رمیس

نشریه داخلی شرکت رمیس
پاییز ۱۳۸۹ . شماره ۵

رمیس مرکز کنترل و عملیات امنیت یک بانک خصوصی را راه‌اندازی می‌کند

آشنایی با پروژه‌های جدید شرکت رمیس

NOC بانک ملی، دیتا سنتر رشد، بیمه ایران، دانشگاه آزاد دزفول و ...

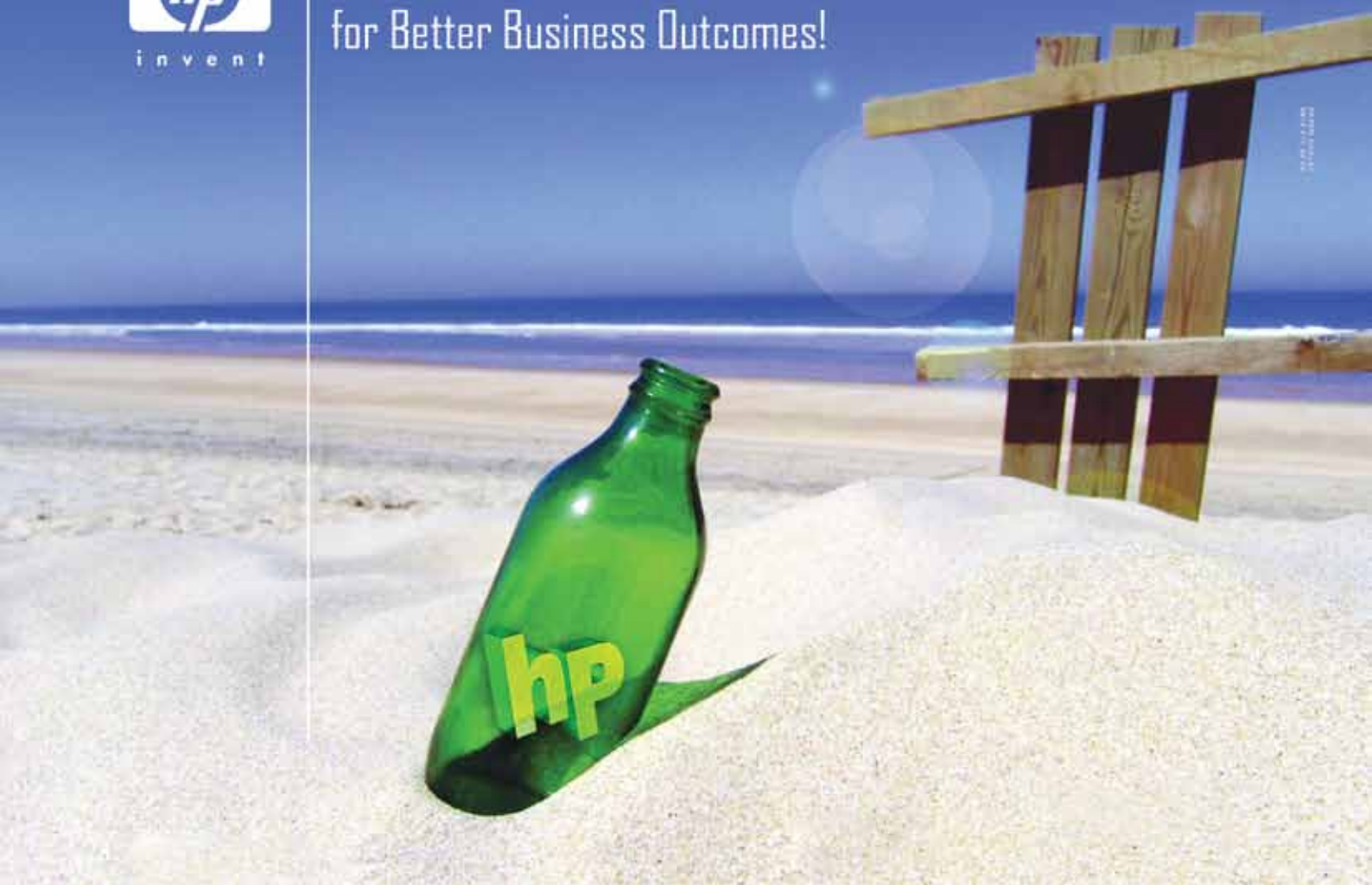
REMIS
رمیس

- مشاوره و فروش انواع سرورهای HP Proliant با گارانتی تعویض
- ارائه راه حل های جامع شامل:
- (SAN) Storage Area Network
- (NAS) Network Attached Storage
- ارائه راه حل های آرشیو خودکار اطلاعات (Backup Solution)
- ارائه، نصب و راه اندازی تجهیزات دیتا سنتر (EVA, MSA)
- مشاوره و اجرای راه حل های Load Balancing, Clustering
- برگزاری دوره های تخصصی HP

تهران، خیابان ولی عصر، خیابان مطهری، خیابان سربداران، شماره ۲۸
تلفن: ۸۸۹۲۵۸۰۸ فکس: ۸۸۹۳۶۰۶۸
info@remisco.com
www.remisco.com

hp
invent

Technology
for Better Business Outcomes!



رمیس

نشریه داخلی شرکت افزار پرداز رمیس. پاییز ۱۳۸۹. شماره ۵

R E M I S

صاحب امتیاز:
شرکت افزارپرداز رمیس
مدیرمسؤول:
امیرعباس تقی‌پور
سردبیر:
امیر لعلی
تحریریه:
ساره جعفرقلی، اویس طوفانی
عکس:
علی جورابچی، امیر امیری
نشانی:
تهران، خیابان مطهری، خیابان سربداران، پلاک ۲۸
تلفن:
۸۸۹۲۵۸۰۸
دورنگار:
۸۸۹۳۶۰۶۸
نشریه داخلی
شرکت افزارپرداز رمیس
از خوانندگان وعلاقمندان دعوت می‌شود در صورت تمایل، مطالب خود را برای چاپ در نشـــریه به پست الکترونیک info@remisco.com ارسال نمایند.

فهرست

سرمقاله

کاهش هزینه‌ها با حفظ مشتری

رضایت مشتری بی‌شک یکی از موضوعات بسیار راهبردی در شرکت‌هاست. مشتریان بقای شرکت را رقم می‌زنند و به همین دلیل شرکت‌ها نمی‌توانند به انتظار و خواسته‌های مشتریان بی‌تفاوت باشند، آنها باید همه فعالیت‌ها و توانمندی‌های خود را متوجه رضایت مشتری کنند، زیرا تنها منبع برگشت سرمایه، مشتریان هستند. بنابراین نخستین اصل در دنیای کسب‌وکار امروزی ایجاد ارزش‌های مشتری‌پسند است. در این میان اطلاع از تصویر ذهنی و ادراک مشتریان نسبت به خدمات ارائه شده از اهمیت خاصی برخوردار است و ضمن برملا ساختن نقاط قوت و ضعف شرکت، زمینه‌ای را برای اتخاذ راهبردهای مناسب و ارتقای سطح عملکرد فراهم می‌آورد. از این رو باید پیوسته در جست‌وجوی علت‌ها بود تا عوامل مثبت تقویت و جنبه‌های منفی برطرف شوند، ضمن اینکه توجه به این نکته ضروری است که هر شرکتی باید در گسترش برنامه‌های ارزشیابی خود پیشتاز و نوآور بوده و برنامه‌ها و استراتژی‌ها را برمبنای نیازهای سازمانی و مشتریان خود استوار کند. تنها در این صورت است که نتایج بررسی‌ها برای مدیریت مفید خواهد بود و منجر به پیشرفت‌های آینده می‌شود. در دنیای رقابتی امروز، همه می‌دانند حفظ مشتری‌های موجود نسبت به جذب مشتری‌های جدید هزینه کمتری دارد. مردم متوجه موفقیت و سودآوری در شرکت‌های مشتری محور شده‌اند و آن را تحسین می‌کنند. آنها توانسته‌اند بدون داشتن کمترین هزینه یا صرف مبالغ زیاد در تبلیغات، رضایت مشتری‌ها را به‌خوبی جلب کرده و موجب تداوم کسب و کارشان شوند. در نتیجه ارتباط شدیدی بین رضایت مشتری، حفظ مشتری و سوددهی وجود دارد. بر همین مبنا، رضایت مشتری هدف عملیاتی خیلی از سازمان‌ها شده است. آنها در جاهایی که بهبود عملکرد تأثیر زیادی بر رضایت مشتری دارد (نظیر کیفیت ارائه خدمات به مشتری) سرمایه‌گذاری زیادی کرده‌اند. شرکت‌ها برای نزدیکی بیشتر با مشتری‌هایشان، در پایگاه داده‌های بازاریابی، مدیریت روابط و برنامه‌ریزی مشتری سرمایه‌گذاری می‌کنند. سازمان‌ها در بخش عمومی، منشور مشتری‌مداری را برای نمایش دادن تعهد خود نسبت به خدمت به مشتری به کار گرفته‌اند و بیانیه مأموریت آنها شامل جلب رضایت و افزایش خشنودی مشتری‌ها شده است. بر اساس گزارش بیزینس مانیتور، به طور متوسط شرکت‌ها سالانه حدود ۱۰ تا ۳۰ درصد از مشتری‌هایشان را از دست می‌دهند، اما اغلب نمی‌دانند چه مشتری هایی را در چه زمان و به چه دلیل از دست داده‌اند. اغلب شرکت‌ها بدون نگرانی از مشتری‌هایی که از دست می‌دهند، به طور سنتی تأکید زیادی بر جذب مشتری‌های جدید دارند. چنین شرکت‌هایی مانند سطلی ته سوراخ هستند که مشتری‌های خود را همچون آب از دست می‌دهند و مدیران شرکت به‌جای مسدودکردن سوراخ، در جست‌وجوی منابع جدیدی برای جذب هرچه بیشتر مشتری‌ها هستند. توجه به این موضوع ضروری است که فرایند جذب مشتری بیشتر زمانی اثربخش خواهد بود که ضعف سازمان و مؤسسه در وفادار نگهداشتن مشتریان برطرف شود. یعنی به دلیل محدود بودن بازارها (حتی در مقیاس جهانی) و تعدد رقبا در عرصه تجارت، حفظ مشتریان موجود، پایه‌ای قابل اتکا برای درامدهای آتی است اما اینکه چرا گاهی شرکت‌ها مشتریان خود را از دست می‌دهند، موضوع دیگری است که در شماره بعد به آن خواهیم پرداخت.

■ **امیر عباس تقی پور**

مدیر امور مشتریان واحد ICT رمیس معتقد است این شرکت به دلایل متعددی از جمله به‌روز بودن، در حوزه‌های دانش ICT استفاده از نیروهای تخصصی، ایجاد اعتماد در مشتری و... جایگاه مطلوبی در بین شرکت‌های فعال در حوزه IT کشور دارد. با مهندس شفیعی در مورد برنامه‌های واحد ICT شرکت رمیس گفت‌وگویی انجام داده‌ایم که می‌خوانید.

گفت‌وگو با مدیر امور مشتریان واحد ICT رمیس

جایگاه مناسب رمیس در بازار رقابتی IT

رمیس شما به عنوان مدیر امور مشتریان واحد ICT رمیس، وضعیت شرکت را در مقایسه با رقبای دیگر چگونه ارزیابی می‌کنید؟

ملاک رسمی در مقایسه شرکت‌ها، ارزیابی و رتبه‌بندی شورای عالی انفورماتیک است که خوشبختانه شرکت رمیس دارای رتبه بسیار خوبی در این ارزیابی است.

اما مسأله مهم، شناخت مشتریان بالقوه و بالفعل شرکت است. موارد بسیاری مشاهده می‌شود که مشتریان مستقیماً با توجه شناختی که نسبت به شرکت دارند، با شیوه‌های مختلف (استعلام کتبی یا تلفنی، درخواست جلسه و...) با ما ارتباط برقرار کرده و نیازهای خودشان را مطرح می‌کنند. در کل، شرکت را در مقایسه با سایرین در جایگاه مناسبی می‌بینم ولی به دلیل وجود رقابت تنگاتنگ در این صنعت، این امر باعث نمی‌شود به صورت مستمر جهت ارتقاء این جایگاه تلاش نکنیم.

رمیس چه توانمندی‌های ویژه‌ای در شرکت رمیس وجود دارد که می‌تواند به جذب مشتریان بیشتر بیانجامد؟

وجود توانمندی‌های بسیار زیاد در شرکت رمیس باعث تحکیم روابط کاری با مشتریان فعلی و جذب مشتریان جدید می‌شود که از جمله این عوامل می‌توان به شناخت نیازهای مشتریان و عرضه محصولات و خدمات جدید اشاره کرد. درک دقیق از شرایط موجود بازار IT، استفاده از نیروهای انسانی متخصص، به‌روزرسانی دانش فنی کارشناسان، مدیریت روزآمد، استفاده از ابزارهای مدرن مدیریتی مانند ERP و CRM، بهره‌گیری از همکاری شرکت‌های تراز اول خارجی، سنجش مستمر رضایت مشتریان، توجه به منابع انسانی موجود، دقت نظر در جذب کارشناسان و کارکنان جدید و... نیز از دیگر عوامل افزایش کیفیت خدمات و در نتیجه عوامل تأثیرگذار در جذب مشتریان هستند.

رمیس راهکارهای بازاریابی شرکت برای جذب مشتریان جدید چیست؟

شرکت همواره تلاش کرده است از روش‌های علمی و شناخته شده بازاریابی جهت تثبیت و افزایش سهم بازار استفاده مفید کند که از جمله آنها می‌توان از برگزاری سمینارهای تخصصی، معرفی مستمر محصولات و خدمات در ارتباط رو در رو با مشتریان و همچنین از طریق وب‌سایت شرکت، درج آگهی در نشریات تخصصی پر تیراژ، درج مشخصات شرکت در پایگاه‌های اطلاعاتی، تهیه و به‌روزرسانی پروفایل و رزومه شرکت و ارسال آن برای مشتریان و بالاخره انتشار نشریه رمیس نام برد. با تمام اینها شرکت همواره بهترین مبلغین خود را مشتریان فعلی خود می‌داند؛ مشتریانی که از مهم‌ترین سرمایه‌های شرکت به حساب می‌آیند و با پشتیبانی‌های خود نقش تعیین‌کننده‌ای را در پیشبرد اهداف شرکت به عهده داشته‌اند.

رمیس چه راهکارهایی در شرکت برای حفظ مشتریان فعلی مدنظر قرار گرفته است؟

به نظر من بهترین شیوه حفظ مشتریان موجود، ایجاد و تقویت حس اعتماد در آنها است.

رمیس با چه روش‌هایی؟

در موارد بسیاری مشاهده شده است که مشتریان در صورت حصول اطمینان از توانایی شرکت و همچنین کیفیت کالا و خدماتی که در اختیارشان قرار داده می‌شود، حتی حاضر به هزینه کردن مبالغ بیشتری هم هستند و به‌طور خلاصه ترجیح می‌دهند «کار را به کاردان بسپارند».

نکته بعدی اینکه شرکت به موازات توسعه طولی (کمی) هیچ‌گاه از توسعه عرضی (کیفی) نیز غافل نبوده است، به این معنا که گستردگی فعالیت‌ها و افزایش مشتریان به هیچ عنوان موجب غفلت مدیریت از تقویت زیرساخت‌ها یا کم‌توجهی به مشتریان موجود و حتی کارکنان خود نگشته است. به این معنا که شرکت مصالح خود، مشتریان و کارکنان را جدا از هم ندیده و به عبارت دیگر تمرکز فعالیت‌های خود را در فصل مشترک منافع مشتریان، منافع کارکنان و منافع شرکت قرار داده است.

رمیس لطفاً وظایف واحد ICT و برنامه‌های آتی این واحد را تشریح کنید.

واحد ICT یا فن‌آوری‌های پیشرفته با ساختار جدید خود فعالیتش را از دی‌ماه سال قبل آغاز کرده است. بر این اساس، این واحد علاوه بر مسؤولیت‌های قبلی خود که به‌طور عمده ارائه پشتیبانی فنی به بخش‌های مختلف شرکت بود، اکنون وظیفه برقراری ارتباط مستقیم با مشتریان را به منظور مشاوره و ارائه راهکارهای مورد نیازشان در زمینه‌های تعریف شده، در قالب شرکت در مناقصات، پاسخ به استعلام‌ها و... بر عهده دارد. مهم‌ترین این زمینه‌ها شامل مشاوره، طراحی و راه‌اندازی مراکز داده، طراحی و راه‌اندازی شبکه‌های بزرگ دیتا، مشاوره و پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات (ISMS)، اجرای عملیات تست نفوذپذیری (Penetration Test) و ارائه گواهینامه بین‌المللی در این زمینه، مشاوره و برقراری سیستم‌های امنیت شبکه، پیاده‌سازی Network Operations Center (NOC) و پیاده‌سازی Security Operations Center می‌شود. این واحد که در حال حاضر به صورت Strategic Business Unit (SBU) اداره می‌شود، تاکنون توانسته است با اتکا به دانش فنی متخصصین ایرانی و بهره‌گیری از تجارب و تخصص شرکای تجاری خارجی خود خدمات بسزایی را به جامعه انفورماتیک کشور ارائه کند. برنامه‌های آتی این واحد طبعاً تمرکز بیشتر و افزایش سهم بازار در زمینه‌های ذکر شده، در عین حفظ و ارتقاء رضایت مشتریان و همچنین ارائه محصولات و خدمات جدید بر اساس نیازهای فعلی و آتی مشتریان است. تدوین فرآیندهای عملیاتی نیز از برنامه‌های در دست اجرای این واحد است. از جمله برنامه‌های سال جاری با توجه به نیاز مبرم کشور، ارائه سرویس WAN Optimization است که با بهره‌گیری از جدیدترین فناوری روز دنیا در اختیار سازمان‌ها و ارگان‌ها قرار خواهد گرفت. برای معرفی هرچه بیشتر این سرویس به بازار انفورماتیک کشور، برنامه‌های گسترده‌ای در نظر گرفته شده است که از آن جمله می‌توان به برگزاری سمینارهای در این خصوص در پاییز امسال اشاره کرد.

