onderzoek heeft zowel zijn sterke als minder sterke punten. Eén van de zwakkere punten is het feit dat niet kan gecontroleerd worden of de deelnemers aan de vragenlijsten eerlijk antwoorden. Bovendien is het niet ondenkbaar dat bv. de secretaresses niet eerlijk durven antwoorden op bepaalde vragen omdat hun werkgevers (de dokters) de antwoorden ook te zien krijgen. Een ander zwak punt is het feit dat de beveiliging afhangt van het blijvend toepassen van de richtlijnen. Tijdens de introductie leefden de artsen, secretaresses en systeembeheerder deze laatste goed na. Of ze dit in de toekomst -bij mijn afwezigheid- zullen blijven doen is onzeker.

Een van de sterke punten van dit onderzoek is dat het de artsen, secretaresses en systeembeheerder goed heeft geïnformeerd van het belang van computer-beveiliging. Deze bewustvorming heeft geleid tot een motivatie en wil tot verandering. Een ander sterk punt van dit onderzoek is het feit dat de artsen, secretaresses en systeembeheerder met de praktijkrichtlijnen een makkelijk op te volgend leidraad hebben. Dit maakt de computer-beveiliging in de praktijk een stuk praktischer en makkelijker toe te passen.

Zelf heb ik door de concrete uitwerking van de verbeteringen heel wat praktische kennis opgedaan die ik zeker zal kunnen toepassen bij de opstart van mijn eigen praktijk volgend jaar. Ik merk dat bij de

huisartsen in mijn kenniskring er ook een vraag is naar concrete informatie i.v.m. computerbeveiliging, die ik hen dan ook met veel plezier geef. Het lijkt mij echter ook interessant de kennis opgedaan in dit onderzoek te implementeren in andere praktijken. Dit zou bv. gedaan kunnen worden via presentaties op LOK-vergaderingen en op seminaries voor HAIO's. Ook zou een draaiboek i.v.m. computer-beveiliging in de huisartspraktijk beschikbaar kunnen worden gesteld voor huisartsen. Moest in de toekomst de opportuniteit zich voordoen om mee te werken aan een richtlijn i.v.m. veilig omgaan met elektronisch opgeslagen patiëntendata dan zou ik hier met plezier aan meewerken.

VI Referenties

1. Wat is de relatie tussen het eHealth-platform en de Kruispuntbank van de Sociale Zekerheid? Beschikbaar via:https://www.ehealth.fgov.be/nl/over-het-ehealth-platform/veelgestelde-vragen/relatie-tussen-ehealth-en-ksz, eHealth-platform. Geraadpleegd 2014 maart 1.
2. Anseeuw K. Hoe is het gesteld met de beveiliging van de huisarts-pc? Proefschrift in het kader van het behalen van de master in de geneeskunde VUB 2012.
3. De Wolf L. Het reportagemagazine "Koppen" op Eén heeft vastgesteld dat het erg makkelijk is om door te dringen in databases met vertrouwelijke gegevens. Dat blijkt uit een reportage van "Koppen" over veiligheid van persoonsgegevens. Deredactie.be 2014. Beschikbaar via: http://deredactie.be/cm/vrtnieuws/binnenland/1.2120513. Geraadpleegd 2014 oktober 12.
4. Petitjean F. Gekraakte database mensura treft al duizend belgen. ZDNETBENELUX 2014. Beschikbaar via: http://www.zdnet.be/nieuws/159272/gekraakte-database-mensura-treft-al-duizend-belgen. Geraadpleegd op 2014 november 20.
5. ICT reglement apotheek. De Koninklijke Nederlandse Maatschappij ter bevordering der Pharmacie is de beroeps- en brancheorganisatie voor apothekers 2013. Beschikbaar via: http://http://nen7510.knmp.nl/toolkit. Geraadpleegd op 2014 maart 13.
6. Huyghens M. Informatiebeveiliging in kleinere organisaties. Open Universiteit Nederland 2013. Beschikbaar via: http://dspace.ou.nl/handle/1820/4579 20/11/2012. Geraadpleegd op 2014 april 20.
7. Volonino L, Anzaldua R. Computer Forensics For Dummies. USA: Wiley; 2008. p. 388.
8. Altheide C, Harlan. Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on TargetSystems: Windows, Mac, Linux, Unix, etc. USA: Elsevier; 2011. p. 288.
9. Karsten Nohl S, Lell K. BadUSB — On accessories that turn evil. Security Research Labs 2014. Beschibaar via: https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf. Geraadpleegd 2014 juli 30.
10. ZHENG M, et al. Understanding the robustness of SSDS under power fault. FAST 2013; 271-284.
11. Bradbury D. Can we make email secure?. Network Security 2014; 3: 13-16.
12. Password Protection Policy. Sans Institute 2014. Beschikbaar via: https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy. Geraadpleegd 2014 maart 20.
13. Orgill GL, Romney GW, Bailey GM. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Proceedings of the 5th conference on Information technology education. New York: ACM; 2004: p. 177-181.
14. Hoffman C. 6 ways windows 8 is more secure than windows 7, Howtogeek.com 2012. Beschikbaar via: http://www.howtogeek.com/128182/6-ways-windows-8-is-more-secure-than-windows-7. Geraadpleegd 2014 maart 20.
15. Cavit D, Meyer M, Salido D. Microsoft security intelligence report: Global threat assessments for 117 countries/regions 2010. Beschikbaar via: https://www.microsoft.com/en-us/download/details.aspx?id=17030. Geraadpleegd 2014 maart 20.
16. Goodin D. Meet KeySweeper, the $10 USB charger that steals MS keyboard strokes. Always-on sniffer remotely uploads all input typed into Microsoft Wireless keyboards. Ars Technica 2015. Beschikbaar via: http://arstechnica.com/security/2015/01/13/meet-keysweeper-the-10-usb-charger-that-steals-ms-keyboard-strokes. Geraadpleegd 2015 januari 1.

