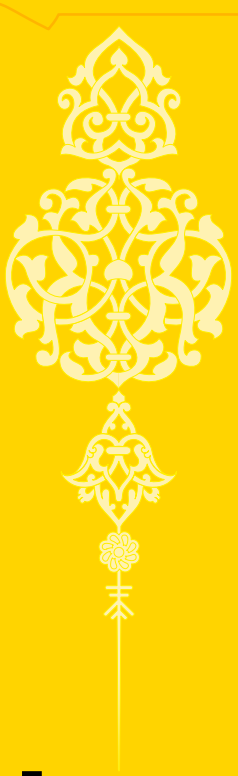
بسم الله الرحمن الرحیم



دیده‌بان فناوری

ماهنامه اقتصاد و مدیریت فناوری اطلاعات

سال اول .شماره اول . اسفند ۱۳۹۳

سال اول | شماره اول | اسفند ماه ۱۳۹۳
FEBRUARY 2015
ماهنامه اقتصاد و مدیریت فناوری اطلاعات | ۱۲ هزار تومان

گفتگو با دکتر غلامرضا جلالی
سند چشم‌انداز را بازنگری کرده‌ایم

میزگرد فعالان حوزه آموزش آی‌تی
تعریف مشاغل آی‌تی در کشورمان صحیح نیست

گفتگو با مهندس مسیح قائمیان
نباید از اهمیت شبکه‌های اجتماعی در بانکداری غافل شویم

دیدبان فناوری

پرونده‌ای برای شروع چهارمین دوره هیئت مدیره سازمان نصر

این سیمرغ نتوانست سیمرغ شود

ماهنامه اقتصاد و مدیریت فناوری اطلاعات
اسفندماه ۱۳۹۳ | سال اول | شماره اول

فهرست | CONTENTS

FEBRUARY 2015 | VOL01 | NO.01

Monthly Magazine

شناسنامه
WHO WE ARE

Monthly Magazine

۱

صاحب‌امتیاز و مدیر مسئول این نشریه **علیرضا صالحی** است که سردبیری را نیز بر عهده دارد. این نشریه در هلدینگ رسانه‌ای دیده‌بان تهیه و آماده‌سازی می‌شود که مدیر برنامه‌ریزی و ارتباطات آن **فریبا یاراحمدی** است.

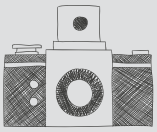
۲

چشم‌نوازی صفحات این ماهنامه حاصل ذوق **حمیدرضا جواهری** به‌عنوان مدیر هنری است

۳

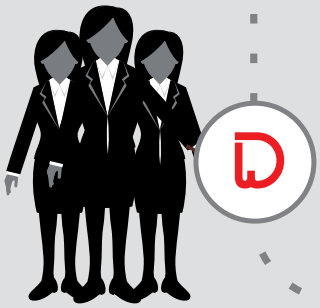
علیرضا اورعی نیز در کنار او کارهای صفحه‌آرایی و گرافیک را انجام داده است.

۴



عکس‌های خوب این شماره، حاصل نگاه **عماد دولتی** از لنز دوربین است.

۵



مسئولیت هماهنگی‌ها و درواقع روابط عمومی نشریه با **فاطمه رضوی** بوده که به مدد آن توانسته‌ایم حجم مناسبی از گفتگو و میز گرد را برای شماره نخست گرد هم بیاوریم. **فاطمه یحیایی** نیز با وی در این کار همکاری داشته است. پاکیزگی مناسب و ویراستاری را مدیون **سودابه محمدپور** هستیم و **ارشاد نیکخواه** به همراه **حسین رسولی** نیز ترجمه مطالب را انجام داده‌اند.

همچنین باید در این شماره تشکر ویژه داشته باشیم از سید محمدحسن مقدم‌فر و سادینا آبایی که بدون یاری ایشان، قطعاً برخی گفتگوهای جذاب را از دست می‌دادیم. همچنین مدیون صبر و حوصله و شکیبایی این عزیزان هم هستیم: غلامرضا جلالی، امیرحسین سعیدی نائینی، حسین سرکانی، علی حکیم جوادی، مسیح قائمیان، فریبا مهدیون، محمد گرکانی نژاد، کاظم آیت‌اللهی، مازیار گنجه‌ای، عطاءا... همایون، هومن تصدیقی و مجید امینی. دیگر اینکه عباس چیتگری نظارت چاپ این شماره از دیده‌بان فناوری را بر عهده داشته و بقیه کارهای دفتری از جمله هماهنگی، بخش اشتراک و تدارکات را **مهرنوش کاوه** و **علی‌اکبر محمودی** انجام داده‌اند.

دیده‌بان فناوری در نشانی تهران، **سهروردی شمالی، کوچه حاج حسنی، شماره ۵۵، طبقه اول**، آماده‌سازی می‌شود که با تلفن ۸۸۷۴۹۴۱۰ در دسترس است و این شماره از نشریه در چاپخانه خاتم با شماره تلفن ۸۸۹۱۰۷۶۹ منتشر شده است.

اگر برای این نشریه می‌خواهید ایمیل ارسال کنید از نشانی info@dfe.ir استفاده کنید. دیده‌بان فناوری همانند همه نشریات هم از اسپانسری استقبال می‌کند و هم از اشتراک و خرید نشریه. برای مورد نخست شماره ۸۸۷۴۹۴۱۴ پاسخگو است و برای دومی شماره تلفن ۸۸۷۴۹۴۱۰ و ضمن آنکه فرم اشتراک هم در صفحه ۱۷ آمده است.

ما آمده‌ایم برای یادآوری آن که فناوری صنعت است...

علیرضا صالحی
salehi@dfe.ir

نگاه مرد مسافر به روی میز افتاد
«چه سیب های قشنگی!
حیات نشئه تنهایی ست.»
و میزبان پرسید:
قشنگ یعنی چه؟
قشنگ یعنی تعبیر عاشقانه اشکال
و عشق، تنها عشق
ترا به گرمی یک سیب می کند مانوس... *

حکایت فرهنگ و نشر و مطبوعات، در کشـورمان از جنس عشق است. کاری است که بی عشق نه می آید و نه می پاید.
فرهنگ سازی در این زمانه که کاری است دشوار و نشـریه کاغذی در آوردن که از آن هم سخت‌تر است، وقتی با هم ترکیب شوند، احتمالا چیزی می شود از جنس همین دیده بان فناوری که شماره نخست آن اکنون در دست شماست.
دیده‌بان فناوری داعیه آن دارد که می‌خواهد نخستین نشریه تخصصی باشد که از اقتصاد و مدیریت فناوری اطلاعات حرف می‌زند. پس همه را دعوت می کنیم در این خوان گسترده، کنار ما باشند تا شاید بتوانیم با همدیگر از صنعت بزرگی به‌نام فناوری اطلاعات بنویسیم؛ بگوییم و بخوانیم.
پس تعجب نکنید اگر در این نشریه از نوآوری در بانکداری الکترونیکی سخن بگوییم یا از دریچه امنیت به مدیریت فناوری نگاه کنیم.
پس عجیب نخواهد بود اگر به واشکافی ایران در افق ۱۴۰۴ بپردازیم و در کنار آن از بزرگ داده ها که متحول کننده دنیای ما خواهند بود صحبت کنیم. و تعجبی نخواهد داشت که در این نشریه به همه حوزه های مدیریت سرک بکشیم تا تاثیر آن ها را در اقتصاد فناوری اطلاعات ببینیم.
سینما، کشاورزی،خودرو،سلامت،آموزش و ... همه و همه را می‌توانید در دیده‌بان فناوری ببینید و البته با دیدگاه اقتصاد و مدیریت.
و سرخوشـانه تکرار می کنیم که دیده‌بان فناوری از نشر همه دیدگاه‌ها و سلیقه‌ها نه تنها استقبال که دفاع می کند.

* شعر از سهراب سپهری

Monthly Magazine
FEBRUARY 2015 | VOL 01 | NO. 01

InfoSecurity
امنیت اطلاعات

تغییر نگاه به امنیت سازمانی

گفت‌وگو با دکتر سردار غلامرضا جلالی

سند پدافند سایبری را بازنگری کرده‌ایم

با دکتر سردار غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور برای دومین بار به گفتگو می‌نشینیم. بار نخست سال قبل تر بود با مرور یک سال افتای ایرانی. این بار اما پس از برگزاری موفق هفته پدافند غیرعامل و عبور سازمان از ده سالگی گفتگویی دیگر داریم. نگاه فرهنگ محور جلالی در کنار تلاش برای نفوذ پدافند غیرعامل در همه ارکان تصمیم گیری و تصمیم سازی کشور ستودنی و جالب است. از پدافند غیرعامل شروع کردیم و به بحث جنگ سایبری و الزامات دفاع سایبری رسیدیم و اینکه تجربه چهار سال اخیر در تدوین سند پدافند سایبری کشور، سازمان را به این نتیجه رسانده که باید خیلی سریع تر با روند تحولات جلو برود. بازنگری این سند یکی از اقدامات مهم امسال هم بوده است.

گام اساسی دیگری که برداشتیم، شناسایی اقلام اساسی فضای سایبر یا پدافند سایبری است و گام بعد، سیاست‌گذاری، برنامه‌ریزی، هدایت و راهبری تولید داخل کشور آن‌ها با رویکرد استفاده از شرکت‌های دانش بنیان و بخش خصوصی است

■ لطفا برای شروع بفرمایید که امسال در هفته پدافند غیر عامل چه اتفاقاتی افتاد و بعد درباره پدافند سایبری صحبت کنیم.

