

رمیس

نشریه داخلی شرکت رمیس
بهار ۱۳۸۹، شماره ۴

گفت و گو با مهندس احسان پورمند

رمیس یکی از سه شرکت خصوصی برتر IT

آشنایی با مرکز عملیات امنیت SOC

حضور تیم رمیس در مسابقات فوتسال جام انفورماتیک

- مجری پروژه‌های ملی فناوری اطلاعات و ارتباطات
- تحویل در کوتاه‌ترین زمان ممکن
- کامل‌ترین تیم پشتیبانی فنی (CCIE, CCNP, CCNA)
- گارانتی تعویض
- ارائه خدمات پس از فروش در مراکز استان‌ها
- ارائه تجهیزات اصلی سیسکو به صورت هولوگرام دار



REMISCO
مراجعه به مرکز خرید

CISCO

Create
your own
CISCO

**CISCO Integrated Service
Routers & Switches**

Consulting, Designing & Implementing
Network Infrastructure (LAN, MAN, WAN)
خیابان ولی‌عصر، خیابان استاد مطهری
خیابان سرسبزداران، شماره ۲۸
تلفن: ۸۸۹۲۵۸۰۸، فکس: ۸۸۹۳۶۰۶۸
www.remisco.com

فهرست

- ۴ رمیس یکی از سه شرکت خصوصی برتر IT است
- ۶ پشتیبانی ۴ هزار نقطه در سراسر کشور
- کیفیت و قیمت رمیس، با دیگر شرکت‌ها قابل مقایسه نیست
- ۸ رمیس جام اخلاق را به دست آورد
- ۹ افزایش وفاداری کارکنان
- ۹ کشاورز دانا
- ۹ رمیس حامی مجموعه خیریه دارالاکرام
- ۱۰ گزارش تصویری
- ۱۲ آشنایی با مرکز عملیات امنیت SOC
- ۱۴ معرفی نرم‌افزار HP NNM
- ۱۷ پیام‌های مدیریتی بزرگان
- ۱۷ گزیده‌ای از کتاب مدیریت بر قلب‌ها
- ۱۸ آشنایی با CS-MARS
- ۲۱ بهداشت حرفه‌ای در کار با رایانه

R E M I S

- ◀ صاحب امتیاز: شرکت رمیس
- ◀ مدیر مسئول: امیرعباس تقی‌پور
- ◀ سردبیر: امیر لعلی
- ◀ تحریریه: ساره جعفرقلی، الهام تقی‌پور، اویس طوفانی
- ◀ عکس: علی جوزابچی
- ◀ نشانی: تهران، خیابان مطهری، خیابان سرداران، پلاک ۲۸
- ◀ تلفن: ۸۸۹۲۵۸۰۸
- ◀ دورنگار: ۸۸۹۳۶۰۶۸
- ◀ نشریه داخلی شرکت افزار پرداز رمیس



◀ از خوانندگان و علاقمندان دعوت می‌شود در صورت تمایل، مطالب خود را برای چاپ در نشریه به پست الکترونیک info@remisco.com ارسال نمایند.

سرمقاله

تأثیر تکنولوژی اطلاعات بر استراتژی‌های سازمان‌ها

در سال ۱۹۸۶ به دنبال مطالعه‌ای که توسط کارگزاران و مدیران اجرایی سیستم‌های اطلاعات (INFORMATION SYSTEMS) صورت پذیرفت، اهمیت و نقش حیاتی مدیریت سیستم‌های اطلاعات مورد تأکید قرار گرفت و ارتقا و بهبود برنامه‌ریزی استراتژیک در درجه اول اهمیت قرار داده شد. یک برنامه‌ریزی مؤثر نیازمند نظم و توان پیش‌بینی مشکلات (تهدیدها) و فرصت‌ها در یک محیط متلاطم و پیچیده و نیز قابلیت توسعه استراتژی‌ها و سیاست‌هایی براساس تکنولوژی‌های اطلاعات است که به سرعت در حال تغییرند. استفاده از سیستم‌های اطلاعات به عنوان یک مزیت رقابتی در درجه دوم اهمیت قرار دارد. امروزه سیستم‌های اطلاعات یک ابزار و سلاح استراتژیک اصلی در بسیاری از شرکت‌ها تلقی می‌شود. این مزیت رقابتی نتیجه تشخیص فرصت‌ها و به دنبال آن اجرای مؤثر و سریع تکنولوژی‌های اطلاعات برای استفاده از آنهاست. در بسیاری از شرکت‌ها، سه سطح برای تعریف استراتژی وجود دارد: در بالاترین سطح، استراتژی خطوطی را که شرکت در آن تجارت می‌کند و نحوه تخصیص منابع کلیدی شرکت به هر یک از این خطوط را مشخص می‌کند. در یک اقتصاد متلاطم، هویت شرکت و تخصیص منابع، ممکن است طی زمان دستخوش تغییر شود. سطح دوم استراتژی در ارتباط با واحدهای تجاری استراتژیک (STRATEGIC BUSINESS UNIT-SBU) است که می‌تواند یک بخش فرعی یا خط تولید در شرکت باشد. هرگاه استراتژی شرکت متحول شود، منابع تخصیص یافته به واحدهای تجاری موجود یا جدید ممکن است تغییر کند. سطح سوم استراتژی، همان استراتژی عملیاتی است. وقتی استراتژی یک واحد تجاری تعریف می‌شود، هر یک از نواحی عملیاتی درون آن واحد باید اعمالی را برای پشتیبانی استراتژی مربوطه انجام دهند. از آنجا که ممکن است استراتژی‌های عملیاتی گوناگون (مانند استراتژی‌های فروش، استراتژی تحقیق و توسعه و استراتژی ساخت) برای واحدهای تجاری مختلف وجود داشته باشد، شاهد ظهور روزافزون یک استراتژی عملیاتی برای بهره‌برداری از منابع و تکنولوژی‌های اطلاعات به منظور پشتیبانی از واحدهای تجاری و دیگر استراتژی‌های عملیاتی هستیم. در سطح صنعت، تکنولوژی اطلاعات بر طبیعت محصولات، خدمات و بازارهای صنعت یا اقتصاد تولید و توزیع تأثیر می‌گذارد. در سطح مؤسسه، تأثیر تکنولوژی اطلاعات توسط نیروهای رقابتی خاصی تعیین می‌شود که مؤسسه با آنها روبه‌روست. این نیروها ساختار صنعت و میدان رقابت را برای هر مؤسسه شکل می‌دهند. این پنج نیرو عبارتند از تأمین کنندگان، خریداران، تازه‌واردان به حوزه صنعت، محصولات جایگزین و رقبای درون صنعت. تکنولوژی اطلاعات می‌تواند وابستگی‌های بین این نیروها و مؤسسه را تغییر دهد. این نیروها اهدافی هستند که مؤسسه در مقابل آنها استراتژی‌های رقابتی خود را ایجاد می‌کند. در سطح استراتژی، تکنولوژی اطلاعات می‌تواند بر توان مؤسسات برای اجرای یک استراتژی خاص تجاری تأثیر بگذارد. انواع مختلفی از استراتژی‌های کلی وجود دارند مانند هدایت بر مبنای هزینه، وجه تمایز، تمرکز، رشد، پیمان و نوآوری که هر یک می‌تواند تهاجمی یا تدافعی باشد.

■ امیرعباس تقی‌پور

گفت‌وگو با مهندس احسان پورمند رمیس یکی از سه شرکت خصوصی برتر IT است



مهندس احسان پورمند مدیر فناوری اطلاعات رمیس است. مدیری جوان و در عین حال باتجربه که دانش تئوریک سخت‌افزار و نرم‌افزار را با تجربه و علم مدیریت و اقتصاد در آمیخته است. وقتی قرار می‌شود در آغاز گفت‌وگو از خودش بگوید، قولی از یکی از شاعران معاصر نام‌اشنا را روایت می‌کند با این مضمون که چه تفاوتی می‌کند که کی و کجا به دنیا آمده باشیم و به همین سبب، محور گفت‌وگو با پورمند به فعالیت‌های واحد تحت مدیریتش در رمیس تبدیل می‌شود.



دوستانمان به نتیجه رسید. همین‌طور در پروژه مناقصه طراحی دیتاستر رشد برنده شدیم که کار بسیار ارزشمندی است. این که ما بتوانیم در حوزه دیتاستر وارد شده و به یک شرکت برتر در این زمینه تبدیل شویم جزو اهدافی بود که برای سال ۸۸ ترسیم شده بود و خوشبختانه به آن رسیدیم.

در کنار این موارد، سیستم مدیریت پروژه را نیز بهبود دادیم. یعنی از سال ۸۷، دفتر مدیریت پروژه را تأسیس کرده بودیم که در سال ۸۸ به بلوغ رسید و فرآیند آن استقرار پیدا کرد. نتیجه کار و گزارش‌ها به مدیریت ارایه شد و مدیریت براساس این گزارش‌ها، تصمیماتی اتخاذ کرد و به نظر می‌آید، این کار نیز کار خوبی بود. طبیعتاً اشکالاتی هم در سیستم وجود داشت که امیدواریم در سال ۸۹ برطرف شوند.

چشم‌انداز سال ۸۹ را با توجه به کارنامه سال ۸۸ چگونه می‌بینید؟

ما فکر می‌کنیم که در نیمه اول سال ۸۹، استراتژی اصلی شرکت را بر مبنای رشد کم و تثبیت در نظر بگیریم. به این معنا که فرصت بیشتری را صرف خواهیم کرد برای این که در زیرساخت‌های شرکت بازنگری و در صورت لزوم آنها را تقویت کنیم. به عبارت دیگر یک سری نقاط ضعف در شرکت داریم که فرصت بیشتری وجود دارد تا به آن نقاط ضعف بپردازیم. این نقاط ضعف عمدتاً در سیستم مالی و سیستم منابع انسانی شرکت است که توسط آقای غیاث‌الدین در حوزه مالی و آقای نوربخش در حوزه نیروی انسانی پیگیری می‌شود.

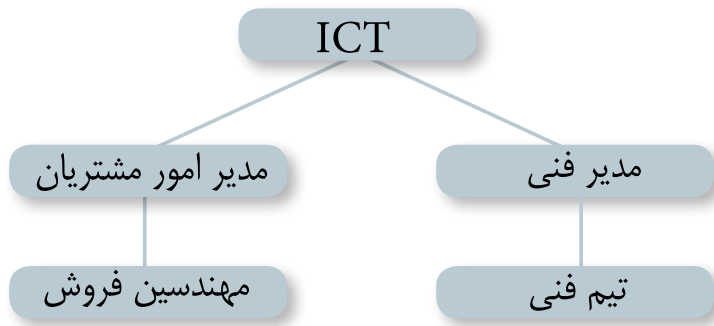
ضعف دیگری که احساس می‌شود، ساختارهای ارایه خدمات به مشتری بود. در ساختار قبلی یک مدیر فروش و یک مدیر فنی زیر نظر مدیر عامل قرار داشت که هر کدام دارای تیم مستقل بوده‌اند. بنابراین مشتری درخواست خود را به واحد فروش ارایه می‌کرد و آن درخواست توسط نیروهای فنی اجرایی می‌شد. با گذشت زمان و بلوغی که در فناوری اطلاعات کشور اتفاق افتاد، به این نتیجه رسیدیم که فروش را تخصصی کنیم. یعنی این که دیگر شاید کارشناسی که در زمینه فروش سخت‌افزار تخصص دارد، نتواند به آن مشتری نیازمند راه‌حل، پاسخ‌گو باشد.

بنابراین با هدف این که بتوانیم به مشتریان پیشرو در صنعت فناوری اطلاعات، ارایه خدمت کنیم و فقط فروشنده تجهیزات نباشیم، تغییراتی را در سیستم اعمال کردیم. به این ترتیب که یک واحد استراتژیک یا یک واحد تجاری راهبردی تشکیل شد که استراتژی آن ارایه راهکار به مشتری است. ما در این بخش بر فروش تجهیزات تمرکز نداریم. فروش تجهیزات کماکان در قسمت فروش سخت‌افزار و پروژه‌های فناوری اطلاعات مانند پروژه بیمه ایران در این واحد انجام می‌شود.

