رویداد

الزام مخابرات به رعایت سهم PAPها از بازار

■ **تلنا:** مصوبه شورای رقابت مبنی بر تعیین سهم مخابرات از خدمات مشترک با PAPها لازم‌الاجرا بوده و در صورت تخلف از آن طبق قانون فعالیت مخابرات در آن حوزه متوقف خواهد شد. جمشید پژویان در این‌باره بیان کرد، از سوی دیگر برای حمایت از بخش خصوصی و شرکت‌های ندا حوزه فعالیت مخابرات در برخی استان‌ها را محدود کرده تا بتوانند سهم خود از بازار اینترنت را به حدی برسانند که این ارتباط و سهم حفظ شود. رییس شورای رقابت ادامه داد: نبود دستورالعمل در نحوه ارایه خدمات میان بخش خصوصی و مخابرات ایران، به خصوص مخابرات استانی باعث شد برای سرعت بخشیدن به گسترش دایره فعالیت‌شان و کسب درآمد در برخی از استان‌ها برای بخش خصوصی محدودیت‌هایی ایجاد کنند. به گفته وی وظیفه شورای رقابت جلوگیری از تمرکز و ایجاد انحصار در بازار است و نبود تمرکز در بازار اینترنت و سرعت پایین رشد آن در میان مردم نیز به دلیل رقابت نادرست میان بخش خصوصی و مخابرات است چرا که اگر اجازه رشد سریع به بخش خصوصی داده می‌شد تمرکز بر این بازار نیز بیشتر می‌شد.

مدیرعامل شرکت مخابرات:

موافق مصوبات شورای رقابت نیستیم

■ **نود آی‌سی‌تی:** به گفته مدیرعامل شرکت مخابرات هنوز مصوبه محدود شدن فعالیت مخابرات به میزان ۱۰ درصد در جاهایی که شرکت‌های PAP در آنجا حضور دارند، توسط شورای رقابت به ما ابلاغ نشده است. صابر فیضی، در این‌باره گفت: از آنجا که هنوز این موضوع به ما ابلاغ نشده و از جزییات آن اطلاع نداریم فعلا نمی‌توانیم اظهار نظری در این خصوص بکنیم. وی ادامه داد: براساس قانون مصوبات شورای رقابت لازم‌الاجراست و ما هم به قانون تمکین می‌کنیم اما قطعا موافق این موضوع نیستیم و موضوع را پس از ابلاغ رسمی قطعا پیگیری خواهیم کرد. وی افزود: نکته ظریفی در مصوبه شورای رقابت وجود دارد و آن هم اینکه مخابرات در جاهایی که شرکت‌های PAP حضور ندارند، می‌تواند سهم بیشتری از بازار داشته باشد. وی بیان کرد اینکه چرا PAPها در مناطق محروم اقدام به ارایه سرویس نمی‌کنند به دلیل نبود صرفه اقتصادی است که قطعا این مساله شامل مخابرات هم می‌شود و این موضوع را حتما با شورای رقابت طرح و پیگیری می‌کنیم.

