Sicherheitsbericht

Ungeschützte Patientendaten im Internet

Cyber Resilience Report

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

Copyright Greenbone Networks GmbH, 2019

2019-09-18

Inhaltsverzeichnis

1. Zusammenfassung 3
2. Arbeitsweise 4
3. Funde 6
   3.1. Schwachstellen-Analyse 11
   3.2. Webaccess 12
4. Angriffsszenarien und Wert der Daten 12
   4.1. Wert der Daten 14
5. Grenzen dieser Analyse 14
6. Behebung der Lücken 15
7. Anlagen 15
   7.1. Listendarstellungen 16

Alle genannten Produkte und Unternehmen können markenrechtlich geschützte Begriffe sein und gehören dem entsprechenden Inhaber. Deren Verwendung in diesem Text dient der Information des Lesers und bedeutet weder, dass eine Verbindung zwischen Greenbone Network und dem Unternehmen oder Produkt besteht, noch ist es als Wertung zu sehen.

1. Zusammenfassung

Im Zeitraum Mitte Juli 2019 bis Anfang September 2019 hat Greenbone Networks eine Analyse von etwa 2.300 mit dem öffentlichen Internet verbundenen medizinischen Bildarchivierungssystemen durchgeführt. Diese sogenannten PACS Server (Picture Archving and Communication Systems) werden im Gesundheitssektor genutzt, um Bilder, die durch radiologische Verfahren entstanden sind, zu archivieren und behandelnden Ärzten zur Betrachtung bereit zu stellen. Das dafür verwendete Protokoll wird DICOM genannt (Digital Imaging and Communications in Medicine).

Dass PACS Server angreifbar bzw. auslesbar sind, ist keine neue Information. Es gab in der Vergangenheit eine Reihe von Berichten zu diesem Thema. Kein Bericht jedoch geht auf die Breite und Tiefe der Problematik eines nicht abgesicherten PACS-Servers ein.

Die Analyse ergab, dass mehrere hundert Systeme weltweit ohne jegliche Art von Schutz der auf ihnen gespeicherten persönlichen und medizinischen Daten mit dem öffentlichen Internet verbunden sind. Ein nicht unerheblicher Teil dieser Systeme erlaubt sogar den Zugriff auf die einzelnen Bilddaten eines beliebigen Patienten.

Alle identifizierten System geben den Namen des Patienten, das Geburtsdatum, das Datum der Untersuchung und einige medizinische Anmerkungen zum Grund der Untersuchung preis.

In Deutschland sind ca. 15.000 Datensätze von Bundesbürgern öffentlich zugänglich, wobei diesen Datensätzen etwa 2,85 Mio. Bilder zugeordnet sind. Davon sind wiederum 1,38 Mio. abrufbar (ohne Passwort oder Authentifizierung)[1].

Weltweit sind 590 Archivsysteme identifiziert worden, die 24,5 Mio. Datensätze von Menschen preisgeben. Dabei sind mehr als 737 Mio. Bilddaten mit diesen Patientendaten verknüpft, von den etwa 400 Mio. auch einsehbar sind bzw. aus dem Internet heruntergeladen werden können. Hinzu kommen 39 Systeme die via unverschlüsseltem http-Webviewer Zugriff auf Patientendaten ermöglichen – auch dies ohne jeglichen Schutz.

Abgeleitet aus bekannten Angriffen und Recherchen einiger Sicherheitsbehörden, hätte ein solches zusammengefasstes Datenpaket im Darknet vermutlich einen Gegenwert von mehr als einer Milliarde US-Dollar.

Diese Daten könnten von Angreifern zu unterschiedlichen Zwecken ausgenutzt werden. Dazu zählen die Veröffentlichung einzelner Namen und Bilder, um dem Ansehen der Person zu schaden; die Verknüpfung der Daten mit anderen Quellen aus dem Darknet um Phishing-Angriffe und Social Engineering noch ‚erfolgreicher' zu machen; das Auslesen und automatisierte Verarbeiten der Daten zur Suche nach wertvollen Identittätsinformationen (z.B. die amerikanische Social Security Number) um einen Identitätsdiebstahl vorzubereiten.

Dieses globale Datenleck berührt Regelungen zum Datenschutz in Europa (Europäische Datenschutz-Grundverordnung; DSGVO) sowie in den USA (Health Insurance Portability and Accountability Act ; HIPAA; zum Schutz von medizinischen Daten) und einer ganzen Reihe von gesetzlichen Bestimmungen in anderen Ländern. Überprüft wurden IP-Adressen bzw. Systeme aus 93 Ländern und Territorien.

Die folgenden Kapitel beschreiben die Vorgehensweise, die Funde, mögliche Angriffszenarien und Wege der Behebung im Detail.

[1] Etwa 3 Wochen nach Meldung der betroffenen Systeme an das Bundesamt für Sicherheit in der Informationstechnik waren diese nicht mehr erreichbar.

Im Anhang befindet sich eine Liste mit Dateien. Diese enthalten die einzelnen Datensätze, die für diesen Sicherheitsbericht verwendet wurden. Diese Dateien werden nur auf Nachfrage und nur Organisationen mit berechtigtem Interesse zur Verfügung gestellt.

Es muss hevorgehoben werden, dass zur Auswertung dieses Datenlecks keinerlei Programmentwicklung, also kein Coding, nötig war. Es wurden weder Exploits geschrieben, noch unbekannte/unveröffentlichte Schwachstellen ausgenutzt. Auch wurden keine kompletten Datensätze oder vollständige Archive heruntergeladen oder gespeichert.

2.Arbeitsweise

Zur Identifikation von PACS-Servern weltweit wurden verschiedene Quellen herangezogen. Dazu gehören die bekannten Quellen Shodan.io und Censys.io. So erhielten wir eine Liste von etwa 2.300 IP Adressen und Portnummern des DICOM-Protokolls.

Das DICOM-Protokoll verwendet standardmäßig die Ports 104/TCP und 11112/TCP für die Kommunikation zwischen DICOM-fähigen Anwendungen. Das Protokoll dient dem Laden von durch bildgebende Geräte (Röntgen, CT, MRT) produzierte Bilddaten und Patienteninformationen in das Archivsystem . Weiter erlaubt es den lesenden Abruf dieser Daten, z.B. durch den behandelnden Arzt.

Das DICOM-Protokoll bzw.-Format ist in dieser Analyse von wesentlicher Bedeutung und wird im englischen Standard wie folgt beschrieben:

„DICOM (Digital Imaging and Communications in Medicine) is a standard for handling, storing, printing, and transmitting information in medical imaging. It includes a file format definition and a network communications protocol. The communication protocol is an application protocol that uses TCP/IP to communicate between systems. DICOM files can be exchanged between two entities that are capable of receiving image and patient data in DICOM format."

