یادداشت

اعتماد را نمی‌توان قسطی کرد

حکمرانی ارتباطات در اقتصاد تورمی

پیام فیض
کارشناس ارشد روابط عمومی

سبقت قیمت‌ها از تصمیم خرید، لحظه پرداخت را از یک کنش روزمره اقتصادی به یک شوک روانی تبدیل کرده است. وقتی اعداد روی تابلوها و فاکتورها، روزانه قد می‌کشند، مصرف‌کننده برای حفظ کیفیت زندگی‌اش به «اعتبار» پناه می‌برد و بنگاه‌های اقتصادی برای زنده‌ماندن، فروش را به آینده و اقساط موکول می‌کنند. آمارهای اخیر از ثبت ۱۳۲ هزار میلیارد تومان تراکنش اعتباری (BNPL) در یک سال، شاید برای پلتفرم‌های مالی یک دستاورد باشد، اما در لایه‌های عمیق‌تر اجتماعی، آژیر خطری است از فشار نقدینگی بر گلوی خانوار ایرانی. در این بزنگاهِ پرالتهاب، یک پرسش استراتژیک مطرح می‌شود: وقتی سازمان مجبور است قیمت را بالا ببرد تا زنده بماند، چگونه می‌تواند مشتری را حفظ کند و هم‌زمان درباره هزینه‌ها و محدودیت‌ها با او صادق بماند؟ اینجاست که مرز میان یک «روابط‌عمومی نمایشی» و «حکمرانی ارتباطات» مشخص می‌شود.

روابط‌عمومی؛ سپر بلا یا پل ارتباطی؟

بزرگ‌ترین خطای استراتژیک در بسیاری از سازمان‌های ایرانی این است که روابط‌عمومی را صرفا «واحد اعلام گرانی» یا «توجیه‌کننده شرایط» می‌دانند. وقتی هزینه تأمین مواد اولیه (طبق گزارش‌های رسمی شامخ) به‌شدت بالا می‌رود، مدیران پشت درهای بسته تصمیم به افزایش قیمت می‌گیرند و سپس از روابط‌عمومی می‌خواهند تا با ادبیاتی مبهم، این افزایش را برای مشتری عادی‌سازی کند. این سکوت یا توجیه ناشیانه، خیانت به برند است. حکمرانی ارتباطات یعنی عبور از توجیه و رسیدن به «شفافیت عملیاتی». روابط‌عمومی باید در هسته تصمیم‌سازی حضور داشته باشد تا پیش از اجرای هر کمپین فروش یا افزایش قیمتی، مشخص کند مسئول توضیح این تغییر کیست و مشتری دقیقا بابت چه ارزش افزوده‌ای باید بهای بیشتری بپردازد.

الگوی جهانی: شفافیت به‌جای پنهان‌کاری

برای درک این مهم، نیازی نیست اقتصادهای باثبات را مثال بزنیم. در دوران اوج تورم جهانی پس از کرونا، برندی مثل «استارباکس» با بحران شدید افزایش قیمت مواد اولیه (قهوه و شیر) مواجه شد. استارباکس به‌جای پنهان‌کردن افزایش قیمت‌ها یا استفاده از کلمات فریبنده، استراتژی شفافیت و «حکمرانی همدلی» را انتخاب کرد. این برند به صراحت اعلام کرد قیمت‌ها بالا می‌رود، اما هم‌زمان به‌طور گسترده در رسانه‌ها نشان داد که این افزایش قیمت برای جلوگیری از کاهش کیفیت قهوه و مهم‌تر از آن برای «حفظ دستمزد و امنیت روانی پرسنل و باریستاها» اعمال می‌شود. مشتری استارباکس گرانی را پذیرفت، چون ارتباطات سازمان به او نشان داد که این پولِ اضافه، خرج حفظ استانداردهایی می‌شود که مشتری به آنها اعتماد دارد.

