ایندکو
Ayco

بسته امن سازی شبکه سازمان

راهکاری جامع، یکپارچه و آینده‌نگر
برای ایمن‌سازی شبکه‌های سازمانی

در سال‌های اخیر، تهدیدات سایبری به‌طور چشمگیری افزایش یافته‌اند و سازمان‌ها را با چالش‌های بی‌سابقه‌ای مواجه کرده‌اند. بر اساس گزارش‌های معتبر جهانی:

- در سه‌ماهه سوم سال **۲۰۲۴**، میانگین حملات سایبری به هر سازمان به **۱,۸۷۶** مورد در هفته رسید که نسبت به مدت مشابه سال قبل **۷۵٪** افزایش داشته است.
- در سال **۲۰۲۴**، **۸۳٪** از سازمان‌ها حداقل یک حمله از داخل سازمان (insider attack) را تجربه کرده‌اند.
- مطالعات نشان می‌دهد که مهاجمان می‌توانند به شبکه **۹۳٪** از سازمان‌ها نفوذ کنند، حتی اگر این سازمان‌ها از راهکارهای امنیتی استفاده کرده باشند.

این آمارها نشان می‌دهند که حتی سازمان‌هایی که از راهکارهای امنیتی بهره می‌برند، در برابر تهدیدات پیشرفته و پیچیده‌ی امروزی آسیب‌پذیر هستند. دلایل اصلی این آسیب‌پذیری‌ها عبارتند از:

- عدم پیکربندی صحیح تجهیزات امنیتی
- به‌روزرسانی‌های ناقص یا ناهماهنگ
- عدم شناسایی نقاط ضعف در ساختار شبکه
- فقدان آموزش‌های کاربردی برای تیم‌های فناوری اطلاعات

باتوجه‌به این چالش‌ها، شرکت آیکو تصمیم گرفته است تا با ارائه‌ی بسته امن‌سازی شبکه سازمان، راهکاری جامع و تخصصی برای ارتقاء سطح امنیتی سازمان‌ها فراهم آورد. این بسته با رویکرد Hardening، به‌معنای تقویت و ایمن‌سازی ساختار شبکه و تجهیزات موجود، طراحی شده است تا:

- نقاط ضعف و خلأهای امنیتی شناسایی و برطرف شوند.
- تنظیمات و پیکربندی‌های تخصصی بر روی تجهیزات اعمال گردد.
- آموزش‌های کاربردی در حوزه امنیت و مانیتورینگ به تیم‌های فناوری اطلاعات ارائه شود.
- و در نهایت، سازمان‌ها به سطحی از امنیت دست یابند که در برابر تهدیدات پیشرفته مقاوم باشند.

1 مقدمه

2
چرا این بسته طراحی شده است؟

در فضای پرتلاطم امنیت سایبری امروز، صرفاً برخورداری از چند ابزار یا محصول امنیتی نمی‌تواند ضامن ایمنی یک سازمان در برابر تهدیدات روزافزون باشد. تجربه‌ی سال‌های اخیر و بررسی‌های میدانی متخصصان ما نشان داده است که اغلب سازمان‌ها علی‌رغم سرمایه‌گذاری‌های قابل توجه در حوزه امنیت، همچنان در برابر حملات هدفمند آسیب‌پذیر هستند. طراحی بسته امن‌سازی شبکه سازمان، پاسخی هوشمندانه به این خلأهای پنهان و تهدیدات ساختاری است. دلایل اصلی شکل‌گیری این بسته به شرح زیر است:

۱. غلبه نگاه محصول‌محور بر راهکارمحور

در بسیاری از سازمان‌ها، امنیت سایبری به خرید چند محصول امنیتی تقلیل یافته است، بدون آنکه طراحی معماری امنیتی، پیکربندی صحیح، تحلیل دقیق نیازها و آموزش نیروهای انسانی مورد توجه قرار گیرد. این رویکرد نه‌تنها ناکارآمد، بلکه بعضاً خطرآفرین نیز بوده است. از همین‌رو، این بسته با تمرکز بر «راهکار یکپارچه و هدفمند» طراحی شده است.

