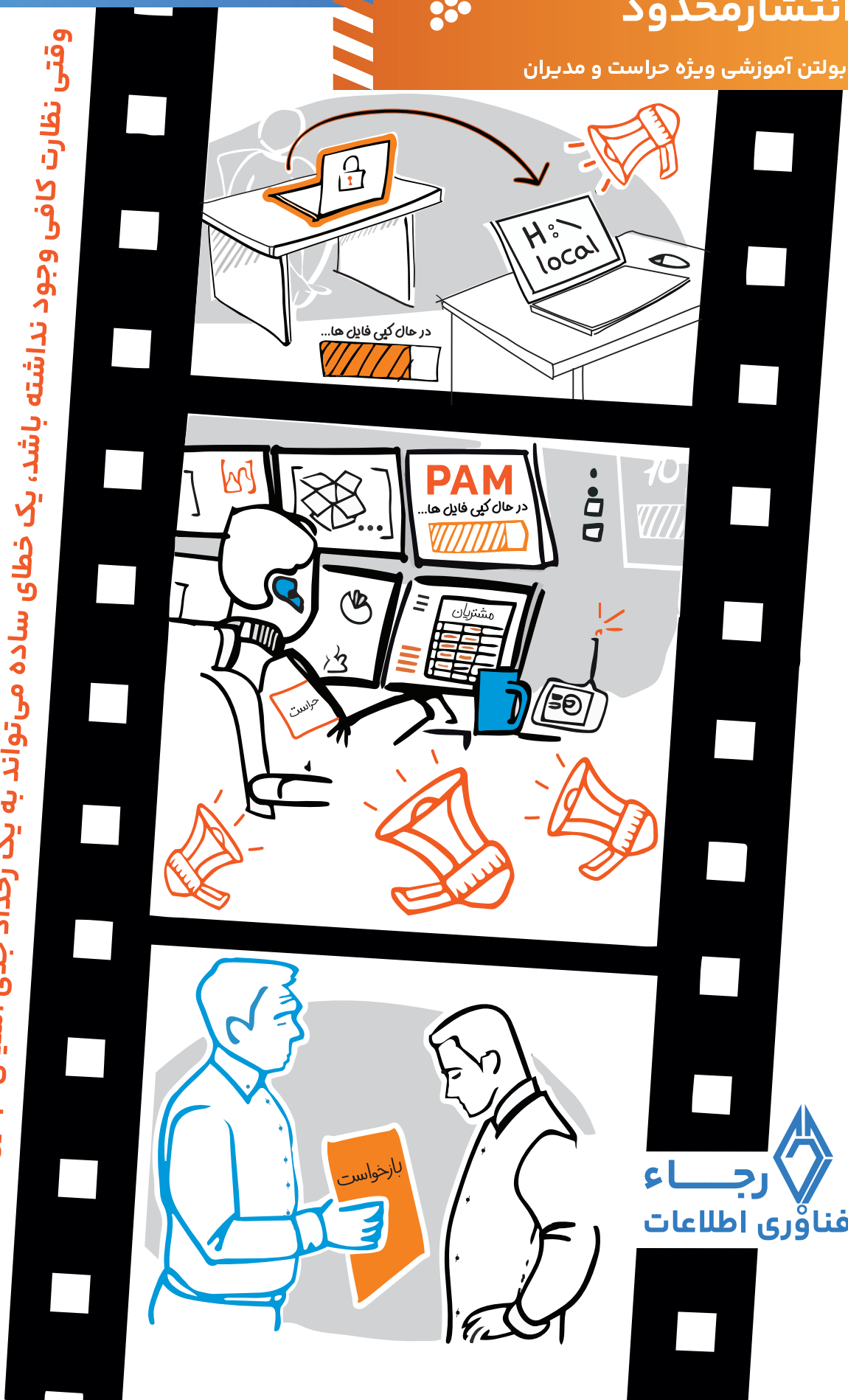
موضوع، فراتر از شماست!

انتشارمحدود

بولتن آموزشی ویژه حراست و مدیران

وقتی نظارت کافی وجود نداشته باشد، یک خطای ساده می‌تواند به یک رخداد جدی امنیتی تبدیل شود.



رجاء
فناوری اطلاعات

RAJA CyberSecurity Operator

پلتفرم مقابله با تهدیدات داخلی

در دنیای امروز، تهدیدات امنیت اطلاعات تنها از بیرون سازمان شکل نمی‌گیرند. بخش قابل توجهی از ریسک‌های امنیتی در داخل سازمان و از سوی کارکنان، پیمانکاران، کاربران دارای دسترسی یا حتی خطاهای انسانی ایجاد می‌شود. برای شناسایی و کنترل این تهدیدات، سازمان‌ها به مجموعه‌ای یکپارچه از ابزارهای امنیتی نیاز دارند؛ راهکاری که بتواند بر جریان اطلاعات، فعالیت کاربران، زیرساخت فناوری اطلاعات و دارایی‌های حیاتی سازمان نظارت مستمر داشته باشد. شرکت فناوری اطلاعات رجاء در قالب یک پلتفرم واحد، مجموعه‌ای از فناوری‌های تخصصی را در اختیار سازمان قرار می‌دهد تا بتواند :

- ترافیک ورودی و خروجی اطلاعات را کنترل کند؛
- از اطلاعات محرمانه و حساس در رایانه‌ها، سرورها و پایگاه‌های داده محافظت کند؛
- فعالیت کاربران را نظارت، ردیابی و تحلیل کند؛
- رویدادهای زیرساخت فناوری اطلاعات را پایش کند؛
- ریسک‌های مرتبط با منابع انسانی را ارزیابی کرده؛ و هرگونه نقض سیاست‌های امنیتی را در کوتاه‌ترین زمان ممکن شناسایی و گزارش دهد.

این پلتفرم با ترکیب قابلیت‌هایی مانند UBA، PAM، FileAuditor، DRM، DLP، Antivirus، FIM و سایر ماژول‌های امنیتی، دیدی جامع از تهدیدات داخلی در اختیار مدیران قرار می‌دهد و امکان واکنش سریع به رخدادهای پرخطر را فراهم می‌کند.