استفاده از ای میل خارجی برای مشتریان درعملیات بانکی و بیمه‌ای ممنوع شد

ای‌میل ملی در مسیر اجباری شدن

حامد شفیعی

وزیر ارتباطات و فناوری اطلاعات در دو نامه جداگانه بیمه‌ها و بانک‌های کشور را به استفاده از شبکه ملی اطلاعات ملزم کرد. رضا تقی‌پور در نامه‌ای به وزیر امور اقتصاد و امور دارایی نوشت: «با توجه به ماده ۶ قانون برنامه پنجم توسعه این وزارت مکلف به ایجاد شبکه ملی اطلاعات در کشور است. در این راستا ضروری است دستور فرمایید تمامی بیمه‌ها اعم از دولتی و غیردولتی نسبت به اقدام موارد زیر اقدام لازم را به عمل آورند: ۱- استفاده از پسوند دامنه کشوری «Ir.» در تمامی وب‌سایت‌ها و پورتال‌ها اجباری است. بدیهی است استفاده از پسوندهای عمومی نظیر «org.»، «com» و... برای بیمه‌ها به عنوان پسوند اصلی ممنوع است و درصورت ثبت دامنه‌های فوق باید به دامنه اصلی با پسوند ir. منتقل شود. ۲- ضروری است میزبانی پورتال‌ها و وب‌سایت‌های فوق در داخل انجام گیرد و مدیران وب‌سایت‌ها و پورتال‌ها با مراجعه به سایت ثبت دامنه کشوری (www.nic.ir) علاوه بر ثبت nsهای اینترنتی نسبت به ثبت nsهای اینترانتی اقدام کنند. ۳- لازم به ذکر است در صورتی که میزبانی وب‌سایت‌ها و پورتال‌های فوق به صورت داخلی و توسط بیمه انجام می‌شود لازم است نسبت به اتصال مرکز داده خود به شبکه ملی اطلاعات از طریق لینک اینترنتی اقدام کنند. ۴- مسوولان فناوری اطلاعات بیمه‌ها به منظور کسب اطلاعات بیشتر می‌توانند به سازمان فناوری اطلاعات ایران (معاونت توسعه و مدیریت شبکه) مراجعه کنند. پیش از این نیز رضا تقی‌پور وزیر ارتباطات و فناوری اطلاعات با ارسال نامه‌ای به محمود بهمنی رییس کل بانک مرکزی، استفاده از ای‌میل‌های عمومی و ای‌میل‌های با میزبانی خارجی از جمله Hotmail، Gmail، Yahoo و MSN را در مراودات بانکی مشتریان ممنوع اعلام کرد. بر اساس این گزارش تقی‌پور در این نامه خواستار ممنوعیت قبول ای‌میل‌های عمومی و خارجی در هنگام افتتاح حساب و نیز عدم ارسال صورت‌حساب‌های بانکی مشتریان به این ای‌میل‌ها شده و پیشنهاد داده وسیله‌ای مهیا شود که مشتریان بانک‌ها در صورت نداشتن ای‌میل داخلی بتوانند در همان بانک، پای اینترنت برای خود ای‌میل داخلی بسازند. این نامه‌ها در حالی از سوی وزیر ارتباطات و فناوری اطلاعات به رییس کل بانک مرکزی و وزیر اقتصاد و دارایی ارسال می‌شود که پیشتر مسوولان این وزارتخانه و همچنین رییس سازمان پدافند غیرعامل از جاسوسی بودن خدمات شرکت‌هایی مانند گوگل و یاهو خبر داده بودند. آنها همچنین در توجیه عدم دسترسی کاربران به برخی خدمات این سایت‌ها بیان کرده بودند که به دلیل شیطنت‌هایی که بعضا این شرکت‌ها انجام می‌دهند، ما باید مراقب کاربران ایرانی باشیم. بنا بر اظهارات کارشناسان این اقدامات پس از ماجرای افشای اسرار خصوصی حساب‌های بانکی میلیون‌ها ایرانی قوت گرفته و تلاشی است تا سازمان‌ها و ادارات دولتی ملزم به استفاده از شبکه ملی اطلاعات شوند. به گفته سعید مهدیون مدیرعامل شرکت فناوری اطلاعات ایران اینکه تمام اطلاعات خود را از طریق سایت‌هایی مثل yahoo و google در