هدف ما از مباحث برگزاری هفته پدافند غیر عامل بیشتر ترویج اهداف و فرهنگ‌سازی در این زمینه است. در این برنامه‌ها که این دومین سال برگزاری آن بود، سعی کردیم تا به این اهداف دست یابیم. امسال یک رویکرد جدید با عنوان پدافند تخصصی یا پدافند متناسب با تهدیدات جدید در این همایش داشتیم، چون امسال یازدهمین سالگرد تشکیل سازمان پدافند غیر عامل کشور است و ما از یک دهه عبور کرده‌ایم. در این یک دهه فرایندهایی را دنبال کردیم و امروز به این نتیجه قطعی رسیدیم که از امسال باید یک تغییر رویکرد کلان در این موضوع داشته باشیم.

به این خاطر که احساس کردیم تهدیدات در حال تنوع و تغییر به لحاظ ماهیتی هستند وبر اساس صحبت های تدابیر مقام معظم رهبری، ایشان هم معتقد نیستند که تهدید نظامی تهدید اول کشور است و معتقدند تهدید نظامی مقداری از کشور دور شده و در اولویت بندی جای خود را به تهدیدات جدیدتری داده است؛ البته نه این که از بین رفته باشد. در واقع ما نتایجی که از مطالعات روی استراتژی و دکترین امریکایی‌ها علیه خودمان استنتاج می کنیم و جهتی که آن‌ها می‌روند، رویکردهای دشمن را دسته بندی کرده و از این طریق استراتژی تهدیدگر را تعیین بررسی می کنیم. کار ما در پدافند غیرعامل بنا به فرمایش رهبر معظم انقلاب اسلامی ، حذف اثر تهدید بر کشور است.

به گفته ایشان پدافند غیرعامل مثل مصونیت بخشی به بدن انسان است و این یعنی اگر دشمن تلاش کند هیچ اثری از اعمالش اقداماتش نبیند و اگر تهدیدش را عملی کند ما باید کاری کنیم که این تهدید اثری نداشته باشد.

این اثر نکردن یا آسیب ناپذیرسازی کشور اگر بخواهد تعریف عملیاتی شود، ممکن است سه سطح آسیب را بتوان برای آن تعریف کرد: آسیب ناپذیری برای بالاترین سطح، حداقل آسیب پذیری در سطح پایین تر و آسیب پذیری نسبی را در سطحی دیگر که با این نگاه، تهدیدشناسی، محور ما می‌شود و بعد از آن باید ببینیم که رویکردهای پدافند غیر عامل ما چه باشد.

■ شما این تهدیدات را چگونه دسته بندی می کنید؟

ما به طور عمومی تهدید را به سه دسته تقسیم کردیم: دسته اول، تهدیدهای سخت یا نظامی که در این موضوع مقوله امنیتی و نظامی باهم دیده می‌شوند و شامل ۴ یا ۵ تهدید را در برمی گیرند. دسته دوم، تهدیدات مردم محور که طی آن حدود ۴ نوع تهدید با اهداف غایی اثرگذاری بر مردم را شناسایی کرده‌ایم و محور کلی آن این گونه است: اول این که اجازه ندهد مردم همراه جمهوری اسلامی باشند، دوم بی‌تفاوت کردن مردم به نظام، سوم رودررویی مردم و نظام و چهارم قرار دادن مردم در کنار خود برای براندازی نظام.

بستر این تهدید مردم هستند اما ابزار آن می‌تواند متفاوت باشد؛ مثمثلا در جایی تهدید نرم و تهدید اقتصادی است و جایی تهدید زیستی و بیولوژی یک و یا چیزهای دیگر.

دسته سوم، تهدیدات فناوری محورند که این فناوری‌ها در کنار خدمت، می‌توانند تهدید هم محسوب شوند و بنا به شرایط و موضوعات مختلف متفاوت‌اند و می توانند تغییر هم بکنند مثلا در ۱۹۹۵ حوزه سایبر به جنگ اطلاعات شناخته می‌شد و امروزه ما چیزی به اسم جنگ سایبری را به عنوان یک تهدید جدی داریم. تهدیدات زیستی، تهدیدات الکترومغناطیس و تهدیدات کل حوزه فناوری در این بخش جای می گیرند.

از سوی دیگر از انتظارات رهبری این است که مصون‌سازی در این حوزه در کل پیکره یا همان کالبد و زیرساخت‌های کشور سپس در جامعه و میان مردم و بعد از آن در دستگاه‌های اجرایی اتفاق بیفتد.

رهبری از ما می‌خواهد که در این سه حوزه اثر تهدید را به صفر برسانیم. وانگهی تهدیدها را چه دسته‌بندی می کنیم و چه روبه‌روی هم قرار می‌دهیم، خروجی ما به سمت دو رویکرد عملیاتی و رویکرد بنیادی یا غیر عملیاتی است.

■ نحوه مواجهه با این تهدیدات چگونه است؟ مثلا ایجاد قرارگاه و غیره.

ما دو رویکرد عملیاتی و بنیادین داریم.

در رویکرد عملیاتی، چهار حوزه قرارگاه پدافند سایبری، قرارگاه پدافند زیستی، قرارگاه پدافند شیمیایی و قرارگاه پدافند پرتوی را داریم که اگر اتفاقی در کشور بیافتد باید در آن‌ها اقدام عملیاتی صورت بگیرد. بر فرض ما کشور هسته‌ای هستیم و ممکن است زیرساخت ما نشت پیدا کند یا به هر دلیلی با آلودگی هسته‌ای مواجه شویم و در آن هنگاما باید توان مدیریت آن شرایط را داشته باشیم.

ما کشور صنعتی هستیم و زیرساخت‌های

شیمیایی زیادی داریم البته منظور این نیست که بمباران شیمیایی برای کشور اتفاق بیفتد اما مثلاً ممکن است یک کارخانه شیمیایی نشت پیدا کند یا کپسول‌های کلری که برای تصفیه آب به کار می‌برند، نشت پیدا کنند کمااین که چنین موضوعی چندوقت پیش هم اتفاق افتاده بود و یا اتفاقی مثل آنچه که در زاهدان یا عسلویه روی داده بود. ما باید توانایی کنترل تمام پیامدهای چنین حوادثی اعم از مراحل درمان و همه شرایط جاری بر اثر آن اتفاق را داشته باشیم.

حوزه زیستی هم بسیار وسیع است و بر فرض امروز که ابولا و کرونا تمام دنیا را تهدید می‌کند، کشور ما باید آمادگی رو در رویی و تحقیق و مبارزه با این شرایط را داشته باشد.

در حوزه بنیادی، یک پدافند کالبدی یا فنی مهندسی داریم که یعنی ما چگونه باید اثر تهدید را بر کالبد کشور حذف کنیم. این جا رویکرد کلا فنی، مهندسی و صنعتی است. دومین پدافند، مردم‌محور است که در کشورهایی مثل لهستان هم طبق مطالعات ما پدافندی به اسم civilian passive defenses یعنی پدافند غیرعامل مردمی دارند.

ما ۶ ماموریت اساسی برای این پدافند تعریف کردیم شامل چگونگی حفظ، صیانت، اداره، تامین نیازمندی‌های مردم و حفاظت از مردم در برابر هر حادثه و یک بند به عنوان حفظ انسجام حکومت و مردم که در واقع رویکردی اساسی است نیز در آن گنجانده‌ایم. این به آن مفهوم است که با رویکردی مردم محور نسبت به بی اثر کردن اثر تهدیدات به مردم اقدام نمود

■ پدافند در حوزه اقتصادی چگونه معنا پیدا می کند؟

بحث دیگر ما پدافند اقتصادی است. طبق گفته رهبری معظم انقلاب ما درگیر یک جنگ تمام عیار اقتصادی هستیم؛ لذا یک جنگ اقتصادی، دفاع اقتصادی می‌طلبد.

شاید این جا قدری با اقتصاد مقاومتی زاویه داشته باشیم چون ما صرفاً در حوزه پدافند و دفاع متمرکز می‌شویم و ممکن است که در عرصه اقتصادی مثلاً افزایش کارآمدی و چیزهایی از این دست که رهبری معظم به آن اشاره داشتند نیز اضافه شود؛ لذا ما با کمی دقت و با حذف جایگزین واژه مقاومتی آن را پدافند اقتصادی نامیدیم چون بخشی از آن کاملاً مربوط به ما می‌شود؛ مثلاً حفظ ذخایر اقلام اساسی مردم، حفظ ذخیره انرژی، دو کارکردی کردن تولید برق و آب و مباحث زیربنایی حوزه اقتصادی و یا حفاظت از سبد کالای مردم تا تهدیدات اقتصادی بر آن

ساختار دفاع سایبری را از پایین ترین تا بالاترین سطح معماری کردیم که این کار تقریباً جدیدی بود که ما ببینیم در کجا به چه ساختاری نیاز داریم

سند جدید پدافند سایبری

در گام دوم بر اساس این نگاه، سند پدافند سایبری را تولید و با پشتوانه علمی آن نظریه، سند راهبردی و چشم‌اندازها و رویکردهای‌مان را تعریف کردیم. این سند را طی جلساتی با حضور ۳۰۰ نفر از کارشناسان این حوزه و آقای انتظاری، دبیر شورای فضای مجازی که آن زمان عضو کمیسیون امنیت فضای سایبر شورای عالی امنیت ملی بود، طی نشستی پنج روزه در هتل گاجره پس از بحث‌های خوب علمی و دقیق و دو جلسه تلفیق و ویرایش ایجاد کردیم. پس از آن ساختار دفاع سایبری را از پایین ترین تا بالاترین سطح معماری کردیم که این کار تقریباً جدیدی بود که ما ببینیم در کجا به چه ساختاری نیاز داریم.

