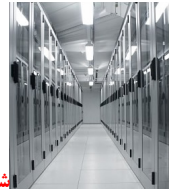


مصاحبه <<= دیتاستری ایرانی که امن است



شماره : 1
تاریخ : 25 شهریور ماه 1387

وقتی صحبت از امنیت اطلاعات می شود، به ناچاه نگاهها متوجه مکان هایی می شود که این مراکز در آنجا نگهداری می شوند. حال اگر این قصد داشته باشیم این اطلاعات را بر روی شبکه اینترنت منتقل کنیم مراکز داده IDC خود را نشان خواهد داد و بالطبع حفظ امنیت در این مراکز از اهمیت به سزایی برخوردار خواهد بود. بر این اساس بی ربط ندیدیم اگر در این شماره که به بحث امنیت پرداخته ایم به سراغ یکی از این IDC های ایرانی برویم و از امنیت در آن مکان جو با سویم. در این مصاحبه که در دفتر امامی یکی از مدیران شرکت پارس آنلاین و با حضور ایشان برگزار شد، روبروی ما حسین لطفی، مدیر جوان IDC این شرکت نشسته بود، مدیری که در عین جوانی دارای تجربه فنی و مدیریتی بسیار زیاد در این زمینه است.

• مطمئناً بارها به سیوال چرا هاستینگ در ایران پاسخ داده اید، یک بار دیگر به این سیوال از دید امنیتی جواب دهید.

اول باید به این نکته توجه کنیم که ما هر چه شبکه را محدودتر کنیم امنیت بیشتر است، یعنی اگر اطلاعات شما در ایران استفاده می شود، اگر مسیر دسترسی به اطلاعات را محدود به کشور ایران کنیم، چون مسیر کمتر است، و از گره های کمتری رد می شود امنیت بیشتر حفظ می شود. شما در صورتی که در خارج کشور هاست کنید فقط برای وارد کردن نام کاربری و رمز باید این اطلاعات را بر روی بسته ای به خارج کشور بفرستید و خدا می داند که این اطلاعات از چه مسیری می رود و در این مسیر چه اتفاقاتی می تواند برای این اطلاعات بیفتد، اما در صورت وجود دیتاستر و شبکه مطمئن داخلی این اطلاعات نیازی به رفت و برگشت به خارج کشور ندارد. مساله دیگر تایید هویت است. بسیاری از حمله ها بخاطر این است که کسی خودش را به جای شما جا می کند و بارها دامنه های .com بسیاری به همین علت از دست کاربران خارج شده است ولی همین حمله ها بر روی دامین .ir یا اتفاق نمی افتد و یا در صورت وقوع با مراجعه حضوری به سرعت قابل رفع شدن است.

این مساله بارها در مساله هاستینگ رخ می دهد و به راحتی در ایران برای مشتری ایرانی قابل پیگیری استنکته دیگر اینکه همه هاستینگ هایی که در خارج کشور وجود دارد، پیشرفته نیست، دارای محیط مناسب برای هاستینگ نیست، شاید بسیاری مسایل امنیتی در آنجا رعایت نمی شود. امروزه به خاطر مسایل تحریم بسیاری از هاستینگ هایی که ایران سرویس می دهند در کشور خودشان جزو بهترین ها نیستند و حتی برخی از آنها خدمات خود را به قیمت های ارزان تری ارائه می کنند و این برای مشتری ایرانی جذاب است در صورتی که مسایل امنیتی در آنها رعایت نمی شود، اما شما می توانید به راحتی با دیتاستر پارس آنلاین آشنا شوید. ساختمان این مجموعه را که اصولاً فقط به این منظور طراحی شده را ببینید، با تدابیر به کار رفته امنیتی و تجهیزات مورد استفاده در آن آشنا شوید و ...

• نقش مراکز داده در امنیت چیست؟

در جواب سیوال شما من باید نکته ای را خدمتان عرض کنم. ما امروزه با بسیاری سازمان ها در حال فرهنگ سازی هستیم که مزایای هاستینگ در داخل کشور را به آنها توضیح دهیم. در مورد خصوصی ها این انتخاب بین ایران و خارج است و در بین دولتی ها که موظف شده اند در داخل کشور هاست کنند، هم 2 انتخاب وجود دارد، ساختن یک دیتاستر و یا استفاده از دیتاسترهای موجود در کشور. در جریان این فرهنگ سازی متوجه شده ایم که تقسیم وظایف در زمینه امنیتی به خوبی تبیین نشده و ما در حال حاضر یکی از فعالیت هایی که انجام می دهیم تشریح امنیت و وظیفه هر کدام از عناصر در آن است. در بحث امنیت هر روزه می بینیم که سردمداران امنیتی دنیا هر روزه مورد آسیب قرار می گیرند و این نشان دهنده این است که امنیت صد درصدی وجود ندارد ولی ما تلاش می کنیم اقداماتی که خود انجام داده ایم و مزایای هاستینگ در داخل را توضیح دهیم و به آنها بگوییم در این بخشی که وظیفه امنیت بر عهده ماست، تا چه میزان کار آیی دارد. بخشی

از تامین امنیت بر عهده شبکه حامل اطلاعات و بخشی دیگر بر عهده فرد استفاده کننده از آن اطلاعات است.

