مدیریت بحران در جنگ
با تمرکز بر زیرساختهای فناوری اطلاعات در صنعت بیمه

مدرس:
دکتر میثم میرزازاده


بسم الله الرحمن الرحيم

پیشینه کارگاه

- تحول مفهوم مدیریت بحران در عصر دیجیتال
- زیرساخت‌های فناوری اطلاعات؛ هدف استراتژیک در نبردهای نوین
- تجارب تاریخی و شکاف‌های موجود

اطلاعات مدرس و همکاران

جناب آقای دکتر میرزازاده، رئیس مرکز فناوری، امنیت اطلاعات و توسعه هوشمند

جناب آقای مهندس پژمان، مشاور مرکز فناوری اطلاعات، ارتباطات و توسعه هوشمند

جناب آقای مهندس حاتمی، رئیس اداره مدیریت امنیت و نظارت بر فضای تبادل اطلاعات


سازمان توانمند
تاب‌آوری پایدار

بیان مسأله و ضرورت انجام کارگاه

صنعت بیمه کلید پایداری اقتصادی و بازسازی ملی در بحران‌هاست؛ اما در جنگ‌های نوین، وابستگی مطلق این صنعت به زیرساخت‌های فناوری اطلاعات، آن را به هدفی استراتژیک تبدیل کرده است. مسئله اصلی اینجاست که در صورت تخریب فیزیکی یا سایبری دیتاسنترها، تداوم خدمات بیمه‌ای متوقف شده و منجر به فروپاشی اعتماد عمومی می‌گردد. بنابراین، چالش اساسی:

طراحی الگوی مدیریتی است که بتواند تاب‌آوری را از طریق صیانت از "مرکز ثقل" دیجیتال صنعت بیمه در میانه جنگ تضمین کند.

سوابق مطالعاتی و پژوهشی مربوطه

در تدوین این پژوهش، سه محور اصلی از مطالعات پیشین و تجارب عملیاتی مورد واکاوی قرار گرفته است:

- **تحلیل تطبیقی استانداردهای پدافند غیرعامل سایبری:** بررسی اسناد بالادستی و استانداردهای بین‌المللی نظیر **NIST SP 800-34** و **ISO/IEC 27031**؛ با تمرکز بر انطباق‌سازی پروتکل‌های «تاب‌آوری فناوری اطلاعات» با شرایط بحرانی ناشی از نبردهای نظامی.
- **مطالعه موردی بحران‌های بین‌المللی:** واکاوی تجربه شرکت‌های بیمه بزرگ در بحران‌های اخیر (مانند جنگ‌های سایبری اوکراین و اختلالات زیرساختی در خاورمیانه) جهت شناسایی نقاط گلوگاهی در زنجیره تأمین خدمات دیجیتال.
- **ارزیابی الگوهای تداوم کسب‌وکار در صنعت مالی:**

مرور پژوهش‌های داخلی و بین‌المللی در خصوص مدل‌های بازیابی فاجعه؛ با هدف گذار از روش‌های سنتی (Back-up) به سمت معماری‌های نوین توزیع‌شده و ابری در شرایط جنگی.


بسیاری از مدیران فناوری اطلاعات در کشور، برنامه بازیابی
از بحران و راه‌اندازی سایت پشتیبان با هدف تداوم
کسب‌وکار و افزایش تاب‌آوری سازمانی را اجرا نمی‌کنند!

نقش حیاتی فناوری اطلاعات در بیمه

تغییر نقش فناوری اطلاعات: گذار از «ابزار پشتیبان» به «موتور محرک کسب‌وکار»

زنجیره ارزش دیجیتال: پیوستگی کامل فرآیندها (از ارزیابی ریسک تا پرداخت خسارت) به زیرساخت فنی.

داده‌ها به مثابه دارایی: صیانت از پایگاه داده‌ها به عنوان سرمایه اصلی صنعت.

پایداری سیستم عاملِ پایداری خدمات: عدم امکان تداوم عملیات در صورت اختلال زیرساختی.