در گام چهارم، ما یک‌سری سخت‌افزار و نرم‌افزار، یعنی سامانه اصلی در فضای سایبری داریم که دارای ارزش اساسی هستند و فونداسیون و ستون این فضا را شکل می‌دهند و لذا ما این‌ها را شناسایی کردیم که تقریبا حدود ۲۰ تا ۲۵ سامانه شدند.

ما در سندمان به این نتیجه رسیدیم که نیازمند یک صنعت پدافند سایبری بومی هستیم و این هم بحث‌های مختلفی اعم از این که چگونه و توسط چه کسانی و مسایلی از این دست را شامل می‌شد.

ما مصوبات این طرح را جمع‌بندی کرده و به وزیر دفاع از طریق ستاد کل نیروهای مسلح ابلاغ کردیم و مبنای آن را در وزارت دفاع گذاشتیم و البته تاکید داشتیم که منظور ما تصدی گری نیست و چیزهایی را باید خودمان تولید کنیم و چیزهایی هم باید حمایت شوند و در واقع این جلساتی که در وزارت علوم برگزار می‌شود و مشارکت در داخل و رقابت با خارج که قبلا برعکس آن رایج بود، باید انجام شود. خلاصه این که ما این ۲۵ قلم را در لیست تولید داخلی گذاشتیم و برای آن سالانه اعتبار تعیین کردیم و اکنون نزدیک چهار سال است که ما مورد به مورد محصولات را وارد این مکانیزم کرده و حمایت و تولید می‌کنیم و این‌ها بعد از کنترل و ارزیابی امنیتی به عنوان محصولی ملی معرفی و از آن‌ها استفاده می‌شود که این مقوله درهرحال اعتبار زیادی هم از ما می‌گیرد و لیست آن نیز موجود است. مثلاً در سخت‌افزارها سوییچ روتر از محصولاتی است که روی آن‌ها کار کردیم و بخش‌هایی از آن‌ها به نتیجه رسیده و بخش‌هایی نیز در حال تست است، مثل زبرافزار و چیزهایی از این دست. اگر نخواهم وارد جزییات شوم گام اساسی دیگری که برداشتیم، شناسایی اقلام اساسی فضای سایبر یا پدافند سایبری است و گام بعد، سیاست‌گذاری، برنامه‌ریزی، هدایت و راهبری تولید داخل کشور آن‌ها با رویکرد استفاده از شرکت‌های دانش بنیان و بخش خصوصی است که این هم یک رویکرد دایمی است که در طول چهار سال ادامه داده‌ایم و سقف اعتبار و موضوعات را هم بیشتر کرده‌ایم و از آن حمایت می‌کنیم تا در کشور به کار گرفته شوند. یکی از بخش‌هایی که دنبال می‌کردیم، طرح پدافندی یا طرح عملیات دفاعی است که تعریف وضعیت سفید، زرد، نارنجی و قرمز داشته باشد و در هر وضعیتی تعیین تکلیف شود که رییس و مرئوس کیست و وظایف هر کسی معلوم شود و در واقع بخشی از همان معماری دفاعی و تعیین وضعیت‌ها بود که این هم نهایی شد و به تصویب رسید و ابلاغ شد به شکلی که اگر حادثه‌ای در مقیاس مثلاً جنگ سایبری اتفاق افتاد در این دستورالعمل معلوم شده که مسوول تشخیص، تصویب و ابلاغ کیست.

رویکردهای جدید پدافند غیرعامل

رویکرد عملیاتی	پدافند سایبری
	پدافند زیستی
	پدافند پرتوی
	پدافند شیمیایی
رویکرد بنیادین	پدافند کالبدی
	پدافند اقتصادی
	پدافند مردم‌محور
رویکرد عمومی	پدافند سخت
	پدافند امنیتی

جدول سطوح تهدیدات سایبری

سطوح تهدید	پیامد تهدید	منشاء تهدید	سطح تولید خطر	مسئولیت مقابله
فردی	امنیت فردی	فرد	امنیت فردی	فرد
عمومی	امنیت عمومی	گروه	امنیت عمومی	فرد + وزارت اطلاعات ج.ا.ا
ملی	امنیت ملی	یک کشور	جنگ سایبری	قرارگاه پدافند سایبری کشور
فراملی	امنیت بین المللی	چند کشور	جنگ سایبری بین المللی	قرارگاه پدافند سایبری کشور

تاثیری نگذارد و آن را تغییر ندهد.
این رویکرد کلی امسال بود که طی آن تلاش کردیم که از این ۷ رویکرد، سند ۴ یا ۵ تای آن‌ها را را آماده و سه تای دیگر را نیز در دست کار داریم.
ما در گذشته یک رویکرد عمومی داشتیم اما کم کم دیدیم که سایبر یک جریان خاص دارد و لذا حوزه‌ها به مرور زمان و به تناسب شرایط پیش آمده، کم کم از هم جدا می‌شوند و حوزه خاص خود را پیدا می کنند؛ البته فصل مشترکی هم در کارکردها و رویکردها دارند اما ادبیات اجرایی هر کدام خاص خودشان است.
ما در دهه دوم کارکرد پدافند غیرعامل، این رویکرد کلی پدافند تخصصی را بسیار جدی گرفتیم و سازوکارها را نیز در این مسیر آورده و تلاش می کنیم که به نتیجه برسانیم.

■ روز چهارم هفته پدافند غیرعامل به پدافند سایبری اختصاص داشت که طی آن همایشی هم برگزار شد. در این همایش چه اتفاقی افتاد و درباره سندهایی که در این مراسم رونمایی شد، بفرمایید.

حدود ۴ سال است که در حوزه پدافند سایبری شروع به فعالیت کرده‌ایم و سال گذشته به این نتیجه رسیدیم که تحولات فضای سایبر نسبت به سایر تحولات، سریع‌تر است ولذا باید سند قبلی را بازنگری کنیم. ما کارگروه‌هایی تشکیل دادیم تا با دنیا همگام باشیم و رویکردهایمان به روز باشد.
چهار سال قبل، اولین مشکل ما این بود که ادبیاتی به نام پدافند سایبر خیلی کم وجود داشت و در بعضی کشورها مخلوطی از امنیت و پدافند را شامل می‌شد و ما قصد تفکیک داشتیم چون زمینه‌هایی دیده می‌شد که دشمنان ما دارند به سمت لایه‌های آفند می‌روند؛ لذا آفند را هم دسته‌بندی کردیم و در یک دوره حدودا دوساله توانستیم مبانی تفکیک حوزه‌های جنگی و دفاعی را از حوزه امنیتی و ایمنی داشته و در کنار آن تلفیق این مبانی با حوزه‌هایی مثل علوم استراتژیک، علوم دفاعی، علوم سیاسی و امنیت ملی را که مفاهیم بین رشته‌ای حوزه پدافند سایبری در این مقیاس هستند، دنبال کنیم.
کاری که ما تا کنون در حوزه دفاع پدافند سایبری انجام دادیم، تولید نظریه پدافند سایبری و تفکیک لایه‌های مختلفی از تهدید است.
امروز تهدید از نظر ما چهار مقیاس دارد که مقیاس‌های ایمنی، امنیت، امنیت ملی، امنیت بین‌المللی را در برمی گیرد. امروزه وقتی می‌بینیم که ناتو و چند کشور اعلام مانور می کنند یعنی این که آن‌ها احساس تهدید فراتر از حوزه امنیت داخلی می کنند.
خوشبختانه اکنون پس از بحث‌ها و کارهای کارشناسی سه رشته دکترا و یک رشته ارشد ایجاد کرده‌ایم که البته تولید محتوا در این حوزه‌ها نیز کار سختی است و باید تلاش‌های بین رشته‌ای برای پربار کردن این محتواها همچنان انجام شود.
در حال حاضر دوره دوم کارشناسی ارشد پدافند سایبری را و دوره اول مدیریت سایبری، پدافند سایبری و امنیت سایبری در مقطع دکتری را نیز

این همان سرزمین یا قلمرو است که ما حداقل به صورت منطقی باید تعریف، مشخص و بعد برای چگونگی دفاع از آن طراحی و برنامه‌ریزی کنیم

گرفته‌ایم که ترم دوم یا سوم آن در حال برگزاری است و تمام این‌ها، گام اول ما در این راه هستند.

■ درخصوص فرهنگ سازی و اطلاع رسانی چه اقداماتی صورت گرفته است؟

بخشی هم تحت عنوان سیاست‌های اطلاع‌رسانی داشتیم که اگر یک موقع به کشور حمله سایبری شود باید چه کسی، چگونه و چه پاسخی بدهد که این هم تهیه شـد و به تصویب رسـید و در دبیرخانه شورای عالی امنیت ملی هم به تایید رسید و تکلیف آن معلوم شد.