Universitair Ziekenhuis Brussel

Vrije Universiteit Brussel

COMMISSIE MEDISCHE ETHIEK (O.G. 016)
Reflectiegroep Biomedische Ethiek
Laarbeeklaan 101
1090 BRUSSEL

Tel + 32 2 477 55 84
Fax + 32 2 477 55 94
commissie.ethiek@uzbrussel.be

PROF. DR. D. DEVROEY
VAKGROEP HUISARTSGENEESKUNDE
VUB

Brussel, 15-04-2014

Ons Kenmerk: **2014/090**

ADVIES VAN DE COMMISSIE MEDISCHE ETHIEK

Betreft :
Hoe kan de beveiliging van de huisarts-PC verbeterd worden? Wat zijn de lacunes? Hoe te verbeteren?
B.U.N. 143201420547

Na kennis genomen te hebben van de documenten betreffende het bovenvermelde project, besluit de Commissie Medische Ethiek tijdens haar vergadering van **15 april 2014**

dat de voorziene studie mag ondernomen worden.

Deze goedkeuring blijft geldig voor de duur van het project. De Commissie wenst een jaarlijks overzicht van de stand van zaken van het project te ontvangen. De studieresultaten dienen overgemaakt te worden aan de Commissie bij het beëindigen van de studie. Zij herinneren de verantwoordelijke van het experiment eraan dat dit experiment onder zijn persoonlijke verantwoordelijkheid zal worden uitgevoerd. Het gunstig advies van de Commissie betekent geenszins dat de Commissie de verantwoordelijkheid van het experiment op zich neemt. De Commissie Medische Ethiek werkt en is georganiseerd volgens de richtlijnen van ICH-GCP.

Met de meeste hoogachting,

A. Van Steirteghem, voorzitter

Cc: FAGG, Departement R&D, Eurostation blok 2, Victor Hortaplein 40 / 40, 1060 BRUSSEL

Universitair Ziekenhuis Brussel

Vrije Universiteit Brussel

COMMISSIE MEDISCHE ETHIEK (O.G. 016)
Reflectiegroep Biomedische Ethiek
Laarbeeklaan 101
1090 BRUSSEL

tel + 32 2 477 55 84
Fax + 32 2 477 55 94
commissie.ethiek@uzbrussel.be

Meeting date: 15-04-2014

Ons Kenmerk : 2014/090

MEMBERS OF THE MEDICAL ETHICS COMMITTEE UZ BRUSSEL - VUB (since 20-11-2013)