Für diesen Sicherheitsbericht war nur der Anwendungsfall ‚lesender Zugriff' von Interesse, eine mögliche Manipulation von Bilddaten und der anschließende Upload wurde nicht untersucht.

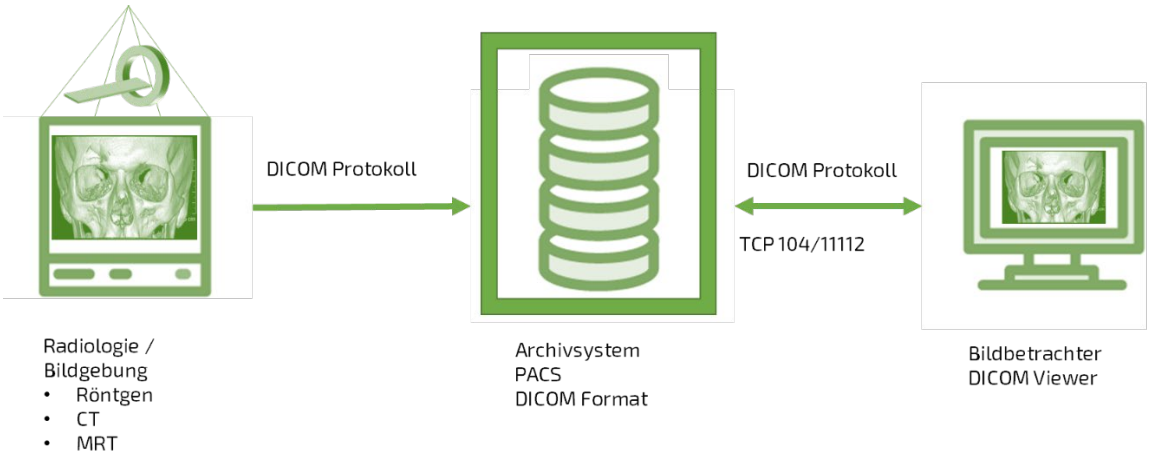


Bild 1: Skizzierter Ablauf im DICOM Protokoll / Format

Im Sinne der C-I-A Triade (Confidentiality-Integrity-Availability) beschäftigt sich dieser Bericht nur mit der Vertraulichkeit (Confidentiality) der Daten. Unsere Analyse zeigt, dass diese für oben genannte Daten definitiv nicht gewährleistet ist.

Um zu verdeutlichen, wie einfach ein Auslesen dieser medizinischen Daten ist, wurde der Radiant DICOM Viewer verwendet. Andere Tools sind zum Nachvollziehen der Arbeitsweise nicht nötig. Der

Radiant DICOM Viewer ist ausreichend im Internet dokumentiert[2]. Die Konfiguration der Anwendung kann somit jeder internet-affinen Anfänger durchführen.

Zur Konfiguration des Viewers werden die Server-Parameter IP und Port benötigt – auch diese lassen sich öffentlich ermitteln (siehe Shodan / Censys) – sowie zwei weitere Angaben, deren Inhalt komplett willkürlich gewählt werden kann (ae-title und description).

Nach erfolgter Konfiguration kann mithilfe des Viewers überprüft werden, ob das PACS Daten sendet oder weitere Schutzmaßnahmen getroffen wurden. 1.700 der überprüften System zeigten sich geschützt.

Sollten keine weiteren Schutzmaßnahmen vorhanden sein, sendet das PACS die Patientendaten an den Viewer. Darüber hinaus erlaubt der Viewer auch das Betrachten der Bilder, wobei hier eine Einschränkung bestehen kann (möglicherweise eine Frage der Bildkompression, nicht Gegenstand der Analyse).

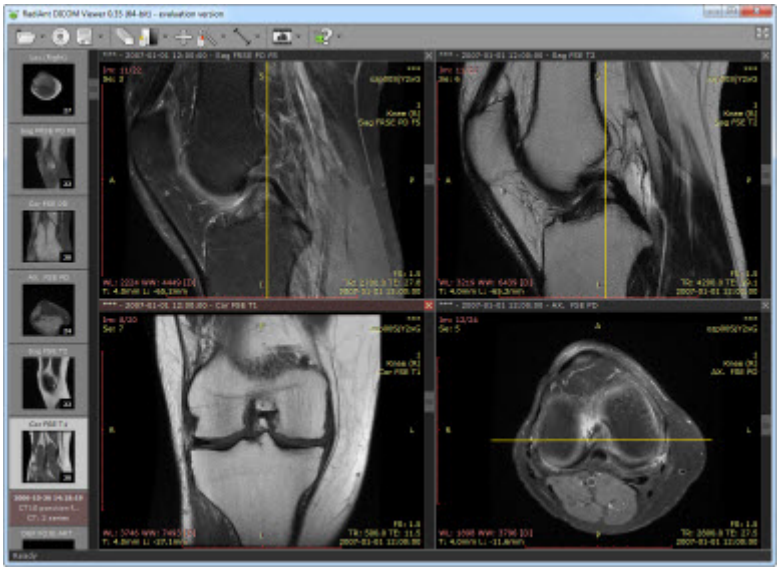


Bild 2: Radiant DICOM Viewer Inhalte,
Quelle: https://commons.wikimedia.org/wiki/File:RadiAnt_DICOM_Viewer.jpg

Sowie der Viewer die Daten erhält werden die einzelnen Patientendaten in einer Tabellendarstellung angezeigt und dabei gezählt. Dies wurde für die Analyse benutzt, um die Zahl der betroffenen Patientendatensätze zu ermitteln.

Zu jedem einzelnen Datensatz finden sich fast immer auch Angaben zur Anzahl der mit dem Datensatz verknüpften medizinischen Bilder. Diese Listung über alle Datensätze wurde gemittelt und mit der Anzahl der Datensätze multipliziert, um eine Schätzung über die Anzahl an Bildern im Archivsystem zu erhalten.

Aus den ersten Elementen der Liste wurde zufällig ein Eintrag ausgewählt, um den eigentlichen Zugriff auf die Bilddaten zu verifizieren. Sobald ein stabiler Datenstrom im Viewer darauf hindeutete, dass Bildinformationen übertragen werden, wurde dies abgebrochen. In einem Teil der Fälle erfolgte die Bildübermittlung jedoch so schnell, dass auch Patientenbilder angezeigt wurden.

