تهدید مدرن؛ حملات سایبری

مرور «شرق» بر حملات سایبری در یک سال گذشته و بررسی نظر کارشناسان در این زمینه

عکس: AFP

مریم لطفی: حملات سایبری در ایران هم مانند همه جای دنیا هست؛ اما به نظر می‌رسد این ماجرا در یک سال گذشته قوت بیشتری گرفته است. از شهریور سال گذشته اخباری مبنی بر هک چند سایت دولتی مانند بانک مرکزی، درگاه ملی دولت هوشمند و وزارت فرهنگ و ارشاد اسلامی منتشر شد و برخی کاربران اعلام کرده بودند نمی‌توانند به این سایت‌ها دسترسی داشته باشند.

هرکدام از این موارد هم با حاشیه‌هایی همراه بود؛ مثلا درباره حمله سایبری به بانک مرکزی سخنگوی این بانک هک سایت بانک را تکذیب کرد و گفت که درگاه اینترنتی بانک مرکزی صرفا دقایقی به دلیل حمله به کانال ارائه‌دهنده خدمات اینترنتی به بانک مرکزی، از دسترس خارج شده بود و کمی بعد هم رفع اشکال شده و سایت در دسترس مخاطبان قرار گرفته است. همان روز، ۳۰ شهریور ۱۴۰۱ گروه هکری «انانیموس» با انتشار پیامی علیه ایران مدعی شد که هک‌کردن سایت دولت از طرف این گروه انجام شده است.

انانیموس به معنای گمنام است. انانیموس خودش را گروهی نامتمرکز از متخصصان امنیت شبکه‌های رایانه‌ای معرفی کرده که به صورت ناشناس به‌عنوان هکتیویسم فعالیت می‌کند.

ماجرای هک برخی سایت‌های دولتی یا حملات سایبری به آنها گامی جدی‌تر از همین اختلال موقتی بود که در بانک مرکزی عنوان شد. پیش از این موارد و در خرداد سایت شهرداری تهران هک شد. ماجرا به قدری جدی بود که تا مدتی بیخ پیدا کرد و سایت «تهران من» چند هفته از دسترس کاربران خارج شد. همان موقع شهرداری تهران در اطلاعیه‌ای گفت که حملات خرابکارانه به برخی سایت‌های خدماتی شهر تهران با هدف ایجاد نارضایتی و اختلال در خدمت‌رسانی صورت گرفته است. قابل ذکر است که قبل از هک سامانه شهرداری، سیستم پمپ بنزین‌ها هم هک شده بود. هک پمپ بنزین‌ها نیمه آذر ۱۴۰۱ اتفاق افتاد. سایت‌های داخلی نوشتند به دنبال بروز اختلال، جایگاه‌های سوخت در استان‌های مختلف کشور از مدار توزیع سوخت سهمیه‌ای خارج شدند، هم‌اکنون توزیع سوخت به صورت آزاد در حال انجام است. ۱۲ آذر ۱۴۰۱ خبرگزاری مهر به نقل از یک منبع نزدیک به شورای عالی امنیت ملی، حمله سایبری به جایگاه‌های سوخت را در حالی تأیید کرد که احمد وحیدی، وزیر کشور، ماجرا را تنها «ناشی از یک اشکال فنی و سامانه‌ای در ارائه خدمات در برخی از پمپ‌های بنزین» عنوان کرد. امسال هم اخبار حملات سایبری گاه به گاه به گوش می‌رسد. پریروز اعلام شد که سامانه ثبت احوال هک شده و یک گروه هکری مسئولیت این حمله را بر عهده گرفته و اعلام کرده است که اطلاعات ۱۳۰ میلیون نفر را به دست آورده است. گرچه به نظر می‌رسد موضوع چندان روشن نیست و هنوز علت از دسترس خارج‌شدن وب‌سایت این سازمان اعلام نشده است. پیش از آن هم خبر هک‌شدن پلتفرم تپسی بلوای شدیدی به پا کرده بود. ۱۱ شهریور امسال میلاد منشی‌پور، مدیرعامل تپسی، از هک‌شدن این شرکت به دست یک گروه هکری خبر داد و انگیزه آنها از این اقدام را اخاذی عنوان کرد. آن موقع اعلام شد که هکرها به اطلاعات شش میلیون راننده و ۱۲۷ میلیون مسافر شامل نام و کد ملی و جزئیات دیگری دسترسی پیدا کرده‌اند و گفته‌اند که در ازای دریافت ۱۳۵ هزار دلار از انتشار این اطلاعات پرهیز می‌کنند. تپسی هم رک و روشن گفت که با هکرها همکاری نمی‌کند و البته تا می‌توانست هم از سوی برخی متخصصان حوزه فاوا نواخته شد. این موضوع نگرانی‌های زیادی ایجاد کرده بود و درحالی‌که کارشناسان حوزه فناوری اطلاعات در شبکه‌های اجتماعی در حال بررسی و تحلیل بودند، سرهنگ رامین پاشایی، معاون اجتماعی پلیس فتا، به مهر گفت که شرکت تپسی از این گروه هکری شکایت کرده و بعد از انجام اقدامات قضائی، منبع آلودگی برطرف شده است و جای هیچ‌گونه نگرانی وجود ندارد. البته نگرانی برای برخی همچنان پابرجاست؛ چون با گذشت بیش از دو هفته از این موضوع هنوز تکلیف اطلاعات سرقت‌شده از تپسی مشخص نشده است.