Name	Function	Gender	participated in vote	present
Prof. Dr. Em. A. Van Steirteghem, MD	CHAIRMAN UZ BRUSSEL	M	☒	☒
Dr. J. Marchand, MD	VICE- CHAIRMAN Pediatrics UZ BRUSSEL	M	☒	☒
Dr. Y. Adriaenssens, MD	General Practitioner Van Hoeystraat 7, Mechelen	M	☐	☐
Dr. K. Beeckman, PhD	Nursing and Midwifery research group UZ BRUSSEL	F	☐	☐
Dr. Apr. V. Caveliers, PhD	Pharmacist UZ BRUSSEL	F	☒	☒
Prof. Dr. H. De Boeck, MD	Pediatric Orthopedics UZ BRUSSEL	M	☒	☒
Prof. Dr. J. De Grève, MD	Medical Oncology UZ BRUSSEL	M	☒	☐
Prof. Dr. J. De Mey, MD	Radiology UZ BRUSSEL	M	☒	☐
Mrs. M. De Win	External Member	F	☒	☒
Mr. D. Danschutter	Head Nurse UZ BRUSSEL	M	☐	☐
Prof. Dr. P. Haentjens, MD	Faculty of Medicine and Pharmacy VUB	M	☒	☐
Prof. Dr. P. Lacor, MD	Internal Medicine UZ BRUSSEL	M	☒	☒
Prof. Dr. J. Poelaert, MD	Anesthesiology UZ Brussel	M	☐	☐
Prof. Dr. J. van der Werff ten Bosch, MD	Pediatrics UZ BRUSSEL	F	☒	☐
Prof. Dr. T. Vanhaecke, MD	Toxicology - Faculty of Medicine and Pharmacy VUB	F	☒	☒
Dr. L. Wostyn, MD, Master of Laws	Master of Laws VUB External member	M	☐	☐

If member of the Ethics Committee, the investigator does not participate to the vote

Studieprotocol: Hoe kan de beveiliging van de huisarts-pc verbeterd worden? Wat zijn de lacunes? Hoe te verbeteren? (werktitel)

1. **Context**

   Dit onderzoek is een vervolg op de masterproef *"Hoe is het gesteld met de beveiliging van de huisarts-pc? Een onderzoek naar de veiligheid van de digitale patiëntgegevens bij de huisarts."*
   Waar er bij dit eerste onderzoek gekeken werd hoe het gesteld is met de veiligheid van de gemiddelde huisarts-pc ligt de nadruk bij dit onderzoek meer op hoe deze veiligheid best kan worden verbeterd in het kader van een praktijk-verbeterend project.
   In dit onderzoek zullen de eerder gevonden algemene zwakke punten i.v.m. computer-beveiliging van de huisarts-pc afgetoetst worden en waar nodig aangepakt worden in een praktijk-verbeterend project.
   Het is m.a.w. de bedoeling te gaan kijken hoe het gesteld is met de veiligheid van de computers in een specifieke praktijk rekening houdend met de algemene lacunes in de beveiliging van de huisarts-pc die naar voor kwamen in het eerder onderzoek.

2. **Vraagstelling**

   Hoe kan de beveiliging van de huisarts-pc verbeterd worden? Wat zijn de lacunes en hoe kan dit worden aangepakt?

3. **Methode**

   In dit praktijk-verbeterend project zal in een eerste fase d.m.v. een vragenlijst voor de artsen werkzaam in de praktijk worden nagegaan hoe het gesteld is met de beveiliging van de de computers gebruikt in de praktijk. Deze vragenlijst is opgesteld d.m.v. de kennis opgedaan in het eerdere masterproef-onderzoek. Aan de hand van de vastgestelde lacunes zal een voorstel worden gedaan ter verbetering van deze computer-beveiliging d.m.v. concrete richtlijnen.
   In een tweede fase zal onderzocht worden hoe deze richtlijnen zijn opgevolgd en wat het effect hiervan is op de computer-beveiliging. Iedere arts zal na het ontvangen van de richtlijnen trachten deze zo goed mogelijk na te leven. Het zal sowieso een uitdaging zijn om deze richtlijnen allemaal en correct in de praktijk te implementeren. Er bestaat geen twijfel over dat ook op het punt van deze implementatie tijdens de voortgang van deze thesis verbeterpunten

voor onze praktijk zullen ontdekt worden.