از سوی قائم‌مقام مدیرعامل صورت گرفت

تشریح پروژه‌های جدید شرکت رمیس

قائم‌مقام مدیرعامل شرکت رمیس پروژه‌های جدید شرکت را تشریح کرد.

مهندس مازیار نوربخش اظهار داشت: در حال حاضر هم قراردادهای جدیدی با سازمان‌های مختلف منعقد کرده و هم بسیاری از قردادهای قبلی خود را به دلیل رضایت مشتریان از عملکرد رمیس تمدید کرده‌ایم، به عنوان مثال قرارداد تعمیر و نگهداری و پشتیبانی شعب بانک تجارت برای یکسال دیگر نیز تمدید شد که در قرارداد جدید، پشتیبانی از سایت‌های استان‌های یزد و آذربایجان شرقی و همچنین پشتیبانی از سایت ساختمان‌های مدیریت تدارکات و چیتگر بانک تجارت هم به تعهدات ما افزوده شد.

مدیر بخش تعمیر و نگهداری در ادامه به تشریح قراردادهای جدید رمیس پرداخت و گفت: پنج قرارداد جدید در این خصوص منعقد شده که پشتیبانی از سایت مرکزی و دیتاسنتر شرکت ساپکو و طراحی و پشتیبانی از شبکه و دیتاسنتر پژوهشگاه صنعت نفت از جمله آنهاست.

نوربخش افزود: ما قراردادهای جدیدی نیز با پزشکی قانونی و مؤسسه مطالعات بهره‌وری و نیروی انسانی منعقد کرده‌ایم که در این قراردادها متعهد به پشتیبانی از سخت‌افزار و شبکه این دو سازمان شده‌ایم. همچنین مشاوره و پشتیبانی شبکه وزارت ارتباطات و فن‌آوری اطلاعات از دیگر قراردادهای جدید شرکت است.

وی ادامه داد: بیشتر قراردادهای پشتیبانی از جمله پشتیبانی شرکت‌های راهداری و حمل‌ونقل جاده‌ای و صادرات گاز که شامل پشتیبانی سخت‌افزاری و نرم‌افزاری شبکه می‌شود نیز مجدداً تمدید شده است.

قراردادهای جدیدی نیز با پزشکی قانونی و مؤسسه مطالعات بهره‌وری و نیروی انسانی منعقد شده است که در این قراردادها متعهد به پشتیبانی از شبکه و دیتاسنتر این دو سازمان شده‌ایم. همچنین مشاوره و پشتیبانی از شبکه وزارت ارتباطات و فن‌آوری اطلاعات از دیگر قراردادهای جدید شرکت است

قائم‌مقام مدیرعامل شرکت رمیس گفت: در بخش آموزش، دوره جدید آموزش تجهیزات سرور HP از اواخر شهریورماه و اوایل ماه مهر سال جاری آغاز خواهد شد که این دوره چهارمین دوره آموزش‌های HP خواهد بود. تاکنون سه دوره از این آموزش‌ها برگزار شده است که در هر دوره به فراگیران مدرک حضور در دوره اعطا شد.

وی افزود: کارآموزان این دوره‌ها می‌توانند برای اخذ مدرک بین‌المللی در کشورهای دیگر اقدام کنند. همچنین در کنار این دوره، ۱۰ دوره آموزشی دیگر در زمینه‌های مختلف سیسکو، مایکروسافت و... نیز ارائه می‌شود.

قائم مقام مدیر عامل خاطر نشان کرد: بخش آموزش رمیس یک کسب و کار مستقل (Business Unit) بوده و در ساختمان خیابان زرتشت قرار دارد.

مهندس نوربخش تصریح کرد: در بخش ICT که مدیریت آن برعهده مهندس پورمند است نیز پروژه‌های بسیاری در دست اجرا داریم که از این موارد می‌توان به پروژه شبکه دیتاسنتر بیمه ایران اشاره کرد که این دو پروژه برای ما بسیار ارزشمند و مهم هستند. همین‌طور اجرای پروژه طراحی دیتاسنتر «رشد» نیز به ما سپرده شده که ما نیز درصدد اجرای آن به نحو احسن هستیم.

وی گفت: در بخش منابع انسانی، ما طرح آموزش پرسنل را به صورت OUT SOURCE آغاز کرده‌ایم که در این طرح در مرحله اول با پرسنل شرکت به ترتیب مصاحبه‌هایی انجام می‌شود و تمام مدارک تحصیلی و دوره‌هایی که سپری کردند، جمع‌آوری شده و مورد بررسی قرار می‌گیرد.

وی اظهار داشت: با این طرح مشخص می‌شود نیروهای ما چه دوره‌هایی را سپری کرده‌اند و به چه دوره‌هایی برای آموزش نیاز دارند. در حال حاضر اجرای این طرح آغاز شده و در صدد هستیم تا دو ماه دیگر این بررسی‌ها به پایان برسد تا بتوانیم پرونده پرسنل شرکت را ساماندهی کنیم.

قائم مقام مدیر عامل شرکت رمیس اظهار داشت: طرح دیگر ما در جهت نظام‌مندسازی بخش منابع انسانی شرکت، ساماندهی نظام جذب پرسنل است که براساس این طرح از این پس استخدام پرسنل و جذب نیروهای قراردادی با یک شیوه هدفمند و ساماندهی شده خواهد بود.

نوربخش در پایان گفت: هم‌اکنون شرکت به سمت پشتیبانی از دیتاسنتر بانک‌ها و شرکت‌ها حرکت کرده است که رقابت در آنها کمتر است و رمیس جزء معدود شرکت‌های کشور است که تخصص کاملی در این حوزه دارد. تیم فنی شرکت با گذراندن دوره‌های تخصصی و فشرده و همچنین انبار کردن تجهیزات و قطعات مورد نیاز موجب تجهیز شرکت به تخصص کامل در این بخش شده است. حرکت به سمت پشتیبانی از دیتاسنتر بانک‌ها نیز یک رویکرد جدید و مهم است که باب آن در شرکت باز شده است و می‌توانیم به راحتی برای سازمان‌های دیگر نیز این خدمت را ارائه کنیم.

گفت‌وگوی اختصاصی با مدیرعامل شرکت ارتباطات زیرساخت در مورد پروژه شبکه ملی IP

با همکاری رمیس چالش‌ها را برطرف کردیم

این شبکه باعث می‌شود هر اپراتور و مشتری بزرگی بتواند با ایجاد شبکه مجازی در بین نقاط مختلف کشور، شبکه خاص خود را ایجاد و هرگونه تبادل اطلاعات اعم از صوت، تصویر و حتی مولتی مدیا را برقرار کند

مدیرعامل شرکت ارتباطات زیرساخت در زمینه پروژه شبکه ملی IP اظهار داشت: این پروژه، یکی از بزرگ‌ترین پروژه‌هایی است که برای توسعه زیرساخت اطلاعاتی کشور اجرا می‌شود. این پروژه، شاهراه اطلاعاتی را فراهم می‌کند که می‌توان روی آن خدمات و سرویس‌های متعددی را تعریف کرد.

محمود خسروی در گفت‌وگو با خبرنگار رمیس خاطرنشان کرد: افزایش قابلیت‌ها و ظرفیت شبکه ملی IP با نگاه به شبکه‌های نسل جدید (NGN)، ارائه سرویس به شرکت‌های PAP، ایجاد VPN سازمان‌ها و شرکت‌ها در سطح کشور و همچنین ایجاد زیرساخت‌های پرظرفیت جهت ترانزیت ترافیک منطقه‌ای و بین‌المللی، از اهداف اجرای این پروژه است.

وی تصریح کرد: در این پروژه، شهرها و شهرک‌های صنعتی کشور تحت پوشش این شبکه قرار می‌گیرند و بستر مناسبی برای رسیدن ضریب نفوذ کاربران اینترنت به ۳۰ درصد و ضریب نفوذ اینترنت به ۴۲ درصد فراهم شده است.

وی افزود: توسعه و افزایش ظرفیت شبکه ملی دیتا برای حداقل یک میلیون و ۵۰۰ هزار پورت پرسرعت، مدیریت یکپارچه و متمرکز به منظور ارائه سرویس‌های با کیفیت مطلوب، مدیریت نگهداری و مدیریت مشتریان از مزایای اجرای این پروژه است.

مدیر عامل شرکت ارتباطات زیرساخت اظهار داشت: از دیگر مزایای این پروژه می‌توان به ارائه بستر مناسب برای توسعه کاربردهای الکترونیکی از قبیل دولت الکترونیکی، تجارت الکترونیکی و غیره با هدف نیل به گسترش فناوری اطلاعات و افزایش رضایتمندی ملی و عدالت اجتماعی اشاره کرد.

وی بیان داشت: در حال حاضر شبکه دیتای کشور با تجهیزات سیسکو مشغول به کار است و مناقصه شبکه ملی IP برای افزایش ظرفیت آن توسط شرکت ارتباطات زیرساخت برگزار شد.

وی افزود: نتیجه مناقصه اول (ارتقای شبکه دیتای کشور) اسفندماه ۸۷ مشخص شد که طبق آن شرکت افزارپرداز رمیس برنده مناقصه شد. خسروی تصریح کرد: هم‌اکنون نصب این تجهیزات به پایان رسیده است و افزایش ۲۵ درصدی پروژه به‌منظور توسعه و گسترش شبکه تعداد دیگری از استان‌های کشور در دستور کار قرار دارد. خسروی گفت: این مناقصه که پایه‌های آن در دولت قبل گذاشته شده بود و با پایان دوره دولت هشتم، برگزاری آن به دولت نهم به ارث رسید، تاکنون چندین بار از سوی متولیان مختلف آن که ابتدا شرکت فن‌آوری اطلاعات بود و بعد از آن به شرکت ارتباطات زیرساخت واگذار شد، تجدید و تمدید شد. خسروی گفت: وظیفه شبکه ملی IP، توزیع ترافیک دیتا در سطح کشور، ارتباط با اینترنت جهانی از طریق خطوط درگاه بین‌الملل، ترانزیت ترافیک بین‌الملل در راستای تبدیل ایران به هاب منطقه‌ای و پشتیبانی ترافیک صوتی و تصویری کاربران در قالب شبکه‌های یکپارچه نسل آینده خواهد بود.

وی ادامه داد: این شبکه باعث می‌شود هر اپراتور و مشتری بزرگی بتواند با ایجاد شبکه مجازی در بین نقاط مختلف کشور، شبکه خاص خود را ایجاد و هرگونه تبادل اطلاعات اعم از صوت، تصویر و حتی مولتی مدیا را برقرار کند. مدیر عامل شرکت ارتباطات زیرساخت تأکید کرد: بی‌اغراق همیشه پروژه‌های بزرگ در عرصه ارتباطات و فن‌آوری اطلاعات، حداقل در ایران چالش‌های فراوانی داشته‌اند ولی ما توانستیم با هم‌فکری مناسب با شرکت برنده مناقصه یعنی رمیس این چالش‌ها را از بین ببریم و هم‌اکنون اجرای این پروژه بسیار جلو رفته است.

گسترش قرارداد پروژه IP تکمیلی به دلیل رضایت شرکت ارتباطات زیرساخت

به دلیل اعلام رضایت شرکت ارتباطات زیرساخت از عملکرد شرکت رمیس، قرارداد پروژه IP تکمیلی گسترش پیدا کرد.

علیرضا صنعتی، معاون پروژه ارتقای شبکه ملی IP کشور در شرکت رمیس گفت: در پروژه IP تکمیلی مقرر شده است زیرساخت‌های اینترنتی مخابرات استان‌ها ارتقاء یابد که در آن روترهای ۷۵۰۰ به ۷۶۰۰ سیسکو ارتقاء پیدا می‌کنند.

وی گفت: در فاز اول پروژه IP تکمیلی وظیفه ارتقای تجهیزات مخابراتی در ۱۳ استان بر عهده رمیس قرار گرفت که با توجه به کیفیت انجام کار توسط رمیس و تجهیزات سیسکوی مستقر شده و پس از اعلام رضایت شرکت ارتباطات زیرساخت، ۱۰ استان دیگر نیز به این پروژه اضافه شد.

صنعتی اظهار داشت: در اجرای این پروژه همچنین رمیس مشاوره‌هایی نیز برای برطرف کردن مشکلات موجود در شبکه‌های مخابراتی استان‌ها ارائه داد و موجب شد تا اشکالات موجود شناسایی شده و درصدد رفع آنها برآیند.

وی تصریح کرد: در زمان بهبود سیستم‌ها به‌گونه‌ای عمل شد که کمترین اختلال و قطعی در شبکه رخ دهد که همین موضوع بسیار مورد توجه شرکت ارتباطات زیرساخت قرار گرفته است.

با برنده شدن در مناقصه؛

رمیس مرکز کنترل و عملیات امنیت یک بانک خصوصی را راه‌اندازی می‌کند

شرکت رمیس به‌عنوان یکی از شرکت‌های پیشرو در عرصه طراحی مراکز کنترل و عملیات امنیت، به همراه شریک تجاری خود (پالادیون) در مناقصه راه‌اندازی مرکز کنترل و عملیات امنیت (SOC) یک بانک خصوصی دیگر شرکت کرد که توانست رتبه اول فنی و قیمتی را در بین شرکت‌کنندگان در این مناقصه کسب کند.

مهندس پورمند، مدیر فناوری اطلاعات شرکت رمیس با بیان این مطلب اظهار داشت: این پروژه از شهریورماه سال جاری آغاز شده و مدت‌زمان اجرای آن سه ماه خواهد بود.

وی گفت: مرکز کنترل و عملیات امنیت، دیدی بلادرنگ و جامع نسبت به وضعیت امنیتی کسب و کار بانک ایجاد خواهد کرد و در واقع این مرکز به‌واسطه اطلاع‌رسانی‌های اتوماتیک حوادث و وقایع، تولید گزارشات جزئی و کلی و پاسخ‌دهی اتوماتیک به حوادث و وقایع، رویکردی پیشگیرانه را در جهت مدیریت ریسک‌های امنیتی ایجاد خواهد کرد.

وی ادامه داد: مرکز کنترل و عملیات امنیت تمامی جوانب مرتبط با امنیت بانک را به‌صورت آنی و از یک نقطه متمرکز مدیریت و مورد پایش قرار خواهد داد. این مرکز با شناسایی آنی حوادث و وقایع، بر اساس سطح ریسکی که هر یک از آنها ایجاد خواهند کرد، وقایع و حوادث را اولویت‌بندی کرده، دارایی‌های متأثر شده از وقایع اتفاق افتاده را مشخص کرده و راهکارهای اصلاحی یا پیشگیرانه را پیشنهاد داده یا مواردی از پیش تعیین‌شده را اجرا می‌کند.

مدیر فناوری اطلاعات شرکت رمیس افزود: این مرکز با ارائه گزارشاتی در سطوح مختلف، نیازمندی‌های مربوط به فرآیندهای ممیزی، مانیتورینگ بلادرنگ و همچنین ارزیابی بخشی از ریسک‌های عملیاتی بانک را اعلام می‌کند. همچنین اطلاعات امنیتی زیادی را از ابزارهای امنیتی مانند دیواره آتش، آنتی‌ویروس، سیستم‌های تشخیص نفوذ و انواع نرم‌افزارهای کاربردی و زیرساختی در سطح شبکه جمع‌آوری، سپس اطلاعات آن را نرمال‌سازی کرده و گزارشی بلادرنگ از آنچه در حال اتفاق است را فراهم می‌کند.