کارشناسان چه می‌گویند؟

«حمله سایبری زمانی اتفاق می‌افتد که مجرمان سایبری سعی دارند به داده‌های الکترونیکی ذخیره‌شده در رایانه یا شبکه، دسترسی غیرقانونی پیدا کنند. هدف از این کار ممکن است واردکردن صدمه به شهرت، آسیب‌رساندن به یک کسب‌وکار یا یک شخص یا حتی به سرقت بردن داده‌های ارزشمند باشد. این در حالی است که حملات سایبری می‌تواند افراد، گروه‌ها، سازمان‌ها یا دولت‌ها را هدف قرار دهد». این تعریفی است که برخی سایت‌های تخصصی ارائه داده‌اند. همچنین گفته می‌شود «حملات سایبری داده‌هایی را نشانه می‌گیرند که مهاجمان می‌توانند کنترل‌های امنیتی شناخته‌شده مانند احراز هویت دومرحله‌ای را دور بزنند؛ بنابراین سازمان‌ها و شرکت‌های امنیتی باید بیشتر به رویکرد خود درباره امنیت سایبری فکر کنند».

سال گذشته باشگاه خبرنگاران در گزارشی به نقل از techjury خبر داد که در سراسر جهان روزانه ۳۰ هزار وب‌سایت هک می‌شوند. ۶۴ درصد از شرکت‌ها در سراسر جهان حداقل یک نوع حمله سایبری را تجربه کرده‌اند. در ماه مارس سال ۲۰۲۱، ۲۰ میلیون نقض داده اتفاق افتاده است. در سال ۲۰۲۰، موارد باج‌افزار ۱۵۰ درصد رشد کرد. ایمیل‌ها مسئول حدود ۹۴ درصد از کل بدافزارها هستند. هر ۳۹ ثانیه یک حمله جدید در جایی در وب رخ می‌دهد. روزانه به طور متوسط حدود ۲۴ هزار برنامه تلفن همراه مخرب در اینترنت مسدود می‌شود.

