ماهنامه

پالسی نو

A New Pulse

First year - November 2025 No:04

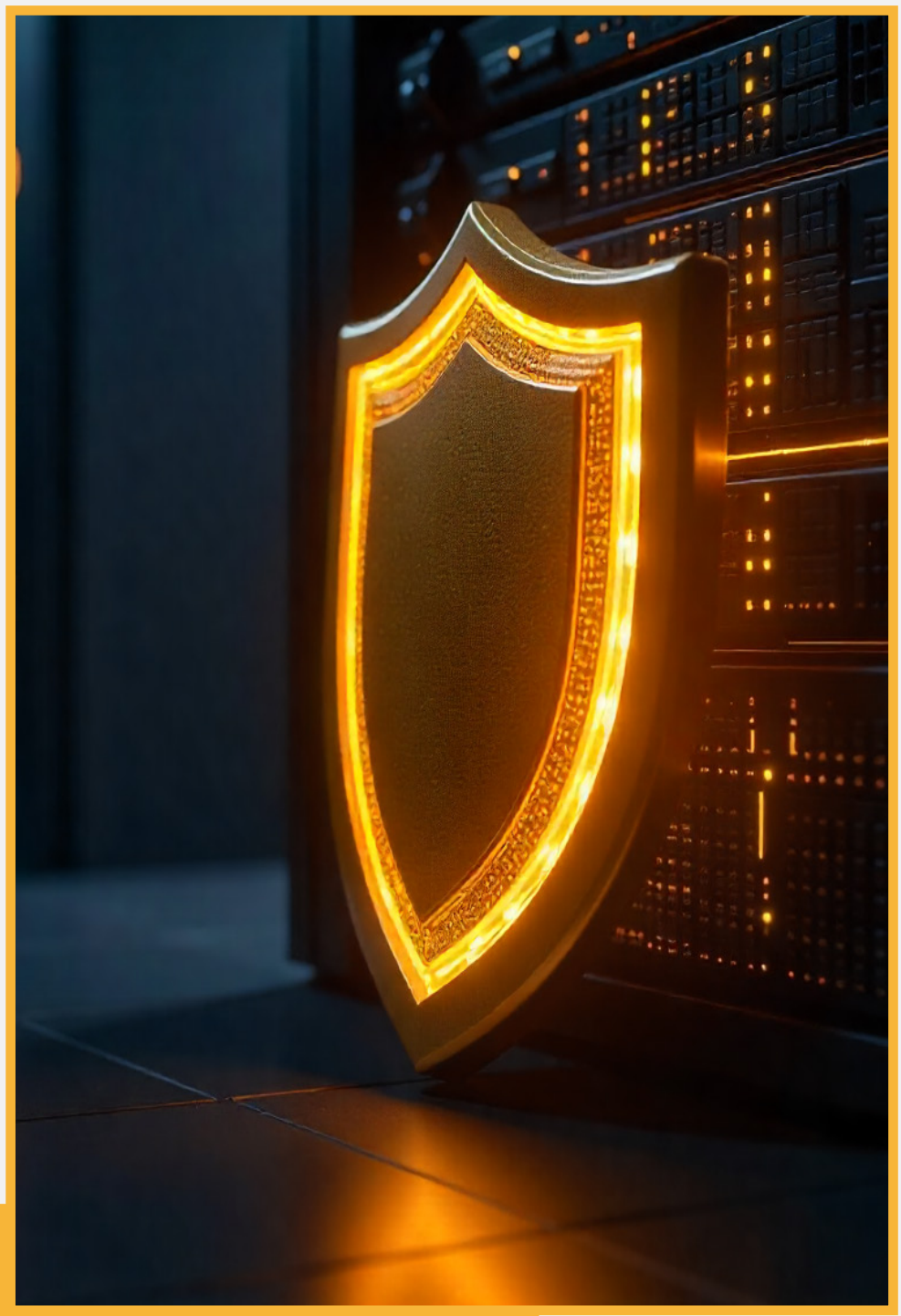
سال اول – شماره چهارم – آبان ۱۴۰۴

ویژه‌نامه: سپر خاموش در فناوری اطلاعات (پدافند غیرعامل)

... امنیت اطلاعات به دغدغه اصلی سازمان‌ها در بخش‌های مختلف تبدیل شده است. در حالی که اغلب توجه زیادی به دفاع فعال دفاع غیرفعال نیز به همان اندازه مهم است ... ص ۸

... در اتاق‌های سرور تاب‌آوری فقط یک پیکربندی یا کانفیگ نیست، بلکه هماهنگی سیستم‌ها، رویه‌ها و افرادی است که برای حفظ ثبات عملیاتی با هماهنگی با هم کار می‌کنند ... ص ۱۲

... زیرساخت غیرفعال، ستون فقرات فیزیکی را تشکیل می‌دهد که تمام لایه‌های بالایی به آن وابسته هستند. یک لایه غیرفعال انعطاف‌پذیر، نقاط شکست منفرد را کاهش می‌دهد ... ص ۱۴



مدیریت آمار، فناوری اطلاعات و امنیت فضای مجازی
دانشگاه علوم پزشکی تبریز

فهرست مطالب

سرمقاله..... ۳
نقش هوش مصنوعی و یادگیری ماشین در پشتیبانی سیستم و بهینه سازی منابع در تاب‌آوری زیرساخت‌ها..... ۴
امنیت اطلاعات و پدافند غیرعامل: نقش کارکنان فناوری اطلاعات..... ۸
دل‌نوشت برای خوانندگان پالسی نو..... ۱۱
تاب‌آوری عملی؛ اتاق‌های سرور..... ۱۲
تاب‌آوری عملی؛ تجهیزات غیرفعال شبکه..... ۱۴
ویکی‌واژه..... ۱۸
پزشکی از راه دور در نظام سلامت ایران؛ فرصتی برای عدالت، کارآمدی و تاب‌آوری..... ۲۰
آموزش فناوری اطلاعات؛ مبانی هک اخلاقی(بخش چهارم)..... ۲۱
داشبوردهای سلامت: تحولی در مدیریت و تصمیم‌گیری در حوزه سلامت..... ۲۵
استفاده از شبیه‌سازها در آموزش پزشکی: انقلابی در یادگیری و مراقبت..... ۲۷

مدیر مسئول و صاحب امتیاز: دکتر طاها صمد سلطانی

سردبیر: مهندس نویده خدائی

دبیر علمی: دکتر امیر تراب

شورای سیاستگذاری: دکتر احمدرضا جودتی، دکتر سعید اصلان آبادی، دکتر محمدرضا سیاهی، دکتر حسین عبداللهی، دکتر خسرو ادیب‌کیا، دکتر احمد کوشا، دکتر اصغر جعفری روحی، دکتر مهدی نظری.

شورای نویسندگان: مهندس صابر درسخوان، مهندس وحید عباس‌زاده، مهندس جواد فرهادی، سیدمحمدحسن الهی، سوگند حبیبی

مدیر اجرایی: دکتر سعید سقطی زاد

طراح و برنامه نویس: سیدمحمدحسن الهی

روابط عمومی: الناز هوشیان

سرمقاله

دکتر طاها صمدسلطانی
دانشیار انفورماتیک پزشکی
مدیرآمـــار، فنـــاوری اطلاعـــات و
امنیـــت فضـــای مجـــازی دانشـــگاه

تاب‌آوری علمی در دوران تحولات جهانی؛

فناوری اطلاعات و پایداری دانشگاه‌ها

جهان امروز بیش از هر زمان دیگری درگیر تحولات پیچیده و پیش‌بینی‌ناپذیر است. تغییرات سیاسی، اقتصادی و فناورانه، مرزهای سنتی علم و آموزش را دگرگون ساخته‌اند و دانشگاه‌ها را در برابر چالش‌های تازه‌ای قرار داده‌اند. در چنین شرایطی، پایداری علمی و تداوم جریان آموزش و پژوهش، به یکی از مهم‌ترین مؤلفه‌های قدرت ملی تبدیل شده است.
دانشگاه‌ها، به‌عنوان نهادهای تولید دانش و اندیشه، ناگزیرند رویکرد خود را از اتکا به منابع محدود بیرونی به سمت خوداتکایی فناورانه و استقلال دانشی سوق دهند. در این میان، فناوری اطلاعات نقشی کلیدی در حفظ و تقویت تاب‌آوری دانشگاهی ایفا می‌کند. شبکه‌های آموزشی هوشمند، زیرساخت‌های دیجیتال امن، سامانه‌های مدیریت دانش، و پلتفرم‌های یادگیری تطبیقی، ستون‌هایی هستند که استمرار آموزش، تحقیق و ارتباط علمی را حتی در شرایط ناپایدار جهانی تضمین می‌کنند.
در عصر جدید، مدیریت فناوری اطلاعات فراتر از نگهداری زیرساخت‌ها عمل می‌کند و به‌عنوان یک راهبرد کلان در حکمرانی علمی شناخته می‌شود. مفاهیمی چون معماری سازمانی دیجیتال، حاکمیت داده، امنیت سایبری، و چابکی فناورانه، به ابزارهایی برای تقویت تاب‌آوری دانشگاه‌ها بدل شده‌اند. دانشگاه‌هایی که بتوانند با بهره‌گیری از تحلیل داده‌های کلان، هوش مصنوعی، و سامانه‌های تصمیم‌یار، مسیرهای نوآورانه‌ای برای آموزش و پژوهش ترسیم کنند، در برابر بحران‌ها مقاوم‌تر خواهند بود.
در این میان، نقش فناوری اطلاعات در کشورهای تحت تحریم، از جمله ایران، اهمیتی دوچندان می‌یابد. تحریم‌ها، دسترسی به منابع علمی، نرم‌افزارهای بین‌المللی، و زیرساخت‌های ابری را محدود می‌کنند؛ اما همین محدودیت‌ها می‌توانند به فرصتی برای توسعه‌ی پلتفرم‌های بومی، تقویت استقلال دانشی، و پرورش مهارت‌های فناورانه در سطح ملی تبدیل شوند. دانشگاه‌های ایرانی با سرمایه‌گذاری در تولید نرم‌افزارهای متن‌باز، ایجاد شبکه‌های علمی داخلی، و توسعه‌ی مراکز داده‌ی ملی، می‌توانند مسیر پایداری علمی را با اتکا به توان داخلی ادامه دهند.
تحولات اخیر جهان نشان داده است که آن دسته از نظام‌های علمی که سرمایه‌گذاری هدفمندتری در حوزه‌ی فناوری اطلاعات، داده‌محوری و امنیت دیجیتال داشته‌اند، توانسته‌اند مسیر توسعه خود را با ثبات بیشتری ادامه دهند. ایجاد زیرساخت‌های ملی برای آموزش الکترونیکی، توسعه‌ی پلتفرم‌های بومی پژوهش، و آموزش مهارت‌های فناورانه به اعضای هیئت علمی و دانشجویان، از ارکان این پایداری هوشمند به شمار می‌روند.
پژوهش و آموزش در جهان جدید، تنها در پرتو مدیریت آگاهانه منابع اطلاعاتی، صیانت از دارایی‌های دانشی، و تقویت همبستگی علمی داخلی می‌تواند مسیر رشد خود را ادامه دهد. در این مسیر، مفاهیمی چون تاب‌آوری دیجیتال، استقلال زیرساختی، و حکمرانی فناورانه، به کلیدواژه‌های راهبردی بدل شده‌اند.
در نهایت، رمز موفقیت دانشگاه‌ها در دوران تحولات جهانی، در توان سازگاری، چابکی دیجیتال و اتکای هوشمند به فناوری اطلاعات نهفته است؛ همان نیروی آرام و بی‌ادعایی که ضامن پایداری و استمرار حیات علمی کشور خواهد بود، به‌ویژه در سرزمینی که تحریم‌ها نه مانع، بلکه محرکی برای نوآوری و خوداتکایی شده‌اند.

نقش هوش مصنوعی و یادگیری ماشین در پشتیبانی تصمیم و بهینه‌سازی منابع در تاب‌آوری زیرساخت‌ها

نویده خدائی
دانشجوی دکتری مدیریت فناوری اطلاعات

چکیده

در عصر تحول دیجیتال و افزایش پیچیدگی تهدیدات، تاب‌آوری زیرساخت‌های حیاتی به یکی از ارکان اصلی امنیت ملی غیرنظامی تبدیل شده است. هوش مصنوعی (AI) و یادگیری ماشین (ML) ابزارهایی نوین برای تحلیل داده‌های پیچیده، پیش‌بینی بحران‌ها، و تصمیم‌گیری هوشمند در شرایط عدم قطعیت فراهم کرده‌اند. این مقاله با هدف بررسی نقش AI و ML در پشتیبانی از تصمیم‌گیری و بهینه‌سازی منابع، به تبیین مبانی نظری، کاربردهای کلیدی و چالش‌های پیاده‌سازی این فناوری‌ها در تقویت تاب‌آوری زیرساخت‌ها می‌پردازد. نتایج نشان می‌دهد که هوش مصنوعی، با تلفیق داده، تحلیل و تصمیم، به یکی از ستون‌های اصلی حکمرانی هوشمند و مدیریت بحران آینده تبدیل خواهد شد.

