نگاهی تحلیلی به خطرات پنج گانه امنیت سایبری در نظام سلامت...

در بسیاری از سازمان‌ها، به‌ویژه سازمان‌های کوچک ...

در دنیای فناوری اطلاعات، بحران‌ها غیرقابل اجتناب هستند ...

ویکی واژه
WIKIWORD

در عصری که تهدیدات دیجیتال روز به روز پیچیده تر می شود ...

ماهنامه

پالسی نو

سال اول – شماره اول – مرداد ۱۴۰۴

A New Pulse

First year - August 2025 No:01

ویژه نامه امنیت اطلاعات

بخش قابل توجهی از تصاویر این نشریه، با بهره گیری از ابزارهای هوش مصنوعی تولید شده‌اند.

فهرست مطالب

آغازین سخن

دکتر طاها صمدسلطانی
دانشیار انفورماتیک پزشکی
مدیرآمار، فناوری اطلاعات و امنیت فضای مجازی دانشگاه

تحول دیجیتال در سازمان، ضرورتی اجتناب ناپذیر برای پیشرفت ایران در عصر فناوری اطلاعات

در عصر حاضر، فناوری اطلاعات (IT) به عنوان موتور محرکه پیشرفت جوامع شناخته میشود. این فناوری نه تنها ابزاری برای تسهیل امور است، بلکه زیرساخت اساسی برای مدیریت دانش، ارتقای سواد دیجیتال و تحول در شیوه های حکمرانی محسوب میشود. در این میان، وطن عزیزمان ایران با وجود پتانسیلهای فراوان، به دلیل موانع ساختاری و برنامه ریزی نادرست، در مسیر تحول دیجیتال با چالشهای جدی مواجه بوده و گره گشایی از این مشکلات نیازمند عزمی راسخ در تغییر دانش، نگرش و رفتارها در برابر این موج بیدار و زنده می باشد.

پیاده سازی حکمرانی داده مبنا و امکان ترجمان دانش و تبدیل کلان داده ها به دانش و خرد جهت اتخاذ تصمیمات راهبردی و دقیق، تسهیل دسترسی عادلانه و شفاف به اطلاعات برای تمام اقشار جامعه و ایجاد بسترهای نوین ارتباطی و آموزش الکترونیک از نقش های اصلی تحول دیجیتال در توسعه ملی می باشد. علاوه بر این در زمینه ارتقای خدمات عمومی با دولت الکترونیک، می توان تحول در نظام های مردم محور همچون سلامت را ایجاد نمود که شفافیت و سرعت را به ارمغان خواهد آورد.

در این مسیر چالش های مهمی وطنمان ایران را احاطه نموده است. موانع ساختاری که فقدان یک سند ملی در زمینه تحول دیجیتال را نشان می دهند. این سند برای حفظ و حراست از سرمایه های انسانی و علمی فناوری اطلاعات، پیشگیری از پراکندگی و ناهماهنگی در پروژه های دستگاه های اجرایی و تقویت زیرساخت های ارتباطی به ویژه در شرایط بحرانی لازم به نظر می رسد. تحریم های ناجوانمردانه در زمینه تحقیقات و فناوری نیز مزید بر علت شده اند تا زیرساخت های فناوری اطلاعات کشور متناسب با حرکت شتابان جهانی نبوده و عقب ماندگی ها بصورت روز افزون بیشتر شود.

از طرفی چالش های نگرشی وفرهنگی نیز اهمیت این حوزه را کمرنگ نموده است. مقاومت در برابر تغییر در بدنه مدیریتی کشور، سواد دیجیتال پایین در میان عموم مردم و کارکنان دولتی و نبود نظام آموزشی همسو با نیازهای عصر دیجیتال، جامعه را در سطح کاربر عادی فناوری نگه داشته و مانع از رشد فزاینده این زیست بوم شده است و علیرغم محدودیت های فنی و انسانی، بهره گیری از ظرفیت موجود را بصورت موثر و کارآمد سلب نموده است. لذا طبق تاکید منابع مدیریت فناوری اطلاعات، آموزش و فرهنگسازی کلید پیشرفت دیجیتال می باشد و راهبردهای کلان در نظام حاکمیتی بدون همراهی مردم و نگرش صحیح و مبتنی بر شواهد ایشان پیش نخواهد رفت.

ما در مدیریت آمار، فناوری اطلاعات و امنیت فضای مجازی، هرچند با دغدغه هایی روزمره و فراوان، اما ملتزم و متعهد به گام های توسعه ای می باشیم و به آموزش و ترجمان دانش به عنوان یکی از پیشرانه های حرکت در شاهراه تحول دیجیتال باور داریم. برای نیل به این هدف نشریه پالسی نو که بصورت دیجیتال منتشر می شود را به عنوان راهکاری موثر در ارتقای جایگاه دانشگاه و نظام سلامت استان می دانیم.

پالسی نو با هدف تقویت دانش تخصصی و سواد دیجیتال، بهبود کیفیت خدمات از طریق تصمیم‌گیری مبتنی بر داده و داده کاوی، تسهیل تحول دیجیتال سازمانی، افزایش تعامل و شبکه‌سازی تخصصی، توسعه مهارت‌های حرفه‌ای، ارتقای امنیت سایبری، کاهش هزینه‌های عملیاتی و کاهش مقاومت در برابر تغییرات مثبت در صف انتشار می باشد. قصد داریم با مشارکت هم از طریق معرفی بهترین تجربیات جهانی و ابزارهای افزایش بهره‌وری، سازمان را در مسیر تبدیل شدن به یک مرکز پیشرو در سلامت دیجیتال در کشور قرار دهیم. این سرمایه‌گذاری علمی نه تنها موجب توانمندسازی نیروی انسانی می‌شود، بلکه با کاهش هزینه‌های آموزشی و افزایش بازدهی سرمایه‌گذاری‌های فناورانه، نقش کاتالیزور تحول سازمانی را ایفا می‌کند.

سرمقاله

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

در مسیر رشد و تحول دانشگاه‌های علوم پزشکی، فناوری اطلاعات دیگر صرفاً ابزاری برای ارائه خدمات نیست.

نخستین شماره نشریه "پالسی نو" را با محوریت "امنیت سایبری در سازمان" تقدیم حضوراندیشمندان، متخصصان و دغدغه‌مندان حوزه آموزش، سلامت، بهداشت، درمان و فناوری می‌کنیم؛ آنان که با نگاه علمی و آینده‌نگر، مسیر پویای فناوری اطلاعات در نظام آموزش عالی و علوم پزشکی در سطح ملی و جهانی را نه‌فقط رصد، بلکه در آن نقش‌آفرینی کرده‌اند.

در مسیر رشد و تحول دانشگاه‌های علوم پزشکی، فناوری اطلاعات دیگر صرفاً ابزاری برای ارائه خدمات نیست؛

اگر به سال‌های گذشته بازگردیم، فناوری اطلاعات بیشتر به‌عنوان یک واحد پشتیبانی‌کننده شناخته می‌شد که مأمور اجرای امور فنی، راه‌اندازی شبکه‌ها، یا ارائه خدمات نرم‌افزاری بود. اما با گسترش زیرساخت‌ها، افزایش پیچیدگی سیستم‌ها، رشد داده‌های بالینی و توسعه آموزش‌های دیجیتال، این حوزه به یکی از ارکان اصلی حیات دانشگاه تبدیل شده است. در تمامی زمینه ها شامل آموزش و پژوهش و بهداشت و درمان، از مدیریت بیمارستان‌ها گرفته تا درمان بیماران، از پایش سلامت عمومی تا ارزیابی کیفیت مراقبت، این فناوری در لایه‌های مختلف سازمان تنیده شده است. به طور خلاصه می توان گفت، امروزه فناوری اطلاعات به ابزاری برای تصمیم‌سازی، تحلیل، سیاست‌گذاری و ارزیابی بدل شده است.

در چنین فضایی، نشریه «پالسی نو» با هدف بازتاب دقیق و همدلانه این تحولات و ایجاد محیط گفت و گو، اندیشه و شفاف سازی، آغاز به کار کرده است.

نه فقط برای بازتاب عملکرد، بلکه جهت ایجاد یک بستر علمی و تحلیلی تا اعضای دانشگاه بتوانند درباره فناوری حرف بزنند، به انتقال تجربه بپردازند و نقش خود را در ایجاد آینده ای مطلوب ایفا نمایند.

در حال حاضر ساختار فناوری اطلاعات دانشگاه علوم پزشکی تبریز، از چهار واحد تخصصی تشکیل شده که هریک نقش کلیدی در پشتیبانی و هدایت تحول دیجیتال ایفا می‌کنند:

۱. گروه زیرساخت فناوری اطلاعات- به عنوان ستون فقرات اتصال و ارتباطات پایدار دانشگاه.
۲. گروه امنیت اطلاعات - تامین کننده محرمانگی، یکپارچگی و اعتماد اطلاعات.
۳. گروه نرم‌افزار- پشتیبانی از نرم افزارها و سامانه های اطلاعاتی و مدیریت پورتال دانشگاه.
۴. گروه آمار و تحلیل داده‌ها - جمع آوری و ثبت داده ها جهت بکارگیری در تصمیم‌سازی کلان و خرد در دانشگاه

ما در این نشریه بر آنیم که پُل ارتباطی میان این چهار گروه با بدنه علمی، آموزشی، پژوهشی، بهداشتی، درمانی، مدیریتی و دانشجویی دانشگاه باشیم.

همچنین معتقدیم که تحول دیجیتال، زمانی اثربخش خواهد بود که با مشارکت تمامی اعضای دانشگاه همراه شود. هر فرد، در جایگاه خود، می‌تواند نقش ایفا کند: از شناسایی خلأهای موجود در سامانه‌های درمانی و آموزشی، تا ارائه راه‌حل‌هایی برای تصمیم‌گیری هوشمندتر و منطبق‌تر

معتقدیم که تحول دیجیتال، زمانی اثربخش خواهد بود که با مشارکت تمامی اعضای دانشگاه همراه باشد. هر فرد، در جایگاه خود، می‌تواند نقش ایفا کند: از شناسایی خلأهای موجود در سامانه‌های بهداشتی، درمانی و آموزشی و پژوهشی، تا ارائه راه‌حل‌هایی برای تصمیم‌گیری هوشمندتر و منطبق‌تر با واقعیت میدانی.