بنابراین ماجرا محدود به ایران نیست و در عصر ارتباطات و فناوری اطلاعات این ماجرا گریبان‌گیر تمام دنیاست. در یکی، دو سال گذشته که حملات سایبری در ایران هم نمود بیشتری پیدا کرد، جلسات بحث و بررسی درباره موضوع امنیت کم نبود. در خلال یکی از همین جلسات، رضا اخلاقی، نایب‌رئیس کمیسیون افتا (امنیت فضای تبادل داده) سازمان نظام صنفی رایانه‌ای استان تهران عنوان کرد که راهکارهای موجود در مواجهه با حمله هکری جواب نمی‌دهد و باید بتوانیم در وسط کار که از ابعاد حمله اطلاعات درستی به دست آوردیم، جلوی آن را بگیریم؛ «این مهم بدون داشتن اطلاعات فنی، آموزش و پایش دائمی میسر نیست و تنها با تکیه بر نیروی درون‌سازمانی نمی‌توان به آن دست پیدا کرد، بلکه باید آنچه را که از چشم مغفول مانده، بررسی کرد که این به معنای در اختیار داشتن اطلاعات دقیق است».

او همچنین به اهمیت رتبه‌بندی پیمانکاران و شرکت‌های طرف قرارداد در حوزه امنیت سایبری اشاره کرد: «متأسفانه اجرای مناقصه در حوزه امنیت سایبری سبب شده شرکت‌های بزرگ که دارای بدنه کارشناسی فنی و زبده‌ای هستند، از میدان رقابت خارج شده و شرکت‌های کوچک با تأمین حداقل‌ها، پروژه‌های حوزه امنیت سایبری را انجام دهند؛ درحالی‌که روش رتبه‌بندی باید تغییر کند و اولویت‌های جدیدی مدنظر قرار گیرد». رضا واحدی‌فر هم زمانی که عهده‌دار معاونت شبکه و امنیت سازمان فاوای شهرداری بود، پس از ماجرای حمله سایبری به سایت شهرداری، گفته بود که مشکلات موجود در جذب نیروی متخصص در اکوسیستم فناوری اطلاعات موضوع مهمی در مواجهه با حمله‌های سایبری است و در سطوح مختلف نیاز به پایش داریم تا بدانیم به لحاظ بلوغ امنیتی در چه سطحی قرار داریم.

آیدین عدالت، عضو هیئت‌مدیره و رئیس رسته سخت‌افزار و ارتباطات سازمان نظام صنفی رایانه‌ای تهران نیز به ایسنا گفته که در سال‌های گذشته تمرکز بر امنیت نه به اندازه کافی و شاید کمتر از مقداری که باید باشد، در این حوزه بوده و اشکال هم آنجاست که امنیت در حوزه فناوری اطلاعات بیشتر با فرایندها و روش‌ها اجرا می‌شود، نه با تجهیزات. به اعتقاد او «بودجه‌هایی که در سازمان‌ها وجود دارد، قدیمی هستند و هر سال حداکثر به اندازه تورم رشد دارند. اما دو موضوع مهم دراین‌باره وجود دارد؛ اول اینکه قیمت تجهیزات امنیتی در دنیا، جدا از نرخ ارز، به دلیل کمبود چیپ‌ست در سه سال اخیر، به دلیل بیماری کرونا بیش از سه برابر افزایش داشته است. مسئله دیگر محدود و معدودشدن تخصص امنیت و متخصصان آن است؛ یعنی سازمان‌ها انتظار دارند یک تکنیسین متخصص شبکه که فقط کارهای ابتدایی را انجام می‌دهد و حقوق آن به طور مثال ۱۰ میلیون تومان است، بتواند امنیت زیرساخت یک وب‌سایت دولتی را تأمین کند؛ بنابراین شاید مهم‌ترین موضوع بحث نیروی انسانی باشد که به‌عنوان مهره ایجاد امنیت در زیرساخت شبکه به شمار می‌رود و به عقیده کارشناسان بزرگ‌ترین پاشنه‌آشیل امنیت سایبری در ایران نیروی انسانی است و باید به مشکلات موجود در این بخش توجه شود».