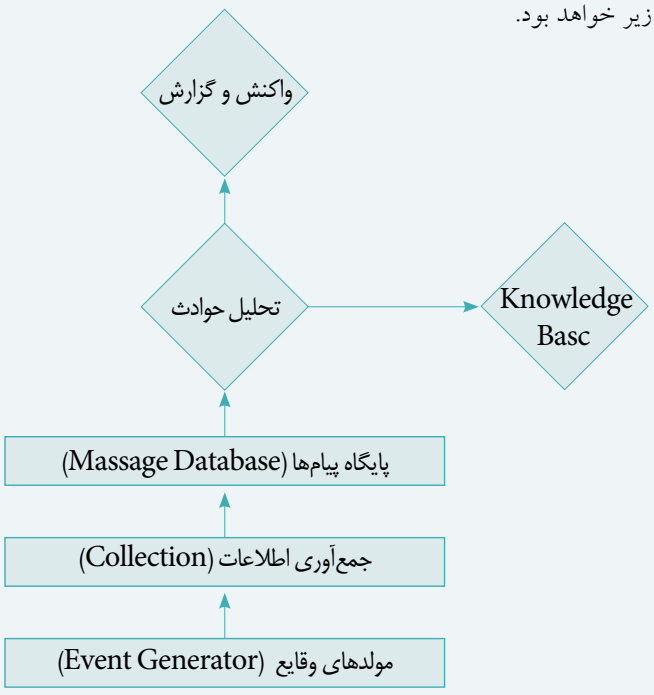
پورمند تصریح کرد: اجرای پروژه راه‌اندازی مرکز کنترل و عملیات امنیت (SOC) این بانک خصوصی در راستای ارائه بهتر سرویس‌های بانکی و احراز هویت امنیتی برتر در منطقه از سوی این بانک در زمینه فناوری اطلاعات و ارتباطات با ارائه خدمات نوین و ایمن در حوزه‌های گوناگون با استفاده از جدیدترین و مناسب‌ترین راهکارها جهت پیشگیری، شناسایی و برطرف کردن تهدیدها و آسیب‌پذیری‌ها در حداقل زمان ممکن با کمترین تلفات منابع اطلاعاتی و اختلال در سیستم‌هاست.

وی در تشریح اهداف کلان راه‌اندازی مرکز کنترل و عملیات امنیت (SOC) این بانک خصوصی گفت: از مهم‌ترین دستاوردهای مرکز کنترل و عملیات امنیت، تداوم و ارتقای امنیت در سیستم‌های اطلاعاتی بانک شامل نرم‌افزارهای کاربردی، تجهیزات امنیت فیزیکی، شبکه‌های ارتباطی، پایگاه‌های داده و سرویس‌های زیرساختی فناوری اطلاعات و... و ایجاد اطمینان در سرویس‌گیرندگان و افزایش اعتبار کاری و حرفه‌ای بانک خواهد بود.

وی ادامه داد: این مرکز با هدف ایجاد فضایی امن و سالم برای جلوگیری و مقابله با انواع تهدیدات خارجی به سیستم‌های اطلاعاتی بانک و همچنین تهدیدات درون شبکه با قابلیت مانیتورینگ، تشخیص و تحلیل رخدادهای امنیتی بر روی کلیه لینک‌های شبکه طراحی می‌شود. همچنین این مرکز به صورت ماژولار و با قابلیت توسعه متناسب با توسعه آتی سیستم‌های اطلاعاتی بانک در نظر گرفته خواهد شد.

مدیر فناوری اطلاعات شرکت رمیس گفت: مرکز کنترل و عملیات امنیت (SOC) دارای سایت پشتیبان (Back up) نیز خواهد بود.

پورمند اظهار داشت: مرکز عملیات امنیت شبکه از پنج ماژول شامل مولدهای وقایع، جمع‌آوری اطلاعات، پایگاه داده پیام، موتورهای تحلیل و مدیریت واکنش تشکیل می‌شود که ارتباط بین این ماژول‌ها مطابق نمودار زیر خواهد بود.



پروژه طراحی و ارتقای مرکز داده رشد* به شرکت رمیس واگذار شد

شرکت رمیس با برنده شدن در مناقصه پروژه طراحی و ارتقای مرکز داده رشد، اجرای این پروژه را آغاز کرد.

علی بیزمارک، مدیر پروژه طراحی و ارتقای مرکز داده رشد در شرکت رمیس با بیان این مطلب اظهار داشت: نظر به توافقنامه منعقد شده فی‌مابین شرکت فناوری اطلاعات ایران و وزارت آموزش و پرورش در راستای اجرای فاز اول پروژه تجهیز و اتصال یکصد هزار مدرسه به شبکه ملی اینترنت، مناقصه طراحی جامع مرکز داده رشد برگزار و شرکت افزارپرداز رمیس به عنوان مجری این طرح انتخاب شد.

وی در خصوص روند اجرای این پروژه گفت: پروژه یاد شده شامل فازهای تأمین تجهیزات مورد نیاز مرکز داده رشد جهت مرحله ارتقاء و نصب و راه‌اندازی تجهیزات مذکور در سازمان رشد و شناخت، تحلیل، ارزیابی، امکان‌سنجی و طراحی مرکز داده رشد جهت پوشش نیازهای آتی وزارت آموزش و پرورش در برنامه پنج ساله پنجم است.

بیزمارک تصریح کرد: در فاز اول این پروژه تجهیزاتی مانند Command View، EVA4400 و سرورهای HP DL Series توسط شرکت رمیس تأمین و در محل سازمان رشد نصب می‌شود. همچنین در این فاز طرح بهینه دیتاسنتر در حوزه‌های تجهیزات ذخیره‌سازی و شبکه اترنت توسط شرکت رمیس ارائه و اجرا می‌شود. وی ادامه داد: در فاز دوم پروژه که یکی از بزرگ‌ترین فعالیت‌های طراحی در زمینه IT در کشور محسوب می‌شود، طرح ایده‌آل دیتاسنتر رشد طی یک برنامه ۵ ساله تدوین و در اختیار سازمان رشد قرار می‌گیرد. این طرح شامل تهیه و تنظیم اسناد فنی تجهیزات سخت‌افزاری و نرم‌افزاری و معماری زیرساخت‌های نرم‌افزاری و سخت‌افزاری مورد نیاز برای مرکز داده رشد است.

مدیر پروژه طراحی و ارتقای مرکز داده رشد در شرکت رمیس تصریح کرد: به‌طور کلی اهداف این طرح عبارت است از: حمایت از ایجاد زیرساخت‌های لازم جهت توسعه دولت و آموزش الکترونیک، طراحی و ارتقای مراکز داده رشد جهت ارائه سرویس‌های الکترونیکی برای حداقل یکصد هزار مدرسه، تسریع در تحقق دولت و آموزش الکترونیک در وزارت آموزش و پرورش و....

در همین حال مدیر پروژه اتصال صد هزار مدرسه به شبکه ملی اینترنت در آموزش و پرورش درباره تأمین زیرساخت‌های شبکه‌ای و ارائه محتوا برای مدارس به معنای طراحی و ارتقاء مرکز داده رشد طی پروژه اتصال یکصد هزار مدرسه به شبکه ملی اینترنت، گفت: در فاز یک طرح اتصال، فراهم کردن قابلیت‌های لازم به منظور ارائه خدمات کامل الکترونیکی نظیر آموزش الکترونیکی، سرویس‌های سازمان الکترونیکی و سرویس‌های عمومی به جامعه دانش‌آموزی کشور شامل کلیه دانش آموزان، پرسنل وزارت آموزش و پرورش و نیز اولیای دانش‌آموزان از طریق یک درگاه واحد و پویا (پورتال) مدنظر قرار دارد. امیرحسین محبعلی در بیان اهداف کلان این پروژه اظهار کرد: فراهم کردن امکان دسترسی مدارس متصل شده به شبکه ملی اینترنت و نیز از طریق آن به شبکه جهانی اینترنت با رعایت و اعمال سیاست‌های آموزشی فرهنگی مصوب، فراهم کردن سرویس پست الکترونیکی رایگان برای تمامی دانش‌آموزان، اولیاء و پرسنل آموزش، ایجاد زیرساختی مناسب برای راه‌اندازی سیستم آموزش الکترونیکی مدارس در سطح کشور، فراهم کردن دسترسی دانش‌آموزان به محتوای دروس الکترونیکی کتب درسی و کمک آموزشی و آزمایشگاه‌های مجازی در مرکز داده رشد و فراهم کردن امکان ارتباط مجازی مستقیم میان دانش‌آموزان و معلمان از جمله اهداف این پروژه است.

به گفته محبعلی به منظور رسیدن به این اهداف، پروژه در دو مرحله اجرا می‌شود؛ مرحله اول ارتقاء مرکز داده فعلی به جهت عبور از وضعیت موجود به وضعیت گذار جهت برآورده‌سازی نیازهای سرویسی فاز یک طرح و در مرحله دوم ایجاد طرحی جامع جهت عبور از مرحله گذار به وضعیت مطلوب جهت برآورده‌سازی نیازهای آتی وزارت آموزش و پرورش.

*** از سازمان‌های وابسته به وزارت آموزش و پرورش**

کارشناس منابع انسانی شرکت خبر داد:

اجرای سیستم آموزش کارکنان و تعیین نیازهای آموزشی مشاغل در رمیس

در پروژه بازنگری جذب کارکنان یک پروپزال تعریف شده که در صورت تصویب آن از سوی مدیریت، تمام کارمندان از این پس طبق این طرح جذب و استخدام خواهند شد

محسن تقیون، کارشناس منابع انسانی شرکت رمیس گفت: در شرکت پروژه جدیدی تحت عنوان سیستم ساماندهی نظام آموزش کارکنان آغاز شده است.

وی افزود: در این پروژه سعی شده تا تمام اطلاعات مربوط به کارکنان در یک پرونده ساماندهی شود و بر اساس آنها آموزش‌هایی که کارمندان به آن نیاز دارند، مورد توجه قرار گیرد.

وی تصریح کرد: برای شناخت بیشتر از وضعیت کارکنان، یکسری فرم برای آنان ارسال می‌شود تا آنها را تکمیل کنند. مصاحبه حضوری نیز با برخی انجام خواهد شد تا تمام کارهای روزانه و روتین آنها مشخص شده و مورد بررسی قرار گیرد که امیدواریم این موضوع تا سه ماه دیگر به اتمام برسد.

تقیون گفت: بعد از انجام این پروژه، آموزش‌هایی را در نظر خواهیم گرفت تا به کارکنان ارائه شود. این آموزش‌ها از دو دیدگاه مورد توجه است؛ عدالت در استفاده از امکانات و تسهیلات آموزشی. به عبارتی با ارائه این آموزش‌ها می‌توان جذب و نگهداری کارکنان را برای شرکت راحت‌تر کرد.

تقیون در ادامه به پروژه بازنگری جذب کارکنان اشاره کرد و گفت: در این طرح یک پروپزال تعریف شده که در صورت تصویب آن از سوی مدیریت، تمام کارمندان از این پس طبق این طرح جذب و استخدام خواهند شد.

وی در پایان در زمینه نظرسنجی‌ای که برای کارکنان در خصوص برگزاری برنامه‌های رفاهی تدوین شده، اظهار داشت: در این نظرسنجی چند عامل مورد توجه قرار گرفته است که عبارتند از: زمان برگزاری برنامه، نوع ارائه، نحوه اطلاع‌رسانی، نحوه محاسبه هزینه‌های برنامه و در نهایت نظر کلی در مورد این برنامه‌ها.

همچنین یکسری پیشنهادات از سوی همکاران مطرح شده که به مدیریت شرکت نیز ارائه شده است.

سرپرست بخش اداری شرکت رمیس:

هر ماه یک برنامه رفاهی برای همکاران خواهیم داشت

سرپرست بخش اداری شرکت رمیس برنامه‌های ورزشی و فوق برنامه شرکت را تشریح کرد.

محمد مهدی محبوبی گفت: یک سالن در مجموعه ورزشی هنگام (آبفا) رزرو کردیم و این امکان فراهم شد که سه‌شنبه‌ها همکاران در این سالن به تمرین فوتبال بپردازند.

از همین تمرین‌ها یک تیم فوتبال آماده حضور در مسابقات هر ساله در جام انفورماتیک نظام صنفی رایانه‌ای شرکت می‌کند و ما توانستیم با همین تیم در سال گذشته در جام ۲۲ بهمن، جام اخلاق را کسب کنیم.

وی ادامه داد: همچنین برای همه همکاران کارت راهیان سلامت خریداری کردیم و همه می‌توانند علاوه بر استخر از امکانات و مجموعه‌های ورزشی و تفریحی دیگر مانند سالن بدنسازی، کشتی و.... استفاده کنند. این کارت‌ها برای همکاران در حدود ۵۰ درصد تخفیف دارد.

وی تصریح کرد: سال گذشته در مسابقات شطرنج نیز توانستیم مقام دوم را کسب کنیم. امسال هم جام شطرنج بعد از ماه رمضان برگزار خواهد شد که امیدواریم در این دوره مسابقات نیز بتوانیم موفقیت‌های خوبی کسب کنیم.

محبوبی در ادامه سخنان خود به برنامه‌های رفاهی و فوق‌برنامه این شرکت اشاره کرد و گفت: در مردادماه گذشته توانستیم همکاران را به تئاتر «منهای ۲» ببریم که خدا را شکر ۷۹ درصد از شرکت‌کنندگان از آن رضایت داشتند و ما در نظر داریم بعد از ماه رمضان هر ماه یک برنامه رفاهی داشته باشیم.

طراحی و اجرای دیتاسنتر مرکزی پالایش و پخش به رمیس محول شد

طراحی و ساخت دیتاسنتر مرکزی شرکت ملی پالایش و پخش فرآورده‌های نفتی ایران با برگزاری مناقصه‌ای به شرکت رمیس واگذار شد، چرا که رمیس طرح فنی و مالی بهینه را ارائه کرد.

طراحی و ساخت دیتاسنتر مرکزی شرکت ملی پالایش و پخش فرآورده‌های نفتی ایران دارای بخش‌های مختلفی است که کلیه بخش‌های یک دیتاسنتر فیزیکی را در بر می‌گیرد که عبارتند از: طراحی و پیاده‌سازی سیستم‌های کنترل دسترسی، سرمایش و گرمایش، اطفاع حریق، سقف و کف کاذب، روشنایی، برق اضطراری (UPS) و.... همچنین در این پروژه دوره آموزشی آشنایی با مرکز داده شرکت پالایش و پخش فرآورده‌های نفتی ایران برای کارشناسان این شرکت برگزار خواهد شد.

شرکت ملی پالایش و پخش فرآورده‌های نفتی ایران

با ارائه طرح بهینه فنی و مالی

پروژه طراحی مراکز داده و پیاده‌سازی مرکز داده اصلی بیمه ایران به رمیس سپرده شد

پروژه مشاوره و طراحی مراکز داده اصلی و پشتیبان و تأمین تجهیزات و پیاده‌سازی مرکز داده اصلی شرکت سهامی بیمه ایران به شرکت رمیس واگذار شد.

مهندس احسان پورمند، مدیر فناوری اطلاعات شرکت رمیس با بیان این مطلب گفت: شرکت رمیس توانست با ارائه طرحی فنی و برآورد اقتصادی مطلوب از اجرای پروژه، در مناقصه طراحی مراکز داده و پیاده‌سازی مرکز داده اصلی بیمه ایران برنده شود.

وی افزود: مأموریت این پروژه، ایجاد مرکز داده اصلی بیمه ایران، جهت استقرار مطمئن و کارآمد سرویس‌ها و نرم‌افزارهای کاربردی مختلف و ارائه خدمات به تمامی مراکز ستادی، شعب و نمایندگی‌های شرکت بیمه ایران در سطح کشور با کیفیت سرویس مناسب است.

پورمند اظهار داشت: با توجه به اینکه محل در نظر گرفته شده جهت پیاده‌سازی مرکز داده در حال حاضر عملیاتی است، به‌گونه‌ای برنامه‌ریزی شده است که عملیات ساختمانی و تأسیساتی مورد نیاز با کمترین درخواست قطعی سیستم عملیاتی فعلی و در ساعات غیر اداری صورت گیرد.

توسط رمیس انجام شد

راه‌اندازی نرم‌افزارهای مدیریت شبکه سیسکو در بانک مسکن

راه‌اندازی پیشرفته‌ترین و پیچیده‌ترین نرم‌افزارهای مدیریت شبکه سیسکو در بانک مسکن توسط شرکت رمیس پایان یافت.

سه نرم‌افزار مدیریت شبکه Cisco CNS، Cisco ANA و Cisco ISC توسط شرکت رمیس در بانک مسکن راه‌اندازی شد.

بر اساس گزارش خبرنگار رمیس، Cisco ANA دارای قابلیت نمایش و مانیتورینگ شبکه در لایه ۳ (مانند نمایش ترافیک شبکه و نمایش ترافیک VPN)، مدیریت، انجام تغییرات و شبیه‌سازی شبکه در لایه ۳ است. Cisco ISC نیز قابلیت پیاده‌سازی سرویس‌های VPN، MPLS VPN و Tunneling از طریق اینترفیس در حجم زیاد را داراست. همچنین قابلیت Cisco CNS مدیریت و انجام تغییرات بر روی روترها و سوئیچ‌ها به صورت گرافیکی و ساده با امکانات بالاست.

با ارائه طرحی مبتنی بر مجازی‌سازی؛

بانک ملی ایران پروژه NOC خود را به رمیس سپرد

پروژه پیاده‌سازی مرکز شبکه (NOC) بانک ملی ایران به شرکت رمیس واگذار شد. مجید علیمرادپور، مجری این پروژه در شرکت رمیس با بیان مطلب فوق اظهار داشت: در مناقصه‌ای که به این منظور توسط بانک ملی برگزار شد، شرکت رمیس توانست با ارائه یک طرح مالی و فنی بهینه بر مبنای VMware و مجازی‌سازی، رتبه اول را کسب کند.