۲. فقدان رویکرد جامع و یکپارچه در حوزه امنیت

بخش‌های مختلف سازمان‌ها، از زیرساخت تا نرم‌افزار و حتی مدیریت ارشد، عموماً نگاه‌های متفاوت و گاه متضادی به مقوله امنیت دارند. بسته پیشنهادی ما، با در نظر گرفتن تمامی لایه‌ها و سطوح عملیاتی، رویکردی جامع، هماهنگ و فرابخشی ارائه می‌دهد.

۳. رشد فزاینده تهدیدات هدفمند علیه سازمان‌های داخلی

باتوجه‌به افزایش کمّی و کیفی حملات سایبری هدفمند به سازمان‌های ایرانی در سال‌های اخیر، نیازی مبرم به راهکاری فعال، پیش‌نگر و منطبق با واقعیت‌های بومی احساس می‌شود. این بسته با همین هدف و مبتنی بر تجربیات میدانی طراحی گردیده است.

۴. نبود مستندسازی دقیق تنظیمات و سیاست‌های امنیتی

یکی از چالش‌های پنهان بسیاری از سازمان‌ها، عدم آگاهی از وضعیت دقیق شبکه، تجهیزات و تنظیمات اعمال‌شده است. در چنین شرایطی، هرگونه ضعف یا اشتباه پیکربندی می‌تواند منجر به رخنه‌های جدی امنیتی شود. مستندسازی فنی و تخصصی، یکی از ارکان اصلی این بسته به شمار می‌رود.

۵.خلأ آموزش کاربردی و به‌روز برای مدیران فناوری اطلاعات

مدیران فناوری اطلاعات در سازمان‌ها، تحت فشار بالای مسئولیت‌های جاری، اغلب فرصت کافی برای به‌روزرسانی دانش تخصصی در حوزه امنیت ندارند. این بسته با ارائه آموزش‌های هدفمند، عملیاتی و همچنین فراهم‌سازی بستر بازدید از نمایشگاه تخصصی Gitex دبی، گامی مؤثر در راستای ارتقای دانش تصمیم‌سازان حوزه فناوری اطلاعات محسوب می‌شود.

3
اجـــزای بستـــه امن‌سازی شبکه

بسته امن‌سازی شبکه سازمان، بر پایه نیازسنجی دقیق، دانش فنی روز و تجارب عملی متخصصان حوزه امنیت طراحی شده است. این بسته شامل مجموعـه‌ای از اقدامـات ساختاریافته و تخصصی در سه محور اصلی «تحلیل وضعیت موجود»، «اصلاح، ایمن‌سازی و بهینه‌سازی» و «آموزش و ارتقاء دانش سازمانی» می‌باشد. در ادامه، مهم‌ترین اجزای این بسته به تفکیک تشریح شده است:

۱ ارزیابی امنیتی و شناخت وضعیت موجود

- تهیه نقشه‌ی دقیـق دارایـی‌های شبکه (Network Asset Inventory)
- شناسایی نقاط آسیب‌پذیر در تجهیزات، سیاست‌ها و فرآیندهای امنیتی
- بررسی تنظیمات تجهیزات امنیتی موجود نظیر فایروال‌ها، آنتی‌ویروس‌ها، ایمیل سرورها و ...
- تحلیل سطح دسترسی کاربران، گروه‌ها و سیاست‌های کنترلی
- ارائه گزارش جامع آسیب‌پذیری‌ها و شکاف‌های امنیتی

۲ طراحی معماری امنیتی بهینه و قابل پیاده‌سازی

- تدویـن نقشـه راه امـن‌سـازی متناسـب بـا ساختـار سازمـان
- تعریف مدل Zero Trust در لایه‌های مختلف شبکه (در صورت امکان‌پذیری)
- طراحـی سیاسـت‌های طبقه‌بنـدی اطلاعات و کنتـرل دسترسـی
- ارائه پیشنهادات برای بهینه‌سازی زیرساخت امنیتی با در نظر گرفتن منابع موجود سازمان

۳ پیاده‌سازی تنظیمات تخصصی (Hardening)