اختیار خارجی‌ها بگذاریم یا اینکه اطلاعات خود را برای ثبت در سایت‌های داخلی بدون اعتماد قرار دهیم، اصلا خوب نیست. حتی اگر کیفیت سرویس داخلی کم است، باید به آن اعتماد کنیم تا کیفیت با استفاده از آن بالا برود. وزیر ارتباطات و فناوری اطلاعات نیز بر این عقیده است نباید برای مبادله اطلاعات داخلی، هم هزینه بالاتری را بپردازیم و هم ناامنی را تحمل کنیم، باید آن مقدار از اطلاعاتی که گردش آن در داخل است از طریق شبکه ملی اطلاعات انجام شود. پیش از این مسوولان سازمان فناوری اطلاعات گفته بودند استفاده از پست الکترونیکی داخلی برای کارکنان و مسوولان وزارتخانه‌ها، سازمان‌ها، شرکت‌ها و... اجباری خواهد بود اما خبری از کاربران عادی نبود. در این راستا خبرآنلاین با طرح این پرسش که مگر بانک‌ها چه اطلاعاتی را قرار است به ای‌میل مشتریان خود بفرستند که مشتریان حتما باید ای‌میل داخلی داشته باشند؟ می‌نویسد: در حالت موجود اغلب بانک‌ها در صورت درخواست مشتری برای فعال کردن خدمات بانکداری الکترونیک یا اینترنت بانک، تنها اطلاعات رسید پرداخت، مانند پرداخت قبض‌ها یا جابه‌جایی به حساب دیگر را به مشتری اطلاع می‌دهند که آن هم تنها جنبه اطلاع به مشتری را دارد. بنابراین این سوال باقی می‌ماند که چرا باید مشتریان ای‌میل داخلی داشته باشند؟ سعید مهدیون در پاسخ به این پرسش بیان می‌کند امنیت پست الکترونیکی ملی به مراتب بالاتر از سرویس‌های خارجی است چرا که حداقل اطلاعات حیاتی و عمومی کاربران در داخل قرار دارد. او همچنین اعتقاد دارد که حتی اگر این سرویس ملی امن نباشد باید به آن اطمینان کرد تا با گذشت زمان به استاندارد لازم برسد و در صورت استفاده کاربران از این سامانه، اطلاعات موجود در پست الکترونیکی آنها به خارج از کشور منتقل نمی‌شود. در حالی مسوولان سازمان فناوری اطلاعات درباره امن بودن ای‌میل ملی نسبت به ای‌میل‌های خارجی تاکید دارند، که باید گفت این پست الکترونیکی فاقد گواهینامه امنیتی بین‌المللی است. دسترسی دهها میلیون کاربر ایرانی اینترنت که برای ارتباطات مجازی خود، از سرویس‌دهنده‌های خارجی مانند گوگل و یاهو استفاده می‌کنند، حال در صورت چنین عملی از سوی بانک‌ها، مراکز بیمه مساله حقوق شهروندی را به میان می‌آورند. هر چند به گفته مسوولان این کار در راستای امنیت اطلاعات رد و بدل‌شده میان بانک و مشتریان صورت می‌گیرد. اما نکته اینجاست که برای ثبت‌نام در این سرویس شخصی‌ترین اطلاعات کاربران نظیر کد ملی، آدرس دقیق پستی، شماره تلفن ثابت و همراه از متقاضیان دریافت می‌شود. هر چند استفاده از ای‌میل ملی تنها برای جابه‌جایی داده‌های میان بانک‌ها و مشتریان مورد استفاده قرار گیرد، اما ضریب امنیتی پایین و احتمال مورد سوءاستفاده و مورد حمله قرار گرفتن اطلاعات کاربران شک و تردیدهایی را مبنی بر استفاده از این خدمات برای کاربران به وجود می‌آورد. از این رو دولت باید در این زمینه تضمین‌های لازم امنیتی را به کاربران و حتی بانک‌ها درخصوص حفظ اسرار ارایه دهد و صرف اجباری شدن استفاده از ای‌میل ملی برای رد و بدل کردن اطلاعات میان بانک و مشتریان کافی نیست.