با واقعیت میدانی.
سیاست محتوایی نشریه بر چند محور کلیدی استوار است:

- تبیین نقش فناوری اطلاعات در تصمیم‌سازی‌های کلان و میدانی.
- پرداختن به کاربردهای آن در آموزش، پژوهش، بهداشت، درمان و سلامت عمومی.
- رصد تحولات نوظهور و انطباق آن‌ها با بسترهای بومی.
- تقویت نگاهی میان‌رشته‌ای، با پیوند میان علوم پزشکی، مدیریت، فناوری و انسان‌شناسی دیجیتال.
- دعوت به نوشتن، نقد کردن و مشارکت اندیشمندانه.
- و مهم‌تر از همه، دعوت به مشارکت فعال در شکل‌دهی آینده‌ای هوشمند، ایمن و پایدار.

امید داریم این نشریه، سکویی برای اندیشه‌ورزی، تجربه‌آموزی و طراحی آینده‌ای هوشمند، انسانی و ایمن باشد.

دل‌نوشت

برای خوانندگان پالسی نو

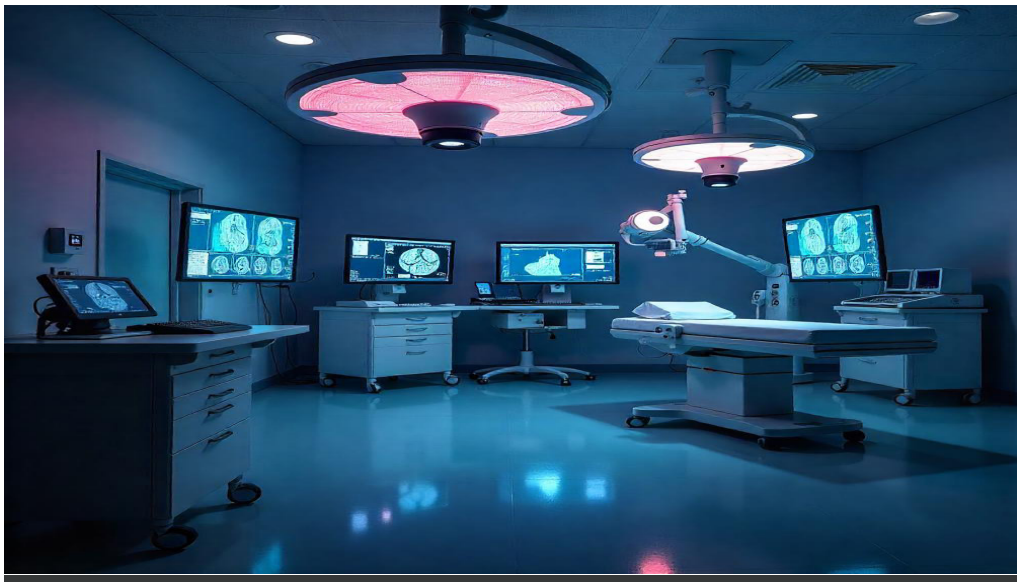
سید محمدحسن الهی

در بخشی از دانشگاه علوم پزشکی، جایی که **پالس** دانش و درمان به هم گره خورده، واحدی پر مشغله به نام فناوری اطلاعات نفس می‌کشد. این واحد، همانند قلبی پنهان در پسِ سازوکارهای سازمان، بی‌صدا می‌تپد و **پالس** دارد تا جریان اطلاعات را در رگ‌های دانشگاه جاری نگه دارد. اما این **پالس** ها، گاه در سایه بی‌توجهی‌ها و کاستی‌ها، با چالش‌هایی دست‌وپنجه نرم می‌کند که کمتر دیده می‌شود.

کارکنان فناوری اطلاعات، رزمندگان خاموش دنیای دیجیتال هستند اگر چه دیده نمی شوند، روز و شب در تلاش تا سامانه‌های پیچیده را سرپا نگاه دارند، شبکه‌ها را ایمن کنند و نرم‌افزارهایی را که ستون فقرات آموزش و پژوهش و درمان و بهداشت هستند، به‌روز نگاه دارند. آن‌ها با دقتی بی‌وقفه، خطاها را رهگیری می‌کنند، مشکلات را حل می‌کنند و گاه در لحظات بحرانی، چون پزشکی که جان بیماری را نجات می‌دهد، سیستم‌های ازکارافتاده را احیا می‌کنند. اما این تلاش‌ها، در میان هیاهوی روزمره سازمان، اغلب نادیده گرفته می‌شود.

جایگاه فناوری اطلاعات در دانشگاه، جایگاهی است شایسته تقدیر، اما کمتر قدر می‌بینند. این واحد، نه‌تنها پشتیبان فرآیندهای آموزشی و پژوهشی است، بلکه پلی است میان گذشته و آینده، میان سنت‌های دیرین و روش های قدیمی و نوآوری‌های دنیای مدرن. با این‌حال، کمبود منابع، فشارهای مداوم برای پاسخگویی سریع، و انتظارات فزاینده از سیستمی که گاه با ابزارهای محدود کار می‌کند، سایه‌ای سنگین بر دوش کارکنان این واحد انداخته است. در دنیایی از کد و داده، با چالش‌هایی بسیار خاص روبرو هستند: نبود بودجه کافی برای به‌روزرسانی زیرساخت‌ها، کمبود نیروی انسانی متخصص، و گاه، عدم درک عمیق از سوی دیگر بخش‌های سازمان درباره پیچیدگی‌های این حوزه!!! اما با این وجود کارکنان فناوری اطلاعات با عشقی خاموش به رسالت خود ادامه می‌دهند، چرا که می‌دانند هر کلیک، هر داده و هر سیستمی که روان کار می‌کند، گامی است به‌سوی پیشرفت دانشگاه و خدمت به این جامعه.

این متن، ادای احترامی است به این تلاشگران بی‌ادعا که در پشت صحنه، با دستان خالی اما ذهنی پر از ایده، چرخ‌های فناوری را در دانشگاه به حرکت درمی‌آورند. باشد که روزی جایگاه واقعی این قلب تپنده و **پالس** آن در سازمان شناخته شود و مشکلاتش، با همدلی و حمایت، به فرصتی برای رشد و شکوفایی بدل گردد.



امید داریم این نشریه، سکویی برای اندیشه‌ورزی، تجربه‌آموزی و طراحی آینده‌ای هوشمند، انسانی و ایمن باشد.

پیام نخستین ریاست محترم دانشگاه برای انتشار ماهنامه علمی – تحلیلی پالسی‌نو

در سالهای اخیر، شاهد بوده ایم که چگونه فناوری اطلاعات، چهره نظام سلامت را دگرگون ساخته است. از سامانه های پرونده الکترونیک سلامت تا هوش مصنوعی در تشخیص بیماریها، از شبیه سازها در آموزش پزشکی تا طراحی دارو و واکسن با محاسبات رایانه ای هر یک نشان دهنده ظرفیتهای بی نظیر فناوری اطلاعات در ارتقای کیفیت خدمات بهداشتی و درمانی هستند. ما با درک این ضرورت، همواره کوشیده ایم تا با ایجاد زیرساختهای مناسب، تربیت نیروی انسانی متخصص و حمایت از پژوهشهای میان رشته ای، سهمی اثرگذار در این تحول دیجیتال ایفا نماییم.

امروز در عصری زندگی می‌کنیم که فناوری اطلاعات نه تنها به عنوان یک ابزار، بلکه به عنوان یک پارادایم تحول‌آفرین در تمامی عرصه‌های علمی، آموزشی و خدماتی ایفای نقش می‌کند. نشریه علمی-تحلیلی پالسی‌نو که در مدیریت آمار، فناوری اطلاعات و امنیت فضای مجازی دانشگاه علوم پزشکی تبریز برای نشر آن برنامه ریزی شده، فرصتی است تا با نگاهی ژرف و تحلیلی، آخرین دستاوردها، چالش‌ها و افق‌های پیش‌رو در حوزه فناوری اطلاعات سلامت و سلامت دیجیتال را بررسی کنیم. این نشریه تنها مجموعه‌ای از مقالات نیست، بلکه آیینه‌ای از تلاش‌های جمعی همکاران محقق و با انگیزه ما هستند تا با ترجمان و انتقال دانش فناوری اطلاعات به کادر مدیریتی، درمانی و اجرایی نظام سلامت، زمینه را برای تحول دیجیتال با دانش و نگرشی صحیح ایجاد نمایند.

امیدوارم مطالب این نشریه انگیزه‌ای برای همگرایی بیشتر بین رشته‌های پزشکی و مهندسی فناوری اطلاعات باشد. به عنوان رئیس دانشگاه، از تمامی دست اندرکاران این نشریه صمیمانه تقدیر می‌کنم. همچنین از همه همکاران دانشگاه می‌خواهم که با مطالعه این نشریه، نه تنها مصرف کننده دانش، بلکه خالقان اندیشه‌های نو باشند. آینده علوم پزشکی در گرو توانمندی ما در ادغام دانش بالینی با فناوریهای پیشرفته است و این مسیر، بدون مشارکت فعال شما فرهیختگان ممکن نخواهد بود.

احمدرضا جودتی - رئیس دانشگاه

نگاهی تحلیلی به خطرات پنجگانه امنیت سایبری در نظام سلامت کشور

دکتر طاها صمدسلطانی
دانشیار انفورماتیک پزشکی
مدیرآمار، فناوری اطلاعات و امنیت فضای مجازی دانشگاه

بخش سلامت مجموعه‌ای حیاتی و پیچیده از محصولات، خدمات و سیستم‌هاست که به حفظ و ارتقای سلامت عمومی و مراقبت‌های پزشکی کمک می‌کند. این بخش سهم عمده‌ای در اقتصاد جهانی دارد، محرک نوآوری است و از نظر فوریت و تقاضا منحصربه‌فرد است. از زمان ظهور اینترنت، جای تعجب نیست که این بخش به هدف اصلی برای مجرمان سایبری و افرادی تبدیل شده که به دنبال دستکاری در داده ها و نهادهای سلامت هستند. تیم‌های متخصص امنیت سایبری در کشورهای پیشرو سال‌هاست که برای مقابله با این خطرات تلاش می‌کنند و یک رویکرد عملیاتی برای بخش سلامت دارند.