4. **Timing**

-Literatuurstudie, bepalen definitieve variabelen en afnemen vragenlijst: mei 2014 tot en met juli 2014.
-Gegevensverzameling, verwerking naar werkbare formaten en opstellen van richtlijnen: juli 2014 tot en met oktober 2014.
-Toepassen en evaluatie van effect richtlijnen: oktober 2014 tot en met februari 2015
-Verwerken van resultaten en verder schrijven van masterproef: februari 2015 tot en met april 2015.

5. **Literatuur**

– Anseeuw K. Hoe is het gesteld met de beveiliging van de huisarts-pc? Een onderzoek naar de veiligheid van de digitale patiëntgegevens bij de huisarts. Thesis master of medicin, VUB
– Nog aan te vullen...

1. Vragen voor artsen en secretaresses

1.1. Perceptie

1.1.1. Hoe schat u de beveiliging van de computers in de praktijk in?
1.1.2. Hoe schat u uw kennis over informatica in het algemeen?
1.1.3. Vindt u dat u genoeg wordt geïnformeerd door de overheid inzake computerbeveiliging
1.1.4. Vindt u dat u genoeg wordt geïnformeerd door uw vakvereniging (domus medica) inzake computerbeveiliging
1.1.5. Indien deze makkelijk beschikbaar was zou u dan graag meer informatie krijgen over een goede beveiliging van uw pc?
1.1.6. Vind u het de taak van de huisarts om zich bezig te houden met computerbeveiliging?
1.1.7. Vindt u dat er bepaalde verplichtingen omtrent computer beveiliging zouden moeten worden gesteld aan huisartsen?
1.1.8. Bent u van mening dat de beveiliging van de computers in uw praktijk beter is dan bij de gemiddelde huisartspraktijk?
1.1.9. Bent u van mening dat u het nodige doet om een goede beveiliging van de computers in uw praktijk te verzekeren?
1.1.10. Hoe goed scoort u volgens uzelf op het vlak van computerbeveiliging in vergelijking met uw collega's in de praktijk?
1.1.11. Hoe belangrijk vindt u de beveiliging van de pc's in uw praktijk in het kader van een goede patiëntenzorg?

1.2. Fysieke beveiliging van de pc

1.2.1. Zet u uw pc uit of meldt u zich af uit Windows als u uw kabinet verlaat (korte periodes om naar het toilet te gaan of een nieuwe patiënt te halen uitgesloten).
1.2.2. Sluit u uw kabinet af als u het verlaat? (korte periodes om naar het toilet te gaan of een nieuwe patiënt te halen uitgesloten).
1.2.3. Sluit u soms opslagmedia (usb-stick/cd-rom/externe harde schijf) die u ook buiten de praktijk gebruikt aan op uw praktijk-pc? (bv usb stick die u ook gebruikt voor privé-gebruik)

1.3. Computerhygiëne

1.3.1. Communiceert u met uw collega artsen (binnen en buiten de praktijk) over patiënten-dossiers via email?
1.3.2. Worden dit email-verkeer geëncrypteerd?
1.3.3. Gebruikt u uw e-healthbox om te communiceren met collega artsen over patiëntendossiers?
1.3.4. Gebruikt u uw praktijk-pc voor niet praktijk gerelateerde zaken?
1.3.5. Geeft u telefonisch/per fax/via e-mail informatie door aan derden zonder dat u deze kent (bv een voor u onbekende collega die om informatie vraagt over een patiënt)

1.4. Paswoordgebruik

In deze sectie worden vragen gesteld over de paswoorden die u gebruikt op uw praktijk-pc. Dit zijn o.a. uw paswoord om in Windows in te loggen, uw paswoord om in windoc in te loggen, uw paswoord van uw e-health sessies, uw paswoord om uw

mailbox te openen,...