دیدگاه

باید با «گوگل» مذاکره کرد؟

محمود اروجزاده*: پیداست اقدام گوگل بدون فعل و انفعالات پشت پرده و لابی‌های گسترده سیاسی انجام نشده که با اندکی فشار احساساتی در فضای وب، به‌راحتی بازگشت‌پذیر باشد. در پی بروز تنش‌های اخیر میان کشورمان با برخی همسایگان جنوبی، دامنه این بحث و جدل‌ها از عرصه سیاست به حوزه مجازی نیز کشیده شده، که البته امری طبیعی است، چرا که امروزه فضای مجازی در عمل، کم و بیش بازتابی از فضای عمومی جوامع را نشان می‌دهد. در این میان شاید مهم‌ترین اتفاق، اقدامی است که گوگل صورت داد و علی‌الظاهر برای پا پس کشیدن از دنیای سیاست، نام خلیج‌فارس را در نقشه جهانی خود حذف کرد. فضای وب فارسی هم (به ویژه شامل شبکه‌های اجتماعی) واکنش نشان داده و می‌دهد، عکس‌العملی که به‌خودی خود غیرطبیعی نیست، هر چند البته در کارگر بودن آن چندان تضمینی نیست، چراکه پیداست اقدام گوگل بدون فعل و انفعالات پشت پرده و لابی‌های گسترده سیاسی انجام نشده که با اندکی فشار احساساتی در فضای وب، به‌راحتی بازگشت‌پذیر باشد. اگر بخواهیم مانند همیشه، راه‌حل مساله را به یک موج احساسی سطحی تقلیل دهیم و به فکر حل و فصل مهندسی آن نباشیم، البته تکلیف معلوم است و چیزی هم تغییر نخواهد کرد. اما اگر تجربه جدیدی را پیش رو قرار می‌دهیم که علاقه‌مندیم به راه‌حلی معقول‌تر (و البته مسوولانه‌تر) ختم شود، بهتر است کمی متفاوت نگاه کنیم. به راستی چه راه‌های متفاوتی می‌توان یافت؟ یک راه جالب و البته کاملا تازه مقابل روی ماست: «تعامل و مذاکره.» چطور؟ خیلی ساده، جملات زیر را بخوانید: «...این شورا یک فرادستگاه است و فراقوه دیده شده است تا بتواند ساماندهی حاکمیتی را در این حوزه بر عهده گیرد. اکنون نهادهای جدیدی در سطح بین‌المللی در حال شکل‌گیری است، گوگل نهادی مثل فیفاست. در مملکت تعریف شده که چه کسی باید با فیفا صحبت کند... مثلا می‌خواهیم با گوگل تعامل کنیم، چه کسی تعامل کند؟ کارهایی است که در سطح فراقوه‌ای و در سطح ملی در معنای دقیق کلمه است. به طور مثال می‌خواهیم به گوگل بگوییم من یک کلمه‌ای را جست‌وجو می‌کنم اول این نتایج را نشان نده، این نتایج در فرهنگ ما زیاد کاربرد ندارد یا چیز خوبی نیست...» اینها بخشی از سخنان حجت‌الاسلام حمید شهریاری است که در مقام عضو حقیقی (و عملا از بازیگران اصلی) نهاد تازه‌تاسیس «شورای‌عالی فضای مجازی» در گفت‌وگو با هفته‌نامه «عصرارتباط» گفته است. به طور کامل مشخص است که از این پس در فضای مجازی و به‌طور کلی مدیریت صنعت فناوری اطلاعات و ارتباطات، مفهومی به عنوان «مذاکره در عرصه بین‌المللی» گنجانیده خواهد شد که مسوولیت آن هم با شورای جدید است. نکته جالب‌تر در این میان، مثال ایشان است که کاملا با حال و هوا و نیاز فعلی ما منطبق است. از طرف دیگر، اگر نتوان با گوگل در زمینه موضوع تاریخی مشخص و مستندی مانند خلیج‌فارس مذاکره کرد، طبعا حساب مذاکره درباره فیلترینگ نتایج جست‌وجو، از اساس منتفی خواهد بود. بنابراین ظاهرا راه‌حل مورد نظر ما ابهامی ندارد؛ راهکار که معلوم، دستگاه مسوول هم که مشخص (و کاملا هم داوطلب این کار) است.

***مدیرمسوول پایگاه خبری ایتنا**

گذرگاه

نکته‌های پنهان از چشمان مدیران

گلنوش عامری*

■ در برخی موارد بدون آگاهی و ناخواسته، بسیاری از حوزه‌های فناوری اطلاعات به همدستان مجرمان اینترنتی تبدیل شده‌اند. این نوشتار روش‌های متعددی را که حوزه‌های فناوری اطلاعات جرایم اینترنتی را فعال می‌کنند توضیح می‌دهد و راه‌حل‌هایی برای جلوگیری از این خطر ارایه می‌کند. مقاله ارایه‌شده درباره راهکارهایی است که امروزه در ایجاد جرایم اینترنتی نقش دارند و بر اساس تحقیقاتی که توسط متخصصان و محققان کسپرسکی انجام شده، راه‌حل‌هایی برای توقف این جرایم پیشنهاد می‌کند.