مقدمه

تاب‌آوری زیرساخت‌ها به معنای توانایی سیستم‌های حیاتی در مقابله، بازیابی و سازگاری با تهدیدات طبیعی، فناورانه یا انسانی است. در دهه‌های اخیر، تغییرات اقلیمی، افزایش وابستگی به فناوری‌های دیجیتال، و ظهور تهدیدات سایبری، پیچیدگی مدیریت بحران و امنیت را چندین برابر کرده است. در چنین محیطی، تصمیم‌گیری‌های انسانی به‌تنهایی پاسخ‌گو نیستند و نیاز به ابزارهایی است که بتوانند حجم عظیمی از داده‌های متغیر را تحلیل و در کوتاه‌ترین زمان ممکن، گزینه‌های بهینه تصمیم را ارائه کنند.
هوش مصنوعی و یادگیری ماشین در این مسیر نقش حیاتی دارند. این فناوری‌ها با تحلیل داده‌های بلادرنگ، پیش‌بینی روندها، و بهینه‌سازی تخصیص منابع، به مدیران و سیاست‌گذاران کمک می‌کنند تا تصمیماتی سریع، دقیق و داده‌محور اتخاذ کنند. به‌ویژه در حوزه امنیت ملی غیرنظامی، این فناوری‌ها می‌توانند پایه‌گذار نسلی از سامانه‌های تصمیم‌یار هوشمند باشند که به ارتقای پایداری و کارایی سیستم‌های حیاتی کشور کمک می‌کنند. [۱] [۲]

مبانی نظری و چارچوب مفهومی

در ادبیات تاب‌آوری زیرساختی، سه محور کلیدی برای استفاده از هوش مصنوعی و یادگیری ماشین تعریف می‌شود:

۱. پیش‌بینی و تشخیص تهدیدات: از طریق تحلیل داده‌های حسگرها، شبکه‌های اجتماعی و سیستم‌های نظارتی برای شناسایی خطرات احتمالی پیش از وقوع بحران.

۲. پشتیبانی تصمیم: به‌کارگیری الگوریتم‌های تحلیلی و پیش‌بینی‌کننده برای ارائه راهکارهای هوشمند در شرایط عدم قطعیت.
۳. بهینه‌سازی منابع: مدیریت مؤثر منابع انسانی، لجستیکی و انرژی با هدف افزایش کارایی و کاهش اتلاف در شرایط بحرانی.

هوش مصنوعی با ایجاد مدل‌های شناختی از محیط، قادر است میان داده‌های نامتجانس (از تصاویر ماهواره‌ای تا پیام‌های اضطراری) ارتباط برقرار کند و تصمیم‌گیرندگان را در طراحی واکنش‌های مؤثر یاری دهد.

کاربردهای هوش مصنوعی و یادگیری ماشین در پشتیبانی تصمیم و بهینه‌سازی منابع

در این بخش، مهم‌ترین کاربردهای **AI** و **ML** در ارتقای تاب‌آوری زیرساخت‌ها و بهینه‌سازی منابع تبیین می‌شود.

۱. سامانه‌های هوشمند پشتیبانی تصمیم: سیستم‌های پشتیبانی تصمیم مبتنی بر هوش مصنوعی می‌توانند داده‌های بلادرنگ را از منابع مختلف جمع‌آوری و تحلیل کنند تا تصمیمات مؤثرتری اتخاذ شود.

- تحلیل بلادرنگ داده‌ها: سامانه‌های هوشمند داده‌های محیطی، ترافیکی و ارتباطی را به‌صورت لحظه‌ای تحلیل کرده و الگوهای تهدید را شناسایی می‌کنند.
- ارائه سناریوهای تصمیم: مدل‌های شبیه‌سازی هوشمند، پیامدهای مختلف تصمیم‌ها را می‌سنجند و به تصمیم‌گیرندگان پیشنهاد بهینه ارائه می‌دهند.
- کاهش خطای انسانی: یادگیری تقویتی با یادگیری از نتایج تصمیم‌های گذشته، دقت تصمیم‌سازی در بحران‌های جدید را افزایش می‌دهد [۳].

۲. پیش‌بینی و شناسایی تهدیدات: یادگیری ماشین با استفاده از داده‌های تاریخی و لحظه‌ای می‌تواند الگوهای تهدید را تشخیص داده و هشدارهای پیشگیرانه ارائه دهد.

- پایش زیرساخت‌های فیزیکی: با بینایی ماشین، ترک‌ها یا لرزش‌های غیرعادی در پل‌ها، سدها و نیروگاه‌ها شناسایی می‌شوند.
- تحلیل شبکه‌های اجتماعی: پردازش زبان طبیعی (**NLP**) به شناسایی موج‌های نگرانی، شایعات یا بحران‌های اجتماعی احتمالی کمک می‌کند.
- تشخیص حملات سایبری: مدل‌های یادگیری عمیق با تحلیل ترافیک شبکه، حملات ناشناخته را تشخیص داده و پاسخ خودکار فعال می‌کنند [۴].

۳. بهینه‌سازی تخصیص منابع در شرایط بحرانی: در بحران‌هایی که منابع محدود و نیازها متغیرند، هوش مصنوعی به عنوان ابزار برنامه‌ریزی پویا عمل می‌کند.

- تخصیص پویا: بر اساس داده‌های مکانی و نیازهای منطقه‌ای، منابع انسانی و تجهیزاتی در اولویت‌های صحیح مستقر می‌شوند.
- بهینه‌سازی زنجیره تأمین: الگوریتم‌های پیش‌بینی تقاضا مسیرهای انتقال منابع حیاتی را تعیین و از اتلاف جلوگیری می‌کنند.
- مدیریت زمان و عملیات: مدل‌های چندهدفه (**MULTI-OBJECTIVE**) میان سرعت امدادرسانی، هزینه و ایمنی تعادل برقرار می‌کنند. [۵] [۶]

۴. تاب‌آوری سایبری و امنیت زیرساخت‌های دیجیتال: زیرساخت‌های حیاتی امروز مانند شبکه برق، بیمارستان‌ها و ارتباطات، به شدت به فناوری اطلاعات وابسته‌اند. **AI** می‌تواند این سیستم‌ها را در برابر تهدیدات سایبری مقاوم

کند.

- تشخیص نفوذ: سیستم‌های مبتنی بر یادگیری عمیق، الگوهای ترافیک ناهنجار را شناسایی و از گسترش حمله جلوگیری می‌کنند.
- پاسخ خودکار: در صورت وقوع تهدید، الگوریتم‌ها مسیرهای جایگزین را فعال کرده و سیستم را بدون دخالت انسانی بازآرایی می‌کنند.
- پیش‌بینی ریسک سایبری: با تحلیل داده‌های تاریخی، احتمال بروز نقص در سیستم‌های دیجیتال پیش‌بینی می‌شود [۷].

۵. مدل‌سازی سناریوها و شبیه‌سازی هوشمند: هوش مصنوعی با استفاده از مدل‌های عامل‌محور و داده‌محور، سناریوهای بحران را شبیه‌سازی می‌کند.

- مدل‌سازی: رفتار شهروندان، سازمان‌ها و زیرساخت‌ها در برابر تهدیدات مختلف مدل‌سازی می‌شود.
- شبیه‌سازی داده‌محور: از داده‌های واقعی برای پیش‌بینی نحوه گسترش بحران‌ها (مانند آتش‌سوزی، همه‌گیری یا حملات سایبری) استفاده می‌شود.
- آموزش تصمیم‌گیرندگان: این مدل‌ها در آموزش مدیران بحران و سنجش سیاست‌های پیشنهادی بسیار مؤثرند [۸].

۶. مدیریت دانش و یادگیری سازمانی: یکی از چالش‌های اساسی در بحران‌ها، از بین رفتن دانش سازمانی است. هوش مصنوعی می‌تواند دانش حاصل از رویدادهای گذشته را مستندسازی و بازیابی کند.

- تحلیل گزارش‌ها: الگوریتم‌های **NLP** از اسناد و گزارش‌های بحران‌ها، درس‌آموخته‌ها و خطاهای انسانی را استخراج می‌کنند.
- سیستم‌های خبره: تجربه متخصصان در قالب سیستم‌های یادگیرنده ذخیره می‌شود تا در بحران‌های بعدی مورد استفاده قرار گیرد.
- یادگیری تطبیقی سازمانی: سازمان‌ها با کمک **AI** می‌توانند از خطاهای گذشته بیاموزند و فرآیندهای خود را بهبود دهند [۹].

۷. برنامه‌ریزی شهری و زیرساختی تاب‌آور: در سطح کلان، هوش مصنوعی به مدیران شهری کمک می‌کند تا ساختار شهری و زیرساخت‌ها را در برابر تهدیدات آینده مقاوم‌تر طراحی کنند.

- پیش‌بینی مصرف منابع: مدل‌های هوش مصنوعی می‌توانند روند مصرف انرژی و آب را تحلیل کرده و طرح‌های پایداری شهری ارائه دهند.
- مدیریت ترافیک و آلودگی: سیستم‌های یادگیری ماشین برای کنترل هوشمند ترافیک و کاهش انتشار آلاینده‌ها استفاده می‌شوند.
- تحلیل اثرات متقابل بحران‌ها: **AI** روابط میان سیستم‌های حیاتی (مانند برق، ارتباطات، حمل‌ونقل) را شناسایی و واکنش‌های زنجیره‌ای را پیش‌بینی می‌کند [۱۰].

چالش‌ها و ملاحظات پیاده‌سازی

اگرچه هوش مصنوعی ظرفیت‌های بی‌سابقه‌ای برای ارتقای تاب‌آوری دارد، اما ملاحظاتی نیز وجود دارد:

۱. امنیت و حریم خصوصی داده‌ها: دسترسی به داده‌های حیاتی باید با ملاحظات اخلاقی همراه باشد.
۲. شفافیت الگوریتمی: مدل‌های پیچیده گاهی فاقد توضیح‌پذیری هستند و این امر اعتماد به تصمیمات آنها

را دشوار می‌کند.

۳. وابستگی فناورانه: اتکا بیش از حد به سامانه‌های هوشمند می‌تواند در صورت بروز نقص، آسیب‌پذیری جدیدی ایجاد کند.

۴. نیاز به سیاست‌گذاری هوشمند: ایجاد چارچوب‌های حکمرانی داده و **AI** ضروری است تا استفاده از این فناوری‌ها در مسیر منافع ملی هدایت شود. [۱۱] [۱۲]

نتیجه‌گیری

هوش مصنوعی و یادگیری ماشین به‌سرعت در حال تبدیل شدن به مؤلفه‌های بنیادین حکمرانی هوشمند و امنیت غیرنظامی هستند. این فناوری‌ها با فراهم‌سازی توان تحلیل، پیش‌بینی و تصمیم‌سازی هوشمند، به مدیران و سازمان‌ها کمک می‌کنند تا منابع محدود را به‌صورت بهینه تخصیص دهند و تاب‌آوری زیرساخت‌ها را در برابر بحران‌ها افزایش دهند.

آینده امنیت و تاب‌آوری، در گرو هم‌افزایی بین انسان و ماشین است؛ جایی که هوش مصنوعی به‌عنوان بازوی تحلیلی و انسان به‌عنوان عامل اخلاقی و تصمیم‌ساز نهایی عمل می‌کند.

منابع:

1. Batarseh, F. A., & Yang, R. (2021). Data Democracy: At the Nexus of Artificial Intelligence, Software Development, and Knowledge Engineering. Elsevier.
2. Haenlein, M., Kaplan, A., Tan, C. W., Tan, B. C., & Zhang, P. (2023). Artificial Intelligence and Decision Support: The Next Frontier. MIS Quarterly.
3. Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach. Pearson.
4. Li, D., & Liu, Z. (2022). AI-based anomaly detection for infrastructure resilience. Safety Science, 150, 105703.
5. Wang, L., & Xu, J. (2023). Machine learning for resource optimization in emergency management. Journal of Safety Research, 86, 233–245.
6. Chopra, S., & Meindl, P. (2019). Supply Chain Management: Strategy, Planning, and Operation. Pearson.
7. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy.
8. Epstein, J. M. (2006). Generative Social Science: Studies in Agent-Based Computational Modeling. Princeton University Press.
9. Nonaka, I., & Takeuchi, H. (1995). The Knowledge-Creating Company. Oxford University Press.
10. Batty, M. (2021). The New Science of Cities. MIT Press.
11. Floridi, L. (2020). Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Springer.
12. European Commission. (2021). Ethics Guidelines for Trustworthy AI. Brussels.

امنیت اطلاعات و پدافند غیرعامل: نقش کارکنان فناوری اطلاعات

جواد فرهادی
کارشناس ارشد نرم افزار

چکیده

در عصری که تهدیدات امنیت سایبری رو به افزایش است، پدافند غیرعامل یکی از اجزای اساسی تاب‌آوری سازمانی را تشکیل می‌دهد. پدافند غیرعامل به آن دسته از اقدامات حفاظتی و غیرواکنشی اشاره دارد که برای کاهش آسیب‌پذیری، تشخیص نفوذ و حفظ یکپارچگی و در دسترس بودن سیستم‌های اطلاعاتی بدون نیاز به درگیری مستقیم با دشمنان طراحی شده‌اند. این مقاله به بررسی مبانی نظری پدافند غیرعامل، بررسی شیوه‌های فعلی و ترسیم نقش‌هایی که کارکنان فناوری اطلاعات باید برای پدافند غیرعامل مؤثر ایفا کنند، می‌پردازد. این مقاله همچنین چالش‌های رایج را شناسایی کرده و توصیه‌هایی برای تقویت پدافند غیرعامل از طریق ظرفیت، سیاست و فرهنگ کارکنان فناوری اطلاعات ارائه می‌دهد.

مقدمه

امنیت اطلاعات به دغدغه اصلی سازمان‌ها در بخش‌های مختلف تبدیل شده است. در حالی که اغلب توجه زیادی به دفاع فعال - اقداماتی که سعی در خنثی کردن، تعقیب یا مختل کردن مهاجمان دارند - می‌شود، دفاع غیرفعال نیز به همان اندازه مهم است. دفاع غیرفعال شامل استراتژی‌های مقدماتی و انعطاف‌پذیر است: ایمن‌سازی سیستم‌ها، اعمال کنترل‌ها، نظارت، ثبت وقایع، پشتیبان‌گیری، آموزش، مدیریت پیکربندی و ارزیابی ریسک. دفاع غیرفعال مؤثر تضمین می‌کند که هنگام وقوع حمله، آسیب به حداقل برسد، بازیابی امکان‌پذیر باشد و عملیات ضروری ادامه یابد.