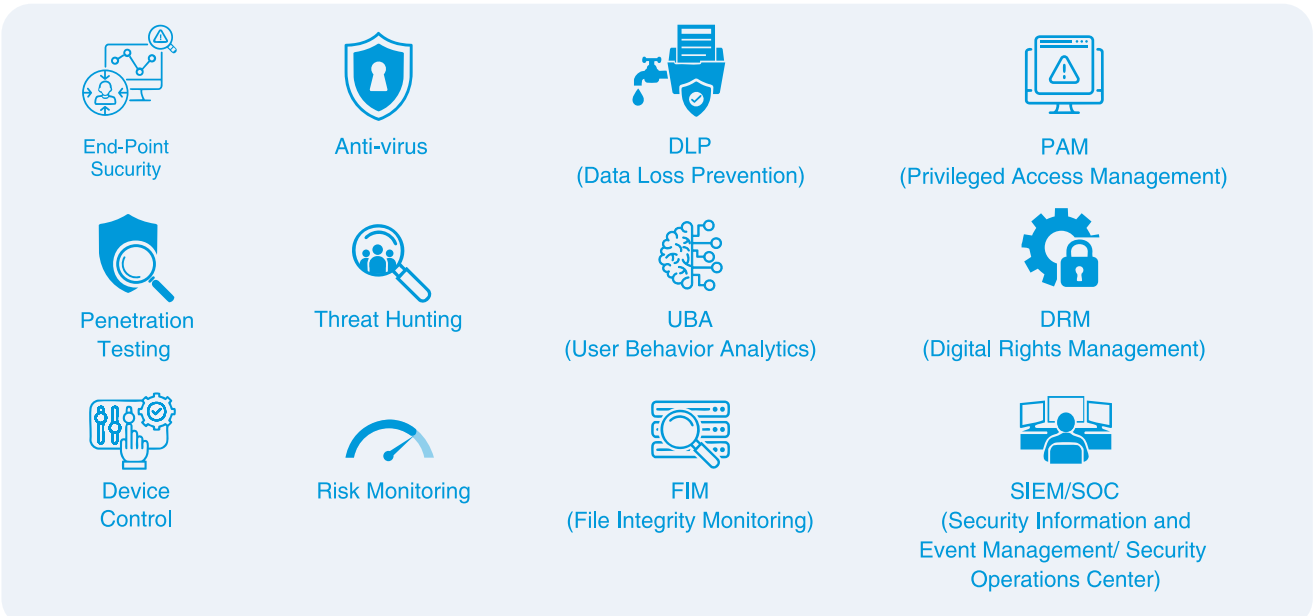
این داستان درباره یک نفر نیست

در همین لحظه که مشغول خواندن این متن هستید، در گوشه‌ای از جهان ده‌ها رکورد اطلاعاتی در حال سرقت، افشا یا نابودی است. نشت اطلاعات دیگر یک اتفاق نادر نیست؛ به بخشی از واقعیت روزمره کسب‌وکارها تبدیل شده است.

هر ثانیه ده‌ها رکورد اطلاعاتی از دست می‌رود و سازمان‌ها را با خسارت‌های مالی، حقوقی و اعتباری مواجه می‌کند. شاید تصور کنید چنین اتفاقی برای سازمان شما رخ نخواهد داد؛ بسیاری از مدیران نیز پیش از وقوع حادثه همین تصور را داشتند. اما تجربه نشان داده است که هیچ سازمانی، صرف‌نظر از اندازه، صنعت یا میزان سرمایه‌گذاری در امنیت، به‌طور کامل از خطر نشت اطلاعات، تقلب داخلی یا سوءاستفاده از دسترسی‌ها مصون نیست. طی سال‌ها فعالیت، با ده‌ها پرونده واقعی روبه‌رو شده‌ایم؛ پرونده‌هایی که نشان می‌دهند یک کارمند ناراضی، یک اشتباه ساده یا یک دسترسی کنترل‌نشده، می‌تواند به بحرانی تبدیل شود که اعتبار و سرمایه یک کسب‌وکار را تحت تأثیر قرار دهد.

داستان‌هایی که در صفحات بعدی می‌خوانید، تنها چند نمونه از رخدادهایی هستند که در سازمان‌های واقعی اتفاق افتاده‌اند؛ رخدادهایی که اگر به‌موقع شناسایی نمی‌شدند، می‌توانستند خسارت‌های جبران‌ناپذیری به همراه داشته باشند.

بر اساس گزارش‌ها و پرونده های واقعی!



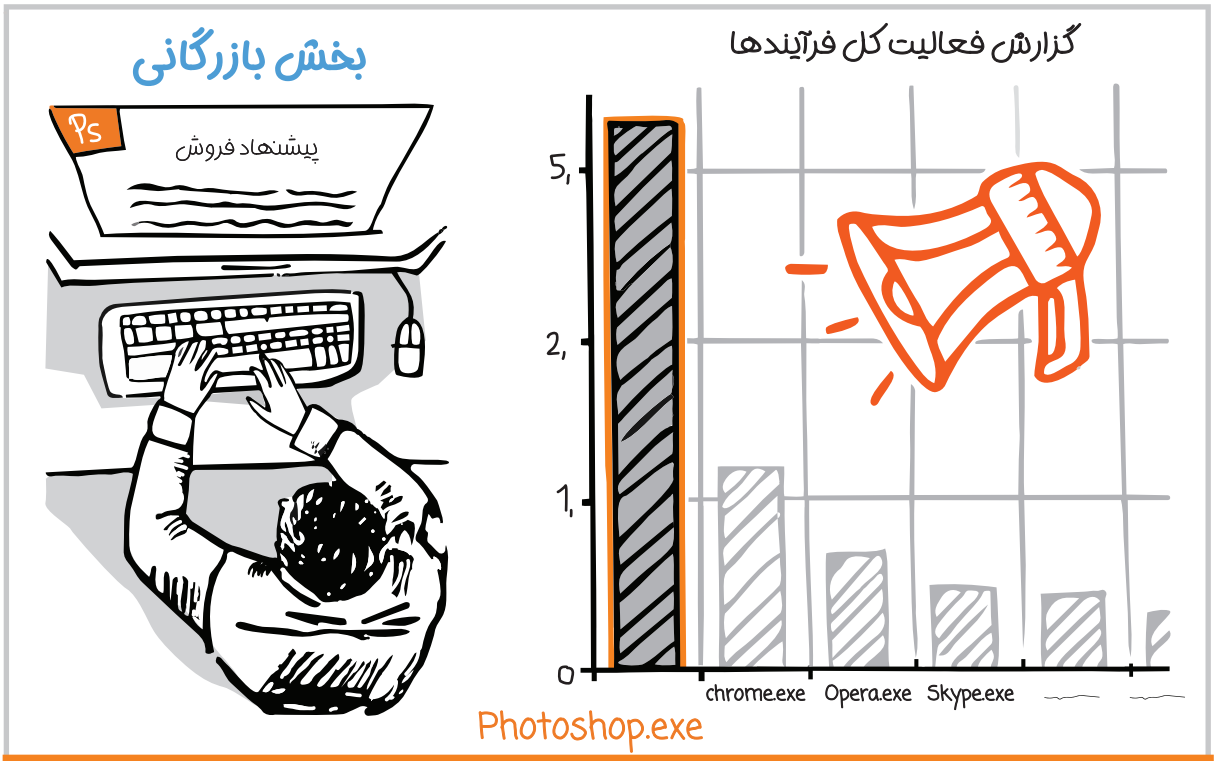
مهـر جعـلی

واحد حفاظت فناوری اطلاعات حراست در جریان تحلیل فعالیت کاربران متوجه شدند نرم‌افزار «Photoshop» روی رایانه یکی از کارشناسان واحد بازرگانی به شکل غیرمعمول و مداوم اجرا می‌شود.

