پروپوزال امن‌سازی شبکه و زیرساخت سازمانی

تفکیک خدمات بصورت ماژولار

Ayco ایندکو

www.ayco.ir

مقدمه

در دنیای پرشتاب و پرریسک امروز، امنیت سایبری دیگر یک انتخاب نیست؛ بلکه ضرورتی راهبردی برای تداوم کسب‌وکار، حفاظت از سرمایه‌های اطلاعاتی، و پایبندی به الزامات قانونی و استانداردهای بین‌المللی است. سازمان‌ها با تنوعی از تهدیدات نوظهور، حملات هدفمند، و مخاطرات ناشی از ضعف‌های زیرساختی مواجه‌اند که هر یک می‌تواند به اختلال، افشا یا از بین رفتن داده‌های حیاتی منجر شود.

شرکت **آیکو** (آینده نگاران)، به‌عنوان **پیشروترین ارائه‌دهنده محصولات و خدمات تخصصی امنیت شبکه در ایران**، با تکیه بر بیش از یک دهه تجربه عملیاتی، تیم فنی مجرب، و همکاری با برندهای بین‌المللی پیشتاز، اقدام به طراحی و ارائه **مدلی ساختاریافته، منعطف و ماژولار** برای امن‌سازی زیرساخت‌های فناوری اطلاعات سازمان‌ها نموده است.

این مدل با هدف پاسخگویی دقیق به نیازهای متنوع سازمان‌های ایرانی ـ اعم از دولتی، صنعتی، مالی و آموزشی ـ توسعه یافته و با بهره‌گیری از **بهترین تجربیات جهانی (Best Practices)**، **استانداردهای مرجع در دنیا**، و ابزارهای پیشرفته امنیتی، به سازمان‌ها این امکان را می‌دهد که:

- **امن‌سازی را بر اساس اولویت‌های واقعی خود آغاز کنند**، بدون الزام به پیاده‌سازی یک‌باره و کامل کل سیستم؛
- **از مزایای خدمات کاملاً تخصصی و قابل سفارشی‌سازی بهره‌مند شوند**؛
- و در نهایت **مسیر بلوغ امنیت سایبری خود را گام‌به‌گام، مستند و قابل اندازه‌گیری طی نمایند**.

در این مدل، **خدمات امن‌سازی به ۱۰ ماژول تخصصی** تفکیک شده‌اند که هر یک با هدف مشخص، برندها و ابزارهای پشتیبانی‌شده، خدمات قابل ارائه، و ارزش‌های افزوده خاص خود طراحی شده‌اند. این ماژول‌ها به‌صورت مستقل یا در قالب یک **پکیج جامع و یکپارچه**، قابل ارائه به سازمان‌ها می‌باشند.

در ادامه، شرح دقیق این ماژول‌ها ارائه خواهد شد.

ماژول ۱: امن‌سازی فایروال‌ها

🎯هدف

فایروال‌ها نخستین خط دفاعی شبکه سازمان هستند. هدف این ماژول، **ایمن‌سازی فایروال‌ها در برابر نفوذ، سوءاستفاده، تنظیمات اشتباه و ضعف‌های امنیتی** است. همچنین، با فعال‌سازی و تحلیل لاگ‌ها، امکان پایش دائمی و کشف سریع تهدیدات فراهم می‌شود.

🛠خدمات قابل ارائه

۱. بررسی و بهینه‌سازی سیاست‌های فایروال
۲. تنظیم کنترل دسترسی به مدیریت فایروال
۳. راه‌اندازی تحلیل لاگ و مانیتورینگ رویدادها
٤. پیکربندی Web Filtering وApplication Control
٥. ارزیابی آسیب‌پذیری و تست نفوذ کنترل‌شده
٦. مستندسازی و گزارش‌گیری مدیریتی و فنی

💡ارزش افزوده

- کاهش سطح حمله (Attack Surface) فایروال و جلوگیری از نفوذهای احتمالی
- افزایش قابلیت رهگیری تهدیدات با لاگ‌های غنی و تحلیل شده
- جلوگیری از خطاهای انسانی در تنظیمات پیچیده فایروال
- اطمینان از کارکرد صحیح ماژول‌های امنیتی مانندIPS ، AV، WAF، App Control

این ماژول به‌ویژه برای سازمان‌هایی که دارای چندین شعبه، دسترسی اینترنت پرمخاطب یا الزامات قانونی (مثل بانک‌ها، شرکت‌های مالی، مراکز داده و...) هستند، **ضروری و قابل توصیه** است.

