



خدمات تاب‌آوری زیرساخت

برای روزهایی که توقف، گزینه نیست

ارزیابی، طراحی، اجرا و آزمون آمادگی زیرساخت، امنیت و بازیابی، برای
سازمان‌هایی که خدمات حیاتی دارند

پشتیبان‌گیری و بازیابی

امنیت و ارتباطات

سایت بازیابی بحران

ارزیابی آمادگی



وقتی چند اختلال همزمان اتفاق می افتند

داشتن نسخه پشتیبان یا سایت دوم به تنهایی کافی نیست. مهم این است که اگر چند بخش **همزمان** از کار بیفتند، خدمات حیاتی تا چه حد ادامه پیدا می کنند.

چهار نوع تهدید که ممکن است همزمان رخ دهند



اختلال فیزیکی

قطع برق، آسیب به دیتاسنتر یا نبود دسترسی به محل؛ چند سرویس ممکن است همزمان متوقف شوند.



حمله سایبری مخرب

باغافزار، بدافزار پاک کننده داده، سرقت رمز عبور یا حمله DDOS؛ نسخه های پشتیبان متصل به شبکه هم ممکن است آسیب ببینند.

همزمان

نه یکی یکی



تأمین و نیروی انسانی

کمبود قطعه، نبود متخصص کلیدی یا روشن نبودن اختیارات در بحران؛ بازیابی طولانی تر می شود.



قطع ارتباطات و خدمات بیرونی

قطع اینترنت بین الملل، سرویس ابری، DNS یا سرور مدیریت لایسنس؛ سرویس های وابسته از کار می افتند.

سه فرض رایج که دیگر جواب نمی دهد

01 «در هر زمان فقط یک خرابی رخ می دهد»

حمله سایبری و اختلال فیزیکی می توانند همزمان رخ دهند.

02 «سایت پشتیبان سالم می ماند»

بدافزار پاک کننده، نسخه های متصل به شبکه را هم پاک می کند؛ سایت نزدیک هم در همان محدوده خطر است.

03 «تأمین کننده همیشه در دسترس است»

لایسنس، به روزرسانی و قطعه ممکن است ماه ها قابل تأمین نباشد.

سؤال درست برای مدیران این نیست که «اگر سرور خراب شد چه کنیم؟»
«اگر چند بخش همزمان از کار بیفتند، کدام خدمات باید ادامه پیدا کنند، با چه ظرفیتی و تا چه مدت؟»

از پیشگیری تا بازیابی، در شش مرحله

هدف این است که احتمال اختلال کم شود، اثر آن محدود بماند و بازیابی در عمل آزموده شود.

شش مرحله

چرخه پیوسته: یافته‌های هر مانور، مرحله شناخت را به‌روز می‌کند

۱ شناخت

شناسایی خدمات حیاتی، تهدیدها، وابستگی‌ها و نقاط
Single Point of Failure

۲ محافظت

تقسیم‌بندی شبکه، کنترل هویت و دسترسی، امن‌سازی و کنترل تغییرات

۳ مهار

تشخیص سریع، جداسازی بخش آسیب‌دیده، محدودکردن حرکت جانبی و حفظ ردپا و آثار حمله

۴ ادامه خدمت

ادامه خدمات ضروری با رویه‌های جایگزین و اولویت‌بندی منابع

۵ بازیابی

بازیابی از نسخه سالم و جدا از شبکه، بررسی پاک بودن و بازگشت مرحله‌ای سرویس

۶ یادگیری

مانور، اندازه‌گیری زمان واقعی بازیابی و به‌روزرسانی طرح

استانداردهای مبنای کار

RTO · RPO

RTO: حداکثر زمان مجاز توقف یک خدمت
RPO: حداکثر داده‌ای که از دست رفتنش قابل قبول است

ISO 22316

راهنمای تاب‌آوری سازمانی؛ برای سنجش آمادگی، راهبری، منابع و یادگیری

ISO 22301

مدیریت تداوم کسب‌وکار؛ برای ساختن و نگهداری برنامه تداوم

این استانداردها مبنای طراحی و ارزیابی ما هستند. استفاده از آن‌ها به معنای داشتن گواهی انطباق نیست؛ گواهی فقط با ممیزی رسمی صادر می‌شود.

اول وضعیت را می‌سنجیم، بعد راهکار می‌دهیم

هر همکاری با ارزیابی شروع می‌شود. آنچه تحویل می‌گیرید مستند و قابل بررسی است: طرح فنی، فهرست موارد نیازمند اصلاح، معیار پذیرش و گزارش آزمون.