فرض اینکه اطلاعات در مرکز داده (data center) هستند: چه لزومی دارد که برای تقویت مرکز داده با پرداخت هزینه و زمان زیاد از فناوری‌هایی مانند Authentication، مدیریت دسترسی، فایروال، جلوگیری از نفوذ شبکه و غیره استفاده شود؟ بیان این مطلب به معنای بی‌اهمیت بودن این فناوری‌ها نیست. به طور قطع آنها از اهمیت بالایی برخوردارند، اما ما احتیاج داریم بر بخشی که اطلاعات در آن متمرکز شده است تمرکز کنیم؛ و این یعنی کاربر نهایی. کاربر نهایی یک تهدید جدی در زمینه از دست دادن داده‌هاست. تحقیقات IDC نیز نشانگر این است که در جهان نوین سایبری، بیشترین هزینه‌ها بابت جابه‌جا شدن اطلاعات پرداخته می‌شود که نشانگر این است که میزان داده‌های بیرون از پایگاه‌های داده سازمان‌ها، بسیار زیاد شده است.

عدم به رسمیت شناختن ارزش داده‌های گوشی تلفن همراه: زمانی که یک دستگاه گم می‌شود یا به سرقت می‌رود، شرکت بیمه تنها بهای بطری خالی را می‌پردازد نه محتویات آن را، بدون توجه به اینکه این محتویات تا چه حد اهمیت دارند. به همین دلیل، راهکارهای حفاظتی روی گوشی بیشتر هم‌تراز قیمت گوشی است تا ارزش داده‌های داخل آن. در حالی که واقعیت این است که در اغلب مواقع ارزش اطلاعات داخل تلفن همراه از ارزش خود تلفن بسیار بیشتر است.

با لپ‌تاپ‌ها و دستگاه‌های موبایل مانند دارایی‌هایی از شرکت برخورد کنید که هرگز نباید از آنها برای موارد شخصی استفاده شود. اعتقاد داشته باشید که اطلاعات شرکت هیچ راهی برای ورود به سیستم‌های شخصی نخواهند یافت.

قبول رسانه‌های اجتماعی بدون محافظت: شبکه‌های اجتماعی آمده‌اند که بمانند! رسانه‌های اجتماعی و فناوری‌های وب، اگر به صورت ایمن استفاده شوند، می‌توانند به بالا بردن بهره‌وری سازمان کمک کنند و سازمان را به سمت بازدهی بیشتر سوق دهند. تمرکز ما باید روی این موضوع باشد که چگونه می‌توان سازمان‌ها را به استفاده از رسانه‌های اجتماعی با رویکردی امن تشویق کرد.

تمرکز بر محافظت مقابل شناسایی و پاسخ: در نظر گرفتن طرح‌های جامع امنیتی قابلیت‌های متعددی را در‌ گیر می‌کند. این قابلیت‌های بنیادی محافظت، شناسایی و پاسخ است. محصولات آنتی‌ویروس اغلب نادیده گرفته می‌شوند و با آنها تنها به عنوان یک کالا که هر سال تمدید می‌شود برخورد می‌شده و در نتیجه قابلیت‌های شناسایی و پاسخ نیز نادیده گرفته می‌شود.

عدم ترویج فرهنگ آگاهی: آگاهی و آموزش به کاربر نهایی در تمام مراحل و سطوح امنیت داده‌ها امری ضروری است. آگاهی از تهدیدات، اثر و روش تکثیر آنها، به هوشیاری کاربران کمک می‌کند و از گرفتن تصمیمات نادرست توسط کاربر که باعث آلودگی سیستم می‌شود، جلوگیری می‌کند.