ماژول ۲: امن‌سازی پایگاه‌داده

🎯هدف

پایگاه‌های داده در قلب بسیاری از فرآیندهای حیاتی سازمان قرار دارند و هرگونه نفوذ یا آسیب به آن‌ها می‌تواند **منجر به افشای اطلاعات محرمانه، دستکاری داده‌ها یا از دست رفتن اطلاعات حیاتی کسب‌وکار** شود. هدف این ماژول، پیاده‌سازی مجموعه‌ای از اقدامات امنیتی استاندارد و تخصصی برای محافظت از دیتابیس‌ها در برابر تهدیدات داخلی و خارجی است.

🛠خدمات قابل ارائه

۱. بررسی پیکربندی و Harden کردن پایگاه داده
۲. رمزنگاری داده‌ها در حالت سکون و حین انتقال(Data-at-Rest / In-Transit)
۳. راه‌اندازی تحلیل لاگ و مانیتورینگ رویدادها
٤. بررسی و محدودسازی دسترسی‌های شبکه‌ای
٥. ارزیابی آسیب‌پذیری و انجام تست امنیتی

💡ارزش افزوده برای سازمان

- محافظت از داده‌های حساس مشتریان، پرسنل و اطلاعات مالی
- کاهش احتمال رخدادهایی مانند SQL Injection وData Leakage
- افزایش شفافیت فعالیت‌ها و دسترسی‌ها برای حسابرسی و گزارش‌دهی
- اطمینان از انطباق با استانداردهای امنیتی مانندISO 27001 ، GDPR، یا مقررات داخلی

این ماژول، به‌خصوص در سازمان‌هایی که با داده‌های حساس کاربران، مالیات، سلامت یا اطلاعات تجاری سروکار دارند، **نقش اساسی در ایجاد اعتماد و کاهش ریسک‌های سازمانی** دارد.

ماژول ۳: امن‌سازی ویندوز سرورها

🎯هدف

ویندوز سرورها، به‌ویژه نقش‌هایی مانند **Active Directory**، **DNS**، **File Server** و **Remote Desktop Services**، جزء اهداف اصلی مهاجمان سایبری هستند. این ماژول با هدف ایجاد یک لایه امنیتی مستحکم در سطح سیستم‌عامل، دسترسی‌ها و سرویس‌ها طراحی شده تا **از نفوذ، گسترش تهدیدات و دسترسی غیرمجاز جلوگیری کند**.

🛠خدمات قابل ارائه

۱. Harden کردن سیستم‌عامل بر اساس استانداردهای حوزه امنیت
۲. اصلاح دسترسی‌ها و نقش‌های کاربران
۳. راه‌اندازی تحلیل لاگ و مانیتورینگ رویدادها و سیستم هشداردهی
٤. غیرفعال‌سازی سرویس‌های ناایمن یا غیرضروری
٥. راه‌اندازی Event Log Forwarding
٦. نصب آنتی‌ویروس سازمانی (در صورت درخواست مشتری)

💡ارزش افزوده ماژول برای سازمان

- **افزایش امنیت حیاتی‌ترین اجزای شبکه سازمان** که به‌صورت پیش‌فرض بیشترین دسترسی را دارند
- **کاهش شدید احتمال Privilege Escalation** از طریق کاربران یا بدافزارهای داخلی
- **مانیتورینگ متمرکز لاگ‌ها و رفتارهای مشکوک** برای واکنش سریع به تهدیدات
- **ایجاد شفافیت و مستندسازی امنیتی** قابل ارائه به تیم مدیریت یا حسابرسی امنیتی

این ماژول، به‌خصوص برای سازمان‌هایی که زیرساخت آن‌ها بر پایه دامنه و خدمات مایکروسافتی است، **یک اقدام بنیادی برای کنترل سطح حمله و جلوگیری از نفوذ زنجیره‌ای** محسوب می‌شود.

