بررسی، توضیح و طراحی سیستم امنیتی در سامانه های تله مدیسین

مهندس سعید سعیدی نژاد
دانشجوی کارشناسی ارشد رشته مدیریت فناوری اطلاعات پزشکی – دانشگاه امیر کبیر
saeedis@aut.ac.ir

دکتر حمید کشوری
عضو هیات علمی دانشکده مهندسی پزشکی – دانشگاه امیر کبیر

دکتر مهرداد ایمان زاده
پزشک و مدرس دانشکده مهندسی پزشکی- دانشگاه امیر کبیر

مهندس مهدی شرف خواه
دانشجوی کارشناسی ارشد رشته مدیریت فناوری اطلاعات پزشکی –دانشگاه امیر کبیر
sharafkha@sums.ac.ir

چکیده

تفکر امنیت در سیستم تله مدیسین مانند تمام شبکه های مبتنی بر ICT دیگر برای دستیابی به سه عامل مهم طراحی میگردد که این سه عامل با یکدیگر مثلث امنیتی این سیستم ها را تشکیل می دهند. این عوامل عبارتند از: راز داری و امانت داری (Confidentiality)، یکپارچگی (Integrity) و در نهایت در دسترس بودن همیشگی (Availability) . این سه عامل (CIA) اصول اساسی امنیت اطلاعات در سیستم های تله مدیسین را تشکیل می دهند بگونه ای که تمامی تمهیدات لازمی که برای امنیت این سیستم ها اتخاذ میشود و یا تجهیزاتی که به این منظور ساخته می شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط های نگهداری و تبادل اطلاعات میباشد. البته نباید فراموش کرد که سیستمهای تله مدیسین بدلیل ارائه خدمات در حوزه سلامت ملزم به رعایت حساسیتهای ویژه ای در رابطه با امنیت سیستمها هستند که این امر پیچیدگی واهمیت مسئله را دوچندان مینماید در این مقاله تلاش گردیده از طریق جستجوی علمی کلمات کلیدی در پایگاه داده های معتبر و بر مبنای یک مرور ساختار یافته به بررسی ماهیت خاص و اهمیت این سه جنبه امنیتی در سیستمهای تله مدیسین پرداخته و در نهایت به الگو و ساختاری موثر و منسجم در خصوص تامین امنیت سیستمهای تله مدیسین دست پیدا کنیم .

واژه‌های کلیدی: Telemedicine،Availability ،Integrity ،Confidentiality

مقدمه

بطور کلی منظور از تله مدیسین استفاده از فناوری ارتباطات و اطلاعات در پزشکی است با این هدف که بتوان خدمات پزشکی را ازراه دور و بدون نیاز به ارتباط معمول و رودرروی بیمار و پزشک ار ائه کرد کـه ایـن امـر مسـتلزم انتقـال مـتن، تصـویر، صـوت، ویـدئو و یاسیگنال های تبدیل شده الکتریکی است.

بنابراین با دقت و ریشه یابی تعاریف فوق درمیابیم که تله مدیسین نیز یکی از کاربردهای فناوری اطلاعات و ارتباطات میباشد و ماننـد آموزش الکترونیک ، بانکداری الکترونیک ، تجارت الکترونیک و ... بـا شبکه و سیستم های کامپیوتری آمیختـه شـده اسـت. بنـابراین امنیت سیستم تله مدیسین تا حد بسیار زیادی به امنیت زیر ساختهای تکنولوژیک آن یعنی امنیت سخت افـزار هـا و نـرم افـزار هـا و شبکه های ارتباطی وابسته است .

.

مقاله

تدوین سیاست امنیتی به عنوان اولین مرحله ایمن سازی یک سیستم تله مدیسین

باید توجه داشته باشید که امنیت سیستم های تله مدیسین یک تکنولوژی یا یک ابزار نیست که شما با خریداری آن مطمئن باشید که امنیت سیستم خود را فراهم کرده اید .