تفاوت بحران جنگ با بحرانهای عادی

ویژگی	بحران‌های عادی (طبیعی/فنی)	بحران جنگ (نبردهای نوین)
ماهیت تهدید	تصادفی و غیرعمدی	هوشمند، هدفمند و متوالی
دامنه اثر	محدود به جغرافیای خاص	سراسری و فرامرزی
پایداری	کوتاه مدت و قابل پیش‌بینی	طولانی و غیرقابل پیش‌بینی
هدف اصلی	آسیب به تجهیزات فیزیکی	تخریب همزمان زیرساخت فیزیکی و سایبری
منابع انسانی	در دسترس برای امداد	درگیر در بحران و جابجایی

تاب‌آوری زیرساخت دیجیتال، خـط مقـدم صیانت از حاکمیت اقتصادی است.

دسته‌بندی تهدیدات

تهدیدات فیزیکی (Physical Threats): حملات موشکی، تخریب دیتاسنترها و قطع کابل‌های ارتباطی فیبر نوری.

تهدیدات سایبری (Cyber Threats): جنگ الکترونیک، حملات منع سرویس (DDoS)، بدافزارهای تخریبی و جاسوسی صنعتی.

تهدیدات عملیاتی (Operational Threats): کمبود نیروی انسانی متخصص در زمان جنگ، اختلال در زنجیره تأمین قطعات و شکست فرآیندهای مدیریتی.

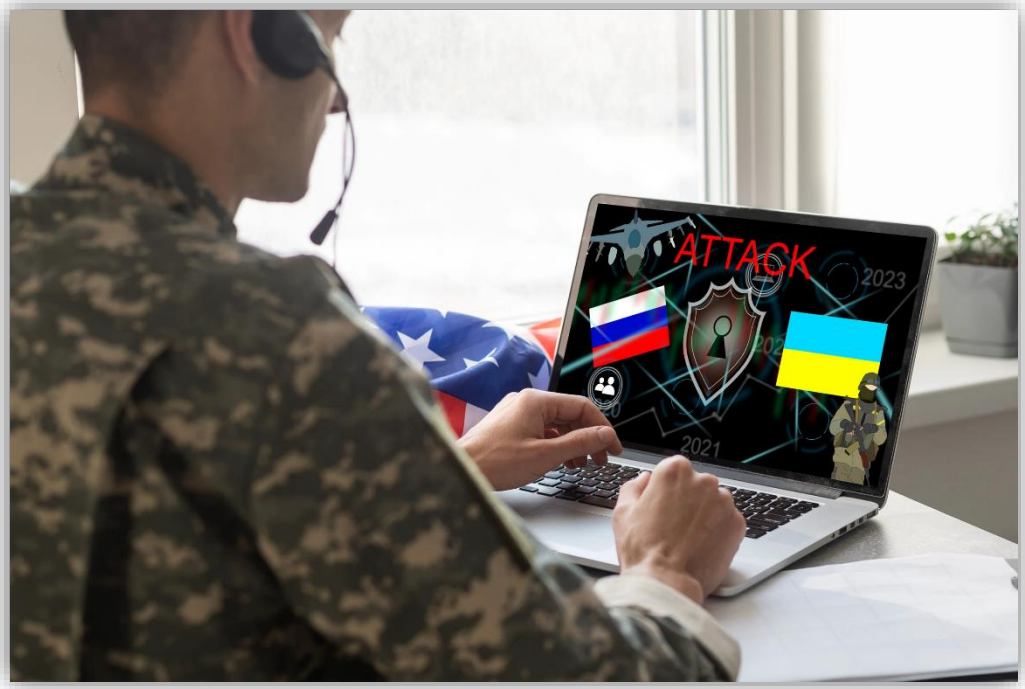
تهدیدات دسترسی و پایداری (Availability Threats): قطع اینترنت بین‌المللی، اختلال در شبکه برق سراسری و عدم دسترسی به سرویس‌های ابری خارجی.

مطالعه موردی؛ نبرد سایبری در بحران اوکراین

نوع حمله: استفاده گسترده از بدافزارهای Wiper (پاک‌کننده داده) به جای باج‌افزار.