بر اساس بررسی ها و گزارش ها پنج نگرانی امنیت سایبری شناسایی شده است که امروزه برای سازمان‌های حوزه سلامت بسیار حیاتی هستند. این تهدیدها عبارتند از:

۱. حملات باج‌افزار (Ransomware)

۲. ریسک فروشندگان شخص ثالث (Third-party vendor risks)

۳. سیستم‌ها و فناوری‌های از رده خارج (Legacy systems and technology)

۴. نقض مقررات حریم خصوصی داده‌ها (data privacy regulations)

۵. فیشینگ و تهدیدات داخلی (Phishing and insider threats)

در این مقاله با رویکردی تحلیلی به این حملات و راهکارهای آن می پردازیم.

۱. حملات باج‌افزار (Ransomware)

موسسات بهداشتی به دلیل وابستگی به دسترسی سریع به داده‌های بیماران ، بسیار مستعد حملات باج‌افزار هستند. مجرمان سایبری از فوریت خدمات سلامت سوءاستفاده می‌کنند، زیرا می‌دانند اختلال در این خدمات می‌تواند عواقب جبران ناپذیری داشته باشد. این فشار باعث می‌شود ارائه‌دهندگان سلامت برای بازیابی داده ها و دسترسی سریع ، باج پرداخت کنند. پیامدهای حمله شامل از دست رفتن داده‌ها، توقف عملیات و فشار مالی شدید از جمله کسورات می باشد. با توجه به اینکه در مدیریت فناوری اطلاعات دانشگاه در محیطی پرشتاب فعالیت می کنیم، قطع سامانه ها می تواند مستقیما به بیماران آسیب برساند. از طرفی پیچیدگی فزاینده حملات باج‌افزاری نیاز به هوشیاری و تخصیص منابع دائمی دارد. تعادل این ریسک با محدودیت‌های بودجه چالش بزرگی است، زیرا باید همزمان سیستم‌های قدیمی و فناوری‌های جدید خریداری و تجهیز نماییم. بهره گیری از مراکز داده موازی اما ایزوله می تواند

راهکار دائمی این تهدید باشد.

۲. ریسک فروشندگان شخص ثالث (Third-party vendor risk)

صنعت سلامت اغلب به فروشندگان

متعدد شخص ثالث برای دستگاه‌های پزشکی، ذخیره‌سازی و راه‌حل‌های نرم‌افزاری وابسته است. این فروشندگان ممکن است سطح بلوغ امنیتی یکسانی نداشته باشند و آسیب‌پذیری‌های سیستم‌های آنها می‌تواند منجر به نفوذ و آسیب به سامانه های بهداشت و درمان شود. این خطر با گسترش وسعت زنجیره تأمین دیجیتال افزایش یافته است.

ما برای همه چیز از دستگاه‌های پزشکی تا خدمات میزبانی وب، به فروشندگان شخص ثالث وابسته‌ایم. رویکردهای امنیتی این فروشندگان مستقیماً بر ما تأثیر می‌گذارد، اما اغلب دید کاملی از مدیریت ریسک آنها نداریم. در این زمینه مرکز مدیریت راهبردی افتا در کشور نقش تعیین کننده ای ایفا می کند. صدور گواهی افتا برای محصولات نرم افزاری و سخت افزاری می تواند بار عملیاتی بسیاری را از دوش سازمان در زمینه انجام تست های امنیتی بردارد. البته چالش های مهمی نیز در این باب از جمله هزینه آزمایش ها و به صرفه نبودن آن و محصولات توسعه یافته درون سازمانی وجود دارد. لذا در بسیاری از سامانه ها اخذ این گواهی انجام نشده است و جایگزینی نیز برای آن وجود ندارد.

۳. سیستم‌های قدیمی و فناوری منسوخ (Legacy systems and outdated technology)

بسیاری از سازمان‌های سلامت به سیستم‌های قدیمی متکی هستند که به‌دلیل سخت‌افزار یا نرم‌افزارهای منسوخ، به‌سختی قابل اصلاح یا ایمن‌سازی هستند. این سیستم‌ها اغلب از پروتکل‌های امنیتی یا رمزنگاری مدرن پشتیبانی نمی‌کنند و هدف آسانی برای مهاجمان هستند. انتقال به سیستم‌های جدید معمولاً با چالش‌های مالی، انطباق و نیاز به عملیات مداوم پیچیده می‌شود. در نظام سلامت نیز علی رغم تاکید بر روزآمدسازی نرم افزاری توسط شرکت ها ، در برخی موارد به سامانه های قدیمی متکی هستیم و هزینه تغییر می تواند بسیار زیاد باشد اما چالش مهم تر مقاومت نیروی انسانی در برابر تغییر سامانه قدیمی و مهاجرت از آن می باشد.

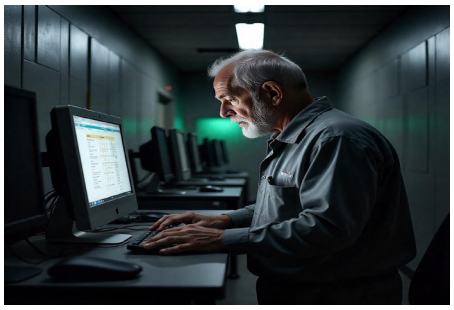
۴. نقض مقررات حریم خصوصی داده‌ها (data privacy regulations)

ارائه‌دهندگان خدمات سلامت باید چارچوب‌های نظارتی ابلاغی از سطوح بالاتر را پذیرفته و رعایت کنند. عدم رعایت این مقررات می‌تواند منجر به جریمه‌های سنگین و آسیب به اعتبارشان شود. در عین حال، تضمین انطباق با قوانین اغلب چالش‌های عملیاتی ایجاد می‌کند، زیرا سازمان‌ها باید بین حریم خصوصی و دسترسی به داده‌های حیاتی بیماران تعادل برقرار کنند. از طرفی ابلاغیه ها گاهی بصورت فراگیر برای تمام سازمان های کشوری ارسال می شود که از لحاظ حجم، وسعت، تعداد کاربران، تنوع و پیچیدگی فرآیندها بسیار با ارائه کنندگان خدمات بهداشتی(به ویژه دانشگاه های علوم پزشکی) تفاوت دارند. برای مثال در دستورالعمل جداسازی فیزیکی شبکه داخلی از اینترنت در سازمانی با ۳۰۰ کاربر به راحتی می توان دو رایانه به هر فرد تخصیص داد اما در تعداد کاربرانی به وسعت ۱۵۰۰۰ نفر چنین امکانی میسر نمی باشد و جداسازی منطقی شبکه ها از هم جایگزین شکل فیزیکی می شود.

۵. فیشینگ و تهدیدات داخلی (Phishing and insider threats)

یکی از تهدیدات مرسوم حملات فیشینگ می باشد. در این نوع حمله با ایجاد صفحات و فرم های جعلی اطلاعات کاربری، مالی و شخصی به سرقت می روند. در این زمینه کارکنان بخش سلامت، از جمله پرسنل بالینی و اداری، ممکن است آگاهی امنیتی کمتری نسبت به سایر بخش‌ها داشته باشند. کمپین‌های فیشینگ و مهندسی اجتماعی می‌توانند منجر به نقض داده‌ها از طریق اطلاعات ورود به سیستم آلوده یا افشای تصادفی داده‌ها شوند. تهدیدات داخلی (عمدی یا غیرعمدی) نیز با توجه به دسترسی بالای کارکنان به داده‌های حساس بیماران، نگرانی فزاینده‌ای است زیرا شامل رفتار انسانی می‌شوند که کنترل آن تنها با فناوری دشوار است. برای غلبه بر این چالش تلاش می کنیم با

برگزاری نشست ها و کارگاه های آموزشی امنیت سایبری، دانش افراد را ارتقا دهیم اما با توجه به کمبود نیروی انسانی و فشار شدید کاری در ارائه کنندگان خدمات بهداشتی و درمانی اشتباهات اجتناب‌ناپذیرند و می بایست تلفیقی از آموزش و فناوری را در این عرصه به خدمت گرفت.



در این مقاله به تهدیدات اولویت دار سایبری در نظام سلامت پرداختیم برای هر تهدید راهکارهایی در سازمان ها پیاده سازی می شود که می توان برنامه جامع امنیت سایبری را در موارد زیر خلاصه نمود:

۱. ارزیابی جامع آسیب‌پذیری‌ها

۲. تشخیص و پاسخ پیشرفته به تهدیدات

۳. پشتیبان‌گیری از داده‌ها و برنامه‌ریزی بازیابی

۴. آموزش و شبیه‌سازی تهدیدات به کارکنان

۵. ارزیابی ریسک و بررسی دقیق فروشندگان نرم افزار

۶. مدیریت دسترسی فروشندگان نرم افزار به سرورها

۷. آماده‌سازی زیرساخت فناوری اطلاعات برای آینده

۸. ارزیابی جامع سیستم‌های قدیمی

مسئولیت‌های کارکنان فناوری اطلاعات در غیاب پرسنل متخصص امنیت اطلاعات

وحید عباس‌زاده
دانشجوی PHD الکترونیک
کارشناس شبکه

در بسیاری از سازمان‌ها، به‌ویژه سازمان‌های کوچک تا متوسط و مؤسسات دانشگاهی، ممکن است افراد متخصص امنیت اطلاعات حضور نداشته باشند و یا حضور آنها مختص به ستاد مرکزی و یا واحدهای بسیار بزرگ باشد. در باقی محیط‌های کوچک، مسئولیت حفظ امنیت سایبری و حفاظت از داده‌ها به‌طور طبیعی بر عهده کارکنان عمومی فناوری اطلاعات است. این کارشناسان باید نقش‌های سنتی خود را به طوری گسترش دهند تا شامل وظایف امنیتی حیاتی واحد خود گردد. این یک توصیف و یا یک آرزوی دور و دست نیافتنی نیست بلکه ماهیت شرح وظایف و مسئولیت ها در واحدهای فاقد کارشناس امنیت اطلاعات می باشد. بخش فناوری اطلاعات در سازمان‌ها و واحدهای کوچک و خرد، معمولاً نقش‌های حفاظتی متعددی را بر عهده دارد. کنترل‌های امنیتی اساسی، از جمله فایروال‌ها، نرم‌افزارهای آنتی‌ویروس و سیستم‌های تشخیص نفوذ باید پیاده‌سازی و مدیریت شوند. نگهداری سیستم یکی دیگر از جنبه‌های مهم وظایف امنیتی آن‌ها را تشکیل می‌دهد. کارکنان فناوری اطلاعات باید وصله‌های امنیتی و به‌روزرسانی‌ها را به‌طور دقیق در سیستم‌عامل‌ها، برنامه‌ها و تجهیزات شبکه اعمال کنند و آسیب‌پذیری‌هایی را که می‌توانند توسط عوامل مخرب مورد سوءاستفاده قرار گیرند، برطرف کنند. آن‌ها همچنین باید سیاست‌های رمز عبور قوی را ایجاد و اجرا کنند.