ارکان سه‌گانه نجات اعتبار

در اقتصاد ناپایدار ایران، به‌ویژه در صنایع حساسی که به‌طور مستقیم با سلامت و جان مردم سروکار دارند (مانند صنعت دارو و تجهیزات پزشکی)، این حکمرانی ارتباطی اهمیتی حیاتی و دوچندان می‌یابد. در حوزه‌ای مثل دارو، افزایش قیمت به صورت مستقیم با اضطراب بقا گره خورده است. در چنین صنایعی، سازمان نمی‌تواند صرفا یک فروشنده حق‌به‌جانب باشد، بلکه باید این سه رکن را در استراتژی ارتباطی خود پیاده کند:

۱. تغییر لحن برند: سازمان باید از موضع «تأمین‌کننده بی‌تفاوت» خارج شده و به «هم‌سنگر مضطرب مشتری در یک اقتصاد تورمی» تبدیل شود. درک متقابل و همدلی در پیام‌های رسمی، اولین قدم برای حفظ اعتماد است.

۲. صداقت در زنجیره تأمین: مشتری حق دارد بداند چرا بهای کالا افزایش یافته است. برجسته‌کردن اقساط کوچک بدون توضیح تعهد نهایی، شاید امروز فروش را حفظ کند، اما رابطه فردا را ویران می‌کند. سازمان باید با شجاعت سهم عوامل مختلف در گرانی را توضیح دهد.

۳. تأمین امنیت روانی درون‌سازمانی: تورم، پیش از مشتری، پرسنل خط مقدم (فروش، پشتیبانی و تولید) را فرسوده می‌کند. روابط‌عمومی باید پیش از بیرون، امید و چشم‌انداز را در داخل سازمان مدیریت کند؛ پرسنلی که خود به برند بی‌اعتماد باشد، نمی‌تواند مشتری را قانع کند.

یادداشت کامل را در سایت شرق بخوانید

سرقت ۶.۳ میلیارد دلاری از بزرگ‌ترین صرافی رمزارز جهان

ردپای کره شمالی در هک بایننس

شرق: بزرگ‌ترین صرافی رمزارز جهان در فاصله‌ای کوتاه شاهد خروج میلیاردها دلار دارایی از کیف‌پول‌های خود بود؛ رخدادی که نه‌تنها رکورد سرقت‌های ثبت‌شده در صنعت رمزارز را جابه‌جا کرده، بلکه بار دیگر پرسش درباره امنیت زیرساخت‌های صرافی‌های متمرکز، امکان جبران خسارت کاربران و نقش شبکه‌های هکری تحت حمایت دولت‌ها در سرقت دارایی‌های دیجیتال را به صدر اخبار بازگردانده است. بایننس می‌گوید برآورد اولیه از این سرقت حدود ۶.۳ میلیارد دلار می‌رسد. از سوی دیگر بررسی‌های اولیه از احتمال نفوذ به کیف‌پول‌های این صرافی رمزارز از طریق لپ‌تاپ یکی از مهندسان این شرکت حکایت دارد. درحالی‌که این صرافی از مسدودشدن میلیاردها دلار دارایی مرتبط با حادثه و تعهد خود به جبران خسارت‌ها خبر داده، شرکت اطلاعات بلاک‌چین TRM Labs حمله را با اطمینان بالا به گروه هکری TraderTraitor، مرتبط با کره شمالی، نسبت داده است؛ ارتباطی که هنوز با گزارش نهایی بایننس یا اعلام رسمی نهادهای قضائی درباره هویت مهاجمان همراه نشده است.