وی افزود: این پروژه از مردادماه سال جاری آغاز شده و طی دو الی سه ماه اجرایی خواهد شد. علیمرادپور خاطر نشان کرد: همچنین مقرر شده است دوره‌های آموزشی VMware را برای کارشناسان بانک ملی ایران برگزار کنیم. گفتنی است پیش از این شرکت رمیس پروژه NOC را در دو مرکز دیگر انجام داده بود.

طراحی سیستم NOC پیش از این به گونه‌ای انجام پذیرفت که نرم‌افزار HP Open View NNM به عنوان نرم‌افزار اصلی این پروژه نصب و نرم‌افزارهای دیگر بعد از نصب به روش‌های مختلف با نرم‌افزار NNM یکپارچه شدند. نرم‌افزار NNM یک نرم‌افزار مانیتورینگ بوده و مانیتورینگ در سطح Enterprise تمام دستگاه‌های تحت شبکه بجز کامپیوترهای موجود توسط این نرم‌افزار انجام می‌گیرد.

همچنین از نرم‌افزار Cisco Works به منظور پیکربندی و تهیه پیکربندی‌های سیستم‌های موجود به صورت یکپارچه با سایر نرم‌افزارها استفاده شده بود.

پروژه طراحی، تأمین، نصب و راه‌اندازی منابع ذخیره‌ساز اطلاعات قوه قضائیه به رمیس رسید

شرکت رمیس در مناقصه طراحی، تأمین، نصب و راه‌اندازی منابع ذخیره‌ساز اطلاعات قوه قضائیه برنده شد.

قوه قضائیه برای دستیابی به حداقل امنیت قابل قبول برای نگهداری از اطلاعات سامانه‌های موجود خود، اقدام به برگزاری مناقصه‌ای جهت طراحی و تأمین منابع ذخیره‌ساز کرد که کارشناسان شرکت رمیس با ارائه طرح بهینه بر مبنای راهکارهای HP موفق به تأمین نظر کارشناسان مرکز آمار و فناوری اطلاعات و ارتباطات قوه قضائیه شده و ضمن کسب رتبه اول فنی، با ارائه قیمت مناسب توانستند در این مناقصه برنده شوند.

در این طرح از دو دستگاه EVA به همراه نرم‌افزارهای Continuous Access جهت ذخیره اطلاعات به‌صورت آنلاین در دو سایت مختلف به عنوان سایت اصلی و back up قوه قضائیه استفاده می‌شود.

فعالیت‌های نمایندگی رمیس در استان هرمزگان

هم‌اکنون تعمیر و نگهداری سیستم‌های کامپیوتری بانک سپه در جزیره قشم و تعمیر و نگهداری شبکه این بانک در کل استان هرمزگان، تعمیر و نگهداری شبکه بانک تجارت استان و گارانتی تجهیزات شبکه بانک مسکن هرمزگان به نمایندگی شرکت رمیس در این استان سپرده شده است.

نبی‌الله امامداری، نماینده تعمیر و نگهداری شرکت رمیس در استان هرمزگان اظهار داشت: تاکنون تمام مشتریان ما از فعالیت‌های انجام شده راضی هستند و رمیس را به‌عنوان شرکت خوب و متخصص می‌شناسند.

امامداری در خصوص همکاری خود با شرکت رمیس گفت: بنده چندین سال است که نمایندگی محصولات این شرکت را در استان هرمزگان عهده‌دار هستم و در بخش‌های فروش، تعمیر و نگهداری تجهیزات شبکه و WAN فعالیت می‌کنیم.

نماینده شرکت رمیس در استان هرمزگان در خصوص کیفیت محصولات شرکت رمیس گفت: محصولات این شرکت از نظر کیفیت و قیمت قابل مقایسه با سایر شرکت‌ها نیست و این امر مرهون مدیریت خوب در این شرکت است.

وی ادامه داد: رمیس همکاری خوبی با نمایندگی‌های خود در سراسر ایران دارد و به محض بروز هر مشکل و ارائه درخواست یک قطعه، این قطعه سریع برای ما ارسال می‌شود.

تشریح عملکردهای جاری واحد فروش سخت‌افزار و شبکه رمیس

سرپرست واحد فروش سخت‌افزار و شبکه شرکت رمیس در خصوص فعالیت‌های این واحد اظهار داشت: در حال حاضر فعالیت اصلی این واحد ارائه سرورها و تجهیزات ذخیره‌سازی HP و نیز تجهیزات شبکه Cisco است.

مهرداد امامی‌مهر افزود: فروش بیش از یک هزار دستگاه سرور طی شش ماه اول سال جاری مرهون وفاداری مشتریانی است که به جهت دریافت تجهیزات اصلی و نیز خدمات پس از فروش بدون قید شرط، هر روز ارتباطشان با رمیس قوی‌تر می‌شود.

وی ادامه داد: از جمله پروژه‌هایی که طی شش ماه اول امسال در واحد سخت‌افزار و شبکه اجرا شده است می‌توان به تأمین و تحویل سرورها، تجهیزات ذخیره‌سازی و شبکه بانک سپه، وزارت صنایع و معادن، شرکت اکتشاف نفت، بانک ملی ایران، دانشگاه آزاد خوراسگان اصفهان و ... اشاره کرد.

سرپرست واحد فروش سخت‌افزار و شبکه شرکت رمیس گفت: خوشبختانه هر روز تعداد تماس‌های مشتریان برای خرید تجهیزات HP و Cisco از اقصی نقاط کشور بیشتر می‌شود و همین امر به انرژی ما برای پاسخگویی سریع‌تر و بهتر به مشتریان می‌افزاید.

از سوی شرکت رمیس انجام شد:

اجرای موفقیت‌آمیز پروژه ایمن‌سازی و ارتقای شبکه و دیتاسنتر دانشگاه آزاد دزفول

پروژه ایمن‌سازی، توسعه و ارتقای شبکه و دیتاسنتر دانشگاه آزاد واحد دزفول با موفقیت از سوی شرکت رمیس به پایان رسید.

محمد مهدی نیک‌عهد، مدیر این پروژه در شرکت رمیس با بیان این مطلب گفت: شبکه دانشگاه آزاد دزفول دارای بیش از یک‌هزار کاربر، ۲۰ سرور و ۵۰ عدد سوئیچ در سه لایه بوده که برای ارتقای امنیت شبکه ابزارهای 802.1x پیاده‌سازی شد که برای احراز هویت کاربران مورد استفاده قرار می‌گیرد.

وی افزود: همچنین ضمن ارتقاء و طراحی مجدد سرویس‌های پایه نظیر DHCP، نسبت به طراحی مرکز مانیتورینگ، پایش شبکه و دیتاسنتر دانشگاه با استفاده از آخرین نرم‌افزارها و تکنولوژی‌های مربوطه اقدام شد.

نیک‌عهد تصریح کرد: در این پروژه مدیریت دسترسی متمرکز کاربران نیز با استفاده از Cisco Secure ACS راه‌اندازی شده و سرویس ایمیل داخلی دانشگاه با استفاده از Exchange server 2008 و به صورت کلاستر ایجاد شد.

از عملکرد رمیس رضایت داریم

علیرضا نخیلی، کارشناس امنیت شبکه دانشگاه آزاد دزفول نیز در گفت‌وگو با خبرنگار رمیس، ضمن تشریح پروژه ساماندهی شبکه اینترانت و بهبود سرورهای دانشگاه اظهار داشت: این پروژه همان‌طور که از اسمش پیدا است، در زمینه ارتقای شبکه، افزایش و بهبود تجهیزات سخت‌افزاری و نرم‌افزاری و همچنین افزایش ضریب امنیت شبکه دانشگاه بود که طراحی این پروژه از دو سال پیش انجام شده ولی به دلیل برخی مشکلات امکان واگذاری و اجرای آن به‌وجود نیامد.

در ابتدا ۱۰ شرکت برای انجام این پروژه اعلام آمادگی کردند که در مرحله اول بر اساس نمایندگی‌های شرکت‌ها و سوابق آنان، امتیازبندی انجام شد که شرکت رمیس نیز جزء ۶ شرکت برتر قرار گرفت. در مرحله بعدی پس از بازگشایی پاکات، شرکت رمیس از نظر قیمت و پس از بررسی‌های انجام شده از سوی تیم کارشناسی دانشگاه، برنده این مناقصه عمومی شد

وی افزود: از سال گذشته نیاز به ارتقای شبکه و افزایش امنیت آن به شدت احساس شد، لذا دانشگاه تصمیم گرفت با برگزاری مناقصه‌ای، این پروژه را پیاده‌سازی کند.

وی ادامه داد: در ابتدا ۱۰ شرکت برای انجام این پروژه اعلام آمادگی کردند که در مرحله اول بر اساس نمایندگی‌های شرکت‌ها و سوابق آنان، امتیازبندی انجام شد که شرکت رمیس نیز جزء ۶ شرکت برتر قرار گرفت. در مرحله بعدی پس از بازگشایی پاکات، شرکت رمیس از نظر قیمت و پس از بررسی‌های انجام شده از سوی تیم کارشناسی دانشگاه، برنده این مناقصه عمومی شد.

نخیلی خاطر نشان کرد: پروژه ما بسیار گسترده و در ابعاد بسیار کلانی انجام شد که شامل به‌روزرسانی سرورهای مانیتورینگ، بهبود سرورهای DNS، به‌روزرسانی آنتی‌ویروس‌های شبکه، ارتقای امنیت شبکه، افزایش تجهیزات سخت‌افزاری و نرم‌افزاری، افزایش سرورهای شبکه و... بود که به‌طور کلی می‌توان گفت با انجام این پروژه، شبکه داخلی دانشگاه و سرورها به صورت کامل متحول شد.

وی در ادامه سخنان خود اجرای این پروژه را از سوی شرکت رمیس رضایت‌بخش عنوان کرد و گفت: ما از عملکرد شرکت رمیس بسیار رضایت داریم و این شرکت توانست به خوبی این پروژه را با وجود گستردگی بالا، با کیفیت فنی مناسب اجرا کند.

وی اضافه کرد: در ابتدای انجام پروژه مشکلاتی از قبیل اجرای زمان‌بندی طرح وجود داشت که بیشتر به دلیل دیر حاضر شدن تجهیزات اعم از نرم‌افزاری و سخت‌افزاری و همچنین هم‌زمانی پروژه با کلاس‌های آموزشی بود ولی این امر با همفکری و همکاری مناسب رمیس به سرعت ساماندهی شد.

کارشناس امنیت شبکه دانشگاه آزاد دزفول اظهار داشت: در حال حاضر پروژه تمام شده و تحویل نهایی آن هم انجام گرفته است و ما هم‌اکنون در حال تست شبکه و بررسی تغییرات و احیاناً رفع مشکلاتی که هنوز به‌وجود نیامده هستیم.

وی اظهار امیدواری کرد: انشاءالله در آینده بتوانیم با همکاری شرکت رمیس پروژه‌های بزرگ‌تری را در دانشگاه برای بهبود و ارتقای سیستم‌های آموزشی انجام دهیم.

توسط علی حامدی، کارشناس ارشد دیتاسنتر رمیس صورت گرفت

اخذ گواهینامه VMware 4 برای نخستین بار در ایران

رمیس لطفاً در مورد مدرک جدیدی که اخذ کردید (VMware Certified Professional 4)، توضیح دهید.

در تابستان سال گذشته همراه با عرضه محصول جدید VMware یعنی vSpher ، Certificate و مراحل اخذ آن نیز دچار تغییر شد و امتحان جدیدی تحت نام VCP4 یا VMware Certified Professional4 جایگزین مدرک قبلی (VCP3) شد. ساختار دریافت مدارک شرکت VMware با کمپانی‌های دیگری از جمله Cisco و HP متفاوت است. برخلاف این کمپانی‌ها که شما بدون گذراندن دوره‌های رسمی آنها در امتحانات بین‌المللی شرکت می‌کنید، سیاست‌های VMware بدین صورت است که متقاضیان شرکت در امتحان بین‌المللی باید ابتدا مطابق با Certification Plan ارائه شده در سایت این شرکت، در دوره‌های رسمی این کمپانی شرکت و سپس در صورت تأیید VMware می‌توانند در امتحان بین‌المللی شرکت کنند. با مساعدت شرکت رمیس این امکان برای من فراهم شد تا در دوره رسمی کمپانی VMware شرکت کرده و شرایط شرکت در امتحان بین‌المللی این کمپانی را پیدا کنم.

رمیس در ایران کسی این گواهینامه را دارد؟

تا آنجایی که من اطلاع دارم این اولین بار است که یک ایرانی موفق به اخذ این مدرک شده است.

رمیس امتحان کجا برگزار شد؟

تایلند.

رمیس نمایندگی شرکت در تایلند بود؟

امتحان شرکت VMware مانند شرکتCisco توسط کمپانی VUE برگزار می‌شود.

رمیس یعنی شما تنها فردی بودید که از ایران در این آزمون شرکت کردید یا اینکه افراد دیگری هم شرکت کردند اما موفق نشدند؟

در پاسخ به این سؤال باید به دو نکته اشاره کنم: اولا با توجه به تحریم ایران از سوی اغلب کمپانی‌های IT، از قبیل VMware، Cisco و HP، امکان دریافت یا اطلاع از لیست افرادی که از این کشور مدارک مذکور را دریافت کرده‌اند، وجود ندارد اما با توجه به کوچک بودن بازار IT در ایران، اغلب همکاران از این مسأله که چه افرادی موفق به اخذ چه مدارکی شده‌اند، مطلع می‌شوند. ثانیاً دلایل متعددی وجود دارد که خود به خود تعداد متقاضیان شرکت در این امتحان کاهش می‌یابد که مهم‌ترین این دلایل عبارتند از: در نظر گرفتن پیش‌نیاز جهت شرکت در دوره‌های رسمی VMware در داخل کمپانی مذکور، مشکلات موجود برای ایرانیان جهت شرکت در دوره‌های بین‌المللی IT، جدید بودن بحث مجازی‌سازی و هزینه قابل توجه شرکت در دوره‌های رسمی درخارج از کشور.

رمیس قصد تدریس این دوره را دارید؟

شرکت VMware یک‌ساختار رسمی جهت دریافت امکان تدریس رسمی دوره‌های این شرکت درنظر گرفته است که مهم‌ترین مورد آن اخذ نمره بالای ۴۰۰ از ۵۰۰ امتیاز در امتحان بین‌المللی است که اینجانب موفق به دریافت نمره ۴۸۰ از ۵۰۰ شدم.

رمیس فکر می‌کنید از چه زمانی امکان تدریس این دوره میسر شود؟

نخستین گواهینامه بین‌المللی VMware Certified Professional 4 به‌نام کارشناس ارشد مرکز داده شرکت رمیس صادر شد. علی حامدی، کارشناس ارشد واحد ICT شرکت رمیس توانست با گذراندن موفق دوره‌های آموزشی و آزمون شرکت VMware، این گواهینامه را از آن خود کند. با او در این خصوص گفت‌وگو کرده‌ایم که می‌خوانید.

مرکز آموزش رمیس تلاش می‌کند زیرساخت‌های مورد نیاز از نظر تجهیزات برای برگزاری دوره‌های آموزشی را فراهم کند که پس از فراهم آمدن زیرساخت‌ها، برپایی این دوره‌ها را می‌توانیم آغاز کنیم.