یک واحد تجاری راهبردی به این مفهوم است که اختیاراتی در این مجموعه وجود داشته و تا حدی خودگردان است، به این مفهوم که بودجه مستقلی برای آن در نظر گرفته شده و

با توجه به اینکه سال ۸۸ پشت سر گذاشته شده و فعالیت در سال ۸۹ آغاز شده است، بد نیست که ارزیابی از عملکرد رمیس در سالی که گذشت داشته باشید. رمیس سال ۸۸ را چگونه پشت سر گذاشت؟

سال ۸۸ برای ما سال خوبی بود. ما هر سال، یک سری برنامه‌ها و اهداف استراتژیک سالانه ترسیم می‌کنیم تا بتوانیم به آنها برسیم. به صورت مشخص اگر بخواهم آن اهداف را نام ببرم باید به آنهایی که وزن بیشتری داشتند اشاره کنم. افزایش فروش یکی از آنها بود که خوشبختانه محقق شد و توانستیم نسبت به سال ۸۷، درصد افزایش فروش را مطابق با پیش‌بینی‌هایمان محقق کنیم. البته اهداف ما عادی و قابل دسترس ترسیم شده و به نوعی بلندپرواز نیستیم. به همین دلیل هم دستیابی به اهداف، باعث خوشحالی ما و همکارانمان می‌شود. پروژه‌های بسیار خوبی در سال ۸۷ انجام دادیم. هدف دیگری که محقق شد، افزایش و توسعه توان حرکت ما در زمینه دیتاستر بود. ما در سال ۸۸، در دو مناقصه بزرگ برنده شدیم. اولین مناقصه، طراحی و پیاده‌سازی دیتاستر بیمه ایران بود که در یک ماراتن نفس‌گیر و با تولید حدود ۶۰۰، ۷۰۰ صفحه مستندات فنی توانستیم برنده شویم. بیش از ۲۰ نفر از پرسنل فنی ما در این پروژه مشارکت کردند و توانستند برای مشتری پیشنهاد فنی استخراج کنند. از این پیشنهاد دفاع کردیم و امسال در اوایل سال به ما اعلام کردند که در این پروژه برنده شده‌ایم. ما هم از این موضوع خوشحالیم چرا که تلاش



کشور در این حوزه فعالیت است. به این مفهوم که به لحاظ نمرات در بین شرکت‌ها نمرات یک تا سه را کسب کرده‌ایم. این ارزیابی سازمان‌های مختلف از ما بوده و طبیعتاً بر مبنای یک سری معیارهایی است که سازمان‌های دولتی در نظر گرفته‌اند. این جایگاه، جایگاه مناسبی است. ما نقطه ضعف‌هایی هم داریم که باید به آن بپردازیم. هدف ما قرار گرفتن به عنوان اولین شرکت خدمات فناوری اطلاعات است. چشم‌انداز خود من این است که بتوانیم در منطقه و حتی کشورهایی که برای حضور در بازار آنها مزیت رقابتی داریم مانند عراق، امارات، سوریه و... دامنه‌های خدماتمان را گسترش دهیم.

بر همین اساس برای این که در کلاس یک شرکت ارائه‌دهنده خدمات فناوری قرار بگیریم یا صادرکننده خدمات فناوری باشیم باید به استانداردهای بین‌المللی برسیم. در حال برنامه‌ریزی برای رسیدن به آن استانداردها هستیم تا بتوانیم با رقبای خارجی رقابت کنیم.

درباره نقاط ضعف و قوت رمیس گفتید که البته به داخل مجموعه بازمی‌گردد. لطفاً درباره فرصت‌ها و تهدیداتی بگویید که در فضای کسب و کار این حوزه در کشور برای رمیس وجود دارد؟

برخلاف خیلی از دوستان، ما فضای کشور را در حوزه فناوری اطلاعات فضای مثبتی ارزیابی می‌کنیم. یعنی احساس می‌کنیم بازار بکر است؛ به عبارت دیگر نیازهای ما در حوزه فناوری اطلاعات در کشور به حدی زیاد است که سازمان‌های بزرگ مثل مخابرات به عنوان دنیایی از کار و بانک‌ها که به شدت حوزه فناوری اطلاعات را گسترش می‌دهند، نیازمند ارائه خدمات به صورت جدی هستند.

به نظر می‌رسد اگر نقطه ضعفی باشد آن به ما و در واقع شرکت‌های ارائه‌دهنده خدمات در این حوزه بازمی‌گردد.

بعضاً گفته می‌شود که بودجه اختصاص نمی‌دهند و برنامه‌ریزی نیست. به نظرم این نکات به نوعی فزاینده است تا نقاط ضعف داخلی را پوشش دهیم. اگر بتوانیم نقاط قوت خودمان را تقویت و نقاط ضعف را بپوشانیم، به جرأت می‌گویم که کارهای بزرگی وجود دارد و برنامه‌ریزی‌های لازم در حوزه فناوری اطلاعات انجام شده است. ضعف ما شرکت‌های خصوصی است که نمی‌توانیم به سوی سیستم‌های دولتی حرکت کنیم و اطمینان بدهیم که کار آنها را انجام می‌دهیم. صحبت من ناظر به پروژه‌های ۱۰ یا ۲۰ میلیارد ریالی نیست و بحث من پروژه‌های کلان بالای ۱۰۰ میلیارد ریال را شامل می‌شود که به نظرم آمادگی انجام آن وجود دارد و ضعف متوجه خودمان است. باید خودمان را تقویت کنیم.

درآمد و هزینه جداگانه‌ای نیز دارد. این واحد را می‌توانیم به شکل یک شرکت مستقل فرض کنیم که مدیرعاملی دارد و نقش آقایان غیث‌الدین و نوربخش که مدیرعامل و قائم‌مقام رمیس هستند، نقش هیأت مدیره‌ای می‌شود که بر عملکرد این شرکت نظارت دارند.

به لحاظ قانونی آقای غیث‌الدین به‌عنوان مدیرعامل یا سایر دوستانی که امضای رسمی دارند، اسناد ما را امضا می‌کنند. بنابراین از نظر قانونی، تغییری در فعالیت‌ها به وجود نیامده و این تغییر ساختار منطقی است. نکته بعدی این است که ما در این ساختار بر مبنای توان پرسنل فنی برنامه‌ریزی می‌کنیم. به عبارت بهتر ایده ما این بود که همکاران فنی شرکت به بلوغی رسیده‌اند که می‌توانند مشتری را قانع کنند و به او راه‌کار ارائه دهند. در این فضا، همکاران فنی ما نقش ساختار فروش را نیز بازی می‌کنند. فکر می‌کنم مشتری‌ها هم تمایل بیشتری دارند تا به جای این که یک نیروی فنی فروش در کنار آنها باشد با کسی مواجه شوند که هم تکنیک‌های فروش بلد است و هم می‌تواند قیمت تمام شده را حساب کند.

این کارشناس، راه‌حل‌های مختلف را از نظر هزینه فایده بررسی می‌کند و با توجه به این که به لحاظ فنی هم مسلط است، راه‌کارهای مختلف و نقاط قوت و ضعف هر پیشنهاد را ارائه می‌دهد. ما با توجه به همکاران فنی خوبی که داریم، به موفقیت خودمان با این روش جدید امیدواریم. این روش البته مانند سایر امور یک‌ساله در نظر گرفته شده که بازبینی می‌شود و شاید اصلاحاتی در آن اعمال شود.

پس واحد فروش سخت‌افزار فقط تجهیزات می‌فروشد؟

بله. فروش سخت‌افزار به عهده واحد فروش سخت‌افزار و فروش راهکار به عهده ماست. آقای شفیع هم که تازه به تیم ما ملحق شده‌اند، بالغ بر ۲۵ سال سابقه در زمینه فناوری اطلاعات دارند و به عنوان مدیر امور مشتریان فعالیت می‌کنند. مدیر امور مشتریان در زیرمجموعه خودش، مهندسین فروش را دارد و با آن سیستمی که عرض کردم، در زیرمجموعه مدیر فنی این واحد هم، مدیران پروژه و همین‌طور همکاران فنی را داریم. امور مشتریان به معنی ارائه راهکار به مشتری است. به عبارت بهتر اگر مشتری دقیقاً نیازمندی سخت‌افزاری خود را بداند و پارت‌نامبر تجهیزات را کاملاً مشخص کرده باشد به واحد فروش سخت‌افزار هدایت می‌شود. اما اگر نیازمندی شخصی داشته باشد و برای آن به دنبال راه‌حل باشد واحد ICT به او سرویس مربوطه را ارائه می‌کند.

ما مشتریانی داریم که فقط از ما مطالبه سخت‌افزار نمی‌کنند و دنبال آن هستند که هر لحظه فرایندهای فن‌آوری و اطلاعات خودشان را بهینه کنند. برای پاسخ به نیاز آن دسته از مشتری‌ها این کار را انجام داده‌ایم.

جایگاه فعلی رمیس را در فضای فناوری اطلاعات کشور و در مقایسه با رقبا چگونه ارزیابی می‌کنید؟

همیشه باید عیاری برای سنجش وجود داشته باشد. یکی از اشکالاتی که در بازار فناوری اطلاعات داریم، این است که اطلاعات این بازار به صورت مدون و جامع وجود ندارد. لذا من نمی‌توانم به شما بگویم که رمیس چه سهمی از بازار دارد. ای کاش شرکت‌هایی باشند که این اطلاعات را گردآوری و طبقه‌بندی کنند.

اما اگر معیار را حضور و برنده شدن در مناقصات در نظر بگیریم، می‌توانم بگویم رمیس جزو سه شرکت برتر خصوصی



فضای کشور را در حوزه فناوری اطلاعات فضای مثبتی ارزیابی می‌کنیم. یعنی احساس می‌کنیم بازار بکر است؛ به عبارت دیگر نیازهای ما در حوزه فناوری اطلاعات در کشور به حدی زیاد است که سازمان‌های بزرگ مثل مخابرات به عنوان دنیایی از کار و بانک‌ها که به شدت حوزه فناوری اطلاعات را گسترش می‌دهند، نیازمند ارائه خدمات به صورت جدی هستند.

گفت‌وگو با سرپرست سایت تعمیر و نگهداری شبکه WAN بانک تجارت؛ پشتیبانی ۴ هزار نقطه در سراسر کشور



پیکربندی‌های موجود، مشکلات حل می‌شود. وی گفت: نرم‌افزار دیگری هم تهیه کردیم که تغییرات به‌وجود آمده در شبکه را گزارش می‌دهد. حدود ۵۰ درصد از این نرم‌افزارهایی که یاد شده تحت وب است. کمپلیان یادآور شد: با تلاش‌های انجام شده کارهای بانک ظرف مدت کوتاهی انجام می‌شود و رضایت خاطر کارفرما فراهم آمده است. برای مثال بانک از ما می‌خواهد که لیست روترهای ۱۶۰۰ در کل شبکه را به ما بدهید، ما با استفاده از نرم‌افزاری که طراحی کرده‌ایم این کار را به سرعت انجام می‌دهیم.

سرپرست سایت تعمیر و نگهداری شبکه WAN بانک تجارت افزود: آخرین نرم‌افزاری که طراحی شد، نرم‌افزار جامع IP addressing بانک تجارت بود. پیش از این، چنین فرآیندی به صورت دستی انجام می‌شد اما در حال حاضر نرم‌افزار IPها را چک و تعیین می‌کند که چنین IPای وجود دارد یا نه.

وی افزود: براساس اقدامات انجام شده اعتماد بسیار خوبی بین بانک و شرکت رهبر به وجود آمده و حتی تعدادی از کارشناسان بانک، از تجارب مشاوره‌ای ما برای بهبود شبکه استفاده می‌کنند. کمپلیان خاطر نشان کرد: ما دو شیفت کاری داریم. از ۷ صبح تا ۷ شب و بالعکس. البته معمولاً نیم ساعت ابتدایی و انتهایی شیفت‌ها با هم همپوشانی دارند. شیفت شب ما یک نفره است و در شیفت روز ۵ نفر حضور دارند. روزهای تعطیل و جمعه‌ها هم هستیم.

سرپرست سایت تعمیر و نگهداری شبکه WAN بانک تجارت ادامه داد: روترهایی که ما در این شبکه از آنها استفاده می‌کنیم سری ۷۶۰۰ است و بیشتر ارتباطات ما از بستر ارتباطی مخابرات برقرار می‌شود. البته در برخی نقاط صعب‌العبور از تجهیزات ماهواره‌ای VSAT استفاده می‌کنیم.

به این وسعت به روش مدیریتی که از پیش جریان داشت، امکان‌پذیر نیست. بنابراین قبل از شروع قرارداد در این محل حضور پیدا کرده و کارها را بررسی کردیم.

وی افزود: در جریان این بررسی‌ها متوجه شدیم سیستم قبلی در اجرای کار با مشکلاتی روبروست و بانک هم از کیفیت خدمات ناراضی است. بنابراین تصمیم گرفتیم که با طراحی و کمک گرفتن از برخی نرم‌افزارها، شرایط را بهبود بخشیم.

کمپلیان با اشاره به این مطلب که به دلیل نبود چنین نرم‌افزارهایی خطای انسانی بالا رفته و انجام امور جاری وقت‌گیر و خسته‌کننده شده بود ادامه داد: برای مثال تغییر رمز ورود ۲ هزار و ۵۰۰ روتر؛ حدود ۲۵ روز طول می‌کشید و ما برای حل این مشکل، نرم‌افزاری نوشتیم که مدت زمان لازم برای اجرای این فرآیند به ۳۵ تا ۴۰ دقیقه کاهش پیدا کرد.

سرپرست سایت تعمیر و نگهداری شبکه WAN بانک تجارت افزود: به دلیل نوع فعالیت بانک، مسایل امنیتی هم باید مورد توجه قرار می‌گرفت. با توجه به آنکه سیستم‌هایی که در بانک اجرایی شده بود سازمان‌یافته نبود و شرکت‌های گوناگونی عهده‌دار ارائه خدمات در ۸ سال گذشته بودند، لذا برخی مستندات مربوط به سالیان گذشته می‌شد.

کمپلیان ادامه داد: مشکل بعدی عدم دسترسی به سوابق پیکربندی روترها بود. برای مثال اگر در جایی قطعی صورت می‌گرفت، به دلیل نبود اطلاعات ضرورت داشت تا برای کارشناسی مراجعه شود. در حال حاضر ما به صورت روزانه از پیکربندی‌ها بانک اطلاعاتی می‌گیریم و وب‌سایتی داریم که در اختیار کارشناسان ما است. در صورت بروز مشکل، کارشناسان ما به این سایت مراجعه می‌کنند و براساس اطلاعات

حمیدرضا کمپلیان که سرپرست سایت تعمیر و نگهداری شبکه WAN بانک تجارت است، آبان ماه سال گذشته به رهبر پیوسته است.

