کنفرانس ملی ارتقای سلامت و چالش‌های حقوقی و پزشکی فراروی آن
NATIONAL CONFERENCE ON HEALTH PROMOTION & IT'S LEGAL & MEDICAL CHALLENGES

امنیت سایبری تجهیزات بیمارستانی

جمال بیگی
دانشیار، گروه حقوق جزا و جرم شناسی، مرکز تحقیقات حقوق، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
(نویسنده مسئول)
jamalbeigi@iau-maragheh.ac.ir

زهرا اقبالی
دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
Zahra.eghbali7@yahoo.com

چکیده

فناوری های هوشمند مزایای بسیاری را در صنعت پزشکی فراهم می کنند. اما همراه با این مزایا، چالش هایی در زمینه امنیت سایبری نیز به وجود آمده است. چنین وسایلی به پزشکان امکان می دهد تا به سرعت و به طور مداوم بیماران و وضعیت پزشکی آنها را کنترل کنند. علاوه بر این، فناوری های هوشمند امکان تجزیه و تحلیل دقیق تر و تشخیص زودتر مسائل پزشکی را فراهم می کنند. با توجه به تقاضای روز افزون استفاده از سامانه های ذخیره سازی و انتقال تصاویر پزشکی، شناسایی و انتخاب نرم افزار هایی که از مراحل فیلتر های امنیتی عبور کرده باشد اهمیت بالایی دارد. تحقیق حاضر به روش توصیفی – تحلیلی و با هدف تبیین امنیت سایبری تجهیزات بیمارستانی نگارش یافته است، یافته های تحقیق حاکی از آن است که: با اجرای استراتژی های مناسب جهت مدیریت تهدیدات سایبری و شناسایی و ارزیابی منابع خطر می توان امنیت سایبری در تجهیزات بیمارستانی را تا حدود زیادی بهبود بخشید و از هک شدن دستگاه ها جلوگیری کرد. تنها پلتفرمی که در ایران از تمامی مراحل و آزمون های امنیتی عبور کرده و مورد تایید است و همچنین دارای گواهینامه ارزیابی امنیت از سازمان افتا می باشد، متریک است.

کلید واژه ها: امنیت سایبری، فضای سایبری، حمله هکرها، تجهیزات بیمارستانی

۱.بیان مسأله

با توجه به پیشرفت تکنولوژی در صنعت پزشکی دستگاه‌های هوشمند به‌صورت فزاینده‌ای در بیمارستان‌ها به‌کار برده می‌شوند. بعلاوه، تکنولوژی‌های هوشمند، امکان تجزیه و آنالیز بادقت‌تر و تشخیص سریع‌تر مسائل حوزه سلامت را به‌وجود می‌آورند. فناوری IoT این روزها در همه جا هست و حوزه پزشکی یکی از حوزه‌هایی است که اینترنت اشیا در آن رواج پیدا کرده است. به عبارت دیگر با کاهش هزینه ساخت حسگرهای میکروسکوپی و رایانش ابری که سازمان‌ها را قادر می‌سازد به منابع محاسباتی دسترسی پیدا کنند، فناوری‌های اینترنت اشیا (IoT) در نظر گرفته شده‌اند که مراقبت‌های بهداشتی را مختل کنند اینترنت اشیای پزشکی یا به اختصار IoMT، یکی دیگر از موارد ضروری است که به امنیت آن بایستی توجه شود.

با بیشتر شدن محبوبیت IoMT، بالا رفتن تهدیدهای امنیتی آن را هم مشاهده می‌کنیم. هکرها موسسه‌های بهداشتی در سرتاسر دنیا را هدف می‌گیرند و هدف‌های اصلی هکرها به‌صورت معمول، بیمارستان‌ها هستند. در ارتباط با امنیت سایبری در اینترنت اشیای پزشکی باید بگوییم که حمله‌های سابیری به موسسه‌های بهداشتی، مشکل‌های زیادی را به‌وجود آورده است. آن‌ها باعث مختل شدن خیلی از خدمات ضروری شده‌اند، خسارت‌های مالی به‌وجود آورده‌اند و موجب کاهش میزان اعتماد بیماران نسبت به کل سیستم مراقبت‌های بهداشتی شده‌اند. این حملات باعث ایجاد خطر برای ایمنی سلامتی مریض ها و نقض حریم شخصی ان ها نیز شده‌اند. بدین ترتیب، از دغدغه هایی که این روزها در عرصه پزشکی می باشد هک شدن وسایل پزشکی بوده که با این وجود تولید کنندگان باید توجه ویژه ای به امنیت تجهیزات پزشکی قائل شوند. در حقیقت اگر به امنیت این تجهیزات توجه شود جان بیماران از نظر حمله های امنیتی نیز محافظت خواهد شد. متاسفانه امروزه برخی تولید کنندگان تجهیزات پزشکی موضوع امنیت را نادیده گرفته اند ولی در آینده نه چندان دور تجهیزات پزشکی باید از امکانات امنیتی قوی تری برخوردار باشند.

بدین ترتیب، هدف این مقاله خلاصه ای از مطالعات اخیر در حوزه امنیت سایبری برای PACS و تصویربرداری پزشکی است. این نتایج می تواند برای پژوهشگران و کارشناسان فناوری اطلاعات پزشکی و همچنین مدیران CIO یا PACS که به دنبال مقایسه امنیت سایبری مرکز خود با جدیدترین تکنولوژی‌های موجود هستند، مفید واقع شود. در عمل برای پیشگیری از حوادثی مانند تنظیم مجدد بایگانی تصاویر به نحوی که دسترسی بدون محدودیت از طریق اینترنت به آن‌ها امکان پذیر باشد، اقدامات امنیتی مختص PACS باید همراه با اقدامات قابل اجرا در زیرساخت IT به صورت یکپارچه اجرا شود. مطالعات نشان می دهد که صدها سیستم PACS در سراسر جهان در معرض دسترسی از طریق اینترنت قرار دارند و تعداد آن‌ها با گذشت زمان افزایش نیز می‌یابد. بنابراین اقدامات امنیتی بیشتری باید در این حوزه انجام تا از تهدیدات سایبری جلوگیری شود.

۲.پیشینه تحقیق

مهدی زاده گوهری و ناصر اسدی(۱۳۹۴) طرحی را ارائه داده اند که درآن استفاده از امضا دیجیتال به منظور اطمینان از عدم دسترسی افراد غیر مجاز به اطلاعات پیشنهاد شده است. امضا دیجیتال یک مکانیزم اعتبارسنجی است. به این صورت که فرستنده می تواند یک کد منحصر به فرد به متن اصلی اختصاص دهد. این کارمعمولا با استفاد از امضا کردن متن انجام می شود. در این صورت امضا دیجیتال با استفاده از کلید خصوصی فرستنده ایجاد می شود و هرکس که کلید عمومی متناظر با این کلید خصوصی را داشته باشد، می تواند امضا را مشاهده و اعتبار آن را بررسی کند. برای اینکه از امضا دیجیتال در پرونده های بیماران استفاده کنیم باید ابتدا پرونده های کاغذی پزشکی به پرونده های الکترونیکی سلامت تبدیل شوند.

