PACSONWEB

Beoordeling van radiologiebeelden op afstand: veiligheidsrisico's beheren en optimale prestaties waarborgen

Whitepaper

Door:
Jan Dobbenie
CEO DOBCO Medical Systems

+32 (52)77 01 16
info@dobcomed.com
Nachtegaalstraat 6, 9240 Zele, België
www.pacsonweb.com

Inhoudsopgave

1. Inleiding 3

2. De veiligheidsrisico's van beoordeling op afstand 4

2.1 VPN-verbindingen op een eigen pc of laptop 4

2.2 Werkstations in eigendom en beheer van het bedrijf 6

2.3 VPN in combinatie met oplossingen voor virtuele desktops 7

3. Uitdagingen op het gebied van software en bandbreedte: lokaal versus cloud 8

4. Veilig en volledig native cloud-PACS 9

5. De evolutie van het native cloudplatform in de gezondheidszorg 11

6. PACSonWEB: native cloud-PACS voor beoordeling op afstand en meer 12

7. Literatuur 14

1. Inleiding

Radiologen beoordelen al vele jaren onderzoeksbeelden vanuit huis of vanaf andere locaties. Aanvankelijk werden de beelden geraadpleegd vanaf andere locaties in het ziekenhuis of in een privépraktijk via een LAN (Local Area Network) verbonden met een PACS (Picture Archiving And Communication System) van het ziekenhuis. Tegenwoordig zijn de mogelijkheden voor beoordeling op afstand aanzienlijk uitgebreid. Radiologen kunnen altijd en overal, thuis of via een WAN (Wide Area Network), toegang krijgen tot beelden met volledige PACS-functionaliteit.

De mogelijkheid om beelden te bekijken vanaf elke gewenste locatie buiten het ziekenhuis is bijzonder nuttig gebleken tijdens de coronapandemie. In deze periode is beoordeling op afstand uitgegroeid tot een belangrijke manier om sociale contacten te beperken en kwetsbare radiologen en anderen in het ziekenhuis te beschermen. Bovendien garandeert beoordeling op afstand naadloze interpretatiemogelijkheden in noodscenario's, zo blijkt uit een open-access-artikel dat voorafgaand aan de gedrukte versie elektronisch is gepubliceerd door het American Journal of Roentgenology (AJR).[1]

Om te voldoen aan de vraag naar beoordeling op afstand, worden organisaties in de gezondheidszorg echter geconfronteerd met meerdere uitdagingen: van het leveren van de juiste middelen aan radiologen voor beoordeling van thuis tot het bieden van een veilige werkomgeving.

In dit whitepaper onderzoeken we de verschillende mogelijkheden en veiligheidsaspecten, evenals de uitdagingen op het gebied van software en bandbreedte die beoordeling op afstand met zich meebrengt. We kijken ook naar de evolutie van het webgebaseerde cloudplatform in de gezondheidszorg en de voordelen van PACS in de cloud.

“Tegenwoordig zijn de mogelijkheden voor beoordeling op afstand aanzienlijk uitgebreid. Radiologen kunnen altijd en overal, thuis of via een WAN (Wide Area Network), toegang krijgen tot beelden met volledige PACS-functionaliteit.”

2. De veiligheidsrisico's van beoordeling op afstand

Tegenwoordig de dag worden IT-afdelingen met een hele reeks uitdagingen geconfronteerd. Volgens onderzoeks- en analyse-experts van Gartner behoren de schaarste aan technisch beveiligingspersoneel, de naleving van wetten en regelgeving en de gestage toename van nieuwe bedreigingen tot de belangrijkste beveiligingsuitdagingen.[2] Daarnaast heeft COVID-19 een enorme druk gelegd op organisaties om verder te digitaliseren en cloudcomputing te omarmen.

Daarbij komt dat IT-afdelingen in de gezondheidszorg niet groot zijn en een breed scala aan verantwoordelijkheden hebben. Het is niet altijd mogelijk om medisch personeel snel te voorzien van veilige laptops of andere apparaten van de werkgever. Hierdoor gebruiken veel radiologen hun persoonlijke apparaten (laptop, smartphone, tablet) om op afstand verbinding te maken en toegang te krijgen tot gegevens.