این زمان، مصادف می‌شود با برنده شدن رهبر در مناقصه مدیریت شبکه WAN بانک تجارت و به همین دلیل، کمپلیان از ابتدای همکاری‌اش با رهبر در بانک تجارت مستقر شده است.

در قالب این پروژه شرکت رهبر متعهد شده تا در حدود ۲ هزار و ۶۰۰ نقطه که شامل شعب و باجه‌های این بانک در سراسر کشور می‌شود را پشتیبانی کند که البته با احتساب ATMها تعداد نقاط مورد پشتیبانی در کشور به ۴ هزار می‌رسد.

کمپلیان با اشاره به این مطلب که ۱۰ نفر از همکاران رهبر برای اجرای این پروژه در بانک تجارت مستقر شده‌اند گفت: تمام همکاران ما که در بانک مستقر هستند دوره‌های تخصصی شبکه را گذرانده‌اند.

وی افزود: کل خدماتی که ما به بانک تجارت ارائه می‌کنیم، UP نگه داشتن شبکه WAN بانک تجارت در سراسر کشور را شامل می‌شود. البته در بعضی قراردادهای روترهای سرپرستی را نگهداری می‌کنند اما براساس تعهدات ما نگهداری روترهای داخل شعب هم برعهده رهبر می‌گذاشته شده است. برای مثال تعمیر و نگهداری روتری در فیروزکوه یا تجهیزات باجه‌ای در کیش از وظایف ما به شمار می‌رود.

کمپلیان با اشاره به این مطلب که بعضاً با ورود تجهیزات جدید، تیم مستقر در بانک به شهرستان‌ها مأمور می‌شوند، تصریح کرد: ابعاد این پروژه بسیار بزرگ است و با توجه به تعداد اندک نیروهای مستقر در بانک، کارفرما رضایت کاملی از شرکت رهبر دارد. سرپرست سایت تعمیر و نگهداری شبکه WAN بانک تجارت افزود: با ورود رهبر به مجموعه بانک تجارت، ما به این نتیجه رسیدیم که مدیریت شبکه‌ای



نماینده رمیس در استان کرمانشاه:

کیفیت و قیمت رمیس، با دیگر شرکت‌ها قابل مقایسه نیست



شعبه شهید رستمی بانک تجارت صحنه پیش و پس از عقد قرارداد



شعبه مرکزی سنقر پیش و پس از عقد قرارداد



شعبه مرکزی صحنه کرمانشاه پیش و پس از عقد قرارداد



شعبه مسکن بانک تجارت کرمانشاه پیش و پس از عقد قرارداد



شعبه مطهری بانک تجارت کرمانشاه پیش و پس از عقد قرارداد

هستند که در این استان از خدمات این شرکت بهره‌مند می‌شوند. نماینده شرکت رمیس در استان کرمانشاه با تحسین کیفیت محصولات رمیس ادامه داد: محصولات این شرکت از نظر کیفیت و قیمت قابل مقایسه با سایر شرکت‌ها نیستند.

وی تصریح کرد: این امر مرهون مدیریت خوب در این شرکت است. فخری در خصوص پروژه‌هایی که با محصولات شرکت رمیس به انجام رسانده نیز گفت: پروژه بانک‌های سپه و تجارت در استان کرمانشاه با استفاده از سرویس‌های شرکت رمیس به انجام رسیده که پروژه‌های بسیار خوبی بود. پروژه بانک تجارت هم‌اکنون در دست اجراست و این بانک از فعالیت نمایندگی رمیس در استان بسیار راضی است. حتی براساس ارزیابی که چند روز پیش از تهران انجام شد، بانک تجارت استان کرمانشاه اعلام کرد که از نحوه فعالیت شرکت میکروپرداز ماد به عنوان نماینده شرکت رمیس رضایت کامل دارد.

وی ادامه داد: شرکت میکروپرداز ماد علاوه بر کرمانشاه در استان ایلام نیز فعالیت می‌کند و مسئولیت پروژه وب‌کیوسک‌ها در این استان را بر عهده دارد.

فرشید فخری مدیرعامل شرکت میکرو پرداز ماد است. وی که دانشجوی رشته کارشناسی کامپیوتر در دانشگاه کرمانشاه است، بیش از ۷ سال است که نمایندگی محصولات رمیس در استان کرمانشاه را بر عهده دارد.

فخری در خصوص شروع همکاری با شرکت رمیس گفت: ما از سال ۸۲ تاکنون نمایندگی محصولات این شرکت در استان کرمانشاه را عهده‌دار هستیم. البته در ابتدای کار بنده به عنوان مدیر پروژه در یک شرکت انفورماتیک مشغول به کار بودم.

وی ادامه داد: از سال ۸۷ هم با تأسیس شرکت میکرو پرداز ماد که بنده مدیرعاملش هستم، نمایندگی رمیس به این شرکت انتقال یافت.

فخری در خصوص فعالیت‌های این شرکت گفت: شرکت میکروپرداز ماد ۵ پرسنل دارد که در بخش‌های فروش، تعمیر و نگهداری تجهیزات و WAN فعالیت می‌کنند.

وی با اشاره به این مطلب که شرکت میکرو پرداز ماد نمایندگی چند شرکت دیگر را نیز بر عهده دارد، تصریح کرد: برق منطقه‌ای، بیمارستان حضرت معصومه (س)، بانک‌های تجارت، توسعه صادرات، سپه و شهر و... از جمله سازمان‌هایی



در مسابقات فوتسال جام انفورماتیک رهپیس جام اخلاق را به دست آورد

علی اف افزود: از نظر من یکی از دلایل باخت همین است که شرکت رهپیس از بازیکنان یا مربیان مطرح که در فوتسال نامی دارند استفاده نکرده و به همکاران خود اکتفا نموده است. دلیل دیگر آن را نیز می توان کم بودن تجربه در مسابقات عنوان کرد که این مسأله را برای مسابقات سال ۸۹ مرتفع خواهیم نمود. به امید خدا قرار است تیم زودتر بسته و بازی های دوستانه با تیم های خوب مسابقات جام انفورماتیک برگزار شود تا زودتر به مرز آمادگی برسیم.

سرپرست تیم رهپیس به موضوعی دیگر هم اشاره کرد: سایت مسابقات جام انفورماتیک نیز به بازی های خوب کاپیتان دروازه بان و بازی روان تیم رهپیس اشاره کرد که دلیل همین مدعی است.

در نهمین دوره مسابقات فوتسال جام انفورماتیک که به همت سازمان نظام صنفی رایانه ای کشور از اواسط آبان تا پایان دی ماه سال ۸۸ برگزار شد، تیم رهپیس با ارایه بازی هایی جوانمردانه موفق شد تا جام اخلاق این دوره از مسابقات را از آن خود کند.

تیم رهپیس در گروه B این دوره از مسابقات با سه تیم یاس ارغوانی، نداپرداز انفورماتیک و سازمان نظام صنفی هم گروه بود که البته در دوره مقدماتی در عین شایستگی حذف شد.

احسان پورمند سرپرست و بهرام علی اف مربی تیم رهپیس بودند. فرزاد حیدری، البرز محمودی، مهران یزدان پناه، احسان جلالی مقدم، امیر همت خواه، اکبر نبی زاده، محسن قزل آمادی و امیر میراحمدی هم بازیکنان تیم بودند.

بهرام علی اف در این زمینه می گوید: چند سالی است که شرکت رهپیس جهت رفاه و سلامت کارمندان خود اقدام به تهیه کارت های استخر و اجاره سالن فوتسال نموده است. ۱۸ ماه است که روزهای سه شنبه تعدادی از همکاران علاقه مند برای تفریح و حفظ سلامتی در محیطی مفرح از سالن فوتسال استفاده می کنند. البته ناگفته نماند که برای بالابردن انگیزه همکاران، تیم فوتسال رهپیس نیز تشکیل شده است که در مسابقات جام انفورماتیک حضور داشت و علی رغم تمامی شایستگی ها نتوانست از گروه خود صعود کند.

سرپرست تیم رهپیس ادامه می دهد: متأسفانه در این مسابقات اکثر تیم ها از بازیکنان غیرشرکتی استفاده می کردند. اما رهپیس به این موضوع افتخار می کند که برای تیم خود از همکاران شرکت استفاده کرده است. ناگفته نماند اخلاق در تیم رهپیس حرف اول را می زند و این مهم را با کسب جام اخلاق در مسابقات انفورماتیک دهه فجر به نمایش گذاشتیم.



گفت‌وگو با مسئول صندوق پس انداز کارکنان رمیس؛

افزایش وفاداری کارکنان

سابقه کاری بیشتری در شرکت داشته باشند، جایگاه ویژه‌تری برای دریافت وام دارند هرچند که مبالغ وام صندوق حتی برای کسانی که یک سال است در رمیس کار می‌کنند هم قابل توجه است.

سمیرا محمدی خاطر نشان کرد: از نیمه دوم سال گذشته، از طرف شرکت ۲۰ میلیون تومان به صندوق کمک شد و امروز حدود ۱۳۰ نفر عضو داریم. هدف ما از تأسیس این صندوق کمک به اعضاء جهت رفع بخشی از نیازهای مالی آنها بوده است. وی تصریح کرد: امروز همه همکاران از فعالیت صندوق رضایت دارند و در حال حاضر ۵۰ نفر از اعضا بابت وام‌هایی که دریافت کرده‌اند، در حال پرداخت اقساط به صورت ماهانه هستند.

محمدی در پایان گفت: امیدواریم توانسته باشیم به هدفی که از ابتدا داشته‌ایم برسیم و با کمک به همکاران، وفاداری آنها به رمیس را افزایش داده باشیم.



موجودی وام بدون بهره به آنها تعلق می‌گرفت که البته مبلغ وام اولیه به ۲۰۰ هزار تومان می‌رسید.

مسئول صندوق پس انداز کارکنان رمیس ادامه داد: این روال تا سال ۱۳۸۵ برقرار بود تا اینکه وضعیت صندوق بهتر شد و با درخواست همکاران، مبالغ وام‌ها تا ۱۵ میلیون تومان افزایش یافت.

امروز حتی کارکنان می‌توانند از وام مسکن استفاده کنند. البته اگر موجودی عضویت در صندوقشان بالاتر از ۷۰۰ هزار تومان باشد یا

صندوق پس انداز کارکنان رمیس در سال ۱۳۸۱ با هدف حل بخشی از مشکلات اقتصادی همکاران و با مشارکت ۷ نفر از پرسنل شرکت تأسیس شد.

سمیرا محمدی سرپرست پیشین واحد فروش سخت‌افزار و شبکه که به تازگی به واحد مارکتینگ رمیس پیوسته است، از همان ابتدا مسئولیت این صندوق را بر عهده داشته است.

وی در زمینه فعالیت این صندوق گفت: با توجه به اینکه در ابتدای فعالیت صندوق کمکی از شرکت دریافت نمی‌کردیم، امکان پرداخت وام‌های سنگین وجود نداشت و فقط ماهانه مبلغی از حقوق اعضا کسر می‌شد.

محمدی یادآور شد: در آن زمان در بدو استخدام به همکاران اعلام می‌کردیم که در صورت تمایل، می‌توانند در ازای پرداخت ماهانه ۱۰ هزار تومان به عضویت صندوق درآیند. آنها نمی‌توانستند تا ۶ ماه وام بگیرند و پس از آن به میزان ۲/۵ برابر



داستانک

کشاورز دانا

یکی از کشاورزان منطقه‌ای، همیشه در مسابقه‌ها، جایزه بهترین غله را به دست می‌آورد و به عنوان کشاورز نمونه شناخته شده بود. رقبا و همکارانش، علاقه‌مند شدند راز موفقیتش را بدانند. به همین دلیل، او رازیر نظر گرفتند و مراقب کارهایش بودند. پس از مدتی جستجو، سرانجام با نکته عجیب و جالبی روبرو شدند. این کشاورز پس از هر نوبت کشت، بهترین بذرهاش را به همسایگانش می‌داد و آنها را از این نظر تأمین می‌کرد. بنابراین، همسایگان او باید برنده مسابقه‌ها می‌شدند نه خود او!

کنجکاویشان بیشتر شد و کوشش علاقه‌مندان به کشف این موضوع که با تعجب و تحیر نیز آمیخته شده بود، به جایی نرسید. سرانجام، تصمیم گرفتند ماجرا را از خود او بپرسند و پرده از این راز عجیب بردارند. کشاورز هوشیار و دانا، در پاسخ به پرسش همکارانش گفت: «چون جریان باد، ذرات بارورکننده غلات را از یک مزرعه به مزرعه دیگر می‌برد، من بهترین بذرها را به همسایگان می‌دادم تا باد، ذرات بارورکننده نامرغوب را از مزرعه‌های آنان به زمین من نیاورد و کیفیت محصول‌های مرا خراب نکند!»

همین تشخیص درست و صحیح کشاورز، توفیق کامیابی در مسابقه‌های بهترین غله را برایش به ارمغان می‌آورد.

«گاهی اوقات لازم است با کمک به رقبا و ارتقاء کیفیت و سطح آنها، کاری کنیم که از تأثیرات منفی آنها در امان باشیم.»