در مقاله گلناری و رضایی(۱۳۹۱) مروری بر پنج طرح تصدیق شده است که مقاله شان سعی در اثبات آن دارد که همه آن ها در رسیدن به تصدیق دو فاکتوری شکست می خورند و مهاجم می تواند زمانی که از کارت هوشمند اطلاعات محرمانه به دست آورده باشد، حمله حدس رمز عبور برون خطی را انجام دهد. اما تعدادی از آنها در برابر حملات جعل هویتی، حملات محرمانگی، حملاتReplay، حملات موازی، حملات تغییر و تبدیل و حملات حدس رمز عبور برون خطی مقاومت می کنند.

در طرح پیشنهادی سوسانتو و همکارانش یک رویکرد جدول برای ارزیابی تهدیدات امنیتی ارائه شده است. با استفاده از یک مطالعه موردی در زمینه پزشکی تله مدیسین، مفهوم و مفید بودن برنامه‌های کاربردی تله مدیسین نشان داده شده است. این مطالعه نشان می‌دهد که حتی در یک محیط کنترل شده با مکان‌های ایستا و امنیت، خطرات ناشی از برنامه‌های کاربردی تله‌مدیسین قابل توجه هستند. به کارگیری یک روال جدید تهدید، یک روش آسان برای مدیریت این تهدیدات فراهم می‌کند. (Susanto,Almunawar&Tuan,2011:23-29) .

۳.مفهوم شناسی

در ابتدا، فضای سایبری و امنیت سایبری به منظور بوجود آوردن پایه‌های امنیتی برای شبکه‌ها در حال حاضر و در آینده، تعریف می‌شوند. فضای سایبری یک رسانه جدید از جنس ارتباطات الکترونیکی را برای ارتباط فراهم کرده است. می‌توان فضای سایبری را به عنوان یک محیط مجازی و رسانه‌ای برای شبکه‌های کامپیوتری تعریف کرد که در آن ارتباطات آنلاین انجام می‌شود. این فضا، یک محیط پیچیده و ناشی از تولد اینترنت است که شامل افراد، سازمان‌ها، فعالیت‌ها، خدمات و تجهیزات فناوری است. امنیت سایبری به عنوان یک مجموعه از فرآیندها، تدابیر و تکنیک‌ها برای حفظ امنیت و حریم خصوصی در این محیط مجازی عمل می‌کند. امنیت سایبری برای محافظت از اطلاعات، داده‌ها، سیستم‌ها و زیرساخت‌های فناوری اطلاعات در فضای سایبری بسیار اهمیت دارد و از اهداف اصلی سازمان‌ها و افراد در این حوزه است به عنوان مثال ممکن است در بازی برخط، دنیاهای مجازی بسیاری پول رایجی داشته باشند که برای خرید آیتم های بازی در سایت های بازی اینترنتی استفاده می شود، در نتیجه ارزشی در دنیای واقعی وجود دارد که با پول مجازی و حتی با آیتم های بازی مرتبط است. این آیتم های مجازی به کرات با پول واقعی در سایت های بازی و فعالیت های آنلاین مبادله می شوند، آنچنان که برخی سایت های بازی، برای تبدیل آیتم به پول حقیقی کانالی رسمی با نرخ های مبادله پول مجازی/ حقیقی دارند. این کانال های تبدیل آیتم به پول، دنیای مجازی را هدف حمله قرار می دهد که معمولاً به صورت طعمه گذاری یا سایر روش های سرقت اطلاعات کاربری، انجام می شود. (موسوی، ۱۴۰۰: ۳۱).

تهدیدهای سایبری را می توان به دو شیوه تصادفی یا عمومی دسته بندی کرد. از طرفی تهدیدهای امنیتی ممکن است، فعال یا غیرفعال باشند. تهدیدهای تصادفی، تهدیدهایی هستند که بدون هیچ قصد و نیت قبلی صورت می گیرند. (گیورا، ۱۳۹۹: ۲۹). عملکرد نادرست سیستم، اشکالات نرم افزاری و خطاهای عملیاتی نمونه هایی از تهدیدهای تصادفی هستند. (موسوی، ۱۴۰۰: ۳۱). تهدیدهای عمدی ممکن است دامنه ای از تهدیدها را در برگیرد، آزمون های اتفاقی، استفاده از ابزارهای پایشی در دسترس و حملات دشوار و پیچیده ای که به دانش و مهارت ویژه ای نیاز دارند. تهدید عمدی در صورت وقوع ممکن است به حمله منجر شود. (گیورا، ۱۳۹۹: ۲۹). تهدیدهای غیرفعال، تهدیدهایی هستند که به دستکاری اطلاعات سیستم یا سیستم ها و نیز تغییر وضعیت سیستم و عملیات منتهی نمی شوند. استفاده غیرفعال از استراق سمع سیم برای مشاهده اطلاعات ارسال شده از طریق خطوط ارتباطی نمونه ای از تهدیدهای غیرفعال است. در مقابل، تهدیدهای فعال تغییر اطلاعات سیستم یا تغییر وضعیت سیستم و عملیات را به همراه دارند. (یول یوم، پایک، ۱۳۹۴: ۳۳).

تهدیدها بر دارایی ها تأثیر می گذارند، بنابراین در مرحله اول باید از دارایی هایی که نیاز به محافظت دارند، فهرستی تهیه کرد. در مرحله بعدی تهدید تحلیل می شود و سپس تحلیل نقاط آسیب پذیر که شامل ارزیابی اثر است، انجام می شود. براساس نتایج این ارزیابی، سازوکارهای امنیتی و راهکارهای مقابله با تهدیدها تدوین می شوند. گام های عمده امنیت سایبری به صورت زیر است:

۱. شناسایی نقاط آسیب پذیر سیستم
۲. تحلیل احتمال تهدیدها در نقاط آسیب پذیر شناسایی شده در مرحله قبل
۳. ارزیابی نتایج وقوع موفقیت آمیز هر تهدید

۴. تخمین هزینه هر حمله

۵. تعیین هزینه راهکارهای احتمالی مقابله

۶. انتخاب سازوکارهای امنیتی با استفاده از تحلیل هزینه/ فایده آنها

در برخی موارد ممکن است، معیارهای غیرتکنیکی مانند پوشش بیمه از نظر هزینه برای معیارهای امنیتی تکنیکی مناسب باشد تا میزان ریسک به سطوح قابل قبول کاهش یابد. (بریناتو و همکاران، ۱۳۹۹: ۲۴).