Wat is de beste aanpak om beoordeling op afstand snel en efficiënt op te schalen en tegelijkertijd de veiligheid te waarborgen en radiologen optimale systeemprestaties te garanderen? We bespreken eerst het gebruik van een VPN-verbinding (Virtual Private Network) in verschillende configuraties.

2.1 VPN-verbindingen op eigen pc of laptop

"Hoewel sommige beveiligingsprofessionals dit [het installeren van een VPN op de eigen pc van een werknemer] misschien als een aanvaardbare praktijk beschouwen, geeft dit beleid een hoog risico op een ongewenste aanvalsvector door het geven van toegang tot uw omgeving."

Morey Haber, 'The Dangers Of Using A VPN On Home Computers For Work And What To Do Instead,' Forbes Technology Council [3]

"COVID-19 heeft een enorme druk gelegd op organisaties om verder te digitaliseren en cloudcomputing te omarmen."

Een gangbare aanpak voor beoordeling op afstand is

radiologen te voorzien van een VPN-verbinding die ze kunnen gebruiken op hun eigen pc of laptop thuis. Hoewel deze optie gemakkelijk te installeren is, zijn er verschillende veiligheidsrisico's aan verbonden. De voornaamste zorgen volgens Morey Haber:

- **Meerdere gebruikers vergroten de risico's**

Pc's worden meestal door meerdere gezinsleden gebruikt. Als iemand slachtoffer wordt van phishingfraude of een andere aanval, bestaat de kans dat een virus wordt geüpload naar het virtuele netwerk van de organisatie. Technieken zoals het snel wisselen van gebruiker vergroten het probleem, omdat andere profielen in het geheugen blijven staan. Uiteindelijk zou een gebruiker die niet aan de organisatie is verbonden, gemakkelijk het virtuele netwerk van een hele organisatie in gevaar kunnen brengen als gevolg van de actieve VPN-sessieverbinding met de organisatie.

- **Onvoldoende beveiliging van de host en inadequate authenticatie**

De meeste VPN-oplossingen voor bedrijven integreren een certificaat in gebruikersprofielen of een verbinding om de verbinding te valideren. Dat gebeurt los van de authenticatie die gebruikers moeten verstrekken via inloggegevens en een andere vorm van twee-factorauthenticatie om een beveiligde verbinding te krijgen. De beveiliging van het certificaat en de authenticatiegegevens zijn echter net zo veilig als het beveiligingsonderhoud dat door de organisatie wordt toegepast. Deze vormen een doelwit bij uitstek voor cybercriminelen, die hun eigen verbindingen kunnen opzetten of zelfs sessies van externe werknemers kunnen kapen.
Dit vormt een groot veiligheidsrisico, want wanneer men er niet in slaagt om de host goed te beveiligen, zal dit ook gelden voor de beveiliging van de verbindingssoftware.

"Pc's worden meestal door meerdere gezinsleden gebruikt. Als iemand slachtoffer wordt van phishingfraude of een andere aanval, bestaat de kans dat een virus wordt geüpload naar het virtuele netwerk van de organisatie."

Bovendien kunnen oplossingen voor netwerktoegangscontrole wel versies van antivirushandtekeningen en elementaire hardwarekenmerken valideren, maar niet een thuiscomputer inventariseren en zorgen dat deze net zo goed wordt onderhouden en beveiligd als binnen een bedrijf. Deze beveiligingsgaten en inadequate authenticatie kunnen leiden tot datalekken als gevolg van malware die schermopnames maakt en toetsaanslagen vastlegt.