رمیس اخذ این گواهینامه چه مزایایی برای رمیس ایجاد می‌کند؟

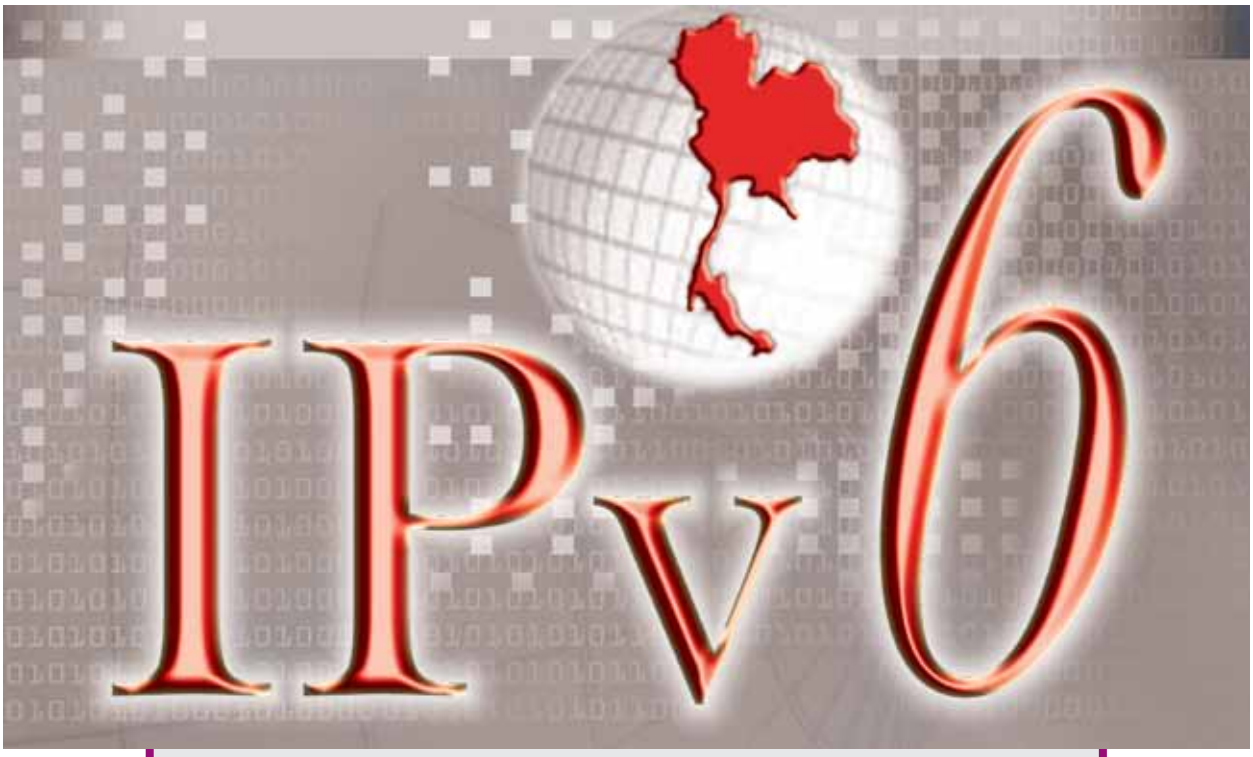
موضوع مجازی‌سازی در یکی دو سال اخیر در بازار طرفداران زیادی پیدا کرده که در مناقصه‌هایی که شرکت در آن مشارکت می‌کند، این موضوع نمود داشته و می‌تواند مورد استفاده رمیس قرار گیرد. اکثر شرکت‌هایی که موضوع مجازی‌سازی را در دستور کار خود قرار می‌دهند، یکی از پیش‌نیازهایی که برای مناقصات در نظر می‌گیرند، وجود نیرویی است که گواهینامه رسمی این دوره‌ها را دارا بوده و تسلط کافی روی این محصول داشته باشد که اخذ این گواهینامه از این جهت حائز اهمیت است.

رمیس پس در جذب مشتری جدید هم مؤثر خواهد بود.

بله.

رمیس بیشتر چه مشتریانی؟

مشتریان این محصول غالباً شرکت‌های دولتی بزرگ هستند. ویژگی‌های این محصول از جمله امکان پیاده‌سازی Business Continuity Plan بدون به‌وجود آمدن down time و تحمل‌پذیری در مقابل خرابی‌های احتمالی، قطعاً مورد توجه مشتریانی از قبیل بانک‌ها و نهادهایی که سرویس‌های عملیاتی دارند، قرار خواهد گرفت.



چکیده: به دلیل پیشرفت روزافزون شبکه‌های مبتنی بر IP و ارائه سرویس‌های مختلف مخابراتی نظیر صوت و تصویر بر روی بستر IP، در سراسر جهان مهاجرت سیستم‌های مخابراتی مختلف به سمت یک شبکه واحد توانا به ارائه سرویس‌های مختلف در بستر IP، در حال انجام است و به نظر می‌رسد نسل آینده شبکه‌ها نیز بر اساس پروتکل IP بنا شود و بسیار محتمل است که به دلیل کاستی‌های بسیار IPv4 در زمینه‌های مختلف از جمله فضای محدود آدرس، پروتکل پایه در شبکه‌های نسل آینده، IPv4 باشد. این مقاله به بررسی این نکته می‌پردازد که آسیب‌پذیری‌های IPv6 از بسیاری جهات به آسیب‌پذیری‌های IPv4 شباهت دارد، چرا که به عنوان مثال مکانیسم پایه برای انتقال بسته‌ها در شبکه تقریباً بدون تغییر باقی مانده است و قراردادهای لایه بالاتر که داده کاربردی واقعی را منتقل می‌کنند، تفاوت چندانی احساس نمی‌کنند. در ادامه، مقاله حاضر به بررسی مسائل و مشکلات امنیتی موجود در شبکه‌های مبتنی بر IPv4 و IPv6 می‌پردازد و با مقایسه تحلیلی آنها مشکلات مشترک و جدید را معرفی می‌کند. این مقاله نشان می‌دهد که با توجه به تغییرات نسبی IPv6 نسبت به IPv4 در برخی موارد بهبودهایی حاصل شده است اما در مواردی نیز تغییری حاصل نشده است.

تجزیه و تحلیل و مقایسه مشکلات امنیتی IPv4 و IPv6

احسان نیری، سید مصطفی صفوی همامی

۱- مقدمه

شبکه‌های نسل آینده (NGN) شبکه‌هایی هستند مبتنی بر بسته که قادر هستند تمامی سرویس‌های مخابراتی را ارائه دهند و بتوانند از تکنولوژی‌های مختلف انتقال باند پهن و قادر به ارائه کیفیت سرویس استفاده کنند. در این شبکه‌ها عملکردهای مربوط به سرویس‌دهی (لایه سرویس) از تکنولوژی‌های مربوط به انتقال (لایه انتقال) مستقل هستند [۲،۱].

به دلیل پیشرفت روزافزون شبکه‌های مبتنی بر IP و ارائه سرویس‌های مختلف مخابراتی نظیر صوت و تصویر بر روی بستر IP، در سراسر جهان مهاجرت سیستم‌های مخابراتی مختلف به سمت یک شبکه واحد توانا به ارائه سرویس‌های مختلف در بستر IP، در حال انجام است. در حال حاضر، سازمان‌های مختلف فعال در زمینه استانداردسازی مخابرات، مثل اتحادیه جهانی مخابرات (ITU)، سازمان استانداردسازی مخابرات اروپا (ETSI) و کارگروه مهندسی اینترنت (IETF) در حال بررسی و معرفی الزامات و معماری‌های امنیتی جدید هستند و تحقیقات در این زمینه ادامه دارد.

تحقیقات فعلی بر روی شبکه‌های نسل آینده با هدف اطمینان از این مسأله انجام می‌شود که شبکه‌های مبتنی بر IP نسل آینده، قادر باشند تا استانداردهای سرویس‌دهی معمول شبکه‌های مخابرات عمومی را برآورده کنند و این امر نه تنها در سرویس‌هایی مثل تلفن و داده، بلکه برای گسترده‌ترین مجموعه ممکن از کاربردهای چند رسانه‌ای فعلی و آینده قابل دستیابی باشد. در واقع تفاوت عمده بین شبکه‌های نسل آینده و سرویس‌های مخابراتی فعلی اینست که در حال حاضر، شبکه‌ها مجزا و دارای کاربردهای خاص (تلفن، اینترنت، تلفن همراه و ...) هستند، اما در شبکه نسل آینده تنها یک شبکه موجود است که قابلیت ارائه هر سرویس در هر لحظه زمانی و در هر مکانی را دارد [۴،۳ و ۵].

ادامه این مقاله به شرح زیر است، در بخش دو به بررسی شباهت‌ها و تفاوت‌های آسیب‌پذیری در IPv4 و IPv6 پرداخته می‌شود. بخش سوم به بررسی آسیب‌پذیری‌های جدید در IPv6 و میزان تهدید آنها می‌پردازد. نتیجه‌گیری در بخش چهارم

ارائه شده است.

۲- مقایسه آسیب‌پذیری‌های IPv4 و IPv6

آسیب‌پذیری‌ها، مشکلات یا خطاهای مستندشده‌ای هستند که می‌توان با استفاده از آنها سیستم‌ها را به اعمالی وادار کرد که از قبل پیش‌بینی نشده است. این استفاده معمولاً از سر بدخواهی یا دشمنی رخ می‌دهد و می‌تواند خطرات و مسائل ناخواسته بسیاری را موجب شود. متأسفانه معمولاً تمام مشکلات یا خطاهای سیستم‌ها شناسایی نمی‌شوند و بنابراین در تمامی سیستم‌ها آسیب‌پذیری‌های مستندنشده هم وجود دارد. تلاش برای یافتن و آزمایش آسیب‌پذیری‌های مستندنشده کاری مشکل و طاقت‌فرسا است. نکته مهم این است که یک گزارش آسیب‌پذیری فنی تنها نگاهی به حفره‌های امنیتی موجود در سیستم است و حملات بسیاری پس از مشخص شدن آسیب‌پذیری‌ها رخ می‌دهد مگر اینکه سیستم قبل از قرار گرفتن در دسترس عموم مورد بررسی قرار گیرد و نقاط آسیب‌پذیر آن شناسایی و رفع شود.

آسیب‌پذیری‌های IPv6 از بسیاری جهات به آسیب‌پذیری‌های IPv4 شباهت دارد، چرا که مکانیسم پایه برای انتقال بسته‌ها در شبکه تقریباً بدون تغییر باقی مانده است و قراردادهای لایه بالاتر که داده کاربردی واقعی را منتقل می‌کنند، تفاوت چندانی احساس نمی‌کنند. هر چند، از آنجا که در IPv6 استفاده از قرارداد IPsec اجباری است معمولاً گفته می‌شود IPv6 خیلی امن‌تر از IPv4 است. این عبارت ممکن است در یک محیط ایده‌آل که در آن برنامه‌های کاربردی به خوبی نوشته شده‌اند و زیرساخت احراز هویت مقاومی وجود دارد و مدیریت کلید به نحو عالی انجام می‌شود درست باشد؛ اما در واقعیت همان مشکلاتی که در پشتیبانی از IPsec در IPv4 وجود دارد، در IPv6 هم موجود است. حتی اگر IPv6 امن به نحو مناسبی پیاده شود، به خاطر وجود حفره‌های امنیتی که در سطح کاربرد رخ می‌دهد نمی‌توان امنیت بیشتری را تضمین کرد، به خصوص در برابر حملاتی که نمی‌توان به سادگی منبع آنها را معین کرد.

با این همه، تفاوت‌های معناداری بین IPv4 و IPv6 در استفاده از IPsec وجود دارد. این تفاوت‌ها باعث می‌شود نوع حملات به شبکه‌های IPv6 اندکی تغییر داشته باشد. همچنین احتمال اینکه در یک بازه زمانی کوتاه بیش از نیمی از سازمان‌ها و شرکت‌ها کاملاً به IPv6 مهاجرت کنند، بسیار کم است. بیشتر شرکت‌ها تمایل دارند ساختار IPv4 را نگه دارند و در برخی قسمت‌ها از IPv6 استفاده کنند. تا آن زمان، رفتار درست و مناسب در برابر حملات و تهدیدات امکان‌پذیری کمی دارد و تغییرات بسیاری در طراحی دستگاه‌ها و تجهیزات شبکه می‌طلبد.

در ادامه تعدادی از تهدیدات شناخته شده بر ضد IPv4 را بررسی معین می‌کنیم که این حملات یا حملات مشابه چه اثراتی بر IPv6 خواهند داشت. برخی حملات جدید نیز علیه IPv6 قابل انجام است که در ادامه آنها را نیز بررسی کرده‌ایم. باید توجه داشت که امنیت IPv6 یک موضوع پیچیده و بزرگ است. همچنین آزمایش‌ها و بررسی‌های اندکی روی آن صورت گرفته است. بنابراین، برخی از موضوعات بطور مبسوط بررسی نشده است. به عنوان مثال، نسخه شش قرارداد IP موبایل (MIPv4) مورد بررسی قرار نگرفته است. شایان ذکر است که در چندین قسمت از ادامه این بررسی، فرض‌های قابل قبولی انجام شده است اما آزمایش واقعی انجام نشده است که آزمایش آنها می‌تواند موضوع یک تحقیق جدید باشد.

۳- آسیب‌پذیری‌های جدید در IPv6

حملاتی که در ادامه می‌آید، با حملات IPv4 تفاوت‌های قابل توجهی دارند. در مقایسه با IPv4 برخی حملات آسان‌تر شده‌اند، برخی مشکل‌تر و در برخی نیز تنها روش تغییر کرده است. این حملات عبارتند از:

- شناسایی
- دسترسی بدون مجوز
- دستکاری سرآیند و تکه‌تکه کردن بسته
- مشابه‌سازی در لایه‌های ۳ و ۴
- بسط دامنه پخش همگانی (smurf)

رحملات مسیریابی

- ویروس‌ها و کرم‌ها

۳-۱- شناسایی

اولین دسته حمله‌ها، حملات شناسایی هستند که معمولاً اولین حملاتی هستند که توسط افراد متخاصم انجام می‌شود. در این حمله مهاجم سعی می‌کند درباره شبکه قربانی بیشتر و بیشتر بداند. این کار شامل حملات فعال مثل اسکن و حملات غیر فعال مثل یافتن اطلاعات از موتورهای جستجو است. حملات فعال با هدف دست‌یابی مهاجم به اطلاعات ویژه‌ای درباره میزبان‌ها و دستگاه‌های شبکه هدف، اتصال آنها به یکدیگر انجام می‌شود تا با استفاده از آنها سناریوهای حمله طرح شود.

مهاجم IPv4 روش‌های مناسبی برای جمع‌آوری این اطلاعات در اختیار دارد که عبارتند از:

- جاروب Ping، برای معین کردن آدرس‌های IP موجود در شبکه و حدس توپولوژی شبکه،
- اسکن پورت‌ها، پس از شناسایی سیستم‌های قابل دسترس برای یافتن سرویس‌های قابل دسترسی روی میزبان‌های مختلف،
- اسکن آسیب‌پذیری و برنامه‌های کاربردی، برای شناسایی پورت‌های فعال، شناسایی سیستم‌های عامل، شناسایی برنامه‌های کاربردی و نسخه آنها و حتی آزمایش وجود آسیب‌پذیری‌های شناخته شده.

محدود کردن این حمله‌ها معمولاً با استفاده از فیلتر کردن انواع خاصی از بسته‌ها ممکن است. بسته‌هایی را باید فیلتر کرد که توسط مهاجم مورد سوء استفاده قرار می‌گیرد. اما باید توجه داشت که فعالیت‌های شناسایی را نمی‌توان کاملاً متوقف کرد زیرا اجازه برقراری تماس با برخی دستگاه‌ها، برخی از شناسایی‌ها را امکان‌پذیر می‌سازد.

با توجه به تکنولوژی، شناسایی IPv6 با شناسایی IPv4 دو تفاوت عمده دارد. اول اینکه تکمیل جاروب Ping یا اسکن پورت برای شمردن میزبان‌های یک زیرشبکه، در شبکه‌های IPv6 بیشتر طول می‌کشد. دوم اینکه آدرس چندبخشی جدید در IPv6 مهاجمان را قادر می‌سازد که مجموعه‌ای خاص از سیستم‌های کلیدی (مثل مسیریاب‌ها، قرارداد زمان شبکه، سرورها و...) را ساده‌تر بیابد. جدا از این دو تفاوت، تکنیک‌های شناسایی در هر دو نسخه یکسان است. به علاوه شبکه‌های IPv6 به عملکرد ICMPv6 بیشتر وابسته هستند. فیلتر کردن بسته‌های ICMPv6 می‌تواند اثرات منفی روی عملکرد شبکه داشته باشد.

IPv6 آدرس‌های چندپخشی جدید را پشتیبانی می‌کند که می‌تواند مهاجم را در شناسایی منابع کلیدی شبکه یاری کند. این آدرس‌ها می‌توانند خاص باشند. به عنوان مثال تمام مسیریاب‌ها (FF05::2)، تمام سرورهای DHCP (FF05::3). این آدرس‌ها به صورت قانونی استفاده می‌شوند اما ممکن است در حملات سیل‌گونه یا حملات پیچیده‌تر مورد سوء استفاده قرار گیرند. بنابراین باید توجه داشت که فیلتر کردن این آدرس‌های داخلی در لبه خارجی شبکه امری ضروری است.

بسیار جای امیدواری است که هنوز ابزار جدید و مناسبی برای جاروب ping برای IPv6 معرفی نشده است. حتی نرم‌افزار معروف Nmap نیز از این راهکار پشتیبانی نمی‌کند. دلیل این امر می‌تواند بزرگ بودن فضای دامنه IPv6 باشد. در سمت دیگر باید توجه داشت که بسیاری از سیستم‌های IDS از IPv6 پشتیبانی نمی‌کنند و باعث می‌شوند اسکن کردن شبکه بدون جلوگیری انجام شود. از طرفی نرم‌افزارهای بسیاری کمی برای مدیریت شبکه وجود دارند که مشکل عدم استفاده از ping را به نحوی حل کرده باشند. به نظر می‌رسد با رویکرد بیشتر به سمت IPv6 چنین مشکلاتی قابل حل باشد.

۳-۲- دسترسی غیرمجاز

دسترسی غیرمجاز به آن‌دسته از حملاتی اشاره دارد که در آنها مهاجم تلاش می‌کند از سیاست انتقال باز مرتبط با IPv4 بهره‌گیری کند. هیچ‌چیز در پشته پروتکل IP وجود ندارد که از اتصال یک میزبان به میزبان دیگر ممانعت به عمل آورد. مهاجمان از این مسأله استفاده می‌کنند تا اتصالی را به قراردادهای لایه‌های بالاتر و کاربردهای موجود در دستگاه‌های شبکه و میزبان‌های نهایی شکل دهند.