امنیت سیستم های تله مدیسین خود یک سیستم است که شامل مجموعه ای از قوانین ، استانداردها ، رفتار ها و ابزارها است اولین مرحله در ایجاد یک سیستم امنیتی ایجاد سیاست امنیتی متناسب با سازمان های ارائه دهنده خدمات میباشد سیاست امنیتی مناسب جهت سیستم های تله مدیسین ، اعلامیه ای رسمی مشتمل بر مجموعه ای از قوانین است که می بایست توسط دست اندرکاران سیستم های دورا پزشکی رعایت شود . بمنظور تحقق اهداف امنیتی می بایست سیاست های تدوین شده در رابطه با تمامی افراد دست اندرکار از جمله بیماران ، پزشکان معرفی کننده بیمار ، متخصصین ، مدیران شبکه و مدیران عملیاتی سازمان ، اعمال گردد . برای تدوین یک سیاست امنیتی مناسب معمولا به موارد زیر باید توجه نمود.

۱- خدمات سلامت عرضه شده در مقابل امنیت ارائه شده
۲- استفاده ساده در مقابل امنیت
۳- هزینه ایمن سازی در مقابل ریسک از دست دادن اطلاعات

مهمترین هدف یک سیاست امنیتی ، دادن آگاهی لازم به کاربران، مدیران شبکه و مدیران عملیاتی یک سازمان در رابطه با امکانات و تجهیزات لازم ، بمنظور حفظ و صیانت از تکنولوژی و سرمایه های اطلاعاتی است . سیاست امنیتی ، می بایست مکانیزم و راهکارهای مربوطه را با تاکید بر امکانات موجود تبین نماید . از دیگر اهداف یک سیاست امنیتی ، ارائه یک خط اصولی برای پیکربندی و ممیزی سیستم های کامپیوتری و شبکه های دورا پزشکی ، بمنظور تبعیت از سیاست های امنیتی تودین شده است. یک سیاست امنیتی مناسب و موثر ، می بایست رضایت و حمایت تمام پرسنل موجود در هر دو سایت TCC و TSC را بدنبال داشته باشد در غیر اینصورت این سیاست امنیتی به شکست میانجامد.

ویژگی های یک سیاست امنیتی خوب

ـ امکان پیاده سازی عملی آن به کمک روش های متعددی نظیر رویه های مدیریتی، وجود داشته باشد
ـ امکان تقویت آن توسط ابزارهای امنیتی ویا دستورات مدیریتی در مواردیکه پیشگیری واقعی از لحاظ فنی امکان پذیر نیست ، وجود داشته باشد .
ـ محدوده مسئولیت کاربران ، مدیران شبکه و مدیران عملیاتی بصورت شفاف مشخص گردد .

ـ پس از استقرار، قابلیت برقرای ارتباط با منابع متفاوت انسانی را دارا باشد . (قابل فهم برای تمامی کاربران)
ـ دارای انعطاف لازم بمنظور برخورد با تغییرات درشبکه باشد . یعنی در صورتی که نیاز به تغییرات در شبکه وجود داشته باشد نیازی به تغییر سیاست امنیتی نباشد.
حال که با تدوین سیاست امنیتی آشنا شدیم به بررسی قسمتهای مختلف یک سیستم تله مدیسین و چگونگی تامین امنیت آنها میپردازیم

قسمتهای مختلف یک سیستم تله مدیسین:

در این بخش ما تحت یک تقسیم بندی کلی تکنولوژی های بکار رفته در سیستمهای Telemedicine را دسته بندی کرده سپس در هر دسته بندی به اجزای آن گروه از فن آوری ها اشاره خواهیم کرد.
بطورکلی تکنولوژی های بکار رفته در سیستمهای دورا پزشکی شامل سرفصلهای زیر میباشد.

۱- نرم افزارهای سیستم دوراپزشکی
۲- سخت افزارهای سیستم دوراپزشکی

در ادامه بدلیل گستردگی مطلب و تخصصی بودن مباحث ، به صورت اجمالی امنیت بخشهای تشکیل دهنده یک سیستم تله مدیسین را بررسی خواهیم کرد.