و اما، واژه امنیت سایبری را می توان به صورت مجموعه ای از ابزارها، سیاست ها، تدابیر امنیتی، تضمین های امنیتی، رهنمودها، رویکردهای مدیریت ریسک، اقدامات، آموزش و به روش ها تعریف کرد که برای محافظت از دارایی های کاربران، سازمان و محیط سایبری، براساس توصیه نامه اتحادیه بین المللی مخابرات به کار می رود. (موسوی، ۱۴۰۰: ۳۲). اطلاعات و دارایی های فناوری اطلاعات و ارتباطات سازمان و کاربران شامل تجهیزات کامپیوتری متصل به هم، دستگاه های همراه، پرسنل، زیرساخت، برنامه های کاربردی، خدمات، سیستم های مخابرات و نیز کلیه اطلاعات منتقل شده و ذخیره در محیط سایبری می شود. امنیت سایبری می کوشد از کسب، حفظ و نگهداری دارایی های امنیتی سازمان و اطلاعات کاربران در برابر ریسک های امنیتی محیط سایبری اطمینان حاصل کند. (یول یوم، پایک، ۱۳۹۴: ۳۴). اهداف کلی امنیت عبارتند از:

۱. دسترس پذیری

۲. صحت که ممکن است شامل اعتبارسنجی پیام با موجودیت و عدم انکار می شود

۳. محرمانگی

تکنیک های امنیت سایبری برای اطمینان از محرمانگی، عدم انکار، اعتبارسنجی، صحت و دسترس پذیری سیستم استفاده می شوند. به علاوه، امنیت سایبری حریم خصوصی و احترام کاربران را حفظ می کند و به افزایش اعتماد کاربران منجر می شود.

محیط سایبری، نرم افزاری که تجهیزات کامپیوتری را راه اندازی می کند، اطلاعات ذخیره شده یا حتی ارسال شده این تجهیزات و اطلاعاتی که توسط این تجهیزات تولید می شود. تأسیسات و ساختمان هایی که این تجهیزات را در خود جای داده اند، نیز بخشی از محیط سایبری هستند. توجه تمامی این عناصر از الزامات امنیت سایبری است. (موسوی، ۱۴۰۰: ۳۳).

۴.بحث نظری موضوع

۴-۱.تهدیدهای سایبری در فضای سایبری

دسترسی از راه دور و ارتباطات شبکه ای از ملزومات فضای سایبری هستند، اما دسترسی گسترده و مستقل به فناوری های اطلاعات و ارتباطات متصل می تواند منبع اصلی آسیب پذیری های گسترده باشد. نقاط آسیب پذیر، هدف تهدیدهای سایبری هستند. این تهدیدها ویروس ها، کرم ها، اسب های تراوا، بدافزارها، نرم افزارهای جاسوسی، نرم افزارهای تبلیغاتی، حملات حقه بازی، سرقت هویت، هرزنامه ها و حملات سایبری و همه آنچه به وقوع حمله منجر می شود را شامل می شوند. (گروه ترجمه انتشارات آتی نگر، ۱۳۹۴: ۲۶).

برخلاف رایانه‌های رومیزی و سرورها که نرم‌افزارهای ضدویروس و دیگر نرم‌افزارهای امنیتی را اجرا می‌کنند، تنوع بالای دستگاه‌های اینترنت اشیا و عدم توجه به حوزه امنیت دستگاه‌های IoT در مراحل ابتدایی پیدایش آن‌ها، در معرض مشکلات امنیتی بیشتری خواهند بود. در یکی از انواع حمله‌های امنیتی به نام MedJack، حمله‌کننده‌ها نوعی بدافزار به دستگاه‌های پزشکی ارسال می‌کنند تا در سراسر شبکه دستگاه‌ها گسترش یابند. (تیومیم، ۱۳۹۹: ۶۱). داده‌های پزشکی در چنین حمله‌های امنیتی در اختیار حمله‌کننده‌ها قرار می‌گیرند و برای هدف تقلب مالیاتی یا سرقت هویت مورد استفاده قرار می‌گیرند. حتی با دسترسی به نسخه‌های دارویی آنلاین هکرها می‌توانند دارو خریداری کنند و در وب تاریک (Dark Web) به فروش می‌رسند. وب تاریک به شبکه‌ای گفته می‌شود که در دسترس عموم قرار نمی‌گیرد و بیشتر برای مقاصد غیرقانونی مورد استفاده قرار می‌گیرد و همه فعالیت‌های آن غیرقابل ردیابی و شناسایی است. (رحیم زاده ترک و حاتمی، ۱۳۹۷: ۴۱). در این شبکه اطلاعات

جامعی نهفته شده که افراد ناشناس آن‌ها را مدیریت می‌کنند، هکرها و افراد سودجو غالباً این دسته از افراد را تشکیل می‌دهند. این حمله‌های امنیتی به تدریج در حال توسعه هستند. طبق گفته شرکت امنیتی شبکه TrapX، حمله امنیتی MedJack در چند ماه اخیر، روش‌های جدید و پیچیده‌تر را به کار گرفته است. این شرکت از فناوری تقلید (emulation technology) استفاده کرد تا دستگاه‌های جعل هویت مانند دستگاه سی‌تی اسکن را در شبکه تجهیزات پزشکی بیمارستان به کارگیرد. هنگامی که هکرها این دستگاه‌ها را شناسایی کردند تا از آن‌ها در راستای حمله امنیتی بهره گیرند، TrapX متوجه شد که حمله MedJack عمدا از بدافزارهای قدیمی برای هک کردن تجهیزات پزشکی با سیستم‌عامل‌های قدیمی مثل ویندوز اکس‌پی و ویندوز سرور ۲۰۰۳ استفاده می‌کند. با هک کردن دستگاه‌های قدیمی، هکرها از شناسایی شدن در امان می‌مانند. دستگاه‌های به روز در برابر نرم‌افزارهای مخرب قدیمی مقاوم هستند و به عنوان یک تهدید نه چندان قوی طبقه‌بندی می‌شوند. (تیومیم، ۱۳۹۹: ۶۱-۶۲).هکرها با یک بار هک می‌توانند با دیگر انواع حمله‌ها از شبکه سواستفاده کنند. یکی از حمله‌های امنیتی که در حال افزایش است حمله باج‌افزارها (ransomware) هستند. باج‌افزار گونه‌ای از بدافزار است که دسترسی به سامانه را محدود می‌کند و ایجادکننده آن برای برداشتن محدودیت از کاربر می‌خواهد مبالغی را واریز کند. بسیاری از این نوع حمله‌ها با روش‌های سنتی پرونده‌های دیجیتال را رمزنگاری می‌کنند مانند حمله اخیر به کلینیک کودکان Rainbow در تگزاس. در حمله باج‌افزار به مرکز پزشکی پروتستان هالیوود رایانه‌ها برای مدت یک هفته آفلاین شدند و در یک بیمارستان آلمانی، چنین باج‌افزاری باعث شد ایمیل‌ها از کار بیفتند و کارکنان مجبور شدند از کاغذ و دستگاه‌های فکس استفاده کنند. بیمارستان‌ها نه تنها سرمایه خود را برای چنین حمله‌ای از دست می‌دهند بلکه منابع حیاتی و مهم مربوط به درمان بیماران را برای مدتی در اختیار ندارند (ر.ک: بگل و همکاران، ۱۳۹۳: ۵۸).