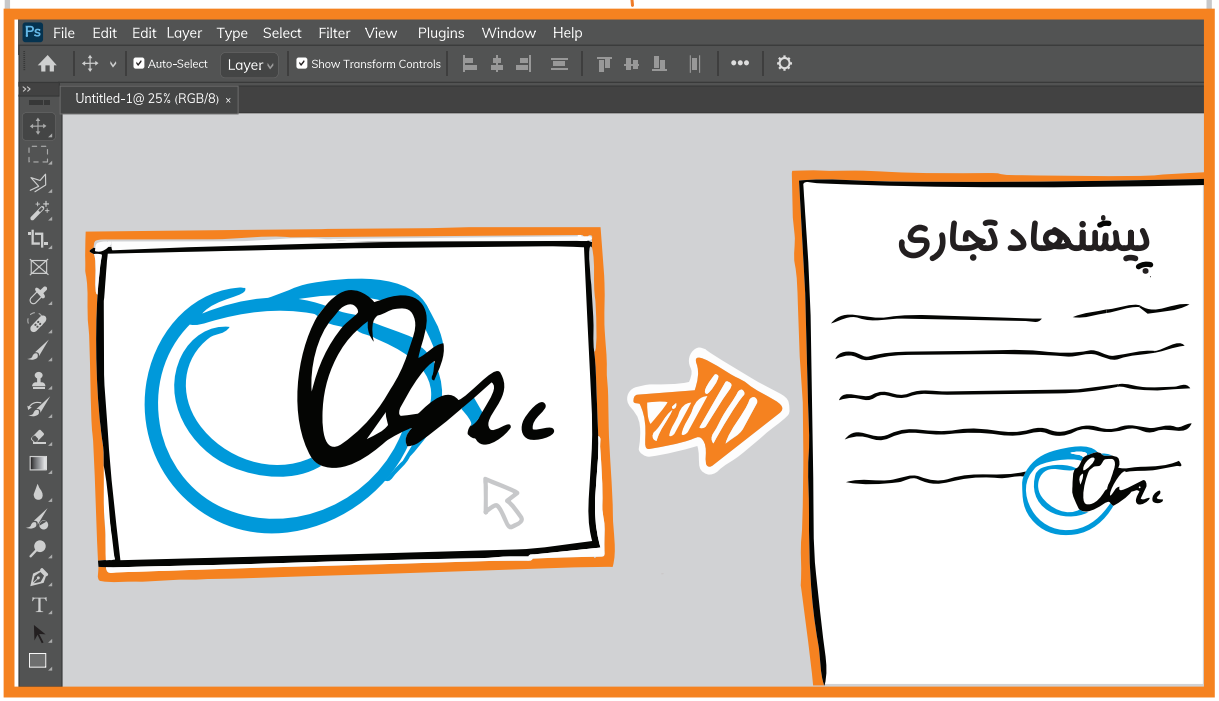
این موضوع عجیب بود؛ زیرا وظایف شغلی این کارشناس هیچ ارتباطی با طراحی گرافیک، بازاریابی یا تولید محتوای تصویری نداشت. برای روشن شدن موضوع، سوابق فعالیت سیستم و تصاویر ثبت‌شده از محیط کاری وی توسط PAM مورد بررسی قرار گرفت. نتایج نشان داد کارشناس مربوطه در حال دستکاری اسناد پیشنهاد قیمت بوده است. او جزئیات پیشنهادهای رقبا را تغییر می‌داد و با استفاده از ابزارهای گرافیکی، مهرها و امضاهای جعلی روی اسناد ایجاد می‌کرد تا برخی تأمین‌کنندگان خاص را در مناقصات و معاملات برنده کند.

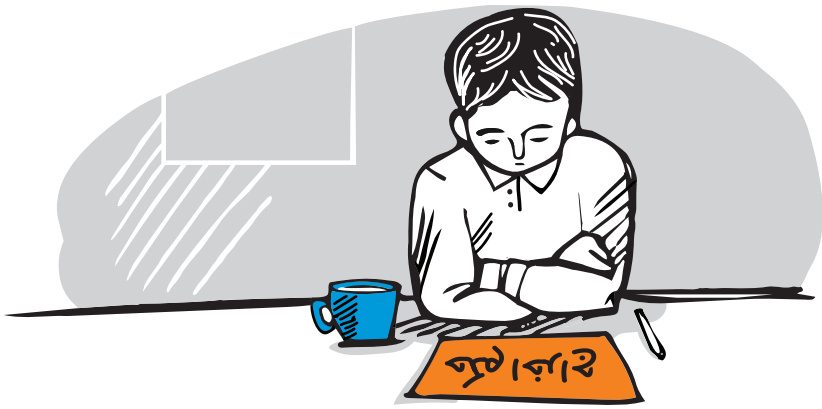
این تخلف می‌توانست خسارت مالی و اعتباری قابل‌توجهی برای شرکت به همراه داشته باشد و فرآیندهای خرید را به‌طور کامل زیر سؤال ببرد. در نهایت تخلف اثبات شد و همکاری این کارشناس با سازمان پایان یافت و روند قضایی مطابق ادله فنی جمع آوری شده، صورت پذیرفت.

راهکارهای مؤثر در کشف و رسیدگی :



PAM Monitoring





نفوذی

یک شرکت وابسته به سازمان دولتی در حال جذب مدیر شبکه فروش بود. مطابق سیاست‌های امنیتی سازمان، فعالیت کارکنان جدید در ابتدای دوره استخدام با دقت بیشتری پایش می‌شد. بررسی‌ها نشان داد فرد تازه‌استخدام‌شده هویتی حرفه‌ای اما اهدافی کاملاً متفاوت دارد. او تلاش می‌کرد به سامانه‌های مالی و حسابداری سازمان دسترسی پیدا کند و اطلاعات حساس را در اختیار رقبا قرار دهد. تحلیل رفتارهای کاربر، کنترل تجهیزات متصل‌شونده و بررسی دسترسی‌های فایل‌ها نشان داد وی در حال جمع‌آوری تدریجی داده‌های ارزشمند سازمان است.

اگر این اطلاعات به دست رقبا می‌رسید، شرکت علاوه بر از دست دادن بخشی از مشتریان خود، متحمل خسارتی بیش از ۱۷ هزار میلیارد تومان در سال می‌شد. پس از تکمیل تحقیقات، همکاری این فرد با شرکت خاتمه یافت و تهدید پیش از تبدیل شدن به یک بحران واقعی متوقف شد.

راهکارهای مؤثر در کشف و رسیدگی :


به محل کار جدیدت
خوش اومدی
در حال کپی فایل ها...