از یک لپ‌تاپ تا خروج میلیاردها دلار دارایی

بایننس در اطلاعیه‌ای که ۳۰ اکتبر (۸ آبان) منتشر کرد، خبر داد که بررسی‌های اولیه نشان می‌دهد این رخداد امنیتی ممکن است با به‌خطر افتادن لپ‌تاپ یکی از مهندسان تیم DevOps شرکت آغاز شده باشد. به گفته این شرکت، مهاجم احتمالاً از طریق این دستگاه به یک محفظه سرویس (Service Container) دسترسی پیدا کرده و توانسته است تراکنش‌های برداشت غیرمجاز را ثبت کند. بایننس تأکید کرده که تاکنون شواهدی از افشای کلیدهای خصوصی کیف‌پول‌های خود پیدا نکرده است. این شرکت همچنین گفته پس از تکمیل تحقیقات، گزارش فنی مفصلی از نحوه وقوع حادثه منتشر خواهد کرد. بنابراین، تا زمان انتشار گزارش نهایی، مسیر دقیق نفوذ، نحوه دستیابی مهاجم به مجوزهای لازم برای اجرای تراکنش‌ها و جزئیات مسئولیت هر بخش از زیرساخت امنیتی بایننس به‌طور کامل روشن نیست. بر اساس گزارش TRM Labs، در ۲۹ اکتبر حدود ۶.۳۶ میلیارد دلار دارایی از کیف‌پول‌های منتسب به بایننس در ۱۰ شبکه بلاک‌چینی خارج شده است. بخش عمده انتقال‌ها در فاصله‌ای حدود ۲۰ دقیقه انجام شده و موج دیگری از تراکنش‌ها نیز در ساعات بعدی ادامه یافته است. این شرکت ارزش دارایی‌ها را بر مبنای قیمت آنها هنگام انتقال محاسبه کرده است؛ ارزش همان دارایی‌ها با قیمت‌های بعدی بازار می‌تواند متفاوت باشد. گزارش TRM Labs نشان می‌دهد دارایی‌های خارج‌شده فقط به یک رمزارز یا یک شبکه محدود نبوده‌اند. اتر، بیت‌کوین، تتر، یواس‌دی‌کوین، ریپل و چندین دارایی دیگر در میان انتقال‌ها قرار داشته‌اند. رویترز در گزارش خود در این مورد نوشته است که این گستردگی، حادثه را از یک برداشت غیرمجاز محدود به یک کیف‌پول متمایز می‌کند و ضرورت بررسی سازوکار امضای تراکنش‌ها و کنترل دسترسی در چند شبکه را برجسته می‌کند.

یک برداشت هوشمند

یکی از جزئیات فنی مهمی که TRM Labs در بررسی این حادثه مطرح کرده، استفاده از سازوکار EIP-7702 در شبکه اتریوم است. این سازوکار به یک حساب معمولی اجازه می‌دهد با امضای مجاز، اجرای عملیات مشخصی را به کد یک قرارداد هوشمند واگذار کند. هدف از طراحی چنین قابلیتی، گسترش امکانات حساب‌های اتریوم است؛ بنابراین، وجود آن به‌خودی‌خود به معنای وجود یک آسیب‌پذیری امنیتی نیست. طبق گزارش TRM Labs، مهاجم در بخش اتریوم از مجوزهای امضاشده‌ای استفاده کرده که از پیش آماده شده بودند و به او امکان می‌دادند یک کیف‌پول گرم بایننس را برای اجرای انتقال دارایی‌ها تحت کنترل عملیاتی خود درآورد. این شرکت از آماده‌سازی ۵۰ مجوز امضاشده پیش از اجرای حمله خبر داده است. در سایر شبکه‌های درگیر نیز انتقال‌ها با امضاهای معتبر ثبت شده‌اند. اهمیت این جزئیات در آن است که یک تراکنش دارای امضای معتبر الزاماً به معنای صدور آگاهانه و مجاز آن از سوی مالک دارایی نیست. اگر مهاجم بتواند به فرایند تأیید یا اجرای تراکنش دسترسی پیدا کند، ممکن است سامانه، تراکنش را از نظر فنی معتبر تشخیص دهد، درحالی‌که هدف واقعی آن با خواست مالک کیف‌پول متفاوت



است. این تفاوت، یکی از چالش‌های اساسی امنیت دارایی‌های دیجیتال است: بلاک‌چین می‌تواند ثبت تراکنش، امضا و جابه‌جایی دارایی را به‌صورت شفاف و تغییرناپذیر نشان دهد، اما به‌تنهایی مشخص نمی‌کند که چه کسی پشت فرایند صدور یک امضای معتبر قرار داشته یا آیا مجوز مورد استفاده به‌درستی به کار گرفته شده است.با وجود اطلاعات منتشرشده درباره EIP-7702، جزئیات نهایی چگونگی دسترسی مهاجم به سامانه‌های داخلی بایننس و رابطه دقیق میان دستگاه مهندس، محفظه سرویس و فرایند امضای تراکنش‌ها هنوز به گزارش رسمی تکمیلی نیاز دارد.