- انجام پیکربندی پیشرفته بر روی تجهیزات امنیتی (Firewall, UTM, IPS, Email Security, etc)
- اعمال تنظیمات کنترلی پیشگیرانه و واکنشی در سیستم‌عامل‌ها، تجهیزات شبکه و سرورها
- پیاده‌سازی سیاست‌های امنیتی متناسب با ریسک‌ها و اهداف سازمان
- اجرای سیاست‌های Monitoring، Logging و Alerting با استفاده از ابزارهای تخصصی

۴ تأمین و ارائه مجوزهای نرم‌افزاری (License) مورد نیاز

- بررسی اعتبار و وضعیت لایسنس محصولات موجود
- ارائه و فعال‌سازی مجوزهای مورد نیاز برای تقویت امنیـت (بسته به نیاز سازمان و راهکارهای مورد تایید آیکو)
- ایجاد هماهنگی بین تجهیزات مختلف با فعال‌سازی ماژول‌های امنیتی مکمـل

۵ آموزش تخصصی و عملیاتی برای تیم فناوری اطلاعات

- برگزاری کارگاه‌های کاربردی امنیت شبکه با تمرکز بر محیط عملیاتی سازمان
- آموزش تشخیص و واکنش به تهدیدات (Incident Detection & Response)
- آموزش نحوه مانیتورینگ، تحلیل لاگ‌ها و اعمال سیاست‌های اصلاحی

۶ آماده سازی شبکه سازمان برای اجرای تست نفوذ تخصصی (به انتخاب سازمان با مجموعه‌ای متفاوت)

- انجام تست نفوذ در سطوح مختلف شبکه، سیستم‌عامل‌ها، سرویس‌ها و تجهیزات (اجرا توسط پیمانکار متفاوت - خارج از پکیج آیکو)
- تحلیل نقاط آسیب‌پذیر شناسایی‌شده در تست و اولویت‌بندی تهدیدها
- تهیه گزارش رسمی و فنی از نتایج تست با ارائه پیشنهادات اصلاحی

۷ رفع آسیب‌پذیری‌های شناسایی‌شده (Post-Test Hardening)

- اصلاح تنظیمات، به‌روزرسانی تنظیمات نرم‌افزارها و بازطراحی سیاست‌های امنیتی در نقاط آسیب‌پذیر
- اعمال تغییرات ساختاری برای جلوگیری از سوءاستفاده مجدد
- تست مجدد بخش‌های اصلاح‌شده جهت اطمینان از برطرف شدن تهدیدات

۸ ارتقاء آگاهی استراتژیک مدیران ارشد فناوری اطلاعات

- برگزاری نشست‌های تخصصی با مدیران برای تشریح نقاط ضعف ساختاری و پیشنهاد مسیرهای بهبود
- ارائه فایل‌های راهنما، مستندات و داشبوردهای مدیریتی برای تصمیم‌گیری مؤثر
- پکیج کامل شرکت در نمایشگاه GITEX دبی جهت آشنایی با جدیدترین روندها، محصولات و فناوری‌های امنیت سایبری در سطح بین‌المللی

4
مزایای بسته امن‌سازی برای سازمان و ویژگی‌های متمایز آن

بسته امن‌سازی شبکه سازمان، تنها یک راهکار فنی نیست؛ بلکه مسیری ساختاریافته برای ارتقای تاب‌آوری سایبری، کاهش ریسک‌های عملیاتی و افزایش اطمینان سازمان از پایداری خدمات فناوری اطلاعات است. طراحی این بسته با هدف ارائه راهکاری جامع، بومی‌سازی‌شده و قابل اطمینان صورت گرفته تا سازمان‌ها بتوانند با اطمینان بیشتر در برابر تهدیدات سایبری ایستادگی کنند .

الف مزایای راهبردی برای سازمان

افزایش سطح امنیت شبکه به‌صورت ساختاریافته و مستند

با اعمال تنظیمات دقیق و مهندسی‌شده، سطح پایه امنیت شبکه سازمان به‌صورت پایدار و قابل‌پیگیری ارتقاء می‌یابد.

کاهش ریسک نفوذ و از کارافتادگی خدمات حیاتی

با شناسایی شکاف‌های امنیتی و اصلاح آن‌ها قبل از بروز حملات، ریسک عملیاتی سازمان به‌طور چشم‌گیری کاهش می‌یابد.