نرم افزار های یک سیستم تله مدیسین و تامین امنیت آنها:

نرم افزار های تشکیل دهنده یک سیستم تله مدیسین عبارتند از :

۱- سیستم عامل
۲- نرم افزار های رابط کاربر جهت ارائه خدمات پزشکی از راه دور
۳- پایگاه داده به عنوان محل نگهداری اطلاعات بیماران

برای تامین امنیت سیستم های دوراپزشکی از لحاظ نرم افزاری باید به موارد زیر توجه کرد:

- **نسخه ها و بهنگام سازی سیستم عامل و نرم افزار های مورد استفاده در سیستم دوراپزشکی**

در صورت امکان، می بایست از آخرین نسخه سیستم های عامل و برنامه های کاربردی بر روی تمامی کامپیوترهای موجود در سیستم های تله مدیسین (سرویس گیرنده ، سرویس دهنده ، سوئیچ ، روتر، فایروال و سیستم های تشخیص مزاحمین) استفاده شود . سیستم های عامل و برنامه های کاربردی می بایست بهنگام بوده و همواره از آخرین امکانات موجود بهنگام سازی , patches) service pack , hotfixes)استفاده گردد . در این راستا می بایست حساسیت بیشتری نسبت به برنامه های آسیب پذیر که زمینه لازم برای متجاوزان اطلاعاتی را فراهم می نمایند ، وجود داشته باشد . برنامه هایی مانند IIS , Internet Explorer , BIND که اغلب به عنوان بستر اجرای نرم افزار های تله مدیسین و یا ارائه مستقیم خدمات پزشکی از راه دور مورد استفاده قرار میگیرند بدلیل وجود نقاط آسیب پذیر می بایست مورد توجه جدی قرار گیرند . متجاوزان اطلاعاتی ، بدفعات از نقاط آسیب پذیر برنامه های فوق برای خواسته های خود استفاده کرده اند . و در صورت عدم رعایت مسائل امنیتی وعدم بهنگام سازی بموقع در برنامه های یاد شده ممکن است به آسانی امکان دسترسی غیر مجاز به اطلاعات بیماران برای نفوذگران ایجاد گردد

- **انتخاب رمز عبور مناسب برای سیستم ها و نرم افزار های دورا پزشکی :**

انتخاب رمزعبور ضعیف ، همواره یکی از مسائل اصلی در رابطه با هر نوع سیستم امنیتی است . کاربران، می بایست متعهد و مجبور به تغییر رمز عبور خود بصورت ادواری گردند . تنظیم مشخصه های رمز عبور در سیستم های مبتنی بر ویندوز، بکمک Account Policyصورت می پذیرد . مدیران شبکه، می بایست برنامه های مربوط به تشخیص رمز عبور را تهیه و آنها را اجراء تا آسیب پذیری سیستم در بوته نقد و آزمایش قرار گیرد . برنامه های john the Ripper و Crack نمونه هائی در این زمینه می باشند و به

کاربرانی که رمز عبور آنان ضعیف تعریف شده است ، مراتب اعلام و در صورت تکرار اخطار داده شود (عملیات فوق، می بایست بصورت متناوب انجام گیرد) . با توجه به اینکه برنامه های تشخیص رمزعبور ، زمان زیادی از پردازنده را بخود اختصاص خواهند داد، توصیه می گردد، رمز عبورهای کد شده (لیست SAM بانک اطلاعاتی در ویندوز) را بر روی سیستمی دیگر که در شبکه نمی باشد، منتقل تا زمینه بررسی رمزهای عبور ضعیف ، فراهم گردد.

عدم اجرای برنامه های با منبع نا مشخص بر روی سیستم های دوراپزشکی

در اغلب حالات ، برنامه های کامپیوتری در یک چارچوب امنیتی خاص مربوط به کاربری که آنها را فعال می نماید ، اجراء می گردند. گاهی ممکن است، هیچگونه توجه ای به ماهیت منبع ارائه دهنده برنامه توسط کاربران انجام نگردد وجود یک زیر ساخت)PKI (Public key infrastructure، در هنگام تهیه نرم افزار های تله مدیسین میتواند در تامین امنیت سیستم های درگیر با تله مدیسین مفید باشد. در صورت عدم وجود زیرساخت امنیتی فوق ، می بایست مراقبت های لازم در رابطه با ترفندهای استفاده شده توسط برخی از متجاوران اطلاعاتی را انجام داد. برای این منظور باید با اطلاع رسانی یا کاهش سطح دسترسی و یا اعمال سیاستهای خاص اجازه اجرای برنامه با منبع نامشخص بر روی سیستم های ارائه دهنده خدمات تله مدیسین را از بین برد.