ماژول ۴: امن‌سازی ایستگاه‌های کاری

🎯هدف

ایستگاه‌های کاری (Workstations) در سازمان، نقاط ابتدایی تعامل کاربران با شبکه هستند و از اصلی‌ترین مسیرهای ورود بدافزار، حملات مهندسی اجتماعی و تهدیدات داخلی محسوب می‌شوند. هدف این ماژول، **افزایش مقاومت کاربران و سیستم‌های آنان در برابر تهدیدات امنیتی** و قطع زنجیره نفوذ از این نقاط به سایر اجزای شبکه است.

🛠خدمات قابل ارائه

۱. امن‌سازی سیستم‌عامل(OS Hardening)
۲. نصب و راه‌اندازی آنتی‌ویروس تحت شبکه
۳. پیاده سازی Web Control وApplication Control
٤. رمزنگاری و محافظت از داده‌ها
٥. امن‌سازی مرورگرها و فعالیت‌های وب
٦. نظارت و گزارش‌گیری امنیتی

💡ارزش افزوده این ماژول برای سازمان

- **افزایش تاب‌آوری کاربران نهایی** در برابر حملات فیشینگ، باج‌افزار و نفوذ از طریق ایمیل یا اینترنت
- **کاهش احتمال گسترش تهدیدات در شبکه** از طریق کنترل نقاط ابتدایی ورود
- **کاهش بار کاری تیم IT و امنیت** از طریق مانیتورینگ متمرکز و مدیریت یکپارچه
- **افزایش امنیت داده‌های حساس ذخیره‌شده در سیستم کاربران**

این ماژول برای سازمان‌هایی که از تعداد زیادی ایستگاه کاری استفاده می‌کنند، به‌ویژه در واحدهای مالی، منابع انسانی، فروش و مدیریت، **کاملاً حیاتی و مقرون‌به‌صرفه** است. پیاده‌سازی اصولی آن نقش کلیدی در جلوگیری از نشت داده و انتشار بدافزار در شبکه دارد.

ماژول ۵: امن‌سازی سیستم‌های مجازی‌سازی

🎯هدف

در اغلب سازمان‌ها، **بسترهای مجازی‌سازی** قلب زیرساخت فناوری اطلاعات را تشکیل می‌دهند. هرگونه آسیب‌پذیری در این لایه، می‌تواند کل سرورها و سرویس‌های حیاتی را به خطر بیندازد. هدف این ماژول، **ایمن‌سازیHypervisor ها، شبکه‌های مجازی، ماشین‌های مجازی و دسترسی‌های مدیریتی** به این بستر است تا از نفوذ، سوءاستفاده، یا اختلال در عملکرد آن‌ها جلوگیری شود.

🛠خدمات قابل ارائه

۱. ایمن‌سازی Hypervisor و تنظیمات مدیریتی
۲. امن‌سازی شبکه مجازی و ارتباطات داخلی
۳. بررسی وضعیت ماشین‌های مجازی
٤. کنترل مهاجرت و دستکاریVM ها

💡ارزش افزوده برای سازمان

- **افزایش امنیت هسته زیرساخت IT سازمان** در برابر تهدیدات داخلی و خارجی
- **کاهش خطر اجرای ماشین‌های مشکوک یا غیرمجاز** در محیط سازمان
- **ایجاد محیطی امن برای رشد سرویس‌های مجازی** با حفظ عملکرد و پایداری بالا
- **کاهش احتمال حملات lateral movement** از طریق تفکیک ترافیک و محدودسازی دسترسی‌ها

این ماژول به‌ویژه برای سازمان‌هایی که به سمت **Cloud Private** یا **Hybrid Infrastructure** حرکت می‌کنند، بسیار حیاتی است. اجرای صحیح آن، امنیت کلی سازمان را به سطح بالاتری می‌برد.

