شرکت انفورماتیـــک ماهان

متخصصـان ما در شـرکت مدیریـت انفورمـاتیـک ماهـان با تـکیه بر تخصـص خـود در حوزه فنـاوری اطلـاعات و ارتبـاطـات با توجـه بـه ضـرورت و نیـاز روبه رشـد حـوزه فنـاوری در استفـاده از تـجهیـزات مطمئـن و توانـمند بومـی بـر آن شد با هـمـت و تـوان خـود دست بـه تـولیـد تجـهیـزات تـخصـصی زیرسـاخـت بـرده و در ایـن راه مـوفـق شـده بخشـی از محصولات خـود را با همـکاری شرکـت های معتبر بین المللی با نام تجاری مانتی در بازار ارائه کند.

راهکار های شبکه و امنیت مانتی
MANTINETWORKS

MantiMan MantiAsset MantiStorage MantiLog
MantiUtm MantiRus MantiVpn MantiWall

MANTIWALL

در اصطلاح فایروال سیستمی است که شبکه و یا کامپیوتر شخصی شما را در مقابل نفوذ مهاجمین، دسترسی های غیرمجاز، ترافیک های مخرب و حملات هکرها محافظت کند. نحوه عملکرد فایروال ها به اینگونه است که بسته ها را بین شبکه ها رد و بدل و مسیریابی (Route) می کند، همچنین ترافیک ورودی به شبکه و نیز ترافیک خروجی از آن را کنترل و مدیریت کرده و با توجه به قوانینی که در آنها تعریف می شود به شخص یا کاربر خاصی اجازه ورود و دسترسی به یک سیستم خاص را می دهند.

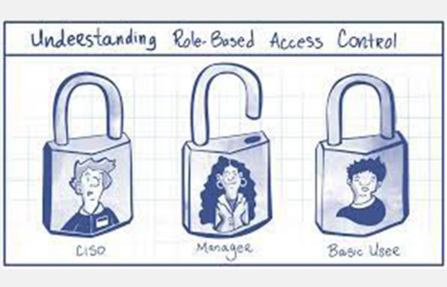
- شبکه مخصوص مجازی به همراه پشتیبانی یکپارچه از IPsec و سرویس های Open VPN، Tinc، wireGuard .....
- جلوگیری از ورود هرزنامه و ویروس در درگاه ورودی شبکه
- فایروال با پشتیبانی از IPv۴ و IPv۶ به همراه نمایش ترافیک زنده مسدود شده و یا عبور داده شده
- تامین امنیت شبکه
- تشخیص نفوذ و پیشگیری از تهدیدات IDS.IPS همگام سازی با suricata،Proofpoint's
- Web Filtering پروکسی وب کاملا یکپارچه با کنترل دسترسی و پشتیبانی از لیست سیاه برای فیلتر کردن ترافیک ناخواسته
- قابلیت اتصال و همراه سازی چند WAN به همراه Packet Loss،Load Balancing،High Latency
- احراز هویت دو عاملی 2FAبرای رابط کاربری و سرویس هایی مانند VPN

Antivirus

اینترنت یکی از ناامن‌ترین فضاهای موجود است. حضور در اینترنت نیاز به اطلاعاتی دارد که از شما در برابر خطرات موجود محافظت کند یا یک راه مناسب تر این است که یک آنتی ویروس در سطح شبکه سازمان فعال شود و این آنتی ویروس ترافیک ورودی و خروجی را مدیریت کند و جلوی خطرات را بگیرد.
مانتی وال قدرت ارائه چنین آنتی ویروسی را دارد. در این آنتی ویروس از سرویس های پروکسی C-ICAP ، HTTPS، HTTP و ClamAV استفاده شده است تا دقیق ترین خروجی ممکن را آن آنتی ویروس داشته باشد.

User Access Control

بسته به سازمان، افراد مختلفی می‌توانند با فایروال مانتی وال دسترسی داشته باشند. داشتن سطح دسترسی کامل همه اعضا به فایروال کار اشتباهی است و می‌تواند مشکلات زیادی درست کند. فایروال مانتی وال این توانایی را دارد که به هرکاربر دسترسی مورد نیازش را بدهد و بقیه دسترسی ها را ببندد و از ایجاد مشکلات متعدد با این اقدام جلوگیری کند .