مدیریت پیشگیرانه تهدید و ارزیابی ریسک

فراتر از حفاظت‌های اولیه، پرسنل فناوری اطلاعات با استفاده از ابزارهای اسکن، ارزیابی‌های منظم آسیب‌پذیری را برای شناسایی نقاط ضعف بالقوه در زیرساخت دیجیتال واحد عملیاتی خود باید انجام دهند. ممیزی‌های امنیتی حساب‌های کاربری، مجوزها و پیکربندی‌های سیستم بررسی و پیاده شوند، حقوق دسترسی غیرضروری حذف می‌شوند و حساب‌های غیرفعال را که می‌توانند به مشکلات امنیتی تبدیل شوند، غیرفعال کنند. تیم فناوری اطلاعات همچنین مسئولیت نظارت بر ترافیک شبکه و گزارش‌های سیستم را بر عهده دارد و باید مراقب الگوهای غیرمعمولی باشد که ممکن است نشان‌دهنده حوادث امنیتی باشند. آنها باید پروتکل‌های پاسخ به حادثه را، ایجاد و نگهداری کنند تا اطمینان حاصل شود که سازمان می‌تواند به طور مؤثر به نقض‌های احتمالی واکنش نشان دهد.

توسعه سیاست و نظارت بر انطباق قوانین امنیتی

در غیاب متخصصان امنیتی در واحدهای کوچک، کارکنان فناوری اطلاعات باید در تهیه و اجرای سیاست‌های امنیتی فعالیت نمایند. این موارد شامل سیاست‌های استفاده قابل قبول برای منابع سازمانی، رویه‌های مدیریت داده‌ها و دستورالعمل‌های استفاده از دستگاه شخصی باشد. کارکنان فناوری اطلاعات واحدهای کوچک تر تلاش می‌کنند تا اطمینان حاصل کنند که افراد دیگر واحد خود الزامات انطباق قوانین امنیتی، چه مقررات خاص کار خودشان و چه استانداردهای عمومی حفاظت از داده‌ها را رعایت می نمایند.

تداوم فعالیت و بازیابی پس از فاجعه

متخصصان فناوری اطلاعات در این محیط‌ها باید استراتژی‌های جامع پشتیبان‌گیری را توسعه داده، حفظ نموده و اطمینان حاصل کنند که داده‌های حیاتی در برابر از دست دادن یا خراب شدن محافظت می‌شوند. باید برنامه‌های بازیابی پس از فاجعه ایجاد و آزمایش شوند تا در صورت خرابی سیستم یا حوادث سایبری، زمان از کار افتادگی به حداقل برسد. آزمایش منظم این رویه‌های بازیابی بخشی از روال عملیاتی آن‌ها است.

در حالی که متخصصان فناوری اطلاعات می‌توانند به طور شایسته‌ای بسیاری از وظایف امنیتی را انجام دهند، سازمان‌ها باید محدودیت‌های این رویکرد را تشخیص دهند. با پیچیده‌تر شدن تهدیدها، حتی کوشاترین کارکنان فناوری اطلاعات نیز ممکن است فاقد تخصص امنیتی لازم باشند. بسیاری از سازمان‌ها باید ارزیابی‌های امنیتی دوره‌ای دهند تا بتوانند قابلیت‌های داخلی امنیتی خود را افزایش دهند.

آگاهی و آموزش امنیتی برای سایر کارکنان

کارکنان فناوری اطلاعات با درک اینکه کارمندان اغلب خط اول دفاع را تشکیل می‌دهند، نقش مربیان امنیتی را بر عهده دارند. آن‌ها برنامه‌های آموزشی توسعه داده و ارائه می‌دهند که شامل آگاهی از فیشینگ، شیوه‌های مرور ایمن در فضای مجازی و مدیریت صحیح اطلاعات حساس است.

مدیریت ریسک فروشنده و شخص ثالث

تیم فناوری اطلاعات نظارت امنیتی خود بر فروشندگان و ارائه‌دهندگان خدمات پشتیبانی را باید گسترش دهند. بررسی قراردادها و توافق‌نامه‌های سطح خدمات IT تحت نظارت کارشناسان فناوری اطلاعات باید باشد تا از وجود تمهیدات امنیتی کافی اطمینان حاصل شود.

چالش‌های پیش‌رو

در حالی که متخصصان فناوری اطلاعات می‌توانند به طور شایسته‌ای بسیاری از وظایف امنیتی را انجام دهند، سازمان‌ها باید محدودیت‌های این رویکرد را تشخیص دهند. با پیچیده‌تر شدن تهدیدها، حتی کوشاترین کارکنان فناوری اطلاعات نیز ممکن است فاقد تخصص امنیتی لازم باشند. بسیاری از سازمان‌ها باید ارزیابی‌های امنیتی دوره‌ای دهند تا بتوانند قابلیت‌های داخلی امنیتی خود را افزایش دهند.

نتیجه گیری

در سازمان‌هایی که پرسنل امنیتی اختصاصی ندارند، کارکنان فناوری اطلاعات با میل و رغبت نقش محافظان سایبری را بر عهده می‌گیرند. نقش گسترده آنها شامل حفاظت‌های فنی، تدوین سیاست‌ها، آموزش کارکنان و آمادگی در برابر حوادث است. در حالی که این رویکرد می‌تواند به طور مؤثر بسیاری از خطرات را مدیریت کند، سازمان‌ها باید مرتباً ارزیابی کنند که آیا نیازهای امنیتی آنها از آنچه کارکنان عمومی فناوری اطلاعات می‌توانند به طور منطقی ارائه دهند، فراتر رفته است یا خیر. چشم‌انداز در حال تحول تهدید در نهایت ممکن است به منابع امنیتی تخصصی‌تر، چه از طریق استخدام، برون‌سپاری یا ابزارهای پیشرفته امنیتی، نیاز داشته باشد.

بازیابی پس از فاجعه:
سنگ بنای فناوری اطلاعات مدرن (Disaster Recovery)

صابر درس‌خوان
کارشناس ارشد شبکه
کارشناس مسئول زیرساخت

در دنیای پرریسک فناوری اطلاعات، بازگشت از فاجعه (Disaster Recovery) یک نیاز اجتناب‌ناپذیر برای پایداری و بقای سازمان‌هاست. سازمان‌هایی که به DR توجه نمی‌کنند، در معرض از دست دادن داده، توقف سرویس‌ها و آسیب جدی به اعتبار خود هستند. هرچند راه‌اندازی یک سیستم کامل DR ممکن است نیازمند منابع زیادی باشد، اما کارشناسان IT می‌توانند با اقدامات هدفمند و عملیاتی، بسیاری از مزایای آن را بدون زیرساخت پیچیده فراهم کنند و سازمان را در برابر فاجعه‌ها مقاوم سازند.

در دنیای فناوری اطلاعات، بحران‌ها غیرقابل اجتناب هستند؛ از حملات سایبری گرفته تا خرابی‌های سخت‌افزاری، بلایای طبیعی و اشتباهات انسانی. این رویدادها می‌توانند به از دست رفتن داده‌ها، توقف فعالیت‌های حیاتی و خسارت‌های سنگین منجر شوند. از همین رو، سازمان‌ها باید برنامه‌ای ساختارمند و مشخص برای بازگشت از فاجعه (Disaster Recovery) داشته باشند تا پس از وقوع حوادث، بتوانند سریع و مؤثر به وضعیت عادی بازگردند.

چیستی

بازگشت از فاجعه (Disaster Recovery - DR) مجموعه‌ای از فرآیندها، ابزارها و سیاست‌هاست که به سازمان‌ها کمک می‌کند در صورت وقوع فاجعه، زودتر بازیابی شوند و حداقل زمان توقف و حداقل از دست دادن اطلاعات را تجربه کنند.

DR معمولاً بخشی از یک برنامه جامع‌تر به‌نام Business Continuity Plan (BCP) است با مفهوم کلی ادامه فعالیت سازمان، اما تمرکز آن بیشتر بر بازیابی سیستم‌ها، داده‌ها و زیرساخت‌های IT است.

سیستم‌های DR اغلب شامل بکاپ‌گیری منظم، شبیه‌سازی سرورها در مکان‌های دیگر، زیرساخت‌های ابری، و روش‌های تست و ارزیابی هستند. هدف اصلی این است که فعالیت حتی در زمان فاجعه هم بتواند ادامه پیدا کند یا سریعاً از سر گرفته شود.