ماژول ۶: امن‌سازی تجهیزات شبکه

🎯هدف

تجهیزات لایه دوم و سوم شبکه مانند سوییچ‌ها و روترها، ستون فقرات ارتباطی هر شبکه‌ای محسوب می‌شوند. عدم امن‌سازی صحیح این تجهیزات، می‌تواند منجر **به شنود ترافیک داخلی (Packet Sniffing)، حملات درون‌سازمانی(Insider Threats) ، افشای دسترسی مدیریتی، یا نفوذ به‌VLAN های دیگر** شود. هدف این ماژول، ایجاد ساختاری مستحکم و مقاوم در برابر چنین تهدیداتی است.

🛠خدمات قابل ارائه

۱. امن‌سازی دسترسی مدیریتی
۲. ایمن‌سازی لایه ۲
۳. ایمن‌سازی لایه ۳ و کنترل ترافیک
٤. مانیتورینگ و لاگ‌برداری

💡ارزش افزوده

- **افزایش امنیت مدیریتی تجهیزات شبکه** با احراز هویت قوی، رمزنگاری و محدودسازی دسترسی
- **جلوگیری از شنود ترافیک داخلی** و سوءاستفاده کاربران دارای دسترسی فیزیکی
- **محافظت از معماری شبکه در برابر تهدیدات داخلی و پیکربندی نادرست**
- **افزایش پایداری و سلامت شبکه** با استفاده از کنترل‌های لایه ۲ و ۳

در شبکه‌هایی که ده‌ها یا صدها تجهیز فعال دارند، اجرای این ماژول با سیاست‌های استاندارد می‌تواند هزینه‌های بلندمدت نگهداری و رخدادهای امنیتی را به‌طور چشمگیری کاهش دهد. این ماژول، هم به‌صورت مستقل و هم به‌عنوان بخشی از یک پروژه جامع امن‌سازی شبکه قابل اجرا است.

ماژول ۷: امن‌سازی سرویس‌های سازمانی

🎯هدف

سرویس‌های حیاتی سازمان مانند ایمیل، DNS، FTP، RDP و SSH به‌عنوان دروازه‌های ارتباطی اصلی در زیرساخت فناوری اطلاعات شناخته می‌شوند. **هرگونه ضعف امنیتی در این سرویس‌ها می‌تواند منجر به نفوذ، سرقت اطلاعات، حملات باج‌افزاری یا از کارافتادگی خدمات شود** .این ماژول با هدف محافظت همه‌جانبه از این سرویس‌ها در برابر تهدیدات رایج و سوءاستفاده‌های هدفمند طراحی شده است.

🛠خدمات قابل ارائه

۱. امن سازی سرویس‌های ایمیل
۲. امن سازی سرویسDNS
۳. امن سازی فایل سرورها
٤. بررسی و پیاده‌سازی محدودیت‌های دسترسی
٥. فعال‌سازی پروتکل‌های رمزنگاری
٦. پیاده سازی سیاست‌های نشست و استفاده ایمن

💡ارزش افزوده

- **محافظت** از زیرساخت‌های حیاتی ارتباطی در برابر تهدیدهای رایج
- **جلوگیری** از انتشار بدافزار، فیشینگ یا اسپم از طریق سرویس‌های ایمیل
- **کاهش** بار شبکه با حذف ترافیک مشکوک و غیرضروری
- **افزایش** انطباق با استانداردهای امنیتی در حوزه انتقال داده و ایمیل
- **پیش‌نیاز** مهم برای پیاده‌سازی ISMS یا ممیزی‌های امنیتی خارجی

این ماژول برای سازمان‌هایی که از سرویس‌های ایمیل داخلی، FTPسرور، IDNSاختصاصی یا دسترسی از راه دور استفاده می‌کنند **یک اقدام ضروری** محسوب می‌شود.

ماژول ۸: جداسازی اینترنت سازمان از اینترانت

🎯هدف

جداسازی اینترنت از شبکه داخلی سازمان، یکی از اقدامات کلیدی در راستای **تقویت امنیت زیرساخت‌های فناوری اطلاعات** است. هدف اصلی این اقدام عبارت است از:

- **کاهش سطح حملات سایبری** با جلوگیری از دسترسی مستقیم کاربران یا سامانه‌های داخلی به اینترنت عمومی.
- **محافظت از داده‌های حساس و حیاتی سازمان** در برابر نفوذ بدافزارها، باج‌افزارها و تهدیدات پیشرفته.(APT)
- **مدیریت و کنترل ترافیک داده‌ها** و جلوگیری از نشت اطلاعات.(Data Leakage)
- **افزایش انطباق با الزامات قانونی، استانداردها و چارچوب‌های امنیتی** نظیرISO 27001 ، GDPR و قوانین بومی امنیت اطلاعات.