به افزایش آگاهی نیازمندیم

بهناز آریا، رئیس کمیسیون افتای سازمان نظام صنفی رایانه‌ای استان تهران، هم در توضیحاتی به «شرق» می‌گوید: «اتفاقی که برای شرکت تپسی و برخی دیگر از سازمان‌ها و مجموعه‌ها نیز رخ داده است، منحصر به ایران نیست. اولین بار نیست که اتفاقات این‌چنینی رخ می‌دهد و چالش بزرگی است که تمام دنیا با آن درگیر هستند. طبق آخرین گزارش‌هایی که وجود دارد، از فوریه سال ۲۰۲۲ میزان حملات سایبری در جهان هشت هزار درصد افزایش پیدا کرده است. این در حالی است که در میانه عصر دیجیتال هستیم و تقریبا همه چیز در آینده نزدیک به هم متصل خواهد بود. با توجه به این مسئله همه چیز قابلیت هک خواهد داشت. درحال‌حاضر مهم‌ترین دارایی، دارایی اطلاعاتی است و صاحبان آنها باید از این دارایی‌ها محافظت کنند. در واقع هم سازمان‌ها و کسب‌وکارها و هم خود افراد باید از این دارایی‌ها مراقبت کنند و مسئول هستند».

او معتقد است در موضوع امنیت مبحث بسیار مهم آگاهی‌رسانی است: «اهمیت این مسئله به این خاطر است که انسان‌ها ضعیف‌ترین حلقه‌ها در زنجیره امنیت هستند. باید تلاش شود تا با آگاهی‌رسانی، دانش افراد در این زمینه افزایش پیدا کند. در این مسیر باید دانش عمومی جامعه را افزایش دهیم و توجه افراد را به این حوزه جلب کنیم. وقتی شرکت‌هایی مثل تپسی که ارائه‌دهنده خدمات عمومی هستند، از این ناحیه ضربه می‌خورند، کاربران نسبت به حفظ اطلاعات خود احساس خطر می‌کنند. در واقع این احساس خطر فرصتی است تا با آگاهی‌رسانی به کاربران، دانش آنها را در این زمینه افزایش دهیم». آریا تأکید می‌کند که فرایند آگاهی‌رسانی در این زمینه باید در جامعه از بالا به پایین باشد و دولت نقش بسیار پررنگی در این زمینه دارد؛ «تمام شرکت‌ها و ارگان‌ها نیز باید او را همراهی کنند. درحال‌حاضر ریسک شماره یک همه کسب‌وکارها در ایران و جهان امنیت سایبری است و در واقع این موضوع باید بیشترین اولویت را برای آنها داشته باشد».

امنیت صددرصدی وجود ندارد

او با اشاره به حملات سایبری اخیر از سایت شهرداری گرفته تا صداوسیما و برخی شرکت‌های خصوصی توضیح می‌دهد: «متأسفانه در حملات اخیر شاهد تکرار رخدادها از آسیب‌پذیری‌های رخدادهای پیشین هستیم. در حوزه امنیت سایبری امنیت صددرصدی وجود ندارد؛ اما وقتی یک حمله امنیتی رخ می‌دهد، اگر اصلاحات و به‌روزرسانی‌های لازم را انجام ندهیم و دوباره با روش قبلی ضربه بخوریم، یعنی عملکرد مناسبی در حفظ امنیت اطلاعات خود نداشته‌ایم. یکی از مواردی که باعث نگرانی بخش خصوصی شده، همین تکرار آسیب‌پذیری با روش‌های قبلی است.

همچنین یکی دیگر از خواسته‌های ما در بخش خصوصی این است که در حدی که مسائل محرمانگی رعایت می‌شود، باید اطلاعات این رخدادها با متخصصان و شرکت‌های امنیت سایبری این بخش به اشتراک گذاشته شود. در واقع باید تلاش شود تا بخش خصوصی به‌عنوان بازوی اجرائی بخش دولتی در این زمینه دیده شود».