گاهی دیده می‌شود که رسانه‌ها در سوالات‌شان روی موضوعاتی حساس‌اند که مسوولان نمی‌توانند به آن‌ها جواب بدهند چون اطلاعاتی را شامل می‌شود که پازل اطلاعاتی دشمن را تکمیل وانعکاس رسانه‌ای این جزییات به دشمن کمک می‌کند. ما با تعیین این سیاست‌ها و تعیین سـخن‌گو کاری کردیم که هم اطلاع‌رسانی شده و هم اسرار حفظ شوند. بخش دیگر امر فرهنگ‌سازی و آموزش و تربیت نیروی انسانی بود که در این راستا چهار دوره ارشد و دکترا راه‌اندازی شده و یک دوره دکترای جنگ سایبری هم در دانشگاه امام حسین هست که فضاهای خاص خود را دارد.

من در همه دوره‌ها بعضـی مقاطع یک درس را برداشتم که با دوسـتان ارتباط داشته باشم. افراد بسیار ارزشمند و خوبی هستند که انشاالله وقتی دوره‌ها را به پایان برسانند، می‌توانند حضور مفیدی داشته باشند.

در مباحث آموزشـی طی قراردادی در حال نهایی کردن محتوای دفاع سایبری هستیم که بر اساس آن، محتوا به صورت e-learning در پنج سـطح برای مدیران مبتدی تا عالی آماده شود و هم به شکل کتاب و هم به شکل elearning و هم به صورت مولتی‌مدیا در اختیار مدیران کشور در سطوح مختلف قرار گیرد تا مدیر ما نسبت به این مساله به طور کامل توجیه شود. که این‌ها را تقریباً تا ۹۵ درصد آماده کرده‌ایم.

همچنین در راستای فرهنگ‌سازی برگزاری هفته پدافند نیز و همین‌طور کارگاه‌های آموزشی در استان‌ها و دانشگاه‌ها را داشتیم و یک بسته فرهنگی شامل ۱۲ برنامه ۲۵ دقیقه‌ای تلویزیونی تولید کردیم که در این پکیج بسته ، مفهوم ، تهدید، راه‌حل و چهارچوب‌ها را با به‌کارگیری حدود ۳۰ نفر از نخبگان کشور در این زمینه توضیح داده و میان دستگاه‌ها توزیع کردیم.

■ یکی از لایه‌های موجود در ساختار دفاعی امنیت بین‌المللی است. در قرارگاه پدافند سـایبری هم قطعاً پیمان‌هایـی با کشـورهای دیگر و همسـایگان وجود دارد که بتوانیم دفاع منطقه‌ای هم انجام دهیم.

یکی از الزاماتی که موجب شد تا ما تصمیم بگیریم سندمان را بازنگری کنیم، تغییر چهره و ماهیت تهدیدات سایبری است. اتفاقاتی که در اکراین و گرجستان افتاد و همچنین در مساله استاکس نت به نوعی جنگ سایبری به شکل ملموسی بروز و ظهور یافت و با سایر جنگ‌ها تلفیق شد. مثلاً روس‌ها وقتی خواستند به اکراین گرجستان حمله کنند هم‌زمان نظام اداری سیستم روبه‌روی خود را به هـم زدند. همین دیـروز در یکی از کلاس‌ها فیلمی دیدیم که کارشناس امریکایی با صراحت می‌گفت این کاری که ما در حوزه سایبری می‌کنیم، یک بمباران هوایی نمی‌تواند انجام دهد.

وقتی چنین رویکردی هست، طبیعتاً تعدادی از کشورها قربانی و گروهی دیگر مهاجم می‌شوند. کاری هم که امریکایی‌ها در مورد چین انجام دادند، قابل تأمل است و برای اولین بار رسماً دکترین جنگ سایبری خود را به چینی‌ها دادند و ادعاشان این بود که ما در فضای سایبری می‌خواهیم با شما رو بازی کنیم و این یعنی این‌که این دست تعاملات در دنیا در حال اتفاق افتادن است.

مثلاً ناتو، در حال تمرین دفاع از ۳۹ کشور دسته جمعی در فضای سـایبری اسـت یا در دو ماه گذشته، شاهد تمرین دفاع سایبری اتحادیه اروپا بودیم. لذا طبیعتاً لزوم ایجاد سازوکار یک دفاع جمعی به وجود آمده اسـت و این دفاع جمعی چهار راه بخش دارد: تبادل اطلاعات، تعامل یا اشتراک اطلاعات با مثلاً کشورهای همسایه یا از راه آموزش، دفاع دسته‌جمعی و دیگری هم اگر اتفاقی افتاد دفاع حقوقی است.

این‌ها باید در داخل کشـور با محوریت وزارت امور خارجه اتفاق بیافتـد و ما این‌ها را خدمت آقای وزیر ارائه کردیم و اسـم آن را دیپلماسی پدافند سایبری گذاشـتیم اما در داخل کشور هنوز مسوولان به اجماع نرسیده‌اند.

اصل موضوع را برای وزیر وزارت امور خارجه مطرح کردم و پذیرفتند منتهی به خاطر مسایل ۱+۵ و این مذاکرات، اولویت‌ها تا حدودی به آن سمت است. ما در سازمان در حال آماده کردن این نظام به صورت تئوری هستیم و فکر می‌کنم هم‌سویی خوبی می‌تواند میان ایران، روسیه، چین و هند در این زمینه وجود داشته باشد.

■ این هماهنگی در جنگ سایبری، چون بحث سـرزمین خیلـی معنا نمی‌دهـد، چگونه می‌توانـد اتفاق بیافتد؟

من کمی با سؤال شـما مخالفم. ترکیب کلمه سرزمین در فارسی ما را به سمت مقوله وجود یک تکه زمین منحرف می‌کند اما در انگلیسی واژه territory به معنی قلمرو استفاده می‌شود. بر فرض وقتی که اسراییلی‌ها می‌گویند گنبد پدافند سایبری یعنی از سرزمینی دفاع می‌کنند که شامل جایی می‌شود که فضای سایبری در آن شکل بگیرد و روی آن تأثیر بگذارد. در واقع این مساله قلمرو سایبری تریتوری باید توسط کشورها تعریف شود.

مثلاً اگر هاسـتینگ‌ها میزبانی داده ها و دیتا سنترهای ما همگی در فضای فیزیکی خارج از سرزمین ما تعریف شود، امکان دارد سرزمین قلمرو سایبری ما جای دیگری باشد و بخشی از آن در اختیار ما نباشد.

دریایی را فرض کنید که شامل چندین جزیره است و شـما باید از این جزایرتان دفاع کنید. حالا تعدادی کشتی می‌خواهند از راه این دریا و از میان این جزایر عبور کنند. شما یا باید برای تک‌تک این جزایر دفاع پیش‌بینی کنید یا خطی دور این جزایر بکشید و بگویید من دفاع خود را در این حوزه انجام می‌دهم که این دومی منطقی‌تر به نظر می‌رسد و یا می‌تواند تلفیقی از هر دوی این‌ها باشد.

به نظر من یکی از کارهای خوبی که می‌توانیم انجام دهیم، تعریف سرزمین قلمرو خودمان در فضای سایبر است.

ما باید در مقابل حمله به کجا عکس‌العمل نشان دهیم و کجا سرزمین ما محسوب می‌شود تا ما از آن نگهبانی و دفاع کرده و حساسیت به خرج دهیم. این همان سـرزمینی قلمروی اسـت که ما حداقل به صورت منطقی باید تعریف، مشخص و بعد برای چگونگی دفاع از آن طراحی و برنامه‌ریـزی کنیم.یکی از ضرورت‌های ما در سطح منافع ملی، تعریف این سرزمین قلمرو است تا بعد سازوکارهای دفاعی خاص آن را پیاده کنیم وگرنه ما نطنز مجازی را جزو خاک خود حساب نمی‌کنیم و وقتی به آن حمله سایبری صورت می‌گیرد، عکس‌العملی انجام نمی‌دهیم درحالی که نطنز جزو سرزمین ماست.

مبنای این موضوع فناوری اطلاعات است اما به مسائل استراتژیک، امنیتی، سیاسی و دفاعی نیز مرتبط است.

در مباحث آموزشی طی قراردادی در حال نهایی کردن محتوای دفاع سایبری هستیم که بر اساس آن، محتوا به صورت e-learning در پنج سطح برای مدیران مبتدی تا عالی آماده شود

امنیت ابری در مقابل امنیت در ابر

تفاوت آن‌ها در چیست؟

امنیت ابری و امنیت در ابر به نظر می‌رسد که یک مفهوم را می‌رسانند، ولی دو نوع کاملاً متفاوت از امنیت هستند. اولی، به امنیت خود ابر برای اجرای اپلیکیشن‌ها، ذخیره سازی داده‌ها و پردازش تراکنش‌ها می‌پردازد. این یکی از نگرانی‌های شرکت‌های بزرگ است که می‌خواهند با هزینه‌ی پایین از مزایای راهکارهای امنیت ابری، بدون آلوده شدن اطلاعات سازمانی و اطلاعات مشتریان بهره مند شوند. از طرفی، امنیت در ابر، یعنی استفاده از رایانش ابری برای مهیاکردن راهکارهای امنیتی برای یک سازمان. مانند فروش و دیگر اپلیکیشن‌هایی که در یک ابر فعالیت می‌کنند، امنیت در ابر از یک‌بار نصب برای تمام کاربران سود می‌برد و نیازی نیست تا این اپلیکیشن برای تمام دستگاه‌ها نصب شوند.