تمرکز شبکه‌های IPv4 بر محدود کردن دسترسی غیر مجاز با به کارگیری روش‌های کنترل دسترسی

است. این کنترل‌ها در سیستم‌های انتهایی و در گیت‌وی‌ها بین نقاط انتهایی IPv4 به کار می‌روند و می‌توانند در لایه سه و لایه چهار باشند. روش‌های کنترل دسترسی در IPv4 با بالاتر رفتن در پشته پروتکل پیچیده‌تر می‌شوند.

در لایه IP، محافظ شبکه از لیست‌های کنترل دسترسی (ACLs) ساده استفاده می‌کند تا تنها به میزبان‌های تأیید شده اجازه ارسال بسته به دستگاه را بدهد. لیست کنترل دسترسی برای محدود کردن دسترسی به (یا از طریق) یک دستگاه به کار می‌روند و از سیاست‌های امنیتی استفاده می‌کنند. در شبکه‌های IPv4، این کنترل‌های دسترسی در دستگاه‌های شبکه‌بندی (مثل دیواره آتش) و روی خود میزبان‌های انتهایی (دیواره‌های آتش میزبان) پیاده‌سازی می‌شوند. با اینکه دیواره‌های آتش می‌توانند سیاست‌های امنیتی را فقط بر اساس سرآیندهای IPv4 اعمال کنند، بهترین استفاده از آنها زمانی است که با بازرسی TCP/UDP و اطلاعات لایه کاربرد ترکیب شوند.

نیاز به تکنولوژی‌های کنترل دسترسی در IPv6 نیز همانند IPv4 است اما به هر حال کاربرد اجباری IPsec می‌تواند تا حدی این کنترل دسترسی به میزبان‌ها را در IPv6 ساده‌تر کند. محافظ شبکه می‌خواهد دسترسی مهاجمان به شبکه را محدود کند. توانایی کنترل دسترسی بر مبنای IPv6، هم موجب تغییر اطلاعاتی می‌شود که می‌تواند در سرآیند لایه سه فیلتر شود و هم روش آدرس‌دهی و سیستم‌های مسیریابی را نیز تغییر می‌دهد.

علاوه بر فضای آدرس، سیستم آدرس‌دهی IPv6 نیز با IPv4 متفاوت است، چرا که به یک آداپتور شبکه در یک گره IPv6 اجازه می‌دهد چند آدرس IPv۶ داشته باشد. این آدرس‌های IPv6 چندگانه به منظور برقراری ارتباط در زیرشبکه محلی (لینک محلی- FE80::/10)، درون یک سازمان (سایت محلی- FC00::/16 یا FC00::16 بر اساس انتخاب گروه کاری)، یا روی اینترنت (آدرس‌های تک‌پخشی) به کار می‌روند. طراح شبکه می‌تواند با استفاده از ترکیب سیستم مسیریابی و این محدوده‌های آدرس‌دهی، دسترسی به گره‌های انتهایی IPv6 را محدود کند. به عنوان نمونه، طراح شبکه می‌تواند با IPv6، یک آدرس تک‌پخشی سراسری را فقط به دستگاهی بدهد که به ارتباط با اینترنت سراسری نیاز دارد در حالی که به همان سیستم یک آدرس محلی تخصیص دهد که بتواند فقط با گره‌های درون سازمان مربوط ارتباط برقرار کند. همچنین، اگر یک دستگاه به برقراری ارتباط فقط در یک زیرشبکه خاص نیاز دارد، فقط آن آدرس به دستگاه داده می‌شود. به علاوه، استفاده از الحاقات محرمانگی می‌تواند زمانی را که هر آدرس IPv6 قابل دسترسی و در خطر حمله است کاهش دهد.

هر چند بسیاری از دیواره‌های آتش که از IPv6 پشتیبانی می‌کنند در بازار وجود دارند، اما بسیاری از آنها برای ارائه زودتر محصول به بازار تجاری، راه‌حل‌های جزئی برای IPv6 ارائه کرده‌اند. به عنوان مثال برخی دیواره‌های آتش فقط قسمت اندکی از سرآیند-های توسعه را می‌شناسند و فقط ترافیکی را فیلتر می‌کنند که شامل آن سرآیندها باشند. مثالی از چنین دیواره‌های آتشی، دستگاهی است که منطقی برای پردازش سرآیند مسیریابی ندارد. اگر چنین دیواره آتشی بسته‌ای با سرآیند مسیریابی دریافت کند، آن را دور می‌اندازد. این عمل هنگام محافظت از میزبان‌ها برخی منافع امنیتی را به دنبال دارد. اما در مقابل چنین دستگاهی را نمی‌توان برای پشتیبانی از تحرک‌پذیری و قرارداد MIPv6 به کار برد. با این حال سیستم‌های جدیدتر تا حد زیادی می‌توانند این مشکل را مرتفع سازند.

۳-۳- دستکاری سرآیند و تکه‌تکه کردن بسته

سومین دسته از حملات، تکه‌تکه کردن بسته و سایر حملات دستکاری در سرآیند است. این دسته از حملات در ابتدا به چند دلیل به کار گرفته شد. اولین هدف استفاده از تکه‌تکه‌سازی به عنوان ابزاری برای گریز از دستگاه‌های امنیتی شبکه، مثل سیستمهای کشف نفوذ و یا دیواره‌های آتش حالتمند بود. دومین هدف از حمله استفاده از تکه‌تکه کردن یا سایر دستکاری‌ها در سرآیند بسته، حمله مستقیم به زیرساخت شبکه بود.

تکه‌تکه کردن بسته، تکنیکی است که در IPv4 برای تنظیم کردن داده‌گرام IPv4 به کمترین MTU در مسیر بین نقاط انتهایی به کار می‌رود. به عبارت دیگر، تکه‌تکه کردن در IPv4 به عنوان یک تکنیک برای عبور از کنترل‌های دسترسی در دستگاه‌هایی نظیر مسیریاب یا دیواره آتش به کار رفته است. این روش برای حملات سردرگم‌کننده برای عبور از سیستم‌های امنیتی شبکه نیز به کار گرفته شده است. بسیاری از دیواره‌های آتش جدید و سیستم‌های کشف نفوذ پیشرفته، تلاش می‌کنند تا بسته‌ها را دوباره سرهم کنند و آنها را با قواعد کنترلی یا امضاهای حمله مطابقت دهند. در حالت کلی، تعداد زیاد بسته‌های تکه‌تکه شده به عنوان یک شاخص زودهنگام برای تلاش‌های دستیابی و نفوذ استفاده می‌شود.

در IPv6 تکه‌تکه کردن بسته در گره‌های میانی ممنوع است. یکی از پرکاربردترین حملات تکه‌تکه کردن، ایجاد همپوشانی بین تکه‌ها برای گمراه کردن دستگاه‌های امنیتی IPv4 است. در IPv6 این کار انجام‌پذیر نیست، چون این تکه‌ها به راحتی به عنوان حمله، شناسایی و معدوم می‌شوند. به علاوه، اگر سیستم‌های امنیتی شبکه به تکه‌های دارای همپوشانی اجازه عبور بدهند، بسیاری از سیستم-عامل‌ها در پشته IPv6 خود، این تکه‌ها را دور می‌ریزند. هر چند، اگر سیستم‌عامل‌های انتهایی چنین بسته‌هایی را بپذیرند، هیچ راهی برای جلوگیری از سوء استفاده از چنین بسته‌هایی وجود نخواهد داشت. در این صورت مهاجمان می‌توانند با استفاده از این بسته‌ها سیاست‌های دستگاه‌های امنیتی شبکه را دور بزنند و به همان اهداف موجود در IPv4 دست یابند. به علاوه، مهاجم می‌تواند این بسته‌ها را برای دور زدن امضاهای حمله در سیستم‌های کشف نفوذ استفاده کند.

در فصل پنجم استاندارد IPv6 [۶] آمده است که حداقل MTU باید ۱۲۸۰ اکتت باشد. به همین دلیل، مدیر شبکه می‌تواند دستگاه امنیتی را تنظیم کند تا تکه‌هایی با طول کمتر از ۱۲۸۰ اکتت را دور بیندازد، مگر اینکه بسته آخرین بسته در جریان باشد. مدیر شبکه در صورتی می‌تواند این عمل را انجام دهد که سیستم عامل فرستنده قطعه‌ها، بسته‌های اصلی را در حد MTU معرفی شده در پیام PMTU تکه‌تکه کند و این کار را تا زمانی انجام دهد که آخرین قطعه از بسته را ارسال می‌کند. اگر سیستم عامل مبدأ چنین عملی را انجام ندهد، دستگاه امنیتی باید تکه‌هایی با طول کمتر از ۱۲۸۰ را نیز بپذیرد و پردازش کند. این عمل به حملات فریبنده کمک می‌کند. چنین حملاتی با ارسال تعداد زیادی از بسته‌های تکه‌تکه شده قابل انجام است. برای بررسی امکان‌پذیری چنین کاری در واقعیت، باید سیستم عامل‌های فعلی مورد آزمایش قرار گیرند.

ترکیب چند سرآیند توسعه و تکه‌تکه کردن در IPv6 آسیب‌پذیری‌ای را ایجاد می‌کند که در تکه‌های نخستین IPv4 وجود ندارد. این مسأله اعمال سیاست‌های لایه ۴ را در دستگاه‌هایی که بازسازی بسته انجام نمی‌دهند دچار مشکل می‌کند. مثالی از این مسأله می‌تواند یک مسیریاب سیسکو باشد که ویژگی‌های دیواره آتش آن برای بازسازی بسته فعال نشده است. این مسیریاب هنگام کار با بسته‌های IPv6، بسته‌های غیر نخستین و بسته نخستینی که فیلد پروتکل آن نامشخص است عبور می‌دهد؛ که می‌تواند مشکلات بسیاری را به وجود آورد.

دیواره‌های آتش و سیستم‌های کشف نفوذ فعلی IPv6 نیز همانند IPv4 بازسازی و سایر بررسی‌ها را روی بسته‌های تکه‌تکه شده اعمال می‌کنند تا احتمال حمله را کاهش دهند. این بررسی تکه‌ها شامل تکه‌های خارج از دنباله و سوئیچ کردن آنها به دنباله و همچنین بررسی تعداد تکه‌های تولید شده در یک IP منفرد نیز می‌شود تا بتوان از حملات ممانعت از سرویس جلوگیری کرد.

با این همه هنوز وجود ابزار حمله‌ای مبتنی بر تکه‌تکه کردن بسته‌ها برای حمله روی IPv6 تأیید نشده است.

۳-۴- مشابه‌سازی در لایه‌های ۳ و ۴

یک عنصر کلیدی که انواع مختلفی از حملات IP را ممکن می‌سازد، توانایی مهاجمان برای تغییر آدرس IP و پورت بسته‌هایی است که روی شبکه

می‌فرستند. با این کار به نظر می‌رسد که از محل دیگر یا برنامه کاربردی دیگری استفاده می‌کنند. این دسته از حملات بسیار شایع هستند.

امروزه، حملات مشابه‌سازی آدرس در IPv4، به ویژه در لایه سوم، بسیار صورت می‌گیرد. با این کار ردگیری حملات ممانعت از سرویس، اسپم‌ها، کرم‌ها و ویروس‌ها بسیار مشکل می‌شود. حملات مشابه‌سازی لایه سوم معمولاً در حملات تراکنشی به کار نمی‌روند؛ زیرا ترافیک بازگشتی به محلی می‌رود که به عنوان آدرس منبع در بسته وجود دارد. بنابراین مهاجم باید حدس بزند که ترافیک برگشتی شامل چه چیزهایی است. با این همه، مشابه‌سازی در لایه ۴ می‌تواند در حملات تراکنشی به کار رود تا ترافیک را به شکلی جلوه دهد که به نظر برسد از محل دیگری در جریان است (مثل تزریق پیام‌های نادرست مدیریت شبکه (SNMP) یا ورودی‌های ثبت رویداد غلط).

مستند [۷] روش‌هایی را مشخص کرده‌است که با فیلترکردن ترافیک ورودی از ترافیک مشابه‌سازی شده جلوگیری کند. روش ارائه شده در [۷] به پیاده‌سازی همه‌جانبه برای عملکرد مناسب نیاز دارد اما متأسفانه چنین روشی به صورت گسترده به کار نرفته است. این امر باعث می‌شود حملات مشابه‌سازی آدرس بسیار زیاد رخ دهند. باید توجه داشت که در مستند مذکور تنها با تقلید قسمت شبکه مقابله می‌شود و به قسمت میزبان پرداخته نشده است. بنابراین در زیر شبکه ۲۴ بیتی‌ای مثل 192.0.2.0/24 فیلترینگ تضمین می‌کند که مثلاً ترافیک منشأ گرفته از آدرس 192.0.3.0 حذف می‌شود اما مهاجمانی که هر آدرسی در زیرشبکه 192.0.2.0/24 را مشابه‌سازی کنند، موفق خواهند بود. مستند RFC 2827 به مدیر شبکه اجازه می‌دهد که حملات انجام شده به یک سازمان خاص را پیگیری کند.

علاوه بر متوقف کردن مشابه‌سازی محدوده آدرس‌های معتبر در فضای آدرس IPv4، تعداد بسیار زیادی از آدرس‌های IPv4 تخصیص داده نشده‌اند و آدرس‌های رزرو هم اغلب تخصیص داده نشده است. این محدوده‌ها را می‌توان به صورت سراسری مسدود کرد تا حملاتی که از این آدرس‌های تقلیدی استفاده می‌کنند موفق نباشند.

یک از امیدوار کننده ترین مزایای IPv6 از دیدگاه تقلید لایه ۳، طبیعت آدرس‌های سراسری و مجتمع IPv6 است. بر خلاف IPv4، در IPv6 تخصیص‌ها طوری تنظیم می‌شوند که در نقاط متفاوت شبکه به راحتی خلاصه شوند. این کار فیلترینگی شبیه RFC 2827 را ممکن می‌سازد. با این کار ارائه دهندگان سرویس اطمینان حاصل می‌کنند که: حداقل مشتریان آنها نمی‌توانند آدرس‌های خارج از محدوده آنها را مشابه‌سازی کنند. متأسفانه این مسأله استاندارد نشده است و پیاده‌سازی آگاهانه‌ای در سمت متصدیان را می‌طلبد. با این همه، حملات لایه ۴ تغییری نکرده‌اند، چرا که پروتکل‌های لایه ۴ تغییر نکرده‌اند.

نکته دیگری که باید توجه کرد این است که میزان زیرشبکه‌ها در IPv6 می‌تواند بسیار بزرگ باشد، بنابراین حتی با وجود فیلترینگی مانند RFC 2827 نیز، مهاجم محدوده بزرگی از آدرس‌ها برای تقلید دارد. از نقطه نظر انتقال، مکانیسم‌های تونل‌کشی مختلف، به مهاجمان این امکان را می‌دهد که با اتصال IPv4 یا IPv6، برای ارسال هر نسخه‌ای از IP استفاده کنند. به عنوان مثال، مهاجمان می‌توانند از مسیریاب‌های رله ۶ به ۴ استفاده کنند تا ترافیک را به یک شبکه IPv6 تزریق کنند و همزمان پیگیری آنها کاری سخت و پیچیده باشد. شایان ذکر است که این امر بدتر از پیگیری در IPv4 نیست. اما برخی بررسی‌ها باید در رله انجام گیرد، مثل اینکه آدرس‌های IPv4 منبع خارجی با آدرس‌های موجود در منبع IPv6 همخوانی دارد یا نه.

۳-۵- بسط دامنه پخش همگانی

حملات بسط دامنه پخش‌همگانی، معمولاً با نام حملات «smurf» شناخته می‌شوند. این حملات، ابزارهای حملات ممانعت از سرویس هستند و از قابلیت ارسال یک پیغام تقاضای اکو با آدرس مقصد قربانی به صورت پخش همگانی در یک زیرشبکه استفاده می‌کنند. قبل از ارسال چنین پیامی، آدرس منبع تولید پیام مشابه‌سازی می‌شود و برابر آدرس IP هدف مورد حمله قرار داده می‌شود. اتفاقی که می‌افتد این است که تمام میزبان‌های انتهایی موجود در زیرشبکه، پاسخی به آدرس منبع مشابه‌سازی‌شده (آدرس هدف حمله) ارسال می‌کنند که دریافت سیلابی از بسته‌های پاسخ در گیرنده را موجب خواهد شد. این مسأله می‌تواند منشاء آسیب‌های بسیاری در سیستم گیرنده پاسخ گردد.

یک راه حل ساده برای مقابله با این حمله در شبکه‌های IPv4 وجود دارد. اگر پخش همگانی بر مبنای IPv4 در مسیریاب‌ها پشتیبانی نشود، هنگامی که یک مهاجم چنین پیام‌هایی را ارسال کند، تنها یک پیام پاسخ به میزبان مورد حمله ارسال می‌شود. این مسأله امروزه به صورت پیش‌فرض در اغلب مسیریاب‌ها وجود دارد. به همین دلیل این حمله کمتر انجام می‌پذیرد، اما هنوز هم می‌تواند به عنوان یک حمله ممانعت از سرویس مؤثر به کار گرفته شود.