وسایل پزشکی مانند ساعت و وسایل سنجش سلامت که برای سال‌ها در بازار موجود هستند نیاز به رویکردهای امنیتی مانند نظارت بر امنیت و روش‌های آسان دانلود به روزرسانی‌ها دارند. از سوی دیگر، نسل‌های آینده دستگاه‌های پزشکی باید امکانات امنیتی قوی‌تر و پایدارتر داشته باشند. بسیاری از تولیدکنندگان مسئله امنیت را در مراحل ابتدایی کار نادیده می‌گیرند و از برنامه‌های شخص سوم (third-party component) استفاده می‌کنند که خود باعث آسیب‌پذیری بیشتر می‌شود. برنامه‌های شخص سوم، برنامه‌هایی هستند که برای کار درون سیستم‌عامل‌ها نوشته شده اما به وسیله افراد یا شرکت‌ها به غیر از تولیدکننده سیستم‌عامل نوشته می‌شوند. (Faddis,2018:28).

۴-۲.هک شبکه ها و تجهیزات پزشکی، بزرگترین تهدید امنیت سایبری

بر اساس نتایج تحقیق موسسه فورستر آمریکا (Forrester)، در ۲۵ سال گذشته هکرها از باج افزارها برای اخاذی از قربانیان خود استفاده می‌کردند؛ اما اکنون به نظر می‌رسد هکرها در نظر دارند از روشی مشابه برای هک دستگاه‌های تزریق انسولین یا تنظیم‌کننده‌های ضربان قلب نیز استفاده کنند. کارشناسان امنیتی معتقدند استفاده از باج افزارها در تجهیزات پزشکی، بزرگ‌ترین تهدید امنیت سایبری جهان در سال ۲۰۱۶ میلادی خواهد بود.

هک شدن تجهیزات پزشکی، امروزه واژه آشنایی برای همه است؛ اما توجه زیادی به این موضوع نمی‌شود. بسیاری معتقدند هک شدن پمپ تزریق دارو در یک بیمارستان، هیچ فایده‌ای برای هکرها ندارد. این موضوع در حقیقت زمانی اهمیت بالایی پیدا خواهد کرد که به هشدارهای شرکت‌های ارائه دهنده خدمات درمانی و بیمه‌ای در ماه‌های اخیر توجه کنیم. بسیاری از آن‌ها اعلام کرده‌اند توسط هکرها مورد تهاجم قرارگرفته‌اند و این موضوع نشان می‌دهد هکرها تمرکز خود را بر روی تجهیزات و صنعت پزشکی، قرار داده‌اند. بزرگترین تهدید برای امنیت بیمارستان از کارافتادن کامل شبکه بیمارستانی می باشد. هکرهایی که از راه رشوه گیری اقدام به فعالیت می کنند در زمینه انتخاب بین یک بیمار و یا بیمارستان معمولا بیمارستان ها رو مورد تهدید خود قرار داده به گونه ای که چندین مورد حمله در سال های اخیر گزارش شده است از جمله آن می توان به حمله WannaCry که سرویس ملی سلامت در بریتانیا (NHS) رو مورد حمله قرار داده بود اشاره کرد.

این حملات با بهره گیری از خطاهای امنیتی موجود در سیستم عامل مایکروسافت به همه ما نشان داد بیمارستان ها تا چه اندازه در برابر این حملات ناکارآمد هستند. به علت شبکه بودن تجهیزات بیمارستانی زمانیکه شبکه بیمارستان مورد حمله قرار می گیرد تنها اطلاعات پزشکی بیمار مورد آسیب نخواهد بود. دسترسی فرد هکر مهاجم به اطلاعات بیمار می تواند باعث تغییر آن اطلاعات و آسیب زدن به روند درمانی افراد شود.

صنعت مراقبت های بهداشتی در پنج نقطه بسیار آسیب پذیر است. هکرها این را می دانند. آنها حملات خود را با درنظر گرفتن این موارد طراحی می کنند:

۱. خاموش شدن وسایل پزشکی می تواند موجب مرگ بیماران و به تاخیر افتادن درمان فوری پزشکی شود.

۲. از دست دادن سابقه پزشکی بیمار می تواند درمان شرایط پزشکی را به تاخیر بیندازد.

۳. امکان مواجهه با تحقیقات فدرال و جنایی و جریمه یا تحریم. برخی از ارائه دهندگان پزشکی به کنترل های امنیتی مجهز نیستند، اما بسیاری از آنها خطرات را دست کم می گیرند.(براتی پور، ۱۰:۱۳۸۶).

۴. هکرها می‌توانند از فروش اطلاعات سلامت شخصی (PHI) که ارزش آن بیشتر از اطلاعات شناسایی شخصی «معمولی» است، سود به دست آورند. شما می توانید کارت اعتباری یا حتی SSN خود را تغییر دهید، اما نمی توانید سابقه پزشکی خود را از بیماری ها، درمان ها یا جراحی ها تغییر دهید. (Kuesr,Frederick,Jacobson&Monticone,2017:25)

بدین ترتیب، توجه ویژه به امنیت تجهیزات پزشکی اهمیت دارد. از یک سو بیماران باید در برابر چنین حمله‌های امنیتی محافظت شوند، از سوی دیگر در یک شبکه بیمارستانی دستگاه‌های پزشکی به تعداد زیادی حسگر و دستگاه‌های نظارت متصل هستند و به هکرها اجازه می‌دهند به سابقه پزشکی بیماران دسترسی داشته باشند و یا سامانه‌های حیاتی موجود در بیمارستان را در اختیار بگیرند و از مدیران بیمارستان تقاضای پول کنند.

۴-۳.امنیت در مراقبت های بهداشتی IT

نشریات در حوزه امنیت سایبری از سال ۲۰۱۲ افزایش چشمگیری داشته‌اند. استانداردهای متعدد موجود، مقررات دولتی، دستورالعمل‌های ارائه دهنده بهترین روش‌ها و مقالات علمی، هر کدام در حوزه امنیت سایبری بحث کرده و توصیه‌هایی را ارائه می‌دهند. امنیت در مراقبت های بهداشتی IT یکی از موارد حیاتی است که باید در تمامی سیستم های بهداشتی، از جمله بیمارستان ها، کلینیک ها و مراکز بهداشتی، به آن توجه شود. با توجه به اینکه در سیستم های بهداشتی، اطلاعات حساسی در مورد بیماران و پزشکان در دسترس هستند، به همین دلیل امنیت در این سیستم ها بسیار مهم است. اولین گام برای افزایش امنیت در مراقبت های بهداشتیIT ، آموزش پرسنل و کاربران در مورد امنیت سایبری و مدیریت ریسک است. همچنین، نیاز است تا سیستم های بهداشتی با استفاده از فناوری های امنیتی نظیر رمزنگاری، تصدیق هویت و کنترل دسترسی محافظت شوند. همچنین، لازم است تا سیستم های مانیتورینگ و پشتیبانی مداوم برای تشخیص و جلوگیری از حملات سایبری و جرم دیجیتال فعال شوند .علاوه بر این، باید سیاست های رمزنگاری داده ها و پشتیبانی را برای حفظ اطلاعات بیماران و کاربران در نظر گرفت. همچنین، باید سیستم های مدیریت ریسک، برنامه های پشتیبانی و نیز سیاست های بازیابی در صورت بروز حملات سایبری به روز رسانی شود. در نهایت، پیشگیری از هر گونه حمله سایبری، شامل مانیتورینگ و تشخیص هر نوع فعالیت شبیه سایبری، مهم است.