1. Sommige van mijn paswoorden zijn gelijk aan mijn login
2. Ik gebruik hetzelfde paswoord voor verschillende toepassingen
3. Sommige van mijn paswoorden zijn korter dan acht symbolen
4. Mijn paswoorden bestaan uit een combinatie van letters en cijfers/ letters en leestekens/ cijfers en leestekens/ letters, cijfers en leestekens

5. Andere mensen kennen één/meerdere van uw paswoorden?
6. Mijn paswoord(en) staat(n) ergens opgeschreven zodat ik ze makkelijk kan lezen (bvb post-it op pc)
7. Mijn paswoord is/ bestaat gedeeltelijk uit
   - naam van familielid/huisdier
   - een bestaand woord dat in het woordenboek terug te vinden is
   - een opeenvolgende reeks van letters van tekens (bvb 123456789, abcdefg,...)
8. Ik verander mijn paswoord(en) regelmatig (min. 1x om de 6 maand)?
9. Ik denk dat mijn paswoorden makkelijk te raden zijn
10. Ik zou graag meer informatie ontvangen over hoe ik een goed paswoord maak.
11. Als u zich inschrijft voor een bepaalde dienst (bvb het online kunnen raadplegen van labo uitslagen) dan krijgt u een standaard paswoord. Veranderd u dit standaard paswoord na ontvangst?

2. Vragen voor systeembeheerder

2.1. perceptie

2.1.1. Bent u van mening dat de informatica-systemen in de praktijk goed beveiligd zijn?
2.1.2. Bent u van mening dat u voldoende middelen en tijd ter beschikking krijgt om in een goede beveiliging van het ict-systeem in de praktijk te voorzien?
2.1.3. Bent u van mening dat er hardware-matige veranderingen in de praktijk nodig zijn om de computer-beveiliging te verbeteren?
2.1.4. Bent u van mening dat er software-matige veranderingen in de de praktijk nodig om de computer-beveiliging te verbeteren?
2.1.5. Bent u van mening dat de dokters en secretaresse in de praktijk hun gedrag ivm. computerbeveiliging zouden moeten aanpassen om in een goede beveiliging van het ict-systeem in de praktijk te voorzien?
2.1.6. Bent u van mening dat de artsen/personeel in de praktijk een goede computerbeveiliging belangrijk vinden.
2.1.7. Bent u van mening dat de artsen/personeel in de praktijk openstaan voor veranderingen die de beveiliging van de computers zou verbeteren?

2.2. Fysieke beveiliging

2.2.1. Is er een UPS aanwezig in de praktijk?
2.2.2. Is er een stroompiekbeveiliging aanwezig in de praktijk?
2.2.3. Worden back-ups gemaakt van de computergegevens?
2.2.4. hoe vaak?
2.2.5. op welke mediums (nas/externe hd/cloud)?
2.2.6. bevindt deze back-up zich op een plaats buiten de praktijk?

2.2.7. Wordt er een hardware firewall gebruikt om het Lan-netwerk van de praktijk af te schermen?

2.2.8. Hoe regelmatig wordt de firmware van deze firewall geüpdatet?

2.3. Software-matige beveiliging

2.3.1. Zijn de computers in de praktijk beschermd tegen malware d.m.v. een antivirus-programma?

2.3.2. Ontvangt deze automatisch updates van malware-definities?

2.3.3. Hoe vaak voert u een handmatig scan van de systemen uit om malware te detecteren?

2.3.4. Welke besturingssystemen worden in de praktijk gebruikt? (keuze win…)

2.3.5. Ontvangen al deze besturingssystemen automatische updates?

2.3.6. Hoe vaak gebeurd er een update van de software op de pc? (bv java/adobe reader/…)

2.3.7. Wordt er software gebruikt in de praktijk waar geen licentie voor werd betaald?

2.3.8. Wordt de data op de harde schijven van de server/pc's/nas geëncrypteerd? (via bv Windows bitlocker, truecrypt, andere encryptie software)

2.4. Preventie

2.4.1. Worden er audits gedaan van de computerbeveiliging?

2.4.2. Is er een beleid naar de gebruikers van de computer systemen toe inzake paswoord gebruik (specifieke regels en afspraken over de samenstelling en het gebruik van paswoorden)?