پایبندی به مفهوم کمترین امتیاز در دسترسی به سیستم هاو منابع تله مدیسین

اختصاص حداقل امتیاز به کاربران سیستم های تله مدیسین ، محور اساسی درپیاده سازی امنیت این سیستم ها است رویکرد فوق بر این اصل مهم استوار است که کاربران می بایست صرفا" دارای حقوق و امتیازات لازم بمنظور انجام کارهای مربوطه باشند (بذل و بخشش امتیازات در این زمینه شایسته نمی باشد!) . رخنه در سیستم امنیتی از طریق کدهای مخربی که توسط کاربران اجراء می گردند، تحقق می یابد . در صورتیکه کاربر، دارای حقوق و امتیازات بیشتری باشد ، آسیب پذیری اطلاعات در اثر اجرای کدهای مخرب ، بیشتر خواهد شد.

ممیزی برنامه های تله مدیسین

برنامه های سرویس دهنده خدمات دوراپزشکی باید به گونه ای طراحی شود که دارای قابلیت های ممیزی باشند . ممیزی می تواند شامل دنبال نمودن حرکات مشکوک و یا برخورد با آسیب های واقعی باشد . با فعال نمودن ممیزی برای برنامه های سرویس دهنده وکنترل دستیابی به برنامه های کلیدی که معمولا در ارتباطات شبکه ای ازآنها استفاده میشود شرایط مناسبی بمنظور حفاظت از اطلاعات فراهم می گردد.

عدم اجرای پروتکل ها و سرویس های غیر ضروری بر روی سیستم عامل تجهیزات عضو سیستم تله مدیسین.

سخت افزار های یک سیستم تله مدیسین و تامین امنیت آنها:

سخت افزار های یک سیتم تله مدیسین:

۱- سیستم های سخت افزاری (پرینتر ، کامپیوتر و...)

۲- شبکه و تجهیزات آن

۳- تجهیزات پزشکی

امنیت کامپیوتر و تجهیزات سخت افزاری سیستم تله مدیسین:

- **سرویسهای غیر لازم مانند به اشتراک گذاری فایل و چاپگر را غیر فعال کنید .**

بیشتر سیستم عاملها بطور پیش فرض این سرویسها را فعال نمی‌کنند. اما اگر در حال به روز کردن و ارتقای سیستم عامل کامپیوتر خود هستید و این سرویسها در این کامپیوتر فعال هستند، ممکن است سیستم عامل جدید نیز این سرویسها را فعال نماید. از آنجایی که ممکن است سیستم عامل جدید آسیب پذیریهای جدیدی نیز داشته باشد، بهتر است که قبل از ارتقای سیستم عامل خود، سرویسهای به اشتراک گذاری فایلها و چاپگر را غیر فعال کنید و پس از نصب اصلاحیه های لازم آن را مجددا فعال نمایید.

- نرم افزار آنتی ویروس مناسب را بر روی تمامی کامپیوتر های سیستم دوراپزشکی نصب و مرتبا آنها را بروز رسانی نمایید.
- به منظور حفظ اصل Availability به عنوان یکی از اصول امنیت سیستم های تله مدیسین، برای تجهیزات حیاتی حتما UPS در نظر بگیرید تا در زمان قطعی برق خدمات رسانی با مشکل مواجه نشود.
- در صورت امکان جهت پشتیبانی و سرویس دوره ای تجهیزات سخت افزاری نسبت به استخدام متخصص سخت افزار و یا عقد قرارداد با یک شرکت خصوصی اقدام نمایید . این امر نه تنها باعث افزایش طول عمر تجهیزات میشود بلکه با زمان برطرف کردن مشکلات احتمالی به حداقل ممکن میرسد
- از تجهیزات سخت افزاری که در خدمات رسانی دوراپزشکی نقش حیاتی دارند حتما Backup تهیه کنید این امر باعث میشود در صورت بروز مشکل تا تعمیر تجهیزات معیوب بتوان از تجهیزات Backup مربوطه استفاده نمود و Availability سیستم را به حداکثر مقدار ممکن میرساند.