نقش کارکنان فناوری اطلاعات در دفاع غیرفعال بسیار مهم است. متخصصان فناوری اطلاعات به عنوان طراحان، مجریان، نگهدارنده‌ها و ناظران سیستم‌ها، در موقعیت تصویب، اجرا و تکامل کنترل‌های امنیتی غیرفعال قرار دارند. این مقاله در پی شفاف‌سازی مسئولیت‌های کارکنان فناوری اطلاعات در دفاع غیرفعال و ارائه بهترین شیوه‌ها است تا سازمان‌ها بتوانند محیط‌های اطلاعاتی امن‌تر و انعطاف‌پذیرتری ایجاد کنند.

مرور ادبیات

دفاع غیرفعال در مقابل دفاع فعال تعریف می‌شود. به گفته دنینگ و استراوسر، اقدامات دفاع سایبری فعال و غیرفعال از این نظر متمایز هستند که دفاع غیرفعال بر مقاوم‌تر کردن دارایی‌های سایبری در برابر حمله تمرکز دارد، در حالی که دفاع فعال شامل اقدامات مستقیم علیه تهدیدات است. دفاع غیرفعال شامل رمزنگاری، ثبت وقایع، پشتیبان‌گیری، مدیریت پیکربندی، ارزیابی ریسک و آموزش است[۱]. مروری بر ابزارها و فناوری‌های عملیات دفاعی فضای مجازی، روش‌های فعال و غیرفعال را دسته‌بندی می‌کند. روش‌های غیرفعال، روش‌هایی هستند که هدفشان محافظت و شناسایی است تا پاسخ تهاجمی[۲]. مطالعات تجربی نشان می‌دهد که آگاهی، ارزیابی ریسک و کاربرد پیشگیرانه اقدامات غیرفعال با رفتار امنیتی بهتر در بین متخصصان فناوری اطلاعات همبستگی دارد. به عنوان مثال، آگاهی از تهدید و آگاهی از اقدامات متقابل، بخش قابل توجهی از رعایت پروتکل‌های امنیتی دسکتاپ در بین کارکنان فناوری اطلاعات را توضیح می‌دهد[۳].حوزه امنیت سیستم‌های اطلاعاتی دانشگاهی نیز بسیاری از کنترل‌های کوتاه‌مدت و بلندمدت پدافند غیرفعال - پدافند پیرامونی، امنیت تجهیزات، پدافند شبکه،

پدافند کاربردی - را به کارکنان فناوری اطلاعات واگذار می‌کند[۶].

پدافند غیرعامل: مؤلفه‌های کلیدی

قبل از پرداختن به نقش کارکنان فناوری اطلاعات، برشمردن مؤلفه‌های رایج پدافند غیرعامل مفید است. این مؤلفه‌ها شامل موارد زیر می‌شوند، اما محدود به آنها نیستند:

- ارزیابی ریسک و مدیریت آسیب‌پذیری: شناسایی دارایی‌ها، مدل‌های تهدید، آسیب‌پذیری‌ها؛ اسکن و ارزیابی مداوم سیستم‌ها.
- مدیریت پیکربندی و پیکربندی امن: حفظ استانداردها، وصله‌گذاری، تضمین حداقل امتیازات لازم، حذف تنظیمات پیش‌فرض.
- کنترل‌های دسترسی و احراز هویت: سیاست‌های رمز عبور، احراز هویت چند عاملی، کنترل دسترسی مبتنی بر نقش.
- ثبت وقایع، نظارت و ردیابی ممیزی: جمع‌آوری لاگ‌های سیستم و شبکه، تشخیص نفوذ (در صورت عدم پاسخگویی پیشگیرانه)، ممیزی دوره‌ای.
- پشتیبان‌گیری، بازیابی فاجعه و افزونگی: اطمینان از اینکه در صورت به خطر افتادن سیستم یا از دست دادن داده‌ها، بازیابی - یا بازیابی مجدد - امکان‌پذیر است.
- آگاهی و آموزش امنیتی: آموزش کارکنان غیر فناوری اطلاعات و کارکنان فناوری اطلاعات برای تشخیص تهدیدها، پایبندی به سیاست‌ها و گزارش مشکلات.
- سیاست، استانداردها و انطباق: ایجاد سیاست‌های سازمانی، اجرای آنها، حصول اطمینان از انطباق با قوانین یا استانداردهای صنعت.

نقش کارکنان فناوری اطلاعات در پدافند غیرعامل

کارکنان فناوری اطلاعات مسئولیت‌های متعدد و مرتبطی در اجرا و حفظ پدافند غیرعامل دارند. نقش‌های آنها را می‌توان در دسته‌های استراتژیک، عملیاتی و نظارتی دسته‌بندی کرد.

نقش	مسئولیت
استراتژیک	مشارکت در تعریف سیاست‌های امنیتی، استانداردها و تحمل ریسک.
	مشاوره به رهبری در مورد سرمایه‌گذاری در پدافند غیرعامل: به عنوان مثال ابزارها، زیرساخت‌ها، آموزش.
	نگاشت دارایی‌های حیاتی به اهداف تجاری به طوری که سطوح حفاظت با ارزش دارایی‌ها مطابقت داشته باشند.
کاربردی	پیاده‌سازی و نگهداری کنترل‌های فنی مانند مدیریت وصله‌ها، پیکربندی‌های امن، کنترل‌های دسترسی.
	اطمینان از وجود و آزمایش سیستم‌های پشتیبان‌گیری و فرآیندهای بازیابی داده‌ها.
	استقرار و نظارت بر مکانیسم‌های ثبت وقایع و هشدار؛ انجام ارزیابی‌ها و ممیزی‌های دوره‌ای آسیب‌پذیری.
	اطمینان از طراحی ایمن سیستم‌ها و شبکه‌ها (به طور پیش‌فرض ایمن).
آگاهی سازی و فرهنگ سازی	ارائه یا تسهیل برنامه‌های آموزشی و آگاهی‌بخشی برای همه کارکنان.
	ارتقاء امنیت سایبری: به عنوان مثال، شیوه‌های تعیین رمز عبور، آگاهی از فرایندهای فیشینگ.
	تشویق به گزارش مشکلات احتمالی، تهدیدات داخلی یا عدم انطباق با سیاست‌ها.
نظارت و بهبودسازی	بررسی منظم وضعیت امنیتی؛ انجام تجزیه و تحلیل شکاف‌ها و تهدیدها
	اطلاع مداوم از آسیب پذیری های جدید و تهدیدات نوظهور
	اطمینان از انطباق با استانداردها و الزامات قانونی

چالش‌های پیش روی کارکنان فناوری اطلاعات

موانع متعددی ممکن است مانع اجرای اقدامات مؤثر پدافند غیرعامل شوند:

- محدودیت‌های منابع: بودجه محدود، نیروی انسانی ناکافی یا کمبود ابزار ممکن است ظرفیت نگهداری سیستم‌های به‌روز، انجام آموزش یا انجام نظارت مستمر را کاهش دهد.
- شکاف‌های دانش و کمبود مهارت: تهدیدهای به سرعت در حال تکامل نیاز به دانش تخصصی دارند. کارکنان فناوری اطلاعات ممکن است در زمینه ارزیابی ریسک، پیکربندی امن یا فناوری‌های دفاعی جدیدتر آموزش ندیده باشند[۵].
- فرهنگ و پشتیبانی سازمانی: اگر رهبری و مدیریت ارشد امنیت اطلاعات را در اولویت قرار ندهد، ممکن است اقدامات غیرفعال نادیده گرفته شوند. به طور مشابه، کارکنان ممکن است امنیت را به عنوان یک مانع به جای یک عامل توانمندساز ببینند.
- پیچیدگی سیستم‌ها: سیستم‌های ناهمگن، زیرساخت‌های قدیمی، وابستگی‌های شخص ثالث، پیکربندی و نگهداری را دشوار می‌کنند و سطح حمله را افزایش می‌دهند.
- شکاف سیاست-عمل: حتی زمانی که سیاست‌ها وجود دارند، تضمین پایبندی مداوم چالش برانگیز است؛ مکانیسم‌های اجرایی ممکن است ضعیف یا با کمبود منابع مواجه باشند.

توصیه‌ها

برای تقویت توانایی کارکنان فناوری اطلاعات در پدافند غیرعامل، سازمان‌ها باید موارد زیر را در نظر بگیرند:

۱. ظرفیت‌سازی: سرمایه‌گذاری در آموزش مداوم، صدور گواهینامه و توسعه مهارت برای کارکنان فناوری اطلاعات، به ویژه در زمینه‌های اسکن آسیب‌پذیری، طراحی امن، ارزیابی ریسک و ثبت وقایع.
۲. منابع کافی: اطمینان از نیروی انسانی، ابزار و بودجه کافی برای فعالیت‌های پدافند غیرعامل (وصله‌سازی، پشتیبان‌گیری، ممیزی، نظارت).
۳. نهادینه‌سازی سیاست امنیتی: تدوین سیاست‌های روشن و اجرای آنها؛ ادغام امنیت در فرآیندهای تجاری؛ شفاف‌سازی پاسخگویی.
۴. اولویت‌بندی مبتنی بر ریسک: اولویت‌بندی محافظت از حیاتی‌ترین دارایی‌ها؛ انجام ارزیابی‌های منظم ریسک؛ تمرکز بر آسیب‌پذیری‌های با تأثیر بالا در ابتدا.
۵. به‌کارگیری دفاع لایه‌ای (دفاع در عمق): استفاده از چندین کنترل غیرفعال هم‌پوشان به طوری که عدم موفقیت یکی منجر به نقض فاجعه‌بار نشود.
۶. ارتقاء فرهنگ و آگاهی امنیتی: آموزش منظم، مانورها، ارتباطات؛ تشخیص و پاداش انطباق؛ تشویق گزارش‌دهی و شفافیت.
۷. نظارت و بررسی مداوم: حسابرسی، تحلیل لاگ، اسکن آسیب‌پذیری، تست نفوذ، بررسی‌های پس از حادثه.

نتیجه‌گیری

پدافند غیرفعال همچنان یک ستون اساسی در معماری امنیتی گسترده‌تر هر سازمانی است. اگرچه به خودی خود مانع از همه حملات نمی‌شود، اما به طور قابل توجهی خطر را کاهش می‌دهد، آسیب را محدود می‌کند و امکان بازیابی را فراهم می‌کند. کارکنان فناوری اطلاعات نقش محوری در طراحی و عملیاتی کردن اقدامات پدافند غیرفعال دارند. مسئولیت‌های آنها شامل مشاوره استراتژیک، اجرای کنترل‌های فنی، تقویت آگاهی و تضمین بهبود مستمر است. غلبه بر چالش‌های منابع، مهارت‌ها و فرهنگ سازمانی حیاتی است. سازمان‌هایی که از کارکنان فناوری اطلاعات خود در این نقش‌ها پشتیبانی می‌کنند، در حفظ محرمانگی، یکپارچگی، در دسترس بودن و تاب‌آوری سیستم‌های اطلاعاتی خود در موقعیت بهتری قرار خواهند گرفت.

منابع:

[1]. Denning, D. E., & Strawser, B. (2013). Framework and Principles for Active Cyber Defense. Naval Postgraduate School.

[2]. National Research Council. (1999). Realizing the Potential of C4I: Fundamental Challenges. Washington, DC: The National Academies Press.

[3]. Goethals, P. L., & Hunt, M. E. (2019). A review of scientific research in defensive cyberspace operation tools and technologies. Journal of Cyber Security Technology, 3(1), 1-46.

[4]. Hanus, M. D., & Wu, A. (2018). The impact of security awareness on information technology professionals' behavior. Computers & Security, 79, 68-79.

[5]. The cybersecurity workforce and skills. (2021). Computers & Security, 100, 102080.

[6]. MePRiSIA: risk prevention methodology for academic information systems. (n.d.). Redalyc.

Redalyc

دل نوشت

برای خوانندگان پالسی نو

سید محمدحسن الهی

در هر سازمانی، پاسبانانی وجود دارند که در سکوت کار می‌کنند، نام آنها به ندرت در جلسات شنیده می‌شود و تلاش‌های آنها اغلب از چشم پنهان است. با این حال، بدون آنها، هیچ سیستمی زنده نمی‌ماند، هیچ خدمتی ادامه نمی‌یابد و هیچ استراتژی‌ای پایدار نمی‌ماند. این پاسبانان، کارمندان فناوری اطلاعات هستند و نقش آنها در حوزه پدافند غیرعامل چیزی کمتر از سپر نامرئی سازمان نیست.

پدافند غیرعامل بر روی دیوارهای بتنی یا پشت دروازه‌های فولادی و یا در ژرفناهای پنهان ساخته نشده است. این پدافند بر اساس تاب‌آوری، آمادگی و قدرت دانشی ساخته شده است که هرگز نباید شکست بخورد. در این زمینه، کارمندان فناوری اطلاعات در خطوط مقدم ایستاده‌اند، اگرچه به ندرت دیده می‌شوند. میدان نبرد آنها شبکه است، زره آنها دانش است و سلاح آنها هوشیاری است.

وقتی سیستم‌ها مورد حمله قرار می‌گیرند، وقتی داده‌ها در معرض خطر واقع می‌شوند، این چهره‌های اتاق‌های مدیران نیستند که برای دفاع از تهاجم صف می‌بندند. این کارکنان فناوری اطلاعات هستند که اغلب در سکوت، شریان حیاتی سازمان را که همانا داده و خدمات و ارتباطات است؛ حفظ می‌کنند. آنها هرگز پرچم پیروزی را بالا نمی‌برند آنها صدایی برای فریاد زدن ندارند. آنها اصلا تریبونی در اختیار ندارند اما کارشان و عملکردشان بلندتر از هر کلمه‌ای سخن می‌گوید و فریاد می‌زند.