او ادامه می‌دهد: «یکی از چالش‌های جدی دیگر این حوزه ترک فعل مدیران به‌ویژه در سازمان‌های دولت است. وقتی یک سازمان دولتی یا زیرساخت عمومی دچار مشکل امنیتی می‌شود، هیچ‌کس پاسخ‌گو نیست. تنها کسی که در این زمینه معمولا مقصر شناخته می‌شود، بخش خصوصی است. این در حالی است که مقصر اصلی بخشی است که خدمت اصلی را ارائه داده است، چه در بخش خصوصی و چه در سازمان دولتی و دستگاه اجرائی و باید پاسخ‌گو باشد. حاصل این وضعیت این بوده است که امنیت به چشم اولویت دیده نمی‌شود و صنعت مهم افتا به‌درستی رشد نمی‌کند. متأسفانه حملات این‌چنینی اتفاق می‌افتد، بدون آنکه ما اصلاحی را در این وضعیت ببینیم».

آریا می‌گوید برای جلوگیری از این اتفاقات، باید در درجه اول صنعت افتا به‌عنوان یکی از صنایع اولویت‌دار، پرکاربرد و دارای نقش اقتصادی بسیار مهم دیده شود؛ «همچنین بخش خصوصی باید نقش اجرائی پررنگ‌تری داشته باشد. درعین‌حال باید روش‌ها و دستورکارهای فعلی را در سازمان‌های مختلف اصلاح کنیم و به امنیت در سمت بهره‌بردار هم علاوه بر مبادی ورودی تأکید کنیم. باید نظارت مستمر بر امنیت سازمان‌ها و مجموعه‌ها انجام شود و از تست نفوذهای دوره‌ای، باگ بانتی و آموزش افراد و موارد مشابه غافل نشویم».

او تأکید می‌کند: «راهی جز تقویت صنعت افتا برای ارتقای سطح امنیت کشور و دارایی‌های اطلاعاتی وجود نداشته و نقش بخش خصوصی و تشکل‌های بخش خصوصی در این صنعت انکارناپذیر است».

اخبار برگزیده

کلاف پیچیده امنیت

ایسنا: بستر مجازی اینترنت، فضای مناسبی را برای مجرمان فراهم آورده است و کاربران برای آنکه سیستم و رایانه خود را از آسیب این افراد محافظت کنند، باید برخی راهکارهای امنیتی را به کار ببندند. طبق آمارهای رسمی، بدافزارها و حملات فیشینگ می‌توانند به‌طور متوسط ۲.۴ میلیون دلار به شرکت‌ها و کسب‌وکارها خسارت وارد کنند و این رقم روز به روز در حال افزایش است؛ زیرا شمار کاربران اینترنت نیز دائما بالا می‌رود. در واقع رشد روزافزون سایت‌ها و کاربران اینترنتی، پای افراد سودجو و سارقان را به این حوزه باز کرده است. کاربران ممکن است هر لحظه مورد حمله سایبری قرار بگیرند و اطلاعات یا اموال خود را از دست دهند. بنابراین برای در امان ماندن از این حملات باید راهکارهایی از قبل به کار گرفته شود تا گرفتار تله این افراد سودجو نشوند. حملات سایبری معمولا با چهار روش کلی امنیت سیستم یا وب‌سایت کاربران را تحت تأثیر قرار می‌دهند؛ بدافزارها، آسیب‌پذیری وصله‌های امنیتی، ترافیک غیرانسانی و مهندسی اجتماعی. در این روش مجرمان از طریق ایمیل یا هر چیز دیگری با مخاطب خود ارتباط برقرار کرده و با قانونی جلوه‌دادن عملکرد خود آنها را فریب می‌دهند، سپس کاربران اطلاعات خود را در اختیار این افراد قرار می‌دهند، بدون آنکه از پیامد این کار خود مطلع باشند. مثلا مجرمی با مخاطب خود تماس گرفته و به او می‌گوید قصد دارد که برای سایتش به‌صورت رایگان تست امنیت را انجام دهد در نتیجه به داده‌ها نیاز دارد. از این طریق کاربران مجاب می‌شوند که این کار قانونی است و بهتر است داده‌ها در اختیار این فرد قرار بگیرند؛ غافل از اینکه حمله سایبری صورت گرفته و امنیت سایت زیر می‌رود.