🛠خدمات قابل ارائه

۱. طراحی و پیاده‌سازی معماری جداسازی
۲. راه‌اندازی و پیکربندی تجهیزات امنیتی
۳. مجازی‌سازی وDesktop Isolation
٤. نظارت، پایش و مدیریت مداوم
٥. تدوین سیاست‌های امنیتی مرتبط با استفاده از اینترنت.

💡ارزش افزوده

کاهش چشمگیر ریسک‌های امنیتی ناشی از حملات اینترنتی.
افزایش سطح کنترل و نظارت بر دسترسی کاربران به اینترنت.
محافظت از داده‌های محرمانه و حیاتی سازمان در برابر تهدیدات بیرونی.
ارتقای انطباق با استانداردها و الزامات قانونی داخلی و بین‌المللی.
بهبود بهره‌وری شبکه داخلی با کاهش بار غیرضروری اینترنت بر شبکه سازمانی.
امکان پاسخ سریع و مؤثر به رخدادهای امنیتی به دلیل ساختار جداسازی‌شده.
کاهش هزینه‌های ناشی از رخدادهای امنیتی و حملات سایبری.

ماژول ۹: پایش، ارزیابی مشاوره و نظارت بر قراردادهای امنیتی

🎯هدف

این ماژول با هدف **ارزیابی مستمر و دقیق عملکرد امنیتی پیمانکاران فناوری اطلاعات یا واحدهای داخلی سازمان** طراحی شده است. بسیاری از سازمان‌ها پروژه‌های مرتبط با امنیت را به پیمانکاران برون‌سپاری می‌کنند یا آن را به واحدهای داخلی خود می‌سپارند؛ اما بدون نظارت حرفه‌ای، امکان بروز ضعف‌های امنیتی، تأخیر در اجرای تعهدات، یا حتی گزارش‌دهی نادرست وجود دارد. بنابراین، این ماژول به شما کمک می‌کند تا با یک نگاه حرفه‌ای و فنی، از تطابق عملکرد پیمانکاران یا تیم‌های داخلی با **استانداردها، SLAها و اهداف امنیتی سازمان** اطمینان حاصل کنید.

🛠خدمات قابل ارائه

در قالب این ماژول، مجموعه‌ای از خدمات تخصصی و قابل سفارشی‌سازی بسته به نوع قرارداد و پروژه امنیتی ارائه خواهد شد:

🔍بررسی مفاد قرارداد وSLA های امنیتی

- مطالعه دقیق قراردادها و اسناد توافق‌شده با پیمانکاران
- تحلیل سطح توافق‌نامه‌های خدماتی(Service Level Agreement – SLA)
- ارزیابی پایبندی پیمانکار به تعهدات زمانی، کیفی و امنیتی
- بررسی فرآیندهایIncident Response ، Backup، Patch Managementو...

🛡انجام اسکن‌های دوره‌ای آسیب‌پذیری(Vulnerability Assessment)

- استفاده از ابزارهای شناخته‌شده بین‌المللی مانند **Qualys**، **Nessus**، **OpenVAS**
- برنامه‌ریزی اسکن‌های زمان‌بندی‌شده (ماهانه، فصلی یا موردی)
- تحلیل آسیب‌پذیری‌ها و مقایسه آن‌ها با تعهدات پیمانکار در رفع آن‌ها
- ارائه گزارش اصلاحات انجام‌شده و نقاط ضعف باقی‌مانده

📊تحلیلLog ها، Alertها و رویدادهای امنیتی

- بررسی رویدادهای ثبت‌شده توسطSIEM ، فایروال، آنتی‌ویروس سازمانی و سایر تجهیزات

- ارزیابی نحوه واکنش پیمانکار به رویدادها(Detection & Response)
- تشخیص تهدیدهای پنهان یا نادیده‌گرفته‌شده
- استخراج الگوهای تکرارپذیر از لاگ‌ها و هشدارها برای شناسایی نقاط ضعف پایدار