حقیقت بایستی توسط مدیران با گرمی و احساس و احترام پذیرفته شود و حقیقت اینست که بدون کارمندان فناوری اطلاعات، پدافند غیرعامل در حوزه فناوری اطلاعات مفهومی توخالی و پوچ خواهد بود. هوشیاری آنها تضمین می‌کند که یک حمله سایبری موسسه را هرگز فلج نخواهد کرد. دوراندیشی آنها تضمین می‌کند که حتی در بحران، دانشگاه محکم و استوار بایستد. آنها محافظان ثبات و پایداری در عصری هستند که جنگ‌ها دیگر فقط با سلاح‌ها انجام نمی‌شوند، بلکه با داده‌ها، سیستم‌ها و دانش روی می‌دهند.

بنابراین، اجازه دهید به همه و با وضوح و با صدای بلند گفته شود:

سپر دفاعی فقط مربوط به ساختارهای قابل مشاهده و امنیت فیزیکی و... نیست. روح آن در دستان متخصصان فناوری اطلاعات است که بی‌صدا در هر گوشه‌ای از سیستم دانشگاه، مستقر هستند. آنها صرفاً کارکنان عادی نیستند آنها پاسبانان بقا و حیات سیستم هستند.

لطفا بگذارید احترامی که شایسته آن هستند به آنها داده شود و نقش آنها نه در پس‌زمینه، بلکه به عنوان ستون فقرات دفاع دانشگاه شناخته شود زیرا که در پسِ زحمات آنها، قدرت همگی‌مان نهفته است.

پس بیایید سقف‌ها را بشکافیم و از این پَس طرحی نو در اندازیم و به گونه ای دیگر ببینیم... آنگونه که هست و آنگونه که باید باشد... این **پالسی نو** هست.

تاب‌آوری عملی؛ اتاق‌های سرور

صابر درس‌خوان
کارشناس ارشد شبکه
کارشناس مسئول زیرساخت

مقدمه

تاب‌آوری در فناوری اطلاعات (IT) به ظرفیت سیستم‌ها، زیرساخت‌ها و اپراتورهای انسانی برای پیش‌بینی، جذب، بازیابی و سازگاری با رویدادهای مخرب اشاره دارد (NIST، 2022) . در اتاق‌های سرور تاب‌آوری فقط یک پیکربندی یا کانفیگ نیست، بلکه هماهنگی سیستم‌ها، رویه‌ها و افرادی است که برای حفظ ثبات عملیاتی با هماهنگی با هم کار می‌کنند.
از آنجایی که سازمان‌های مدرن به طور فزاینده‌ای به دسترسی بدون وقفه به داده‌ها وابسته هستند، تاب‌آوری بسیار مهم شده است. یک خرابی واحد در یک محیط سرور می‌تواند ارتباطات، ارائه خدمات و اعتماد نهادی را فلج کند (Gartner Re-search، 2023). بنابراین، تاب‌آوری در اتاق‌های سرور صرفاً یک چالش فنی نیست، بلکه یک اولویت استراتژیک است که ارتباط نزدیکی با اهداف و تداوم فعالیت و امنیت اطلاعات دارد (ISO، 2018).

مبانی تاب‌آوری فنی

تاب‌آوری در اتاق سرور با قابلیت اطمینان زیرساخت آغاز می‌شود. یک اتاق سرور صحیح مهندسی‌شده، افزونگی، تحمل خطا و کنترل محیطی را در بر می‌گیرد (BSI، 2019). اجزای حیاتی - مانند منبع تغذیه بدون وقفه (UPS)، سیستم‌های خنک‌کننده - یک معماری دفاعی در برابر اختلالات پیش‌بینی‌نشده ایجاد می‌کنند.
حفاظت از داده‌ها و افزونگی، لایه منطقی تاب‌آوری را تشکیل می‌دهند. همانطور که اسمیت (۲۰۲۱) تأکید می‌کند، تکثیر و آینه‌سازی داده‌های بلادرنگ در مکان‌های جغرافیایی متنوع، ضروری هستند، نه اختیاری. این استراتژی‌ها، از دست دادن داده‌ها را به حداقل می‌رسانند و بازیابی سریع را در هنگام خرابی‌ها امکان‌پذیر می‌کنند. علاوه بر این، تأیید پشتیبان‌گیری منظم و آزمایش بازیابی فاجعه (DR)، اقدامات امنیتی غیرفعال را به شیوه‌های تاب‌آوری فعال تبدیل می‌کنند (ISO،2018).
نظارت پیشگیرانه یکی دیگر از جنبه‌های حیاتی است. به گفته تان و رودریگز (۲۰۲۲)، سیستم‌های نظارت هوشمند مجهز به تجزیه و تحلیل پیش‌بینی‌کننده می‌توانند انحرافات در عملکرد و پایداری محیطی را قبل از تبدیل شدن به خرابی‌های بحرانی شناسایی کنند. با ادغام سیستم‌های اتوماسیون و هشداردهنده، سازمان‌ها زمان پاسخ را کاهش داده و وضعیت تاب‌آوری خود را تقویت می‌کنند.

امنیت به عنوان هسته تاب‌آوری

تاب‌آوری بدون امنیت قوی نمی‌تواند وجود داشته باشد. کنترل دسترسی فیزیکی، تأیید بیومتریک، نظارت و حسگرهای محیطی به طور جمعی از لایه فیزیکی اتاق سرور محافظت می‌کنند (BSI، 2019). در همین حال، اقدامات امنیت سایبری - مانند تقسیم‌بندی شبکه، تشخیص نفوذ و سیاست‌های اعتماد صفر - دفاع دیجیتال را تقویت می‌کنند (NIST، ۲۰۲۲).
این لایه‌های امنیتی به صورت همزیست هستند: نقض‌های فیزیکی می‌توانند سیستم‌های دیجیتال را به خطر بیندازند و برعکس. بنابراین، تاب‌آوری نیاز به یک دیدگاه جامع دارد که در آن ایمنی محیطی، یکپارچگی فیزیکی و حفاظت سایبری جدایی‌ناپذیر هستند. نقض در هر بُعدی، کل اکوسیستم تاب‌آوری را تهدید می‌کند.

بُعد انسانی تاب‌آوری

اگرچه فناوری زیرساخت تاب‌آوری را تشکیل می‌دهد، اما انسان‌ها هوش و انضباط آن را فراهم می‌کنند. متخصصان فناوری اطلاعات در اتاق‌های سرور مظهر هوشیاری، دقت و پاسخگویی هستند. آگاهی، آموزش و مستندسازی مداوم آنها تضمین می‌کند که برنامه‌های تاب‌آوری از ساختارهای نظری فراتر رفته و به عمل زنده تبدیل شوند.
همانطور که گارتنر ریسرچ (۲۰۲۳) اشاره می‌کند، عامل انسانی همچنان متغیر تعیین‌کننده در سرعت و دقت بازیابی است. رویه‌های عملیاتی استاندارد، چارچوب‌های مدیریت حادثه و پروتکل‌های ارتباطی تیمی، همگی منعکس‌کننده سهم انسان در

تاب‌آوری هستند. علاوه بر این، فرهنگ یادگیری مداوم - که در آن هر حادثه بررسی و هر ضعف اصلاح می‌شود - تجربه را به قدرت سازمانی تبدیل می‌کند (اسمیت، ۲۰۲۱).
بنابراین، عمل تاب‌آوری به همان اندازه که به ماشین‌آلات مربوط است، به طرز فکر نیز مربوط می‌شود. یک تیم آموزش‌دیده، که با رویه‌های روشن هدایت می‌شود و برای اقدام قاطعانه توانمند است، سازگارترین شکل تاب‌آوری را تجسم می‌بخشد.

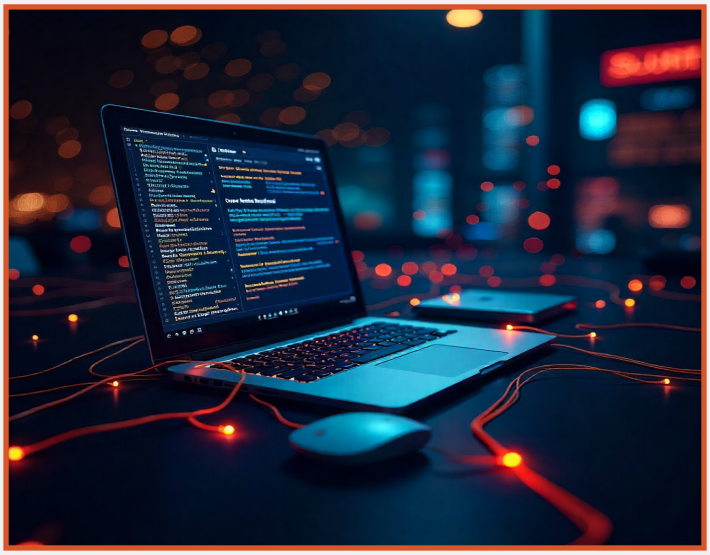
تاب‌آوری به عنوان یک فرآیند پویا و در حال تکامل

تاب‌آوری یک دستاورد ایستا نیست، بلکه یک فرآیند مداوم است. استاندارد ISO ۲۲۳۰۱ تداوم کسب‌وکار و تاب‌آوری را به عنوان "فعالیت‌های بهبود مستمر همسو با جهت استراتژیک سازمان" تعریف می‌کند (ISO، ۲۰۱۸، صفحه ۱۲). در اتاق سرور، این اصل از طریق آزمایش منظم، شبیه‌سازی خرابی‌ها و ارزیابی پس از حادثه آشکار می‌شود. تکامل فناوری، از مجازی‌سازی تا ادغام در فضاهای ابری، دائماً استراتژی‌های تاب‌آوری را تغییر شکل می‌دهد. زیرساخت‌های ترکیبی به معماری‌های پشتیبان

جدید و پروتکل‌های بازیابی چند پلتفرمی نیاز دارند (Tan & Rodriguez, 2022). بنابراین، تاب‌آوری باید همگام با نوآوری تکامل یابد - نه تنها آسیب‌پذیری‌های فعلی، بلکه خطرات آینده را نیز پیش‌بینی کند.
تاب‌آوری واقعی در نهایت نه با عدم وجود خرابی، بلکه با سرعت و یکپارچگی بازیابی سنجیده می‌شود. مقاوم‌ترین اتاق‌های سرور، اتاق‌هایی هستند که اختلال را به فرصت تبدیل می‌کنند و به طور مداوم سیستم‌ها و کارکنان خود را از طریق درس‌های آموخته شده اصلاح می‌کنند.

نتیجه‌گیری

تاب‌آوری در عمل در اتاق‌های سرور، هم یک نظم فناوری



و هم یک تعهد اخلاقی را نشان می‌دهد. این امر از ضربان قلب عملیات سازمانی - جریان داده‌ها، ارتباطات و اعتماد - محافظت می‌کند. متخصصان فناوری اطلاعات از طریق برنامه‌ریزی آگاهانه، دفاع لایه‌ای و هوشیاری انسانی، از وعده خاموش تداوم حمایت می‌کنند.
هر چراغ سوسو زننده در یک رک سرور، نماد تعامل مداوم بین آسیب‌پذیری و محافظت است. پشت هر سیستم پایدار، تیمی ایستاده است که غیرقابل پیش‌بینی‌ها را پیش‌بینی می‌کند، شکسته‌ها را بازیابی می‌کند و ضعیف‌ها را تقویت می‌کند. در آن فضای نادیده‌ی فن‌ها و فیبرهای نوری، تاب‌آوری یک اصطلاح انتزاعی نیست - بلکه روزانه زیسته، آزمایش شده و اثبات می‌شود.

منابع:

- British Standards Institution. (2019). BS EN 50600: Information technology – Data centre facilities and infrastructure. BSI. https://doi.org/10.3403/BSEN50600
- Gartner Research. (2023). Building resilient IT infrastructure for the digital enterprise. Gartner, Inc.
- International Organization for Standardization. (2018). ISO 22301: Business continuity management systems – Requirements. ISO.
- National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
- Smith, J. (2021). Resilient IT infrastructure: Strategies for sustainable operations. IT Journal of Systems Management, 15(4), 112–129.
- Tan, L., & Rodriguez, A. (2022). Predictive resilience: Monitoring and adaptation in modern data centers. Journal of Information Systems Engineering, 8(2), 45–59.

تاب‌آوری عملی؛ تجهیزات غیرفعال شبکه

وحید عباس‌زاده
دانشجوی PHD الکترونیک
کارشناس شبکه

مقدمه

تاب‌آوری در لایه فیزیکی شبکه‌های ارتباطی، جزء اساسی قابلیت اطمینان کلی شبکه است. در حالی که عناصر فعال شبکه (سوئیچ‌ها، روترها، سرورها) توجه زیادی را به خود جلب می‌کنند، تجهیزات شبکه غیرفعال - کابل‌های فیبر، پچ پنل‌ها، کانکتورها، محفظه‌های اتصال، لوله‌ها و تقسیم‌کننده‌های نوری غیرفعال - بستری را فراهم می‌کنند که خرابی آن اغلب باعث اختلال گسترده در سرویس می‌شود تاب‌آوری در شبکه‌سازی معمولاً در لایه‌های سرویس و پروتکل مورد بحث قرار می‌گیرد، با این حال زیرساخت غیرفعال، ستون فقرات فیزیکی را تشکیل می‌دهد که تمام لایه‌های بالایی به آن وابسته هستند. یک لایه غیرفعال انعطاف‌پذیر، نقاط شکست منفرد را کاهش می‌دهد، آسیب فیزیکی را محدود می‌کند و امکان بازیابی سریع پس از حوادثی مانند حفاری‌های تصادفی، آتش‌سوزی، سیل و خرابی اتاق تجهیزات را فراهم می‌کند. محیط عملیاتی مدرن نیازمند توجه مجدد به تاب‌آوری غیرفعال است که طراحی توپولوژی، حفاظت فیزیکی سخت‌گیرانه و نظم عملیاتی را با هم ترکیب می‌کند.