2 https://www.radiantviewer.com/dicom-viewer-manual/

Die folgenden Datenpunkte wurden für die Analyse erfasst:

- Anzahl der Patientenakten (im DICOM Viewer „Studies“ genannt),
- Gesamtanzahl der Bilder auf dem PACS Server,
- Aktualität der Daten (z.B. Patientendaten aus AUG/SEP 2019)
- Zugriff auf Bilder erlaubt
- human- oder veterinärmedizinisches Archiv

Zusätzlicher Scan auf Schwachstellen

Im weiteren Verlauf der Analyse wurden die IP-Adressen mit einem Schwachstellen-Scan überprüft und dies als weiteren Datenpunkt hinzugefügt. Gesucht wurde nach „high severity vulnerabilities“.

Die Auswertung des Schwachstellen-Scans ergab einige Hinweise auf bereits erfolgte Kompromittierung von Systemen. Diese Information wurde auch als Datenpunkt hinzugefügt.

In Ergänzung zur eigentlichen Analyse wurden Seitenfunde geprüft, so z.B. Hinweise auf frei herunterladbare DICOM Archive oder WebApps, die unkontrollierten Zugang zu Patientendaten erlauben.

Details dazu finden sich im Kapitel 3 „Funde“.

3.Funde

Die Analyse der Systeme ergab folgende Summen und Detailfunde:

In Summe sind weltweit etwa 24,3 Millionen Datensätze abrufbar, dabei werden in der überwiegenden Mehrheit folgenden personenbezogene Daten gelistet:

- Vor- und Nachname
- Geburtsdatum
- Datum der Untersuchung
- Umfang der Untersuchung
- Art des bildgebenden Verfahrens
- Behandelnder Arzt
- Institut (Klinik)
- Anzahl der erzeugten Bilder

In Deutschland sind diese Informationen durch die DSGVO geschützt. In den USA schützt HIPAA, der Health Insurance Portability and Accountability Act, diese Informationen. Auch in anderen Ländern gibt es entsprechende Regelungen, so z.B. in

- Republik Südafrika: Protection of Personal Information Act (POPI Act)
- Brasilien: Lei Geral de Proteção de Dados Pessoais (LGPD)
- Indien: Information Technology Act 2000, Data Privacy Rules
- Türkei: Personal Data Protection Law no. 6698

Aus den o.g. einzelnen Datenpunkten ergeben sich zwei weitere Summen. Die Anzahl der mit den 24,3 Millionen Datensätzen verknüpften Bilder beläuft sich auf geschätzte 733,5 Millionen, wobei auf geschätzte 399,5 Millionen Bilder (aus den über 700 Mio.) Zugriff, Anzeige und Download möglich ist.

Die Summe dieser Datenlecks an ungeschützt im Internet zu findenden Patientendaten sind damit eine der bisher größten Datenpannen weltweit. 52 Staaten und Territorien der Welt sind betroffen, darunter alle führenden Wirtschaftsnationen sowie die bevölkerungsreichsten Länder der Welt.

Zu den betroffenen Ländern gehören:

Argentinien, Australien, Brasilien, Kanada, China, Ägypten, Frankreich, Deutschland, Indien, Iran, Italien, Japan, Korea, Mexiko, Niederlande, Russland, Südafrika, Spanien, Schweiz, Türkei, Grossbritannien, und die Vereinigten Staaten von Amerika.

Für ausgewählte Länder in Europa ergeben sich folgende Zahlen.

Bild 3: Zahlen in Europa

Die Anzahl der betroffen Systeme ergibt sich aus der unstenstehenden Tabelle.

Land	CH	CZ	DE	ES	FR	IT	NL	UK
Systeme	2	2	6	1	7	10	4	5

Für Nordamerika sind die Daten wie folgt:

Bild 4: Zahlen in Nordamerika

Die Anzahl der betroffen Systeme ergibt sich aus der unstenstehenden Tabelle.

Land	CA	MX	US
Systeme	5	10	187

Die Zahlen für Südamerika sehen so aus:

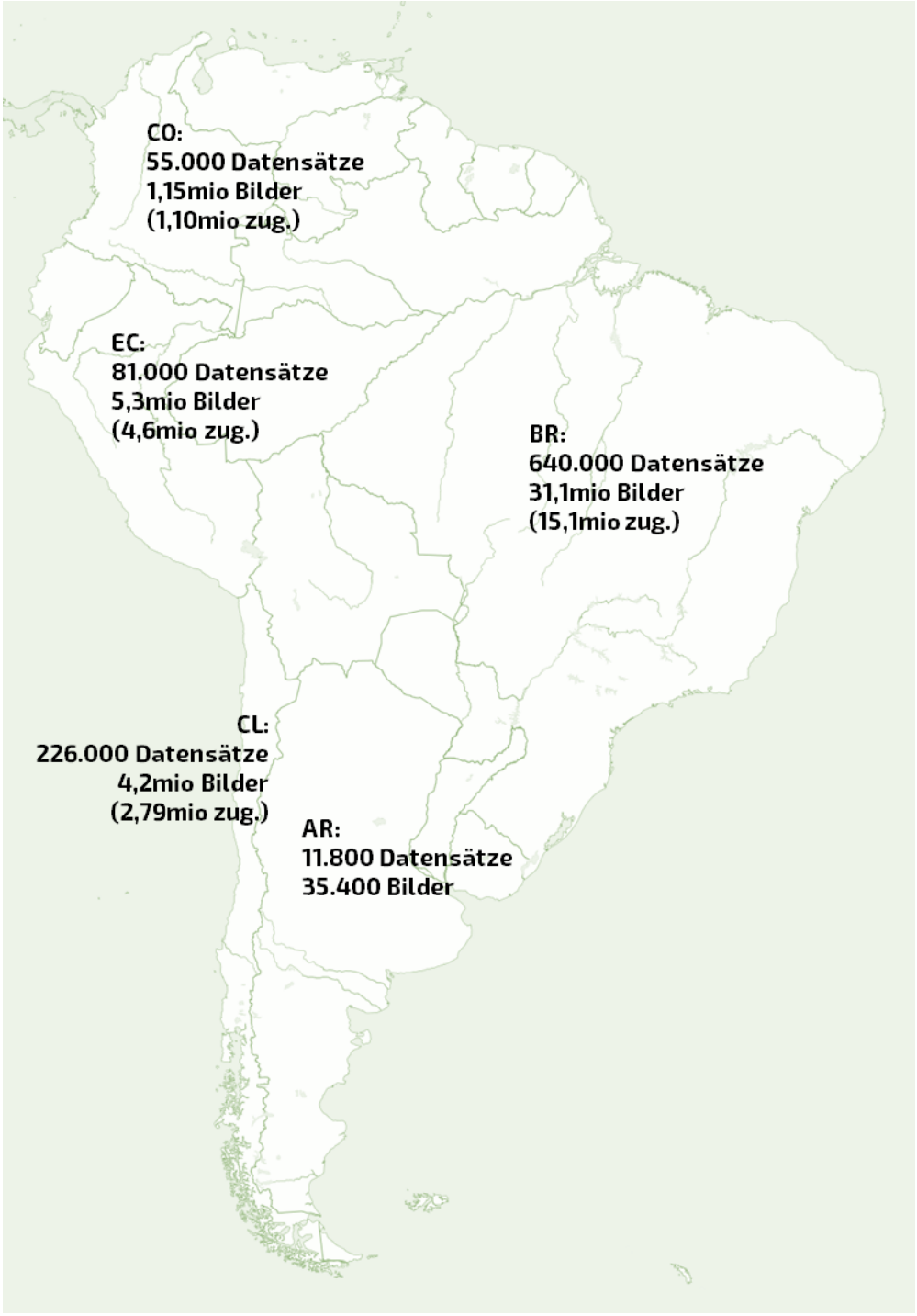


Bild 5: Zahlen in Südamerika

Die Anzahl der betroffen Systeme ergibt sich aus der unstenstehenden Tabelle.