چرا مسدودشدن دارایی به معنای پایان بحران نیست؟

بایننس اعلام کرده است با کمک شرکای خود در صنعت بلاک‌چین، حدود ۳ میلیارد دلار از دارایی‌های مرتبط با این حادثه را مسدود کرده است. بااین‌حال، گزارش TRM Labs از مسدودشدن حدود ۲.۷ میلیارد دلار دارایی، شامل استیبل‌کوین‌ها و دارایی‌هایی در شبکه آربیتروم، حکایت دارد. این ارقام به زمان و دامنه محاسبه هر گزارش وابسته‌اند و نباید بدون بررسی تراکنش‌ها و احتمال هم‌پوشانی، به‌عنوان دو رقم مستقل با یکدیگر جمع شوند. از طرفی مسدودسازی دارایی‌ها در شبکه‌های رمزارزی یکسان نیست. صادرکنندگان متمرکز استیبل‌کوین‌هایی مانند تتر و یواس‌دی‌کوین می‌توانند در شرایط مشخص، آدرس‌هایی را که با فعالیت غیرقانونی مرتبط تشخیص داده شده‌اند، در فهرست مسدودسازی قرار دهند. چنین اقدامی می‌تواند انتقال یا خرج‌کردن توکن‌های مربوط را متوقف کند. در شبکه‌هایی مانند بیت‌کوین، سازوکار مشابهی برای مسدودسازی مستقیم یک آدرس به دست صادرکننده وجود ندارد؛ زیرا بیت‌کوین صادرکننده متمرکزی ندارد که بتواند دارایی‌های یک آدرس را به‌طور یک‌جانبه متوقف کند. همین تفاوت، زمان را به عاملی تعیین‌کننده در مهار سرقت تبدیل می‌کند. مهاجم می‌تواند تلاش کند دارایی‌های قابل‌مسدودسازی را به دارایی‌های دیگر تبدیل کند یا آنها را از مسیرهای مختلف انتقال دهد. در گزارش TRM Labs، به تبدیل بخشی از استیبل‌کوین‌ها از طریق معامله‌گران بازار و استفاده از پروتکل وام‌دهی Aave اشاره شده است. در مقابل، ردیابی تراکنش‌ها و شناسایی آدرس‌های مرتبط با مهاجم به‌تنهایی به معنای بازگرداندن دارایی‌ها نیست. برای بازپس‌گیری وجوه ممکن است همکاری صرافی‌ها، صادرکنندگان توکن، پلتفرم‌های معاملاتی و نهادهای اجرای قانون لازم باشد. بنابراین، رقم دارایی‌های مسدودشده را نباید با رقم دارایی‌های بازگردانده‌شده یا میزان زیان نهایی یکسان دانست.

خسارت جبران می‌شود

بایننس اعلام کرده است تمام زیان‌های ناشی از حادثه را از محل صندوق اضطراری SAFU و منابع مالی شرکت جبران خواهد کرد. این صندوق که با هدف حمایت از کاربران در شرایط اضطراری ایجاد شده، پیش‌تر نیز برای پوشش خسارت یک رخداد امنیتی در بایننس مورد استفاده قرار گرفته بود. بااین‌حال، به گفته تحلیلگران اعلام تعهد به جبران خسارت با انتشار صورت‌حساب نهایی جبران و تأیید مستقل وضعیت ذخایر یکسان نیست. بایننس گفته است پس از تکمیل اقدامات اصلاحی، گزارش به‌روزشده اثبات ذخایر خود را منتشر می‌کند. انتشار این گزارش می‌تواند برای ارزیابی وضعیت دارایی‌های پشتیبان کاربران اهمیت داشته باشد؛ هرچند اثبات ذخایر به‌تنهایی جایگزین حسابرسی جامع صورت‌های مالی، بدهی‌ها و تمام تعهدات یک شرکت نیست. این صرافی همچنین از تعلیق موقت واریز و برداشت‌ها در جریان بررسی‌های امنیتی و لغو مجوزهای مربوط به آدرس‌های آسیب‌دیده خبر داده است. وضعیت نهایی خدمات، میزان دقیق دارایی‌های بازیابی‌شده و نحوه اجرای جبران خسارت به اطلاعیه‌های بعدی شرکت وابسته است. در چنین رخدادی، مسئله تنها این نیست که شرکت چه میزان منابع مالی در اختیار دارد؛ بلکه مهم است آیا می‌تواند در زمانی کوتاه به تعهدات خود عمل کند، دارایی‌های پشتیبان را شفاف نشان دهد و اعتماد کاربران را حفظ کند؟ در یک صرافی متمرکز، کاربران معمولاً کنترل مستقیم کلیدهای خصوصی دارایی‌های سپرده‌گذاری‌شده را در اختیار ندارند و به همین دلیل، توان عملیاتی و مالی صرافی در زمان بحران اهمیت ویژه‌ای پیدا می‌کند.