مرور ادبیات و استانداردها

- رویکردهای توپولوژی و معماری: تحقیقات اخیر، توپولوژی‌های درختی، ستاره‌ای، حلقه‌ای مقایسه می‌کند و نشان می‌دهد که انتخاب‌های توپولوژیکی به طور قابل توجهی بر قابلیت بقا و استفاده از منابع در سناریوهای خرابی تأثیر می‌گذارند. طرح‌های ترکیبی و مبتنی بر حلقه اغلب ویژگی‌های بازیابی بهتری را در مقایسه با معماری‌های تک درختی ارائه می‌دهند. توپولوژی‌های ترکیبی نوظهور، برای ارائه قابلیت بقا بهبود یافته برای شبکه‌ها پیشنهاد شده‌اند.
- استانداردها و شیوه‌های اندازه‌گیری: استانداردهای نصب، اندازه‌گیری و تأیید کابل‌کشی، مبنایی را برای اطمینان از اینکه اجزای غیرفعال نصب شده انتظارات عملکرد و قابلیت اطمینان را برآورده می‌کنند، فراهم می‌کنند. خانواده **ISO/IEC 14763** (شامل نسخه ۲۰۲۱ و اصلاحیه) اندازه‌گیری و راهنمایی عملیاتی را برای کابل‌کشی مشخص می‌کند. رعایت چنین استانداردهایی، نقص‌های نهفته‌ای را که بعداً به صورت قطعی برق ظاهر می‌شوند، کاهش می‌دهد.
- تحقیقات عملیاتی و ادبیات بهترین شیوه‌ها: مطالعات و راهنمایی‌های صنعتی همچنان بر نقش مدیریت کابل، کنترل شعاع خمش و انتخاب لوازم جانبی (سینی‌های اتصال، پچ پنل‌ها) در حفظ عملکرد بهینه و به حداقل رساندن آسیب‌های تصادفی در حین تعمیر و نگهداری تأکید دارند. راهنمایی‌های عملی صنعتی (به عنوان مثال، یادداشت‌های فنی فروشندگان تجهیزات) با تبدیل اقدامات تاب‌آوری به شیوه‌های قابل نصب، کار را تکمیل می‌کنند.

تهدیدات مربوط به تاب‌آوری تجهیزات غیرفعال

زیرساخت‌های غیرفعال در برابر چندین دسته تهدید آسیب‌پذیر هستند:
۱. آسیب فیزیکی (حفاری/حفاری، جوندگان، ساخت و ساز)
۲. عوامل استرس‌زای محیطی (سیل، گرما، اشعه ماوراء بنفش، قرار گرفتن در معرض مواد شیمیایی)
۳. عوامل انسانی (برچسب‌گذاری ضعیف، سوکت‌زنی نادرست، خمیدگی بیش از حد کابل)
۴. پیری و تخریب مواد (سایش کانکتور، شکنندگی روکش کابل).

هر تهدید دارای احتمال و پیامدهای متفاوتی است. کنترل‌های طراحی و عملیاتی باید بر اساس ریسک اولویت‌بندی شوند. به عنوان مثال، حفاری‌های تصادفی رویدادهایی با تأثیر بالا هستند که با تنوع مسیر و عمق دفن کاهش می‌یابند، در حالی که عوامل انسانی تا حد زیادی با مستندسازی، برچسب‌گذاری و استانداردهای کار کاهش می‌یابند.

اقدامات عملی برای بهبود تاب‌آوری

- توپولوژی و تنوع فیزیکی: تنوع فیزیکی (کانال‌های جداگانه، مسیرهای متمایز) مانع از آن می‌شود که یک حادثه ساختمانی واحد، تمام ارتباطات بین نقاط را قطع کند. در جایی که تنوع کامل امکان‌پذیر نیست، مسیرهای منطقی (**Logical Path**) متنوع در کانال‌های داخلی یا دسته‌های مجرا، خطر خرابی همبسته را کاهش می‌دهند. کارهای تجربی و شبیه‌سازی نشان می‌دهد که طرح‌های هیبریدی، تلفات کل را در خرابی‌ها کاهش می‌دهند.
- حفاظت فیزیکی و قرارگیری دارایی‌ها در شرایط سخت: کابل‌های حیاتی با مسافت طولانی باید در اعماق محافظت‌شده، با محفظه بتنی یا حفاری جهت‌دار در جایی که خطر حفاری مکرر توسط شخص ثالث وجود دارد، قرار گیرند. تجهیزات غیرفعال (اتصالات، پچ پنل‌ها) که در اتاق‌ها قرار می‌گیرند باید دارای امنیت فیزیکی مناسب، موانع سیل و نظارت بر محیط (دما، رطوبت، تشخیص نشت) باشند.
- نصب با کیفیت، کانکتورها و مدیریت کابل: در زمان آزمایش پذیرش کابل‌کشی، از استانداردهای **ISO/IEC 14763-4** و استانداردهای معادل **IEC/ANSI** برای تأیید پارامترهای سر تا سر و عملکرد کانکتورها استفاده گردد. عدم تأیید باعث ایجاد خطاهای پنهان می‌شود. مسیریابی مناسب، مدیریت شل شدن و استفاده از محدودکننده‌های خمش، فیبرهای نوری را از تلفات خمش محافظت می‌کند. راهنماهای تولیدکننده بر حفظ حداقل شعاع خمش و استفاده از لوازم جانبی مناسب برای فیبر تأکید دارند. نمودارسازی دقیق، برچسب‌گذاری و سوابق دارایی قابل جستجو، خطای انسانی را در طول نگهداری به شدت کاهش می‌دهد و مداخلات سریع‌تر و ایمن‌تری را امکان‌پذیر می‌کند.
- نظارت، آزمایش و شیوه‌های پیش‌بینی: تست‌های زمان‌بندی‌شده در بازه زمان (**OTDR**) و بررسی‌های کانکتور/اتصال می‌توانند تخریب را قبل از خرابی فاجعه‌بار شناسایی کنند. اندازه‌گیری باید از استانداردهای پیکربندی و گزارش‌دهی آزمایش پیروی کند.
- ظرفیت اضافی و تخریب قابل تحمل: فیبرهای یدکی در مجراهای کابل در نظر گرفته شود و از پچ پنل‌های ماژولار استفاده گردد که امکان پیکربندی مجدد در زمان مورد نیاز را فراهم می‌کنند. این امر امکان تغییر مسیر ترافیک را بر روی ظرفیت فیزیکی موجود بدون اتصال فوری میدانی فراهم می‌کند. حالت‌های تخریب سرویس قابل قبول تعریف شود و رویه‌هایی را برای انتقال سرویس گیرندگان به مسیرهای جدید تا زمان تعمیرات پیش‌بینی گردد.
- انعطاف‌پذیری زنجیره تأمین و چرخه عمر: در صورت امکان، کانکتورها و پنل‌های ماژولار استانداردی انتخاب گردد تا از وابستگی به یک فروشنده و تولید کننده و زمان طولانی تعویض جلوگیری شود. شوک‌های زنجیره تأمین، نیاز به تأمین منابع جایگزین و موجودی قطعات برای اجزای غیرفعال حیاتی را برجسته می‌کند.

توصیه‌ها – یک چک لیست عملی برای تاب‌آوری

۱. طراحی برای تنوع: در صورت امکان، مسیرهای فیزیکی جداگانه برای لینک‌های حیاتی در نظر گرفته و پیاده سازی شود. معماری‌ها یا توپولوژی‌های ترکیبی برای شبکه‌های داخلی برنامه‌ریزی گردد.
۲. از استانداردهای تایید شده پیروی شود. برای آزمایش‌های پذیرش و مستندسازی نتایج آزمایش، استاندارد **ISO/IEC 14763-4** توصیه می شود.

۳. از نظر فیزیکی همواره محافظت لازم انجام شود. برای مسیرهای آسیب‌پذیر از کانال‌های دفنی، کانال‌های داخلی، کانال‌های دارای نوار هشدار، جداسازی کانال و محفظه‌های اتصال گردد.
۴. مدیریت کابل ها انجام شود. سیاست‌های میزان خمش، شلی طول مناسب، مراقبت در رک‌ها و اتصالات اعمال شود.
۵. در نهایت نظارت و آزمایش دائمی و مداوم انجام شود. به صورت دوره‌ای و پریودیک مسیر کابلها بررسی گردد و از صحت مسیر و اتصالات اطمینان حاصل گردد. همچنین وضعیت فیزیکی کابل ها و اتصالات نظیر پوسیدگی و یا حملات حیوانات جونده بررسی شود.
۶. قطعات یدکی در نظر گرفته شود. پچ کوردها، آداپتورها، کیت‌های اتصال و ... یدکی موجود و در دسترس باشد. همچنین کانال‌های تدارکات سریع و تامین منابع و مجوزها تعریف و در دسترس باشد. دفترچه‌های راهنمای تعمیرات (وظایف بازیابی فیزیکی گام به گام) ایجاد و تمرین‌های بازیابی انجام شود.

نتیجه‌گیری

تاب‌آوری تجهیزات شبکه غیرفعال نیازمند ترکیبی از مهندسی خوب، پایبندی به استانداردها و عملیات منظم است. انتخاب توپولوژی، حفاظت فیزیکی و مدیریت دقیق کابل، استراتژی‌هایی موثر هستند. اندازه‌گیری و نظارت منظم، همراه با ظرفیت اضافی و رویه‌های بازیابی خوب، احتمال و تأثیر خرابی‌های فیزیکی را کاهش می‌دهد. با به‌کارگیری بینش‌های تحقیقاتی معاصر در کنار استانداردهای تعیین‌شده و بهترین شیوه‌های میدانی، صاحبان شبکه می‌توانند به‌طور قابل‌توجهی قابلیت بقا و تداوم خدمات زیرساخت خود را بهبود بخشند.

منابع:

- Kumari, M., Sharma, R., & Sheetal, A. (2023). Wheel-Based MDM-PON System Incorporating OCDMA for Secure Network Resiliency. Photonics, 10(3), 329. https://doi.org/10.3390/photonics10030329
- Zentani, A., Zulkifli, N., & Ramli, A. (2022). Network resiliency and fiber usage of tree, star, ring and wheel based wavelength division multiplexed passive optical network topologies: A comparative review. Optical Fiber Technology, 73, 103038. https://doi.org/10.1016/j.yofte.2022.103038
- ISO/IEC. (2021). ISO/IEC 14763-4:2021 — Information technology — Implementation and operation of customer premises cabling — Part 4: Measurement of end-to-end links, modular plug terminated links and direct attach cabling (2nd ed.). International Organization for Standardization. https://www.iso.org/standard/82769.html
- ISO/IEC. (2022). ISO/IEC 14763-4:2021/Cor 1:2022 — Technical corrigendum 1 to ISO/IEC 14763-4:2021. https://www.iso.org/standard/85690.html
- Chatsworth Products (Blog). (2024, November 4). Fiber protection best practices: How to preserve cable performance and longevity. Chatsworth. https://www.chatsworth.com/en-us/resources/blogs/2024/space-saving-infrastructure-solutions-for-retail
- Catheria / ANETFiber. (2024, March 27). Fiber optic patch panel types & best practices. https://catheria.anetfiber.com/fiber-optic-patch-panel-types-best-practices/
- Ananth, C. (2024, Aug 19). Effective data center cable management: Ensuring optimal performance and reliability [Conference paper]. ResearchGate. https://www.researchgate.net/publication/383232272_Effective_Data_Center_Cable_Management_Ensuring_Optimal_Performance_and_Reliability
- IEC Webstore. (2021). ISO/IEC 14763-4:2021 (E). International Electrotechnical Commission. https://webstore.iec.ch/en/publication/65030
- Xiong, W. (2025). Semiconductor supply chain resilience and disruption: A review. International Journal of Production Research. (Discusses supply chain impacts and the importance of parts strategy.) https://doi.org/10.1080/00207543.2024.2387074

خطاب به مخاطبان «پالسی نو»

اکنون که چهارمین شماره «**پالسی نو**» در اختیار شماست، بیش از پیش به همراهی و همفکری شما دلگرمیم. رسالت این نشریه فراتر از انتشار چند مقاله و یادداشت است؛ ما باور داریم که «**پالسی نو**» تنها در پرتو تعامل سازنده با شما معنا پیدا می‌کند.

از شما مخاطبان گرامی دعوت می‌کنیم با نقدهای سازنده، پیشنهادهای ارزشمند و مطالب ارزنده خود، در مسیر پویاتر شدن این رسانه شریک باشید. ما صمیمانه مشتاقیم تا دیدگاه‌ها و دغدغه‌های شما را بشنویم و آنها را در شماره‌های آینده بازتاب دهیم.

بیایید با هم نشریه‌ای بسازیم که نه تنها بازتاب‌دهنده اندیشه‌ها و تجربیات امروز باشد، بلکه چراغی برای فردای روشن‌تر در حوزه نوآوری، فناوری و سیاست‌گذاری نیز گردد.

