ناوک هوشمند پویان

Edge Intelligent Enterprise

مشاوره و خدمات
بازرسی امنیت سایبری

www.navak-ai.ir

مشاوره و خدمات
بازرسی
امنیت سایبری

در عصر تحول دیجیتال، اطلاعات به‌عنوان ارزشمندترین دارایی سازمان‌ها شناخته می‌شود و حفاظت از آن‌ها به یکی از چالش‌های کلیدی هر سازمان بدل شده است. تهدیدات سایبری هر روز پیچیده‌تر و هدفمندتر می‌شوند و به‌سرعت در حال گسترش‌اند. برای مقابله با این تهدیدات، اتخاذ رویکردی جامع و نظام‌مند در حوزه امنیت اطلاعات ضروری است. ارائه مجموعه‌ای یکپارچه از خدمات تخصصی امنیت سایبری، سازمان‌ها را قادر می‌سازد تا علاوه بر افزایش سطح امنیت، از آسیب‌های احتمالی و خسارات سنگین ناشی از نفوذها جلوگیری نمایند.

تحلیل وضعیت فعلی امنیتی

اولین گام برای ارتقاء امنیت، درک صحیح از وضعیت فعلی است. در این بخش، خدماتی جهت بررسی سطح فعلی امنیت اطلاعات سازمان ارائه می‌شود:

- شناسایی زیرساخت‌های حیاتی فناوری اطلاعات
- تحلیل ساختار شبکه، نقاط ورود و مسیرهای حمله احتمالی
- بررسی سیاست‌های امنیتی، مجوزهای دسترسی و مکانیزم‌های کنترلی
- ارزیابی بلوغ امنیتی با استفاده از مدل‌هایی چون CMMI ، NIST CSF
- مستندسازی نقاط قوت و ضعف فعلی

این تحلیل پایه‌ای برای برنامه‌ریزی اقدامات امنیتی بعدی خواهد بود.

ارزیابی آسیب‌پذیری‌ها و تست نفوذ

تست نفوذ یکی از مؤثرترین راهکارها برای ارزیابی واقع‌گرایانه سطح امنیت است. در این خدمت:

- استفاده از روش‌های تست نفوذ مشکی(Black Box) ، خاکستری (Gray Box) و سفید(White Box)
- انجام اسکن‌های دستی و خودکار جهت شناسایی آسیب‌پذیری‌ها در سرویس‌ها، پورت‌ها، پایگاه‌های داده و برنامه‌های وب
- شبیه‌سازی حملات واقعی جهت ارزیابی کارایی سیستم‌های دفاعی
- تست مهندسی اجتماعی برای بررسی میزان آمادگی منابع انسانی
- تهیه گزارش تحلیلی با جزئیات فنی و مدیریتی، و ارائه راهکارهای اصلاحی

این مرحله به تصمیم‌گیران امکان می‌دهد تا سرمایه‌گذاری امنیتی خود را بر اساس خطرات واقعی برنامه‌ریزی کنند.

021-88109330
0933-6889690
www.navak-ai.ir
info@navak-ai.ir

مشاوره و خدمات
بازرسی
امنیت سایبری

پایش مداوم تهدیدات و پاسخ به حوادث امنیتی

تهدیدات سایبری محدود به یک نقطه‌زمانی نیستند؛ از این‌رو، پایش دائمی رفتارهای غیرعادی و پاسخ سریع به حوادث حیاتی است:

- طراحی و استقرار سیستم SIEM برای جمع‌آوری، نرمال‌سازی و تحلیل داده‌های امنیتی
- تعریفKPI های امنیتی و تنظیم هشدارهای مبتنی بر رفتار
- تشکیل تیم پاسخ‌گویی به حوادث (IRT) با دستورالعمل‌های دقیق عملیاتی(Playbook)
- ایجاد روال‌های شناسایی، مهار، ریشه‌یابی و بازیابی پس از حادثه
- تهیه گزارش نهایی برای تحلیل ریشه‌ای علت وقوع حادثه و اقدامات اصلاحی

این سامانه و فرآیندها، زمان شناسایی تهدید را کاهش و بهره‌وری عملیات امنیتی را افزایش می‌دهد.