Land	AR	BR	CL	CO	EC
Systeme	10	34	18	8	19

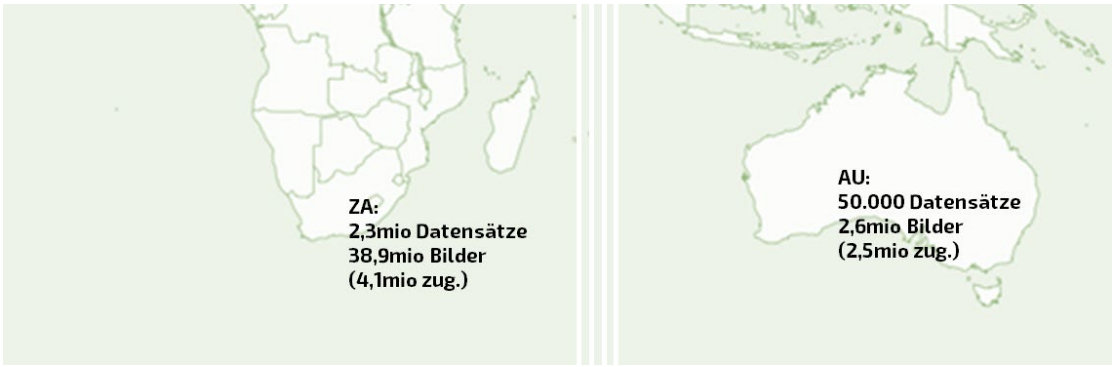
Fur Asien ergibt sich folgende Karte:

Bild 6: Zahlen in Asien

Die Anzahl der betroffen Systeme ergibt sich aus der unstenstehenden Tabelle.

Land	CN	IN	JP	RU	TR
Systeme	14	96	3	5	36

Südafrika und Australien:

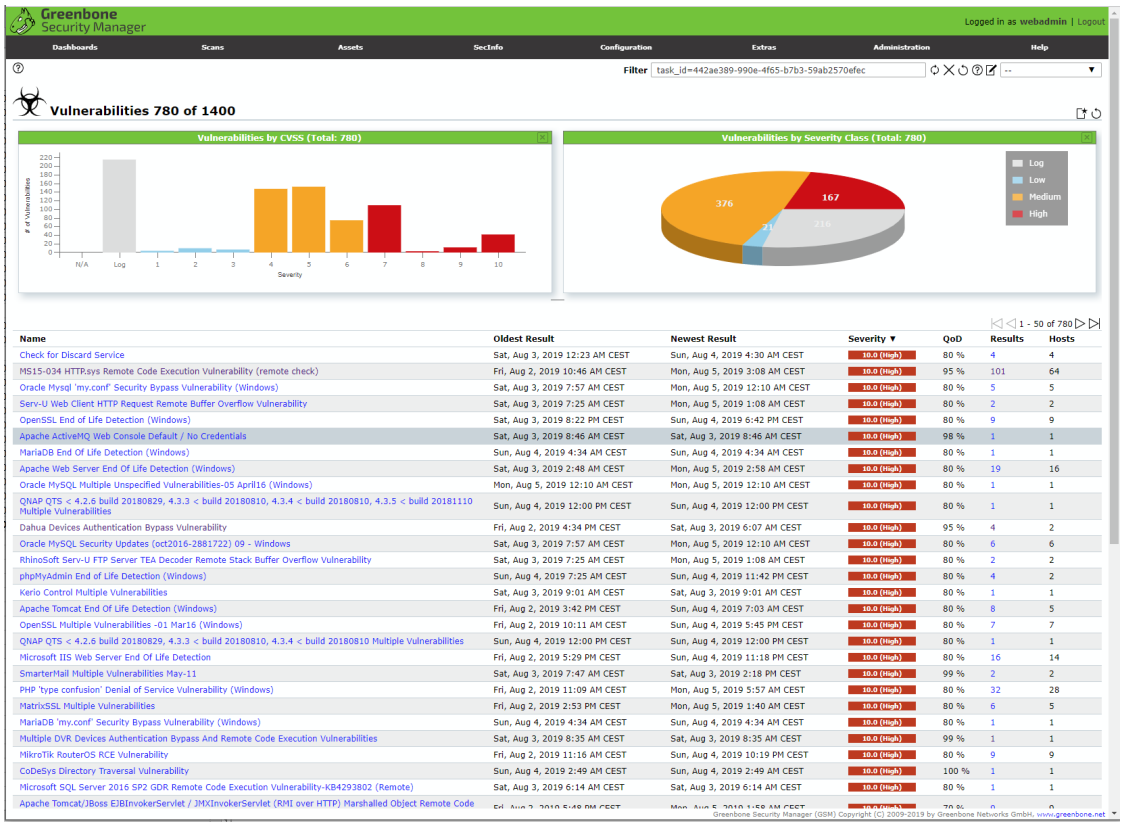


In Südafrika fanden wir 30 Archivsysteme und in Australien weitere 6 Systeme, die betroffen sind.

3.1. *Schwachstellen-Analyse*

Darüber hinaus wurden eine ganze Reihe von Schwachstellen, die zum Teil bereits mehrere Jahre alt sind, auf den geprüften Systemen identifiziert.

Der Screenshot zeigt einige Infos dazu:



In Summe haben wir mehr als 10.000 Schwachstellen auf den Systemen identifiziert. Etwas über 2.000 davon sind als „High Severity“ katalogisiert. In dieser Kategorie haben mehr als 500 Schwachstellen dem höchsten Schweregrad im Common Vulnerability Scoring System (CVSS 10,0).

In diesen CVSS10-Schwachstellen finden sich verwundbare Webanwendungen und Datenbanken am häufigsten, die auch die gängigen Angriffsziele für Hacker sind.