فروش غیرقانونی

یکی از تولیدکنندگان تجهیزات صنعتی هنگام اجرای پروژه شکارتهدیدات (Threat Hunting) خود با نشانه‌هایی از یک شبکه فروش پنهان مواجه شد.

سه کارمند در بخش‌های مختلف سازمان فعالیت می‌کردند و در ظاهر هیچ ارتباطی با یکدیگر نداشتند. اما تحلیل ارتباطات نشان داد هر سه از یک حساب ایمیل مشترک استفاده می‌کنند.

بررسی دقیق‌تر محتوای ذخیره‌شده در این حساب مشخص کرد کارکنان از طریق پیش‌نویس‌های ایمیل(Drafts) درباره فروش محصولات شرکت خارج از کانال‌های رسمی هماهنگی می‌کنند؛ روشی که امکان دور زدن نظارت‌های معمول را فراهم می‌کرد. این افراد در واقع محصولات تولیدکننده را بدون اطلاع شرکت و خارج از شبکه فروش رسمی عرضه می‌کردند. برآوردها نشان داد خسارت مستقیم این فعالیت غیرقانونی حدود ۳۳۸ میلیارد تومان بوده است.

پس از تکمیل تحقیقات، دو نفر اخراج شدند و برای نفر سوم اقدامات انضباطی و کنترلی در نظر گرفته شد.

راهکارهای مؤثر در کشف و رسیدگی :


اداره مالیاتی
شرکت سهامی خاص
نمایندگی فروش
پیشنهاد میکنم با شرکت سهامی خاص ما قرارداد ببندید!
AI
شرکت سهامی خاص
شرکت سهامی خاص
نمایندگی فروش
نمایندگی فروش

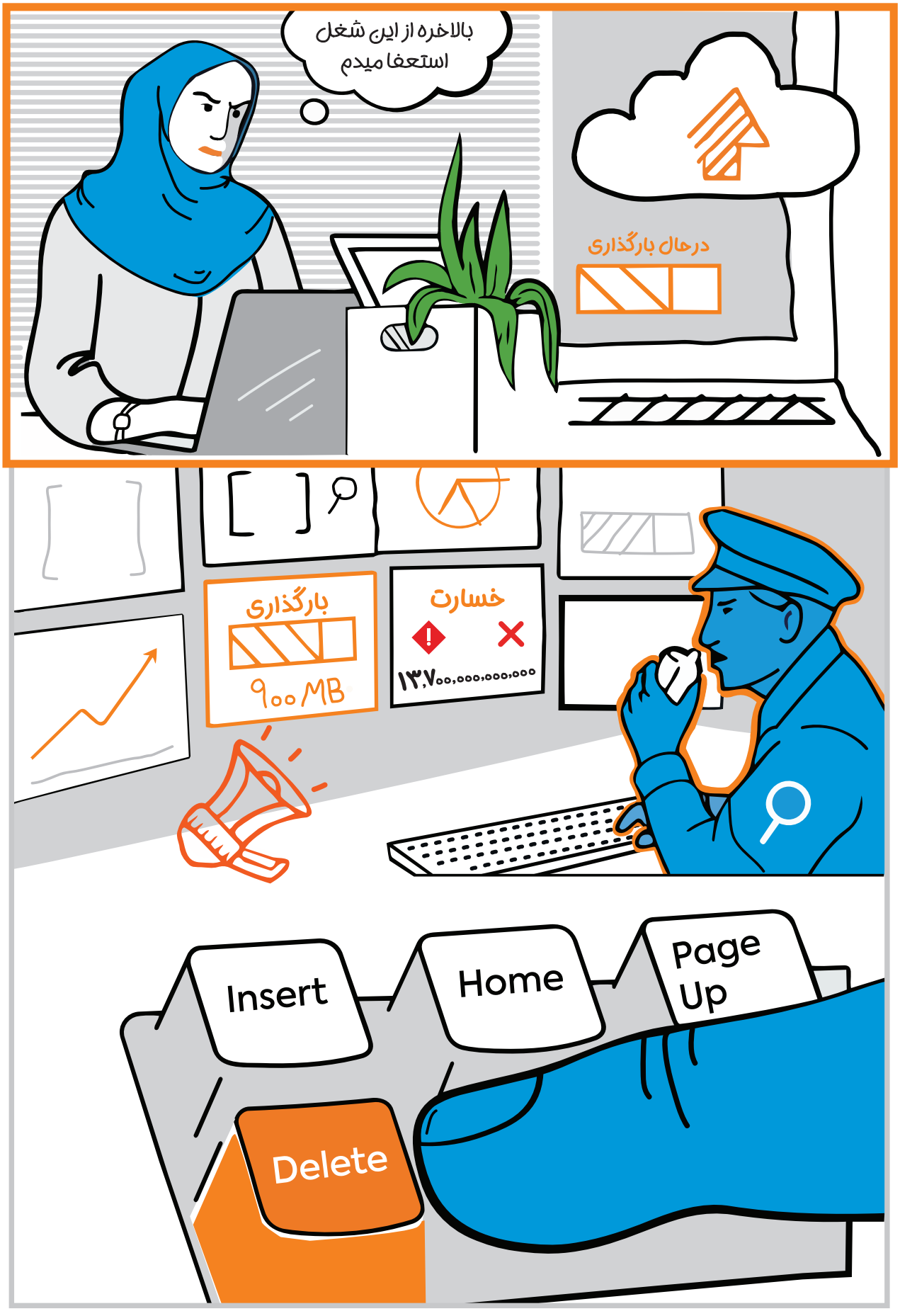
فقط یک فایل کوچک

یک شرکت بازرگانی با چالشی مواجه شد که در ظاهر از یک نارضایتی ساده کارکنان آغاز شد اما می‌توانست به بحرانی بزرگ تبدیل شود. یکی از کارکنان پس از آنکه درخواست افزایش حقوقش رد شد، تصمیم به ترک سازمان گرفت. اما پیش از خروج، آرشیوی شامل حدود ۹۰۰ مگابایت از اطلاعات محرمانه شرکت را روی یک فضای ذخیره‌سازی خارجی بارگذاری کرد. سامانه DLP به‌سرعت این انتقال غیرعادی را شناسایی و محتوای آرشیو را تحلیل کرد. نتایج نشان داد فایل‌های منتقل‌شده شامل پروژه‌های تحقیقاتی و مطالعات بازار شرکت بوده‌اند؛ اطلاعاتی که بخش قابل‌توجهی از مزیت رقابتی سازمان را تشکیل می‌دادند. برآوردها نشان می‌داد در صورت افشای این اطلاعات، هزینه‌های ناشی از توسعه مجدد اسناد، از دست رفتن فرصت‌های تجاری، افشای اطلاعات مشتریان و خسارت‌های عملیاتی می‌توانست به بیش از ۱.۳۷ هزارمیلیارد تومان برسد. خوشبختانه به دلیل شناسایی سریع حادثه، فایل‌ها پیش از انتشار از مخزن شخص ثالث حذف شدند.