۴-۳-۱.امنیت سایبری در PACS و تصویربرداری پزشکی

با توجه به اصول امنیت سایبری در فناوری اطلاعات و ارتباطات در حوزه بهداشت و درمان، تعداد محدودی از مقالات تمرکز خاصی بر روی امنیت پیشرفته و الزامات PACS و تصویربرداری پزشکی دارند. در حالی که بسیاری از مقالات موجود در زمینه برنامه‌های تله‌رادیولوژی/تله‌پزشکی یا سوابق الکترونیکی بهداشت (EHR) تمرکز دارند. استریکلند در مورد خطرات مرتبط با

استقرار و بهره‌برداری از PACS بحث می‌کند، اگرچه به امنیت سایبری توجه کافی نمی‌کند. دژاردین و همکاران یک نمای کلی از مسائل امنیت سایبری مربوط به استفاده از استاندارد DICOM ارائه می‌دهند و توصیه‌هایی برای رادیولوژیست‌ها، کارکنان فناوری اطلاعات و نهادهای استانداردسازی و قانون‌گذاری را ارائه می‌دهند. (ر.ک: رحیم زاده ترک و حاتمی، ۱۳۹۷: ۴۴-۴۵).

PACS به یک سیستم دیجیتالی اطلاق می‌شود که برای ذخیره و به اشتراک گذاری تصاویر پزشکی بین سیستم‌های مختلف و پزشکان مختلف به کار می‌رود. تصویربرداری پزشکی به مجموعه‌ای از فناوری‌هایی اطلاق می‌شود که برای تولید تصاویر پزشکی استفاده می‌شود، در حالی که PACS به یک سیستم ذخیره‌سازی و به اشتراک گذاری تصاویر پزشکی بین سیستم‌های مختلف و پزشکان مختلف اشاره دارد. در واقع، PACS یکی از راه‌حل‌هایی است که در تصویربرداری پزشکی برای ذخیره، مدیریت و به اشتراک گذاری تصاویر پزشکی استفاده می‌شود. این سیستم امکان دسترسی به تصاویر پزشکی را به صورت آنلاین و با استفاده از شبکه‌های ارتباطی فراهم می‌کند. به عبارت دیگر، PACSبه پزشکان این امکان را می‌دهد که به راحتی تصاویر پزشکی بیمار را بررسی کنند و برای تشخیص، پیشگیری و درمان بیماری‌ها از آن استفاده کنند.

PACS به معنای سامانه‌ی تصویربرداری پزشکی دیجیتالی باشد و امنیت سایبری در PACS از اهمیت بسیاری برخوردار است. برای اینکه اطلاعات پزشکی بیماران در سامانه PACS محافظت شود، باید اقداماتی انجام شود که در زیر به برخی از آن‌ها اشاره می‌کنیم:

استفاده از رمزنگاری: برای جلوگیری از دسترسی غیرمجاز به اطلاعات پزشکی بیماران، از رمزنگاری استفاده می‌شود. با این روش، اطلاعات پزشکی بیماران تنها با رمزگشایی صحیح در دسترس کاربران قرار می‌گیرد.

محدود کردن دسترسی: برای جلوگیری از دسترسی غیرمجاز به اطلاعات پزشکی بیماران، باید دسترسی کاربران به سامانه PACS محدود شود. به این صورت که تنها کاربرانی که دسترسی لازم را دارند، به اطلاعات پزشکی بیماران دسترسی دارند.

پشتیبانی از آخرین نسخه‌ی نرم‌افزار: برای جلوگیری از نفوذ به سامانه PACS، باید از آخرین نسخه‌ی نرم‌افزار استفاده شود. این نسخه‌ها تعمیرات امنیتی برای مسدود کردن نقاط ضعف در سامانه PACS دارند.

آموزش کاربران: کاربران باید با اهمیت و محدودیت‌های دسترسی به اطلاعات پزشکی بیماران آشنا شوند و از آن‌ها پیروی کنند.

پشتیبانی از تهیه‌ی پشتیبان از داده‌ها: برای جلوگیری از از دست دادن داده‌های پزشکی بیماران، باید تهیه‌ی پشتیبان از اطلاعات در سامانه PACS انجام شود.

انواع تصاویر پزشکی: سامانه PACS انواع مختلفی از تصاویر پزشکی را پشتیبانی می‌کند، از جمله تصاویر رادیولوژی، سونوگرافی، اندوسکوپی، اشعه‌ی فرابنفش و ...

با بررسی مزایا و معایب استفاده از سامانه PACS، می‌توانید درک بهتری از این سامانه داشته باشید. به عنوان مثال، برای مزایا می‌توان به افزایش دقت تشخیصی و افزایش سرعت در تحلیل تصاویر پزشکی اشاره کرد و برای معایب می‌توان به هزینه‌ی بالای سامانه PACS و نیاز به پشتیبانی فنی اشاره کرد.

۴-۴.چالش های اصلی امنیتی صنعت بهداشت و درمان

امنیت در حوزه پزشکی در فضای سایبری با چالش های زیر مواجه می باشد:

۴-۴-۱.تاخیر زمانی

تاخیر زمانی می‌تواند به دلیل محدودیت منابع، عدم هماهنگی بین سیستم‌های مختلف، کاستی در فناوری و سایر موارد رخ دهد. مشکلاتی مانند تاخیر زمانی می‌توانند باعث کاهش کیفیت خدمات بهداشتی و درمانی شوند و در برخی موارد می‌توانند منجر به صدمات جدی برای بیماران شوند. به طور مثال، در صورتی که تاخیر زمانی در برقراری ارتباط بین بیمار و پزشک اتفاق بیافتد، پزشک نمی‌تواند به بهترین شکل ممکن به بیمار خدمات پزشکی لازم را ارائه دهد.

از دیگر مواردی که تاخیر زمانی ممکن است به عنوان یک چالش امنیتی در صنعت بهداشت و درمان مطرح شود، می‌توان به تاخیر در اعمال تغییرات و بهبودهای امنیتی در سیستم‌ها و تجهیزات پزشکی اشاره کرد. در صورتی که تغییرات امنیتی به موقع اعمال نشوند، احتمال بروز مشکلات امنیتی و حملات سایبری برای سیستم‌های پزشکی و بیماران بیشتر می‌شود. به علاوه، خدمات بهداشتی و درمانی از راه دور، مانند ویزیت بیماران و تشخیص بیماری از راه دور در حال رشد است، بنابراین اطلاعات پزشکی باید همواره در دسترس باشند. به همین دلیل، تکنولوژی‌های پشتیبانی کننده باید با نسخه‌های فعلی پروتکل انتقال دیتا G۵ هماهنگ بوده و همچنین لبه WAN بهینه‌سازی شده و سازگار باشد.

۴-۴-۲.یکپارچگی داده ها

یکپارچگی داده ها در صنعت بهداشت و درمان بسیار مهم است و عدم آن می‌تواند به عنوان یکی از چالش‌های امنیتی مطرح شود. در حال حاضر، بسیاری از اطلاعات پزشکی، شامل اطلاعات پزشکی بیماران، تاریخچه پزشکی، نتایج آزمایش‌های پزشکی و داروهای مصرفی، به صورت دیجیتال ذخیره و پردازش می‌شوند.