مشخصات یک سیستم Disaster Recovery موفق

یک راهکار مؤثر برای بازگشت از فاجعه در IT،

دارای ویژگی‌ها و الزامات زیر است:
پشتیبان‌گیری منظم (Scheduled Backups): داده‌ها باید به‌صورت دوره‌ای و خودکار ذخیره شوند.
- بازیابی سریع (Rapid Restoration): سیستم باید بتواند در کوتاه‌ترین زمان داده‌ها را بازیابی کند.
- ذخیره‌سازی در مکان‌های مجزا (Off-Site Storage): نسخه‌های پشتیبان باید در مکانی متفاوت یا در فضای ابری ذخیره شوند.
- برنامه مستند بازگشت از فاجعه (DR Plan): تمام مراحل بازیابی باید به‌صورت کتبی و قابل اجرا تدوین شده باشند.
- تست و ارزیابی دوره‌ای: سناریوهای شبیه‌سازی‌شده برای بررسی اثربخشی برنامه DR باید به‌طور منظم اجرا شوند.
- اولویت‌بندی سیستم‌ها و داده‌ها: مشخص‌بودن اینکه کدام اطلاعات و سامانه‌ها حیاتی‌تر هستند و باید زودتر بازیابی شوند.
- اطلاع‌رسانی و هماهنگی در زمان فاجعه: سیستم اطلاع‌رسانی داخلی برای تیم‌ها و کاربران در زمان بروز فاجعه.

اهداف اصلی Disaster Recovery

برنامه بازگشت از فاجعه با اهداف مشخصی طراحی و اجرا می‌شود که عبارتند از:
- کاهش زمان از کار افتادگی (Downtime): تلاش برای کم‌کردن مدت زمانی که خدمات سازمان در دسترس نیستند.
- حداقل‌سازی از دست رفتن داده (Data Loss): جلوگیری از حذف یا نابودی دائمی اطلاعات.
- تضمین تداوم خدمات حیاتی: تضمین این‌که خدمات حیاتی بدون وقفه یا با کمترین وقفه ادامه پیدا کنند.

افزایش آمادگی سازمانی: ارتقاء آگاهی و آمادگی کارکنان در مواجهه با فاجعه‌ها.
- ایجاد اعتماد در ذی‌نفعان: نمایش قابلیت سازمان برای حفظ پایداری و امنیت.
- تطابق با الزامات قانونی و مقرراتی: رعایت استانداردهای بالادستی و انطباق کامل با آنها

نقش کارشناسان فناوری اطلاعات

حتی اگر یک سازمان هنوز زیرساخت کامل DR را راه‌اندازی نکرده باشد، کارشناسان باید با اقدامات هوشمندانه بسیاری از اهداف DR را پوشش دهند:
- راه‌اندازی فرآیند پشتیبان‌گیری منظم: تنظیم نرم‌افزارهایی برای تهیه خودکار نسخه پشتیبان از پایگاه‌داده‌ها و فایل‌ها.
- ذخیره‌سازی بکاپ در فضای ابری یا سیستم ثانویه: استفاده از سرورهای ثانویه داخل و خارجی توصیه می شود.
- تدوین و مستندسازی فرآیند بازیابی: نوشتن دستورالعمل‌های گام‌به‌گام برای بازیابی سیستم‌ها و داده‌ها.
- ایجاد لیست اولویت‌های بازیابی: شناسایی سامانه‌ها و اطلاعات حیاتی برای بازیابی سریع‌تر.
- اجرای آزمایش‌های شبیه‌سازی فاجعه: طراحی سناریوهای ساده برای تمرین نحوه پاسخ به فاجعه.
- مستندسازی اطلاعات تماس اضطراری: تهیه لیستی از افراد کلیدی، اطلاعات تماس و نقش‌های آنان در زمان فاجعه.
- آموزش و توانمندسازی پرسنل: آموزش کاربران برای پاسخ مناسب در زمان از دست رفتن داده یا دسترسی نداشتن به سیستم‌ها.
- نظارت پیوسته بر سلامت سیستم‌ها: استفاده از مانیتورینگ برای پیشگیری از فاجعه پیش از وقوع.

نتیجه‌گیری

در دنیای پرریسک فناوری اطلاعات، بازگشت از فاجعه (Disaster Recovery) یک نیاز اجتناب‌ناپذیر برای پایداری و بقای سازمان‌هاست. سازمان‌هایی که به DR توجه نمی‌کنند، در معرض از دست دادن داده، توقف سرویس‌ها و آسیب جدی به اعتبار خود هستند. هرچند راه‌اندازی یک سیستم کامل DR ممکن است نیازمند منابع زیادی باشد، اما کارشناسان IT می‌توانند با اقدامات هدفمند و عملیاتی، بسیاری از مزایای آن را بدون زیرساخت پیچیده فراهم کنند و سازمان را در برابر فاجعه‌ها مقاوم سازند.

ویکی واژه

ویکی واژه
WIKIWORD

در عصری که تهدیدهای دیجیتال روز به روز پیچیده‌تر می‌شوند، درک زبان فنی دیگر تنها در حوزه متخصصان نیست. بخش ویکی‌واژه در «پالسی نو» با هدف پر کردن شکاف بین اصطلاحات فنی و درک روزمره ارائه شده است. در هر شماره، ویکی‌واژه مجموعه‌ای منتخب از مفاهیم را معرفی می‌کند که با دقت به دلیل ارتباط، عمق و تأثیرشان انتخاب شده‌اند. این بخش از طریق توضیحات روشن و زمینه عملی، خوانندگان را با واژگانی که کمتر شناخته شده اند اما اساسی و پایه ای هستند آشنا می کند تا با آگاهی و اعتماد به نفس بیشتری در دنیای دیجیتال فعالیت کنند.

سید محمدحسن الهی

داده بَرداری

خروج اطلاعات، که با نام داده بَرداری اطلاعات نیز شناخته می‌شود، انتقال غیرمجاز داده‌ها از یک رایانه یا شبکه سازمانی است. برخلاف حملات آشکاری که داده‌ها را از بین می‌برند یا رمزگذاری می‌کنند، خروج اطلاعات اغلب مخفیانه و به سختی قابل تشخیص است. مهاجمان ممکن است از طریق بدافزار، افراد خودی (بسیار معمول) یا حساب‌های کاربری آسیب‌دیده برای دسترسی و استخراج داده‌های حساس استفاده کنند.

Data Exfiltration

Data Exfiltration

معماری اعتماد صفر

یک مدل امنیتی است که فرض می‌کند هیچ کاربر یا سیستمی - چه در داخل و چه در خارج از شبکه - نباید به طور پیش‌فرض مورد اعتماد باشد. این مدل نیاز به تأیید هویت دقیق، حتی برای دستگاه‌های داخل محیط دارد. برخلاف مدل‌های سنتی که فرض می‌کنند همه چیز در داخل شبکه امن است، اعتماد صفر این فرض را حذف کرده است. سازمان‌هایی که از اعتماد صفر استفاده می‌کنند، از چندین لایه کنترل امنیتی از جمله احراز هویت قوی، تقسیم‌بندی شبکه به واحدهای خُردتر و نظارت مداوم استفاده می‌کنند.

Zero Trust Architecture

Zero Trust Architecture

فناوری اطلاعات سایه

به استفاده از نرم‌افزار، دستگاه‌ها یا خدمات در یک سازمان بدون تأیید صریح بخش فناوری اطلاعات اشاره دارد. کارکنان ممکن است ابزارهای خود (مانند برنامه‌های پیام‌رسان یا پلتفرم‌های اشتراک‌گذاری فایل) را برای راحتی خودشان نصب کنند، این عمل تهدید بزرگی برای امنیت داده‌ها و انطباق با قوانین فناوری اطلاعات محسوب می‌شود زیرا بخش فناوری اطلاعات از محل ذخیره یا انتقال اطلاعات حساس بی‌اطلاع است.

Shadow IT

Shadow IT

Attack Surface

Attack Surface

سطح حمله

سطح حمله تعداد کل نقاطی است که یک کاربر غیرمجاز می‌تواند سعی کند از طریق آنها وارد سیستم شود یا از آن داده و اطلاعات استخراج کند. این نقاط می توانند شامل اشکالات نرم‌افزاری، پورت‌های باز، API های برنامه و حتی رفتارهای کارمندان باشد. کاهش سطح حمله، کلید امنیت قابل قبول است.

Security Posture

Security Posture

وضعیت امنیت اطلاعات

وضعیت امنیتی به قدرت کلی امنیت سایبری یک سازمان اشاره دارد که ترکیبی از سیاست‌ها، رویه‌ها، فناوری‌ها و آمادگی برای شناسایی و پاسخ به تهدیدها می باشد. یک وضعیت امنیتی قوی شامل اقدامات پیشگیرانه مانند اسکن آسیب‌پذیری، آموزش کارکنان، برنامه‌های واکنش به حوادث و رعایت استانداردها است. این وضعیت یک معیار پویا و همواره در حال تکامل است نه یک ارزیابی یک‌باره.

Security Through Obscurity

Security Through Obscurity

سند باکس

سندباکسینگ یک مکانیسم امنیتی است که در آن کد بالقوه غیرقابل اعتماد در یک محیط کنترل شده و جدا از سیستم اصلی اجرا می‌شود. اغلب برای آزمایش فایل‌ها یا برنامه‌ها برای رفتارهای مخرب بدون به خطر انداختن یکپارچگی سیستم استفاده می‌شود.

این رویکرد در تشخیص تهدیدات مدرن، به ویژه برای تجزیه و تحلیل تهدیدات جدید یا ناشناخته، بسیار مهم است.

Sandboxing

Sandboxing

امنیت از طریق ابهام

امنیت از طریق ابهام به تکیه بر پنهان‌کاری طراحی یا پیاده‌سازی به عنوان روش اصلی ایمن‌سازی یک سیستم اشاره دارد. به عنوان مثال، پنهان کردن صفحه ورود یا استفاده از یک پورت غیراستاندارد برای دسترسی ها. در حالی که ابهام می‌تواند یک لایه جزئی از محافظت را فراهم کند، هرگز نباید مکانیسم دفاعی اصلی باشد. شیوه‌های امنیتی قوی، شناخته شده و کاملاً آزمایش شده همیشه باید در ترکیب با آن استفاده شوند.