در IPv6، مفهوم پخش‌همگانی منشأ گرفته از IP از قرارداد حذف شده است و در طراحی قرارداد سعی شده است تا امکان چنین حملاتی وجود نداشته باشد. بویژه برای حملات smurf،[۸] تأکید شده است که یک پیام ICMPv6 نباید با آدرس گیرنده همگانی تولید شود. این محدودیت برای آدرس‌های چندپخشی یا همگانی لایه پیوند وجود دارد. اگر نقاط انتهایی با این استاندارد همخوانی داشته باشند آنگاه حملاتی نظیر smurf در IPv6 نمی‌تواند رخ دهد.

بررسی نشان می‌دهد که بسیاری از سیستم‌عامل‌های مشهور، با استاندارد مذکور همخوانی دارند و به چنین پیغام‌هایی پاسخ نمی‌دهند. اما برخی ابهامات نیز وجود دارد. مثلاً اینکه نقاط انتهایی شبکه چگونه باید به یک پیام ICMP با آدرس منبع چندپخشی یا همگانی پاسخ دهند. اگر نقاط انتهایی به چنین آدرس‌هایی پاسخ دهند، باز یک مهاجم می‌تواند یک حمله بسط دامنه را با هدف ممانعت از سرویس به انجام برساند که این مسأله نیز به IPv6 ارتباط اندکی دارد.

۳-۶- حملات مسیریابی

حملات مسیریابی بر ایجاد اختلال یا تغییر مسیر جریان ترافیک در شبکه متمرکز می‌شوند. این کار به روش‌های گوناگونی انجام می‌شود که حملاتی مانند حملات غرقه‌سازی flooding، حملات اعلان سریع، حذف مسیریاب‌ها و اعلان نادرست مسیریاب‌ها را شامل می‌شود. مشخصات این حملات، بسته به پروتکل مورد استفاده آنها متفاوت است.

پروتکل‌های مسیریابی در IPv4 معمولاً با

تأیید رمزنگاری شده برای امن کردن اعلان‌های بین مسیریاب‌ها محافظت می‌شوند. پر کاربرد ترین پیاده‌سازی این سیستم‌ها تأیید با استفاده از الگوریتم‌های چکیده پیامی چون MD5 است که با استفاده از کلیدهای از پیش مشترک بین مسیریاب‌ها کار می‌کند. متأسفانه الگوریتم MD5 و برخی نظایر آن، شکسته شده و دیگر نمی‌تواند امنیت را تضمین کند. اما هنوز مسیریاب‌های بسیاری وجود دارند که این مسأله را حل نکرده‌اند. بنابراین مهاجم می‌تواند با شنود اعلانات بین مسیریاب‌ها و رمزگشایی آن، به رمز مشترک پی‌ببرد و حمله خود را پایه‌ریزی کند.

چندین پروتکل مسیریابی وجود دارند که مکانیسمهای امنیتی خود را هنگام پشتیبانی از IPv6 تغییر نداده‌اند. به عنوان مثال، پروتکل مسیریابی دروازه مرزی (BGP) که از چند قرارداد مختلف پشتیبانی می‌کند، برای حمل اطلاعات IPv6 بین دامنه‌ها توسعه داده شده است [9]. اما هنوز هم بر مبنای استفاده از MD5 و TCP برای تأیید کار می‌کند. پروتکل سیستم‌میانی به سیستم‌میانی (IS–IS) نیز از IPv6 پشتیبانی می‌کند، اما باز سیستم تأیید آن بدون تغییر مانده است. این پروتکل برای تأیید بسته‌های وضعیت لینک (LSPs)، از روش افزودن اطلاعات احراز هویت به عنوان بخشی از این بسته استفاده می‌کند. هر چند، تأیید مبتنی بر کلمات عبور ساده است و از رمزنگاری نیز استفاده نمی‌کند. در [10] یک تأیید مبتنی بر رمزنگاری برای IS–IS پیشنهاد شده است که می‌تواند برای محافظت در IPv6 هم به کار گرفته شود. در الگوریتم OSPF جدید نیز فیلدهای تأیید سرآیند OSPF حذف شده است. در قرارداد RIPng نیز نحوه احراز هویت حذف شده است. در دو پروتکل OSPF و RIPng برای تأمین امنیت اطلاعات داخلی بین مسیریاب‌ها بر اساس پروتکل‌های AH و ESP ارائه شده در IPsec عمل می‌شود. این پروتکل‌ها برای ارائه جامعیت، قابلیت اعتماد، احراز هویت و مقابله با ارسال مجدد استفاده می‌شوند.

به نظر می‌رسد مکانیسم‌های امنیتی برای امن کردن پروتکل‌هایی که با IPv6، OSPFv3 و RIPng تغییر کرده اند، در تجهیزات شبکه فعلی به خوبی پیاده‌سازی نشده باشند. این مسأله به مشکلات استفاده از IPsec باز می‌گردد و باعث بسط آسیب‌پذیری‌های IPsec به این پروتکل‌ها نیز می‌شود.

۳-۷- ویروس‌ها و کرم‌ها

امروزه، ویروس‌ها و کرم‌ها به عنوان یکی از مهمترین آسیب‌پذیری-های شبکه‌های مبتنی بر IP خودنمایی می‌کنند. نگاهی به اخبار و اطلاعات منتشر شده نشان می‌دهد که تقریباً مخرب‌ترین حملات عمومی در سال‌های اخیر توسط یک ویروس یا کرم و گروه متحد با آنها انجام گرفته است.

ویروس‌ها و کرم‌ها در IPv4 نه تنها به خود میزبان‌ها صدمه زده‌اند، بلکه بسیاری از آنها توانسته‌اند قابلیت انتقال شبکه را بسیار کاهش دهند و حجم وسیعی از منابع شبکه نظیر مسیریاب‌ها و سرورهای ایمیل را مشغول کنند. به عنوان مثال «SQL slammer» به خاطر آهنگ سریع اسکن شبکه خود، باعث ایجاد سیلاب‌های حجیم بسته‌ها در شبکه شد (اما هر بسته حمله تنها یک پیام UDP بود!). از تکنیک‌هایی که در IPv4 برای مقابله با این حملات به کار گرفته شده اند، می‌توان پوشش مناسب یا حذف حفره‌های امنیتی به صورت مرتب، استفاده از آنتی‌ویروس‌ها در میزبان‌ها و کشف زودهنگام و انسداد مجراهای آسیب‌پذیری را نام برد. کشف زودهنگام را می‌توان به سادگی با کشف سیستم‌های با رفتار غیر عادی انجام داد. برخی مواقع سیستم‌هایی در شبکه قرار داده می‌شوند که دسترسی به آنها امنیت کمتری لازم دارد. این سیستم‌ها نقاط حمله جذابی برای بسیاری از مهاجمان هستند، اما پس از اعمال حمله توسط مهاجم یا ویروس، عملکرد سیستم توسط مدیر بررسی می‌شود تا آسیب‌پذیری را شناسایی و سایر سیستم‌ها را نسبت به آن آسیب‌پذیری مقاوم کند. ویروس‌های قدیمی با IPv6 تغییر چندانی نکرده‌اند. ویروس‌های مبتنی بر ایمیل یا آنها که رسانه‌های قابل حمل (مثل کارت‌های حافظه، فلاپی، فلش دیسک و...) را مورد هجوم قرار می‌دادند، به قوت خود باقی هستند. هرچند، کرم‌ها یا کرم و ویروس‌هایی که از برخی اسکن‌های اینترنت استفاده می‌کردند تا میزبان‌های آسیب‌پذیر خود را بیابند، ممکن است با موانع قابل توجهی مواجه شوند؛ و به خاطر مسائلی مثل افزایش اندازه زیر شبکه که قبلاً بررسی شد، نتوانند به سرعت قبل به انتشار خود ادامه دهند. تحقیقات زیادی لازم است تا مشخص شود این تغییر چه میزان تأثیری در تکنیک‌های نویسندگان کرم‌ها به وجود خواهد آورد و آیا دیگر کرم‌ها مثل امروز مخرب خواهند بود یا نه. به عنوان مثال انتظار می‌رود کرم‌های شبیه به «SQL–slammer» در IPv6 تأثیر بسیار کمتری داشته باشند چرا که اسکن شبکه و یافتن میزبان‌های آسیب‌پذیر برای حملات غرقه‌سازی بسیار مشکل‌تر خواهد بود.

روش‌های پیشگیری و مقابله‌ای که در IPv4 استفاده می‌شدند، در IPv6 نیز قابل انجام هستند. هر چند، محصولات کشف نفوذ زیادی برای IPv6 هنوز در دسترس نیست.

۴-نتیجه‌گیری

در این مقاله، لزوم استفاده شبکه‌های نسل آینده از ر بررسی شد و پس از آن به بررسی و مقایسه آسیب پذیری‌های IPv4 و IPv6 پرداخته شد. با توجه به مباحث مطرح شده می‌توان گفت آسیب‌پذیری‌های IPv6 از بسیاری جهات به آسیب‌پذیری‌های IPv4 شباهت دارد، چرا که مکانیسم پایه برای انتقال بسته‌ها در شبکه تقریباً بدون تغییر باقی مانده است و قراردادهای لایه بالاتر که داده کاربردی واقعی را منتقل می‌کنند تفاوت چندانی احساس نمی‌کنند.

با توجه به این مسأله، ذکر این نکته نیز ضروری است که تغییرات IPv6 نسبت به IPv4 در موارد بسیاری باعث جلوگیری از حملات قدیمی می‌گردد، اما در مواردی نیز ممکن است راهکارهای جدید به کار گرفته شده در IPv6، برای حمله مورد استفاده قرار گیرد. از طرف دیگر، بسیاری از آسیب‌پذیری‌هایی که می‌تواند در رابطه با IPv6 مطرح باشد، مربوط به پیاده‌سازی‌های یا تنظیمات نادرست، سیاست‌های اشتباه مدیران شبکه یا سازندگان تجهیزات امنیتی و کاربردی شبکه است و به طور مستقیم به IPv6 مربوط نمی‌شود.

با این همه، همان طور که گفته شد وجود ابزارهای مناسب برای حملات جدید یا حملات مشابه حملات قدیمی، هنوز تأیید نشده است و هم انجام حملات بر اساس IPv6 با مشکلات بیشتری (نسبت به IPv4) همراه است و این مسأله می‌تواند امیدواری‌هایی به سیاست‌گذاران زیر ساخت انتقال شبکه نسل آینده دهد، که سناریوهای خود را بر اساس IPv6 بنا نهند. برای نیل به چنین اهدافی پیشنهاد می‌شود مطالب مطرح شده در این مقاله با تجهیزات واقعی در شرایط مختلف مورد بررسی قرار گیرد.

همچنین برای بررسی میزان پشتیبانی تجهیزات شبکه نسل آینده از IPv6 و قابلیت پیکربندی و تنظیم آنها، بایستی بتوان راهکارهایی ارائه داد. ارائه روش‌های برای غلبه بر آسیب‌پذیری‌های لایه‌های بالاتر نیز از کارهایی است که می‌تواند در این زمینه انجام پذیرد.

[1] ITU-T Rec. Y.2001, "General Overview of NGN.", 2004-12
[2] ITU-T Rec. Y.2011, "General Principles and General Reference Model for Next Generation Network.", 2004-10
[3] ETSI TR 180 000, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology", 2006-2
[4] ETSI TR 180 001, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1;Release definition", 2006-3
[5] ETSI ES 282 001, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1" , 2005-8
[6] Deering, S., Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
[7] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, May 2000
[8] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998
[9] Marques P. and F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing," RFC2545,March 1999
[10] Li, T. and R. Atkinson, "Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication," RFC 3567, July 2003

راه‌های حفظ مشتری

یکی از مشکلات امروز کسب و کار، حفظ مشتری است. مفهوم «مشتری مادام‌العمر» دست‌نیافتنی است. هر مدیری خواهان آن است که مشتری خود را برای همیشه حفظ کند ولی آیا این موضوع تحقق می‌یابد؟ روی وفاداری مشتری برای همیشه نمی‌توان حساب کرد. در مقابل، مفهوم وفاداری محدود مشتری مطرح شده است. مدیران با رعایت موارد ذیل می توانند وفاداری مشتری را افزایش دهند و چشم‌انداز حفظ طولانی‌تر مشتری را بهبود بخشند.

۱ به مشتری یک تضمین پیشنهاد دهید. هر کسب و کاری می‌تواند یک تضمین مطلوبی در اختیار مشتری قرار دهد که برایش جالب توجه باشد.

۲ دسترسی آسان به تلفن را برای مشتری فراهم کنید. قراردادن شماره تلفن‌های آزاد در اختیار مشتری به این معنی است که شرکت توجه خاصی به مشتری دارد.

۳ به مشتری پیشنهادهایی ارائه دهید که کمک حال او باشد. هر کسب و کاری با سؤال‌های زیادی مواجه است. شما سعی کنید با انتشار جزوه‌ای به صورت سؤال و جواب اطلاعات لازم را دراختیار مشتری قرار دهید.

۴ به‌طور مرتب با مشتری در ارتباط باشید. با این کار شما این ذهنیت را در مشتری ایجاد می‌کنید که او را فراموش نکرده‌اید و به مسایل او توجه دارید. حتی می‌توانید اطلاعات مورد نیازش را برایش ارسال دارید. مشتری مایل است بداند که شرکت غیر از فروش کالا، چه مسایلی برایش جالب است.

۵ همیشه جانب مشتری را بگیرید و در اکثر مواقع با او اظهار همدردی کنید.

۶ آدرس پست الکترونیک را در اختیار مشتری قرار دهید. این کار به مشتری این احساس را می دهد که امکان دسترسی به شرکت همیشه وجود دارد.

۷ سعی کنید وعده‌هایی که می‌دهید، واقع‌گرایانه باشد. در شرایطی که رقابت دشواراست، سنگ بزرگ انداختن کار ساده‌ای است اما فراموش نکنید که این کار شرایط را دشوار می سازد. بهتر است همیشه واقع‌گرا باشید.

۸ به حرف‌های مشتری خوب گوش دهید. گوش دادن به مشتری یعنی دادن اطلاعات مفید به او و بهبود خدمات.

۹ به موقع به سؤال مشتری پاسخ دهید.

اکثر شرکت‌ها به درخواست‌های مشتری طبق اولویت‌های خود پاسخ می‌دهند که این مسأله چندان خوشایند نیست.

۱۰ همیشه همان لحظه تصمیم‌گیری کنید. این عبارت که «بعداً راجع به این موضوع صحبت خواهیم کرد» مشتری را به دامن رقیب خواهد انداخت. هیچ چیز به اندازه تصمیم‌گیری در همان لحظه مشتری را خوشحال نمی‌کند.

۱۱ صورتحساب‌ها را خیلی ساده، مشخص و خوانا بنویسید.

۱۲ ارتباطات را همیشه مشخص کنید. مثلاً نامه‌ای را برای مشتری ارسال نکنید که روی آن نوشته شده «مشتری عزیز» بلکه مشتری را به اسم خطاب کنید. اگر اسم او را درست بلد نیستید، نامه را ارسال نکنید.

۱۳ راه‌های پایین آوردن هزینه‌ها را به مشتری بگویید. قبل از اینکه مشتری درمورد کاهش هزینه‌ها سؤال کند، شما پیش‌قدم شوید.

۱۴ تلفن‌ها را کامل جواب دهید و در این کار عجله نکنید. عجله کردن مشتری را می‌آزارد. ارتباط عجولانه میزان هیجان مشتری را بالا می‌برد و در نتیجه ارتباط خوب انجام نخواهد شد.

همه آنچه که گفته شد، همه آن چیزی نیست که می‌توان وفاداری مشتری را برای همیشه حفظ کرد.

البته راه‌های دیگری هم وجود دارد ولی این نکته نباید فراموش شود که اگر این حداقل‌ها هم رعایت نشود، مطمئن باشید که مشتری به دامن رقیب شما پناه خواهد برد.

بهداشت حرفه ای در کار با رایانه

اعتیاد اینترنتی

ساعت ۱۱:۳۰ شب است. بسیار خسته است، به طوری که چشمانش باز نمی‌شوند. فردا هم از همان اول صبح کلی کار دارد. اما مگر می‌تواند بدون چک کردن ایمیل‌هایش بخوابد؟ پای رایانه‌اش می‌نشیند و به اینترنت وصل می‌شود. با خود می‌گوید: فقط نیم ساعت. بعد می‌خوابم. چند ایمیل چک می‌کند و چندتا هم جواب می‌دهد. دو سه نفر از دوستانش آنلاین هستند. شروع به صحبت با او می‌کنند. همزمان مشغول خواندن خبرهای روز در سایت‌های مختلف است. ناگهان به طور تصادفی چشمش به گوشه پایینی سمت چپ مانیتور می‌افتد و ساعت سیستم را می‌بیند. ساعت ۲:۳۰ بامداد است و او هنوز بیدار است.

تا به حال این اتفاق برای شما افتاده است؟ اگر پاسخ مثبت است، باید بگویم که علائم یک بیماری اینترنتی یعنی اعتیاد به وب یا WebAddiction در شما به چشم می‌خورد.