🧩بررسی کارایی سیاست‌های امنیتی و مستندسازی فنی

- ارزیابی اینکه آیا سیاست‌های امنیتی تدوین‌شده به‌درستی اجرا می‌شوند یا صرفاً روی کاغذ باقی مانده‌اند
- بررسی کامل مستندات فنی تحویلی از طرف پیمانکار (نقشه شبکه، لیست تجهیزات، تنظیمات امنیتی و ...)
- تحلیل شکاف بین سیاست‌های مدون و عملیات اجرایی روزمره

📝ارائه گزارش مدیریتی و فنی

- **گزارش مدیریتی** شامل وضعیت کلی امنیت، میزان انطباق با تعهدات، نکات بحرانی برای تصمیم‌گیری مدیران
- **گزارش فنی** شامل یافته‌های دقیق، تحلیل‌های عددی، لاگ‌ها، آسیب‌پذیری‌ها و پیشنهادات اصلاحی

💡ارزش افزوده

- **ایجاد نظارت هوشمندانه و مبتنی بر داده** بر عملکرد پیمانکاران یا تیم‌های امنیتی داخلی
- **جلوگیری** از خطرات ناشی از سهل‌انگاری امنیتی یا ضعف فنی
- **شناسایی زودهنگام انحراف‌ها** در اجرای پروژه‌های امنیتی
- **مستندسازی** قابل استناد برای مذاکره، تمدید یا فسخ قراردادها
- **ایجاد اطمینان برای مدیران ارشد** در مورد امنیت سازمان و نحوه عملکرد پیمانکاران

این ماژول به‌ویژه برای سازمان‌هایی توصیه می‌شود که امنیت را به پیمانکار برون‌سپاری کرده‌اند یا در حال ارزیابی اثربخشی داخلی تیم‌های IT هستند. ما با تجربه‌ی میدانی و ابزارهای تخصصی، ضمانت می‌کنیم که ضعف‌ها از دید پنهان نمانند.

جمع‌بندی

در دنیای امروز که تهدیدات سایبری به‌سرعت در حال گسترش هستند، سازمان‌ها ناگزیرند رویکردی جامع، ساختاریافته و تدریجی برای حفاظت از زیرساخت‌های حیاتی خود اتخاذ کنند. پروپوزال حاضر، با **طراحی مدل ماژولار و منعطف**، مجموعه‌ای از ۱۰ ماژول تخصصی را ارائه می‌دهد که هر یک به بخشی از زیرساخت و سرویس‌های فناوری اطلاعات می‌پردازد. این مدل با بهره‌گیری از استانداردهای جهانی، تجربیات عملیاتی و ابزارهای پیشرفته، به سازمان‌ها امکان می‌دهد:

زیرساخت‌های حیاتی خود را به‌صورت مرحله‌ای و براساس اولویت‌ها امن‌سازی کنند.
از **خدمات** قابل سفارشی‌سازی متناسب با نیازها و الزامات قانونی بهره‌مند شوند.
بلوغ امنیت سایبری خود را مستند، قابل پایش و مطابق با استانداردهای بین‌المللی ارتقا دهند.

ماژول‌های ارائه‌شده شامل:

- امن‌سازی فایروال‌ها، پایگاه‌های داده، ویندوز سرورها، ایستگاه‌های کاری، تجهیزات شبکه و سیستم‌های مجازی‌سازی
- محافظت از وب‌سرورها و سرویس‌های حیاتی
- جداسازی اینترنت از اینترانت
- پایش قراردادهای جاری

این رویکرد علاوه بر **کاهش سطح حملات و تهدیدات، شفافیت، انطباق‌پذیری و پاسخ‌گویی سریع به رخدادهای امنیتی** را برای سازمان‌ها به ارمغان می‌آورد و به‌عنوان یک نقشه راه عملیاتی برای ایجاد محیطی امن و پایدار عمل می‌کند.

برای کسب اطلاعات بیشتر، با واحد امن سازی شرکت آیکو در ارتباط باشید.