در جریان بررسی‌های بعدی، موضوع مهم‌تری نیز کشف شد؛ این کارمند پیش از ترک سازمان بخشی از اسناد مالی را دستکاری کرده بود. اگر این تغییرات به موقع شناسایی نمی‌شد، شرکت با جرائم مالیاتی، مشکلات حسابرسی و حتی مسدود شدن برخی فعالیت‌های مالی مواجه می‌شد.

این پرونده نشان داد که خروج یک کارمند ناراضی، تنها به معنای از دست دادن یک نیروی انسانی نیست؛ بلکه می‌تواند به تهدیدی جدی برای دارایی‌های اطلاعاتی و اعتبار سازمان تبدیل شود.

راهکارهای مؤثر در کشف و رسیدگی :

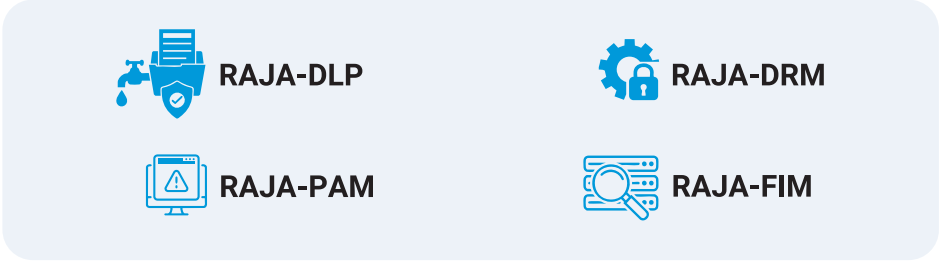

بالاخره از این شغل استعفا میدم
درحال بارگذاری
بارگذاری
۹۰۰ MB
خسارت
۱۳,۷۰۰,۰۰۰,۰۰۰,۰۰۰
Insert
Home
Page Up
Delete

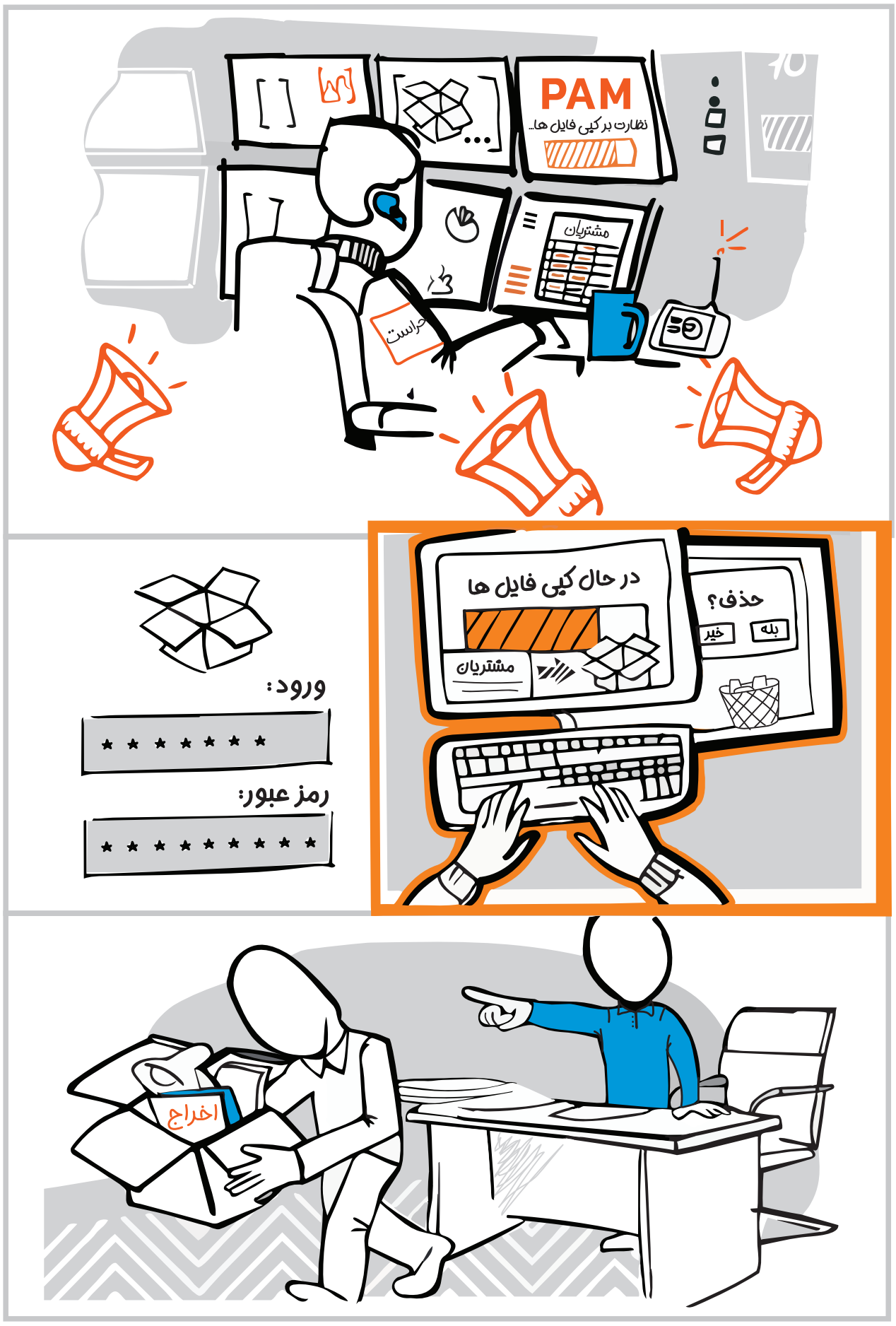
نشت اطلاعات به فضای ابری

سامانه DLP یک هشدار فوری صادر کرد: حجم بسیار بزرگی از اطلاعات در حال انتقال به حسابی در Dropbox بود. کارشناسان امنیت بلافاصله وارد عمل شدند. با استفاده از قابلیت‌های نظارتی سامانه، مشخص شد فرآیند بارگذاری همچنان در حال اجراست و اطلاعات به‌طور مستقیم از رایانه یکی از کارکنان در حال انتقال است. بررسی زنده سیستم کاربر نشان داد وی در حال کپی کردن پایگاه داده مشتریان بوده و هم‌زمان تلاش می‌کند نسخه‌های موجود روی رایانه سازمان را حذف کند تا آثار فعالیت خود را از بین ببرد.

واکنش سریع تیم امنیت اطلاعات باعث شد پیش از تکمیل فرآیند انتقال، دسترسی به سیستم کاربر برقرار شود و عملیات متوقف گردد. سپس از کارمند خواسته شد تمامی اطلاعات بارگذاری‌شده را از فضای ابری حذف کند. این اقدام از وقوع یک نشت گسترده اطلاعات جلوگیری کرد؛ رخدادی که می‌توانست مشتریان، قراردادها و سرمایه اطلاعاتی شرکت را در معرض خطر قرار دهد.