گزارش‌های نقض امنیت: گزارش‌های نادرست به شرکت‌ها این باور غلط را می‌دهد که تهدیدات ناشی از نرم‌افزارهای مخرب و رشد مجرمان اینترنتی کاهش یافته است. اما واقعیت این است که تهدیدات بیش از ۲۳ درصد افزایش یافته‌اند، ولی به دلیل کامل گزارش نشدن سرقت اطلاعات که در هر روز اتفاق می‌افتد، FBI قادر به ارایه گزارش دقیق نیست. این در حالی است که شرکت‌ها از آگاهی درباره این سرقت‌ها، چگونگی انجام آنها و راه‌های مقابله با آنها در موارد مشابه، سود بیشتری خواهند برد.

الگوهای امنیتی: پیروی از مقررات و امنیت فناوری اطلاعات همیشه هم‌معنی نیستند. شما همیشه می‌توانید از یکسری مقررات وضع‌شده پیروی کنید و در عین حال همیشه در مقابل تهدیدات ایمن نباشید. بسیاری از سازمان‌ها به محافظت در مقابل بدافزارها تنها به چشم یک بخش برای چک کردن نگاه می‌کنند. صرف پیروی از مقررات، اغلب یک روش «بالا به پایین» است. امنیت زمانی که به درستی پیاده‌سازی شود یک رویکرد «پایین به بالا» است. زمانی که شما در حال طراحی یک نرم‌افزار یا معماری جدید برای شبکه سازمان خود هستید باید عناصر امنیتی را در نظر بگیرید. همان‌طور زمانی که در حال طراحی یک نرم‌افزار تغییرات احتمالی بعدی را در نظر می‌گیرید، در استفاده از عناصر امنیت نیز باید این نکته را در نظر بگیرید که شبکه در طول مدت گسترش، باید مورد بازبینی مداوم قرار گیرد.

فرض اینکه همه چیز خوب است: اگرچه ممکن است سیستم‌ها ضدگلوله باشند، اما در نهایت انسان‌ها از این سیستم‌ها استفاده می‌کنند. در بسیاری از موارد مشکلات در نتیجه عناصر انسانی مانند اشتباهات ساده، فقدان دانش لازم و آموزش کافی به وجود می‌آید. کارکنان یک شرکت باید درباره مدیریت اطلاعات، مانند چگونگی رفتار درست در شرایط خاص، چگونگی پیروی از سیاست‌های شرکت و چگونگی جلوگیری از بدافزارها آموزش ببینند و نگاهی دقیق بر رویدادهای امنیتی احتمالی در شرکت خود داشته باشند. همه چیز خوب نیست. همه ما می‌توانیم راه‌های بیشتری برای جلوگیری از سرقت اطلاعات مهم خود پیدا کنیم.