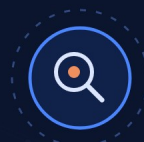
۱۵-۱۰

روز کاری · برآورد

نقطه شروع هر همکاری 01 / 04

ارزیابی آمادگی در برابر بحران

Resilience & Crisis Readiness Assessment



- مصاحبه با مدیران و تیم فنی، شناسایی خدمات حیاتی و وابستگی‌ها
- شناسایی نقاط Single Point of Failure در حوزه فنی، انسانی و تأمین
- بررسی سناریوهای ترکیبی: قطع ارتباط، از دست رفتن سایت، آلوده شدن پشتیبان
- سنجش ۹ ویژگی تاب‌آوری سازمانی بر مبنای ISO 22316

تحویل می‌گیرید گزارش مدیریت، نقشه ریسک و برنامه اقدام اولویت‌بندی‌شده با برآورد هزینه

02 / 04

طراحی و اجرای سایت بازیابی بحران (DR)

Disaster Recovery Site



- سایت دوم دور از محدوده خطر سایت اصلی، با برق و ارتباط مستقل
- حالت Active-Active یا Active-Standby، متناسب با RTO و RPO هر سرویس
- طراحی ساختار یکپارچه داده (Replication) و دستورالعمل‌های بازیابی
- پشتیبان جدا از شبکه و غیرقابل تغییر (Immutable و Air-Gapped)

تحویل می‌گیرید سایت بازیابی آماده به کار، زمان بازیابی اندازه‌گیری‌شده در مانور و دستورالعمل‌های بازیابی آزموده‌شده

امنیت، ارتباطات و تأمین تجهیزات

03 / 04

امنیت شبکه و ارتباطات اضطراری

Cyber Defense & Communications Resilience



- دسترسی اضطراری امن از راه دور، با حداقل سطح دسترسی لازم
- تقسیم‌بندی شبکه برای جلوگیری از حرکت جانبی (Lateral Movement)
- مرکز عملیات امنیت (SOC)، سامانه تحلیل رخداد (SIEM) و مرکز پایش شبکه (NOC)
- فایروال، حفاظت برنامه‌های کاربردی و ارزیابی آسیب‌پذیری

تحويل می‌گیرید شبکه تقسیم‌بندی‌شده، پایش رخدادهای امنیتی و امکان جدا کردن بخش آلوده با کمترین اثر بر سایر خدمات

04 / 04

تأمین تجهیزات و قطعات حیاتی

Spare Parts & Supplier Resilience



- بررسی وابستگی به تأمین‌کننده، لایسنس و به‌روزرسانی خارجی
- تعیین قطعات حیاتی و میزان ذخیره لازم
- شناسایی تجهیزات جایگزین قابل تأمین
- تأمین تجهیزات شبکه، امنیت، سرور و ذخیره‌سازی از پیشنهاد فنی تا تحويل

تحويل می‌گیرید فهرست قطعات حیاتی با ذخیره پیشنهادی و برآورد مدت قابل دوام بدون واردات

قرارداد پشتیبانی سالانه

آمادگی با یک پروژه تمام نمی‌شود و باید نگهداری شود: مانور دوره‌ای، بازبینی سالانه، به‌روزرسانی دستورالعمل‌ها و پشتیبانی فنی با سطح خدمات توافق‌شده (SLA).



امنیت و زیرساخت، با هم طراحی می‌شوند

به جای کنار هم گذاشتن ابزارهای جدا از هم، کنترل‌ها را بر اساس دارایی‌ها، کاربران، مسیر داده و اثر هر اختلال طراحی می‌کنیم.

شش حوزه طراحی

اتصال امن و افزونه

شبکه داخلی، ارتباط شعب و وایرلس، با مسیر جایگزین در نقاط حساس

هویت و دسترسی

احراز هویت مرکزی، دسترسی بر اساس نقش، احراز هویت چندمرحله‌ای (MFA) و مدیریت سطوح دسترسی (PAM)

حفاظت و بازرسی ترافیک

فایروال مرزی و داخلی، کنترل برنامه‌ها، حفاظت وب و کنترل دسترسی از راه دور

تقسیم‌بندی و مهار

جدا کردن بخش کاربران، سرورها، مدیریت، مهمان، تجهیزات صنعتی و پشتیبان؛ و محدود کردن ارتباط بین بخش‌ها