اگر داده های پزشکی در سیستم های مختلف و در قالب های مختلف ذخیره شوند و همگام نباشند، امنیت و حریم خصوصی بیماران به خطر می‌افتد و تهدیدی برای بهداشت عمومی می‌شود. برای مثال، اگر داده های پزشکی در یک سیستم ذخیره شده و در سیستم های دیگر در دسترس نباشد، ممکن است به یک بیمار درمان ناصحیح داده شود، به دلیل اینکه اطلاعات در دسترس نبوده است. برای جلوگیری از تهدیدات امنیتی، باید داده های پزشکی به صورت یکپارچه و در سیستم های مرکزی ذخیره شوند. همچنین، اطمینان حاصل شود که سیستم های مورد استفاده، مطابق با استانداردهای امنیتی و حریم خصوصی بین‌المللی هستند و از روش های قابل اعتماد برای رمزگذاری و محافظت از داده ها استفاده می‌کنند.

۴_۴_۳.گزارش های انطباق:

این گزارش‌ها ممکن است شامل اطلاعات حساس و شخصی بیماران باشند که باید محرمانه باشند. همچنین، برای اطمینان از اینکه این گزارش‌ها درست و صحیح هستند، باید از روش‌های امنیتی قوی استفاده شود تا هرگونه دسترسی غیرمجاز به اطلاعات بیماران به دست نیاید. بنابراین، باید از روش‌های امنیتی قوی برای محافظت از گزارش‌های انطباق استفاده کرد و همچنین اطمینان حاصل کرد که دسترسی به این گزارش‌ها محدود به افرادی باشد که دارای مجوز و دسترسی مجاز به آنهاست. حوزه های قضایی در سراسر دنیا همچنان قوانینی مخصوص به مراقبت های بهداشتی وضع می کنند. حفاظت از اطلاعات الکترونیکی بیماران نیز، هم به دلیل مراقبت از بیماران حائز اهمیت است و هم به دلیل رعایت قوانین. همه مراکز بهداشتی و درمانی از اطلاعات مالی بیماران و اطلاعات منابع انسانی گذشته و فعلی کارمندان خود نگهداری می کنند. بنابراین سازمان های بهداشتی و درمانی می بایست دارای اصول و قوانینی باشند تا استانداردها را رعایت کنند.

۴_۵.عوامل ایجاد امنیت سایبری تجهیزات بیمارستان ها

امنیت سایبری در حوزه سلامت و تجهیزات پزشکی در بیمارستان ها به موارد زیر بستگی دارد:

۴-۵-۱.امنیت سایبری و فیزیکی

اولین و مسلماً بارزترین سطح امنیت سایبری، سطح فیزیکی است. اگر یک مهاجم بتواند به راحتی وارد اتاق سرور شود و رایانه‌ها یا مدیاهای ذخیره سازی را بدزدد، اقدامات کاهش اثر فنی مانند رمزهای عبور، اسکنر ویروس یا سطح دسترسی کاربر، ارزش کمی دارد. یک مطالعه ENISA گزارش می‌دهد که امنیت فیزیکی و محیطی پس از حوادث سایبری، مهم‌ترین نیاز امنیتی در

سلامت الکترونیکی است. یک اصل اساسی برای حفاظت فیزیکی از داده‌ها، اطمینان از قرار گرفتن سرورهای فایل در مناطق ایمن است که از دسترسی غیر مجاز و تهدیدهای محیطی مانند آتش سوزی، سیل، قطع برق و غیره محافظت شوند. (پورفیضی و عراقی زاده، ۱۴۰۱: ۴).

از اینرو، مراکز مراقبت های بهداشتی و درمانی باید از امنیت استاندارد فیزیکی برخوردار بوده تا در شرایط غیر منتظره هم آمادگی کامل داشته باشند. بیمارانی که با تشخیص بیماری های جدی و یا جراحت های سخت، وارد این مراکز می شوند، توسط دوستان و خانواده بیمار، نوسانات احساسی پیش می آید. به علاوه، مهاجمان نیز به منظور ایجاد اختلال و همچنین هدف قرار دادن افرادی که انواع مراقبت های جنجالی و بحث برانگیز را انجام می دهند، به این مراکز مراجعه می کنند. به طور خلاصه می توان گفت در صنعت بهداشت و درمان، امنیت فیزیکی نیز به اندازه امنیت سایبری اهمیت دارد.

بهترین روش جهت بهینه سازی امنیت فیزیکی، یکپارچه سازی و ادغام دوربین های نظارتی با ساختار امنیتی کلی است تا از این دستگاه ها در برابر حملات سایبری، محافظت گردد. در ضمن یکپارچه ساختن سیستم تلفن با همان شبکه، موجب برقراری ارتباط ایمن بین پرسنل و متخصصان امنیت و مجریان قانون می شود. (Kobayashi, Furuie &Baretto,2018:582-589)

فورتی نت فرصتی را ایجاد کرده تا موسسات بتوانند علاوه بر ادغام عملکردهای امنیتی فیزیکی و سایبری خود، ارتباطات صوتی و سیستم PA را نیز با هم ادغام کنند و از یک کنسول واحد، بر روی آن ها کنترل داشته باشند. این یکپارچه سازی موجب می شود سیستم های تلفن، دوربین های امنیتی، سیستم تشخیص چهره، تکنولوژی تشخیص اسلحه و همچنین ریکورد کردن فیلم، بخشی از ساختار امنیتی سازمان ها گردد. موارد ذکر شده در مبحث حریم خصوصی و همچنین مطلع ساختن سایرین از یک حادثه، کاربردی تر می شوند.

۴-۵-۲.پدافند غیر عامل در نظام سلامت

در کل، هر اقدامی که سلامت و بهداشت فردی و اجتماعی را افزایش داده، به استمرار خدمات بهداشت و درمان کمک کرده و در برابر بحران‌ها و جنگ مقاومت بیشتری را فراهم کند، به عنوان پدافند غیرعامل در نظام سلامت در نظر گرفته می‌شود. این اقدامات، به علاوه اصول پایه‌ای پدافند غیرعامل، شامل تمامی تحقیقات، دانش‌های علمی و فنی است که باعث توانمندی و اقتدار ملی در حوزه‌های علوم و فناوری، پیشگیری، تشخیص، درمان و بازتوانی می‌شود. اقتدار و توانمندی هر کشوری نتیجه پیشرفت‌های علمی و فنی آن است. پیشرفت علمی در حوزه بهداشت و درمان باعث کاهش صدمات و آسیب‌های ناشی از سوانح و بحران‌ها می‌شود. توسعه فرهنگ ایمنی فردی و جمعی و حفاظت، نقش مهمی در کاهش آسیب‌پذیری در حوادث و بلایا، حتی در سوانح انسان‌ساز مانند جنگ، دارد. (تیومیم، ۱۳۹۹: ۸۳).به عنوان مثال، ژاپن کشوری با بیشترین میزان وقوع زلزله، به دلیل توسعه فرهنگ ایمنی فردی و جمعی و مقاوم سازی تاسیسات، کمترین میزان تلفات را در مقایسه با کشورهای دیگر دارد. این نشان‌دهنده اهمیت فرهنگ‌سازی ایمنی و نهادینه کردن آن در بین مدیران و مردم است. هدف از اجرای اصول پدافند غیرعامل، کاهش خسارات و آسیب‌پذیری به تاسیسات، تجهیزات و نیروهای انسانی در نتیجه بحران‌های طبیعی و تهاجم دشمن است.