رمیس، حامی مؤسسه خیریه دارالاکرام

شرکت رمیس در فعالیتی خداپسندانه، به جمع نیکوکاران مجموعه خیریه دارالاکرام پیوسته و در اقدامات خیرخواهانه این مجموعه مشارکت می‌کند. این مجموعه ضمن تحت پوشش قرار دادن دانش‌آموزان ممتاز ایتم، بیماران مستمند را نیز تحت پوشش قرار می‌دهد. همچنین دارالاکرام؛ هدایت، نظارت و مساعدت با مددجویان جوایای کار را تا رسیدن به مرحله تولید و کسب درآمد به عهده می‌گیرد. منابع مالی این مؤسسه از دو طریق داخلی و بیرونی تأمین می‌شود. در واقع علاوه بر موسسین و افراد خیر حاضر در هیأت امان و هیأت مدیره، مبالغی به صورت کمک بلاعوض و یا به صورت سرمایه امانی در اختیار دارالاکرام قرار داده شده است که فعالیت‌های گذشته دارالاکرام متکی بر همین کمک‌ها بوده است. شرکت رمیس نیز یکی از موسساتی است که به کمک نیکوکاران دارالاکرام شتافته و در این فرآیند خیرخواهانه با این مجموعه همراه شده است. در کارنامه این مؤسسه می‌توان به مواردی چون یاری‌رسانی به هلال‌احمر برای کمک به زلزله‌زدگان قزوین، کمک به ساخت یک باب مدرسه در بسم پس از رویداد ناگوار زلزله و پرداخت کمک مالی ماهیانه بلاعوض در موارد گوناگون اشاره کرد. همکارانی که تمایل دارند تا با این مؤسسه خیریه همکاری نمایند، می‌توانند با شماره تلفن ۸۸۶۹۹۱۵۲ تماس گرفته و یا با پست الکترونیکی darol.ekram@gmail.com مکاتبه نمایند.

همچنین همکارانی که تمایل داشته باشند، می‌توانند کمک‌های نقدی خود را به حساب پس‌انداز شماره ۳۰/۱۱۵/۴ و جاری شماره ۱۰/۸ بانک ملت شعبه شهرک ژاندارمری (کد ۶۷۷۶۹) واریز نمایند.

گزارش تصویری

هشتمین سالگرد تأسیس رمیس جشن گرفته شد

هشتمین سالگرد تأسیس رمیس با حضور تمام همکاران این شرکت و خانواده‌های آنها جشن گرفته شد. در این مراسم مهندس غیاث‌الدین و مهندس نوربخش مدیرعامل و قائم‌مقام شرکت رمیس سخنرانی کردند، امیر تاجیک آواز خواند، مسابقه و قرعه‌کشی برگزار شد و پس از بریدن کیک هشتمین سال تولد رمیس؛ همکاران با یکدیگر عکس یادگاری گرفتند.





آشنایی با مرکز عملیات امنیت SOC

در مرکز عملیات امنیت چه کارهایی انجام می‌گیرد؟

مرکز عملیات امنیتی که به درستی مدیریت و پیکربندی شده باشد همانند مغز شبکه عمل می‌کند. مرکز عملیات امنیت SOC اطلاعات زیادی از ابزارهای متنوعی مانند (دیواره آتش، آنتی ویروس، سیستم‌های تشخیص نفوذ و...) در سطح شبکه جمع‌آوری، سپس آن اطلاعات را نرمال‌سازی و مرتبط کرده و گزارش‌دهی بلادرنگی از آنچه در حال اتفاق است فراهم می‌کند. بنابراین اپراتورها توانایی مدیریت و پاسخگویی مناسبی در مقابل حوادثی که وقوع آنها باعث به خطر افتادن سازمان می‌شوند را خواهند داشت. در مواردی که جلوگیری کامل در مقابل خطرات امکان‌پذیر نباشد، گزارش‌دهی SOC به اپراتورها امکان تشخیص حمله و کاهش خسارات آن قبل از انتشار در شبکه را می‌دهد. امروزه در بسیاری از سازمان‌ها به منظور کنترل و مدیریت ترافیک شبکه مراکز عملیات شبکه NOC راه‌اندازی شده است، هرچند که این مرکز فاقد روشی برای مدیریت متمرکز حوادث امنیتی است. فعالیت اولیه مرکز عملیات شبکه NOC نگهداری و اطمینان از صحت و سلامت شبکه و زیرساخت سازمان است در حالی که مرکز عملیات امنیت SOC مدیریت حوادث امنیتی را به منظور حفاظت شبکه بر عهده دارد. بنابراین به منظور افزایش بازدهی و کارایی سازمان‌ها، از طریق پاسخگویی مناسب به حوادث امنیتی مانند ویروس‌ها و حملاتی که منجر به از دست رفتن یکپارچگی شبکه می‌شود، وجود این مرکز در کنار مرکز NOC بسیار موثر خواهد بود.

مرکز عملیات امنیت SOC می‌تواند برای حل سریع‌تر مسایل امنیتی منبع اطلاعاتی مناسبی برای مرکز عملیات شبکه NOC باشد.



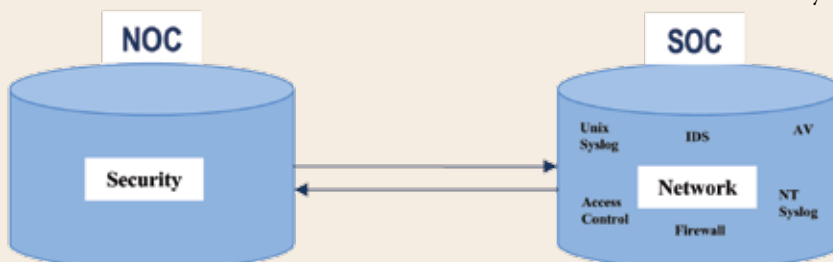
• بهارک نانکلی

امروزه مدیریت حوادث امنیتی در بسیاری از سازمان‌ها، پرسنل IT را با چالش‌های بالایی مواجه ساخته است. راهکارهای امنیتی بی‌شماری مانند نرم‌افزارهای آنتی ویروس، دیواره آتش، سیستم‌های جلوگیری از نفوذ، سیستم‌های تشخیص نفوذ، کنترل‌های دسترسی و سیستم‌های شناسایی که در سطح شبکه استفاده می‌شوند وجود دارند. همگی آنها اطلاعات و گزارش‌هایی در فرمت‌های متفاوت ایجاد کرده که در مکان‌های متفاوتی ذخیره شده و به افراد خاصی نیز ارسال می‌شوند. بنابراین سازمان‌ها روزانه با میلیون‌ها پیام از این تکنولوژی‌های امنیتی ناسازگار مواجه هستند که نتیجه آن ازدیاد اطلاعات امنیتی است. این ازدیاد اطلاعات منجر به افزایش بار کاری و تلاش پرسنل IT شده و در نهایت یک سیستم امنیتی ضعیف برای سازمان را به همراه خواهد داشت. برای جبران خسارات ناشی از حوادث امنیتی و حفاظت از عملیات تجاری سازمان‌ها، مدیران امنیت شبکه وجود سیستم مدیریت امنیتی بلادرنگ، متمرکز و یکپارچه متناسب با توانایی‌های مراکز مانیتورینگ NOC را لازم می‌دانند. مرکز عملیات امنیت SOC نمایی از وضعیت امنیتی شبکه را از طریق اعلام‌های اتوماتیک و گزارش‌های مناسب از وضعیت شبکه فراهم می‌کند. مرکز عملیات امنیت SOC تمام زوایای امنیتی را به صورت بلادرنگ از یک نقطه مرکزی مدیریت و مانیتور کرده و تمام حوادث امنیتی را کشف و اولویت‌دهی می‌کند. این سیستم سطح ریسک و دارایی‌هایی را که تحت تاثیر قرار خواهند گرفت تشخیص داده و راهکارهای مناسبی برای آن اجرا یا ارایه می‌کند.

تعریف مرکز عملیات امنیت SOC

مرکز عملیات امنیت SOC واحدی متمرکز برای رسیدگی به حوادث و وقایع امنیتی در سازمان‌ها بوده که هدف از آن تشخیص و واکنش سریع در برابر حوادث امنیتی است. این مرکز از طریق یک کنسول مرکزی وضعیت آنچه را که در حال حاضر در شبکه در حال اتفاق است را نشان می‌دهد. مرکز عملیات امنیت SOC از ۵ ماژول به ترتیب زیر تشکیل شده است:

- Events Generator
- Event Based Data generator: ایجاد وقایع در صورت انجام عملیات خاصی توسط سیستم عامل یا برنامه‌های کاربردی در سطح شبکه
- Status Based Data Generator: ایجاد وقایع در صورت واکنش در برابر یک محرک خارجی مثل Ping
- Message Database
- Events Collectors
- Reaction Management Software
- Analysis Engines
- Storage
- Collection
- Security Events Generation
- Reaction
- Analysis



مراحل راه اندازی مرکز عملیات امنیت SOC

در این قسمت چگونگی راه اندازی مرکز عملیات امنیت SOC و همچنین ۶ فاز پاسخگویی به حوادث امنیتی توضیح داده شده است. با پیگیری مرحله به مرحله فازها می توان برای تشخیص، حل و کاهش حوادث امنیتی فرایندهای مناسبی را ایجاد نمود.

۱- طراحی ساختار مرکز عملیات امنیت SOC
ساختار SOC نشان دهنده آن است که چه اطلاعات امنیتی جمع آوری، چگونه آنالیز، پردازش و به هم مرتبط شده اند. (شکل شماره یک)

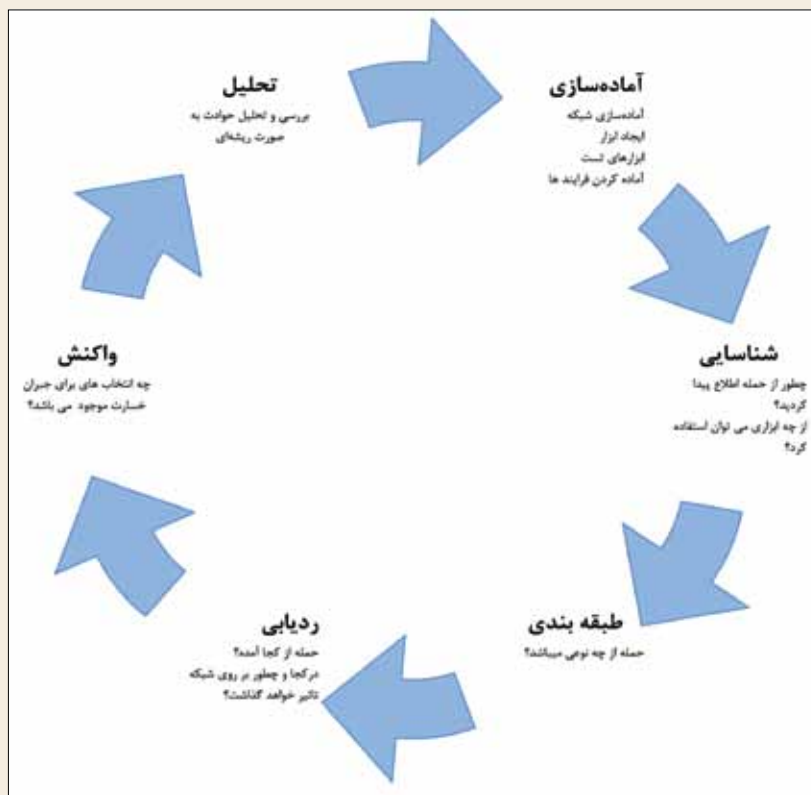
شکل شماره یک ▼



۲- ۶ فاز پاسخگویی به حوادث امنیتی

پس از طراحی ساختار SOC باید به حوادث امنیتی که هنوز پوشش داده نشده اند پاسخ مناسب و موثری داده شود. در زیر به ۶ فاز پاسخگویی به حوادث اشاره شده است: (شکل شماره دو)

شکل شماره دو ▶



۳- خروجی SOC

مرکز عملیات امنیت باید خروجی های زیر را در قالب گزارش ارائه دهد:

- مانیتورینگ امنیت برای مدیریت ریسک
- تحلیل ریسک های امنیتی
- دسترسی امن بر اساس نقش و وظیفه
- گزارشات سیاست های امنیتی
- مانیتورینگ بلادرنگ و وضعیت تیکت ها و حوادث
- روند اتفاقات و حوادث امنیتی و ...
- ارزیابی بلادرنگ حوادث در کنار گزارش های هفتگی و ماهیانه
- گزارشات حوادث امنیتی

نتیجه گیری

مرکز عملیات SOC به شما این امکان را می دهد تا شبکه و اطلاعات مربوط به آن را از خطر تهدیدات امنیتی، ایمن نگه دارید.

با طراحی مناسب و پیگیری فرایندهای سیستماتیک برای پاسخگویی به حوادث امنیتی، می توان خطرات و تاثیر تهدیدات و حملات بر روی شبکه را تا حد قابل ملاحظه ای کاهش داد.

معرفی نرم افزار HP NNM



■ علی بیزمارک

از POLLING استفاده می کند به طوری که خود نرم افزار در زمان های مشخصی که قابل تنظیم است به نودها وصل شده و وضعیت آنها را بررسی می کند؛ چنانچه مشکلی در نود وجود داشته باشد یک پیغام خطا برای مدیر ایجاد می کند. همچنین می توان روی دستگاه ها TRAP را تنظیم کرد تا چنانچه برای نود مشکلی به وجود بیاید قبل از اینکه نرم افزار عمل POLLING را انجام دهد پیغام خطا در سیستم ایجاد شود. این تنظیمات به سادگی در سیستم قابل تعریف بوده و می توان به آسانی نیز بازه های زمانی برای عمل POLLING تعریف کرد. نرم افزار NNM تمام پیغام ها را از دستگاه ها گرفته

موضوع مهم دیگر پروتکل ارتباطی است که بتوان با آن، ارتباط سرور با دستگاه ها را درون شبکه فراهم کرد. چنانچه برای دستگاه هایی که مدیر شبکه می خواهد وضعیت آنها را مانیتور کند اتفاقی رخ دهد، باید بتوان خطا را در کم ترین زمان ممکن در سرور مشاهده کرد.