مدیریت و اتوماسیون

مدیریت متمرکز تنظیمات، کنترل تغییرات، نسخه‌بندی پیکربندی و شناسایی تغییرات ناخواسته

پایش و پاسخ‌گویی

جمع‌آوری رخدادها، تحلیل هشدارها، پایش سلامت زیرساخت و رویه پاسخ به رخداد

ترتیب طراحی، از کسب‌وکار تا پاسخ

01 دارایی‌ها و فرایندهای کسب‌وکار

02 کاربران و سطح دسترسی

03 سیاست دسترسی و تقسیم‌بندی

04 اجرای کنترل‌های امنیتی

05 داده‌های پایش و تحلیل

06 پاسخ، بازیابی و بهبود

برند و محصول را بعد از شناخت وضعیت موجود، نیاز عملیاتی، مهارت تیم و امکان تأمین انتخاب می‌کنیم؛ طراحی به برند خاصی وابسته نیست.

نسخه پشتیبان دارید؛ اما می‌توانید آن را بازیابی کنید؟

موفق بودن پشتیبان‌گیری کافی نیست. معیار اصلی این است که خدمت در زمان توافق‌شده و با کمترین داده از دست‌رفته برگردد.

چهار اصل بازیابی مطمئن

پشتیبان غیرقابل تغییر

جلوگیری از حذف یا رمزگذاری پشتیبان در دوره نگهداری؛
مکمل جداسازی و آزمون است، نه جایگزین آن

پشتیبان جدا از شبکه

پشتیبانی که با دسترسی‌های روزمره و حساب‌های مدیریتی
شبکه اصلی قابل حذف نباشد

آزمون سناریومحور

تمرین بازیابی، اندازه‌گیری RTO و RPO واقعی و اصلاح
دستورالعمل اجرایی بازیابی

بازیابی پاک

بررسی آلودگی و سالم بودن پشتیبان، پیش از اتصال دوباره
به شبکه

سناریوهای پیشنهادی برای مانور

01 از دست رفتن سایت اصلی یا بخشی از دیتاست

02 رمزگذاری سرورها و پشتیبان‌های متصل به شبکه توسط باج‌افزار

03 قطع ارتباط بیرونی یا از کار افتادن سرویس احراز هویت، DNS یا لایسنس

04 در دسترس نبودن نیروی کلیدی، مستندات یا تجهیزات جایگزین

معیار پذیرش، پیش از مانور با شما توافق می‌شود

آزمون عملکرد سرویس

زمان اندازه‌گیری‌شده

داده قابل بازیابی

سرویس‌های مشمول

مسئول تأیید

مبنای فنی: راهنمای CISA برای مقابله با باج‌افزار و استاندارد ISO 22301.

مسیر روشن، تحويل مشخص

حدود ۵ روز کاری

مرحله صفر - ارزیابی سریع

بررسی مستندات، چند مصاحبه کوتاه و بررسی سناریوهای اصلی؛ تحويل پنج مورد مهم نیازمند اصلاح با برآورد اولیه

حدود ۱۰ تا ۱۵ روز کاری

مرحله ۱ - ارزیابی جامع

نقشه خدمات و وابستگی‌ها، نقاط Single Point of Failure، سنجش آمادگی و برنامه مرحله‌بندی‌شده

به ترتیب اولویت

مرحله ۲ - طراحی و اجرا

طراحی تفصیلی، انتخاب کنترل‌ها و تجهیزات، پیاده‌سازی، مستندسازی و تعریف معیار آزمون و تحويل

قرارداد سالانه با SLA

مرحله ۳ - مانور و پشتیبانی

مانور دوره‌ای، بازبینی تغییرات، به‌روزرسانی رویه‌ها، پایش و پشتیبانی با SLA توافق‌شده

آنچه تحويل می‌گیرید

- ✓ فهرست خدمات حیاتی و وابستگی‌ها
- ✓ برنامه اقدام با مسئول، زمان و هزینه برآوردی

- ✓ گزارش مدیریتی و نقشه ریسک
- ✓ نقشه وضعیت موجود و طرح پیشنهادی
- ✓ طرح آزمون، معیار پذیرش و گزارش مانور

بدون تعهد خرید

هر مرحله تحويل مستقل و معیار پذیرش مشخص دارد

گزارش بی‌طرف

سطح آمادگی شما، همان‌طور که هست، در گزارش درج می‌شود

محرمانگی

قرارداد عدم افشا پیش از شروع؛ کار در محل شما

زمان‌ها برآوردی است؛ دامنه، زمان و هزینه نهایی پس از جلسه شناخت و بررسی مستندات مشخص می‌شود.