۴-۵-۳.حفاظت در برابر تهدیدات داخلی

تحقیقات اخیر Verizon خاطر نشان کرد در بین همه صنایع، صنعت مراقبت های بهداشتی و درمانی، بیشترین احتمال خطر در برابر تهدیدات داخلی را دارد. دو فاکتور «ارزش بالای اطلاعات پزشکی در بازار سیاه» و «گردش مالی بالا در این حوزه» بر روی این موضوع تاثیر دارد. (ر.ک: مشارزموحد و شایگان، ۱۳۹۲: ۱۰۱). تهدیدات داخلی ممکن است تصادفی باشند و یا از روی عمد اتفاق بیافتد که تهدیدات تعمدی، با دلایل مختلف رخ می دهند. حملاتی که در این صنعت رخ می دهد خطرات جبران ناپذیر مانند مرگ به همراه دارند. در ضمن افشای اطلاعات پزشکی نیز مسئولیت سنگینی برای سازمان خواهد داشت.

مسلما مقابله با تهدیدات داخلی مستلزم رویکردی چندلایه و هماهنگ است. ابتدا امر باید شبکه به بخش های مختلف تقسیم

شده تا دسترسی کاربران به قسمت مورد نیاز خود محدود شود. به علاوه، تمام درخواست ها به منابع شبکه، باید هم از منظر کاربر بررسی شود و هم دستگاه. رویکرد zero-trust به مسدود کردن فعالیت های نامناسب توسط تهدیدات داخلی قبل از هر گونه آسیبی کمک فراوانی می کند. سیستم یکپارچه امنیت فورتی نت (Security Fabric) در برابر کلیه تهدیدات داخلی اعم از تصادفی و تعمدی، محافظت می کند. از طرفی قابلیت intent-based segmentation دسترسی افراد را بر حسب نوع نیاز، مجاز می داند. ابزارهای مدیریت و شناسایی، احراز هویت کاربر را تایید نموده و UEBA، رفتارهای مشکوک افراد مجاز را کنترل می کند. از طرفی presence analytics دسترسی افراد غیر مجاز را توسط لوکیشن فیزیکی آن ها شناسایی کرده و تکنولوژیdeception، توسط طعمه های به کار گرفته، مهاجمان را شناسایی می کند. راهکارهای network access control (NAC)) و advanced endpoint security نیز وظیفه تایید دستگاه ها را بر عهده دارند . (Hailey, Ohinmaa & Roine, 2009: 28-31).

۴-۵-۴.صنایع نوظهور و اجرای قوانین

حوزه های قضایی همچنان، قوانین مختلفی را وضع می کنند و فناوری جدید، مقررات و استانداردهای جدیدی را تصویب می کنند، از این رو انطباق با استانداردهای صنعت بهداشت و درمان، هر روز پیچیده تر از قبل می گردد. از طرف دیگر، دستگاه های پزشکی نوظهور و امثال آن نیز تغییرات مداوم آینده را پیش بینی می کند. کاری که سازمان ها باید انجام دهند، ایجاد امنیتی قوی و منعطف است تا بتواند با ابزارهای جدید، هماهنگ گردد، بدون این که نیاز باشد سیستم کلی را هر چند سال یک بار تغییر داد.

سیستم یکپارچه امنیت فورتی نت (Security Fabric)، یک سیستم عامل قوی و انعطاف پذیر ارائه می دهد تا مجموعه گسترده ای از ابزارهای فورتی نت را با هم ادغام کند. استفاده از راهکارهای یکپارچه امنیت فورتی نت در محیط های فیزیکی و فضاهای ابری، کمک به اتوماسیونِ کاملِ مراحلِ تامین امنیت (از شناسایی تهدیدات گرفته تا مقابله با آن ها) می کند. علاوه بر این، «ابزارهای مدیریتی»، «آنالیز» و «مدیریت رخدادها»، به تیم امنیت کمک می کنند تا در پروسه تامین امنیت سازمانی، «رویکرد شناسایی نقاط ضعف امنیتی» و «افزودن فرایندهایی برای شناسایی تهدیدات قبل از وقوع آن ها»، داشته باشند نه مقابله با حملات. (رحیم زاده ترک و حاتمی، ۱۳۹۷: ۵۳).

۴-۵-۵.زیرساخت ترکیبی فضای ابری

زیرساخت سازمان های بهداشتی و درمانی شامل اطلاعات مهم می گردد، مانند: «اطلاعات مالی»، «اطلاعات پزشکی خصوصی»، «سوابق منابع انسانی» و «اپلیکیشن های مهم مورد نیاز بخش درمان». در حال حاضر، عملکرد اکثر موسسات بر روی چندین فضای ابری خصوصی (private) و عمومی (public) می باشد که این امر منجر به شکاف های امنیتی می گردد. بنابراین سازمان ها با مدیریت و ارائه امنیت مداوم برای این محیط های مختلف، دست و پنجه نرم می کنند. (مشارموحد و شایگان، ۱۳۹۲: ۸۶). همین امر باعث می شود امکان گزارش های مداوم از وضعیت امنیت عملا غیر ممکن گردد. سازمان هایی که دارای ساختار امنیتی غیریکپارچه در محیط های ترکیبی ابری خود هستند، در حقیقت قادر به حل مشکلات نیستند. درست است که ابزارهای امنیتی ارائه شده توسط محیط های ابری، وظیفه خود را به درستی انجام داده و در حد نیاز، مفید هستند؛ اما می بایست موسسات، روشی داشته باشند تا همه سیستم های فضاهای ابری را با زیرساخت فیزیکی تجمیع کرده و در نهایت امکان مدیریت بر همه آن ها را از یک کنسول واحد فراهم کند. (Smith,1997:6) .

ابزارهای Adaptive Cloud Security فورتی نت که بخشی از سیستم یکپارچه امنیت آن است، اقدام به یکپارچه سازی زیرساخت های ترکیبی فضاهای ابری نموده و امکان مدیریت متمرکز برای کل زیرساخت فراهم می کند. این راهکارها به گونه ای طراحی شده اند که:

۱. به صورت بومی با تمام ارائه دهندگان خدمات فضای ابری عمومی یکپارچه شوند.
۲. حفاظتی گسترده ارائه دهند تا تمام سطح حملات را پوشش دهند.
۳. قابلیت های مدیریتی و اتوماسیون ارائه دهند و در مقابل حملات، رویکرد proactive از خود نشان دهند.
۴. گزارش های انطباق را به صورت خودکار انجام دهند. (رحیم زاده ترک و حاتمی، ۱۳۹۷: ۴۶).