یکی دیگر از مزایای امنیت در ابر این است که با هکرها در سطح خودشان مواجه می‌شود. هکرها دینامیک حملات خود را تغییر داده‌اند. آن‌ها از این موارد سود می‌جویند:

- حملات متفاوتی که دستگاه‌های سیار را هدف قرار می‌دهند، که معمولاً سطح امنیتی پایین‌تری نسبت به کامپیوترهای شخصی دارند.
- تکنیک‌های شبکه‌های اجتماعی تا کاربران را قانع کنند که لینک‌ها و ایمیل‌هایی که ارسال می‌کنند سودمند هستند و از منابع قابل‌اعتمادی ارسال‌شده‌اند.

(برخی از استراتژی‌های متداول شامل ایمیل‌هایی است که به دریافت‌کننده می‌گویند که در قرعه‌کشی یک بانک خارجی برنده‌شده‌اید، و یا اینکه ایمیل از طرف یکی از شرکت‌های وابسته به بانک آن‌ها ارسال‌شده و نیازمند تأیید احراز هویت مشتریان خود هستند.)

- ویروس‌ها، تروجان‌ها و هرزنامه‌هایی که درون عکس‌ها، فایل‌های PDF و لینک‌های به‌ظاهر سالم کارگذاری شده‌اند.

لازم به ذکر است که نوع و تعداد حملات به‌صورت نمایی در حال افزایش‌اند. تعداد حملات بدافزارها در ۱۸ تا ۲۴ ماه اخیر بیشتر از کل حملات در ۱۸ سال گذشته بوده است.

در بحبوحه‌ی تنوع و افزایش حجم حملات، وظیفه‌ی خطیر IT این است که تعداد رو به افزایش دستگاه‌های نقطه انتهایی را مصون نگه دارد.

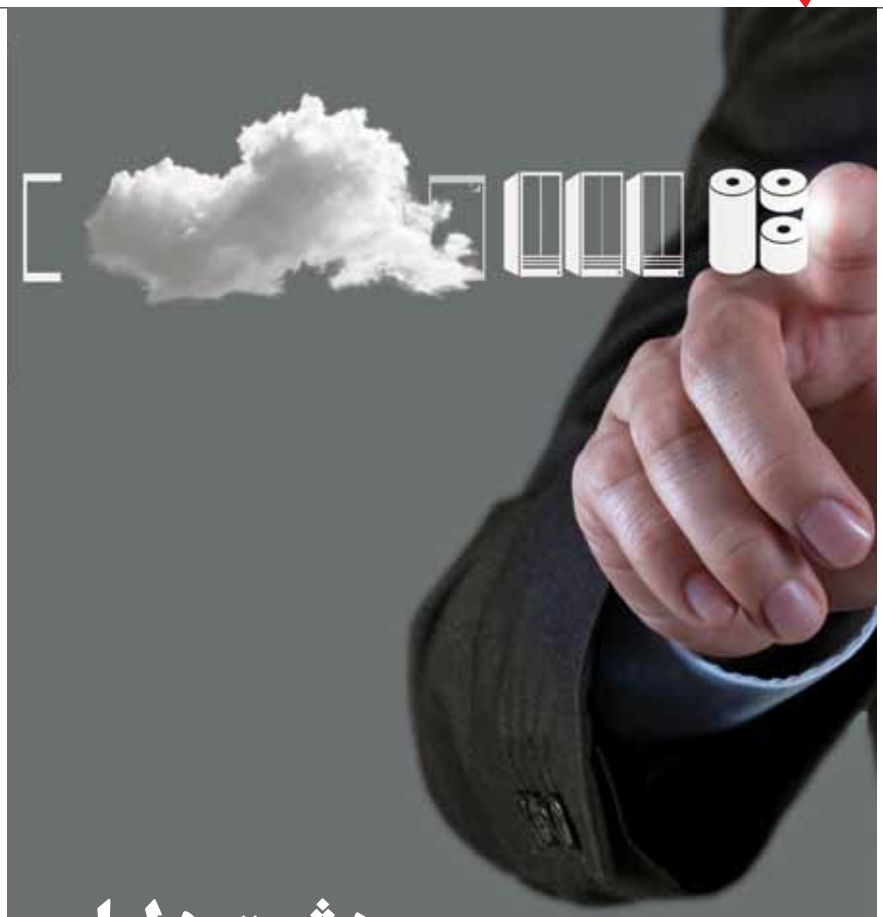
امنیت از طریق رایانش ابری می‌تواند ایمیل‌ها را امن، رمزنگاری و آرشیو کند. همچنین لایه‌ی ابری می‌تواند دسترسی به اینترنت را فیلتر کند تا کاربران نتوانند محتواهای غیرمجاز دانلود کنند. به‌جای حفاظت کردن از هر دستگاه، استراتژی بهتر این است که شرکت، امنیت را در سطح ابری فراهم آورد. این روش باعث می‌شود که با حملات، در سطح خودشان مبارزه شود، به‌جای اینکه بدافزار وارد شبکه‌ی شرکت شود و آنجا با آن‌ها مبارزه شود – روشی که تنها فاجعه را دعوت می‌کند.

امنیت در ابر سومین و تکامل‌یافته‌ترین نوع امنیت است. نخستین نسل همان «امنیت در جعبه» بود (برای مثال یک برنامه‌ی امنیتی که روی هر دستگاه نصب می‌شد). نسل دوم دستگاه‌های امنیتی بودند که روی شبکه‌ی شرکت پیاده‌سازی می‌شدند؛ درحالی که این نسل از نسل اول بهتر بود، ولی هنوز هم ممکن بود بدافزارها را متوقف نکند تا زمانی که آسیبی جدی روی شبکه وارد نکرده باشند.

امنیت در ابر، باقدرت و انعطاف‌پذیری بیشتری، در هر زمان و مکانی امنیت را برقرار می‌کند و وظیفه‌ی سنگین را از دوش کاربر کنار می‌گذارد. از میان مزایای امنیت در ابر می‌توان به این موارد اشاره کرد:

- کنترل و اطمینان از اینکه اقدامات امنیتی مانند پروتکل‌های گذرواژه، فایروال‌ها و وصله‌های امنیتی بروز هستند.
- کارمندان بخش امنیت را از آخرین حملات و استراتژی‌های مورداستفاده‌ی هکرها آگاه می‌کند.
- احراز هویت لایه‌بندی شده تا دسترسی به بخش‌هایی از شبکه را برای مشتریان، بخش‌هایی دیگر را برای کارمندان، و دسترسی وسیع‌تری را برای مدیران فراهم کند.
- جهت‌دهی به تمام درخواست‌های روی شبکه مانند ایمیل‌ها و دسترسی به شبکه از طریق یک ارتباط متمرکز و امن، که با آخرین پروتکل‌های امنیتی بروز می‌ماند، و تمام حملات را قبل از اینکه به شبکه برسند مسدود می‌کند.

بر اساس تحقیقی که توسط شرکت ابردین گروپ صورت گرفت، شرکت‌هایی که از این متد امنیتی استفاده می‌کنند کاهش چشمگیری در رویدادهای مربوط به بدافزارها، آلوده شدن سایت‌ها، گم‌شدگی داده و سرقت اطلاعات، توقف کاری به خاطر مسائل امنیتی و نقص‌های مربوط به بازرسی را گزارش دادند. روی آوردن به امنیت در ابر باید به نخستین خط دفاعی یک استراتژی امنیت یکپارچه تبدیل شود. پیاده‌سازی فایروال‌ها، گذرواژه‌های قدرتمند، امنیت داخلی دستگاه‌ها و آموزش کارمندان همگی المان‌های حیاتی یک «دفاع عمیق» هستند. داشتن این رویکرد جامع در تضمین امنیت شبکه‌ی سازمان بسیار مؤثر است.



هشت دلیل برای واهمه از رایانش ابری

تا سال ۲۰۱۵ انتظار می‌رود که رایانش ابری به یک صنعت فراتر از ۱۵۰ میلیون دلار تبدیل شود. و به دلایل خوبی، کاربر چه از کامپیوترهای رومیزی استفاده کند و چه از دستگاه‌های سیار، هرکجا و در هرزمانی که باشد، کافی است تنها یک ارتباط اینترنتی داشته باشد تا به داده‌هایش دسترسی پیدا کند. برای کسب‌وکارها هم رایانش ابری مزایای بی‌شماری دارد که از میان آن‌ها می‌توان به ذخیره‌سازی مقیاس‌پذیری برای فایل‌ها، اپلیکیشن‌ها و دیگر انواع داده‌ها؛ تعامل بهتر میان اعضای گروه‌ها صرف‌نظر از مکان آن‌ها؛ و صرفه‌جویی در زمان و هزینه برای ایجاد دیتاسنترهای پرهزینه و استخدام کردن گروه‌های IT برای مدیریت آن‌ها اشاره کرد. بااین‌وجود بیشتر کسب‌وکارها دارای این نگرانی هستند که: رایانش ابری دقیقاً چقدر امن است؟ باوجوداینکه بسیاری از ارائه‌دهندگان معتبر رایانش ابری دارای امنیتی در بهترین سطح ممکن هستند، ولی کارشناسان بر این باورند که چیزی به نام امنیت کامل سیستم ابری وجود ندارد.

از حفره‌های امنیتی گرفته تا مسائل مربوط به پشتیبانی، این‌ها ریسک‌های عمده‌ای هستند که کاربران هنگام روی آوردن به رایانش ابری متحمل می‌شوند.