2.4.3. Is er een beleid naar de gebruikers van de computersystemen toe inzake veilig gebruik van de pc?

2.4.4. Hoe frequent worden de paswoorden in de praktijk veranderd?

2.5. Toegang

2.5.1. Hebt u als systeembeheerder toegang tot patiëntengegevens op de pc?

2.5.2. Kent u als systeembeheerder de paswoorden voor het medische programma van de dokters?

Verbeterpunten praktijk

Hieronder vinden jullie de verbeterpunten die naar voor kwamen uit mijn masterproef. Aarzel zeker niet om mij aan te spreken indien er onduidelijkheden zijn.

Uit te voeren door de artsen en secretaresses:

1. **Pc's afmelden/uitzetten:** Bij het verlaten van uw kabinet / bureau voor langere tijd moet de pc worden afgemeld of uitgezet.
2. **Kabinetten afsluiten:** Bij het verlaten van uw kabinet / bureau voor langere tijd moet deze worden afgesloten. Voor de kabinetten is het voldoende de deur dicht te trekken. Voor de front-desk moet de schuifdeur worden gesloten.
3. **USB-sticks:** USB-sticks die buiten de praktijk werden gebruikt mogen niet langer worden gebruikt.
4. **Back-ups:** De externe harde schijf in de serverkast moet elke avond door één van de artsen meegenomen en de volgende dag terug worden meegebracht en aangekoppeld.
5. **Versnipperaar:** Alle geprinte vertrouwelijke patiënten-informatie moet worden vernietigd in een versnipperaar voor deze in de afval container wordt gegooid. Als alternatief kan er gebruik gemaakt worden van het Labo die deze dan vernietigen.
6. **Encryptie communicatie/ Ehealth:** Communicatie over patiënten-dossiers met collega's dient te gebeuren via medimail zodat dit via de ehealth-box verloopt. Gewone email mag niet langer gebruikt worden.
7. **Enkel praktijkgerelateerde activiteiten:** Activiteiten die niet praktijk gerelateerd zijn (recreatief surfen) moeten vermeden worden op de pc's in de praktijk.
8. **Verificatie van ontvangers van patiënten-informatie:** De identiteit van onbekende collega's die om patiënten-informatie verzoeken moet geverifieerd worden. Dit kan telefonisch door zelf de arts terug te bellen op zijn verifieerbaar telefoonnummer. Geschreven communicatie dient via medimail te verlopen.
9. **Paswoord-beleid:** Onderstaande regels dienen te worden gevolgd i.v.m. paswoorden. Dit proces kan makkelijk **geautomatiseerd** worden d.m.v. een paswoord manager zoals **Lastpass**. Dit is een programma dat alle paswoorden voor u onthoudt en u ook bijstaat in het creëren van nieuwe veilige paswoorden. Het is terug te vinden in Firefox rechts bovenaan (rood vierkantje met wit sterretje). Idealiter wordt er gebruik gemaakt van 2 factor authenticatie d.m.v. de Google Authenticator smartphone app.
    - Er mogen geen paswoorden worden gebruikt die gelijk zijn aan de

gebruikersnaam (*zoals nu het geval is bij het inloggen bij Windoc en het telefoon programma aan de receptie)*

- Een paswoord mag slechts voor 1 applicatie gebruikt worden. Voor elke aparte applicatie dient een nieuw paswoord worden gebruikt. Hiervoor kan gebruik gemaakt worden van Lastpass.
- Een paswoord moet minimum 12 karakters lang zijn
- Een paswoord moet minimaal uit een combinatie van *letters en cijfers* of *letters en leestekens* bestaan. Ideaal bestaat het paswoord uit een combinatie van zowel *letters*, *cijfers* en *leestekens*.
- Een paswoord mag het volgende niet bevatten:
  - De naam van een familielid of huisdier
  - Opeenvolgende reeksen zoals bv abcde, 12345, …
  - Bestaande woorden die terug te vinden zijn in een woordenboek *(zoals bv Limburg)*
- Een paswoord mag nergens worden opgeschreven *(zoals bv. op post-its aan de computer schermen)*
- Elk paswoord moet om het half jaar gewijzigd worden.

Aan te kopen door de artsen:

1. **Versnipperaar:** Om de hierboven vermelde geprinte vertrouwelijke informatie te kunnen vernietigen
2. **Keyboards:** De huidige keyboards moeten vervangen worden door veilige keyboards die niet kunnen worden uitgelezen vanop afstand.