اعتیاد، عامل ۲۵ درصد قتل‌ها

به گزارش ایرنا، علیرضا کاظمی، قائم‌مقام دبیرکل ستاد مبارزه با مواد مخدر، گفت: اکنون ۵۵ درصد طلاق‌ها، ۳۰ درصد کودک‌آزاری‌ها و ۲۵ درصد قتل‌ها ناشی از اعتیاد است که نشان‌دهنده آسیب‌های جدید این بحران جامعه‌برانداز است. بحران اعتیاد یکی از چهار بحران بزرگ و خانمان‌برانداز جهان است که پس از فقر، سلاح‌های کشتارجمعی و بحران زیست‌محیطی، سلامت جامعه بشری را تهدید می‌کند. اینکه امروز بیش از ۹۰ درصد جامعه مشکل اعتیاد را مهم‌ترین دغدغه می‌دانند، نشان از اهمیت موضوع اعتیاد در مقایسه با مسائل و دغدغه‌های امنیتی و اقتصادی دارد. پیامدهایی مانند بی‌خانمانی و بحران‌های امنیتی و متلاشی‌شدن خانواده از مهم‌ترین اثرات اعتیاد است که علاوه بر افراد مستقیم، اعضای غیرمستقیم جامعه را نیز مورد تهدید قرار می‌دهد. قائم‌مقام دبیرکل ستاد مبارزه با مواد مخدر بر حرکت پژوهش‌های علمی بر مسیر مسئله‌محوری و حل مشکل تأکید کرد و افزود: امروز کشور چالش‌هایی دارد که لازم است با تکیه بر روش‌ها و پژوهش‌های علمی حل شود. با وجود ۱۱۴ سال مبارزه جهانی با معضل اعتیاد، همچنان روند فزاینده مصرف و شیوع را در دنیا شاهد هستیم که یکی از دلایل آن مربوط به موضوع عرضه و اقتصاد پرسود این حوزه است و گردش ۵۰۰ میلیارد دلاری را به همراه دارد. کاظمی اضافه کرد: علاوه بر این ضعف‌های قانونی که در کشور و دنیا وجود دارد، از دیگر عوامل، روند فزاینده مصرف است. همچنین بحران‌های سیاسی و اجتماعی و بحران‌های روانی و تنوع در نوع مواد مخدر جدید و نبود آگاهی لازم به‌ویژه نسل‌های جوان به این روند فزاینده افزوده است.