توجه ویژه ای به ارتباط با مدیران سیستم‌ها داشته باشید

- کاربران سیستمهای و تجهیزات تله مدیسین افرادی هستند که اغلب، در مورد امنیت کاربردی برای گروهی از سیستم‌ها مسئول هستند.

کاربران سیستم‌ها را درگیر کنید

- کاربران سیستم‌های بخش‌های مختلف تله مدیسین را برای مشاوره در مورد پروسه مدیریت رخدادهای امنیتی دعوت کنید.

آموزش پیش‌گیرانه را هدایت کنید

- کارگاه هایی را برای کاربران سیستم‌ها در مورد بسته های نرم افزاری موجود برای تشخیص حملات و نظارت موثر بر سیستم‌ها فراهم کنید.

پشتیبان گیری منظم از سیستم را ترویج کنید

- نسخه های پشتیبان ناکافی علت بسیاری از فاجعه ها در بازیابی سیستم‌ها پس از رخدادهای امنیتی هستند

آشنایی متخصصین امنیت سیستم تله مدیسین با پیکربندی‌های سرور و سیستم عامل‌ها:

- متخصصان شبکه و امنیت اطلاعات سیستم تله مدیسین باید با پروسه های متعارف سیستم عامل آشنا باشند.

تست نفوذ انجام دهید

یکی از بهترین راه‌ها برای جلوگیری از رخدادها این است که اطمینان حاصل کنید که سیستم‌های شما آسیب پذیر نیستند.

اشتباهات ساده را چک کنید

مثال‌هایی از اشتباهات کوچک شامل خطاهایی در پیکربندی سیستم یا یک برنامه، خطاهای سخت افزاری و خطاهای کاربر یا مدیر سیستم می‌باشد

شواهد را با جزئیات تعیین کنید

از فهرست نشانه هایی که در طول مرحله آمادگی ایجاد کرده اید استفاده کنید و به سرعت نوع احتمالی رخداد را مشخص نمایید.

از سیستم نسخه پشتیبان تهیه کنید

مجرمان رایانه ای روز به روز در انجام فعالیت‌های غیر قانونی و جلوگیری از شناسایی و تعقیب شدن خبره تر می‌شوند. بنابراین بسیار مهم است که یک نسخه پشتیبان کامل ترجیحا با استفاده از تصویر دیسک سیستم تهیه کنید.

نتیجه‌گیری

در پایان پس از بررسی عوامل امنیتی در راه اندازی سیستم تله مدیسین لازم به ذکر است بیان شود که تمامی نکات از سخت افزار ،نرم افزار و کلیه ارتباطات پرسنل درگیر در طرح بایستی استانداردهای امنیتی لازم برایشان تعریف گردد تا بتوان سیستمی امن و مطمئن راه اندازی نمود.

مراجع

١. R. L. Bashshur , T. G. Reardon and G. W. Shannon "Telemedicine: a New Health Care Delivery System", *Ann. Rev. Public Health*, vol. ٢١, pp.٦١٣ -٦١٧ ٢٠٠٠ [CrossRef]

٢. R. S. H. Istepanian , E. Jovanov and Y. T. Zhang "Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity", *IEEE Trans. Info. Tech. Biomed.*, vol. ٨, no. ٤, pp.٤٠٥ -٤١٤ ٢٠٠٤ Abstract | Full Text: PDF (٩٥٦KB)

۳. Network and data security design for telemedicine applications
۱۹۹۷, Vol. ۲۲, No. ۲ , Pages ۱۳۳-۱٤۲

٤. "ISO/TR ۱٦۰٥٦-۱", Health Informatics: Interoperability of Telehealth Systems and Networks

٥.A.Mitra, V.Subba Rao, S.R.M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques", International Journal of Computer Science, Vol.۱ Number ۲, ISSN ۱۳۰٦-٤٤۲۸, ۲۰۰٦

٦.Claude E Shannon, Communication Theory of Secrecy Systems, BellSystem Technieal Journal, pp, ٦٥٦-۷۱٥, ۱۹٤۹