Captive Portal

اینترنت یکی از مهم ترین سرویس‌های هر سازمان است که نیاز به مدیریت دارد. برای مدیریت اینترنت سازمان می‌توانیم از سرویس کپتیو پورتال استفاده کنیم. کپتیو پورتال سرویسی است که قبل از این که کاربران سازمان به اینترنت متصل شوند، کاربران شناسایی می‌کند و سپس اجازه دسترسی اینترنت را می‌دهد.
بعد از صدور مجوز دسترسی به اینترنت هم نظارت بر کاربران را ادامه می‌دهد. به عنوان مثال می‌تواند سرعت دانلود و آپلود از اینترنت را برای هر گروه از کاربران مدیریت کند یا این که اجازه دسترسی به بعضی از صفحات داخل اینترنت را بدهد یا ندهد. ویژگی‌های زیر باعث می‌شود که کپتیو پورتال را برای مدیریت اینترنت سازمان خود انتخاب کنیم.

- مدیریت دسترسی به صفحات اینترنت
- مدیریت پهنای باند شبکه
- مدیریت ارتباط با اینترنت
- مارکتینگ و ایجاد آشنایی با برند

ارزیابی سطح بلوغ امنیتی و ترسیم نقشه راه

مهمترین قدم در فائق آمدن بر هر مشکلی، ارزیابی و شناخت دقیق مشکل است. دلیل اصلی شکست سازمان ها در اجرای پروژه ها ی امنیتی و عدم حصول به نتایج مناسب، به رغم صرف هزینه ها گزاف، عدم شناخت آن ها از وضعیت موجود نیازهای امنیتی خود و همچنین عدم وجود نقشه راه برای ایجاد امنیت در سازمان است. شرکت انفوماتیک ماهان به منظور ترسیم نقشه پیاده سازی امنیت در سازمان ها، خدمات زیر را ارائه می دهد:

- ارزیابی سطوح بلوغ امنیتی بر اساس بهروش CyberResilienceReview
- ارزیابی سطح انطباق امنیت سایبری با چارچوب NISTCSF
- ارزیابی سطح پیاده سازی کنترل های امنیتی بر اساس CIS20
- ارائه گزارش GapAnalysis بر اساس Scale سازمان
- ترسیم نقشه راه امنیت بر اساس مولفه های زمان، سطح بلوغ و بودجه
- انجام ارزیابی های دوره ای به منظور پایش بهبودهای صورت گرفته.

آگاهی رسانی امنیتی

مفاهیم اطلاع رسانی، آگاه سازی و آموزش درزمینه ی امنیت، در سطوح مختلف فرهنگ سازی و اکتساب دانش کاربر دارد. توجه به نقاط اشتراک فراوان این مفاهیم و تنوع سطوح آگاهی مخاطبان و همچنین رسانه های مختلف آموزشی، لزوم ارائه مدل آموزش دقیق و در عین حال منعطف را ضروری می سازد. این فرآیند سبب فرهنگ سازی امنیتی و کمک به کاهش ریسک های امنیتی در سازمان میگردد.
برای ارائه آگاهی امنیتی از روش های مختلف استفاده می شود که در زیر به آنها اشاره می شود:

- مجله، کتاب یا سایت اطلاع رسانی
- ویدئوهای آموزشی شامل فیلم کوتاه، انیمیشن، سخنرانی و...
- موشن گرافیک
- فلش کارت های آموزشی
- تالیف و ترجمه مقاله
- کمپین های ایمیلی و پیامکی
- کارگاه های آموزشی، کنفرانس و سمینار
- اجرای مانورهای امنیتی مانند شبیه سازی حملات فیشینگ، مهندسی اجتماعی و...
- Gamification

امن سازی شبکه ها و سرویس ها

باتوجه به اینکه امروزه تهدیدهای متعددی متوجه دارایی ها و سرمایه های سازمانی هستند برای هدفمند و قانونمند شدن فرآیند امن سازی، کارشناسان شرکت انفورماتیک ماهان با تکیه بر کنترل های امنیتی، مستندات امن سازی ارائه شده توصیه ها و مستندات افتای ریاست جمهوری اقدام به امن سازی در هر بخش از تجهیزات شبکه و زیرساخت به عنوان مرجعی کامل که مورد تایید اغلب کارشناسان این حوزه می باشد، می نمایند.