هدف: نابودی کامل دیتاسنترهای مالی و بیمه‌ای برای ایجاد هرج‌ومرج اجتماعی.

نتیجه: سازمان‌هایی که زیرساخت Cloud-based (خارج از مرزهای فیزیکی) نداشتند، فلج شدند.



تاب‌آوری دیجیتال؛ فراتر از امنیت سایبری

تعریف: توانایی یک سازمان برای پیش‌بینی، مقاومت، بازیابی و انطباق با شرایط بحرانی (نظیر جنگ).

تفاوت بنیادین:

امنیت: تمرکز بر جلوگیری از نفوذ.

تاب‌آوری: تمرکز بر استمرار خدمات در حین وقوع فاجعه.

ارکان چهارگانه:

پیش‌بینی (Anticipate): شناسایی نقاط ضعف زیرساخت قبل از حمله.

مقاومت (Withstand): حفظ عملیات حیاتی تحت شدیدترین فشارها.

بازیابی (Recover): بازگشت سریع به وضعیت عادی.

انطباق (Adapt): درس‌گیری از بحران برای ارتقای توان دفاعی.

ISO 22301:2019
Security and resilience —Business continuity management systems

“هدف از سیستم مدیریت تداوم کسب‌وکار، آمادگی، تأمین و حفظ کنترل‌ها و قابلیت‌هایی است که به سازمان امکان می‌دهد در برابر وقایع وقفه‌ساز، توانایی ادامه فعالیت‌های حیاتی خود را حفظ کند”

شاخص‌های بازیابی از بحران(DR)

حداکثر زمان قابل قبول برای بازگشت سرویس: **(RTO)Recovery Time Objective**

حداکثر میزان داده‌ای که میتوان از دست داد: **(RPO)Recovery Point Objective**

معماری تاب‌آور3DC ؛ پایداری در سطح ملی

اجزای مدل 3DC:

- **سایت اصلی (Production Site):** مرکز فعال سرویس‌دهی روزانه.
- **سایت پشتیبان محلی (Near-Site DR):** در فاصله نزدیک (Sync) برای مقابله با خطاهای سخت‌افزاری.
- **سایت پشتیبان راه دور (Remote-Site DR):** در شهر یا منطقه‌ای دیگر (Async) برای مقابله با شرایط جنگ و بلایای وسیع.

ویژگی‌های کلیدی:

- همگام‌سازی لحظه‌ای (Real-time Replication): حداقل‌سازی میزان از دست رفتن داده‌ها (RPO نزدیک به صفر).
- پایداری جغرافیایی: مصونیت در برابر تخریب فیزیکی یک منطقه شهری در اثر حملات نظامی.
- سوئیچ خودکار: انتقال سریع بار ترافیکی به سایت سوم در صورت سقوط دو سایت اول.

استراتژی‌های تداوم سرویس؛ منطق بهره‌برداری از منابع

معماری Active-Passive(سایت گرم/سرد):

وضعیت: یک سایت فعال و سایت‌های دیگر در حالت آماده‌باش

زمان بازیابی (RTO): نیاز به زمان برای سوئیچ کردن و بالا آمدن سرویس در سایت پشتیبان.

کاربرد: مناسب برای سرویس‌های با حساسیت کمتر.

معماری Active-Activeظرفیت تمام‌فعال

وضعیت: تمام دیتاسنترها همزمان در حال سرویس‌دهی و پردازش ترافیک هستند.

مزیت استراتژیک: حذف زمان وقفه (Zero Downtime)؛ اگر یک سایت منهدم شود، کاربران بدون متوجه شدن، روی سایت‌های دیگر باقی می‌مانند.

کاربرد: برای هسته اصلی معاملات بیمه‌ای و پایگاه داده‌های بانکی.