Uit te voeren door de systeembeheerder:

1. **Serverkast:** De kast moet worden afgesloten. Indien blijkt dat de ventilatiegaten niet voldoende zijn, moet er extra ventilatie worden voorzien.
2. **Automatisch afmelden bij inactiviteit:** Na 15 min niet meer gebruikt te zijn moeten de pc's zich afmelden uit Windows. Om terug verder te kunnen werken moeten de artsenterug inloggen.
3. **Handmatige virus-scan:** Er moet meer frequent een uitgebreide virus-scan worden uitgevoerd. Alternatief kan één van de artsen voldoende rechten worden gegeven zodat deze dit zelf kan doen.
4. **Vervanging Windows Xp:** De pc aan de front-desk moet voorzien worden van een nieuwer besturingssysteem dan het huidige Windows XP. In het geval er bepaalde applicaties op de pc Windows Xp vereisen en er geen alternatieven zijn kan er een virtuele machine worden gedraaid met Windows Xp. Deze virtuele machine mag niet over internet-toegang beschikken.

5. **Frequentere updates:** De software op de pc's (bv. Adobe reader, Java,..) dient frequenter te worden voorzien van updates. Dit kan ook gebeuren door de één van de artsen als die hiervoor de rechten wordt toegekend.

6. **Encryptie van de harde schijven:** Alle harde schijven in de praktijk moeten worden geëncrypteerd. Op de server, externe harde schijven en de pc's kan "Windows Bitlocker-stationsversleuteling" worden gebruikt. Op de NAS dient een optie in het menu worden geactiveerd zodat de harde schijven worden versleuteld.

7. **Draaiboek computer-beveiliging:** het beleid i.v.m. computer-beveiliging concreet te maken d.m.v. een draaiboek.

8. **Bios-lock:** De toegang tot het bios/EFI op de pc's moet afgeschermd worden d.m.v. een paswoord zodat niet langer de optie kan worden ingeschakeld om op te starten vanaf een USB-stick of dvd-rom.

9. **Uitzetten Sticky keys:** Sticky keys en andere hulpprogramma die kunnen misbruikt worden door kwaadwilligen moeten worden gedeactiveerd.

10. **Mac-adres filtering:** Er moet Mac-adres filtering worden toegepast op het netwerk waardoor enkel pc's die gekend zijn kunnen verbinding maken met de LAN.

11. **Uitzetten niet gebruikte wifi functionaliteit:** De draadloze functionaliteit van de printer aan de front-desk moet gedeactiveerd worden.

12. **Paswoord-beleid:**

    De huidige paswoorden dienen veranderd worden aangezien deze niet veilig zijn:

    - *paswoord medisch programma*
    - *paswoord telefoon programma aan de receptie*
    - *paswoord accounts Windows*

    Er moet een paswoord-beleid komen waarbij de paswoorden voldoen aan volgende voorwaarden:

    - De gebruikersnaam en het paswoord mogen niet gelijk zijn *(op dit moment is dit het geval voor Windoc en het telefoon programma aan de receptie)*
    - Een paswoord mag slechts voor 1 applicatie gebruikt worden
    - Een paswoord moet minimum 12 karakters lang zijn *(dit is bij enkel paswoord van toepassing op dit moment)*
    - Een paswoord moet minimaal uit een combinatie van *letters en cijfers* of *letters en leestekens* bestaan. Ideaal bestaat het paswoord uit een combinatie van zowel *letters*, *cijfers* en *leestekens*.
    - Een paswoord mag het volgende niet bevatten:

        - De naam van een familielid of huisdier
        - Opeenvolgende reeksen zoals bv abcde, 12345, …
        - Bestaande woorden die terug te vinden zijn in een woordenboek *(zoals bv. Limburg)*
    - Een paswoord mag nergens worden opgeschreven *(zoals bv. op post-its aan de computer schermen)*
    - Elk paswoord moet om het half jaar gewijzigd worden.

De artsen en secretaresses dienen hierin te worden ondersteund en gecontroleerd. Om dit proces gebruiksvriendelijker te maken kan eventueel gebruik gemaakt worden van een 'paswoord manager' zoals LastPass in combinatie met 'two factor authentication' zoals door 'Google authenticator voorzien. Deze is aanwezig als app in de firefox browser op de pc's.