Weitere Details der Schwachstellen-Analyse können zur Verfügung gestellt werden (der Report ist 300MB groß).

Aus der weiteren Analyse ergab sich, dass einzelne Systeme sogenannte Indicators of Compromise, also Daten, die auf ein möglicherweise kompromittiertes System hinweisen, aufweisen. Auch diesen Aspekt haben wir nicht weiter untersucht.

3.2. *Webaccess*

Neben den Archivsystemen, die ohne Schutz über das DICOM-Protokoll angesprochen und abgefragt werden können, hat unsere Analyse auch einige weitere, teilweise ungewöhnliche, Funde erbracht. Bei diesen wäre es noch einfacher auf gespeicherte medzinische Daten auf dem jeweiligen System zuzugreifen.

- Wir haben 31 Systeme gefunden, die über einen DICOM-Webviewer direkten Zugriff auf Patientendaten zulassen. Dieser Zugriff war ohne Authentifizierung möglich. De Übertragung der Daten erfolgte bei den meisten dieser 31 Systeme via http, also unverschlüsselt in Klartext. Die Webviewer bieten einen Datei-Upload an, den wir nicht weiter untersucht haben. Ob hier Sicherheitsmechanismen installiert sind, bleibt somit fraglich und sollte weiter untersucht werden.
- Sieben Systeme bieten vollständige DICOM-Archive als Download via http (unverschlüsselt) an, in Summe etwa 108 Gigabytes an Daten. Die Archive selbst wurden nicht heruntergeladen bzw. untersucht.
- Sechs Server-Systeme bieten einen unverschlüsselten FTP-Dienste mit sog. anonymen Zugang an, also ohne Passwort oder sonstigen Schutz. Auf mindestens einem System sind Patientendaten direkt auffindbar.
- Ein System ist in einer Weise konfiguriert, die wir schon lange nicht mehr beobachtet haben. Dieses System zeigt via Directory Listing im Webbrowser die Dateien des DICOM-Archivs an. Die jeweiligen Bilder sind ohne weiteres herunterladbar.

4. Angriffsszenarien und Wert der Daten

Die mögliche Angriffszenarien, die sich durch diese Funde ergebne, sind vielfältig. Da es sich um personenbezogene Daten handelt, sind alle Arten von Angriffen denkbar, die diese Daten ausnutzen:

- Social Engineering
- Spear Fishing / Whaling
- Business E-Mail Compromise

Darüber hinaus ist die Verschneidung dieser Daten mit anderen Quellen (bereits geleakten Datensätze) eine weitere Verwendungsoption, um noch gezieltere Angriffe vorzubereiten. Erpressungsversuche sind denkbar, Identitätsdiebstahl ebenfalls (die US-Daten enthalten in Teilen auch die Social Security Number).

Das amerikanische Gesundheitsministerium HHS hat eine Reihe von Szenarien gelistet, die auf geleakte Patientendaten aufbauen:

„Medizinischer Identitätsdiebstahl“:

Das Verwenden von medizinischen Daten einer anderen Person, um eine medizinsche Dienstleistung zu erhalten, dazu zählen

- Rezepte bzw. ärztliche Verschreibungen
- Operationen oder andere medizinische Behandlungen
- Gefälschte Abrechnungen gegenüber Krankenversicherungen

“Weaponizing” von medizinischen Daten:

Das Benutzen von sensiblen medizinischen Daten um einzelne Personen zu bedrohen, zu erpressen oder zu beeinflussen, um so:

- Erpressungsgeld zu fordern
- durch falsche oder echte zusätzliche Daten jemanden herabzuwürdigen
- insbesondere Personen der öffentlichen Lebens sind gefährdet

Bemerkung: Wir haben in unserer Forschungsarbeit nicht nach Namen von prominenten Persönlichkeiten gesucht.

Geldbetrug:

Ausnutzung der in den elektronischen Krankenakten enthaltenen persönlichen Daten (Personally Identifiable Information – PII) für die Erstelllung von Kreditkarten- oder Bank-Profilen, um so einen Finanzbetrug zu ermöglichen.

- Medizin-Dienstleister speichern oft Finanzinformationen zu Patientendaten.
  (Wir haben Hinweise zu Abrechnungsinformationen in den Daten gesehen)
- Kredite bzw. Kreditlinien sind nicht selten an gesundheitliche Daten gekoppelt, die man in Patientenakten findet.
- Steuerbetrug durch Abgabe falscher Abrechnungen

Cyber-Kampagnen:

Medizinische Daten werden als ergänzende Daten in anderen, zukünftigen ‚Hacking Kampagnen‘ verwendet.

- Kontaktinformationen können für Phishing oder Scams (CEO Fraud, s.o.) benutzt werden.
- Credential/Authentication Informationen können für eine „privilege escalation“ genutzt werden.
  (Wir haben nicht nach solchen Informationen in den Daten gesucht.)

Innerhalb der Masse an Daten und persönlichen Informationen sind eine Reihe von Gruppen besonders anfällig, da deren Ausnutzung auf Jahre hinweg unauffällig bleiben kann.

- Kinder und Jugendliche, deren Daten für Identitätsdiebstahl genutzt wird. Diese sind in den gefundenen Daten leicht über das Geburtsdatum zu identifizieren.
- Alte Menschen, verbunden mit der Annahme, dass diese ein leichteres Ziel sind („age-associated financial vulnerability“). Diese Gruppe lässt sich z.B. über den Namen des Instituts identifizieren, der in den gefundenen Daten vorhanden ist (etwa „Senior Care“.)
- Verstorbene Personen, bzw. vermutlich verstorbene Personen. Anhand des Geburtstdatums werden Daten gefiltert von Personen im hohen Alter. Hier ist die zu erwartende Entdeckungsrate sehr gering.

4.1. *Wert der Daten*

Im Verlauf der Analyse stellte sich die Frage, wieviel diese Daten im Darkweb wert sein könnten. Eine genaue Aussage ist schwer zu treffen, es gibt aber einige Anhaltspunkte für eine Näherung.

Im April 2019 hat das Department of Health and Human Services (HHS) der USA ein Intelligence Briefing Update veröffentlicht[3]. Darin wurde der durchschnittliche Wert eines ‚Electronic Health Record' (EHR) mit 250 US-Dollar angeben, der Maximalwert mit etwa 1.000 US-Dollar.

Ein Abgleich mit den 18 Merkmalen, die im HIPAA (s.o.) für einen umfangreichen EHR genannt werden, ergab, dass die gefundenen Daten sieben dieser Merkmale sicher enthalten. Für weitere sieben Merkmale existieren starke Hinweise, dass sie enthalten sind und vier sind unklar bzw. sehr wahrscheinlich nicht enthalten (siehe Anhang).