سازمان شما چقدر برای بحران آماده است؟

برای هر پرسش یک گزینه را علامت بزنید: ۰ = خیر یا نمی‌دانم، ۱ = حدی، ۲ = بله

#	پرسش	۰	۱	۲
01	فهرست مکتوب و اولویت‌بندی‌شده‌ای از خدمات حیاتی سازمان داریم.	☐	☐	☐
02	وابستگی‌های این خدمات (برق، شبکه، احراز هویت، DNS، لایسنس، API خارجی) شناسایی شده است.	☐	☐	☐
03	سایت پشتیبان دور از محدوده خطر سایت اصلی است و برق و ارتباط مستقل دارد.	☐	☐	☐
04	دست‌کم یک نسخه پشتیبان ایزوله یا تغییرناپذیر داریم که از شبکه اصلی قابل حذف نیست.	☐	☐	☐
05	در ۱۲ ماه گذشته بازیابی کامل را واقعاً آزموده‌ایم و زمان آن را می‌دانیم.	☐	☐	☐
06	سرویس‌های حیاتی بدون اینترنت بین‌الملل و کلود خارجی کار می‌کنند.	☐	☐	☐
07	برای قطعات حیاتی سخت‌افزار، ذخیره استراتژیک دست‌کم ۶ ماهه داریم.	☐	☐	☐
08	دسترسی اضطراری امن از راه دور آماده و آزموده است.	☐	☐	☐
09	پایش امنیتی ما (SOC/SIEM) می‌تواند نفوذ را در حد چند ساعت تشخیص دهد.	☐	☐	☐
10	زنجیره تصمیم‌گیری بحران با جانشین و اختیارات مکتوب تعریف شده است.	☐	☐	☐
11	مستندات حیاتی (پیکربندی، رمزهای اضطراری، رویه‌ها) خارج از سامانه اصلی نگهداری می‌شود.	☐	☐	☐
12	در ۱۲ ماه گذشته مانور سناریوی ترکیبی (حمله سایبری همراه با قطع ارتباط) برگزار کرده‌ایم.	☐	☐	☐
جمع امتیاز (از ۲۴)				

آسیب‌پذیر

۰ تا ۱۰

احتمال توقف طولانی زیاد است؛ ارزیابی را زودتر شروع کنید.

آمادگی ناقص

۱۱ تا ۱۸

پایه‌ها وجود دارد، اما چند مورد مهم نیاز به اصلاح دارد.

آمادگی نسبی

۱۹ تا ۲۴

یک مانور واقعی، درستی این امتیاز را نشان می‌دهد.

این پرسش‌نامه فقط تصویری اولیه می‌دهد و جایگزین ممیزی یا ارزیابی رسمی نیست؛ هر پاسخ «نمی‌دانم» خودش یک یافته است. امتیاز را برای ما بفرستید تا در جلسه‌ای حدود ۴۵ دقیقه‌ای مرور کنیم.

یک تیم، از ارزیابی تا پشتیبانی

از سال ۱۳۷۷ در طراحی، اجرا، تأمین و پشتیبانی زیرساخت فناوری اطلاعات فعالیت می‌کنیم. ارزیابی، اجرا و پشتیبانی با یک تیم انجام می‌شود و مسئولیت بین چند پیمانکار پخش نمی‌شود.

مشاوره و طراحی زیرساخت شبکه

نیازسنجی، طراحی و اجرا؛ اتصال امن سازمان‌های پراکنده با SD-WAN، IPSec و MPLS

دیتاسنتر، سرور و ذخیره‌سازی

مجازی‌سازی، پشتیبان‌گیری و بازیابی از بحران

امنیت شبکه و اطلاعات

طراحی NOC و SOC، سامانه تشخیص و جلوگیری از نفوذ (IDS/IPS)، تست نفوذ و ارزیابی آسیب‌پذیری

تأمین تجهیزات IT

تأمین و پیکربندی تجهیزات Cisco، HP، EMC، Fortinet؛ از پیشنهاد فنی تا تحویل

پشتیبانی و راهکار اختصاصی

بهینه‌سازی، مانیتورینگ و پشتیبانی؛ نرم‌افزار اختصاصی مبتنی بر هوش مصنوعی

محصول اختصاصی ما

ORyx | اوریکس

مدیریت متمرکز و خودکارسازی عملیات شبکه

مدیریت متمرکز · پشتیبان‌گیری از پیکربندی و جمع‌آوری لاگ
پیکربندی به صورت کد · استانداردسازی، Rollback و Remediation
هوش مصنوعی · تحلیل لاگ‌ها و دستیار فنی هوشمند
در طرح آمادگی، دید یکپارچه به شبکه و تحلیل لاگ‌ها را فراهم می‌کند.