1 فرد دیگری از داده‌های شما مراقبت می‌کند

برخلاف دیتاسنتر که توسط یک گروه IT داخلی مدیریت می‌شود، رایانش ابری یک سیستم خارج از سازمان است که در آن کاربران داده‌های خود و نیازهای مربوط به آن را برون‌سپاری می‌کنند. ارائه‌کننده‌ی خدمات رایانش ابری همه‌ی کارها را از انجام بروزرسانی‌ها گرفته تا تعمیر و نگهداری تا مدیریت امنیت انجام می‌دهد. به گفته‌ی استیو سانتورلی، از کارآگاه‌های اسبق اسکاتلندیارد و از مدیران گروه تحقیقاتی امنیت اینترنت Cymru: «اگر از بالا نگاه کنیم، می‌بینیم که کاربران دارند به فرد دیگری اعتماد می‌کنند تا از داده‌هایشان محافظت کند.

نقطه‌ی تاریک قضیه این است که شما مسئولیت خود در قبال داده‌ها را فسخ می‌کنید. فرد دیگری به آن دسترسی دارد و فردی دیگر مسئول امن نگه‌داشتن آن است. هیچ کسب‌وکاری نمی‌تواند به‌اندازه‌ی خود شما در صیانت از داده‌هایتان سریع باشد. درنهایت کسب‌وکار آن‌ها این است که از شما درآمدی به جیب بزنند. گاهی اوقات حفاظت از داده‌های شما به یک شعار بازاریابی تبدیل می‌شود تا یک سبک کاری.»

2 حملات سایبری

هر بار که داده‌های خود را روی اینترنت ذخیره می‌کنید، خطر حملات سایبری وجود دارد. و این به‌ویژه زمانی مشکل‌ساز است که شما داده‌های خود را روی ابر ذخیره می‌کنید، جایی که تمام داده‌های شما با انواع کاربرها، روی یک سیستم ابری واحد ذخیره‌شده‌اند.

سانتورلی می‌گوید «قسمت ترسناک ماجرا آسیب‌پذیری در مقابل حملات انکار سرویس گسترده و تمرکز این حجم از داده است. تنها نقطه‌ی ضعف در این حالت همان ابر است. اگر همه‌چیز درست پیش نرود تأثیر آن بسیار وسیع خواهد بود. در این حالت ایجاد اختلال در سطح وسیع و گسترده‌ای راحت‌تر خواهد بود.»

باوجوداینکه بیشتر ارائه‌کنندگان خدمات رایانش ابری از امنیت بالایی برخوردار هستند، ولی با پیشرفته‌تر شدن فناوری، حملات سایبری هم پیشرفته‌تر می‌شوند.

سانتورلی می‌گوید «زمانی که شرکت‌های ارائه‌کننده‌ی خدمات ابری امنیت را به‌خوبی اجرا می‌کنند – و واقعاً شرکت‌های زیادی به این مهم رسیده‌اند – آنگاه تبهکاران سایبری مجبورند برای دسترسی به داده‌ها خلاقیت بیشتری نشان دهند. برای مثال، آن‌ها به‌جای هک کردن ابر،

تلاش می کنند حساب کاربری شما را هک کنند. گذرواژه‌ها و پرسش‌های مخفی به نقطه‌ضعف امنیت شما تبدیل می‌شوند. درست مثل زمانی که بانک‌ها هک شدن حساب‌های آنلاین را سخت‌تر کردند، هکرها به حملات فیشینگ روی آورند تا گذرواژه‌های شما را سرقت کنند.»

3 تهدیدات داخلی

همان‌طور که حملات سایبری در حال افزایش هستند، تهدیدات داخلی هم در حال اوج‌گیری‌اند.

اریک چیو، مدیر و مؤسس شرکت کنترل زیرساخت‌های رایانش ابری «های‌تراست» می‌گوید که «نشت اطلاعات مربوط به دو میلیون کاربر وودافون و اقدامات ادوارد اسنودن در NSA همگی زنگ خطرهایی هستند که جدی‌ترین نشت داده‌ها از طریق تهدیدات داخلی و دسترسی کاربران صورت می‌گیرند.»

زمانی که یک کارمند به ابر دسترسی پیدا می‌کند یا امکان دسترسی را به فردی دیگر اعطا می‌کند، هر چیزی، از اطلاعات محرمانه گرفته تا دارایی‌های فکری در خطر هستند.

به گفته‌ی چیو «رایانش ابری این مشکل را ده برابر می‌سازد زیرا دسترسی به مدیریت پلتفرم ابری، چه توسط یک کارمند و چه توسط فردی که خود را کارمند جا زده است، فرد را قادر می‌سازد تا بدون اینکه شناسایی شود هر ماشین مجازی را کپی کرده و آن را به سرقت ببرد، و یا در عرض چند دقیقه تمام محیط ابری را نابود کند.»

4 نفوذ دولت

پس از افشاگری‌های اخیر در مورد NSA و برنامه‌های جاسوسی آن‌ها، مشخص شد که رقبا تنها کسانی نیستند که می‌خواهند به داده‌های شما سرک بکشند.

اسکات هازدرا، مشاور امنیتی در نئوهاپسیس، یک شرکت مشاوره مدیریت امنیت و ریسک در زمینه‌ی امنیت موبایل و امنیت رایانش ابری می‌گوید که: «اخیراً در اخبار می‌بینیم که نهادهای دولتی و شرکت‌های فناوری محور در ایالات‌متحده و دیگر کشورهای دنیا ممکن است در حال جاسوسی روی داده‌های شما باشند، چه زمانی که داده‌ها منتقل می‌شوند یا زمانی که در قسمتی از اینترنت سکنی گزیده‌اند.»

بااین‌وجود، حریم خصوصی همیشه از نگرانی‌های شایع در مورد رایانش ابری بوده است. ولی به‌جای نگرانی در مورد رقبا، مشتریان یا کارمندان عصبانی که به سیستم امنیتی نفوذ می‌کنند، اکنون کسب‌وکارها نیاز دارند تا در مورد نفوذ نهادهای دولتی هم نگران باشند.

هازدرا می‌گوید «نقض حرم خصوصی و محرمانگی داده‌ها ریسک جدیدی نیست، ولی منبع این تهدیدات ممکن است همان‌هایی نباشد که سازمان‌ها نگرانش بودند. برای مثال ممکن است یک سازمان از ترس رقبا ارسال و ذخیره‌سازی داده‌های خود را رمزنگاری کند. اکنون که نهاد دیگری غیر از رقیب به داده‌های سازمان علاقه نشان می‌دهد، اساساً خود ریسک را تغییر نمی‌دهد.»

5 مسئولیت قانونی

ریسک‌های مربوط به رایانش ابری به نفوذهای امنیتی محدود نمی‌شود. این ریسک‌ها همچنین شامل پیامدها، مانند پرونده‌های حقوقی توسط شما یا علیه شما می‌شوند. به گفته‌ی رابرت جی. اسکات مدیر شرکت Scott & Scott LLP، یک شرکت حقوقی با تخصص در دارایی‌های فکری و فناوری، جدیدترین ریسک برای شرکت‌ها در استفاده از رایانش ابری تطابق با قوانین، مسئولیت‌های قانونی و تداوم کسب‌وکار است. رویدادهای مربوط به نشت داده‌ها در حال اوج‌گیری هستند و درنتیجه پرونده‌های قانونی هم افزایش یافته‌اند.» اسکات می‌گوید در حالی که رایانش ابری سهولت دسترسی، تعامل و تسریع کارها را نتیجه می‌دهد، ولی مزایای آن باید با میزان اقدامات امنیتی سنجیده شود.

وی می‌افزاید «امنیت اطلاعات همیشه در جست‌وجوی یک تعادل میان سهولت دسترسی و اشتراک‌گذاری اطلاعات، در مقابل امنیت مستحکم بوده است. هرچه بیشتر یکی را داشته باشید، کمتر دیگری را خواهید داشت.»

6 فقدان استاندارد

چه چیزی یک ابر را «امن» می‌سازد؟ یک ارائه‌کننده‌ی خدمات ابری ممکن است آخرین امکانات امنیتی را داشته باشد، ولی درنتیجه‌ی فقدان استاندارد مربوط به رایانش ابری، هیچ راهنمای واحدی وجود ندارد تا ارائه‌دهندگان را متحد کند. باوجود سرویس‌های ابری متعدد در بخش‌های مختلف، برای کاربران کاملاً مشکل‌ساز است که تشخیص دهند ابر آن‌ها چقدر امن است. اسکات می‌گوید «این سؤال که رایانش ابری چقدر امن است جنبه‌های متعددی دارد، و جواب آن به ارائه‌کننده‌ی خدمات ابری، نوع صنعت، و قانون‌های مرتبط با آن صنعت وابسته است.» از آنجایی که ارائه‌کنندگان مختلف مانند هم نیستند، ممکن است تعریف «امن» برای یک ارائه‌دهنده‌ی خدمات از تعریف دیگری متفاوت باشد.