نرم افزار NNM از پروتکل SNMP برای مدل مدیریتی استفاده می کند. همان گونه که می دانیم این پروتکل در رده پروتکل های استاندارد مدیریت شبکه است که تمام دستگاه ها معمولاً قابلیت پشتیبانی از این پروتکل را دارند.

نرم افزار NNM به وسیله این پروتکل با ایستگاه های کاری ارتباط برقرار کرده و به وسیله MIB که در این ایستگاه ها ذخیره شده است وضعیت آنها را مورد بررسی قرار می دهد؛ چنانچه مشکلی هم برای دستگاهی به وجود بیاید یک پیغام خطا برای نرم افزار NNM ارسال خواهد شد.

کار نرم افزار NETWORK NODE MANAGER در شبکه

این نرم افزار ساخت کمپانی HP است و توانایی کار با هر دستگاهی که پروتکل SNMP را پوشش دهد، دارد.

از قابلیت های دیگر این نرم افزار پیدا کردن خودکار تمام دستگاه های درون شبکه و ارتباطات آنها در لایه ۲ و ۳ است. همچنین در صورت نیاز می توان دستگاه ها را به صورت دستی در نرم افزار اضافه کرد.

این نرم افزار برای تشخیص مشکل در نودها

خلاصه ای در مورد مدیریت شبکه

مدیریت شبکه توانایی کنترل تمام فعالیت های شبکه از یک نقطه متمرکز و واحد است.

محدوده های استاندارد مدیریت شبکه

طبق استاندارد OSI MANAGEMENT FRAMEWORK مدیریت شبکه در ۵ محدوده زیر تعریف می شود:

- ۱- مدیریت خطا
- ۲- مدیریت تغییرات
- ۳- مدیریت کاربران
- ۴- مدیریت بازدهی
- ۵- مدیریت امنیت

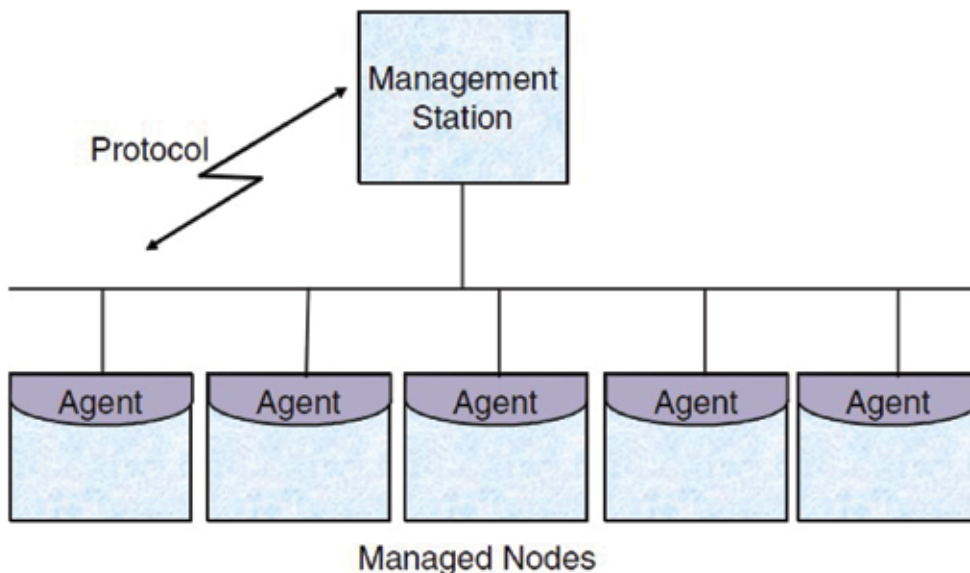
هدف از مدیریت شبکه

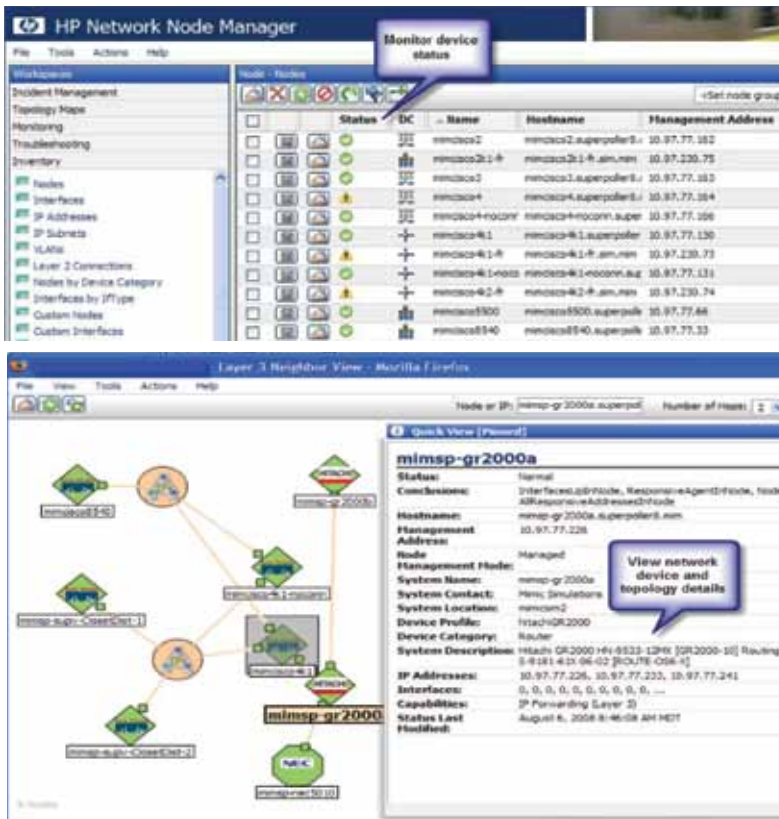
- ۱- کم کردن زمان خطایابی در شبکه
- ۲- استفاده بهینه از منابع سازمان است.

برای دستیابی به اهداف فوق، نرم افزار مدیریت باید بتواند به وسیله ابزارهایی که در اختیار مدیر شبکه قرار می دهد فعالیت های زیر را در شبکه انجام دهد:

- ابزارهای خطایابی
- ذخیره کردن دیتا بیس
- ارزش افزوده

یک مدل مدیریتی استاندارد باید مطابق این شکل باشد، بدین معنی که دارای یک ایستگاه مدیریتی باشد تا تمام اتفاقات درون شبکه را بتوان در آن دستگاه مانیتور کرد؛ همچنین دیتای به دست آمده از دستگاه ها درون این سرور ذخیره شود.





همچنین محیط گرافیکی نرم افزار نیز به صورت بهینه در آمده تا کاربران و مدیران شبکه بهتر بتوانند با آن ارتباط برقرار کنند.

از دیگر تفاوت های نسخه ۷.۵ و ۸ می توان به امکان ایجاد کاربر در نرم افزار اشاره کرد. در نسخه های ۷.۵ زمانی که مدیران شبکه به نرم افزار متصل می شدند، امکان تنظیم امنیتی برای پرسیدن نام کاربری در نرم افزار وجود نداشت؛ ولی در نسخه ۸ این مشکل برطرف شده و چنانچه یک مدیر بخواهد وارد کنسل NNM شود، ابتدا باید اطلاعات کاربری را وارد کرده و در صورت مجاز بودن می تواند به سیستم متصل شود.

همچنین نسخه ۸ صرفاً تحت سیستم عامل های ۶۴ بیتی قابلیت نصب دارد که باعث می شود کارایی نرم افزار به صورت قابل ملاحظه ای افزایش یابد. به وسیله این نرم افزار می توان توپولوژی شبکه را نیز به سادگی مشاهده و وضعیت ارتباطات بین دستگاه ها را بررسی کرد. این توپولوژی شامل ارتباطات Trunk هم بوده و نرم افزار NNM این ارتباطات را نیز مانیتور می کند.

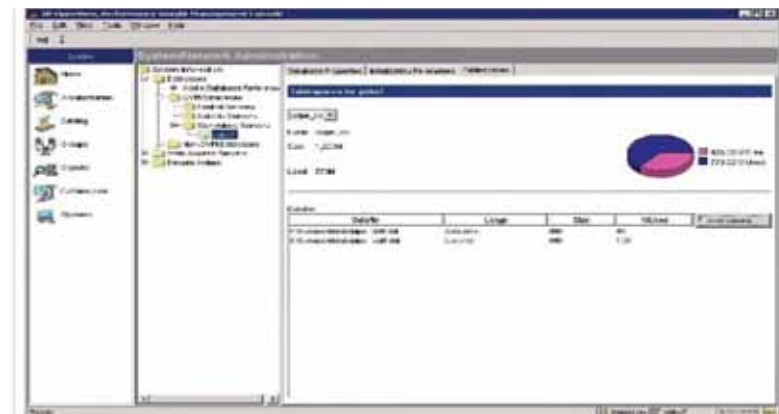
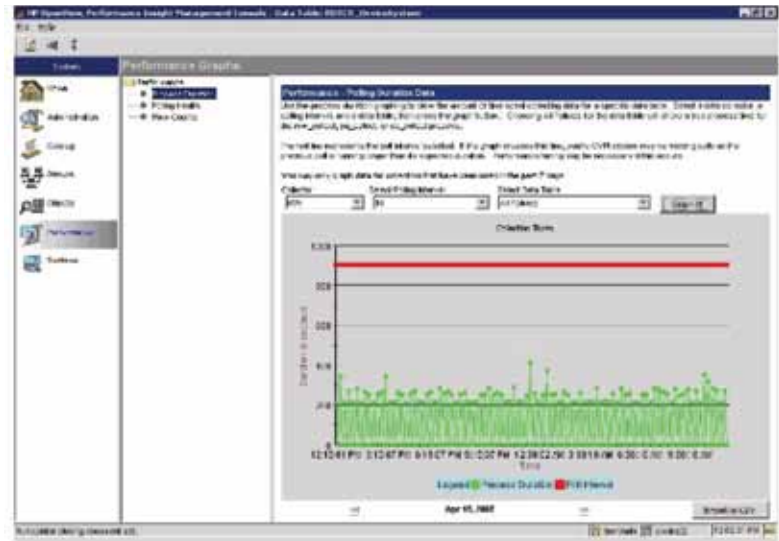
همچنین برای اتصال به نرم افزار NNM، با وارد کردن IP آدرس سرور، می توان از هر نقطه ای در شبکه به آن دسترسی پیدا کرد.

گزارش گیری از نرم افزار NNM

برای استخراج گزارش از نرم افزار باید از ماژول PERFORMANCE استفاده کرد. کار ماژول یاد شده این است که به پایگاه داده نرم افزار وصل شده و هر گزارشی را که مدیر تنظیم کند از نرم افزار NNM دریافت و به صورت گرافیکی در اختیار مدیر شبکه قرار می دهد. همان گونه که در شکل های بالا مشاهده می شود این نرم افزار کاملاً USER FRIENDLY بوده و گزارش ها را به صورت اشکال و گراف های کاملاً واضح در اختیار مدیر شبکه قرار می دهد. چنین قابلیتی باعث می شود مدیر شبکه بتواند طرح جامعی برای بهینه سازی شبکه استخراج و مشکلات شبکه را دقیقاً و همراه با جزئیات مشاهده نماید تا بتواند در کمترین زمان و قبل از اینکه اتفاقی در شبکه رخ دهد از وقوع خطا جلوگیری کند.

پایگاه داده نرم افزار NNM

این نرم افزار به صورت پیش فرض دارای یک DATA WAREHOUSE است که همراه با نصب نرم افزار تمام وقایع و اتفاقات شبکه و اطلاعات کلی مربوط به نودها و ارتباطات درون این پایگاه داده قرار می گیرد. در هنگام درخواست گزارش از نرم افزار، ماژول مربوطه به این پایگاه متصل، اطلاعات لازم را استخراج و به صورت گرافیکی در اختیار مدیر قرار می دهد. همچنین می توان از نرم افزار ORACLE نیز برای ذخیره کردن اطلاعات استفاده کرد که باعث می شود گزارش های بیشتری را از نرم افزار دریافت کرد.



پیام‌های مدیریتی بزرگان

یک ویژگی شخصیتی است و افراد با انگیزه، هر شغل دیگری را با همان شدت و اشتیاق برعهده خواهند گرفت. اما تحقیقات نشان داده است که حتی متعهدترین کارکنان نیز اگر شغل خود را دیگر هدفمند ندانند و یا به موفقیت دست نیابند، انگیزه خود را از دست خواهند داد.

۱۰- مدیران با تجربه و کارآمد باید هوشیارانه موانع موجود برسر راه کارکنان متعهد که اغلب به اشتباه تصور می‌شود نیاز به کمک کمتری دارند را مرتفع سازند. افرادی که بیشتر به کار و تعهد خود اهمیت می‌دهند در صورت مانع تراشی، بیش از بقیه مأیوس می‌شوند.