Lager niveau van verdediging tegen malware

Voor de meeste malware-aanvallen zijn beheerdersrechten vereist om een systeem te kunnen infecteren. Gebruikers van pc's zijn over het algemeen lokale beheerders van hun eigen computers. Als teamleden een ouder besturingssysteem hebben, lopen ze een groter risico. Volgens het AV-TEST 2019/2020 Security Report (AV-TEST is een onafhankelijk onderzoeksinstituut voor IT-beveiliging in Duitsland) zijn vooral Windows-computers kwetsbaar voor aanvallen: in 2019 werden 114 miljoen nieuwe stukjes kwaadaardige programma's ontwikkeld en 78,64 procent van alle aanvallen werd verspreid op Windows-systemen.[4]

Geen beveiligingssoftware

Niet iedereen maakt zich thuis druk om antivirussoftware. Naar schatting 25 procent van de pc's is niet beveiligd met antivirussoftware, en deze hebben ongeveer 5,5 keer meer kans om geïnfecteerd te raken.[5] Hoewel de bewustwording onder gebruikers van eigen computers toeneemt, zijn veel gebruikers niet op de hoogte van aanvullende beveiligingstools zoals Endpoint Detection en Response (EDR) en Endpoint Privilege Management (EPM).

"Veel gebruikers zijn niet op de hoogte van aanvullende beveiligingstools zoals Endpoint Detection en Response (EDR) en Endpoint Privilege Management (EPM)."

2.2 Werkstations in eigendom en beheer van het bedrijf

Sommige organisaties in de gezondheidszorg hebben ervoor gekozen radiologen te voorzien van werkstations die eigendom zijn van het bedrijf en door het bedrijf worden beheerd. Met deze oplossing kunt u ervoor zorgen dat radiologen niet via hun eigen computer thuis gebruikmaken van de VPN van

de organisatie. Het werkstation van het bedrijf werkt als een gewoon PACS-werkstation en het kan zelfs een beheerde asset zijn, wat de eerder besproken risico's tot een minimum zou beperken.

Deze oplossing heeft echter een prijs: deze werkstations moeten worden beheerd, bijgewerkt en ondersteund door de organisatie. In veel gevallen zijn organisaties of IT-afdelingen in de gezondheidszorg niet zo ingericht of gestructureerd dat ze hardware en software buiten de muren van de organisatie kunnen ondersteunen, vooral niet wanneer het gaat om de gespecialiseerde hardware en software die radiologen nodig hebben. Er zijn extra mensen en maatregelen nodig om de systemen bij te werken en te beheren om de veiligheid, de prestaties en het vereiste serviceniveau te waarborgen. Voor radiologen zijn deze werkstations het voornaamste hulpmiddel voor het beoordelen van onderzoeken en dus onmisbaar.

Bovendien kunnen prestaties nog steeds een probleem vormen en daarom moeten dergelijke computers in meerdere scenario's worden geëvalueerd en (stress)tests ondergaan. **In de meeste gevallen worden VPN's opgezet via een gedeelde internetverbinding met de organisatie. Dit betekent dat de vereiste prestaties niet kunnen worden gegarandeerd, omdat er sprake kan zijn van een gebrek aan uploadbandbreedte bij de zorgorganisatie.**

2.3 VPN in combinatie met een oplossing voor virtuele desktops

Dit type oplossing is wijdverspreid binnen organisaties in de gezondheidszorg. Deze oplossingen (zoals Citrix, VirtualBox, Horizon, en andere) maken op de thuiscomputer van de arts een virtuele desktop aan met toegang tot de applicaties van de zorgorganisatie. Het is een geïsoleerde omgeving die de eerdergenoemde risico's tot een minimum beperkt. Deze oplossingen zijn (over het algemeen) uit veiligheidsoogpunt de juiste keuze en bovendien betrekkelijk eenvoudig te implementeren. Hoewel deze dus erg nuttig zijn voor de meeste ziekenhuisapplicaties die een arts thuis nodig heeft

"Oplossingen (zoals Citrix, VirtualBox, Horizon, en andere) maken op de thuiscomputer van de arts een virtuele desktop aan met toegang tot de applicaties van de zorgorganisatie."

(bijvoorbeeld om toegang te krijgen tot het EMR), zijn ze niet geschikt om onderzoeken in PACS te lezen. Scrollen door grote datasets, window leveling, 3D en spraakherkenning werken simpelweg niet goed genoeg via dit soort oplossingen.