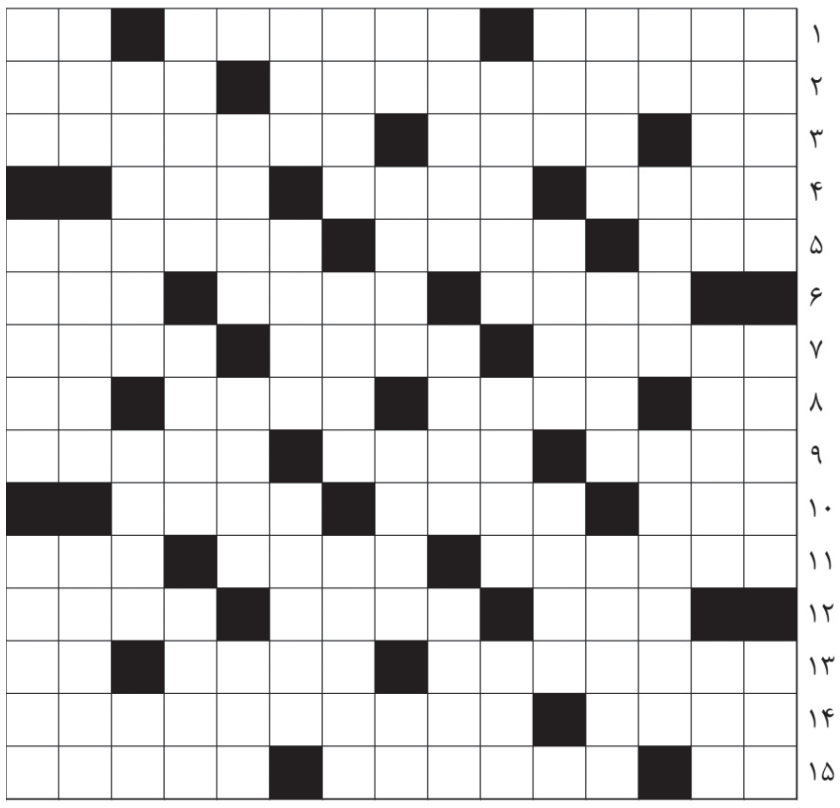
جدول ۴۵۹۵ • طراح: بیژن گورانی

افقی:

۱- یاری‌کننده- غذایی از قطعات گوشت کباب‌شده گاو- نشانه جمع فارسی ۲- داستانی از جان کریستوفر، نویسنده علمی-تخیلی انگلیسی- پروانه وکالت دارد ۳- جوی خون- گلی زیبا- آخرین رهبر شوروی سابق ۴- منطقه آباد در نواحی بیابانی- کننده کاری- از اجزای شلوار ۵- میثاق- خبرگزاری ایتالیا- ارزیابی بدن برای تشخیص بیماری ۶- هر یک از آپارتمان‌های یک ساختمان- فتوادهنده- پلان سینمایی ۷- کهنه و فرسوده- برتر- دوزخ ۸- سوره بیستم قرآن- نسوان- رسوم- زائوترسان ۹- خط تلفن- دستگاه تولید آب سرد برای سیستم‌های تهویه مطبوع- از اصلی‌ترین جزئیات مبلمان شهری ۱۰- میدانی در تهران- عبادت‌کننده- میان‌ها ۱۱- فراوان- صفحات داخلی روزنامه- از شهدای نامی کربلا ۱۲- آخرین سوره- زشت و ناپسند- مردار ۱۳- سنجد- شهری در فرانسه- حرف فاصله ۱۴- ایشان- مؤسسه آموزش موسیقی ۱۵- چنین باری به منزل نمی‌رسد- خوش‌رفتاری- روستای کوچک

عمودی:

۱- شرعی- مورد نظر- شکاف ۲- دستگاهی در موسیقی ایرانی- مخفی- گنجشک ۳- مخفف اگر- اندازه و مقدار- دومین روز هفته ۴- علت آن تحریک مخاط حفره بینی است- خوراک قناری- مدت زمان طولانی ۵- سطل چاه- بهتر- سازمان فضانوردی آمریکا ۶- برای دفع چشم‌زخم در آتش می‌ریزند- ادویه سنتی سیستان‌وبلوچستان- شهری در مازندران ۷- گیاه رنگرزی- همدم- گروی ۸- چاشنی غذایی- آبادکننده- پرنده‌ای با پاهای بلند- زهر ۹- سرزنده و شاداب- تبهکاران-ام‌الشرائین ۱۰- بی‌عرضه- یکپارچه و هماهنگ- بهره هوشی ۱۱- نوعی طلاق- جنس ماده- مسرور ۱۲- ترس نامعقول- پیشانی- ترشی بادمجان ۱۳- هیئت دولت- پناهگاه- نوک بی‌نوک! ۱۴- از مجسمه‌های زیبای ساخته پرویز تناولی- مرطوب- عددی دورقمی ۱۵- حرف اول- نمایش‌نامه معروف شکسپیر- کشت اول سال



حل سودوکو سخت

۴	۸	۷	۳	۹	۵	۱	۶	۲
۲	۱	۳	۶	۸	۴	۹	۷	۵
۹	۶	۵	۷	۲	۱	۴	۳	۸
۱	۳	۲	۹	۴	۶	۵	۸	۷
۶	۴	۹	۵	۷	۸	۲	۱	۳
۵	۷	۸	۲	۱	۳	۶	۴	۹
۳	۲	۶	۱	۵	۷	۸	۹	۴
۷	۹	۴	۸	۶	۲	۳	۵	۱
۸	۵	۱	۴	۳	۹	۷	۲	۶