مجوزها و سوابق اجرایی

اجرای پروژه‌های امنیت زیرساخت به مجوز افتا نیاز دارد. آپادانا رایانه کیمیا سه مجوز افتا و چند گواهی‌نامه صلاحیت دارد.

مجوزهای افتا



سایر گواهی‌نامه‌ها و عضویت‌ها

مجوز رسمی فعالیت در حوزه فاوا

گواهی‌نامه صلاحیت خدمات انفورماتیکی

گواهی رتبه‌بندی شورای عالی انفورماتیک

عضو انجمن کارفرمایان شرکت‌های اینترنتی

عضو سازمان نظام صنفی رایانه‌ای

تأیید صلاحیت ایمنی پیمانکاری

برخی کارفرمایان و پروژه‌ها

آب، انرژی، آموزش و سلامت

وزارت نیرو

پشتیبانی شبکه

آبفا هرمزگان

مشاوره امنیت و بهینه‌سازی زیرساخت

دانشگاه علامه طباطبائی

پشتیبانی شبکه

بیمارستان‌های شهید باهنر، مدنی و

شریعتی

شبکه، فیبر نوری و پشتیبانی

حاکمیتی و شهری

استانداری البرز

زیرساخت و سرویس‌های امنیتی، اتاق سرور،

فیبر نوری

استانداری تهران

کابل‌کشی و آرایش رک دیتاسنتر

شهرداری کرج

امنیت و مدیریت وصله‌های امنیتی، شبکه

سازمان مهندسی و عمران شهر تهران

مشاوره عارضه‌یابی سازمانی

صنعت، معدن و مناطق آزاد

شرکت ملی صنایع مس ایران

مشاوره، نگهداری و امنیت شبکه، تأمین

تجهیزات

فولاد کاوه جنوب کیش

امنیت، مدیریت وصله‌های امنیتی،

Cisco ISE

صنعتی و معدنی گهرزمین

امنیت زیرساخت، تجهیزات و لایسنس

سازمان منطقه آزاد اروند

امنیت زیرساخت، تجهیزات و لایسنس

پیش از بحران، وضعیت را روشن کنیم

برای شروع، یکی از این سه راه را انتخاب کنید:

پیشنهاد ما

A

جلسه ۴۵ دقیقه‌ای

با مدیریت، فناوری اطلاعات و
حراست؛ مرور خودارزیابی و تعیین
دامنه

با هماهنگی شما

B

مرحله صفر

گزارش آمادگی در ۳ سناریو و ۵
مورد مهم نیازمند اصلاح؛ حدود ۴
ساعت از وقت تیم شما

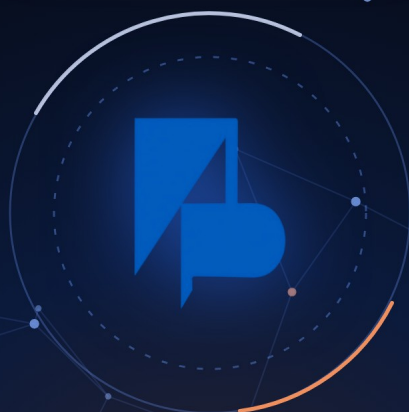
حدود ۵ روز کاری

C

ارزیابی کامل

گزارش مدیریتی و برنامه اقدام
اولویت‌بندی‌شده با برآورد هزینه

حدود ۱۰ تا ۱۵ روز کاری



آپادانا رایانه کیمیا

APADANA RAYANEH KIMIA

زیرساخت، امنیت، تجهیزات و راهکارهای هوشمند

۰۹۲۰ ۸۶۲ ۱۲۶۰

A.Moradi@Kimia-net.com

هماهنگی جلسه و مرحله صفر

آتنا مرادی · مسئول پروژه

۰۲۶-۳۲۲۲۲۱۳۴

امور اداری و مالی

۰۲۶-۳۲۵۱۹۴۹۴

فروش و بازرگانی

sales@kimia-net.com

ایمیل فروش

kimia-net.com

وبسایت

linkedin.com/company/kimianet

لینکدین

oryx.kimia-net.com

پلتفرم ORYX