بررسی مرکز عملیات امنیتی (SOC) و نقش کارشناسان IT در تحقق اهداف آن

جواد فرهادی
کارشناس ارشد نرم افزار

مرکز عملیات امنیتی یا (Security operation Centers باختصار SOC)، یک تیم متمرکز است که مسئولیت نظارت، تجزیه و تحلیل و پاسخگویی به حوادث امنیت سایبری را بر عهده دارد. می توان آن را به معادل دیجیتال یک تیم واکنش سریع نظامی در نظر گرفت که دائماً هوشیار و آماده واکنش به هرگونه فعالیت مشکوک است. هدف اصلی SOC محافظت از دارایی‌های اطلاعاتی یک سازمان با شناسایی، پیشگیری و پاسخگویی به تهدیدات سایبری است.

مرکز عملیات امنیتی چیست؟

مرکز عملیات امنیتی یا (Security operation Centers باختصار SOC)، یک تیم متمرکز است که مسئولیت نظارت، تجزیه و تحلیل و پاسخگویی به حوادث امنیت سایبری را بر عهده دارد. می توان آن را معادل دیجیتال یک تیم واکنش سریع نظامی در نظر گرفت که دائماً هوشیار و آماده واکنش به هرگونه فعالیت مشکوک است. هدف اصلی SOC محافظت از دارایی‌های اطلاعاتی یک سازمان با شناسایی، پیشگیری و پاسخگویی به تهدیدات سایبری است.
SOC از طریق جمع‌آوری و تحلیل داده‌ها از منابع مختلف (مثل فایروال‌ها، آنتی‌ویروس‌ها، سیستم‌های تشخیص نفوذ، و لاگ‌های سیستمی) تلاش می‌کند تهدیدات را در مراحل اولیه شناسایی کرده و از بروز خسارات جلوگیری نماید. علاوه‌براین، SOC نقش مهمی در مدیریت رخدادهای امنیتی، تحلیل بدافزار، پاسخگویی به حملات، و بازیابی پس از حادثه ایفا می‌کند.
SOC ها معمولاً به صورت ۲۴ ساعته و ۷ روز هفته و ۳۶۵ روز سال فعالیت می‌کنند و نظارت و محافظت مداوم را در شبکه بزرگ سازمانی فراهم می آورند. این مرکز ترکیبی از فناوری‌ها، فرآیندها و پرسنل ماهر امنیتی را برای دستیابی به اهداف خود به کار می‌گیرد. مهمترین اجزاعبارتند از:

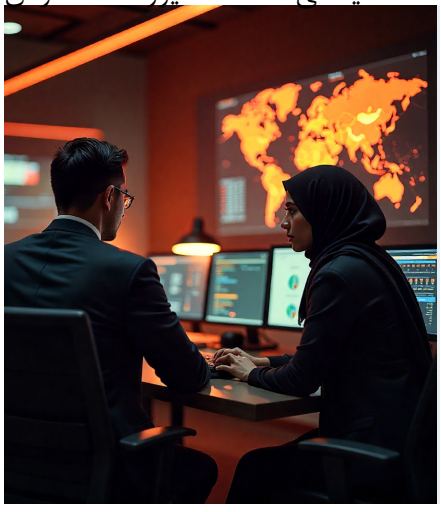
- سیستم‌های مدیریت اطلاعات و رویدادهای امنیتی: این سیستم‌ها گزارش‌های امنیتی را از منابع مختلف جمع‌آوری و تجزیه و تحلیل می‌کنند و یک نمای متمرکز از رویدادهای امنیتی ارائه می‌دهند.
- سیستم‌های تشخیص و پیشگیری از نفوذ (IDS/IPS): این سیستم‌ها ترافیک شبکه را برای فعالیت‌های مخرب رصد کرده و برای مسدود کردن یا کاهش تهدیدات اقدام می‌کنند.
- نظارت مستمر بر لاگ‌ها: بررسی منظم گزارش‌ها و وقایع ثبت‌شده در فایروال، آنتی‌ویروس و سیستم‌عامل‌ها.

- رهگیری اطلاعات تهدید: رهگیری ها شامل اطلاعات به‌روزی در مورد تهدیدات نوظهور، آسیب‌پذیری‌ها و تکنیک‌های حمله هستند که مداوم بروز می گردند و واحد SOC در تعقیب یافتن آنها در شبکه می باشد.
- طرح واکنش به حادثه: یک طرح مستند که مراحلی را که باید در صورت وقوع یک حادثه امنیتی انجام شود، مشخص می کند.

نقش یک مرکز عملیات امنیت (SOC)

مرکز عملیات امنیت (SOC) نقش حیاتی در وضعیت کلی امنیت یک سازمان ایفا می‌کند. وظایف اصلی آن عبارتند از:

- نظارت: نظارت مداوم بر شبکه، سیستم‌ها و برنامه‌ها برای فعالیت‌های مشکوک.
- تشخیص: شناسایی حوادث امنیتی بالقوه از طریق تجزیه و تحلیل گزارش‌های امنیتی، هشدارها و اطلاعات تهدید.
- تحلیل: بررسی حوادث امنیتی برای تعیین دامنه، تأثیر و علت اصلی آنها.
- واکنش: انجام اقداماتی برای مهار و ریشه‌کن کردن حوادث امنیتی، مانند ایزوله کردن



سیستم‌های آلوده یا مسدود کردن ترافیک مخرب.
- پیشگیری: اجرای اقداماتی برای جلوگیری از حوادث امنیتی آینده، مانند وصله کردن آسیب‌پذیری‌ها و بهبود پیکربندی‌های امنیتی.
- گزارش‌دهی: ارائه گزارش‌های منظم در مورد حوادث امنیتی، تهدیدات و آسیب‌پذیری‌ها به مدیریت.

وظایف کارکنان فناوری اطلاعات در غیاب مرکز عملیات امنیت (SOC)

همه سازمان‌ها نیاز به یک مرکز عملیات امنیت اختصاصی ندارند. در غیاب مرکز عملیات امنیت (SOC)، مسئولیت‌های امنیت سایبری اغلب بر عهده کارکنان فناوری اطلاعات است. برخی از وظایف کلیدی که کارکنان فناوری اطلاعات باید انجام دهند، تا به حداقل وظایف SOC و اهداف آن نائل شوند را می توان به شرح ذیل بیان نمود:

- پیاده‌سازی کنترل‌های امنیتی: کارکنان فناوری اطلاعات باید کنترل‌های امنیتی مانند فایروال ها، سیستم های تشخیص نفوذ و نرم‌افزار آنتی‌ویروس را پیاده‌سازی و حفظ و نگهداری کنند.
- مدیریت آسیب‌پذیری ها: اسکن منظم سیستم‌ها برای یافتن آسیب‌پذیری‌ها و سعی در برطرف نمودن سریع آنها و یامدیریت‌صحیح‌نقاط‌آسیب.
- آموزش آگاهی‌بخشی امنیتی: آموزش کاربران در مورد تهدیدات امنیتی و بهترین شیوه‌های مقابله با آنها
- واکنش به حادثه: تدوین و اجرای یک برنامه واکنش به حادثه برای مدیریت مؤثر حوادث امنیتی.
- نظارت و هشدار: نظارت بر گزارش‌ها و هشدارهای امنیتی برای فعالیت‌های مشکوک.
- پشتیبان‌گیری منظم: انجام پشتیبان‌گیری منظم از داده‌های حیاتی برای اطمینان از تداوم فعالیت شبکه سازمانی درصورت‌وقوع‌حادثه‌امنیتی.
- آگاه ماندن و به‌روزبودن: به‌روز ماندن در مورد آخرین تهدیدات و آسیب‌پذیری‌های امنیتی.

باید گفت که در غیاب یک مرکز عملیات امنیت (SOC) اختصاصی، کارکنان فناوری اطلاعات باید در رویکرد خود به امنیت، پیشگیرانه و دقیق عمل کنند. این امر مستلزم درک قوی از اصول امنیتی، تعهد به یادگیری مداوم و تمایل به سازگاری با چشم‌انداز تهدیدهای دائماً در حال تغییر است.

عواقب فعالیت بدون SOC فراتر از تهدیدات فوری است. توانایی سازمان در حفظ انطباق با مقررات، به ویژه در شبکه هایی که الزامات سختگیرانه‌ای برای حفاظت از داده‌ها دارند، به طور قابل توجهی تضعیف می‌شود. علاوه بر این، فقدان یک تیم امنیتی اختصاصی می‌تواند بر کارایی عملیاتی تأثیر منفی بگذارد، زیرا کارمندان ممکن است زمان ارزشمندی را صرف وظایف مرتبط با امنیت کنند که می‌تواند توسط یک SOC تخصصی به طور مؤثرتری انجام شود. این فقدان تخصص و مدیریت متمرکز، احتمال وقوع حوادث امنیتی را افزایش می‌دهد و مانع از توانایی سازمان در بازیابی سریع و کارآمد از چنین رویدادهایی می‌شود. در نهایت، هزینه‌های بلندمدت مرتبط با فعالیت بدون یک مرکز عملیات امنیت (SOC) بسیار بیشتر از سرمایه‌گذاری اولیه برای ایجاد آن است.

آموزش فناوری اطلاعات:
مبانی هک اخلاقی
بخش اول

دکتر طاها صمدسلطانی
دانشیار انفورماتیک پزشکی
مدیرآمار، فناوری اطلاعات و امنیت فضای مجازی دانشگاه

این بخش از مجله به مباحث آموزشی با محوریت موضوعات جذاب در زمینه فناوری اطلاعات خواهد پرداخت. هر مبحث متشکل از مجموعه اپیزودهایی خواهد بود که سلسله وار تا اتمام آن به مخاطب انتقال داده خواهد شد.