بهینه‌سازی عملکرد تجهیزات و بهره‌برداری حداکثری از ظرفیت امنیتی موجود

بسیاری از سازمان‌ها علی‌رغم در اختیار داشتن تجهیزات حرفه‌ای، به دلیل پیکربندی ناکارآمد در معرض تهدید هستند. این بسته بهره‌وری این تجهیزات را به حداکثر می‌رساند.

ارتقای دانش فنی تیم داخلی و کاهش وابستگی به منابع بیرونی

از طریق آموزش‌های عملیاتی و تخصصی، تیم فناوری اطلاعات سازمان توانمندتر شده و در برابر تهدیدات آینده آماده‌تر خواهد بود.

افزایش آمادگی سازمان برای ممیزی‌ها و استانداردهای امنیتی

نتایج مستند و قابل ارائه این پروژه، پشتوانه مناسبی برای موفقیت در ممیزی‌های امنیتی داخلی و بین‌المللی خواهد بود.

دسترسی مستقیم به آخرین فناوری‌ها و ترندهای جهانی

از طریق تور تخصصی Gitex، مدیران فناوری اطلاعات با نوآوری‌های روز دنیا در حوزه امنیت آشنا شده و امکان تصمیم‌گیری به‌روزتری خواهند داشت.

4
مزایای بسته امن‌سازی برای سازمان و ویژگی‌های متمایز آن

ب- ویژگی‌های متمایز این بسته نسبت به راهکارهای رایج بازار

رویکرد پروژه‌محور و متعهد به نتایج

این بسته برخلاف بسیاری از خدمات مقطعی، به‌صورت پروژه‌ای کامل با زمان‌بندی مشخص و خروجی‌های قابل اندازه‌گیری اجرا می‌شود.

پوشش هم‌زمان تجهیزات، سیاست‌ها و رفتارهای سازمانی

امن‌سازی صرفاً محدود به ابزارها نیست. این بسته هم‌زمان به تنظیمات، ساختار دسترسی و رویه‌های امنیتی نیز می‌پردازد.

ترکیب عملیاتی سه عنصر تحلیل - اصلاح - آموزش

تحلیل دقیق، اصلاح ساختاریافته و آموزش هدفمند، سه ضلع این بسته هستند که در کنار هم، منجر به پایداری امنیت می‌شوند.

انجام تست نفوذ واقعی و اصلاح آسیب‌پذیری‌های شناسایی‌شده

برخلاف اغلب پروژه‌ها که تنها به گزارش اکتفا می‌کنند، در این بسته رفع عملیاتی آسیب‌پذیری‌ها جزو تعهدات اصلی است.

همراهی با تیمی متخصص، مورد تأیید برندهای معتبر امنیتی

پروژه توسط کارشناسانی اجرا می‌شود که آموزش‌دیده و مورد تأیید تولیدکنندگان معتبر حوزه امنیت سایبری هستند.

پشتیبانی اختصاصی و مستندسازی کامل مراحل

در طول اجرای پروژه، کلیه اقدامات مستندسازی شده و امکان پیگیری، ارزیابی و ارتقاء مداوم فراهم خواهد بود.

5
مخاطب این راهکار چه سازمان‌هایی هستند؟

بسته امن‌سازی شبـکه سازمـان به‌گونه‌ای طراحی شده است که پاسخ‌گوی نیازهای امنیتی طیف گسترده‌ای از سازمان‌ها در بخش‌های مختلف اقتصادی، صنعتی و خدماتی باشد. این راهکار برای آن دسته از سازمـان‌هایی تدوین شده است که:

- دارای زیرساخت فناوری اطلاعات گسترده، متشکل از تجهیزات شبکه، سرورها، سامانه‌های نرم‌افزاری و کاربران متعدد هستند.
- در برابر تهدیدات سایبری، مسئول حفظ اطلاعات محرمانه، مالی، عملیاتی یا داده‌های شخصی مشتریان و کارکنان خود هستند.
- از راهکارهای امنیتی مختلف استفاده می‌کنند اما به دنبال اطمینان از پیکربندی صحیح، یکپارچگی راهکارها و رفع خلأهای امنیتی موجود هستند.
- ملزم به رعایت الزامات قانونی، حاکمیتی یا استانداردهای بین‌المللی امنیت اطلاعات مانند ISO ۲۷۰۰۱) بوده یا قصد آمادگی برای ممیزی‌های امنیتی دارند.
- تمایل دارند دانش تیم فناوری اطلاعات خود را در زمینه امنیت سایبری افزایش داده و وابستگی به مشاوران خارجی را کاهش دهند.