Auf dieser Basis ist ein Näherungswert von 50 US-Dollar pro Datensatz anzusetzen, was zu einem Gesamtwert der ungeschützt abrufbaren Daten auf etwa 1,2 Milliarden US-Dollar führt.

Dieser Wert ist sicher nicht auf einmal erzielbar und nicht jeder Datensatz wird für 50 US-Dollar gehandelt werden können. Allerdings zeigt diese Summe auf, mit welcher Motivation ein Angreifer nach diesen Daten suchen könnte und dabei sehr wahrscheinlich auch einen höheren technischem Aufwand investieren würde.

5. Grenzen dieser Analyse

Im Rahmen dieser Untersuchung haben wir drei Bereiche identifiziert, die fortan eingehend geprüft werden sollten:

1. Umfeldanalyse:
   Die gefundenen, offenen PACS-Server sind Teil eines medizinischen/klinischen Prozesses. D.h. sie kommunizieren innerhalb eines Netzwerkes mit IP-fähigen Geräten über das DICOM-Protokoll. Ein Netzwerk-Scan im Addressbreich des jeweiligen Systems könnte weitere „lohnende Ziele" für einen Angreifer aufdecken.
   Dabei kann ein Angreifer davon ausgehen, dass auch auf diesen System die Absicherung nicht den gängigen Standards entspricht – analog zum bereits gefundenen PACS-Server.
2. DICOM Brute Force
   Unsere Analyse zeigt, dass eine Reihe von Systemen zwar auf einen „DICOM Ping" (CSP-ECHO) antworten, aber nicht auf die Abfrage von Daten. Hier sind wahrscheinlich entsprechende Einstellungen in den AE-Titles bzw. Descriptions gemacht worden, die eine offene Abfrage verhindern. Ein Review des DICOM-Protokolls zeigt, dass es im Protokoll keine Einschränkungen bei der Anzahl der Versuche gibt, ein System abzufragen. Hier wäre eine Brute-Force Attacke eines Angreifers denkbar, damit weitere Systeme Daten preisgeben. Ein solches Scripting war nicht Teil der Analyse.
3. Upload von Dateien
   Das DICOM-Protokoll beinhaltet Methoden, um Dateien auf einen PACS-Server zu laden (siehe Webaccess weiter oben). Es war nicht Teil der vorliegenden Analyse, ob diese Möglichkeit für einen Angriff auf das System ausgenutzt werden kann (wobei wir eine entsprechende Vermutung haben). Über diesen Weg ist es potenziell möglich, Schadsoftware in den inneren, sensiblen Netzwerkbereich von medizinischen Einrichtungen zu bringen.
4. Manipulation von Bildern
   Dieses Angriffszenario wurde bereits von israelischen Sicherheitsforschern untersucht[4].

[3] https://content.govdelivery.com/attachments/USDHSFACIR/2019/04/25/file_attachments/1199378/Dark%20Web%20primer.pdf
[4] https://arxiv.org/pdf/1901.03597.pdf

6.Behebung der Lücken

Da es sich um eine fehlerhafte Konfiguration der Infrastruktur und des PACS Servers handelt und nicht um eine Software-Schwachstelle, sind auch dort die Möglichkeiten der Behebung bzw. Beseitigung gegeben. Diese sind u.a.:

- Access Control Lists (ACLs) für IP-Adressen bzw. Portfilter
- Zugangskontrolle durch vorgeschaltete AAA-Systeme
- VPN-Zugang für Berechtigte
- Detail-Konfiguration des AE-Titles

Diese möglichen Maßnahmen sind geeignet, den freien Zugang zu den gefundenen Systemen zu erschweren bzw. zu unterbinden. Dabei ist sicherlich zu beachten, welche berechtigten Stellen auf die Daten Zugriff haben müssen (Klinikverbünde oder niedergelassene Ärzte).

Der jeweilige Einzelfall wird die zur Verfügung stehenden Möglichkeiten einschränken. Allerdings gibt es nach unseren Beobachtungen keinen Fall, in dem ein höheres Maß an Absicherung unmöglich ist.

Eine umfassende und widerholt durchgeführte Bestandsaufnahme der IT-Systeme und deren Schwachstellen innerhalb einer Organisation ist der beste Weg, um solche fehlerhaften Konfigurationen aufzudecken.

7.Anlagen

Die folgenden Dokumente zu den Details werden nur auf Nachfrage und nur an Organisationen mit berechtigtem Interesse zur Verfügung gestellt. Dazu zählen insbesondere die Datenschutzbehörden der betroffenen Länder, die sich an security@greenbone.net wenden können.

- Datei „DICOM details per system”
- Datei „PACS Server free web access”

7.1. *Listendarstellungen*

Ergebnisse nach Ländern sortiert (alphabetisch, aufsteigend A-Z)

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
Albania	1	200	1.000	-	-
Anguilla	1	2.972	44.850	-	-
Argentina	10	11.824	25.472	-	-
Australia	6	49.922	2.596.469	2.496.260	-
Barbados	1	14	2.800	-	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Brazil	34	643.892	31.110.131	15.141.864	4
Bulgaria	2	27.058	40.977	40.977	-
Canada	5	117.425	6.019.030	980.500	-
Chile	18	226.886	4.218.279	2.794.898	3
China	14	279.928	4.882.722	376.905	-
Colombia	8	55.345	1.155.195	1.114.602	1
Costa Rica	1	3.202	12.808	12.808	1
Cyprus	1	3.459	1.124.175	1.124.175	-
Czech Republic	2	97.997	674.686	-	-
Ecuador	19	81.363	5.308.881	4.621.285	2
Egypt	2	827	124.130	124.130	-
France	7	47.662	5.275.222	2.668.170	-
Germany	6	15.310	2.859.595	1.394.845	-
Greece	2	10.211	2.557.600	2.557.600	-
Guatemala	4	13.012	1.039.241	1.039.241	2
India	96	627.777	105.941.300	104.120.549	6
Iran	2	118.692	1.903.384	1.903.384	-
Italy	10	102.893	5.843.319	1.174.600	-
Japan	3	10.498	1.725.280	1.719.280	-
Kenya	1	243	14.580	-	-
Korea	2	26.256	86.277	-	1
Malaysia	3	19.922	1.195.320	1.195.320	-
Mexico	10	23.590	965.495	195.475	2
Netherlands	3	11.270	113.408	113.408	-
Netherlands Antilles	1	13.992	209.880	209.880	-
Paraguay	1	22.355	1.676.625	-	-
Peru	2	1.377	177.050	500	1
Portugal	3	5.766	1.581.101	1.581.100	-
Puerto Rico	23	205.691	4.921.604	4.921.604	-
Romania	1	67	737	-	-
Russian Federation	5	9.858	887.042	25.000	-
Sao Tome and Principe	1	13.402	160.824	-	-
Serbia	1	30.484	15.242.000	15.242.000	-
Slovakia	1	127.636	382.908	-	-
South Africa	30	2.338.112	38.941.118	4.093.500	-
Spain	1	17.662	52.986	-	-
Switzerland	2	1.541	231.840	231.840	1
Thailand	8	433.008	433.895	426.773	-
Turkey	36	4.924.141	179.533.940	178.283.858	-
Ukraine	1	1.139	199.325	199.325	-
United Kingdom	6	1.571	13.335	5.070	-
United States	187	13.700.499	303.126.601	45.870.508	15
Uzbekistan	1	35.475	886.875	886.875	-
Vanuatu	1	1.512	1.512	1.512	-
Venezuela	1	76	1.140	1.140	-
Vietnam	1	1.471	1.471	-	-