۷- مدیران روشنفکر به این مسأله پی برده‌اند که کارکنان در پی یافتن معنا و رضایت شغلی هستند. چیزی که فقط به دستمزد مربوط نمی‌شود. این مدیران فهمیده‌اند چگونه کارکنان را برانگیزند و پاداش‌ها را مطابق سازند.

۸- یک مدیر حرفه‌ای می‌داند که در صورت ابهام در تعریف وظایف شغلی، کارکنان متعهدتر، رضایت شغلی کمتری دارند و چه بسا سرخورده می‌گردند.

۹- این سوء تفاهم برای برخی از مدیران وجود دارد که تعهد شغلی یا به عبارتی، انگیزه شغلی بالا

۱- دارایی‌های اصلی بنگاه‌های اقتصادی نوین، اعم از کارخانجات، سازمان‌های خدماتی و...؛ نه در ساختمان‌ها، ماشین‌آلات و مستغلات، بلکه در هوش، دانش، فهم، مهارت و تجربه کارکنان آنها نهفته است.

۲- به جای تحمیل راه‌حل‌ها به کارکنان نافرمان، مدیر باید شرایطی ایجاد کند که این کارکنان بتوانند انگیزه‌های خود را در جهت هدف‌های قابل دستیابی هدایت کنند.

۳- انتظارات یک فرد، تعیین‌کننده رفتار فرد دیگر است. اگر مدیر سطح انتظارات خود را بالا برد، احتمالاً کارکنان هم پیشرفت می‌کند. اگر سطح انتظارات مدیر پایین باشد، چه بسا کارکنان هم افت عملکرد پیدا کند.

۴- خویشتن‌شناسی مدیران بر نظرات و رفتار آنها با کارکنان تأثیر می‌گذارد.

۵- مدیرانی که به جای بهره‌گیری از قدرت در راه تحقق اهداف سازمانی، آن را صرفاً در جهت پیشبرد اهداف شغلی خود مورد استفاده قرار می‌دهند، به دنبال کارکنانی هستند که بیش از وفاداری به سازمان به شخص آنها وفادار باشند.

۶- رابطه بین روحیه کارکنان و مقادیر فروش نشان می‌دهد که مدیران زورمدار کم‌اثرتر از مدیرانی هستند که سبک مدیریتی مردم‌سالارانه‌تری دارند.

منابع

۱- کتاب فراسوی توان افزایی

Brook Manville / Josiah Ober

۲- مقاله انگیزش کارکنان بدقلق

Nigel Nicholson

۳ و ۴- مقاله پیگمالیون در مسند مدیریت

J. Sterling Livingston

۵ و ۶- کتاب قدرت بزرگترین عامل انگیزش

/H. Burnham David David C. Mclelland

۷ و ۸ و ۹ و ۱۰- کتاب سقوط شاهین سیاه

Thomas w. Britt

گزیده‌ای از کتاب مدیریت بر قلب‌ها

۷- بسیاری از مدیران، کار خوب افراد را می‌بینند و می‌پسندند، ولی متأسفانه بیشتر وقتها اندیشه مثبت خود را به زبان نمی‌آورند. اگر خواهان کارکرد شایسته کارکنان تان هستید، باید نشان دهید که کار خوب را تشخیص می‌دهید و به آن توجه ویژه دارید.

۸- مدیران امروزی باید ارزش یک لیخنه را دوباره بیاموزند و گرنه نمی‌توانند کارکردن شادی بخش را به کارکنان خود یاد دهند. اجازه دهید کارمندان از دیدار شما شاد شوند.

۹- مدیریت کردن، صرفاً فرمان دادن به کارکنان نیست، بلکه کار کردن با آنها است.

۱۰- مدیران قوی، همواره نسبت به حفظ حرمت و شخصیت کارمندان خود، توجهی خاص دارند. کارمندی که در محل کارش شخصیت خود را در معرض خطر ببیند، هرگز کارآیی مثبتی نخواهد داشت. مدیران توانمند، مشکلات را تجزیه و تحلیل و سپس برطرف می‌کنند. نباید از بروز مشکلات هراس داشت. زیبایی زندگی و کار با عبور از دیوار مشکلات و فرو ریختن آنها نمایان می‌شود. تنها یک گروه از انسان‌ها بدون مشکل هستند، مردگان.

۱- یکی از مهم‌ترین وظایف مدیران، رهبری است. رهبری یعنی هنر نفوذ در قلب و باورهای دیگران و این هنر از قلب یک رهبر آغاز می‌شود.

۲- یک مدیر باید همواره آگاهی داشته باشد که تصمیماتش، زندگی بسیاری را متأثر می‌سازد. سنگینی بار این مسئولیت شری بر جان مدیران می‌نشانند که در هر کجا که هستند همواره تلاش نمایند که خود را توسعه دهند.

۳- مدیران کارآمد از دو روش، پیشگام کمک به همکاران خود در راه رسیدن به نتیجه‌های خوب می‌شوند:

اول: هدف‌ها را به درستی به آنان می‌شناسانند.

دوم: در راه رسیدن به اهداف، هر چه از دستشان بر آید، اعم از پشتیبانی، تشویق و راهنمایی کوتاهی نمی‌کنند.

۴- مدیران آگاه، برای اندیشیدن، راهبردگذاری و تنظیم اولویت‌ها به خود ایست می‌دهند و اندیشه می‌کنند. اگر چنین نباشد، فقط به سختی کار کرده‌اند و از انجام هوشمندانه کارها بهره‌ای نبرده‌اند.

۵- مدیرانی که تنها به سود می‌اندیشند، مانند تنیس‌بازانی هستند که به جای توپ، چشم به تابلوی امتیازات دوخته‌اند.

۶- اگر کارکنان متعهد می‌خواهید، نیازهایشان را به موقع پاسخگو باشید.

آشنایی با CS-MARS

■ مهدی نیک‌عهد

آنتی‌ویروس‌ها و سیستم‌های دیگری که قابلیت ارسال Log‌های استاندارد را داشته باشند نیز پشتیبانی می‌کند. بعد از جمع‌آوری آنها، CS-MARS، به آنالیز و تجزیه و تحلیل آنها پرداخته و براساس پارامترهای مختلف ارتباط بین آنها را مشخص می‌کند. در نهایت CS-MARS وقایع و رخداد‌های مهم امنیتی را دسته‌بندی کرده و به مدیر شبکه نمایش می‌دهد.



در نگاهی علمی‌تر محصولات مدیریتی امنیتی در دسته‌بندی زیر قرار می‌گیرند:

- Security Event Management (SEM) System
- Security Information Management (SIM) System
- Security Threat Mitigation (STM) System

SEM System و SIM System که سیسکو آنها را به صورت System SIEM معرفی می‌کند، عموماً در فرایند Incidence Handel کار جمع‌آوری و دسته‌بندی اطلاعات و در نتیجه مشخص شدن مبدا و مقصد حمله را به عهده دارند که در اکثر موارد کمک قابل توجهی به مدیریت شبکه محسوب می‌شود، چرا که مشخص شدن مبدا و مقصد حمله در بسیاری از موارد مهم‌ترین بخش برطرف کردن حملات تحت شبکه است. وظایف یک SIEM را می‌توان به صورت زیر تقسیم‌بندی کرد:

- Event Collection and Correlation

جمع‌آوری Event‌ها از تجهیزات مختلف امنیتی و پیدا کردن ارتباط بین آنها جهت تشخیص حمله

- Reporting

گزارش‌گیری از رویدادها

- Alerting

اخطار به هنگام تشخیص رویداد مشکوک یا نادرست
STM System‌ها دارای تمام توانایی‌های System SIEM هستند علاوه بر آن به تحلیل و آنالیز اطلاعات به دست آمده نیز می‌پردازند. در ارتباط با وظایف یک STM در مقایسه با SIEM می‌توان به موارد زیر اشاره کرد:

- Sessionization

توانایی جمع‌آوری Event‌های مربوط به هم از دستگاه‌های مختلف و به طور خلاصه اشاره کردن به اتفاقی که در حال افتادن در شبکه است.

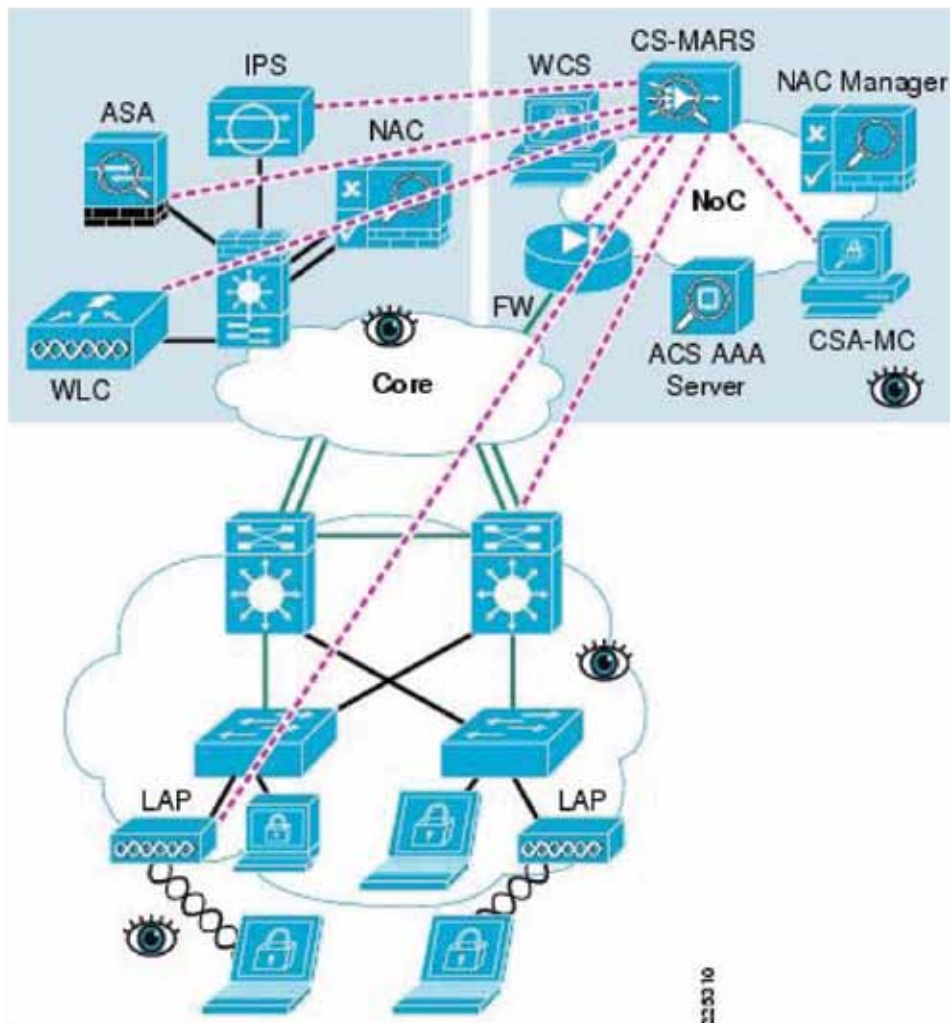
در بازار بزرگ و گسترده IT محصولات امنیتی متنوع و رقابتی زیادی وجود دارد. محصولاتی که Log‌ها و Even‌های تجهیزات مختلف امنیتی را به صورت پایگاه داده جمع‌آوری می‌کنند. مشکل عمده این محصولات به‌ویژه در شبکه‌های بزرگ، تولید حجم بسیار زیاد Log توسط تجهیزات فعال شبکه و از طرفی دیگر گوناگونی این Log‌ها (Syslog، NeFlow، SNMP و...) است. به زبان ساده‌تر استاندارد واحدی برای فرمت و پروتکل Log‌ها وجود نداشته و هر شرکت از

استاندارد خاص خود برای ارسال Log‌ها استفاده می‌کند. از دیگر معایب این تجهیزات خام بودن Log‌ها است به آن معنی که مدیر شبکه با حجم انبوهی Log از دستگاه‌های متفاوت روبروست که آنالیز و بررسی آنها تنها با بسنده کردن به توانایی‌های انسانی دشوار و تقریباً غیرممکن است. شرکت سیسکو با ارائه محصولی به نام Cisco Security, Analysis and Response System یا CS-MARS دغدغه‌های مشتریان در ارتباط با Log‌ها را برطرف کرده است.

CS-MARS جزء نسل سوم ابزارهای امنیتی شرکت سیسکو (محصولات Monitoring و Analyze) است. این نسل از محصولات همان‌گونه که از نام آنها پیداست وظیفه مانیتورینگ، آنالیز و حتی در مواردی مدیریت (Management) را انجام می‌دهند. CS-MARS به صورت Appliance عرضه شده و دارای سیستم عامل مبتنی بر لینوکس و پایگاه داده Oracle است. در گذشته داده‌ها و Log‌های جمع‌آوری شده از تجهیزات امنیتی و شبکه مانند سویچ‌ها، روترها، فایروال‌ها، IPS و IDS‌ها به طور جداگانه در سیستم‌های مختلف گردآوری شده و هر Vendor و گاهی هر محصول، از کنسول خاص خود برای جمع‌آوری Report و Event‌ها استفاده می‌کرد. در نتیجه ارتباطی بین Log‌ها وجود نداشت و مدیران شبکه مجبور بودند که به صورت دستی این تجهیزات را مانیتور کنند.