راهکارهای مؤثر در کشف و رسیدگی :




PAM
نظارت بر کپی فایل ها...
مشتریان
حراست
در حال کپی فایل ها
مشتریان
حذف؟
بله
خیر
ورود:
رمز عبور:
اخراج

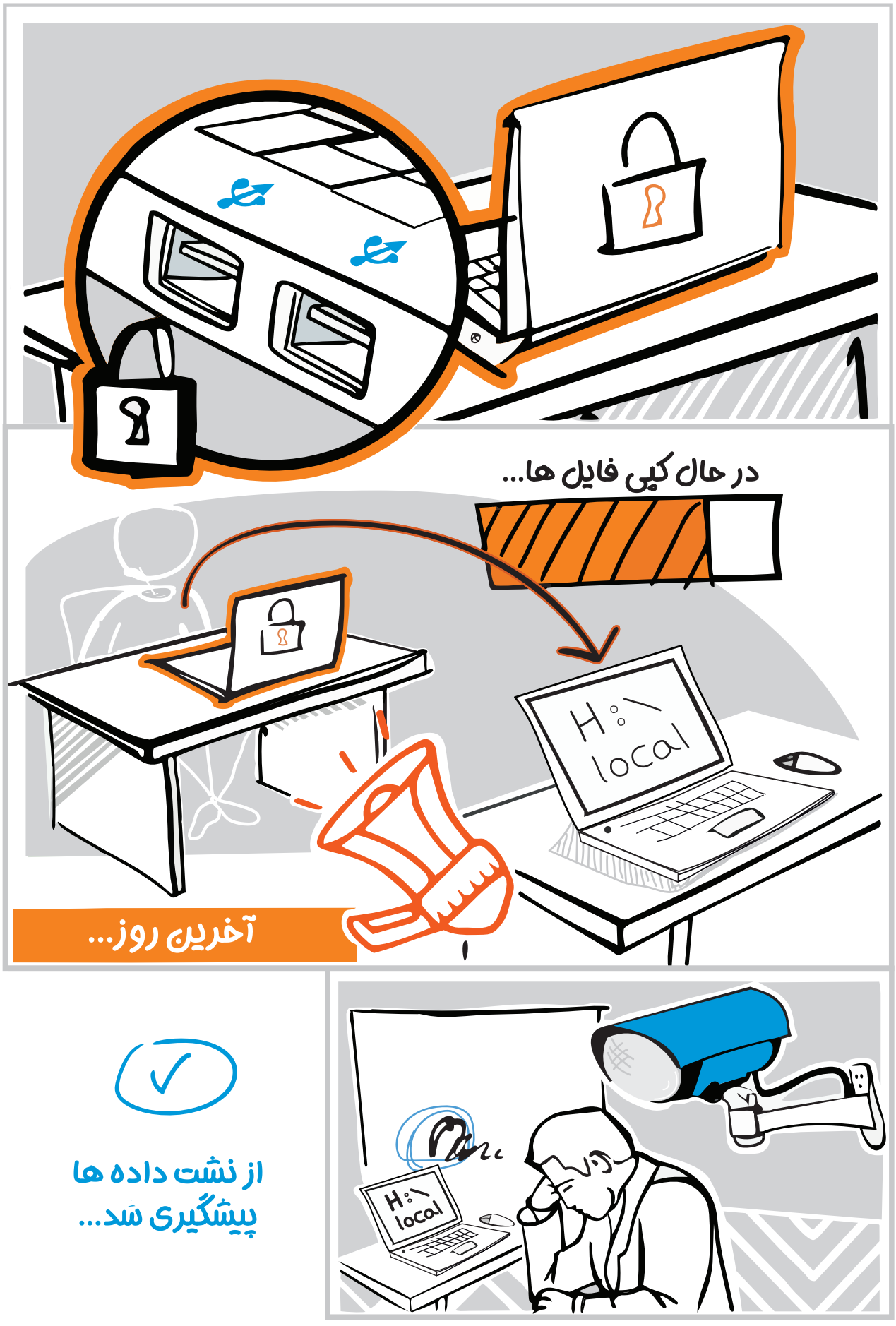
نشت اطلاعات به خاطر یک دوستی

در آخرین روزهای همکاری یکی از کارکنان، محدودیت‌های امنیتی ویژه‌ای روی حساب کاربری او اعمال شده بود. دسترسی به درگاه‌های USB مسدود شده و فعالیت‌هایش با دقت بیشتری تحت نظر قرار داشت.

با این حال، تصاویر ثبت‌شده توسط سیستم مانیتورینگ نشان دادند که کارمند مذکور حجم قابل‌توجهی از اطلاعات را روی درایو محلی یکی از همکاران خود ذخیره می‌کند؛ فردی که همچنان در شرکت مشغول به کار بود. تحقیقات بیشتر مشخص کرد همکار وی از قبل فضای ذخیره‌سازی مورد نیاز را آماده کرده و بلافاصله پس از انتقال داده‌ها، دسترسی لازم را در اختیار او قرار داده است. برنامه این بود که اطلاعات بعداً روی یک حافظه شخصی منتقل و از شرکت خارج شوند.

سامانه‌های امنیتی قبل از خروج اطلاعات از محدوده سازمان این فعالیت را شناسایی کردند و مسیر انتقال متوقف شد. در پایان، نشت اطلاعات خنثی شد، کارمند متخلف با کمک واحد حراست شناسایی و برخورد لازم با وی انجام شد. این سناریو نشان داد حتی زمانی که ابزارهای فیزیکی انتقال داده مسدود می‌شوند، همکاری داخلی میان کارکنان می‌تواند به یک مسیر جایگزین برای خروج اطلاعات تبدیل شود.

راهکارهای مؤثر در کشف و رسیدگی :



از نشت داده ها
پیشگیری شد...