«**پالسی نو**» خانه‌ای است برای گفت‌وگوی شما

آدرس وب سایت نشریه:

anp.tbzmed.ac.ir

آدرس ایمیل برای ارسال مطالب:

anp@tbzmed.ac.ir

صفحه اینستاگرام:

anew_pulse

ویکی واژه

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

الگوریتم‌های رمز نگاری

الگوریتم‌های رمزنگاری، توابع ریاضی هستند که برای درهم‌ریختگی داده‌ها و تبدیل آنها به یک متن غیرقابل خواندن، استفاده می‌شوند. این الگوریتم‌ها ستون فقرات امنیت داده‌های مدرن هستند و تضمین می‌کنند که اطلاعات حساس حتی اگر توسط اشخاص غیرمجاز رهگیری شوند، محرمانه باقی می‌مانند. دو دسته اصلی وجود دارد: الگوریتم‌های کلید متقارن، که از یک کلید برای رمزگذاری و رمزگشایی استفاده می‌کنند (مثلاً **AES، DES**) و الگوریتم‌های کلید نامتقارن، که از یک جفت کلید استفاده می‌کنند - یک کلید عمومی برای رمزگذاری و یک کلید خصوصی برای رمزگشایی (مثلاً **RSA، ECC**). قدرت یک الگوریتم رمزگذاری به پیچیدگی عملیات ریاضی و طول کلید بستگی دارد، کلیدهای طولانی‌تر عموماً امنیت قوی‌تری را فراهم می‌کنند.

الگوریتم‌های کلید متقارن عموماً برای رمزگذاری حجم زیادی از داده‌ها سریع‌تر و کارآمدتر هستند و آنها را برای کارهایی مانند ایمن‌سازی ترافیک شبکه مناسب می‌کنند. الگوریتم‌های کلید نامتقارن، اگرچه کندتر هستند، اما برای تبادل کلید و امضاهای دیجیتال ضروری هستند و امکان ارتباط ایمن بین طرفینی را که قبلاً یک رمز مشترک ایجاد نکرده‌اند، فراهم می‌کنند. سیستم‌های رمزنگاری مدرن اغلب هر دو نوع الگوریتم را با هم ترکیب می‌کنند.

DES

(Data Encryption Standard)

DES یک رمزنگاری بلوکی متقارن قدیمی و منسوخ است که روی بلوک‌های ۶۴ بیتی با کلید مؤثر ۵۶ بیتی عمل می‌کند. این الگوریتم در اواخر قرن بیستم به طور گسترده برای بانکداری و ارتباطات از راه دور استفاده می‌شد، اما به دلیل اینکه کلید کوتاه آن امکان حملات جستجوی فراگیر عملی را فراهم می‌کند، منسوخ شده است.

زمان تخمینی برای شکستن قفل **DES** با یک کامپیوتر شخصی مدرن (حمله بروت فورس روی کلید ۵۶ بیتی) حدودا بین چندین ساعت تا چند روز می باشد.

3DES
(Triple DES)

3DES این الگوریتم فرایند DES را سه بار (با سه کلید متفاوت) برای افزایش امنیت اعمال می‌کند. در این حالت با کلید اول رمزگذاری و سپس باکلید دوم رمز گشایی و پس از آن مجددا با کلید سوم رمزگذاری انجام می شود. اگر چه این الگوریتم نیز در حال حاضر منسوخ می باشد اما هنوز هم در برخی از سیستم‌های تراکنش مالی و برخی توکن‌های سخت‌افزاری استفاده می شود. زمان تخمینی برای شکستن قفل با یک کامپیوتر شخصی مدرن عملاً غیرممکن معادل قرن‌ها می باشد.

AES
(Advanced Encryption Standard)

AES استاندارد یک رمزگذاری بلوکی متقارن مدرن می‌باشد که اندازه بلوک آن ۱۲۸ بیت و اندازه کلید آن ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیت می باشد. به دلیل امنیت قوی و عملکرد بالا در نرم‌افزار و سخت‌افزار از رمزگذاری دیسک و فایل گرفته تا TLS، VPN و ... استفاده می‌شود. زمان تخمینی برای شکستن رمز آن با یک کامپیوتر شخصی مدرن از نقطه صفر عملاً غیرممکن می باشد. با یک کلید ۱۲۸ بیتی میلیاردها تا تریلیون‌ها سال طول می کشد و البته با کلید ۲۵۶بیتی بسیار طولانی‌تر زمان لازم خواهد داشت.

RSA
(Rivest–Shamir–Adleman)

RSA یک الگوریتم نامتقارن برای رمزگذاری و امضاهای دیجیتال مبتنی بر تجزیه اعداد صحیح از اعداد اول بزرگ است. امنیت آن به اندازه مدول (معمولاً ۲۰۴۸ یا ۳۰۷۲ بیت در عمل)بستگی دارد و به طور گسترده برای تبادل کلید، امضاها و سیستم‌های مبتنی بر گواهی (TLS، S/MIME) استفاده می‌شود. زمان تخمینی آن برای شکسته شدن با یک رایانه شخصی مدرن برای مدول ۱۰۲۴ بیتی چندین دهه تا قرن‌ها و برای مدول ۲۰۴۸ بیتی عملاً برای یک رایانه شخصی غیرممکن است.

DH
(Diffie–Hellman)

دیفی- هلمن یک روش تبادل کلید است که به دو طرف اجازه می‌دهد تا یک رمز مشترک را از طریق یک کانال ناامن استخراج و تبادل کنند. در واقع این فرایند روشی برای تبادل کلید در فضای نا امن می باشد. امنیت آن به اندازه عدد اول/ مدول یا منحنی بیضوی مورد استفاده بستگی دارد و زیربنای بسیاری از تبادلات کلید VPN و TLS است. زمان تخمینی برای شکستن قفل آن با یک رایانه شخصی مدرن برای DH با مدول ۱۰۲۴ بیتی به طور بالقوه سال‌ها تا دهه‌ها طول می کشد. DH با مدول ۲۰۴۸ بیتی عملاً غیرممکن می‌باشد و قرن‌ها تا زمان‌های نجومی طولانی نیاز دارد.

پزشکی از راه دور در نظام سلامت ایران؛ فرصتی برای عدالت، کارآمدی و تاب‌آوری

دکتر آیدین محمودعلیلو
فلوشیپ فوق تخصص طب اورژانس کودکان
مرکز آموزشی درمانی فوق تخصصی زهرا مردانی آذر

چکیده

پزشکی از راه دور (Telemedicine) یکی از نوآورانه‌ترین فناوری‌های قرن بیست‌ویکم در نظام سلامت است که امکان ارائه خدمات پزشکی به مناطق محروم و بحران‌زده را فراهم می‌سازد. در ایران، به‌کارگیری این فناوری می‌تواند نقشی کلیدی در ارتقای عدالت سلامت، کاهش هزینه‌های درمانی و افزایش بهره‌وری سیستم سلامت ایفا کند.

مقدمه

تحولات فناورانه دهه اخیر، الگوی مراقبت‌های پزشکی را متحول ساخته است. پزشکی از راه دور با استفاده از زیرساخت‌های ارتباطی و داده‌محور، به پزشکان و بیماران امکان برقراری ارتباط مؤثر بدون نیاز به حضور فیزیکی می‌دهد. در کشوری مانند ایران با پراکندگی جمعیتی و محدودیت منابع درمانی، این فناوری می‌تواند ابزاری کارآمد برای توسعه عدالت در سلامت باشد.

کارکردها و مزایای پزشکی از راه دور

مهم‌ترین کارکرد پزشکی از راه دور، بهبود دسترسی به خدمات تخصصی برای مناطق دورافتاده است. همچنین، کاهش مراجعات غیرضروری به بیمارستان‌ها، پایش بیماران مزمن، و مشاوره‌های فوری از دیگر مزایای این رویکرد محسوب می‌شوند. پژوهش‌ها نشان داده‌اند که استفاده از تله‌مدیسین در مدیریت بیماری‌های مزمن مانند دیابت و فشار خون، موجب کاهش بستری و هزینه‌های درمانی می‌شود.

چالش‌های اجرایی در ایران

با وجود مزایای قابل‌توجه، چالش‌هایی مانند کمبود زیرساخت‌های ارتباطی پایدار، ملاحظات اخلاقی و حقوقی، و نبود پروتکل‌های ملی استاندارد، از موانع اصلی توسعه تله‌مدیسین در کشور هستند. افزون بر آن، موضوع امنیت داده‌های بیماران و حفظ حریم خصوصی باید در سطح سیاست‌گذاری کلان سلامت مورد توجه قرار گیرد.

آینده‌پژوهی و مسیر توسعه

با گسترش هوش مصنوعی، یادگیری ماشین و سامانه‌های تحلیل داده، پزشکی از راه دور در آینده‌ای نزدیک به سطحی نوین از دقت و کارایی خواهد رسید. در ایران، ادغام تله‌مدیسین با پرونده الکترونیک سلامت، ایجاد شبکه ملی مشاوره‌های تخصصی، و آموزش پزشکان در زمینه فناوری‌های دیجیتال، مسیر توسعه این حوزه را هموار می‌کند.

نتیجه‌گیری و پیشنهادها

پزشکی از راه دور می‌تواند نقشی بنیادین در تحقق عدالت و تاب‌آوری نظام سلامت ایران ایفا کند. پیشنهاد می‌شود که وزارت بهداشت، سیاستی ملی برای توسعه تله‌مدیسین تدوین کرده و بسترهای قانونی، فنی و آموزشی لازم را فراهم آورد تا این فناوری بتواند در خدمت اهداف کلان سلامت عمومی قرار گیرد.

منابع:

1. World Health Organization. Telemedicine: opportunities and developments in Member States. WHO, 2021.

2. Bashshur RL, et al. The Empirical Foundations of Telemedicine Interventions in Primary Care. Telemed J E Health, 2022.

۳. وزارت بهداشت، درمان و آموزش پزشکی. سند ملی تله‌مدیسین ایران، ۱۴۰۲.

آموزش فناوری اطلاعات:
مبانی هک اخلاقی
بخش چهارم

دکتر طاها صمدسلطانی
دانشیار انفورماتیک پزشکی
مدیرآمـــار، فنـــاوری اطلاعـــات و
امنیـــت فضـــای مجـــازی دانشـــگاه

در ادامه مبحث مربوط به فاز **FOOTPRINTING** موارد تکمیلی مطرح می شود. همانطور که بیان شد **FOOTPRINTING** یعنی شناسایی و گردآوری اطلاعات از منابع عمومی و نیمه‌عمومی برای شناخت بهتر هدف. این اطلاعات پایه‌ای برای مراحل بعدی مثل اسکن، کسب اطلاعات شبکه و سیستم عامل مورد استفاده هستند.

اطلاعات شبکه (Network Information)

موارد قابل جمع‌آوری در اطلاعات شبکه همانگونه که قبلا نیز ذکر شد شامل دامنه‌های عمومی و داخلی شرکت، آدرس‌های **IP** سیستم‌ها، سرویس‌های **TCP/UDP** فعال، مکانیزم‌های کنترل دسترسی، اطلاعات**VPN** و شماره تلفن‌های مرتبط با شبکه(**VOIP**) می باشد. برخی از این ابزارها از جمله **WHOIS** که بصورت **Passive** می باشند، مورد بحث قرار گرفت. دستور دیگر دستور **nmap** می باشد که از طریق آن می‌توان فهمید که آیا روی **IP** خاصی (مثلاً ۱۹۲.۱۶۸.۱.۱۰ سرویس‌های **SSH** یا **HTTP** فعال هستند یا نه (مطابق شکل دستور در محیط لینوکس کالی اجرا شده است).

```bash
nmap -sS -p 22,80 192.168.1.10
```

دستور یک اسکن نیمه باز(**SYN Scan**) روی پورت های ۲۲ و ۸۰ سیستم هدف انجام می دهد و نشان می دهد که هدف رایانه ای فعال با وضعیت پورت های باز یا بسته هستند.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-10-28 16:30 IRST
Nmap scan report for 192.168.1.10
Host is up (0.0020s latency).

PORT   STATE  SERVICE
22/tcp open   ssh
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

اطلاعات سیستم‌عامل (Operating System Information)

علاوه بر اطلاعات شبکه می توان اطلاعاتی از سیستم عامل هدف نیز به دست آورد. این اطلاعات شامل نام کاربران و گروه‌ها نسخه سیستم‌عامل (مثلاً **Windows 10** یا **Ubuntu 22.04**)، معماری سیستم (**x86, x64**)، نسخه‌های سیستم‌های راه‌دور(**Remote tools**)، نام سیستم‌ها و حتی رمزهای عبور (در صورت افشا یا اشتباهات امنیتی) می باشد.
دستور **nmap** با پارامتر **-o** می تواند اطلاعات سیستم عامل را استخراج کند(مطابق تصویر)

```
Bash

nmap -O 192.168.1.10
```

خروجی شامل نوع و نسخه سیستم عامل و پورتهای باز می باشند. در مثال زیر سیستم عامل هدف لینوکس ۵.۴ بوده و پورتهای ۲۲، ۸۸ و ۴۴۳ از نوع **TCP** باز می باشند.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-10-28 16:35 IRST
Nmap scan report for 192.168.1.10
Host is up (0.0010s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https

Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.4 - 5.10
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 3.21 seconds
```

دستورات رایج دیگری از جمله **ping** نیز وجود دارند که دسترس پذیر بودن هدف را نشان می دهد. دستور **Traceroute** مسیر حرکت داده در شبکه را از ابتدا تا انتها می دهد.

اطلاعات سازمانی (Organization Data)

در مورد اطلاعات درون سازمانی نیز می توان با استفاده از روشهایی نام و سمت کارکنان، وب‌سایت رسمی سازمان، دایرکتوری شرکت و آدرس و شماره تماس‌ها را بدست آورد. این اطلاعات در تئوریهای زیرزمینی هک به ویژه هک اجتماعی نقش مهمی ایفا می کنند.

برای مثال از روی **Linkedin** یا پروفایل **Instagram** می توان اطلاعاتی همچون موارد زیر را به دست آورد:

- نام، سمت، ایمیل، شماره تماس
- محل کار، تخصص، سابقه کاری
- حضور در کنفرانس‌ها یا مقالات منتشرشده

این روش رویکرد امنیتی دارد و به شناخت افراد کلیدی برای حملات مهندسی اجتماعی یا فیشینگ هدفمند منجر می شود.
در مورد وب سایت سازمان نیز می توان به ساختار صفحات، فرم‌های تماس، لینک‌های داخلی، **CMS** یا تکنولوژی‌های استفاده‌شده مثل **WordPress، Drupal** یا نیافام ، اطلاعات تماس، آدرس، ایمیل عمومی و غیره دسترسی داشت. برای مثال اگر نقص امنیتی در **Wordpress** یا پورتال ساز نیافام شناسایی شد به سرعت می توان تمام محصولات و وب سایت های مرتبط با این سامانه های مدیریت محتوا را هدف قرار داد. از این رویکرد برای شناسایی نقاط ورودی برای حملات وب، بررسی فرم‌های آسیب‌پذیر، یا ارسال ایمیل‌های جعلی و ارسال پیامک های حاوی لینک های جعلی شبیه به وب سایت سازمان استفاده می کنند. هکرهای اخلاقی موظفند آخرین بسته ها و وصله های امنیتی را در این زمینه فراهم نمایند.

دایرکتوری شرکت (Company Directory)

با جستجوی سرور فایل ها و دایرکتوری های حاوی فایل های سازمان با همان رویکرد پسیو **Google Dorking** یا روشهای دیگر **Crawling** وب می توان به لیست کارکنان، بخش‌ها، شماره داخلی و ساختار سازمانی (مدیران، تیم‌ها، پروژه‌ها) دسترسی یافت. لذا رعایت نکات امنیتی در این مورد باید به مسئولین سازمانی گوشزد شود. متعاقب این روش، احتمال نفوذ هدفمند به سامانه **VOIP** وجود دارد.
جدول زیر خلاصه ای از مهم ترین رویکردهای مطرح در جلسه آموزشی جاری را ارائه می کند. برای تست هر کدام نیازمند لینوکس کالی یا پاروت بوده و می توانید از **LLM** ها جهت درک بهتر دستورات و توضیح خروجی ها کمک بگیرید.

	ابزار / دستور	هدف / کاربرد اصلی	نمونه دستور یا رویکرد عملی
سازمانی	LinkedIn / Social Media	شناسایی کارکنان، سمت‌ها، ساختار سازمانی	جستجوی "IT Manager at ParsTech" در LinkedIn
	Google Dorking	یافتن فایل‌ها، ایمیل‌ها، صفحات مخفی	site:parstech.ir filetype:pdf
	theHarvester	جمع‌آوری ایمیل و نام از منابع عمومی	theHarvester -d parstech.ir -b google
	Recon-ng	تحلیل ساختار سازمانی و ارتباطات	استفاده از ماژول contacts

	ابزار / دستور	هدف / کاربرد اصلی	نمونه دستور یا رویکرد عملی
شبکه	whois domain.com	شناسایی دامنه و مالکیت	نمایش اطلاعات ثبت دامنه، مالک، ایمیل، NameServerها
	nslookup / dig	بررسی رکوردهای DNS	استخراج رکوردهای A, MX, NS, TXT برای دامنه هدف
	ping target.com	بررسی دسترسی‌پذیری سیستم	ارسال بسته ICMP برای بررسی فعال بودن سیستم
	traceroute target.com	شناسایی مسیر شبکه	نمایش مسیر عبور بسته‌ها از مبدا تا مقصد
	nmap -sS -p 22,80 IP	اسکن پورت‌ها و سرویس‌ها	بررسی پورت‌های باز و سرویس‌های فعال روی IP هدف
	nmap -O IP	تشخیص سیستم‌عامل از طریق شبکه	تخمین نوع سیستم‌عامل با تحلیل پاسخ‌های TCP/IP
	whatweb / Netcraft	تحلیل تکنولوژی وب‌سایت	شناسایی نوع وب‌سرور، سیستم‌عامل، CMS و فریم‌ورک‌ها
	Shodan	جستجوی دستگاه‌های متصل به اینترنت	یافتن IP ها، پورت‌های باز، سرویس‌ها و آسیب‌پذیری‌ها
	telnet domain.com 80	اتصال دستی به پورت‌ها	بررسی پاسخ سرویس‌ها و banner grabbing دستی

	ابزار / دستور	هدف / کاربرد اصلی	نمونه دستور یا رویکرد عملی
سیستم عامل	nmap -O IP	تشخیص نوع سیستم‌عامل	تخمین نوع سیستم‌عامل با تحلیل پاسخ‌های TCP/IP
	p0f	تشخیص سیستم‌عامل به‌صورت غیرفعال	تحلیل ترافیک ورودی بدون ارسال بسته فعال
	xProbe2	تشخیص سیستم‌عامل با اسکن فعال	ارسال بسته‌های خاص برای شناسایی نوع OS
	banner grabbing	شناسایی نسخه نرم‌افزار و سرویس‌ها	دریافت اطلاعات از پاسخ سرویس‌ها مثل SSH یا HTTP
	netcat IP یا telnet IP 80 port	اتصال دستی به سرویس‌ها	بررسی پاسخ اولیه و شناسایی نوع سرور یا OS
	tcpdump / Wireshark	تحلیل بسته‌های شبکه	بررسی TTL، window size، و سایر ویژگی‌های TCP/IP برای تخمین OS
	nmap -A IP	اسکن کامل یا اطلاعات سیستم‌عامل	اسکن پیشرفته شامل OS، نسخه سرویس‌ها، traceroute و اسکریپت‌ها

	ابزار / دستور	هدف / کاربرد اصلی	نمونه دستور یا رویکرد عملی
وب سرور	nslookup / dig	بررسی رکوردهای DNS	استخراج رکوردهای A, MX, NS, TXT برای دامنه هدف
	whois	شناسایی NameServer ها	نمایش NameServer های ثبت‌شده برای دامنه
	whatweb	شناسایی نوع وب‌سرور	شناسایی نوع وب‌سرور (Apache, Nginx, CMS, IIS)
	Wappalyzer	تحلیل تکنولوژی‌های وب‌سایت	افزونه مرورگر برای شناسایی CMS، فریم‌ورک، آنالیتیکس
	BuiltWith	تحلیل ساختار فنی وب‌سایت	نمایش CDN، امنیت، زبان برنامه‌نویسی، کتابخانه‌ها
	SSL Labs	بررسی پیکربندی SSL/TLS	تحلیل امنیت HTTPS، نسخه‌های TLS، گواهی‌نامه‌ها
	netcat یا telnet	بررسی پاسخ سرور (Banner Grabbing)	دریافت پاسخ اولیه از سرور برای شناسایی نسخه
	dig -x IP	تحلیل رکوردهای DNS معکوس	بررسی PTR Record برای یافتن نام دامنه مرتبط با IP

داشبوردهای سلامت: تحولی در مدیریت و تصمیم‌گیری در حوزه سلامت

سوگند حبیبی
کارشناس ارشد فناوری اطلاعات سلامت
کارشناس فناوری اطلاعات سلامت معاونت درمان

داشبوردهای سلامت و داشبوردهای دیجیتال به‌عنوان ابزارهای تحلیلی پیشرفته، نقش مهمی در بهبود مدیریت داده‌ها و تصمیم‌گیری در حوزه سلامت ایفا می‌کنند. این ابزارها با تجمیع و تجسم داده‌های پیچیده از منابع مختلف، امکان پایش بلادرنگ، تحلیل دقیق و تصمیم‌گیری مبتنی بر شواهد را برای متخصصان سلامت، مدیران بیمارستان‌ها و سیاست‌گذاران فراهم می‌کنند. این مقاله به تعریف داشبوردهای سلامت، اهداف، کاربردها، فرآیند استفاده، نمونه‌های موفق جهانی و راهکارهای پیاده‌سازی آن‌ها در ایران می‌پردازد.

تعریف داشبوردهای سلامت

داشبورد سلامت یک رابط کاربری دیجیتال است که داده‌های سلامت را به‌صورت بصری و قابل‌فهم نمایش می‌دهد. این ابزارها داده‌هایی مانند آمار بیماران، عملکرد تجهیزات پزشکی، شاخص‌های کلیدی عملکرد (**KPI**) بیمارستان‌ها یا روند بیماری‌ها را از منابعی مانند پرونده‌های الکترونیک سلامت (**EHR**)، سنسورهای اینترنت اشیا (**IoT**) و پایگاه‌های داده تجمیع کرده و به‌صورت نمودارها، جداول و نقشه‌های حرارتی ارائه می‌کنند. برای مثال، یک داشبورد می‌تواند ضریب اشغال تخت‌های **ICU** یا شیوع یک بیماری در منطقه‌ای خاص را به‌صورت بلادرنگ نشان دهد.

اهداف داشبوردهای سلامت

هدف اصلی داشبوردهای سلامت، بهینه‌سازی مدیریت منابع و بهبود کیفیت مراقبت‌های پزشکی است. اهداف کلیدی عبارت‌اند از:

- پایش بلادرنگ: نظارت بر شاخص‌های سلامت مانند نرخ بستری یا مرگ‌ومیر.
- تصمیم‌گیری مبتنی بر داده: ارائه اطلاعات دقیق برای انتخاب بهترین اقدامات درمانی یا مدیریتی.
- افزایش کارایی: بهینه‌سازی تخصیص منابع مانند تخت‌ها، پرسنل و تجهیزات.
- شفافیت و پاسخگویی: ارائه گزارش‌های قابل‌فهم به ذی‌نفعان، از جمله بیماران و سیاست‌گذاران.

این ابزارها به دنبال افزایش دقت، سرعت و دسترسی‌پذیری اطلاعات در نظام سلامت هستند.

کاربردها و پتانسیل‌ها

داشبوردهای سلامت در حوزه‌های مختلف کاربرد دارند که در جدول زیر خلاصه شده‌اند:

کاربرد	توضیح	پتانسیل
مدیریت بیمارستان	پایش شاخص‌هایی مانند ضریب اشغال تخت، زمان انتظار و عملکرد پرسنل.	بهبود تخصیص منابع و کاهش هزینه‌های عملیاتی.
اپیدمیولوژی	رصد شیوع بیماری‌ها و پیش‌بینی روند اپیدمی‌ها مانند کووید-۱۹.	واکنش سریع به بحران‌های سلامت و کاهش مرگ‌ومیر.
مراقبت‌های شخصی‌سازی‌شده	تحلیل داده‌های بیمار برای ارائه درمان‌های متناسب با نیازهای فردی.	افزایش اثربخشی درمان و رضایت بیماران.
مدیریت زنجیره تأمین	پایش موجودی داروها و تجهیزات پزشکی.	جلوگیری از کمبود اقلام حیاتی و بهینه‌سازی لجستیک.

این کاربردها در ایران، به‌ویژه برای مدیریت بیماری‌های مزمن مانند دیابت یا پایش اپیدمی‌ها، پتانسیل بالایی دارند.

فرآیند استفاده

پیاده‌سازی داشبوردهای سلامت شامل مراحل زیر است:

۱. جمع‌آوری داده‌ها: تجمیع داده‌ها از منابع مختلف مانند **EHR**، سنسورهای **IoT** و گزارش‌های بالینی.
۲. طراحی داشبورد: ایجاد رابط کاربری بصری با استفاده از ابزارهایی مانند **Power BI**، **Tableau** یا پلتفرم‌های بومی.
۳. تحلیل و به‌روزرسانی: تحلیل داده‌ها و به‌روزرسانی بلادرنگ داشبورد برای نمایش اطلاعات جاری.
۴. امنیت داده‌ها: استفاده از رمزنگاری و پروتکل‌های امنیتی برای حفاظت از حریم خصوصی بیماران.

این فرآیند نیازمند زیرساخت‌های فناوری اطلاعات و آموزش کاربران است.

نمونه‌های موفق جهانی

داشبوردهای سلامت در سطح جهانی دستاوردهای قابل‌توجهی داشته‌اند:

- ایالات متحده: داشبوردهای **Epic Systems** در بیمارستان‌های آمریکا برای پایش داده‌های بیماران استفاده می‌شوند و زمان تصمیم‌گیری را تا ۲۰ درصد کاهش داده‌اند.
- انگلستان: **NHS** از داشبوردهای دیجیتال برای رصد شیوع بیماری‌ها استفاده می‌کند که واکنش به اپیدمی کووید۱۹- را تسریع کرد.
- استرالیا: داشبوردهای سلامت در ایالت نیو ساوت ولز برای مدیریت زنجیره تأمین تجهیزات پزشکی به کار گرفته شده و کمبودها را تا ۱۵ درصد کاهش داده است.

مسیر پیاده‌سازی در ایران

ایران با توجه به پیشرفت‌های اخیر در دیجیتالی‌سازی سلامت و نیاز به مدیریت بهتر منابع، ظرفیت بالایی برای استفاده از داشبوردهای سلامت دارد. پیشنهادات برای پیاده‌سازی عبارت‌اند از:

۱. آموزش تخصصی: برگزاری دوره‌های آموزشی برای تحلیلگران داده و کادر درمان در دانشگاه‌های علوم پزشکی.
۲. تمرکز بر اولویت‌ها: هدف‌گذاری روی پایش بیماری‌های مزمن و مدیریت بیمارستان‌ها.