CS-MARS در ابتدا برای حل مشکلی که سازمان‌ها برای جمع‌آوری Log‌ها داشتند عرضه شد. این دستگاه توانایی بالایی در دریافت و خواندن Log‌های موجود در شبکه را داشته و تمام استانداردهای موجود در این حوزه که بعداً در همین مقاله به آنها اشاره خواهد شد را پشتیبانی می‌کند. CS-MARS علاوه بر روتر، سویچ‌ها و تجهیزات امنیتی شبکه؛ از سرورها،





ACL بر روی روتر یا فایروال لبه شبکه از ورود ترافیک آلوده جلوگیری نماید.

در ادامه به تشریح تعدادی از پروتکل‌های مدیریتی که CS-MARS پشتیبانی می‌کند می‌پردازیم:

۱- NetFlow: این پروتکل به منظور رفع برخی از نیازمندی‌های Service Providerها و سازمان‌های بزرگتر ایجاد شد. NetFlow با ایجاد Flowها یا Sessionها براساس بسته‌های عبوری از اینترفیس‌ها برای مدیران شبکه قابلیت مانیتور کردن شبکه به صورت Real-time را فراهم می‌کند. Netflow می‌تواند برای تحقق این اهداف مورد استفاده قرار گیرد:

- Application profiling and monitoring
- User profiling and monitoring
- Network interface monitoring, for capacity planning
- Accounting and billing
- Security monitoring

این پروتکل می‌تواند بر روی اکثر سویچ و روترهای سیسکو فعال شده و استفاده از آن به همراه CS-MARS کمک می‌کند تا دید درستی از اینکه کدام سیستم‌ها و برنامه‌ها بیشترین ترافیک را ایجاد می‌کنند برای ما فراهم کند. این، یکی از روش‌های کلیدی برای تشخیص سریع Worm است.

۲- Syslog: می‌توان گفت که این پروتکل بیشترین و فراگیرترین سطح استفاده را در بین پروتکل‌های هم‌خانواده خود دارد. Syslog یک پروتکل پیام چند منظوره است و قابلیت فرستادن انواع پیام‌ها را از تجهیزات

● Topology awareness

تشخیص توپولوژی شبکه و لینک‌های ارتباطی بین تجهیزات.

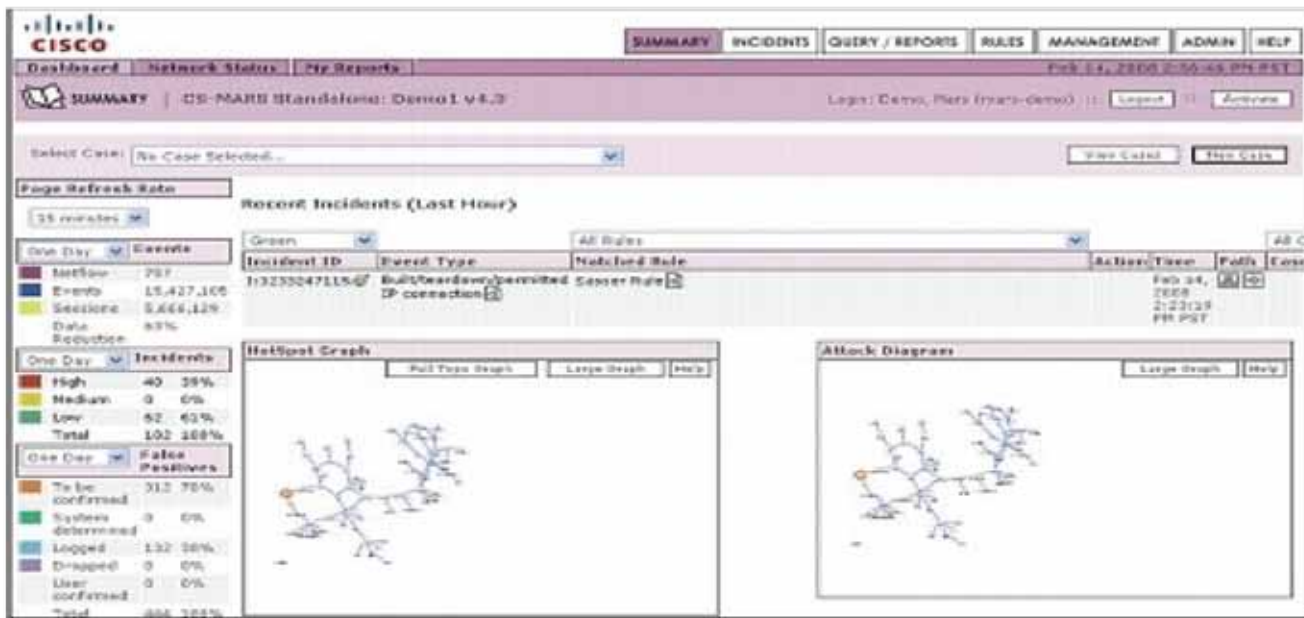
● Mitigation

واکنش نشان دادن نسبت به اتفاقات و Eventهای نادرست. به عنوان مثال با بستن پورت سیستم بر روی سویچ.

با این توضیحات CS-MARS جزء دسته Systemها قرار می‌گیرد. جهت روشن شدن قابلیت‌های CS-MARS به تشریح یک مثل می‌پردازیم. شبکه بزرگی با تمام تجهیزات فعال شامل سویچ، روتر، فایروال، IPS و... را در نظر بگیرید. تمام تجهیزات Logهای خود را به CS-MARS می‌فرستند. حال اگر یکی از سیستم‌های درون شبکه آلوده به Warm شده و شروع به آلوده کردن تمام شبکه نماید، در مدت کوتاهی کل شبکه دچار مشکل می‌شود.

در اینجا CS-MARS با توجه به اینکه تمام پروتکل‌های مدیریتی را پشتیبانی می‌کند، Logها را از تجهیزات جمع‌آوری کرده، با مرتبط کردن آنها و تشخیص Eventهای مربوط به هم، Warm و منشاء، انتشار آن را تشخیص می‌دهد. سپس با ارسال E-mail، SMS یا Alert مدیر شبکه را از این اتفاق مطلع می‌نماید.

در عین حال CS-MARS می‌تواند با استفاده از CAM Table موجود در سویچ‌ها و با استفاده از NetFlow، Mac Address سیستم آلوده را در همان مراحل اولیه Block کرده و به این دستگاه آلوده اجازه انتشار Warm نمی‌دهد. یا در صورتی که یک Attack از بیرون، شبکه را مورد تهدید قرار دهد، CS-MARS پس از تشخیص این امکان را دارد که با اعمال



به eventها را از تجهیزات pull می کند (اصطلاحاً بیرون می کشد) در حالی که SNMP و Syslog از متد Push استفاده می کنند. در حال حاضر سیسکو بر روی تمام تجهیزات IDS و IPS از SDEE استفاده می کند.

در انتها به تعریف چند اصطلاح کلیدی در CS-MARS می پردازیم. **● Event:** هر Log صرف نظر از اینکه چگونه به CS-MARS رسیده یک Event به حساب می آید. یک Event می تواند از طریق هر متد پشتیبانی شده از قبیل Check Point's LEA, Syslog, RDEP, SDEE یا SNMP Log ویندوز دریافت شود.

● Session Event: Sessionهای مرتبط به هم که همه به یک جریان شبکه وابسته باشند، یک session را تشکیل می دهند. این Eventها می توانند از یک دستگاه و یا از چندین دستگاه دریافت شده باشند. Session هنگامی ایجاد می شود که Evenها براساس timestamp یا Hold-down Timer, آدرس مبدأ، آدرس مقصد، پورت مقصد و پروتکل مربوط را تشخیص دهد.

● rule: rule: آنها توصیف رفتار خاصی هستند. آنها با استفاده از Query هایی که می توانند بسیار ساده یا پیچیده باشند، ایجاد می شوند. در حقیقت CS-MARS از این ruleها برای شناسایی فعالیت هایی که شما می خواهید در مورد آنها بدانید استفاده می کند. این ruleها در گزارشها نیز مورد استفاده قرار می گیرند.

● Incidents: یک Incident زمانی که فعالیت های شبکه با رفتارهای تعریف شده در یک rule تطابق پیدا کرد، Trigger می شود. به زبان ساده تر یک Incident در نتیجه تطابق Sessionها با ruleها ایجاد می شود.

● False Positives: زمانی که یک attack علیه هدفش ناموفق باشد، CS-MARS آن را به عنوان False Positive در نظر می گیرد. البته این اسم تا حدودی بی مسمی است چرا که در واقع زمانی که دستگاه، اشتباهی یک Attack را تشخیص دهد یعنی در حقیقت آن یک حمله نبوده است و آن تشخیص False Positive نامیده می شود.

مرجع

Book: Security Monitoring with Cisco Security MARS
<http://www.cisco.com/en/US/products/ps6241/index.html>

مختلف به یک سرور syslog دارد. پیام های syslog به صورت متن ساده (Simple text) بوده و بدون استفاده از نرم افزار خاصی قابل خواندن هستند. فایروالها، روترها و سرورهای یونیکس نمونه ای از سیستم هایی هستند که عموماً از این پروتکل استفاده می کنند. Syslog از پورت UDP 514 برای ارتباط استفاده می کند که به علت Connectionless بودن این پورت، پیامها با سرعت بالایی رد و بدل می شوند. لازم به ذکر است که بعضی از سیستمها به دلیل تضمین دریافت بسته، از TCP برای انتقال Syslog استفاده می کنند.

۳- SNMP (Simple Network Management): این پروتکل به عنوان استاندارد برای ارتباط مدیریتی شبکه ایجاد شده است. SNMP از پروتکل UDP برای برقراری ارتباط استفاده می کند. این پروتکل از طریق پورت ۱۶۲ UDPها را دریافت می کند. Trapهای SNMP به صورت رمزی هستند و معمولاً خواندن آنها بدون نرم افزارهای خاص و بدون کمک MIB (Management Information Base) غیرممکن است. MIB مجموعه ای از اطلاعات است که به صورت سلسه مراتبی سازماندهی شده و یک قالب عمومی را برای سرور به منظور ارتباط با تجهیزات فراهم می کند. درون MIB, Objectهایی هستند که مشخصه های خاصی را برای یک دستگاه خاص نمایش می دهند. سویچها، روترها و نرم افزارهای امنیتی کاربر انتهایی شبکه نمونه هایی هستند که از SNMP استفاده می کنند.

۴- SDEE (Security Device Event Exchange): این پروتکل تقریباً یک استاندارد باز است بدین معنی که می توان از این استاندارد استفاده کرد، ولی در نهایت این استاندارد به ICSA تعلق دارد. SDEE توسط بسیاری از Vendorهای تجهیزات IDS/IPS از قبیل Cisco, ISS, Sourcefire و TruSecure مورد استفاده قرار می گیرد. این پروتکل از XML برای سازماندهی کردن قالب پیامها یا رخدادها استفاده می کند. انگیزه اصلی ایجاد SDEE استانداردسازی قالب رخدادها و هشدارها در میان سازنده های مختلف IDS/IPS بوده است. همان طور که گفته شد چارچوب SDEE براساس XML بوده و از HTTP به همراه SSL/TLS به منظور Encryption و Secure Authentication همراه با پسورد و Certificate برای انتقال استفاده می کند. این پروتکل از TCP جهت انتقال استفاده می کند. SDEE برای جمع آوری Logها از متد Pull استفاده می کند به این معنی که سیستم مانیتورینگ log مربوط



بهداشت حرفه‌ای در کار با رایانه

برخی از مشکلات و عوارض ناشی از کار با رایانه عبارتند از:

مشکلات بینایی

مشکلات بینایی یکی از شایع‌ترین مشکلاتی است که در اثر کار زیاد با رایانه ایجاد می‌شود؛ مانند درد سرخی و سوزش چشم و آبریزش آن، دوبینی، احساس تاری دید که به کاهش قدرت بینایی، خستگی و درد چشم و سردرد منجر می‌شود. چشم‌های انسان عادت دارند تا بسیار راحت بر روی اشیای دور و نزدیک متمرکز شوند؛ به همین دلیل احتمال خستگی ماهیچه چشمی که بر روی کاغذ و صفحه مانیتور متمرکز شده وجود دارد. همچنین ماهیچه‌های دیگر چشم، از تغییرات نور یا درخشندگی یا از تغییر مسیر دید بین صفحه مانیتور و نوشته‌های در حال تایپ خسته می‌شوند و به دلیل جایجایی زیاد کلمات، چشم قدرت تطابق خود را به مرور از دست می‌دهد. افرادی که دارای اختلالات انکساری اصلاح نشده هستند بیشتر در معرض خطر هستند.

عوارض مفصلی و عضلانی

یکی دیگر از شایع‌ترین عوارض کار با رایانه،

دردهای عضلانی و درد مچ دست و بازو است. درد گردن و کمر و درازمدت، خمیدگی پشت، از عوارض دیگر کار زیاد و طولانی با رایانه است.

معمولاً کاربران رایانه، ساعدها، دست‌ها، بازوان، پشت و گردن خود را در یک حالت ثابت قرار می‌دهند و این عمل باعث وارد شدن فشار زیاد، در زمان طولانی، بر روی ماهیچه‌ها و تاندون‌های فرد می‌شود و در نهایت می‌تواند به مشکلات عضلانی و مفصلی نیز منجر شود. در این رابطه، فاکتورهای ارگونومیکی نظیر بارکاری، حرکت تکراری، طرز نشستن، زاویه دید، وضعیت میز و صندلی، ارتفاع صفحه کلید و مانیتور، وضعیت نوری، سرعت تایپ، عدم آرامش روانی و ... می‌تواند از فاکتورهای عمده خطر باشد.