شبکه ارتباطی مقاوم

- پروتکل مسیریابی SD-WAN اختصاصی
- لینک‌های اختصاصی بر بستر توانیر (OPGW)
- پشتیبان ماهواره‌ای اختصاصی(VSAT)
- تنوع اپراتور در لایه MPLS و استفاده از مسیرهای فیزیکی مجزا (Physical Diversity)
- تونلینگ امن (IPsec Over GRE)

پایداری سایبری و پایش متمرکز در شرایط اضطرار

پایش ۲۴/۷ زیرساخت: رصد لحظه‌ای ترافیک شبکه بین تهران و سایت‌های پشتیبان برای شناسایی الگوهای مشکوک و حملات سایبری پیش از وقوع تخریب.

پاسخگویی خودکار به حوادث (SOAR): استفاده از سناریوهای پیش‌فرض برای مسدودسازی خودکار آی‌پی‌های مهاجم و ایزوله کردن بخش‌های آسیب‌دیده بدون نیاز به دخالت انسانی.

صیانت از یکپارچگی داده‌ها: مراقبت ویژه از فرآیند Replicate شدن داده‌ها بین سایت‌ها تا اطمینان حاصل شود که دیتای منتقل شده به سایت‌های دور، آلوده یا دستکاری نشده باشد.

تیم واکنش سریع (CSIRT): استقرار تیم‌های متخصص امنیت به صورت توزیع‌شده (در تهران و محل سایت‌های پشتیبان) برای مدیریت بحران در صورت قطع دسترسی‌های راه دور.

پیاده‌سازی مدل Zero Trust در زیرساخت توزیع‌شده

- حذف مفهوم شبکه داخلی امن
- ریزقطعه‌بندی (Micro-Segmentation)
- دسترسی با حداقل امتیاز (Least Privilege)
- احراز هویت چندعاملی (MFA) سخت‌گیرانه

پیاده‌سازی مدل Zero Trust در زیرساخت توزیع‌شده

- حذف مفهوم شبکه داخلی امن
- ریزقطعه‌بندی (Micro-Segmentation)
- دسترسی با حداقل امتیاز (Least Privilege)
- احراز هویت چندعاملی (MFA) سخت‌گیرانه

مدیریت و صیانت از داده‌های مشتریان (Data Sovereignty)

- همگام‌سازی بی‌وقفه (Real-time Replication)
- رمزنگاری داده‌های در حال حرکت و ساکن
- نسخه‌برداری تغییرناپذیر (Immutable Backup)
- پاکسازی و حذف امن (Data Sanitization)

- ترکیب تیم پاسخگویی
- پروتکل ارتباطی اضطراری
- سطوح تصحیح و تایید
- مانورهای شبیه‌سازی (War Gaming)

ساختار انسانی و فرآیندهای تصمیم‌گیری در شرایط اضطرار

سناریو بحران	وضعیت عملیاتی	اقدام کلیدی (Response)
انهدام یا خروج کامل دیتاسنتر اصلی	بحران سطح قرمز (Critical)	فعال‌سازی پروتکل **Failover**؛ انتقال آنی بار ترافیکی به سایت‌های پشتیبان در دو شهر دور و برقراری سرویس از لایه DR.
حمله باج‌افزاری به زیرساخت فناوری اطلاعات	بحران امنیتی (Security)	ایزوله کردن لایه ذخیره‌سازی؛ قطع دسترسی‌های مشکوک و بازیابی داده‌ها از **Immutable Backup** (بک‌آپ‌های غیرقابل تغییر).
قطع اینترنت بین‌المللی / اختلال سراسری	محدودیت زیرساختی	سوئیچ بر روی سایر زیرساخت های ارتباطی موجود

فناوری‌های نوین؛ پیشران‌های تاب‌آوری هوشمند

- Hybrid Cloud (بر ترکیبی)
- Edge Computing (پردازش در لبه)
- هوش مصنوعی در امنیت
- Cloud-Native DR

نقشه راه پیشنهادی برای شرکتهای بیمه

- ارزیابی وضعیت فعلی
- شناسایی ریسکها و اولویت بندی سرویسها
- طراحی معماری تابآور
- پیادهسازی راهکار بازیابی از بحران
- انجام تستها و مانورهای دورهای

با سپاس از شما