مبحث اول : آشنایی با مفاهیم و واژه شناسی هک اخلاقی (Ethical Hacking)

در دنیای دیجیتال و فضای سایبری به دسترسی غیرقانونی به اطلاعات و نرم افزارهای افراد یا سازمانه ها هک کردن آن گفته می شود. فرد هک شده هدف یا قربانی(Target یا Victim) نامیده می شود و فرد یا تیم هک کننده را Hacker یا Attacker می گویند. فی النفسه هک یک اقدام غیرقانونی می باشد که تحت پیگیرد قانونی قرار می گیرد و مجازات آن در کشورهای مختلف از چند ماه تا بیش از ۱۰ سال و در صورت تهدید امنیت ملی با تشدید می باشد. سالانه ده ها هزار پرونده هک در پلیس فتا که نهاد متولی امنیت در فضای تبادل اطلاعات در ایران می باشد مورد رسیدگی قرار می گیرد. اما از بطن هک مفهومی شکل گرفته که در تضاد با جرایم مرتبط با آن و برای پیشگیری از آن می باشد. هک اخلاقی(Ethical Hacking) هک اخلاقی به فرآیند شناسایی و تست آسیب پذیریهای سیستمهای رایانه ای، شبکه ها و نرم افزارها با مجوز قانونی و در چارچوب اهداف سازمان گفته می شود. هکرهای اخلاقی افرادی هستند که به صورت قراردادی یا دائمی با یک سازمان برای تست امنیت آن همکاری می کنند. آنها از مکانیسم های مورد استفاده سایر هکرها بهره می برند با این تفاوت که این افراد اجازه حمله به سیستم و سامانه ها را برای شناسایی نقاط ضعف دارند و این نقاط ضعف را منتشر نمی کنند. محدوده کارشان نیز در قرارداد ذکر می شود و نباید از ان فراتر رود. در یک دسته بندی از انواع هکرها می توان به موارد زیر اشاره نمود:

- **Script Kiddies ها:** این دسته از هکرها به کلاه صورتی(Pink Hat) نیز معروفند. این هکرها مبتدی و با دانش محدود می باشند و صرفا استفاده از ابزارها و تکنیک های ساده را می دانند و مکانیسم و فرآیند اتفاق افتاده را درک نمی کنند. توانایی آنها محدود بوده و عمدتا با انگیزه های کنجکاوی و آزار اقدام می کنند و ممکن است ناخواسته مرتکب جرم شوند.
- **هکرهای کلاه سفید**(White hat): این هکرها همان هکرهای اخلاقی می باشند که اساسا به دیگران آسیبی نمی رسانند و به آنها متخصصین تست نفوذ(Penetration test) و امنیت نیز می گویند که در ازای قرارداد، وظیفه شناسایی مشکلات و حل آن را دارند.
- **هکرهای کلاه سیاه** (Black Hat): این هکرها کاملا خلاف قانون عمل می کنند و هدفشان سرقت، تخریب و سواستفاده از داده ها و سامانه ها می باشد. آنها با استفاده از بدافزارها(Malware) یا فریب و Phishing کاربران، اطلاعات آنها را سرقت می کنند یا بصورت جزیی یا کامل تخریب می کنند. انگیزه های مالی مثل سرقت از بانکها یا فروش اطلاعات آنها، اعمال خرابکارانه و تروریسم سایبری و جاسوسی از اصلی ترین انگیزه ها می باشد. نمونه هایی از این

در دنیای دیجیتال و فضای سایبری به دسترسی غیرقانونی به اطلاعات و نرم افزارهای افراد یا سازمانه ها هک کردن آن گفته می شود. فرد هک شده هدف یا قربانی(Target یا Victim) نامیده می شود و فرد یا تیم هک کننده را Hacker یا Attacker می گویند. فی النفسه هک یک اقدام غیرقانونی می باشد که تحت پیگیرد قانونی قرار می گیرد و مجازات آن در کشورهای مختلف از چند ماه تا بیش از ۱۰ سال و در صورت تهدید امنیت ملی با تشدید می باشد. سالانه ده ها هزار پرونده هک در پلیس فتا که نهاد متولی امنیت در فضای تبادل اطلاعات می باشد مورد رسیدگی در ایران قرار می گیرند.

خرابکاری ها عبارتند از حمله باج افزاری(Ransomware) با عنوان WannaCry در سال ۲۰۱۷ به سیستمهای اطلاعات بیمارستانی و اخاذی جهت بازگرداندن اطلاعات، سرقت اطلاعات اسنپ فود در سال گذشته و فروش در وب پنهان(Dark Web) ،حمله به زیرساخت های انرژی اوکراین در سال ۲۰۱۵ که باعث خاموشی گسترده شد.

- **هکرهای کلاه خاکستری** (Gray Hat): این هکرها ترکیبی از هک اخلاقی و مخرب می باشند. آنها معمولا بدون مجوز سامانه ها را هک می کنند اما انگیزه تخریبی ندارند و عمدتا برای اثبات خود یا استخدام خود در سازمان ها با نشان دادن توانمندیهایشان هستند. گاهی نیز برای دریافت پاداش یا معروف شدن این کار را می کنند. عمدتا پس از پیدا کردن راه های نفوذ به سازمان اطلاع می دهند یا اعلان عمومی می کنند. از نظر فنی جرم مرتکب شده اند اما چون خرابکاری نمی کنند، سازمان ها با آنها مدارا می کنند یا استخدام می شوند. از موارد مهم به کشف نقص های امنیتی فیسبوک و مایکروسافت برای دریافت پاداش می توان اشاره کرد.

در اپیزود آینده با روشهای تست نفوذ و آشنایی با مراحل هک اخلاقی بحث را ادامه خواهیم داد.

ادامه دارد...

ضرورت راهبردی مدیریت امنیت اطلاعات در دانشگاه‌های علوم پزشکی

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

در عصر دیجیتال، دانشگاه‌های علوم پزشکی در نقش‌های چندگانه آموزشی، پژوهشی، بهداشتی و درمانی، به‌طور فزاینده‌ای وابسته به داده‌های الکترونیکی و زیرساخت‌های اطلاعاتی هستند. تهدیدات سایبری، آسیب‌پذیری‌های انسانی و فنی، و وقوع بحران‌هایی چون پاندمی‌ها، ضرورت توجه راهبردی به امنیت اطلاعات را دوچندان کرده‌اند. این مقاله با مرور تحلیلی بر چالش‌ها، الزامات، فناوری‌ها، و راهکارهای ارتقای امنیت اطلاعات در دانشگاه‌های علوم پزشکی، بر توسعه تاب‌آوری سازمانی تأکید دارد.

مقدمه

امروزه اطلاعات در سازما نها، مؤسسات پیشرفته و جوامع علمی به عنوان شاهرگ حیاتی محسوب می گردد. به طور کلی ارزش اطلاعات به منابع اطلاعات، مکان اطلاعات و زمان اطلاعات بستگی دارد .در هر سازمان روزانه، اطلاعات زیادی تولید می شود و ضروری است نظام های اطلاعاتی قدرتمندی به وجود آید که بتواند این گونه اطلاعات را به طور صحیح و فوری پردازش کند و برای پیشبرد اهداف مدیریت سازمان، اطلاعات مفیدی فراهم سازد. سازمان های آموزشی و دانشگاه ها نیز از این امر مستثنی نیستند و به اطلاعاتی صحیح، دقیق و روزآمد نیاز دارند تا بر مبنای آن بتوانند تصمیماتی بخردانه و درست بگیرند. [۸] تحول دیجیتال در نظام سلامت، منجر به وابستگی گسترده دانشگاه‌های علوم پزشکی به زیرساخت‌های اطلاعاتی شده است. اطلاعات بیماران، پژوهش‌های پزشکی، پرونده‌های آموزشی و سامانه‌های اداری، همگی در معرض تهدیداتی مانند حملات سایبری، نشت داده و اختلال عملکرد قرار دارند. بروز بحران‌هایی مانند همه‌گیری کووید۱۹-، این ضرورت را دوچندان کرده که زیرساخت‌ها نه‌تنها ایمن بلکه تاب‌آور باشند. امنیت اطلاعات در این فضا به عنوان ستون فقرات خدمات سلامت مدرن، به عنوان یکی از اولویت‌های سیاست‌گذاران و مدیران دانشگاهی مطرح خواهد بود. [۱]

تعریف مدیریت امنیت اطلاعات و پیشینه تاریخی

مدیریت امنیت اطلاعات(Information Security Management) ، به مجموعه‌ای از سیاست‌ها، فرآیندها، ابزارها و رویه‌ها اطلاق می‌شود که با هدف محافظت از محرمانگی(Confidentiality)، صحت (Integrity) و دسترسی‌پذیری (Availability) اطلاعات طراحی شده‌اند. این سه اصل به‌عنوان "مثلث CIA" شناخته می‌شوند. [۱]

در نظام سلامت جهانی، نخستین توجه جدی به امنیت اطلاعات با قانون HIPAA در ایالات متحده (۱۹۹۶) آغاز شد که الزامات سخت‌گیرانه‌ای برای حفاظت از اطلاعات سلامت بیماران اعمال کرد. [۹] در اروپا نیز با اجرای GDPR، تمرکز بیشتری بر رضایت بیمار و حفاظت فنی اطلاعات اعمال شده است. در ایران، آیین‌نامه‌های متعددی از سوی وزارت بهداشت منتشر شده‌اند، اما هم‌چنان نیاز به یکپارچگی و الزام اجرایی احساس می‌شود.