ردپای کره شمالی

یکی از مهم‌ترین ابعاد این رخداد، انتساب آن به گروه‌های هکری مرتبط با کره شمالی است. شرکت اطلاعات بلاک‌چین TRM Labs اعلام کرده است با اطمینان بالا، گروه TraderTraitor مسئول این حمله است. این ارزیابی بر مجموعه‌ای از شواهد درون‌زنجیره‌ای و برون‌زنجیره‌ای، از جمله شیوه آماده‌سازی عملیات، الگوهای تأمین مالی کیف‌پول‌ها و شباهت‌هایی با سرقت‌های پیشین استوار است. نام گروه TraderTraitor پیش‌تر نیز در پرونده سرقت از صرافی بای‌بیت مطرح شده بود. در فوریه ۲۰۲۵، حدود ۱.۵ میلیارد دلار دارایی رمزارزی از بای‌بیت خارج شد؛ حمله‌ای که اداره تحقیقات فدرال آمریکا (FBI) آن را به بازیگران سایبری مرتبط با کره شمالی نسبت داد. آن سرقت در زمان وقوع، بزرگ‌ترین سرقت ثبت‌شده از یک پلتفرم رمزارزی بود. در پرونده بایننس نیز TRM Labs به شباهت‌هایی با حملات قبلی اشاره کرده است؛ از جمله آماده‌سازی عملیات پیش از اجرای سرقت، استفاده از برداشت‌های کوچک از سرویس مخلوط‌کننده تراکنش Tornado Cash برای تأمین مالی یک کیف‌پول عملیاتی و آماده‌کردن امضاها پیش از انتقال گسترده دارایی‌ها. بااین‌حال، شباهت فنی یا رفتاری به‌تنهایی برای اثبات هویت یک مهاجم کافی نیست و انتساب نهایی باید بر مجموعه شواهد و بررسی‌های نهادهای مسئول استوار باشد.

گزارش کامل را در سایت شرق بخوانید

بزرگ‌ترین سرقت‌های تاریخ صنعت رمزارز

سرقت‌های بزرگ رمزارزی در یک دهه گذشته، از نفوذ به صرافی‌ها تا سوءاستفاده از پل‌های میان‌زنجیره‌ای و قراردادهای هوشمند، شکل‌های متفاوتی داشته‌اند. در جدول مقابل مهم‌ترین نمونه‌ها را بر اساس ارزش تقریبی دارایی‌های سرقت‌شده یا خارج‌شده در زمان حادثه و اطلاعات موجود درباره انتساب حمله را مرور می‌کنید.