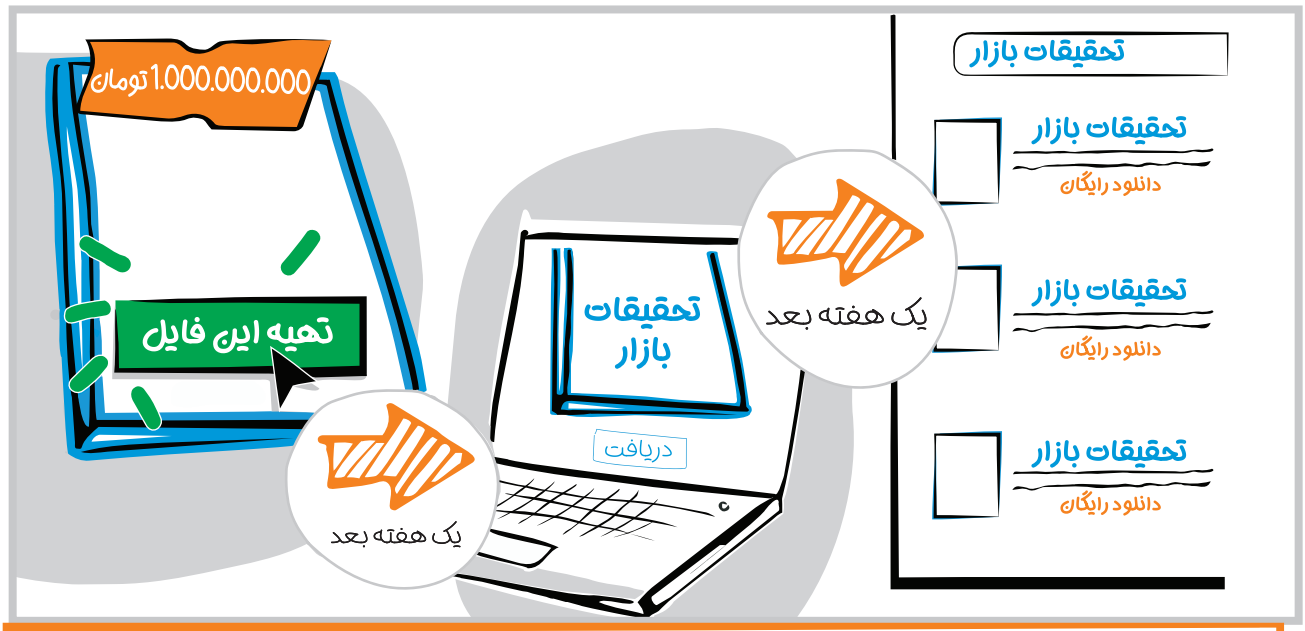
دسترسی بیش از حد؛ دروازه‌ای برای نشت اطلاعات

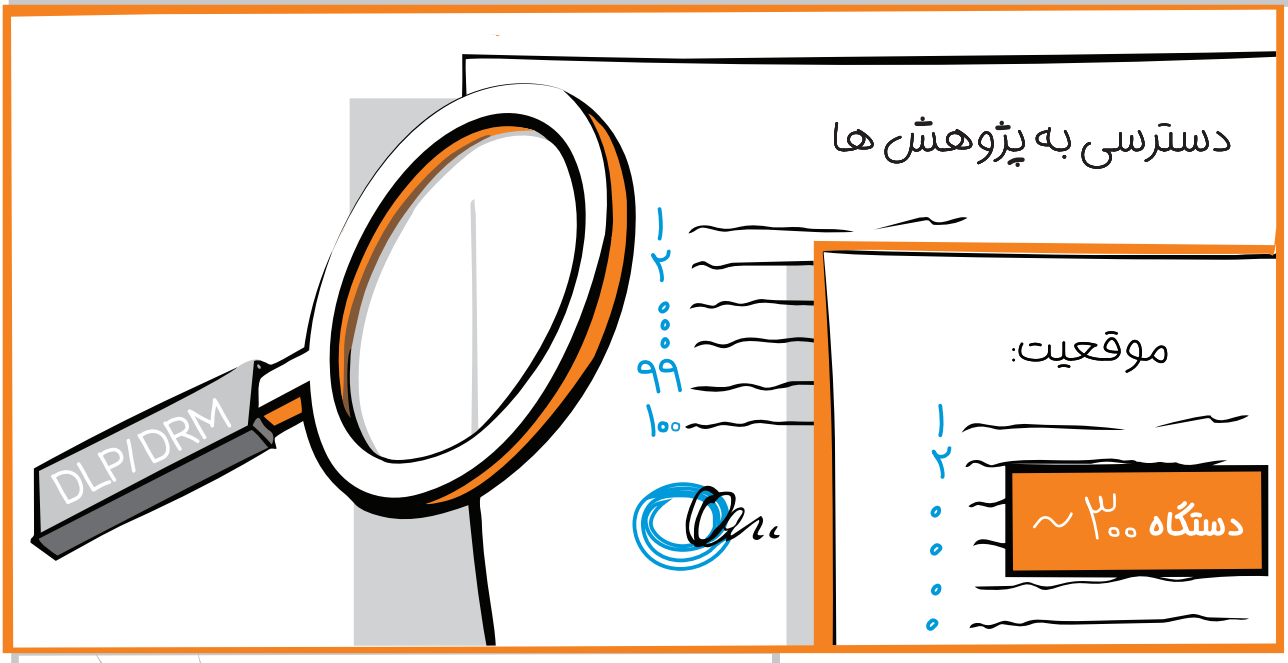
یک شرکت خرده‌فروشی به‌طور مستمر گزارش‌های ارزشمند تحقیقات بازار را خریداری می‌کرد؛ گزارش‌هایی که قیمت هر نسخه از آن‌ها به حدود ۱۰ میلیارد تومان می‌رسید.مدتی بعد واحد امنیت اطلاعات متوجه الگویی مشکوک شد. تنها یک هفته پس از خرید این گزارش‌ها، نسخه‌ای از آن‌ها در دارک‌وب منتشر می‌شد و کمی بعد نیز در دسترس عموم اینترنت قرار می‌گرفت.

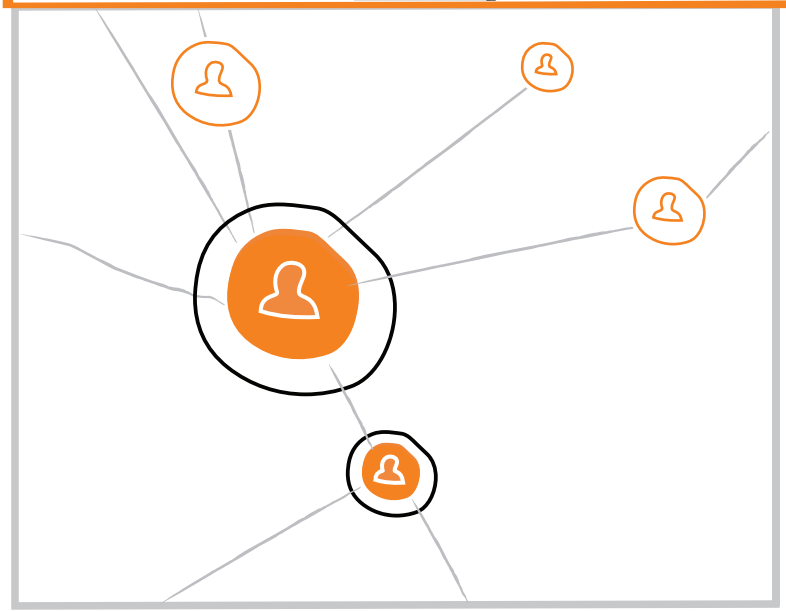
برای شناسایی منبع نشت اطلاعات، با کمک حراست بررسی جامعی روی سطح دسترسی کارکنان انجام شد. انتظار می‌رفت حداکثر ۱۰۰ نفر به این اسناد دسترسی داشته باشند، اما نتایج ابزارهای نظارتی مانند DLP/DRM، واقعیت دیگری را نشان داد. بیش از ۳۰۰ کارمند امکان مشاهده یا دسترسی به این اطلاعات را از طریق رایانه‌های خود داشتند. پس از شناسایی این دسترسی‌های غیرضروری، مجوزها اصلاح و محدود شدند. سپس با استفاده از ابزارهای DLP و PAM بررسی سوابق گذشته، تحقیقات برای یافتن عامل اصلی افشای اطلاعات آغاز شد.