Daar zijn verschillende redenen voor: geen ondersteuning voor meerdere beeldschermen, de vernieuwingsfrequentie van de omgeving, het gebrek aan ondersteuning voor randapparatuur, enzovoort. De algemene ervaring is dat deze omgevingen onvoldoende prestaties bieden om gespecialiseerde applicaties zoals PACS uit te voeren. Daar komt nog bij dat het weergeven van lossless DICOM-beelden met behulp van externe of virtuele desktoptechnieken een potentieel risico vormt, omdat het beeld kan worden gecomprimeerd of vervormd door de virtuele desktopsoftware.

3. Uitdagingen op het gebied van software en bandbreedte: lokaal versus de cloud

Naast de zorgen over de beveiliging moeten IT-teams in de gezondheidszorg de installatie van meerdere software-applicaties en de bandbreedtevereisten beheren voor radiologen, zodat deze op hun eigen pc beelden op afstand kunnen beoordelen. Een standaard PACS-werkstation bestaat uit meerdere beeldschermen en vereist de installatie van verschillende applicaties, zoals de PACS-software, de spraakherkenningssoftware en de RIS-clientsoftware (radiologie-informatiesysteem).

Deze applicaties zijn vooral ontworpen voor LAN-verbindingen, omdat PACS een verbinding met hoge bandbreedte en lage latentie tussen de cliënt en de server vereist. Dat is vanwege de grote datasets die worden verwerkt. Alleen met een LAN-verbinding kan kan een vlotte beeldweergave worden gegarandeerd, met name voor CT- en MR-onderzoeken. Eén enkele CT-scan kan bijvoorbeeld meerdere GB in beslag nemen.

"Webgebaseerde PACS-oplossingen in de cloud daarentegen elimineren de veiligheidsrisico's van het gebruik van een VPN, vereisen geen installatie van software om op afstand lossless DICOM-beelden van hoge kwaliteit te bekijken, en zijn beschikbaar via elke browser op elk apparaat dat met internet is verbonden."

De vernieuwingsfrequentie voor het weergeven van de beelden is ook van belang wanneer de radioloog met beelden werkt, bijvoorbeeld bij gebruik van window leveling. Hoewel radiologen thuis kunnen kiezen voor een internetverbinding met een hogere bandbreedte, moet ook de verbinding van het ziekenhuis de uploadsnelheid aankunnen die nodig is voor meerdere gelijktijdige sessies met verschillende applicaties.

Eén aanpak die verschillende PACS-leveranciers hebben toegepast om bandbreedteproblemen op te lossen, is het cachen van de beelden op het werkstation. In veel gevallen is de inhoud van de cache niet versleuteld, wat leidt tot nog grotere veiligheids- en privacyrisico's voor de patiënt, omdat de gegevens zich op de lokale schijven bevinden. Bovendien zijn internetverbindingen gevoelig voor hoge latentie en verbindingsdips, waarvoor de PACS-werkstationsoftware niet ontworpen is.

Gelet op de beveiligingsuitdagingen, behoefte aan meerdere softwareapplicaties voor medische beeldvorming en aanzienlijke bandbreedte voor radiologen, wat zijn dan alternatieve opties voor een veilige, beveiligde en snelle opschaling voor de beoordeling van radiologiebeelden buiten het ziekenhuis?

"Eén enkele CT-scan kan meerdere GB in beslag nemen."

4. Veilig en volledig, dankzij het cloud- en webgebaseerde karakter

Hoewel het gebruik van een VPN, de installatie van lokale software en het ter beschikking stellen van een pc aan radiologen een aantal van de veiligheids- en prestatie-problemen voor beoordeling op afstand kunnen verhelpen, blijft deze aanpak risicovol en vereist deze aanzienlijke ondersteuning van IT-afdelingen.

Webgebaseerde PACS-oplossingen in de cloud daarentegen elimineren de veiligheidsrisico's van het gebruik van een VPN, vereisen geen installatie van software om op afstand

lossless DICOM-beelden van hoge kwaliteit te bekijken, en zijn beschikbaar via elke browser op elk apparaat dat met internet is verbonden.