مدیریت ریسک اطلاعات و انطباق با استانداردها

شناسایی، تحلیل و کاهش ریسک‌های سایبری از ملزومات مدیریت حرفه‌ای امنیت اطلاعات است. در این حوزه:

- شناسایی دارایی‌های اطلاعاتی و دسته‌بندی آن‌ها بر اساس اهمیت و حساسیت
- تحلیل تهدیدات و آسیب‌پذیری‌های مرتبط با هر دارایی
- سنجش احتمال وقوع و تأثیر ریسک برای اولویت‌بندی اقدامات
- طراحی ماتریس ریسک و تدوین برنامه‌های مقابله و کاهش
- مشاوره جهت پیاده‌سازی چارچوب‌ها و استانداردهای جهانی(ISO 27001, NIST, COBIT, GDPR, HIPAA)

انطباق با استانداردها، ضمن افزایش اعتماد ذی‌نفعان، موجب ارتقاء موقعیت رقابتی سازمان نیز می‌شود.

پیاده‌سازی سیستم مدیریت امنیت اطلاعات بر اساس ISO 27001:2022

این خدمت شامل طراحی و پیاده‌سازی چارچوب جامع مدیریت امنیت اطلاعات (ISMS) مطابق با الزامات استاندارد بین‌المللی ISO/IEC 27001:2022 است:

- تعریف دامنه سیستم مدیریت امنیت اطلاعات
- تحلیل ریسک اطلاعاتی بر اساسISO 27005
- تدوین سیاست‌ها، رویه‌ها و مستندات امنیتی
- طراحی کنترل‌های امنیتی مبتنی برAnnex A
- آموزش پرسنل، اجرای ممیزی داخلی و آمادگی برای گواهی‌نامه

این پیاده‌سازی تضمین می‌کند که امنیت اطلاعات سازمان در چارچوبی رسمی، ساخت‌یافته و قابل پایش مدیریت شود.

021-88109330
0933-6889690
www.navak-ai.ir
info@navak-ai.ir

مشاوره و خدمات
بازرسی
امنیت سایبری

پیاده‌سازی سیستم مدیریت تداوم کسب‌وکار بر اساس ISO 22301:2019

در این خدمت، سیستم مدیریت تداوم کسب‌وکار (BCMS) مطابق استاندارد ISO 22301 پیاده‌سازی می‌شود:

- تحلیل تأثیر کسب‌وکار (BIA) و شناسایی فرآیندهای حیاتی
- ارزیابی ریسک‌های مختل‌کننده عملیات
- تدوین استراتژی‌های بازیابی و طرح‌های پاسخ اضطراری
- طراحی سناریوهای تمرینی و تست برنامه‌های تداوم
- مستندسازی کامل و آمادگی برای ممیزی گواهی‌نامه

هدف، حفظ و بازیابی عملیات کلیدی سازمان در شرایط بحرانی و اضطراری است.

پیاده‌سازی NIST Cybersecurity Framework

چارچوب امنیت سایبری NIST یک مدل بالغ برای مدیریت ریسک سایبری است که بر ۵ حوزه اصلی استوار است: شناسایی، حفاظت، شناسایی تهدید، پاسخ و بازیابی.

- تحلیل وضعیت فعلی سازمان در تطابق باNIST CSF
- طراحی برنامه ارتقاء بلوغ سایبری بر اساس ارزیابی گپ(Gap Analysis)
- پیاده‌سازی سیاست‌ها و کنترل‌های متناسب با هر حوزه
- تنظیم شاخص‌های اندازه‌گیری عملکرد امنیتی(Metrics)
- مستندسازی مدل عملیاتی جهت ممیزی یا انطباق داخلی

این چارچوب برای سازمان‌هایی مناسب است که خواهان ساختار منعطف، قابل اندازه‌گیری و سازگار با الزامات قانونی هستند.

پیاده‌سازی کنترل‌های حریم خصوصی بر اساس استاندارد ISO/IEC 27701

با رشد الزامات قانونی حفاظت از داده‌های شخصی، پیاده‌سازی یک سیستم مدیریت حریم خصوصی (PIMS) مبتنی بر ISO/IEC 27701 ضروری است:

- گسترش ISMS موجود برای پوشش الزامات حریم خصوصی
- تعریف نقش‌های پردازش‌گر (Processor) و کنترل‌گر داده(Controller)
- طراحی سیاست‌ها، فرآیندها و کنترل‌های مرتبط با حفاظت از داده‌های شخصی
- آموزش پرسنل در حوزه حریم خصوصی
- انطباق با قوانین ملی و بین‌المللی مانند GDPR

این خدمت سبب افزایش اعتماد مشتریان و ذی‌نفعان به مسئولیت‌پذیری سازمان در قبال داده‌های شخصی خواهد شد.