7 فقدان پشتیبانی

تصور کنید نتوانید قبل از یک قرار کاری مهم به حساب ابری خود دسترسی پیدا کنید، یا بدتر از آن، وسط یک حمله‌ی سایبری باشید که سایت شما را پایین آورده باشد. و حالا تصور کنید که سعی دارید با ارائه‌دهنده‌ی خدمات خود تماس بگیرید و ببینید که خدمات مشتریان آن‌ها اصلاً وجود خارجی ندارد. درحالی که برخی از ارائه‌کنندگان خدمات مربوط به مشتریان خوبی دارند، برخی دیگر ممکن است شما را تنها رها کنند. آپریل سیج، از مدیران شرکت آنلاین تک، یک ارائه‌دهنده‌ی خدمات رایانش ابری می‌گوید که «ناامیدکننده‌ترین چیز هنگامی که مشکلی پیش می‌آید این است که نتوانید مستقیماً با یک مهندس صحبت کنید.

اگر سیستم‌های شما برای ادامه‌ی مأموریت‌هایتان حیاتی نیستند، نیازی نیست که نگران امنیت و دسترس‌پذیری آن‌ها باشید. ولی اگر سیستم‌های شما برای کسب‌وکار و مأموریت شما حیاتی‌اند، باید روی ابر و ارائه‌کننده‌ای سرمایه‌گذاری کنید که بتواند امنیت متناسب با نیازهای شما را فراهم کند.»

هر بار که داده‌های خود را روی اینترنت ذخیره می‌کنید، خطر حملات سایبری وجود دارد. و این به‌ویژه زمانی مشکل‌ساز است که شما داده‌های خود را روی ابر ذخیره می‌کنید، جایی که تمام داده‌های شما با انواع کاربرها، روی یک سیستم ابری واحد ذخیره‌شده‌اند

8 همیشه ریسک وجود دارد

بزرگ‌ترین ریسک در مورد رایانش ابری این است که هیچ‌وقت نمی‌دانید چه چیزی در انتظار شماست. هکرها از روز نخست حضور داشته‌اند و قرار نیست به این زودی‌ها جایی بروند. و با پیشرفت فناوری‌ها ریسک‌های استفاده از این فنّاوری‌ها هم افزایش می‌یابند.

باوجود خطرات کنونی و آتی، آیا مزایای استفاده از رایانش ابری بر ریسک‌های آن چربش دارد؟ نیل راپ، مؤلف کتاب «خطر سایبری» و مؤسس شرکت سایبر سکیوریتی آرکیتکتس می‌گوید که این امر به کسب‌وکار شما بستگی دارد. او می‌افزاید «رایانش ابری برای هر کسی مناسب نیست. مانند تمام راهکارها، لازم است که سطح ریسک آن را ارزیابی کنید و ببینید که برای شما مناسب است یا خیر.»

برای کسب‌وکارهایی که در حال استفاده از رایانش ابری هستند یا در مورد آن فکر می‌کنند، تمام کاری که می‌توانید بکنید این است که تا جایی که می‌توانید آماده‌باشید. باید تا جایی که می‌توانید ارائه‌کنندگان را بشناسید، هم از دید یک سازمان و هم یک کاربر نقطه انتهایی.

منبع: بیزنس تودی

این وکیل باسابقه، برای مدیران IT که تمایل دارند ریسک‌های مربوط به خودی‌های نفوذی را کاهش دهند توصیه‌هایی دارد.

این نفوذگران خودی

مایکل واتیس یکی از کارشناسان شرکت حقوقی Steptoe & Johnson LLP است. وی روی اینترنت، تجارت الکترونیک و مسائل مربوط به تکنولوژی متمرکز است، و در مورد مسائل مربوط به حریم خصوصی مشاوره‌های قانونی، حقوقی و استراتژیک ارائه می‌دهد. با او صحبت کردیم تا در مورد جنبه‌های مختلف تهدیدات مربوط به خودی‌های نفوذی و نقض قوانین، اطلاعات بیشتری کسب کنیم.

■ از دیدگاه شما، مدیران امنیتی و در کل، دیگر مدیران برای کاهش ریسک مربوط به تهدیدات خودی‌های نفوذی چه باید بکنند؟

باید با کارهای بنیادین کار را آغاز کرد. نخست آن‌ها باید یک ارزیابی ریسک انجام دهند که به‌صورت سالانه بروز می‌شود، و نوع اطلاعاتی که سازمان در اختیار دارد را بررسی می‌کند. این شامل اطلاعات شخصی، مالی و پزشکی؛ بخش‌هایی از شبکه یا دفاتر که این اطلاعات در آن نگهداری شده؛ نوع خطراتی که این اطلاعات را تهدید می‌کند؛ و اقداماتی که هم‌اکنون برای کاهش این گونه ریسک‌ها در حال انجام هستند می‌شود.

دوم اینکه باید یک خط‌مشی امنیتی تدوین کنند، که بر اساس ارزیابی ریسک نگارش می‌شود، و آغازگر فعالیت‌های امنیتی اداری، فنی، و فیزیکی است، و اینکه این فعالیت‌ها هم تهدیدات داخلی و هم خارجی را تحت پوشش قرار دهند.

سوم اینکه باید اطمینان حاصل کنند که زمان نشت داده‌ها برنامه‌ی مناسبی برای تعاملات بعدی دارند، برنامه‌ای که برای به حداقل رساندن زیان‌ها، شناسایی عامل نفوذ، تعمیر کردن آسیب‌پذیری، و تطابق با قوانین و الزامات قانونی، مانند انتشار اعلامیه برای کسانی که تحت تأثیر قرار گرفته‌اند، تدوین‌شده باشد.

■ زمانی که مدارک کافی دال بر انجام کار خطا در شبکه توسط کارمندان وجود داشته باشد، چه مراجع قانونی‌ای وجود دارند؟

مایکل: کارمندانی که در شبکه‌ی سازمان به فعالیت‌های مجرمانه دست می‌زنند، یا توسط خود سازمان و یا توسط دولت به مراجع قانونی فراخوانده می‌شوند.

برای مثال کارمندی که به‌صورت عمدی به شبکه‌ی یک سازمان آسیب وارد می‌کند تحت لایحه‌ی کلاه‌برداری و سوءاستفاده‌ی کامپیوتری (CFAA) تحت پیگرد قانونی قرار خواهد گرفت. همچنین کارمندی که بدون اجازه به ارتباطات الکترونیکی دسترسی پیدا کند تا اطلاعات حساس را به سرقت ببرد، بسته به نوع دلایل و مدارک، تحت لایحه‌های CFAA یا لایحه‌ی حریم خصوصی ارتباطات الکترونیک (ECPA) تحت پیگرد قانونی قرار خواهد گرفت. همچنین بسته به نوع دلایل و مدارک، دیگر قوانین و لایحه‌های مرتبط با جرائم رایانه‌ای می‌تواند موجب شود که فرد خاطی مورد پیگرد قانونی قرار گیرد.

■ آیا به نظر شما این‌که به کارمندان اجازه دهیم در مورد عواقب نقص امنیت داخلی سازمان اطلاعات کسب کنند و آگاه باشند، یک عامل بازدارنده است؟

باید به اطلاع کارمندان رسانده شود که هر گونه فعالیت نامناسب روی شبکه‌ی شرکت یا استفاده از دارایی‌های شرکت می‌تواند منجر به پیگرد قانونی، شامل اخراج، پرونده‌ی حقوقی، یا پرونده‌ی مجرمانه شود.

بازداشتن تهدید عوامل داخلی خیلی بهتر از دست‌وپنجه نرم کردن با یک نقض واقعی امنیت توسط عوامل داخلی است و هشدارهای واضح می‌تواند بازدارنده باشند

توسط عوامل داخلی است و هشدارهای واضح می‌تواند به تأثیر بازدارنده باشند.

این گونه هشدارها باید در خط‌مشی سازمان لحاظ شده و طی جلسات تمرینی متعددی هم به کارمندان منتقل شود.

■ مدیران آی‌تی و امنیتی باید چگونه واکنش نشان دهند اگر به یک تهدید داخلی یا نقض امنیت مشکوک باشند؟

اگر یک شرکت مشکوک باشد که یک کارمند در حال آسیب‌رساندن به شبکه‌ی سازمان است، یا اطلاعات حساس را به سرقت می‌برد یا در هر نوع فعالیت مجرمانه و غیرقانونی دیگری مشارکت دارد، می‌توانید کارهای زیادی انجام دهید.

نخست می‌توانید اطلاعات بیشتری را در مورد فعالیت‌های فرد موردنظر در شبکه جمع‌آوری کنید. این کارها می‌تواند شامل بررسی لاگ‌های فرد روی شبکه، بازبینی ارتباطات فرد روی شبکه، پایش ارتباطات همزمان با برقراری آن‌ها، جست‌وجوی فیزیکی محل کار وی، بازبینی ویدئوهای امنیتی تمام مناطقی که فرد در آن حضورداشته، بشود. این یکی از مزایای داشتن خط‌مشی حریم خصوصی است. زیرا دیگر کارمندان می‌دانند که ارتباطات آن‌ها در شبکه مورد پایش قرار گرفته، محل کارشان ممکن است مورد جست‌وجو قرار گیرد، و اینکه کارمندان نباید انتظار داشته باشند که حریم خصوصی آن‌ها در محل کار رعایت شود. و شرکت باید حتماً تأیید اجازه‌ی کارمند در مورد این خط‌مشی حریم خصوصی را داشته باشد.

پرواضح است که این گونه بررسی‌ها بسیار حساس بوده و سرشار از ریسک هستند، بنابراین توصیه می‌شود که قبل از انجام آن‌ها حتماً با فرد متخصص مشورت صورت گیرد. اصلاً توصیه نمی‌شود که سازمان در این مرحله با کارمندان روبرو شود.