۳. توسعه زیرساخت‌ها: گسترش اینترنت پرسرعت و سرمایه‌گذاری در پلتفرم‌های بومی تحلیل داده.
۴. پروژه‌های آزمایشی: راه‌اندازی داشبوردهای سلامت در بیمارستان‌های بزرگ مانند بیمارستان امام رضا(ع) تبریز.
۵. تدوین قوانین: تنظیم استانداردهای حریم خصوصی و یکپارچگی داده‌ها برای اطمینان از امنیت اطلاعات.

جمع‌بندی

داشبوردهای سلامت با ارائه اطلاعات بصری و بلادرنگ، پتانسیل تحول در مدیریت و تصمیم‌گیری در نظام سلامت را دارند. تجربه‌های موفق جهانی نشان‌دهنده اثربخشی این ابزارها در بهبود کارایی و کیفیت مراقبت‌ها است. در ایران، با رفع چالش‌های زیرساختی و سرمایه‌گذاری در آموزش و توسعه فناوری، می‌توان از داشبوردهای دیجیتال برای ارتقای نظام سلامت بهره برد.

استفاده از شبیه‌سازها در آموزش پزشکی: انقلابی در یادگیری و مراقبت

دکتر امیر تراب میاندوآب
استادیار مدیریت اطلاعات سلامت مرکز تحقیقات آموزش پزشکی

شبیه‌سازها در آموزش پزشکی به‌عنوان ابزاری نوآورانه، امکان یادگیری عملی و بدون ریسک را برای دانشجویان و متخصصان پزشکی فراهم کرده‌اند. این فناوری‌ها، که شامل شبیه‌سازی‌های مجازی، مدل‌های فیزیکی و واقعیت افزوده (**AR**) و واقعیت مجازی (**VR**) هستند، به بهبود مهارت‌های بالینی، افزایش ایمنی بیماران و ارتقای کیفیت آموزش کمک می‌کنند. این مقاله به تعریف شبیه‌سازها، اهداف، کاربردها، فرآیند استفاده، نمونه‌های موفق جهانی و راهکارهای پیاده‌سازی آن در ایران می‌پردازد.

تعریف شبیه‌سازها در آموزش پزشکی

شبیه‌سازها ابزارهایی هستند که محیط‌های واقعی یا مجازی را برای آموزش مهارت‌های پزشکی بازسازی می‌کنند. این ابزارها می‌توانند شامل مانکن‌های پیشرفته (مانند شبیه‌سازهای جراحی)، نرم‌افزارهای شبیه‌سازی مجازی (مانند مدل‌های سه‌بعدی اندام‌ها) یا سیستم‌های واقعیت مجازی باشند که سناریوهای بالینی را شبیه‌سازی می‌کنند. برای مثال، یک شبیه‌ساز جراحی می‌تواند به دانشجو اجازه دهد بدون خطر برای بیمار واقعی، تکنیک‌های جراحی را تمرین کند. این فناوری‌ها با استفاده از داده‌های واقعی و هوش مصنوعی، تجربه‌ای نزدیک به واقعیت ارائه می‌دهند.

اهداف شبیه‌سازها

هدف اصلی شبیه‌سازها بهبود کیفیت آموزش پزشکی و ایمنی بیماران است. اهداف کلیدی عبارت‌اند از:

- ارتقای مهارت‌های بالینی: فراهم‌سازی محیطی امن برای تمرین مهارت‌هایی مانند جراحی یا تشخیص.
- کاهش خطاهای پزشکی: تمرین سناریوهای پیچیده برای کاهش خطاهای بالینی.
- آموزش تیمی: تقویت همکاری بین تیم‌های پزشکی در شرایط شبیه‌سازی‌شده.
- افزایش اعتمادبه‌نفس: آماده‌سازی دانشجویان برای مواجهه با شرایط واقعی بدون استرس.

این اهداف به بهبود عملکرد پزشکان و کاهش هزینه‌های ناشی از خطاهای پزشکی کمک می‌کنند.

کاربردها و پتانسیل‌ها

شبیه‌سازها در حوزه‌های مختلف آموزش پزشکی کاربرد دارند که در جدول زیر خلاصه شده‌اند:

کاربرد	توضیح	پتانسیل
آموزش جراحی	شبیه‌سازی جراحی‌های قلب، مغز یا ارتوپدی با مانکن یا واقعیت مجازی.	افزایش دقت و کاهش عوارض جراحی در دنیای واقعی.
مدیریت بحران	تمرین سناریوهای اورژانسی مانند احیای قلبی-ریوی (CPR).	بهبود واکنش سریع و هماهنگی تیمی در شرایط بحرانی.
آموزش تشخیص	شبیه‌سازی بیماری‌ها برای تمرین تشخیص افتراقی.	کاهش خطاهای تشخیصی و بهبود تصمیم‌گیری بالینی.
آموزش پرستاری	تمرین مهارت‌هایی مانند تزریق یا مراقبت از بیمار.	ارتقای کیفیت مراقبت‌های پرستاری و افزایش ایمنی بیمار.

این کاربردها می‌توانند در ایران، به‌ویژه برای آموزش بیماری‌های شایع مانند بیماری‌های قلبی یا مدیریت تروما، بسیار مؤثر باشند.

فرآیند استفاده

پیاده‌سازی شبیه‌سازها در آموزش پزشکی شامل مراحل زیر است:

۱. طراحی سناریو: ایجاد سناریوهای بالینی واقعی بر اساس نیازهای آموزشی، مانند شبیه‌سازی یک حمله قلبی.
۲. انتخاب ابزار: استفاده از مانکن‌های فیزیکی، نرم‌افزارهای مجازی یا سیستم‌های AR/VR.
۳. اجرای شبیه‌سازی: برگزاری جلسات آموزشی با نظارت مربیان برای تمرین و بازخورد.
۴. ارزیابی و بهبود: تحلیل عملکرد دانشجویان و به‌روزرسانی سناریوها بر اساس بازخورد.

این فرآیند نیازمند زیرساخت‌های مناسب و آموزش مربیان است.

نمونه‌های موفق جهانی

شبیه‌سازها در سطح جهانی نتایج قابل‌توجهی داشته‌اند:

- ایالات متحده: دانشگاه جانز هاپکینز از شبیه‌سازهای جراحی برای آموزش رزیدنت‌ها استفاده می‌کند، که نرخ خطای جراحی را تا ۲۵ درصد کاهش داده است.

- انگلستان: مرکز شبیه‌سازی بیمارستان آدنبروک در کمبریج از واقعیت مجازی برای آموزش مدیریت بحران استفاده می‌کند، که هماهنگی تیمی را بهبود بخشیده است.
- کانادا: دانشگاه تورنتو با شبیه‌سازهای پرستاری، مهارت‌های مراقبت از بیمار را تقویت کرده و رضایت بیماران را افزایش داده است.

مزایا و چالش‌ها

مزایای شبیه‌سازها شامل افزایش دقت مهارت‌ها، کاهش خطاهای پزشکی، بهبود آموزش تیمی و فراهم‌سازی محیطی بدون ریسک است. بااین‌حال، چالش‌هایی مانند هزینه‌های اولیه بالا، نیاز به زیرساخت‌های فناوری (مانند تجهیزات **VR** یا اینترنت پرسرعت) و کمبود مربیان آموزش‌دیده وجود دارد. در ایران، محدودیت منابع مالی و دسترسی نابرابر به فناوری در مناطق محروم می‌تواند مانع پیاده‌سازی باشد.

مسیر پیاده‌سازی در ایران

ایران با توجه به تعداد بالای دانشجویان پزشکی و نیاز به بهبود کیفیت آموزش، پتانسیل بالایی برای استفاده از شبیه‌سازها دارد. پیشنهادات برای پیاده‌سازی عبارت‌اند از:

۱. آموزش مربیان: برگزاری کارگاه‌های آموزشی در دانشگاه‌های علوم پزشکی
۲. تمرکز بر اولویت‌ها: هدف‌گذاری روی آموزش جراحی و مدیریت بحران برای بیماری‌های شایع.
۳. توسعه زیرساخت‌ها: سرمایه‌گذاری در تجهیزات شبیه‌سازی و گسترش دسترسی به فناوری‌های **AR/VR**.
۴. پروژه‌های آزمایشی: راه‌اندازی مراکز شبیه‌سازی در بیمارستان‌های آموزشی
۵. حمایت مالی و قانونی: تخصیص بودجه‌های دولتی و تدوین استانداردهای آموزشی برای استفاده از شبیه‌سازها.

جمع‌بندی

شبیه‌سازها با ایجاد محیط‌های آموزشی ایمن و واقعی، پتانسیل تحول در آموزش پزشکی را دارند. تجربه‌های موفق جهانی نشان‌دهنده اثربخشی این فناوری در بهبود مهارت‌ها و ایمنی بیماران است. در ایران، با رفع چالش‌های مالی و زیرساختی و سرمایه‌گذاری در آموزش مربیان، می‌توان از شبیه‌سازها برای ارتقای کیفیت آموزش پزشکی و مراقبت‌های بالینی بهره برد. پژوهش‌های بومی برای ارزیابی اثربخشی این فناوری در نظام آموزشی ایران ضروری است.

پیام مخاطب

محمدرضا عمرانی‌فر
کارشناسی ارشد مهندسی سازه
رئیس گروه کارشناسان ساختمان دانشگاه

سردبیر محترم پالسی نو

با سلام و احترام
با تشکر از زحمات صورت گرفته، با کسب اجازه مواردی را به شرح زیر به حضور ایفاد می نمایم:

۱. ساختار کلی نشریه

- نشریه انسجام خوبی دارد و تیترها، زیرتیترها و معرفی نویسندگان منظم است.
- ترکیب مقالات علمی، آموزشی و تحلیلی باعث شده خواننده دید چندبعدی نسبت به فناوری‌ها و سیاست‌گذاری پیدا کند.
- تیترهای حرفه‌ای مثل حکمرانی داده، سلامت دیجیتال، هوش مصنوعی، بایگانی الکترونیک لحن علمی و دانشگاهی را حفظ کرده است.
- نکته قابل توجه: گاهی چیدمان متن فشرده است و خوانایی کاهش می‌یابد.

۲. محتوای علمی و تحلیلی

- حکمرانی داده و سلامت دیجیتال: چارچوب نظری و ارتباط با نظام سلامت دقیق است. می‌توان به موانع اجرایی در ایران نیز اشاره کرد تا تحلیل عملی‌تر شود.
- هوش مصنوعی و حریم خصوصی: متن علمی و هشداردهنده است. پیشنهاد می‌شود یک بخش کوتاه آموزشی برای مخاطبان عمومی اضافه گردد تا راهکارهای عملی برای حفظ حریم خصوصی ارائه شود.
- آمادگی الکترونیکی و بایگانی دیجیتال: کاربردی و فنی است. اضافه کردن نقشه فرآیندی یا جدول تطبیق با استانداردهای جهانی باعث غنای علمی‌تر مقاله خواهد شد.
- کاربرد فناوری در آموزش بهداشت: منسجم و علمی است، اما می‌توان مثال‌ها و تجربه‌های داخلی را اضافه کرد تا ملموس‌تر شود.
- هک اخلاقی: جذاب و آموزنده است، اما کمی خشک است. آوردن یک مطالعه موردی یا نمونه واقعی، اثرگذاری آن را بیشتر می‌کند.

۳. لحن و نگارش

- لحن رسمی و علمی است اما قابل فهم برای مخاطب دانشگاهی.
- جمله‌ها طولانی هستند؛ کوتاه کردن آنها باعث روان‌تر شدن متن می‌شود.
- واژگان تخصصی درست استفاده شده‌اند، اما افزودن یک واژه‌نامه کوچک در انتهای نشریه می‌تواند برای مخاطب عمومی مفید باشد.

۴. طراحی و صفحه‌آرایی

- رنگ، فونت و لوگو چشم‌نواز هستند، اما فاصله بین خطوط در برخی صفحات کم است.
- ترکیب متن فارسی و انگلیسی مناسب است؛ بهتر است فونت انگلیسی یکنواخت باشد.
- پیشنهاد می‌شود تیتر انگلیسی هر مقاله زیر عنوان فارسی درج شود تا جلوه حرفه‌ای‌تر داشته باشد.
- تصاویر مناسب هستند، اما برای تقویت هویت بصری می‌توان یک آیکون ثابت برای هر مقاله طراحی کرد.

۵. پیشنهادهای ارتقایی برای شماره‌های آینده

- پرونده ویژه: تحول دیجیتال در آموزش و پژوهش دانشگاهی
- ستون جدید: یک تجربه – One Case مطالعه موردی فنی در دانشگاه‌ها
- افزودن خلاصه انگلیسی (Abstract) برای هر مقاله
- بخش تصویری: اینفوگراف از چرخه داده یا امنیت دیجیتال
- تکمیل شناسنامه مجله (شورای سردبیری، صفحه تماس، آرشیو QR)

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

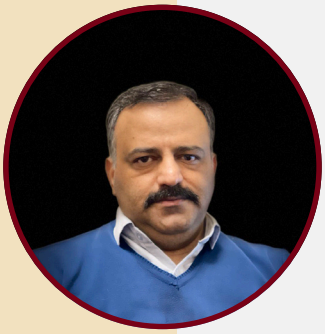
نویده خدائی
دانشجوی دکتری مدیریت فناوری
اطلاعات
کارشناس فناوری اطلاعات

دکترامیر تراب میاندوآب
استادیار مدیریت اطلاعات سلامت
مرکز تحقیقات آموزش پزشکی

دکتر سعید سقطی‌زاد
دکتری حرفه‌ای پزشکی
رئیس دبیرخانه هیأت امنای
دانشگاه

جواد فرهادی
کارشناس ارشد نرم افزار

وحید عباس‌زاده
دانشجوی PHD الکترونیک
کارشناس شبکه



صابر درس‌خوان
کارشناس ارشد شبکه
کارشناس مسئول زیرساخت

دکتر آیدین محمودعلیلو
فلوشیپ فوق‌تخصص
طب اورژانس کودکان
مرکز آموزشی درمانی
فوق‌تخصصی زهرا مردانی آذر

سیدمحمدحسن الهی

سوگند حبیبی
کارشناس ارشد فناوری اطلاعات سلامت
کارشناس فناوری اطلاعات سلامت
معاونت درمان

مدیریت آمار، فناوری اطلاعات و امنیت فضای مجازی
دانشگاه علوم پزشکی تبریز

تصویر روی جلد و پشت جلد نشانگر نقش پدافند غیرعامل همچون سپری نامحسوس و مخفی در شبکه و دیتاستر می باشد.

A New Pulse

Special Issue: Secret Shield in Information Technology

anp.tbzmed.ac.ir

anp@tbzmed.ac.ir

anew_pulse