Ergebnisse nach Systemen sortiert (Anzahl, absteigend)

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
United States	187	13.700.499	303.126.601	45.870.508	15
India	96	627.777	105.941.300	104.120.549	6
Turkey	36	4.924.141	179.533.940	178.283.858	-
Brazil	34	643.892	31.110.131	15.141.864	4
South Africa	30	2.338.112	38.941.118	4.093.500	-
Puerto Rico	23	205.691	4.921.604	4.921.604	-
Ecuador	19	81.363	5.308.881	4.621.285	2
Chile	18	226.886	4.218.279	2.794.898	3
China	14	279.928	4.882.722	376.905	-
Argentina	10	11.824	25.472	-	-
Italy	10	102.893	5.843.319	1.174.600	-
Mexico	10	23.590	965.495	195.475	2
Colombia	8	55.345	1.155.195	1.114.602	1
Thailand	8	433.008	433.895	426.773	-
France	7	47.662	5.275.222	2.668.170	-
Australia	6	49.922	2.596.469	2.496.260	-
Germany	6	15.310	2.859.595	1.394.845	-
United Kingdom	6	1.571	13.335	5.070	-
Canada	5	117.425	6.019.030	980.500	-
Russian Federation	5	9.858	887.042	25.000	-
Guatemala	4	13.012	1.039.241	1.039.241	2
Japan	3	10.498	1.725.280	1.719.280	-
Malaysia	3	19.922	1.195.320	1.195.320	-
Netherlands	3	11.270	113.408	113.408	-
Portugal	3	5.766	1.581.101	1.581.100	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Bulgaria	2	27.058	40.977	40.977	-
Czech Republic	2	97.997	674.686	-	-
Egypt	2	827	124.130	124.130	-
Greece	2	10.211	2.557.600	2.557.600	-
Iran	2	118.692	1.903.384	1.903.384	-
Korea	2	26.256	86.277	-	1
Peru	2	1.377	177.050	500	1
Switzerland	2	1.541	231.840	231.840	1
Albania	1	200	1.000	-	-
Anguilla	1	2.972	44.850	-	-
Barbados	1	14	2.800	-	-
Costa Rica	1	3.202	12.808	12.808	1
Cyprus	1	3.459	1.124.175	1.124.175	-
Kenya	1	243	14.580	-	-
Netherlands Antilles	1	13.992	209.880	209.880	-
Paraguay	1	22.355	1.676.625	-	-
Romania	1	67	737	-	-
Sao Tome and Principe	1	13.402	160.824	-	-
Serbia	1	30.484	15.242.000	15.242.000	-
Slovakia	1	127.636	382.908	-	-
Spain	1	17.662	52.986	-	-
Ukraine	1	1.139	199.325	199.325	-
Uzbekistan	1	35.475	886.875	886.875	-
Vanuatu	1	1.512	1.512	1.512	-
Venezuela	1	76	1.140	1.140	-
Vietnam	1	1.471	1.471	-	-

Ergebnisse nach Datensätzen sortiert (Anzahl, absteigend)

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
United States	187	13.700.499	303.126.601	45.870.508	15
Turkey	36	4.924.141	179.533.940	178.283.858	-
South Africa	30	2.338.112	38.941.118	4.093.500	-
Brazil	34	643.892	31.110.131	15.141.864	4
India	96	627.777	105.941.300	104.120.549	6
Thailand	8	433.008	433.895	426.773	-
China	14	279.928	4.882.722	376.905	-
Chile	18	226.886	4.218.279	2.794.898	3
Puerto Rico	23	205.691	4.921.604	4.921.604	-
Slovakia	1	127.636	382.908	-	-
Iran	2	118.692	1.903.384	1.903.384	-
Canada	5	117.425	6.019.030	980.500	-
Italy	10	102.893	5.843.319	1.174.600	-
Czech Republic	2	97.997	674.686	-	-
Ecuador	19	81.363	5.308.881	4.621.285	2
Colombia	8	55.345	1.155.195	1.114.602	1
Australia	6	49.922	2.596.469	2.496.260	-
France	7	47.662	5.275.222	2.668.170	-
Uzbekistan	1	35.475	886.875	886.875	-
Serbia	1	30.484	15.242.000	15.242.000	-
Bulgaria	2	27.058	40.977	40.977	-
Korea	2	26.256	86.277	-	1
Mexico	10	23.590	965.495	195.475	2
Paraguay	1	22.355	1.676.625	-	-
Malaysia	3	19.922	1.195.320	1.195.320	-
Spain	1	17.662	52.986	-	-
Germany	6	15.310	2.859.595	1.394.845	-
Netherlands Antilles	1	13.992	209.880	209.880	-
Sao Tome and Principe	1	13.402	160.824	-	-
Guatemala	4	13.012	1.039.241	1.039.241	2
Argentina	10	11.824	25.472	-	-
Netherlands	3	11.270	113.408	113.408	-
Japan	3	10.498	1.725.280	1.719.280	-
Greece	2	10.211	2.557.600	2.557.600	-
Russian Federation	5	9.858	887.042	25.000	-
Portugal	3	5.766	1.581.101	1.581.100	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Cyprus	1	3.459	1.124.175	1.124.175	-
Costa Rica	1	3.202	12.808	12.808	1
Anguilla	1	2.972	44.850	-	-
United Kingdom	6	1.571	13.335	5.070	-
Switzerland	2	1.541	231.840	231.840	1
Vanuatu	1	1.512	1.512	1.512	-
Vietnam	1	1.471	1.471	-	-
Peru	2	1.377	177.050	500	1
Ukraine	1	1.139	199.325	199.325	-
Egypt	2	827	124.130	124.130	-
Kenya	1	243	14.580	-	-
Albania	1	200	1.000	-	-
Venezuela	1	76	1.140	1.140	-
Romania	1	67	737	-	-
Barbados	1	14	2.800	-	-