نتیجه‌گیری

در مجموع، یافته های تحقیق حاضر نشان داد که امنیت سایبری در بیمارستان ها از سطح امنیتی پایینی برخوردار می باشد. ضعف این سیستم ها در حوزه استانداردهای مدیریتی و فیزیکی تأیید کننده این مطلب است که برای تأمین امنیت سایبری علاوه بر تأکید بر جنبه های فنی و زیرساخت فن آوری اطلاعات، ضروری است امنیت اطلاعات پزشکی نیز مدنظر قرار گیرد. نتایج به دست آمده از مطالعه حاضر با آشکار ساختن نقاط ضعف امنیت سایبری، بستر مناسبی را برای مدیران بخش های مدیریت اطلاعات سلامت و فناوری اطلاعات بیمارستان ها فراهم می آورد تا در زمینه تدوین خط مشی ها، آموزش کاربران، کنترل دسترسی، مدیریت خطر و سایر ابعاد استانداردهای مدیریتی و فیزیکی، اقدامات اصلاحی مناسبی را اجرا نمایند. بنابراین، به نظر می رسد در جهت افزایش ضریب امنیت اطلاعات الکترونیکی سلامت در مراکز بهداشت و درمان ایجاد سیاست ها و رویه های امنیتی مناسب برای استفاده از تجهیزات بیمارستانی، برگزاری دوره های آگاه سازی برای کارکنان در مورد رفتار های امن در استفاده از تجهیزات، ترویج و توسعه برنامه های آموزشی دقیق در زمینه امنیت سایبری در راستای تعلیم نیروی انسانی کارآمد، اجرای تدابیر فنی امنیتی مانند رمزنگاری و نصب فایروال و آنتی ویروس و مانتورینگ فعالیت های شبکه و سیستم ها ضروری باشد. علاوه بر این لازم است وزارت بهداشت به سرمایه گذاری بر راه حل های فنی و ایجاد زیرساخت مناسب برای بهبود امنیت اطلاعات سلامت توجه ویژه نماید. همچنین، با توجه به اینکه تحقق امنیت، یکی از نگرانی های عمده محسوب می شود، ضروری است تا با تقویت استانداردهای سه حوزه امنیت مدیریتی، فیزیکی و فنی، زمینه لازم برای توسعه استفاده این ابزار در سطح وسیع فراهم گردد.

منابع

۱.یریناتو، اسکات و همکاران (۱۳۹۱)، امنیت سایبری، ترجمه فاطمه کشت ورز، تهران: بی نا.
۲.بگل، مسلم و همکاران (۱۳۹۳)، تجهیزات عمومی بیمارستانی و کلینیک های پزشکی، تهران: انتشارات دوستدار.
۳.تیومیم، دیوید (۱۳۹۹)، امنیت اطلاعات در شبکه های صنعتی، ترجمه فریبا یاراحمدی و علیرضا صالحی، تهران: نشر سایبان.
۴.رحیم زاده ترک، بهزاد، حاتمی، بابک (۱۳۹۷)، امنیت در داده های پزشکی، تهران: پژوهشگران برتر.
۵.کرمی، محسن (۱۳۹۶)، امنیت اطلاعات: از ابتدا تا امروز، نسخه الکترونیک.
۶.گروه ترجمه انتشارات آتی نگر، امنیت فضای سایبری، تهران: سازمان فناوری اطلاعات ایران.
۷.گیورا، آموس (۱۳۹۹)، امنیت سایبری، تهران: انتشارات نسل روشن.
۸.مشارموحد، قاسم، شایگان، محمدرضا (۱۳۹۲)، معرفی و اصول اجرای سیستم های اطلاعات بهداشتی و بیمارستانی، تهران: سخن گستر.
۹.موسوی، سیدعلی (۱۴۰۰)، امنیت سایبری، تهران: انتشارات نسل روشن.
۱۰.یول یوم، هیونگ، پایک، ایوسون (۱۳۹۴)، امنیت فضای سایبری، ترجمه گروه ترجمه انتشارات آتی نگر، تهران: تسهیم دانش.
۱۱. براتی پور، مهدی (۱۳۸۶)، راهکارهای کلان امنیت در تجارت الکترونیک، چهارمین همایش ملی تجارت الکترونیک، تهران.
۱۲. گلناری, آسی و محمدنبی رضایی (۱۳۹۱) بررس طرح های تصدیق برای سیستم های اطلاعات پزشکی از راه دور، اولین همایش ملی فناوری اطلاعات و شبکه های کامپیوتری دانشگاه پیام نور، طبس، دانشگاه پیام نور طبس.
۱۳. پورفیضی، سمانه و عراقی زاده، محمد امین (۱۴۰۱)، بررسی امنیت در سیستم های سایبر فیزیکی، کنفرانس دانشجویان مهندسی

کامپیوتر، فناوری اطلاعات و ارتباطات، تهران.
۱۴. مهدی زاده گوهری، منصوره و ناصراسدی، علی (۱۳۹۴)، امضاهای دیجیتال و کاربرد آن ها در پزشکی، چهارمین همایش پژوهش های نوین در علوم و فناوری، کرمان.
15.Kobayashi, L. O. M., Furuie, S. S., & Barreto, P. S. L. M. (2009). Providing integrity and authenticity DICOM images: a novel approach. IEEE Transactions on Information Technology in Biomedicine in
16.Kesh, framework for analyzing e-commerce security, Information Management & Computer Security. Vol.10, Iss.4, 2002.
17.Faddis, A. The digital transformation of healthcare technology management. Biomed. Instrum. Technol. 2018.
18.World Health Organisation (WHO) on Primary Health Care. Available online:.https://www.who.int/docs/default-source/primary-health-care-conference/digital-technologies.pdf (accessed on 16 July 2021).
19.Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol. Health Care* 2017
20. Susanto12, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS.

Cyber Security of Hospital Equipment

Jamal Beigi
Associate Professor, Department of Criminal Law & Criminology, Law Research Center, Maragheh Branch, Islamic Azad University, Maragheh, Iran (Corresponding Author)
jamalbeigi@iau-maragheh.ac.ir

Zahra Eghbali
Master Student of Criminal Law & Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran
Zahra.eghbali7@yahoo.com

Abstract

Smart technologies provide many benefits in the medical industry. However, along with these benefits, challenges in cybersecurity have also emerged. Such devices allow doctors to quickly and continuously monitor patients and their medical conditions. Additionally, smart technologies provide more accurate analysis and earlier detection of medical issues. Given the increasing demand for medical image storage and transmission systems, it is important to identify and select software that has passed through security filters.This research was conducted using a descriptive-analytical approach with the aim of explaining the cybersecurity of hospital equipment. The findings indicate that with the implementation of appropriate strategies for managing cybersecurity threats and identifying and evaluating risk resources, cybersecurity in hospital equipment can be significantly improved and the devices can be protected against hacking. The only platform that has passed all security stages and tests in Iran and has also been certified by the IT organization is Metric.

Keywords: Cyber Security, Cyber Space, Hacker Attack, Hospital Equipment