تهدیدات رایج

به طور کلی تهدیدات را می توان در سه دسته تقسیم بندی کرد:

- فنی: حملات باج‌افزار، آسیب‌پذیری‌های نرم‌افزار، نفوذ از راه دور
- انسانی: مهندسی اجتماعی، فیشینگ، ناآگاهی کاربران
- سازمانی: عدم تدوین خط‌مشی امنیتی، پاسخ‌دهی ناکارآمد به رخدادها

سامانه‌ها و فناوری‌های امنیت اطلاعات

استفاده از سامانه‌های فناورانه در دانشگاه‌های علوم پزشکی شامل طیف متنوعی از زیرساخت‌ها و نرم‌افزارهای حیاتی است که باید با ملاحظات امنیتی ویژه طراحی و مدیریت شوند:

- Security Information and Event ManagemenT (SIEM):

سامانه مدیریت اطلاعات و رویدادهای امنیتی با هدف جمع‌آوری، همبسته‌سازی و تحلیل بلادرنگ داده‌های امنیتی از منابع گوناگون مانند سرورها، نرم‌افزارها و شبکه‌ها. SIEM کمک می‌کند تهدیدات پیچیده سریع‌تر شناسایی و گزارش‌دهی شوند. [۱۴]

- Next Generation Firewall (NGFW):

فایروال نسل جدید با قابلیت شناسایی تهدید در لایه‌های بالاتر شبکه (برنامه‌ها و محتوا) و کنترل دقیق بر کاربران و داده‌ها. این فناوری نسبت به فایروال‌های سنتی، عملکرد هوشمندتر و انعطاف‌پذیرتری دارد. [۱۵]

- Endpoint Detection and Response (EDR):

سامانه‌های شناسایی و پاسخ به تهدیدات در سطح نقاط پایانی (مانند رایانه‌های کاربران). این ابزارها قابلیت تحلیل رفتار مشکوک، جلوگیری از نفوذ و پاسخ سریع به رخدادهای امنیتی را دارند. [۱۶]

- Mobile Device Management (MDM):

مدیریت امنیتی تجهیزات همراه مانند گوشی‌ها و تبلت‌های مورد استفاده در بیمارستان یا توسط اعضای هیئت‌علمی. با MDM می‌توان سیاست‌های امنیتی مانند رمزگذاری، حذف از راه دور و کنترل دسترسی را پیاده‌سازی کرد. [۱۷]

- Data Loss Prevention (DLP):

سامانه‌های جلوگیری از نشت اطلاعات که با پایش محتوا و فعالیت کاربران مانع خروج داده‌های حساس از سازمان از طریق چاپ، کپی، ایمیل و USB می‌شوند. [۱۸]

- End-to-End Encryption:

رمزنگاری سراسری برای حفاظت از اطلاعات در زمان ارسال یا ذخیره‌سازی. برای تبادل ایمن اطلاعات بیماران، پژوهش‌ها یا مکاتبات رسمی حیاتی است. [۱۹]

- Multi-Factor Authentication (MFA):

استفاده از چند عامل (مثلاً رمز عبور + کد پیامکی یا اثر انگشت) برای احراز هویت ایمن در سامانه‌های اطلاعاتی مانند HIS یا سامانه‌های آموزشی. [۲۰]

- Backup & Disaster Recovery:

سامانه‌های پشتیبان‌گیری و بازیابی اطلاعات در شرایط بحران یا حمله سایبری

برای جلوگیری از از بین‌رفتن داده‌های حیاتی. [۲۱]

راهبردهای امنیتی

راهبردها باید از حالت سنتی دفاعی صرف فراتر رفته و به سمت رویکردهای هوشمند، پیش‌دستانه و چندلایه حرکت کنند:

- پیشگیرانه: سیاست امنیتی، رمزگذاری، محدودسازی دسترسی
- شناسایی: مانیتورینگ مستمر، سیستم‌های هشداردهنده خودکار
- واکنشی: برنامه‌های بازیابی، مراکز واکنش سریع، تمرین بحران

چارچوب‌های مرجع امنیت اطلاعات

چارچوب‌های مرجع امنیت اطلاعات، مجموعه‌ای از استانداردها، دستورالعمل‌ها و بهترین روش‌ها هستند که سازمان‌ها می‌توانند برای مدیریت و حفاظت از اطلاعات خود از آن‌ها استفاده کنند. این چارچوب‌ها به سازمان‌ها کمک می‌کنند تا یک سیستم مدیریت امنیت اطلاعات مؤثر ایجاد کنند و ریسک‌های امنیتی را به حداقل برسانند.

در دنیای امروز که جرایم سایبری و تهدیدات امنیتی رو به افزایش است، استفاده از چارچوب‌های مرجع امنیت اطلاعات برای سازمان‌ها امری ضروری است. این چارچوب‌ها به سازمان‌ها کمک می‌کنند تا از اطلاعات حساس خود محافظت کنند و از آسیب‌ها و خسارات ناشی از حوادث امنیتی جلوگیری کنند.

به طور خلاصه، چارچوب‌های مرجع امنیت اطلاعات یک ابزار حیاتی برای سازمان‌ها هستند تا بتوانند امنیت اطلاعات خود را به طور مؤثر مدیریت کنند و از تهدیدات سایبری محافظت کنند. انتخاب چارچوب مناسب و پیاده‌سازی آن با توجه به نیازها و الزامات سازمان، کلید موفقیت در این زمینه است.

برخی از استانداردها و چارچوب‌های مرجع مهم امنیت اطلاعات عبارتند از:

- Information Security Management System (ISMS - ISO/IEC 27001):

سیستم مدیریت امنیت اطلاعات بر پایه استاندارد بین‌المللی که شامل ارزیابی ریسک، پیاده‌سازی کنترل‌ها، و بهبود مستمر است. [۱]

- ISO 27799:

مکمل ISO 27001 برای محیط سلامت، تمرکز بر محافظت از اطلاعات سلامت بیماران و تضمین امنیت سامانه‌های اطلاعات سلامت دارد. [۲۲]

- Control Objectives for Information and Related Technologies (COBIT):

چارچوب راهبری فناوری اطلاعات که تمرکز آن بر هم‌راستاسازی اهداف IT با اهداف سازمانی و ارزیابی عملکرد و ارزش‌افزایی IT است. [۲۳]

- NIST Cybersecurity Framework (CSF):

چارچوبی شامل پنج حوزه اصلی (شناسایی، حفاظت، شناسایی، واکنش، بازیابی) که به‌طور گسترده برای مدیریت امنیت سایبری در سازمان‌های درمانی و دانشگاهی قابل پیاده‌سازی است. [۲۴]

نتیجه‌گیری

دانشگاه‌های علوم پزشکی به عنوان نهادهای پیشران سلامت عمومی و تولید علم، باید نگاهی همه جانبه و کل‌نگر به امنیت اطلاعات داشته باشند. این امر مستلزم هم‌راستایی حکمرانی دیجیتال، فناوری هوشمند، تربیت منابع انسانی متخصص و به‌کارگیری چارچوب‌های جهانی بومی‌شده است.

منابع:

1. ISO/IEC 27001:2013 - Information security management systems.

2.Brotby, K. (2009). Information security governance: a practical development and implementation approach. John Wiley & Sons.

3.Rahim, M. J., Rahim, M. I. I., Afroz, A., & Akinola, O. (2024). Cybersecurity threats in healthcare it: Challenges, risks, and mitigation strategies. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 438-462.

4.Vaishnav, R., Panditi, M. D. D., Dhiman, V., Aarthy, C. C. J., Kumari, Y. S., & Mohiddin, M. K. (2022). Data security in healthcare management analysis and future prospects. Materials Today: Proceedings, 51, 2202-2206.

5.National Institute of Standards and Technology (NIST). Cybersecurity Framework. Cybersecurity Framework | NIST

6.ISACA. COBIT 2019 Framework COBIT | Control Objectives for Information Technologies | ISACA

7.OWASP Foundation. (2023). OWASP Foundation, the Open Source Foundation for Application Security | OWASP.

8. **شیخ ابومسعودی، روح اله، کوهی حبیبی، سحر، عطایی، مریم، و اسماعیلی، نازیلا.** (1394). **ارزیابی سیستم های مدیریت اطلاعات دانشگاه علوم پزشکی اصفهان با استفاده از استاندارد** ISO/IEC 27001. **مجله دانشگاه علوم پزشکی کرمان**، 12(3 (**پیاپی** 43))، 306- SID. https://sid.ir/paper/519363/fa .316

9.HIPAA Home | HHS.gov

10.General Data Protection Regulation (GDPR) – Legal Text

11.Kanta.fi - Kanta.fi

12.EHR Blockchain - Blockchain-based Electronic Health Records

13.NHS England » Cyber security

14.What Is SIEM? | Microsoft Security

15.What Is a Next-Generation Firewall (NGFW)? - Cisco

16.What Is EDR? Endpoint Detection and Response | Microsoft Security

17.https://www.ibm.com/think/topics/mobile-device-management

18.What is data loss prevention (DLP)? | Microsoft Security

19.https://www.ibm.com/think/topics/end-to-end-encryption

20.What is: Multifactor Authentication - Microsoft Support

21.https://www.ibm.com/think/topics/backup-disaster-recovey

22.ISO 27799:2016 - Information security management in health using ISO/IEC 27002

23.What is COBIT 5? Definition & Explanation

24.Cybersecurity Framework | NIST

دکتر طاها صمد سلطانی

دانشیار انفورماتیک پزشکی

مدیرآمار، فناوری اطلاعات و امنیت فضای مجازی دانشگاه

نویده خدائی

دانشجوی دکتری مدیریت فناوری اطلاعات

کارشناس فناوری اطلاعات

دکترامیر تراب میاندوآب

استادیار مدیریت اطلاعات سلامت

مرکزتحقیقات آموزش پزشکی

صابر درس‌خوان

کارشناس ارشد شبکه

کارشناس مسئول زیرساخت

وحید عباس‌زاده

دانشجوی PHD الکترونیک

کارشناس شبکه

جواد فرهادی

کارشناس ارشد نرم افزار

دکتر سعید سقطی‌زاد

دکتری حرفه‌ای پزشکی

رئیس دبیرخانه هیأت امنای دانشگاه

سیدمحمدحسن الهی

خوانندگان عزیزِ

«ماهنامه پالسی نو»

همواره پذیرای نظرات، پیشنهادات و انتقادات شما هستیم.

ایمیل نشریه:

anp@tbzmed.ac.ir

پرتال نشریه:

anp.tbzmed.ac.ir

مخاطبان و خوانندگان عزیز ماهنامه «**پالسی نو**» درصورتیکه در حوزه فعالیت کاری و تخصصی نشریه پیشنهاد، تجربه یا مقاله‌ای دارید به منظور طرح و انتشار در ماهنامه؛ آثار خود را به آدرس پست الکترونیکی نشریه ارسال نمایید.

A NEW PULSE

FIRST YEAR - AUGUST 2025 - NO:01

SPECIAL ISSUE:

INFORMATION SECURITY