پلتفرم و زمان حادثه	میزان دارایی سرقت‌شده	دلیل سرقت
بایننس، اکتبر ۲۰۲۶	حدود ۶.۳ تا ۶.۳۶ میلیارد دلار	دو سناریو وجود دارد:نفوذ به لپ‌تاپ یکی از مهندسان شرکت و دوم دست داشتن هکرهای کره‌شمالی
بای‌بیت، فوریه ۲۰۲۵	حدود ۱.۵ میلیارد دلار	FBI حمله را به بازیگران سایبری مرتبط با کره شمالی نسبت داد.
Ronin Network، مارس ۲۰۲۲	حدود ۵۴۰ تا ۶۲۵ میلیون دلار	FBI آن را به گروه هکری لازاروس مرتبط با کره شمالی نسبت داد؛ رقم گزارش‌شده بسته به مبنای قیمت‌گذاری متفاوت است.
Poly Network، اوت ۲۰۲۱	حدود ۶۱۰ میلیون دلار	هویت مهاجم به‌طور قطعی مشخص نشد؛ تقریباً تمام دارایی‌های سرقت‌شده بعداً بازگردانده شدند.
BNB Chain Bridge، اکتبر ۲۰۲۲	حدود ۵۷۰ میلیون دلار توکن ایجادشده یا خارج‌شده در مرحله اولیه	نقص در پل میان‌زنجیره‌ای؛ انتساب قطعی به گروه مشخصی اعلام نشد.
Coincheck، ژانویه ۲۰۱۸	حدود ۵۳۰ میلیون دلار	مقام‌های اطلاعاتی کره جنوبی در آن زمان احتمال نقش هکرهای کره شمالی را مطرح کردند؛ انتساب قطعی قضائی اعلام نشد.
Mt. Gox، ۲۰۱۱ تا ۲۰۱۴	نزدیک به ۵۰۰ میلیون دلار بر مبنای ارزش تاریخی	پرونده‌ای طولانی که به ورشکستگی صرافی انجامید؛ هکر یا هکرهای قطعی معرفی نشد
Wormhole، فوریه ۲۰۲۲	حدود ۳۲۰ میلیون دلار	سوءاستفاده از پل میان‌زنجیره‌ای؛ شرکت Jump Crypto بعداً دارایی‌های ازدست‌رفته را جایگزین کرد.
DMM Bitcoin، مه ۲۰۲۴	حدود ۳۰۵ میلیون دلار	مقام‌های آمریکا و ژاپن سرقت را به بازیگران سایبری مرتبط با کره شمالی نسبت دادند.
بایننس، مه ۲۰۱۹	حدود ۴۰ میلیون دلار	سرقت هفت‌هزار بیت‌کوین از کیف‌پول گرم؛ بایننس اعلام کرد خسارت را از محل SAFU پوشش می‌دهد.

توضیح: ارقام تقریبی‌اند و با توجه به قیمت رمزارزها در زمان حادثه، تفاوت روش محاسبه و میزان بازیابی وجوه ممکن است تغییر کنند. رقم ۶.۳ میلیارد دلار بایننس برآورد اولیه تأثیر حادثه است و نباید بدون توضیح، آن را معادل زیان نهایی حسابرسی‌شده دانست.