***کارشناس فنی پارس آتنا دژ**

بازیکده

شاهان وارد بازی می‌شوند

مجید نوردوست: Game of Thrones یک عنوان فانتزی نقش‌آفرینی است که بر پایه خشونت ساخته شده است؛ بازی‌ای که از روی سریال تلویزیونی و کتابی با همین نام در حال ساخت است. در همان نگاه اول، می‌توان به این موضوع پی برد که ساختار اصلی بازی همانند The Witcher 2 است. شخصیت اصلی بازی، ماجرایی همانند گرالت (Geralt) دارد و ریشه‌های زیادی از المان‌های آن بازی در GoT دیده می‌شود. سازندگان بازی، بیشتر کتاب این عنوان را در نظر گرفته‌اند که توسط جورج مارتین (George R. R Martin) نوشته شده است. شخصیت‌های بازی نیز با توجه به سریال این عنوان شناخته شده‌اند تا اینکه آنها برای بازیکنان آشنا باشند و جذابیت بیشتری به بازی ببخشند. آقای سیلویا سچی (Sylvian Sechi) که طراح ارشد بازی است، در صحبت‌هایی به این موضوع اشاره می‌کند که: «ما روی این موضوع فکر کرده بودیم که چه کار کنیم شخصیت‌های بازی همانند کتاب به نظر برسند و سریال نیز تا حدود زیادی به آن چیزی که ما در نظر داشتیم، شبیه بود و المان‌های کلیدی را در خود داشت. ما هم تصمیم گرفتیم که همین المان‌های کلیدی را در بازی خود استفاده کنیم.» تا اینجای کار مشخص شده که سازندگان بازی سعی کرده‌اند رابطه بین شخصیت‌های بازی به همان شکل مرموزی باشد که در کتاب نوشته شده است. این بازی دو قهرمان جدید در خودش دارد که به نوعی با ساختار و زیربنای کتاب هم ارتباط دارند و داستان خاص خودشان را دنبال می‌کنند. حضور دو شخصیت در این بازی باعث شده که دو حالت مختلف را در گیم‌پلی شاهد باشیم و روابط داستانی زیادی را بین آنها مشاهده کنیم. داستان بازی در بین مراحل مختلف، قسمت‌های بسیار هیجان‌انگیزی را در بردارد و در قسمت‌های مختلف قطع می‌شود و با روایت داستان دیگری از بازی، حس جالبی در آن به وجود آورده است. بازی بیش از ۳۰ ساعت گیم‌پلی خواهد داشت و بازیکنان در آن با یک ماجراجویی بسیار خوب مواجه می‌شوند. در بخش گیم‌پلی بازی شاهد ارتقای قدرت‌های شخصیت‌های بازی خواهید بود. دو شخصیت موجود در این بازی می‌توانند قدرت‌ها و قابلیت‌هایشان را تقویت کنند. یک سیستم هوشمند برای این قسمت طراحی شده که بتوانید شخصیت‌های بسیار قدرتمندی را در این بازی خلق کنید. همچنین یک تعادل بسیار خوب هم بین این دو شخصیت برقرار شده است. دو شخصیت بازی که مورس (Mors) و آلستر (Alester) نام دارند، دارای خصوصیت‌های مختلفی هستند. داستان اصلی این عنوان که در کتاب به آن توجه خاصی شده، بر وجود جادو و استفاده از آن توجه زیادی داشته و به همین دلیل شخصیت‌های بازی نیز از این قدرت‌ها برخوردار هستند. همچنین در صحبت‌ها و رابطه‌هایی که در بازی وجود دارد، حالت‌های مختلف طراحی شده است. انتخاب دیالوگ‌ها باعث می‌شود که بتوانید خود را به عنوان یک فرد وفادار یا احمق جلوه دهید! دیالوگ‌ها باعث می‌شود که روند اکشن بازی نیز تغییر کند. سازندگان بازی درباره این موضوع می‌گویند: «سری Mass Effect یکی از الگوهای ما برای این کار بود. این بازی به شکلی بسیار خوب با انتخاب دیالوگ‌ها روند اکشن و شکل بازی را تغییر می‌داد. همچنین ما این بازی را بسیار دوست داریم. البته ما

نمی‌خواستیم روند بازی همانند ME دارای دو نوع دیالوگ خوب و بد باشد، اما شکل دیالوگ‌ها را به صورتی انتخاب کردیم که بازیکنان بتوانند تصمیم‌های جالبی در بازی بگیرند. آقای توماس وکلین (Thomas Veauclin) مدیر پروژه Game of Thrones نیز به این موضوع اشاره می‌کند: «باید به بازیکنان اجازه داد تا بتوانند با روند گیم‌پلی بازی ارتباط برقرار کنند و انتخاب‌های آنها به صورتی باشد که بازی بتواند به شکل مستقیم جواب آن انتخاب‌ها را بدهد که آزادی بازیکنان را نمی‌گیرند، چرا که ما این را نمی‌خواستیم.» استودیوی بازی‌سازی Cyanide تمام تمرکزش را روی این موضوع گذاشته که شخصیت‌های معروف دنیای Game of Thrones به شکل خوبی در بازی پیاده‌سازی شوند. باید تا لحظه عرضه بازی منتظر ماند و دید که آیا این بازی می‌تواند به یک عنوان موفق تبدیل شود یا خیر.