دوم اینکه سازمان می‌تواند مورد را به مراجع اجرای قانون گزارش دهد. معمولاً FBI در این زمینه بسیار متخصص است، ولی سرویس مخفی ایالات‌متحده و همچنین مراجع اجرای قانون محلی هم می‌توانند گزینه‌های دیگر باشند. این نهادها برای بررسی بیشتر ابزارهایی دارند که شرکت‌ها در اختیار ندارند، مانند حکم تفتیش و احضاریه‌ها، یا ردگیری ارتباطات در اینترنت و جایی که کارمند اطلاعات را به آن فرستاده است. این که مورد را به این نهادها گزارش داد یا نه به شرایط پرونده بستگی دارد. گزارش به این نهادها ممکن است عواقب سنگینی برای شرکت داشته باشد، پس این کار را بدون مشورت کردن انجام ندهید.

راهنمای اصطلاحات
رایانش ابری

رایانش ابری

به‌جای ذخیره‌سازی داده‌ها به‌صورت محلی روی کامپیوترهای شرکت یا شبکه‌ی شرکت، رایانش ابری شامل ذخیره‌سازی داده‌ها و منابع به اشتراک گذاشته‌شده‌ی شرکت در یک پلتفرم متمرکز و ایمن است. به‌جای استفاده از سرورهای شرکت، در این روش منابع شرکت در دستان یک سازمان طرف سومی قرار می‌گیرد که وظایف مربوط به تعمیر و نگهداری و در دسترس‌پذیری هر سرویس خریداری‌شده را انجام می‌دهد.

IaaS

بسیاری از سازمان‌ها خودشان سخت‌افزارهای لازم را برای زیرساخت‌های پشتیبان خریداری می‌کنند و زیر هزینه‌های خرید سرورها، نصب و یکپارچه‌سازی، و استخدام نیروهای متخصص برای تعمیر و نگهداری آن له می‌شوند. «زیرساخت به‌عنوان سرویس» یا IaaS این هزینه‌ها را از میان برداشته و هزینه‌های مربوط به سرورهای موردنیاز شرکت را بسیار کاهش داده و نیاز به تعمیر و نگهداری را از میان بر می‌دارد.

PaaS

شرکت‌های نوظهور در عرصه‌ی نرم‌افزار به یک زیرساخت سخت‌افزاری و نرم‌افزاری قدرتمندی نیاز دارند تا اپلیکیشن‌هایی مناسب برای فضای رقابتی توسعه دهند. «پلتفرم به‌عنوان سرویس» یا همان PaaS یک پلتفرم مبتنی بر رایانش ابری مهیا می‌کند که می‌توان از آن برای ساخت، تست کردن و آغاز به کار اپلیکیشن‌ها استفاده کرد.

رایانش ابری در حال تغییر کسب‌وکارها است. این راهکار، روش جدیدی برای تسهیل تعاملات و دسترسی به اطلاعات را از نقاط مختلف جغرافیایی، و بدون هزینه‌های سربار مربوط به نگهداری از منابع، فراهم آورده است. درنتیجه شرکت‌های نرم‌افزاری انعطاف بیشتری داشته و کاربر را قادر می‌سازند تا به‌جای خرید کل بسته‌ی نرم‌افزاری، تنها آن نرم‌افزارهایی را خریداری کند که به آن نیاز دارد.

باوجوداینکه بسیاری از شرکت‌ها از رایانش ابری استفاده می‌کنند، ولی عده‌ی زیادی کاملاً ترمینولوژی رایانش ابری را درک نکرده‌اند. زبان تخصصی رایانش ابری ممکن است گیج کننده باشد، بنابراین در ادامه سعی کرده‌ایم عبارت‌های مصطلح در این زبان را برای شما بشکافیم.

SaaS

مدل سنتی شرکت‌ها و نرم‌افزارها این است که برای هر کاربر یک لایسنس خریداری شود. زمانی که نسخه‌ی بروزرسانی اپلیکیشن‌ها عرضه می‌شود، شرکت مجبور است تا نسخه‌ی جدید را خریداری کرده تا با قوانین و استانداردهای صنعت خود همگام باشد. «نرم‌افزار به‌عنوان سرویس» یا SaaS این مدل را تغییر داده و از یک مدل آبونمان ماهانه مبتنی بر رایانش ابری استفاده می‌کند که در آن، بروزرسانی‌ها سریعاً به اطلاع شرکت خواهد رسید.

XaaS

درحالی که IaaS، PaaS و SaaS همگی به مدل‌های کسب‌وکاری خاصی اطلاق می‌شوند، به‌نوعی می‌توان هر محصول را به‌عنوان سرویس ارائه داد. XaaS یعنی «هر چیزی به‌عنوان سرویس»، و اشاره به این دارد که هر محصولی که بتوان آن را از طریق اینترنت تحویل داد و نیازی به مغازه خرده‌فروشی نباشد را می‌توان با این مدل ارائه داد. IaaS، PaaS و SaaS از متداول‌ترین اشکال XaaS هستند، ولی مدل‌های کسب‌وکاری دیگری از این قبیل وجود دارند مانند ذخیره‌سازی به‌عنوان سرویس (SaaS)، ارتباطات به‌عنوان سرویس (CaaS)، شبکه به‌عنوان سرویس (NaaS) و مانیتورینگ به‌عنوان سرویس (MaaS).

مدل SPI

این یک کلمه‌ی اختصاری است که به متداول‌ترین مدل‌های سرویس‌های رایانش ابری یعنی SaaS، PaaS و IaaS اشاره دارد.

ابر خصوصی

ابر خصوصی یک سرویس ابری برای ذخیره‌سازی و بازیابی داده‌هاست که طراحی آن طوری است که تنها یک سازمان از آن استفاده کند. کارمندان می‌توانند داخل شرکت با داده‌های موجود در این ابر کار کرده و نتایج را با همکاران خود به اشتراک بگذارند، ولی دسترسی به اطلاعات درون ابر برای افراد خارج شرکت امکان‌پذیر نیست. شرکت‌هایی که می‌خواهند از مزایای رایانش ابری استفاده کنند، ولی کنترل کامل را روی آن داشته باشند از این مدل ابری استفاده می‌کنند.

مدل‌های سرویس‌های رایانش ابری

این روزها بسیاری از کسب‌وکارها سرویس‌های مبتنی بر رایانش ابری عرضه می‌کنند که از مدل سنتی لایسنس نرم‌افزارها بهتر است. این مدل‌ها به‌صورت ماهانه وجود دارند و از طریق یک مرورگر وب قابل‌دسترسی بوده و به‌صورت منظم بروزرسانی‌ها را انجام می‌دهد. مدل‌های معمول سرویس‌های رایانش ابری شامل IaaS، PaaS و SaaS می‌شود.

ابر عمومی

سرویس‌های ابری بی‌شماری وجود دارند که با استفاده از یک سرور منابع واحد به شرکت‌های زیادی خدمات ابری عمومی ارائه می‌دهند. درحالی که ابر خصوصی اجازه‌ی دسترسی به ابر را از خارج شرکت سلب می‌کند، یک ابر خصوصی کاربران را طبقه‌بندی کرده تا سطح یکپارچه‌ای از سرویس‌ها را ارائه دهد. کاربران می‌توانند به اطلاعات خود در ابر عمومی دسترسی پیدا کنند، ولی امکان دسترسی به اطلاعات دیگر کاربران را ندارند.

مرکز داده

این یک ساختار است که باهدف میزبانی منابع مبتنی بر رایانش ابری مانند سرورها و دیگر تجهیزات مبتنی بر سرویس ایجاد می‌شود. بسیاری از شرکت‌های مبتنی بر رایانش ابری دارای مرکز داده‌ی خود هستند که در آن داده‌های مربوط به مشتریان خود را نگهداری می‌کنند و دسترس‌پذیری آن‌ها را تضمین می‌کنند. بسیاری شرکت‌ها دارای مراکز داده‌ی متعددی در مناطق مختلف جغرافیایی هستند تا در صورت شکست یا خرابی یکی از آن‌ها، تداوم سرویس‌دهی به مشتریان حفظ شود.

رایانش تجهیزات

زمانی که شرکت‌ها سروری را خریداری می‌کنند، احتمال اینکه از تمام منابع موجود سخت‌افزاری خود استفاده نکنند وجود دارد. با سرویس رایانش ابری، هزینه‌ی شرکت‌ها با مدل رایانش تجهیزات محاسبه می‌شود. یعنی یک سیستم «هرچقدر استفاده می‌کنید همان‌قدر پرداخت کنید» که در آن شرکت‌ها تنها پول منابعی را می‌پردازند که از آن استفاده می‌کنند. این استفاده معمولاً محاسبه‌شده و صورتحساب آن بر اساس فعالیت‌های پهنای باند و سطوح استفاده از داده تهیه می‌شود.

ابر دوگانه

زمانی که یک سازمان سخت‌افزارهای سرور خود را برای یک ابر خصوصی در اختیار دارد، ولی به خاطر افزایش ترافیک نامنظم به منابع بیشتری نیاز پیدا می‌کند، ابر دوگانه راهکاری است که معمولاً مورداستفاده قرار می‌گیرد. این راهکار ویژگی‌های ابر خصوصی و عمومی را باهم ترکیب می‌کند، و معمولاً برای ذخیره‌سازی‌های معمولی از ابر خصوصی استفاده کرده و زمانی که ترافیک اینترنت افزایش پیدا می‌کند، به ابر عمومی روی می‌آورد.