اگر کار صد درصد توسط دیتاستر انجام شود، یعنی پیاده سازی، اجرا و نگهداری توسط دیتاستر است و مشتری فقط کاربر است، سهم عظیمی از امنیت بر عهده دیتاستر است. اما اگر دیتاستر فقط فضا را در اختیار مشتری قرار دهد، و مواردی چون collocate داشته باشیم، در این صورت امنیت آن بیشتر بر عهده مشتری خواهد بود. اما در این صورت هم ما مشتری را تنها نمی گذاریم. ما تجربه خودمان را در این صورت در اختیار مشتری می گذاریم و به نحوی آنها را مورد پشتیبانی فنی قرار می دهیم. به نحوی که برخی از قطعات فنی که در پارس آنلاین وجود دارد تمامی دیتاهای موجود را مورد پشتیبانی قرار می دهد در صورتی که اجرا و راه اندازی این دستگاهها به صورت منفرد هزینه بسیار گزافی را بر مشتری تحمیل می کند.

نکته ای را هم لازم می دانم که متذکر شوم که دیدگاه ما نسبت به امنیت باید به روز باشد. متأسفانه این مساله در بسیاری از دیتاستر و یا سرور رومهایی که برخی از شرکت های دولتی به صورت مجزا تشکیل داده اند مشاهده می شود. یعنی طی یک بودجه تعدادی سرور خریداری می شود و حتی برخی تجهیزات و یا نرم افزارهای امنیتی را خریداری کرده اند. این مدیران به تجهیزات امنیتی مانند سرور نگاه می کنند که تا زمانی که فن دستگاه کار کند، نیازی به هزینه ندارد ولی در زمینه مسایل امنیتی باید به روز باشیم و بخش زیادی از تجهیزات امنیتی هر روز نیاز به به روز رسانی دارد. سیستمی که امروز ایمن است، فرداً حتماً امن نیست.

• حال که جایگاه دیتاستر در امنیت مشخص شد، سیوال دیگری پیش می آید: امنیت در یک دیتاستر چگونه تامین می گردد؟

ما وقتی از یک دیتاستر صحبت می کنیم، 2 بحث مطرح است، امنیت فیزیکی و امنیت شبکه ای. از بحث امنیت فیزیکی آغاز می کنیم. ساختمان دیتاستر پارس آنلاین با هدف کاربری دیتاستر ساخته شده است و با دیدگاه های امنیتی ساخته شده است. در ساخت آن موانع امنیتی پیش بینی شده است. در طراحی آن ما این مساله را پیش بینی کرده ایم که به هر قسمت چه کسانی اجازه تردد دارند و پیش بینی شده که هر کسی نتواند به بخش دیگر وارد شود.

در این ساختمان ما سه منطقه امنیتی داریم و موانع خود ساختمان مانند یک دژ مستحکم منطقه مرکزی را درون خود قرار داده است. منطقه صفر وقتی است که با فرد غیر آشنا طرفیم، مثل وقتی که در سالن آمفی تاتری که در آنجا وجود دارد، برنامه ای در حال اجرا باشد. پرسنل پارس آنلاین اجازه ورود به منطقه 1 را دارند و منطقه 2 که سرورها در آنجا وجود دارند برای بخشی از پرسنل فراهم شده است. جالب اینجاست که این منطقه 7 متر زیر زمین قرار دارد. تازه در آنجا هم منطقه بندی و سگمنت بندی شده است و برای مثال فردی که به تجهیزات ماهواره ای دسترسی دارد، به منطقه دیگر اجازه ورود ندارد. این مساله حتی در بسیاری از دیتاسترهای مطرح رعایت نشده است. دستگاه کنترل دسترسی را از نوع ایرانی انتخاب کرده ایم اما برنامه ای ویژه برای آن درخواست کرده ایم که مثلاً اگر در سایت اتفاقی بیافتد اقداماتی خاص انجام می پذیرد. این دستگاه به صورت SMS، بلوتوث و ... قابلیت ارسال پیام به مدیران حراست و مدیران بخش را دارد.

در این دستگاه چینش دروازه ها به صورتی تعریف شده است که کسی که می تواند مثلاً به اتاق X دسترسی داشته باشد از درهای 1 و 2 و 3 می تواند رد شود و کسی که به اتاق Y امکان دسترسی دارد از درهای 1 و 2 و 4 می تواند رد شود و این فرد امکان رد شدن از در 3 را ندارد و نفر قبلی هم امکان رد شدن از در 4 را ندارد. یا مثلاً ملاقات شونده ساعت ملاقات دارد و بیش از آن امکان ماندن در مجموعه را ندارد و بعد از مدتی کارت، کلید دیگر کار نمی کند. مقاومت ساختمان از نکات جالب فیزیکی ساختمان است و تونلی جاذب شوک دورتادور ساختمان کنده شده و ساختمان را بغل کرده است. کاربرد این تونل به این منظور است که اگر شوکی لرزه ای در اطراف ساختمان اتفاق بیافتد، این شوک باید بسیار قوی باشد تا به سازه برسد چون تونل جاذب شوک بخش زیادی از قدرت آن شوک را به خود جذب می کند و مانع صدمه دیدن ساختمان می شود. سازه ضد زلزله هم طراحی شده است.