جمهوری اسلامی ایران
وزارت امور اقتصادی و دارائی
گمرک ایران
اداره کل خدمات و تدارکات

آگهی مناقصه عام یک مرحله‌ای
تامین خودروهای استیجاری مورد نیاز گمرک ایران

گمرک جمهوری اسلامی ایران در نظر دارد نسبت به تامین خودروهای استیجاری مورد نیاز خود جهت انجام امور اداری و ماموریتهای درون شهری و برون شهری از طریق مناقصه عام یک مرحله ای به شرح ذیل اقدام نماید:

۱- موضوع مناقصه: تامین خودروهای استیجاری مورد نیاز گمرک ایران

۲- نوع تضمین: شرکت در مناقصه به صورت ضمانتنامه معتبر بانکی یا واریز وجه نقد به شماره حساب ۳۷۰۳۰ بنام گمرک جمهوری اسلامی ایران نزد بانک مرکزی جمهوری اسلامی ایران و ارائه فیش بانکی مربوطه

۳- مبلغ تضمین: ۱۵۰/۰۰۰/۰۰۰ ریال (صد و پنجاه میلیون ریال)

۴- مهلت دریافت اسناد مناقصه توسط مناقصه گران: پس از انتشار نوبت دوم آگهی حداکثر به مدت ۷ روز از ساعت ۸/۳۰ صبح الی ۱۴/۳۰ بعدازظهر

۵- مهلت تحویل پاکات پیشنهادات: حداکثر ۱۰ روز پس از آخرین مهلت دریافت اسناد مناقصه توسط مناقصه گران از ساعت ۸/۳۰ صبح الی ۱۴/۳۰ بعدازظهر

۶- زمان بازگشایی پاکات: در اسناد مناقصه ذکر خواهد گردید.

۷- نشانی مناقصه گزار جهت دریافت اسناد مناقصه و تحویل پاکات پیشنهادات: تهران بالاتر از میدان ولیعصر - جنب کوچه ناصر - ساختمان مرکزی گمرک جمهوری اسلامی ایران طبقه اول اداره کل خدمات و تدارکات - اتاق ۴۰۱ - اداره امور قراردادها و مناقصات

لذا از کلیه شرکتهای واجد شرایط که دارای مجوز مرتبط با موضوع مناقصه از مراجع ذیصلاح در زمینه حمل و نقل می باشند دعوت می گردد جهت دریافت اسناد مناقصه به نشانی یاد شده مراجعه نمایند مناقصه گران می توانند جهت کسب اطلاعات بیشتر به آدرس www.irica.gov.ir و پایگاه ملی اطلاع رسانی مناقصات مراجعه و یا با شماره تلفن ۸۲۹۹۲۳۶۹ تماس حاصل نمایند.

اداره کل خدمات و تدارکات گمرک جمهوری اسلامی ایران
اداره امور قراردادها و مناقصات

۵۲۹

سازمان آگهی‌های روزنامه شرق
تلفنی آگهی می‌پذیرد.

۸۸۶۵۸۵۷۵
۸۸۵۲۴۹۷۴
۸۸۷۵۲۴۹۳
۸۸۷۵۲۱۵۹

صندوق تامین اجتماعی

آقای دکتر محمودرضا سرزعیم
پزشک متخصص جراحی عمومی
پلی کلینیک امیدیه استان خوزستان

نظر به اینکه پرونده اتهامی شما در هیات بدوی رسیدگی به تخلفات اداری شماره ۲ صندوق تامین اجتماعی مورد رسیدگی و منتج به صدور رای قابل پژوهش شماره ۶۰۵ مورخ ۹۰/۱۲/۱۵ مبنی بر اخراج از خدمت از صندوق گردیده، لذا بدینوسیله مراتب قانونا به شما ابلاغ می گردد. بدیهی است در صورت داشتن اعتراض به رای صادره از تاریخ انتشار این آگهی حداکثر یک ماه مهلت دارید تا اعتراضیه خود را به اداره کل امور اداری صندوق واقع در تهران خیابان آزادی پلاک ۳۴۵ تسلیم و یا به نشانی تهران صندوق پستی ۱۵۷۵-۱۳۴۴۵ ارسال نمائید در غیر این صورت به استناد تبصره یک ماده ۴ قانون تخلفات اداری رای مذکور قطعیت یافته و لازم الاجرا خواهد بود.

صندوق تامین اجتماعی

۵۵۸