De veiligheid is gewaarborgd doordat de client wordt gereduceerd tot een browser die via https communiceert met de cloudomgeving. Er blijven geen gegevens achter op de lokale pc of het lokale werkstation en er is geen clientbeheer nodig. Deze veilige weboplossingen implementeren technieken voor multifactorauthenticatie en uitgebreide logboekregistratie. Upgrades zijn beperkt tot de cloudomgeving en de software kan op elk apparaat of besturingssysteem draaien. Vanuit de cloud kunnen bandbreedten worden geschaald en verbindingen worden gedupliceerd om een hoge beschikbaarheid te garanderen.

Dankzij de volledige ondersteuning in de cloud kunnen radiologen:

- **(voorlopige) rapporten voorbereiden op een externe locatie, zoals thuis of een ander kantoor;**
- **eenvoudig samenwerken met andere groepen en radiologen bij het beoordelen van beelden;**
- **toegang krijgen tot de volledige PACS-functionaliteit zonder VPN of complexe IT-infrastructuur.**

Bovendien worden beelden en rapporten in realtime aan elkaar gekoppeld en wordt de gedicteerde tekst gelijktijdig op het scherm weergegeven. Na voltooiing wordt het rapport in het lokale radiologie-informatiesysteem (RIS) of het elektronisch medisch dossier (EMR) opgenomen.

5. De evolutie van het webgebaseerde cloudplatform in de gezondheidszorg

Een webgebaseerd cloudplatform is algemeen geaccepteerd en wordt toegepast op talloze gebieden, zoals thuisbankieren, kantoorapplicaties en CRM (Customer Relationship Management), toch is de invoering hiervan op het gebied van IT-software voor de gezondheidszorg, en met name software voor medische beeldvorming, iets langzamer verlopen (maar deze wint steeds meer terrein). Hier zijn verschillende redenen voor:

- **Verleden:** Applicaties voor medische beeldvorming zijn van oudsher thick client-applicaties die lokale resources vereisen en specifieke eisen stellen aan het werkstation. De huidige systemen zijn gebouwd met verouderde architectuur en softwaretechnieken.

- **De technologische lat ligt hoog om elke functie in een webomgeving te implementeren:** Van de weergave van grote CT-/MR-datasets en complexe beeldvormingstools die reken-kracht vereisen (MIP/MPR) tot spraakherkenning, elke functie is nodig om de workflow van de radioloog te ondersteunen, maar is moeilijk te implementeren in een webomgeving. Om deze functies in een pure html-context te bouwen, is veel R&D nodig (vanaf nul) en zijn meer (ontwerp)keuzes nodig dan voorheen.

- **Multitenant-cloud:** Dit concept is nog lang geen standaardoplossing binnen de gezondheidszorg, omdat leveranciers hun oplossingen voornamelijk richten op de individuele zorginstelling. In andere sectoren wordt dit concept wel veel gebruikt (Salesforce, Google, enz.).

"Het concept van een web-gebaseerd cloudplatform is algemeen geaccepteerd en wordt toegepast op andere gebieden, zoals thuisbankieren, kantoor-applicaties en CRM (Customer Relationship Management)."

- **Prestaties:** Deze web- en cloudgebaseerde aanpak vereist betere en slimmere technieken om data sneller beschikbaar te maken via verbindingen met een lagere bandbreedte/hoge latentie.

De voordelen van deze technologie voor de gezondheidszorg zijn echter duidelijk. Pure web- en cloudtechnologieën zullen (zorg)organisaties in staat stellen hun huidige infrastructuur te behouden en te vereenvoudigen, de beheertaken en de totale kosten te verlagen, en een oplossing te bieden voor werken op afstand zonder nadelige gevolgen voor het beveiligingsbeleid.