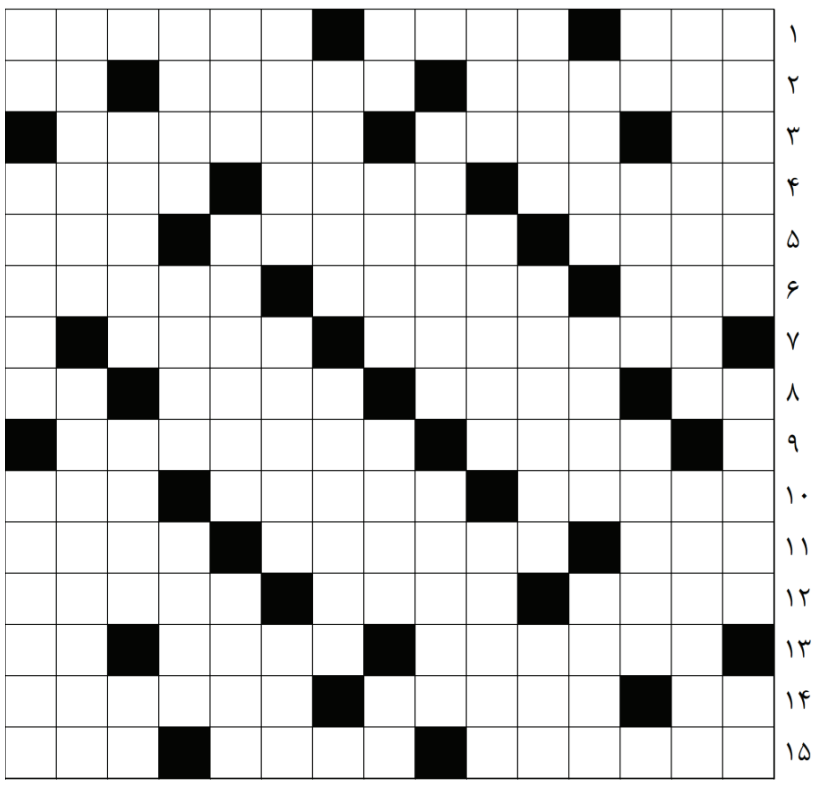
جدول ۵۴۴۶ طراح: بیژن گورانی

افقی:

۱- هریک از مواد قانون اساسی- نماد- به مناسبت رویداد مسرت‌بخش می‌خورند ۲- اشتباهات نمازگزار هنگام خواندن نماز- اتفاق نظر فقها درباره مسائل شرعی- اشاره به دور ۳- جانشین او- پنهان‌شدن برای حمله ناگهانی- شخصیتی در مدرسه موش‌ها ۴- ابزار رایج تبلیغات تجاری- سقف فروریخته- خوراکی با تخم‌مرغ و گوجه‌فرنگی ۵- ایشان- جاده تاریخی که از چین تا دریای مدیترانه بود- درخت انجیر معابد ۶- گرسنه نیست- تندی و درشتی- آهن‌ربا ۷- شیخ اشراق- دومین شیوه معماری ایران پس از اسلام ۸- جام جهان‌نما- رمانی از ساموئل بکت، نویسنده ایرلندی- همبازی هاردی- خاندان ۹- دارای فرهنگ خرافی- از ورزش‌های نوین ۱۰- سراینده مجموعه شعر دشنه در دیس- شادابی- همگانی ۱۱- دستور- حشره‌ای شبیه ملخ- بها ۱۲- پنبه‌زن- روادید- از رایج‌ترین ابزار طراحی ۱۳- جابه‌جا کردن- علم نحو می‌داند- رمق آخر ۱۴- از مباحث مهم ریاضی- زن زیبا- از ماهیان خاویاری دریای خزر ۱۵- مرض- فراموشکار- تخصصی

عمودی:

۱- بی‌چیز و فقیر- در حال جوشیدن- دوستی ۲- نهضت طرفداری از ایجاد میهن یهودی در سرزمین فلسطین- ماده‌ای در ورزش دوومیدانی ۳- نوعی حلوا- پرنده‌ای خوش‌آواز- نام پدر حضرت مریم(س) ۴- بی‌نظیر- فال می‌گیرد- نظر مجتهد در احکام شرعی فرعی ۵- افسانه‌گو- مرکز شهرستان دشتی در استان بوشهر- گوشه‌ای در دستگاه شور ۶- از انجیل‌های معتبر- سکه طلای عهد قاجاری- دارای جنبه داستانی ۷- نیستی و فنا- اصطبل ۸- وسط- جلادهنده کفش- رودی جاری در مازندران- نفس خسته ۹- بدترین نوع جرم- دره‌ای ییلاقی در شمال شرق تهران ۱۰- عمل شمردن- وسیله کمک‌حرکتی کودکان نوپا- گمانه ۱۱- هر که شد محرم دل در حرم ... بماند- تمرین- ظرف طبخ چای ۱۲- زیبا و دلفریب- بی‌آغاز- باز شیمیایی ۱۳- همه- از نام‌های بهشت- محصول آب و صابون ۱۴- پلیمر مصنوعی سبک برای بسته‌بندی- فرمانده یونانیان در جنگ تروا ۱۵- پول ژاپن- خواندن قرآن با قرائت درست و آهنگ خوب- پشت سرهم



حل سودوکو ۴۴۴۱

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

حل سودوکو ۴۴۴۱

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

حل جدول ۵۴۴۵

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

سودوکو سخت ۴۴۴۲

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.

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

سودوکو ساده ۴۴۴۲

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.

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