5

مخاطب این راهکار چه سازمان‌هایی هستند؟

بر این اساس، بسته امن‌سازی شبکه، برای سازمان‌های زیر به‌طور خاص توصیه می‌شود:

- **شرکت‌های بزرگ خصوصی در حوزه‌های مالی، فناوری، تولید، لجستیک، خرده‌فروشی و انرژی**
- **هلدینگ‌ها، شرکت‌های مادر و زیرمجموعه‌های آنها با ساختار فناوری اطلاعات متمرکز یا توزیع‌شده**
- **سازمان‌های نیمه‌دولتی یا عمومیِ غیردولتیِ حافظ منابع حیاتی اطلاعاتی**
- **بانک‌ها، مؤسسات اعتباری، شرکت‌های پرداخت و فین‌تک‌ها**
- **شرکت‌های دارویی، بهداشتی و مراکز درمانی خصوصی**
- **اپراتورها، شرکت‌های فناوری اطلاعات، دیتاسنترها و ارائه دهندگان خدمات ابری**
- **سازمان‌های دولتی دارای نقش حساس در زیرساخت‌های ارتباطی، صنعتی یا اطلاعاتی کشور**

این راهکار به‌صورت خاص برای سازمان‌هایی ارزش‌آفرین است که حفظ تداوم خدمات، اعتبار برند و امنیت اطلاعات، جزو اولویت‌های راهبردی آن‌ها تلقی می‌شود.

6
چـرا آیکـو؟

انتخاب پیمانکار یا شریک امنیتی مناسب، گامی تعیین‌کننده در موفقیت پروژه‌های امنیت سایبری است. شرکت آینده نگاران (آیکو) با سال‌ها تجربـه تخصصی، تیمی از کارشناسان خبره و همکاری با برندهای معتبر جهانی، بهترین انتخاب برای اجرای بسته امن‌سازی شبکه سازمان شماست. دلایل انتخاب آیکو عبارت‌اند از:

تخصص و تجربه اثبات‌شده

کارشناسان آیکو دارای گواهینامه‌ها و آموزش‌های تخصصی در حوزه امنیت شبکه هستند و سال‌ها سابقه موفق در اجرای پروژه‌های مشابه دارند.

رویکرد جامع و سفارشی‌سازی‌شده

آیکو هر پروژه را بر اساس نیازها و ساختار منحصربه‌فرد سازمان طراحی و اجرا می‌کند، به‌گونه‌ای که بهترین نتایج عملیاتی و امنیتی حاصل شود.

همکاری با برندهای پیشرو جهانی

آیکو نماینده رسمی محصولات و راهکارهای معتبر جهانی است که تضمین کیفیت و به‌روز بودن فناوری‌های مورد استفاده را فراهم می‌آورد.

تعهد به کیفیت و رضایت مشتری

آیکو فراتر از اجرای پروژه، به پشتیبانی مستمر و آموزش تیم سازمان متعهد است و موفقیت مشتری را هدف نهایی می‌داند.

مستندسازی کامل و شفاف

تمامی مراحل پروژه با دقت مستندسازی شده و گزارش‌های تحلیلی و عملیاتی به سازمان ارائه می‌گردد تا قابلیت رصد و ارتقاء مداوم فراهم شود.

تضمین رفع آسیب‌پذیری‌ها

آیکو تنها به شناسایی مشکلات بسنده نمی‌کند بلکه متعهد به رفع عملیاتی تمامی آسیب‌پذیری‌های شناسایی‌شده در تست نفوذ است.

7
تماس با ما

شهـــرک غـــرب، بلـــوار دریـا،
۲۱ متری گلها، پلاک ۳۲ واحد ۱

Hardening@ayco.ir

www.ayco.ir

02142305000