021-88109330
0933-6889690
www.navak-ai.ir
info@navak-ai.ir

طراحی معماری امنیتی سازمانی

طراحی امنیت باید از ابتدا در معماری سیستم لحاظ شود تا بتوان تهدیدات را در همان مراحل اولیه کنترل کرد.
این خدمات شامل:

- تحلیل الزامات امنیتی بر اساس ماهیت کسب‌وکار
- طراحی مدل دفاع در عمق (Defense in Depth) شامل چندین لایه کنترل امنیتی
- جداسازی منطقی شبکه‌ها، ناحیه‌بندی (Segmentation) و کنترل ترافیک
- استفاده از معماری Zero Trust برای کاهش سطح اعتماد پیش‌فرض
- طراحی سیاست‌های مدیریت دسترسی، احراز هویت چندمرحله‌ای و رمزنگاری

معماری امنیتی صحیح، بستری پایدار برای توسعه امن سازمان فراهم می‌کند.

استقرار راهکارهای فنی امنیتی

اجرای دقیق راهکارهای فنی امنیتی نقش کلیدی در محافظت از دارایی‌های سازمان دارد. در این فاز:

- پیاده‌سازی تجهیزات سخت‌افزاری مانند فایروال، روتر امن، سیستم کنترل دسترسی فیزیکی
- استقرار نرم‌افزارهای امنیتی مانند آنتی‌ویروس مرکزی، EDR، DLP، CASB
- راه‌اندازی سامانه‌های IDS/IPS برای تشخیص و جلوگیری از نفوذ
- استفاده از سامانه‌های WAF و امنیت ابری برای حفاظت از برنامه‌های تحت وب
- تست صحت‌سنجی، تنظیمات بهینه و مانیتورینگ مستمر عملکرد ابزارها

تجهیزات و ابزارها مطابق با نیاز، اندازه و ریسک‌پذیری سازمان انتخاب می‌گردند.

آموزش، فرهنگ‌سازی و شبیه‌سازی حملات

بدون مشارکت نیروی انسانی، بهترین سامانه‌های امنیتی نیز ممکن است ناکارآمد باشند. بنابراین:

- طراحی برنامه آموزشی امنیتی ویژه سطوح مختلف سازمان (مدیران، کارکنان، فنی)
- برگزاری جلسات آموزش حضوری، آنلاین و آزمون‌های سنجش درک امنیتی
- شبیه‌سازی حملات فیشینگ و تحلیل رفتار کاربران
- ارائه محتوای آموزشی چندرسانه‌ای و تعاملی جهت افزایش تأثیرگذاری
- راه‌اندازی کمپین‌های آگاهی‌بخشی منظم

ایجاد فرهنگ امنیت‌محور در سازمان، یکی از مؤثرترین روش‌ها برای مقابله با تهدیدات است.

021-88109330
0933-6889690
www.navak-ai.ir
info@navak-ai.ir

ارزیابی دوره‌ای و بهبود مستمر

امنیت سایبری فرایندی پویا است که نیاز به ارزیابی‌های مستمر دارد. در این راستا:

- طراحی شاخص‌های کلیدی عملکرد امنیتی(KPI)
- اجرای ممیزی‌های دوره‌ای داخلی و خارجی
- ارزیابی اثر بخشی اقدامات امنیتی قبلی
- پیشنهاد بهبود فرآیندها و به‌روزرسانی سیاست‌ها و راهکارها
- بررسی تکنولوژی‌های نوظهور امنیتی و پیشنهاد جایگزین‌های هوشمندانه

ارزیابی مداوم، موجب تکامل سیستم امنیتی و انطباق آن با تهدیدات در حال تغییر می‌شود.

ناوک هوشمند پویان

Edge Intelligent Enterprise

جهت اطلاعات بیشتر در راستای راه حل فوق با ما در ارتباط باشید

navak-ai.ir

021-88109330

0933-6889690

info@navak-ai.ir

اطلاعات جمع آوری شده توسط تیم تحقیقات **شرکت ناوک هوشمند پویان** به انجام رسیده است.