مشکلات زایمانی و بارداری

برخی پژوهشگران، بر این باورند که زایمان‌ها و بارداری‌های غیرعادی و تولد نارس و ناقص، به استفاده از صفحه نمایش رایانه و وجود تشعشعات آن مربوط است. انسیتو بهداشت شغلی فنلاند، امکان ارتباط بین اشعه ناشی از رایانه و سقط جنین

را مورد مطالعه قرار داده است. در این مطالعات مشخص شد که سقط جنین در زنانی که در معرض میدان‌های مغناطیسی حاصل از رایانه با قدرت بیش از ۰/۹ میکروتسلا (واحد اندازه‌گیری شدت میدان مغناطیسی) قرار دارند شایع‌تر است. (بنابراین تولیدکنندگان و واردکنندگان رایانه باید این موضوع را جدی گرفته و استانداردهای قانونی را رعایت کنند.) همچنین استرس‌ها و فشارهای کاری در امور رایانه‌ای و وضعیت مناسب بدنی در هنگام کار نیز از جمله عوامل ایجاد کننده این عوارض هستند.

مشکلات پوستی

ولتاژ زیاد لامپ تصویر باعث تولید میدان الکترواستاتیک و بارهای الکتریکی مثبت در سطح خارجی صفحه نمایش می‌شود. در میدان بین بارهای مثبت و صورت اپراتور، گرد و خاک و ذرات در تمامی جهات حرکت می‌کنند. اگر چه میزان گرد و خاک و ذرات بسته به نوع تهویه اتاق، کفپوش و عوامل دیگر تغییر می‌کند، همیشه وجود دارند. جریان بارهای مثبت حاصل در این میدان،

ممکن است در کسانی که حساسیت پوستی دارند باعث خشک شدن پوست دست و صورت و ترک خوردن آن شود.

همچنین بررسی‌هایی صورت گرفته که نشان می‌دهد افرادی که از حساسیت‌های پوستی شکایت دارند و هنگام کار بیشتر تحت فشارهای فکری و عصبی قرار می‌گیرند، این فشارها و استرس‌ها می‌تواند باعث تغییرات هورمونی مانند تیروکسین (هورمون غده تیروئید) و پرولاکتین (هورمون هیپوفیز قدامی) و همچنین ضایعات پوستی شود.

در یک مطالعه دیگر نیز که در سوئد صورت گرفته است ارتباط بین ضایعات پوست صورت و کار با رایانه را به فاکتورهای روانی اجتماعی و مسایل محیط کار نسبت داده‌اند. البته فاکتورهای شخصی هم در بروز این ضایعات دخالت دارند.

استرس و مشکلات عصبی - روانی

حجم کار زیاد و دوری از همکاران در محیط کار می‌تواند منجر به بروز مشکلات روانی شود. البته لازم به ذکر است که کار با کامپیوتر افسردگی را نیست بلکه حجم زیاد کار است که در ایجاد استرس روانی نقش دارد.

تنفس گازهای مضر

بدنه رایانه و نمایشگرها بر اثر گرم شدن، بوی مخصوصی از خود متصاعد می‌کنند. از جمله این بوها گاز دیوکسین است که توسط بدنه رایانه (بر اثر حرارت) و صفحه نمایشگر تولید می‌شود. این مواد به عنوان مواد ضد حریق در بدنه نمایشگر و بردهای رایانه به کار می‌روند. همچنین گاز ازن به هنگام کار چاپگر لیزری تولید می‌شود که به بافت مخاطی بینی، چشم و گلو آسیب می‌رساند. بنابراین، رعایت استانداردهای مربوط در این خصوص توسط وارد کنندگان یا تولید کنندگان رایانه ضروری است.

راه‌های پیشگیری از عوارض و بیماری‌های ناشی از کار با رایانه

باید اذعان داشت که کار با رایانه کسی را بیمار نکرده و عوارضی را به وجود نمی‌آورد، بلکه رفتارهای غلط و ناصحیح و غیراصولی، درجه تأثیرپذیری منفی را در کار با رایانه بالا برده و شخص را دچار عوارض مختلف می‌کند. رعایت اصول بهداشت کار، شرط درست و صحیح کار کردن با رایانه است که در زیر به برخی از این اصول اشاره می‌شود:

کارکنانی که با رایانه کار می‌کنند، در زمان استخدام و شروع به کار و سپس به طور سالیانه (در قالب معاینات دوره‌ای) باید توسط متخصصان چشم یا بینایی‌سنجی مورد معاینه و آزمایش‌های لازم قرار گیرند و به توصیه‌های پزشک، توجه جدی شود.

در معاینات قبل از استخدام و دوره‌ای، به عوارض

و بیماری‌های مفصلی و عضلانی توجه شود و کارکنانی که به دردهای مفصلی، کمردرد، شانه و ... مبتلا شده اند به سرعت به پزشک طب کار یا سایر متخصصان مراجعه کنند. در دوران بارداری، زنان از کار با رایانه معاف شوند. محدودیت کار با رایانه در نظر گرفته شود و توأم با استراحت‌های کوتاه مدت در بین کار باشد. توصیه می‌شود برای هر یک ساعت کار مداوم، ۱۵ دقیقه استراحت در نظر گرفته شود. در هنگام استراحت بین کار بایستید، قدم بزنید و فکر خود را به موضوعات دیگر متمرکز کنید. ماهیچه‌های خود را شل و سپس آنها را بکشید و وضعیت آنها را تغییر دهید. نرمش در هنگام استراحت و بین کار سودمند است. (برای رفع خستگی می‌توان از حرکات کششی استفاده نمود). برای کاهش خستگی چشم باید هر چند مدت یک بار به نقطه‌ای در فواصل دور نگاه کنید. در هنگام کار با رایانه اگر بدن کشیده باشد و سر بالا نگاه داشته شود و شانه‌ها آویزان باشد بالا تنه در راحت‌ترین حالت قرار خواهد گرفت، چرا که بدن نشستن انجام کار را سخت تر کرده و منجر به خستگی ماهیچه‌ها و ایجاد عوارض می‌شود.

روشنایی محل کار باید مخلوطی از نور سفید و زرد بوده (ترجیحاً از لامپ مهتابی استفاده شود) و شدت آن در حدود ۳۰۰ لوکس باشد. میز کار طوری قرار گیرد که روشنایی لامپ‌های سقف در طرفین قرار گیرد و از قرار دادن میز در محلی که نور لامپ مستقیماً در برابر کاربر باشد خودداری شود. در استفاده از روشنایی طبیعی نیز نباید صفحه مانیتور در برابر پنجره قرار گیرد. برای به حداقل رساندن فشار بر روی گردن و کمر، استفاده از گیره‌های اوراق یا کاغذ گیر لازم است.

وقتی با رایانه کار ندارید چاپگر آن را خاموش کنید و یا آن را خارج از محیط کار قرار دهید. برای هوای اتاق کار، دمای ۲۳-۱۹ درجه سانتی‌گراد و رطوبت حدود ۵۰ درصد مناسب است. به منظور رفع آثار مخرب و سوء کارهای تولید شده از رایانه و ضمایم آن، بهتر است با باز کردن درب و پنجره‌ها و یا تعبیه دستگاه تهویه، هوای اتاق به طور مرتب تعویض شود. صندلی و میز مورد استفاده در حفظ سلامت و فرم عضلات و اسکلت بدن نقش بسیار مهمی دارند، بنابراین، باید اصول ارگونومیک در انتخاب آنها رعایت شود. در ادامه به مواردی از آنها اشاره می‌شود:

ارتفاع صندلی باید قابل تنظیم باشد. ارتفاع ۴۰/۶ تا ۵۲ سانتی‌متر برای صندلی‌های فشرده یعنی قرار گرفته در زیر باری معادل ۴۵/۴ کیلوگرم توصیه می‌شود. ارتفاع صندلی طوری تنظیم شود که مانع وارد شدن فشار اضافی بر ناحیه زیر ران‌ها شود یعنی ارتفاع صندلی از فاصله کف اتاق تا ناحیه زیر ران‌ها در حالتی که شخص نشسته است کمتر باشد. طول تشک

صندلی ۳۸ تا ۴۳ سانتی‌متر و عرض آن ۴۵ سانتی‌متر باشد. برای افراد چاق صندلی‌های پهن تر توصیه می‌شود.

ضخامت تشک در حدود ۴ تا ۵ سانتی‌متر باشد و رویه آن از جنسی باشد که اصطلاحاً بتواند تنفس کند و لبه جلو صندلی، گرد و لبه بیرونی آن، نرم باشد.

زاویه پشتی با تشک صندلی، حداقل ۹۰ تا ۱۰۵ درجه باشد. برای کاهش فشار وارده بر دیسک‌ها زاویه تا ۱۲۰ درجه ترجیح دارد. عرض پشتی صندلی هم باید حداقل ۳۰/۵ سانتی‌متر در ناحیه کمر باشد. بعضی از صاحب نظران، ارتفاع پشتی صندلی را حداقل ۵۰ سانتی‌متر توصیه می‌کنند. به هر حال، پشتی صندلی باید طوری تنظیم شود تا از مهره‌های کمری محافظت کند.

برای تکیه گاه کمر، استاندارد ANSI تکیه گاهی را توصیه می‌کند که ۲۲/۹-۱۵/۲ ارتفاع و ۳۰/۵ سانتی‌متر عرض داشته باشد و به فاصله ۱۵/۲ تا ۲۵/۴ سانتی‌متر از نقطه مرجع صندلی قرار گیرد. تکیه گاه کمر باید در حدود ۵ سانتی‌متر نسبت به پشتی صندلی برجستگی داشته باشد. صندلی‌های مورد استفاده در کار با رایانه بهتر است دسته دار بوده و دسته آن با ارتفاع میز کار مطابقت داشته باشد. همچنین دارای ۵ چرخ بوده و چرخان باشد. شیب کف صندلی ۵ تا ۱۵ درجه برای تمایل به جلو و ۵ درجه تمایل به عقب را امکان پذیر سازد. در صورت نیاز استفاده از زیرپایی توصیه می‌شود. بهترین وضعیت برای تغییر حالت پا استفاده از تکیه گاه است. میز کار نیز باید قابل تنظیم باشد و سطح کار باید در تراز قرار گیرد که ارتفاع کار کردن را با ارتفاع آرنج هم تراز کند. سطح صفحه کلید، هم ارتفاع با دسته صندلی و آرنج باشد و مچ‌ها به طور عادی روی صفحه کلیدها قرار گیرد، به طوری که هنگام کار، ساعدها تقریباً موازی با افق قرار گرفته و زاویه بین میز دست و ساعد، ۵ تا ۱۰ درجه باشد.

در برخی از بررسی‌ها (ارتفاع سطح کار را حدود ۵۸ تا ۷۱ سانتی‌متر توصیه می‌کنند) موقعیت mouse در همان ارتفاع و فاصله نسبت به صفحه کلید است.

صفحه مانیتور نیز باید طوری تنظیم شود که بالاترین سطح آن در امتداد دید چشم‌ها قرار گیرد و زاویه صفحه آن نسبت به خط فرضی عمود بر میز، ۱۰ تا ۲۰ درجه در نظر گرفته شود. فاصله مناسب بین چشم و صفحه نمایش ۶۰-۵۰ سانتی‌متر است.

بهترین رنگ برای صفحه مانیتور سبز تیره رنگ کهربایی است. سفید بر روی سیاه نیز تباین خوبی دارد، اما ممکن است انعکاس درخشندگی را افزایش دهد ولی سیاه بر روی سفید درخشندگی را کاهش می‌دهد.



سیسکو را آسان بیاموزید

دوره های تخصصی سیسکو و سیستم عامل

- > CCNA, CCDA
- > CCNP, CCDP
- > Routing & Switching, CCLE Security
- > Cisco Works Management Course
- > CCSP
- > CCVP

دوره های تخصصی امنیت شبکه و اطلاعات

- > CISSP
- > ISO 27001 (BS 7799) Introduction, Implementing & Lead Auditor
- > CEH (Certified Ethical Hacker)
- > Application Security. NET



Jump to
CISCO
right now!



مرکز آموزش های پیشرفته رمیس

دارای لابراتوار مجهز تجهیزات شبکه
برگزاری دوره ها مطابق با آخرین سیلابس رسمی سیسکو
امکانات کمک آموزشی شامل فیلم، اسلاید، انواع تست و آزمون های معتبر

تهران، خیابان زرتشت غربی، بین خیابان جویبار و ولی عصر، شماره ۱۴، طبقه اول

تلفن: ۵۰-۸۸۹۱۹۳۴۹ فکس: ۸۸۹۱۹۵۳۸

training@remisco.com

www.remisco.com

REMISCO

Information Technology

● مشاوره، طراحی و پیاده سازی

مراکز داده (Data Center) ، مراکز عملیات امنیت (SOC)
مراکز عملیات شبکه (NOC) ، راهکارهای مجازی سازی (Virtualization)
راهکارهای بهینه سازی شبکه های WAN ، راهکارهای ذخیره سازی (Storage)

● ارائه سرور و تجهیزات شبکه

● نگهداری ، تعمیر و پشتیبانی

● آموزش و آگاهی رسانی

تهران، خیابان ولی عصر، خیابان مطهری، خیابان سرداران، شماره ۲۸

تلفن: ۸۸۹۲۵۸۰۸ فکس: ۸۸۹۳۶۰۶۸

www.remisco.com info@remisco.com