6. PACSonWEB: native cloud-PACS voor beoordeling op afstand en meer

PACSonWEB is een beveiligde en puur webgebaseerde multitenant-cloudoplossing. De belangrijkste PACS-functies zijn altijd, overal en op elke computer beschikbaar vanuit de veilige cloudomgeving. De client is de browser en communiceert alleen via https. **PACSonWEB ondersteunt toepassingen met meerdere beeldschermen en biedt de functies, snelheid en het gebruiksgemak dat een radioloog verwacht van een PACS-werkstation, met behoud van het beveiliginsniveau van de gezondheidszorgorganisatie.** Beoordeling op afstand met spraakherkenning is ingebouwd en de beheertaken van de IT-afdeling worden aanzienlijk teruggebracht. **Alle gebruikers van PACSonWEB, waaronder radiologen, andere specialisten, huisartsen en patiënten, worden volledig ondersteund door een centrale helpdesk, die dient als enig contactpunt voor alle vragen over PACSonWEB.** Deze ondersteuning is beschikbaar in het Engels, Frans, Duits en Nederlands, via de telefoon, e-mail of een programma voor verbinding op afstand zoals LogMeIn of TeamViewer, met gegarandeerde snelle responstijden.

Wilt u meer weten over PACSonWEB voor beoordeling op afstand of wilt u meer informatie over PACSonWEB, ga dan naar:

www.pacsonweb.com

7. Literatuur

1. Srini Tridandapani, Greg Holl en Cheri L. Canon, 'Rapid Deployment of Home PACS Workstations to Enable Social Distancing in the Coronavirus Disease (COVID-19) Era,' American Journal of Roentgenology 2020 215:6, 1351-1353, te vinden op: https://www.ajronline.org/doi/full/10.2214/AJR.20.23495

2. Christy Pettey, 'Gartner Top 9 Security and Risk Trends for 2020,' september 17/20, te vinden op: https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/

3. Morey Haber, 'The Dangers Of Using A VPN On Home Computers For Work And What To Do Instead,' Forbes, Forbes Technology Council, July 17/20, te vinden op: https://www.forbes.com/sites/forbestechcouncil/2020/01/17/the-dangers-of-using-vpn-on-home-computers-for-work-and-what-to-do-instead/?sh=5041735d6349

4. AV-TEST Security Report 2019/2020, van het onafhankelijk onderzoeksinstituut voor IT-beveiliging in Duitsland, te vinden op: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2019-2020.pdf

5. Sophie Anderson, 'Antivirus and Cybersecurity Statistics, Trends & Facts 2021,' SafetyDetectives, January 24/20, te vinden op: https://www.safetydetectives.com/blog/antivirus-statistics/#:~:text=The%20Threats%20Against%20Regular%20Users&text=However%2C%20an%20estimated%20one%2Dfourth,PUPs%20(potentially%20unwanted%20programs).

DOBCO Medical Systems

DOBCO Medical Systems, gevestigd in België, is gespecialiseerd in oplossingen voor medische beeldvorming in de cloud. Het bedrijf werd in 2011 opgericht door Jan Dobbenie en Kristof Coucke, twee veteranen uit de healthcare-IT, en boekte in minder dan acht jaar tijd een jaaromzet van 4 miljoen euro.

Onze visie: Wij geloven dat native cloud-PACS de toekomst is
Wij geloven rotsvast in de kracht van cloud- en webtechnologie om de processen binnen medische beeldvorming te stroomlijnen en medische informatie sneller, accurater en op een veiligere manier beschikbaar te stellen aan artsen en patiënten.

Ons doel is radiologen ondersteunen, zodat zij hun dienstverlening aan patiënten, huisartsen en specialisten, en het ziekenhuismanagement kunnen verbeteren.

Wij zijn vernieuwers. Onze oplossingen voor medische beeldvorming zijn ontworpen om onze klanten te helpen hun patiëntenzorg en bedrijfsdoelstellingen te bereiken door het bieden van een betere dienstverlening.
Ons engagement: zorgen voor een uitstekende ervaring en dienstverlening voor iedereen die toegang heeft tot beelden via de PACSonWEB-oplossing, over het hele spectrum van de patiëntenzorg.

Contactgegevens

+32 (52)77 01 16
info@dobcomed.com
Nachtegaalstraat 6, 9240 Zele, België
www.pacsonweb.com