روانشناسان و محققان در نقاط مختلف جهان مشغول بررسی این مشکل هستند، تا افراد مقدار زمانی را پشت رایانه‌هایشان به سر ببرند که مشکلی برای آنها پیش نیاورد. مطابق تحقیقات جدیدی که در دانشگاه فلوریدا انجام شده و در تاریخ ۷ آگوست منتشر شده است، برای تست اعتیاد به وب باید به ۵ سؤال پاسخ داد و برای به خاطر سپردن این ۵ سوال باید کلمه Mouse را که حرف ابتدای این سوالات است، در ذهن ثبت کرد.

این نکات و سؤالات عبارتند از:

۱) گذراندن زمان بیش از زمان مورد نظر در اینترنت
(More Than intended time spent online)

۲) غفلت از سایر مسؤولیت‌ها
(Other responsibilities neglected)

۳) تلاش‌های ناموفق برای کاهش مدت حضور روی شبکه
(Unsuccessful attempts to cut down)

۴) ناسازگاری در روابط به علت استفاده از اینترنت
(Significant relationship discord because of use)

۵) اضطراب و تفکر بیش از حد در زمان عدم حضور روی شبکه
(Extensive thoughts or anxiety when not online)

محققان دانشگاه فلوریدا این نکات را پس از ارزیابی روانشناسانه حضوری و رودررو روی ۲۰ داوطلبی که احساس می‌کردند دچار این مشکل هستند و ۱۷ دانشجو با سطوح مختلف استفاده از اینترنت، به دست آوردند. داوطلبان همگی افرادی بودند که در هفته بیش از ۳۰ ساعت آنلاین بودند و مدت زمان استفاده غیر ضروری آنها از اینترنت ۱۰ برابر بیش از زمان مورد استفاده برای کار یا تحصیل بود.

جالب است بدانید مطابق تحقیقات انجام شده حدود ۲۵ تا ۵۰ درصد از وابستگی شدید و اعتیاد به وب و اینترنت، در محل کار ایجاد می‌شود که این نکته نشان می‌دهد این عده از افراد برای شرکت در فعالیت‌هایی که ربطی به کارشان ندارد، حقوق می‌گیرند. بنابراین تحقیقات، هرکارمند بیش از یک روز کامل کاری را در هر هفته به مرور صفحات وبی می‌پردازد که ربطی به کارش ندارد.

از طرف دیگر، سر زدن به سایت‌های مختلف و گوناگون از سوی کارمندان باعث به خطر افتادن شبکه‌های داخلی شرکت‌ها می‌شود و احتمال نفوذ ویروس، کرم‌های اینترنتی و کدهای خطرناک را به این شبکه‌ها بالا می برد.

مشکل دیگری که در این مواقع ایجاد می‌شود، ترافیک بالاست. هنگامی که یک یا چند نفر از کارمندان مثلاً در حال دیدن یک فیلم یا گوش دادن به یک آهنگ از روی شبکه هستند، ترافیک ایجاد شده باعث می‌شود تا سایر افراد دسترسی سریع و مناسب به اینترنت نداشته باشند.

این دلایل باعث می‌شود تا شرکت‌های مختلف به فکر استفاده از فایروال و کنترل دسترسی کارکنان به اینترنت بیفتند تا بتوانند کارایی را بالا ببرند و امنیت شرکت خود را حفظ کنند.

سال ۱۹۹۵ روانپزشکی به نام گلدبرگ، اعتیاد

جدیدی را کشـف کرد و با مردمی روبرو شد که برای زل زدن به مانیتور، خانواده را رها کرده‌اند. این مردم ترجیح می دادند که وقت خود را با کامپیوتر و اینترنت، در محیط مجازی بگذرانند. شباهت‌های بسـیاری بین این نوع اعتیاد و اعتیاد به مواد مخدر و الـکل وجود دارد. متخصصان بهداشـت روانی در حال تحقیق بر روی کسـانی هسـتند که بیش از انـدازه آنلاین می شـوند و از نظر تعداد رشـد فزاینده‌ای دارند.

در بعد روانشناختی، اینترنت در کنار فواید غیرقابل انکارش، می‌تواند برای کاربران آسـیب‌های جدی متعـددی از جمله هویت نامشـخص، اضطراب، افسردگی و انزوا، اعتیاد به اینترنت و به خصوص اعتیاد به به چت به همراه داشته باشد.

بنابر یک گزارش، برخی از آمریکایی‌ها تا جایی بـه اینترنت اعتیاد پیدا کرده‌اند که روزانه بیش از ۸ ساعت از وقت خود را با اینترنت می‌گذرانند. این بیماری در آمریکا به جایی رسیده است که دولت و خانواده‌ها دست به دامن کلیساها شده‌اند سرپرست مرکز درمانی اعتیاد دانشگاه استنفورد می‌گوید: «اگر فردی متوجه شد که قادر نیست یک روز را بدون اسـتفاده از آن سپری کند، شکی نیست که این فرد به استفاده از اینترنت معتاد شده است.»

اعتیاد به اینترنت در سال اولیه چندان جدی گرفته نمی‌شد ولی با رشـد روزافزون مبتلایان، رسماً به عنوان یک اعتیاد معرفی شد و در بعضی کشورها، کلینیک‌های مخصوصی برای درمان مبتلایان به این نوع اعتیاد دایر گشت. از جمله این کشورها می‌توان به چین، آمریکا و آلمان اشاره کرد که به علت تعداد زیـاد کاربران اینترنت، دارای بیشـترین معتادان به اینترنت هسـتند. آلمان با حدود ۳۰ میلیون کاربر بیش از یک میلیون معتاد به اینترنت دارد یا در چین از ۹۴ میلیون کاربری که از اینترنت استفاده می‌کنند، ۵/۲ میلیون نفر به اینترنت معتادند.

با رشد روزافزون این پدیده، کشورها اندک اندک وارد مقوله مبارزه با آن می‌شوند. در همین راستا سال گذشته مرکز ترک اعتیادی در چین ایجاد شد تا این کاربران را به سوی زندگی بهتر سوق دهد و دولت هم در حال تصویب قوانینی است تا پدر و مادرها مسـؤولانه تر برفرزندان خود نظارت داشته باشند. اینترنت محدود به مرزها نیست. اعتیاد به اینترنت هم نمی‌تواند محدود به کشورها باشد. ویروس‌های مجـازی حـد و مـرز نمی‌شناسـند، بیماری‌های مجازی نیز چنین‌اند. چقدر پیش می‌آید که پیش از دیسـکانکت شدن به خود بگویید فقط چند دقیقه دیگر؟ هنگام شلوغی خطوط، چقدر تلاش می‌کنید تا به اینترنت وصل شـوید؟ تا چه حدی اتصال به اینترنت را از دیگران مخفی می‌کنید؟ کانکت بودن را چقدر به بیرون رفتن ترجیح می‌دهید؟ نکند شما معتاد هستید؟!

بعد از ده – پانزده سـال مطالعه روانشناسـان بر روی عواقب اسـتفاده زیاد از اینترنت، مثلاً درباره موضوعاتی مثـل اعتیاد اینترنتی، حـالا هفته نامه نیوساینتیست نتیجه کار پژوهشگران در رشته‌های مختلف روانشناسی را تحت عنوان «هشت بیماری اینترنتی» منتشر کرده است:

عنوان اولین بیماری «جسـتجوی خود» اسـت. ایـن بیماری برخی از مردم و احتمالاً، بسـیاری از جماعت روشنفکر و روزنامه‌نگار را شامل می شود. ظاهراً مبتلایان به این بیماری دائم در اینترنت دنبال اسم خودشان می‌گردند. اینکه چند نفر و از کجا به وبلاگ یا سایتشـان لینک داده‌اند، برای آنها بسیار مهم اسـت و مدام کنتور سایتشان را چک می‌کنند و احتمـالاً از کمبود یـا افزایـش بازدیدکنندگان دچار اسـترس می‌شوند. «خود افشاگری وبلاگی» مسـأله دیگری است که محققان آن را یک بیماری خوانده‌انـد. گروهـی از مردم رازها و اسـراری را که معمولاً شـخصی و خصوصی قلمداد می‌شود، روی وبلاگ‌هایشان افشـا می‌کنند که دامنه‌اش از عکس‌های خصوصی گرفتـه تا روابط خصوصی امتداد دارد. اینترنت گردی از همه جا، گوگل‌بازی مفـرط، اعتیاد بـه ویکی پدیا، آشـغال جمع کنی اینترنتی، دلبسـتگی به آلبوم عکس افراد ناشـناس و خود بیمار پنداری اینترنتی، نام بقیه بیماری‌های اینترنتی اسـت که ممکن است نصیب وبگردهای حرفه‌ای شود.

اعتیاد به اینترنت در سال اولیه چندان جدی گرفته نمی‌شد ولی با رشد روزافزون مبتلایان، رسماً به عنوان یک اعتیاد معرفی شد و در بعضی کشورها، کلینیک‌های مخصوصی برای درمان مبتلایان به این نوع اعتیاد دایر گشت. از جمله این کشورها می‌توان به چین، آمریکا و آلمان اشاره کرد که به علت تعداد زیاد کاربران اینترنت، دارای بیشترین معتادان به اینترنت هستند. آلمان با حدود ۳۰ میلیون کاربر بیش از یک میلیون معتاد به اینترنت دارد یا در چین از ۹۴ میلیون کاربری که از اینترنت استفاده می‌کنند، ۵/۲ میلیون نفر به اینترنت معتادند

آینه خودشناسی

یک‌روز وقتی کارمندان به اداره رسیدند، اطلاعیه بزرگی را در تابلوی اعلانات دیدند که روی آن نوشته شده بود: «دیروز فردی که مانع پیشرفت شما در این اداره بود، درگذشت. شما را به شرکت در مراسم تشییع جنازه که ساعت ۱۰ در سالن اجتماعات برگزار می‌شود، دعوت می‌کنیم.»

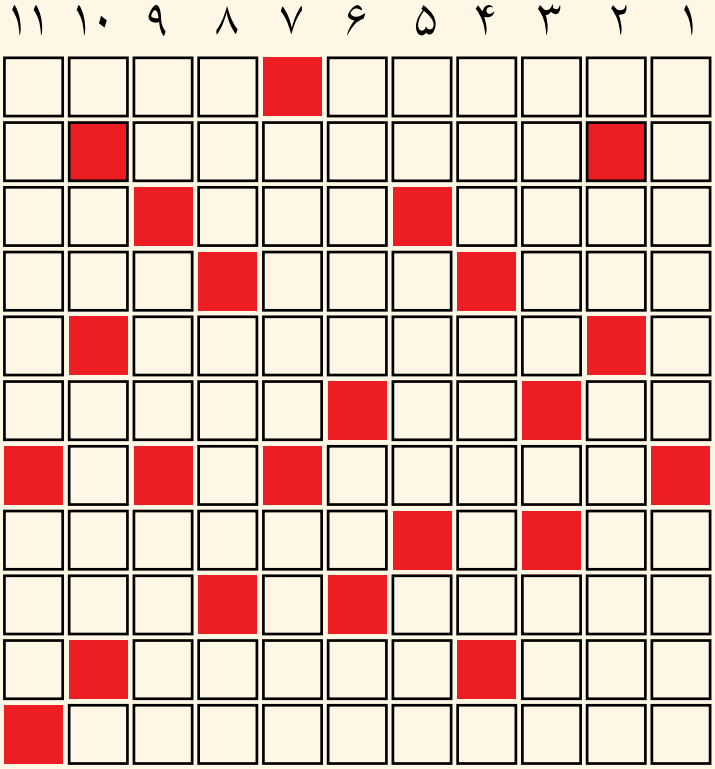
در ابتدا همه از دریافت خبر مرگ یکی از همکارانشان ناراحت شدند اما پس از مدتی کنجکاو شدند که بدانند کسی که مانع پیشرفت آنها در اداره می‌شده که بوده است.

این کنجکاوی تقریباً تمام کارمندان را ساعت ۱۰ به سالن اجتماعات کشاند. رفته‌رفته که جمعیت زیاد می‌شد، هیجان هم بالا می‌رفت. همه پیش خود فکر می‌کردند: این فرد چه کسی بود که مانع پیشرفت ما در اداره بود؟ به هر حال خوب شد که مرد!

کارمندان در صفی قرار گرفتند و یکی‌یکی نزدیک تابوت می‌رفتند و وقتی به درون تابوت نگاه می‌کردند، ناگهان خشکشان می‌زد و زبانشان بند می‌آمد.

آینه‌ای درون تابوت قرار داده شده بود و هر که به درون تابوت نگاه می‌کرد، تصویر خود را می‌دید. نوشته‌ای نیز بدین مضمون در کنار آینه بود: «تنها یک نفر وجود دارد که می‌تواند مانع رشد شما شود و او هم کسی نیست جز خود شما. شما تنها کسی هستید که می‌توانید زندگی‌تان را متحول کنید. شما تنها کسی هستید که می‌توانید بر روی شادی‌ها، تصورات و موفقیت‌هایتان اثرگذار باشید. شما تنها کسی هستید که می‌توانید به خودتان کمک کنید. زندگی شما وقتی که رئیستان، دوستانتان، والدینتان، شریک زندگی‌تان یا محل کارتان تغییر می‌کند، دستخوش تغییر نمی‌شود. زندگی شما تنها فقط وقتی تغییر می‌کند که شما تغییر کنید، باورهای محدودکننده خود را کنار بگذارید و باور کنید که شما تنها کسی هستید که مسؤول زندگی خودتان می‌باشید. مهم‌ترین رابطه‌ای که در زندگی می‌توانید داشته باشید، رابطه با خودتان است. خودتان را امتحان کنید. مواظب خودتان باشید. از مشکلات، غیرممکن‌ها و چیزهای از دست داده نهراسید. خودتان و واقعیت‌های زندگی خودتان را بسازید. دنیا مثل آینه است. انعکاس افکاری که فرد قویاً به آنها اعتقاد دارد را به او باز می‌گرداند. تفاوت‌ها در روش نگاه کردن به زندگی است.»

جدول رمیس



افقی:

۱- برنامه Resco Photo Viewer برای تلفن همراه، نقش کدام نرم‌افزار رایانه را ایفا می‌کند؟- نام برادر شخصیت اصلی بازی شاهزاده ایرانی

۲- مرکز رسیدگی به شکایات مرتبط با جرایم اینترنتی

۳- گیاهی است یک‌ساله یا دوساله که بیشتر به عنوان علوفه برای دام استفاده می‌شود- یکی از بزرگ‌ترین بوکسورهای جهان که تغییر مذهب داده و مسلمان شد- پوسته گرافیکی

۴- ارزش و قیمت هر چیزی- از شهرهای استان فارس- کوزه

۵- به تعداد نقطه‌های رنگی صفحه نمایش اشاره دارد

۶- خط‌کش مهندسی- جنس مذکر- تلاش و کوشش

۷- دستگاه ضبط و پخش صدا و تصویر

۸- من و تو- یک IDE بسیار قدرتمند و خوش‌دست است که اکثر فناوری‌ها را پشتیبانی می‌کند

۹- از لوازم جانبی کامپیوتر که امکان انتقال تصاویر و متن‌ها را به آن فراهم می‌کند - از حیوانات دونده

۱۰- از بانک‌های دولتی- رئیس و فرمانده

۱۱- هم‌سان بودن رزولوشن ویندوز با رزولوشن مانیتور در چه چیزی مؤثر است؟

عمودی:

۱- نرم‌افزاری برای بوت از طریق فلش ممووری- از فیلم‌های دیجیتالی محبوب

۲- از میوه‌های معطر- نوعی پورت

۳- ناگزیر به انجام کاری- از سوره‌های قرآن کریم

۴- از لبنیات- محلی برای نگهداری محکومان و متهمان

۵- بنیاد و پایه هرچیزی- با عجله و شتابان کاری را انجام دادن- نوعی خاک سخت

۶- به هر نقطه در صفحه نمایش می‌گویند- درخت زبان گنجشک- گوشت به زبان ترکی

۷- خواندن و قرائت کردن- هر بیتی که شاعر نام خود را در آن آورد

۸- قسمتی از دستگاه گوارش- صبور و بردبار- از ضمایر اشاره

۹- از حروف ندا- مجلسی که اعضای آن بزرگان و اعیان کشور باشند- کمک و همراهی

۱۰- از کلیدهای صفحه کلید- نوعی سبزی خوراکی معطر

۱۱- ابزار ویرایشگر متن باز محصولی از Activestate- عمل بزرگ‌نمایی روی عکس

cisco

سیسکو را آسان بیاموزید

دوره های تخصصی سیسکو و سیستم عامل

> CCNA, CCDA
> CCNP, CCDP
> Routing & Switching, CCIE 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. NETCCV

jump to CISCO right now!

REMIS

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 ۸۸۹۱۹۳ فکس: ۸۸۹۳۳۹۷۲ و ۸۸۹۱۹۵۳۸

training@remisco.com

www.remisco.com

REMIS

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 سربداران، شماره ۲۸

تلفن: ۸۸۹۲۵۸۰۸ فکس: ۸۸۹۳۶۰۶۸

www.remisco.com info@remisco.com