حل سودوکو ۳۵۹۰

۵	۴	۳	۶	۱	۲	۸	۹	۷
۸	۲	۱	۹	۷	۵	۴	۶	۳
۹	۶	۷	۴	۳	۸	۱	۵	۲
۴	۵	۲	۸	۶	۱	۳	۷	۹
۳	۱	۶	۷	۲	۹	۵	۸	۴
۷	۸	۹	۳	۵	۴	۶	۲	۱
۲	۳	۵	۱	۹	۶	۷	۴	۸
۶	۷	۴	۲	۸	۳	۹	۱	۵
۱	۹	۸	۵	۴	۷	۲	۳	۶

حل جدول ۴۵۹۴

	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
۱	چ	ک	ر	■	م	س	ک	و	ن	ی	■	ک	ب	ر	ی
۲	م	ن	و	چ	ه	ر	ی	■	ا	م	ب	ا	ب	ا	ن
۳	ل	ا	■	پ	ی	ش	د	ا	د	ی	ا	ن	■	ه	ا
۴	■	ه	م	ا	ن	ا	■	م	ا	ن	ی	■	ح	ا	ل
۵	ب	د	ب	و	■	خ	ا	ی	ن	■	ن	ف	ق	ه	■
۶	ت	ر	ی	ل	ر	■	ر	ا	ی	ش	■	ل	ن	ی	ت
۷	ا	ی	ن	■	ا	ن	ک	ل	■	ک	ن	ا	ر	■	ا
۸	د	ا	■	ش	ی	و	ن	■	خ	و	ی	ش	■	م	ر
۹	ی	■	ک	ا	ت	ب	■	م	ا	ر	ک	■	م	ر	ز
۱۰	ن	ی	ن	ی	■	ل	ک	ا	م	■	ل	ا	ن	د	ا
۱۱	■	و	ا	ع	ظ	■	ا	ن	س	ا	■	ب	ی	ا	ن
۱۲	ش	ن	م	■	ه	م	ل	ت	■	ش	ا	ک	ر	د	■
۱۳	ی	ی	■	ف	ی	ز	ی	و	ل	و	ژ	ی	■	ک	م
۱۴	ا	د	م	ی	ر	ا	ل	■	ق	ر	ا	ر	د	ا	د
۱۵	د	و	ی	ل	■	د	ه	ن	ب	ی	ن	■	ب	ن	ت

سودوکو سخت ۳۵۹۱

زمان پیشنهادی: ۴۰ دقیقه

قانون‌های حل جدول سودوکو:

۱- در هر سطر و ستون باید اعداد یک تا ۹ نوشته شود. بدیهی است که هیچ عددی نباید تکرار شود.

۲- در هر مربع ۳×۳ اعداد یک تا ۹ باید نوشته شود و در نتیجه هیچ عددی نباید تکرار شود.

۸		۵		۲			۹	
	۶			۴			۵	۷
			۵		۱	۶		
۳							۶	
	۷			۱			۴	
	۹							۸
		۴	۲		۳			
۱	۲			۶			۳	
	۳			۷		۸		۵

سودوکو ساده ۳۵۹۱

زمان پیشنهادی: ۲۰ دقیقه

سودوکو

سودوکو Sudoku یک واژه ترکیبی ژاپنی به معنای عددهای بی‌تکرار است و امروزه به جدولی از اعداد گفته می‌شود که به عنوان یک سرگرمی رایج در نشریات کشورهای مختلف به چاپ می‌رسد.

۴		۱	۹					
۳	۸	۷		۴				
	۶			۷	۱			
			۶			۸		
۶	۱		۷	۵	۲		۹	۴
		۵			۸			
			۱	۸			۴	
				۹		۲	۸	۶
					۷	۹		۵