Ergebnisse nach verlinkten Bildern sortiert (Anzahl, absteigend)

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
United States	187	13.700.499	303.126.601	45.870.508	15
Turkey	36	4.924.141	179.533.940	178.283.858	-
India	96	627.777	105.941.300	104.120.549	6
South Africa	30	2.338.112	38.941.118	4.093.500	-
Brazil	34	643.892	31.110.131	15.141.864	4
Serbia	1	30.484	15.242.000	15.242.000	-
Canada	5	117.425	6.019.030	980.500	-
Italy	10	102.893	5.843.319	1.174.600	-
Ecuador	19	81.363	5.308.881	4.621.285	2
France	7	47.662	5.275.222	2.668.170	-
Puerto Rico	23	205.691	4.921.604	4.921.604	-
China	14	279.928	4.882.722	376.905	-
Chile	18	226.886	4.218.279	2.794.898	3
Germany	6	15.310	2.859.595	1.394.845	-
Australia	6	49.922	2.596.469	2.496.260	-
Greece	2	10.211	2.557.600	2.557.600	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Iran	2	118.692	1.903.384	1.903.384	-
Japan	3	10.498	1.725.280	1.719.280	-
Paraguay	1	22.355	1.676.625	-	-
Portugal	3	5.766	1.581.101	1.581.100	-
Malaysia	3	19.922	1.195.320	1.195.320	-
Colombia	8	55.345	1.155.195	1.114.602	1
Cyprus	1	3.459	1.124.175	1.124.175	-
Guatemala	4	13.012	1.039.241	1.039.241	2
Mexico	10	23.590	965.495	195.475	2
Russian Federation	5	9.858	887.042	25.000	-
Uzbekistan	1	35.475	886.875	886.875	-
Czech Republic	2	97.997	674.686	-	-
Thailand	8	433.008	433.895	426.773	-
Slovakia	1	127.636	382.908	-	-
Switzerland	2	1.541	231.840	231.840	1
Netherlands Antilles	1	13.992	209.880	209.880	-
Ukraine	1	1.139	199.325	199.325	-
Peru	2	1.377	177.050	500	1
Sao Tome and Principe	1	13.402	160.824	-	-
Egypt	2	827	124.130	124.130	-
Netherlands	3	11.270	113.408	113.408	-
Korea	2	26.256	86.277	-	1
Spain	1	17.662	52.986	-	-
Anguilla	1	2.972	44.850	-	-
Bulgaria	2	27.058	40.977	40.977	-
Argentina	10	11.824	25.472	-	-
Kenya	1	243	14.580	-	-
United Kingdom	6	1.571	13.335	5.070	-
Costa Rica	1	3.202	12.808	12.808	1
Barbados	1	14	2.800	-	-
Vanuatu	1	1.512	1.512	1.512	-
Vietnam	1	1.471	1.471	-	-
Venezuela	1	76	1.140	1.140	-
Albania	1	200	1.000	-	-
Romania	1	67	737	-	-

Ergebnisse nach abrufbaren Bildern sortiert (Anzahl, absteigend)

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
Turkey	36	4.924.141	179.533.940	178.283.858	-
India	96	627.777	105.941.300	104.120.549	6
United States	187	13.700.499	303.126.601	45.870.508	15
Serbia	1	30.484	15.242.000	15.242.000	-
Brazil	34	643.892	31.110.131	15.141.864	4
Puerto Rico	23	205.691	4.921.604	4.921.604	-
Ecuador	19	81.363	5.308.881	4.621.285	2
South Africa	30	2.338.112	38.941.118	4.093.500	-
Chile	18	226.886	4.218.279	2.794.898	3
France	7	47.662	5.275.222	2.668.170	-
Greece	2	10.211	2.557.600	2.557.600	-
Australia	6	49.922	2.596.469	2.496.260	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Iran	2	118.692	1.903.384	1.903.384	-
Japan	3	10.498	1.725.280	1.719.280	-
Portugal	3	5.766	1.581.101	1.581.100	-
Germany	6	15.310	2.859.595	1.394.845	-
Malaysia	3	19.922	1.195.320	1.195.320	-
Italy	10	102.893	5.843.319	1.174.600	-
Cyprus	1	3.459	1.124.175	1.124.175	-
Colombia	8	55.345	1.155.195	1.114.602	1
Guatemala	4	13.012	1.039.241	1.039.241	2
Canada	5	117.425	6.019.030	980.500	-
Uzbekistan	1	35.475	886.875	886.875	-
Thailand	8	433.008	433.895	426.773	-
China	14	279.928	4.882.722	376.905	-
Switzerland	2	1.541	231.840	231.840	1
Netherlands Antilles	1	13.992	209.880	209.880	-
Ukraine	1	1.139	199.325	199.325	-
Mexico	10	23.590	965.495	195.475	2
Egypt	2	827	124.130	124.130	-
Netherlands	3	11.270	113.408	113.408	-
Bulgaria	2	27.058	40.977	40.977	-
Russian Federation	5	9.858	887.042	25.000	-
Costa Rica	1	3.202	12.808	12.808	1
United Kingdom	6	1.571	13.335	5.070	-
Vanuatu	1	1.512	1.512	1.512	-
Venezuela	1	76	1.140	1.140	-
Peru	2	1.377	177.050	500	1
Paraguay	1	22.355	1.676.625	-	-
Czech Republic	2	97.997	674.686	-	-
Slovakia	1	127.636	382.908	-	-
Sao Tome and Principe	1	13.402	160.824	-	-
Korea	2	26.256	86.277	-	1
Spain	1	17.662	52.986	-	-
Anguilla	1	2.972	44.850	-	-
Argentina	10	11.824	25.472	-	-
Kenya	1	243	14.580	-	-
Barbados	1	14	2.800	-	-
Vietnam	1	1.471	1.471	-	-
Albania	1	200	1.000	-	-
Romania	1	67	737	-	-

HIPAA Merkmale für ‚Personal Health Information'

Merkmal	**Vorhanden?**
Patient name	Ja
Dates (birth, treatment, death)	Ja
Physical addresses	Nein
Fax numbers	Wahrscheinlich
Social security numbers	Ja
certificate/license numbers	Nein
phone numbers	Wahrscheinlich
full face photos/other pictures	Ja
URLs/web addresses	Wahrscheinlich
E-mail addresses	Wahrscheinlich
health plan beneficiary information	Wahrscheinlich
Internet Protocol (IP) addresses	(Ja)
medical record #s	Ja
device identifiers and serial #s	Wahrscheinlich
biometric (finger, voice, etc.) info	Nein
account numbers	Wahrscheinlich
vehicle identification information	Nein
Other uniquely identifying info	Ja