تست نفوذ

تست نفوذ شبکه یک سرویس امنیتی است که آسیب پذیری های امنیتی در شبکه‌ها، سیستم ها، میزبان ها و دستگاه ها را با استفاده از تکنیک های مخرب برای آزمایش پاسخ های امنیتی شبکه شناسایی می‌کند. هدف از آزمایش نفوذ شبکه، شناسایی اکسپلویت (Exploits) های امنیتی است که کسب و کار شما را در معرض خطر نقض داده ها و اطلاعات قرار می‌دهند، قبل از اینکه هکرها بتوانند آن ها را کشف و از آن ها بهره برداری کنند. به زبان ساده، تست نفوذ شبکه مانند خدماتی است که کسب و کارها برای کشف ضعیف ترین نقاط خود هزینه پرداخت می‌کنند.

طبقه بندی اطلاعات

در زمینه امنیت اطلاعات، طبقه بندی داده ها و اطلاعات بر اساس میزان اهمیت و آسیب رسانی آن ها به سازمان در صورت افشا شدن و یا از بین رفتن آن ها انجام می شود.
به منظور حفاظت از اطلاعات و داده های سازمان که به مشابه جواهرات بر روی تاج سازمان است. متوجه ساختن کارمندان از اهمیت موضوع ذخیره سازی اطلاعات سازمان در هر نوع دیجیتال و مکتوب باید جهت آگاه سازی در سیاست های سازمان گنجانده شود.
دسته بندی اطلاعات، انواع مختلفی دارد که هر سازمان با توجه به نیازهای خود یک نوع از آن را اتخاذ می کند. برخی از انواع طبقه بندی های معمول دسته بندی اطلاعات عبارتند از: سری، محرمانه، محدود، عمومی و...
برخی معیارها برای جلوگیری از افشای اطلاعات:

- توافق محرمانه
- طبقه بندی داده ها
- استفاده از کانال های انتقال اطلاعات و ابزارهای ذخیره سازی رسمی
- رمزگذاری داده ها
- از رده خارج کردن مناسب ابزار استفاده شده

پایش امنیتی کسب و کار

مهمترین رسالت مراکز عملیات امنیت، کشف حوادث امنیتی و کاهش ریسک های مربوط به استمرار کسب و کار سازمان است. متاسفانه رویکرد غالب در راه اندازی مراکز عملیات امنیت محدود کردن آن به حوزه عملیاتی است و این در حالی است که اکثر مدیران ارشد سازمان ها، علاقه ای به جزئیات کارکرد این لایه ندارند. پایش کارکرد مولفه های موثر در کسب و کار سازمان ها از مهمترین نوآوری های شرکت انفورماتیک ماهان در ایجاد مراکز عملیات امنیت بوده است. این امر سبب ایجاد ارزش افزوده در مراکز عملیات امنیت و نیز ایجاد داشبوردهای مدیریتی می گردد.
هم اکنون پایش کسب و کارهای حوزه پولیو بانکی و نیز اپراتور موبایل، پیاده سازی گردیده است. از قابلیت های مهم Business SOC در حوزه های فوق می توان به موارد زیر اشاره کرد:

- کشف ارتباط بین مشکلات کسب و کار سازمان و حوزه عملیات
- ارائه یک دید جامع به مدیران ارشد از مشکلات زیرساختی که کسب و کار سازمان را تهدید می کند.
- موشن گرافیک
- فلش کارت های آموزشی
- تالیف و ترجمه مقاله
- کمپین های ایمیلی و پیامکی
- کارگاه های آموزشی، کنفرانس و سمینار

برخی از مشتریان ما

جای شما در جمع مشتریان ما خالیست ...

info@mahan-it.com
+9851 - 910 - 12270
www.mahan-it.com