البته ساختمان به قدری مقاوم طراحی شده است که توان تحمل دیش 7 متری که در پشت بام مجموعه قرار است نصب شود را داشته باشد. در بخش امنیت فیزیکی ساختمان موانع شما می توانند در 2 نوع نظارتی و حفاظتی باشند، در این دیتاستر حتی از پیشرفته ترین ابزار حفاظتی با نام ایرلاک هم استفاده شده است. این ابزار به جز این که بدون حضور مامور

امنیتی شما را از لحاظ وسایل چک می کند، از لحاظ وزنی هم شما را چک می کند تا مبادا قطعه‌ای با خود به بیرون برده باشید.

• بخش دیگر امنیت، امنیت شبکه‌ای است، پارس آنلاین چه تمهیداتی برای این بخش سنجیده است؟

امنیت در بخش شبکه‌ای هم 2 قسمت است. یک بخش بخش تحلیل اطلاعات و دیگری فایروال‌ها. یک فایروال موجود بی شعوری است که ترافیک‌ها را به 2 بخش محدود و آزاد غربال می کند. اما همین ترافیک‌های آزاد هستند که سر سیستم بلا می آورند. باید شما خوب و بد ترافیک را مشخص کنید. یک گاری را که وارد یک شهر می شود برای شما مثال می زنم، شما صد تا هم دروازه برای این شهر در نظر بگیرید، تا کسی محصول داخل گاری را زیر و رو نکند این گاری به راحتی از تمام دروازه‌ها عبور می کند. شما باید در جایی داخل بسته‌ها را تحلیل کنید. در بسیاری موارد شما چند دروازه می گذارید به علت اینکه اگر یکی تعدادی از فایل‌های بد را تشخیص داد، دیگری بقیه را مجدداً بررسی کند و تعداد دیگری را تشخیص دهد. یک بار دیگر اشاره می کنم اینها مربوط به فایل‌هایی هستند که برچسب دارند و هنوز بسیاری از تهدیدات امنیتی به عنوان فایل آزاد وارد شده‌اند.

اطلاعات وارد دیتاستر ما که می شود از چند مرحله غربال (فایروال) رد می شود که این تعداد مراحل بستگی به اهمیت اطلاعات و نحوه مشتری و قرارداد فی مابین دارد. بعد بسته اطلاعاتی وارد بلوکی می شود که داخل بسته‌ها را باز می کند و این دیوایس اطلاعات را تحلیل می کند. این دیوایس‌ها به IPS و IDS معروف هستند. مثلاً یکی از روش‌های کار این دستگاه نمره دهی است. یعنی به یک بسته و یا یک IP بسته به رفتاری که انجام می دهد نمره داده می شود و به واسطه دریافت نمره‌های منفی حلقه محاصره تنگ تر می شود. جالب است بدانید که یک 24 ساعت یکی از IPSها حدود 1 میلیون تحدید امنیتی از بین حدود 685 میلیون بسته وارد شده به دیتاستر ما را شناسایی می کند و اینگونه نیست که ما اینجا نشسته باشیم و بی کار باشیم. بعضی از دستگاه‌های ما در روز بارها باید به روز رسانی شوند تا اطلاعات روز، حمله‌های روز را داشته باشند تا بتوانند در مقابل آنها مقاومت نمایند.

• خوب با همین فایروال و IPS امنیت شبکه تامین شد، یعنی دستگاه‌های دیگری هم دارید؟

خیر تازه اطلاعات جدا شدند. شما برای انتقال بعضی اطلاعات نیاز به رمزنگاری دارید، پس دستگاه رمزنگار نیاز دارید. یک سری سیستم‌های تایید هویت نیاز دارید که برای این کار به کلیدها و توکن‌ها نیاز دارید. یک سری نمونه‌گیر از بسته نیاز دارید. برای جرم‌شناسی نیاز به یک سری کپی برداری و رکورد کردن از اطلاعات دارید. یکی از بلوک‌ها هم برای تحلیل داده‌های drop شده است. و یا سیستم‌هایی که برای کنترل و پیدا کردن وجه اشتراک تحدیدات امنیتی کاربرد دارند. تمام اتفاقات تا اینجا برای این است که اتفاقی نیفتد، حالا اگر افتاد چه کارهایی می توانید انجام دهید. برای این مرحله مثلاً backup گیری را داریم، اما وقتی شما اطلاعات یک بانک و یا بیمه را دارید، backup یعنی اطلاعات روز قبل و یا حتی ساعت قبل که این یعنی فاجعه. ما برای این کار به سراغ راه‌حل‌ها و امکاناتی رفتیم که بتوانیم اطلاعات فقط آن ناحیه آسیب دیده را بازگردانیم که داستان آن هم مفصل است و در حوصله این مصاحبه نمی گنجد.

منبع : خبرگزاری ایتنا