این پرونده نشان داد که گاهی بزرگ‌ترین تهدید امنیتی، نه حمله خارجی، بلکه دسترسی‌های بیش از حدی است که در طول زمان بدون کنترل باقی مانده‌اند.

راهکارهای مؤثر در کشف و رسیدگی :


تحقیقات بازار
تحقیقات بازار
دانلود رایگان
تحقیقات بازار
دانلود رایگان
تحقیقات بازار
دانلود رایگان
یک هفته بعد
تحقیقات بازار
دریافت
1.000.000.000 تومان
تهیه این فایل
یک هفته بعد


دسترسی به پژوهش ها
۱
۲
۹۹
۱۰۰
موقعیت:
۱
۲
دستگاه ۳۰۰ ~
DLP/DRM



دسترسی
رد شد

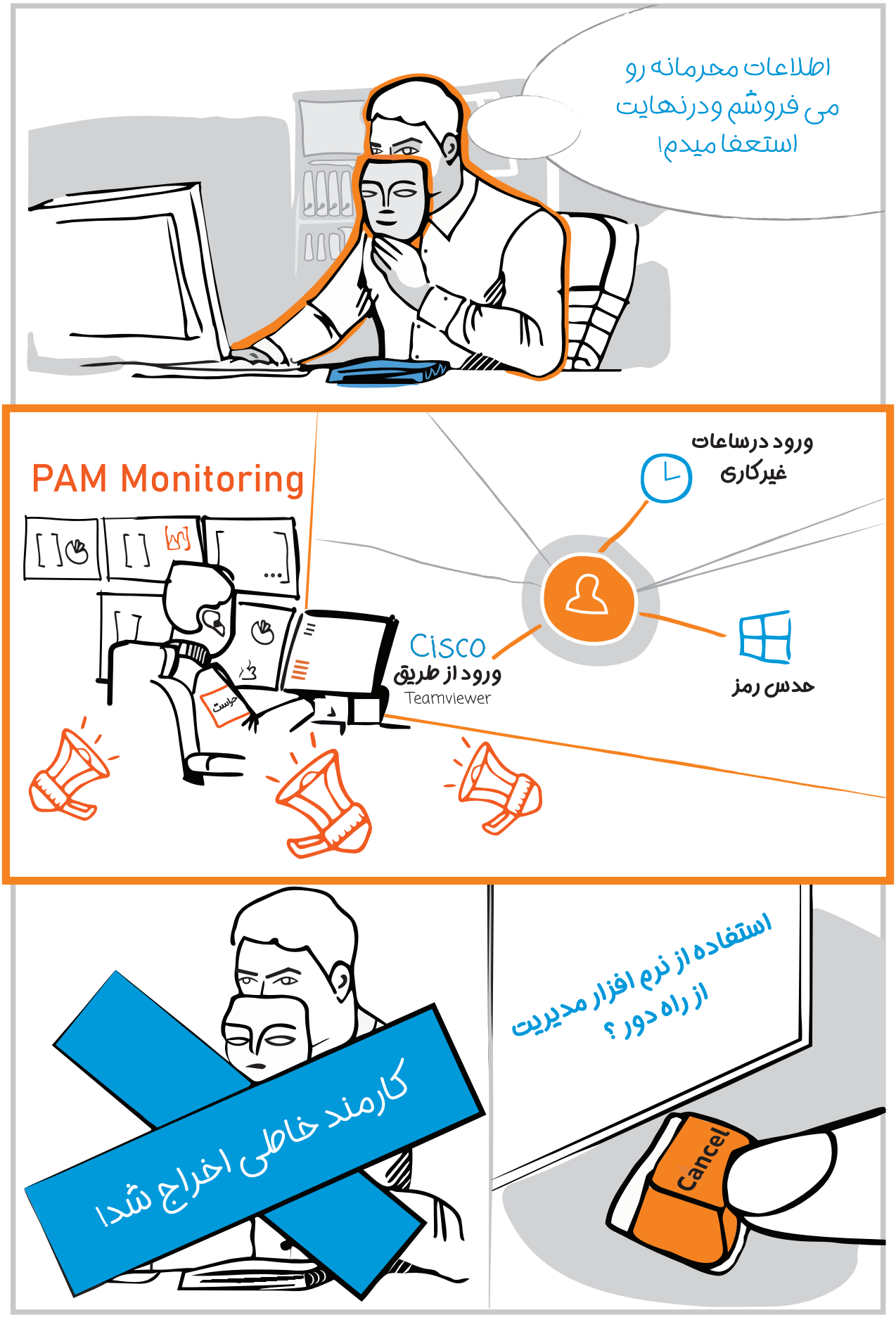
سوءاستفاده از حساب های کاربری

واحد امنیت اطلاعات یک سازمان در جریان پایش مستمر زیرساخت فناوری اطلاعات، به مجموعه‌ای از رویدادهای غیرعادی برخورد کرد. بررسی لاگ‌های امنیتی نشان می‌داد تلاش‌های متعددی برای حدس زدن رمز عبور کاربران انجام شده و در ادامه، ورود موفقی به شبکه از طریق نرم‌افزار TeamViewer خارج از ساعات اداری ثبت شده است. در نگاه اول این رویداد می‌توانست صرفاً یک دسترسی غیرمجاز معمولی باشد، اما هم‌زمان سامانه DLP نیز انتقال اطلاعات محرمانه از طریق همان کانال ارتباطی را شناسایی کرد. همین موضوع باعث شد تیم امنیت با کمک حراست، تحقیقات گسترده‌تری را آغاز کند.

با تحلیل رویدادها، مسیر دسترسی و فعالیت‌های انجام‌شده بازسازی شد. نتایج نشان داد فردی که از این حساب کاربری استفاده کرده، در حال جمع‌آوری و انتقال اطلاعات حساس سازمان بوده است. در نهایت مشخص شد عامل این تخلف یکی از مدیران میانی سازمان است؛ مدیری که مدتی بود از شرایط کاری خود رضایت نداشت و تصمیم گرفته بود سازمان را ترک کند. او پیش از خروج تلاش می‌کرد بخشی از دارایی‌های اطلاعاتی سازمان را در اختیار خود قرار دهد. واکنش سریع و هماهنگ تیم امنیت اطلاعات و حراست باعث شد این فعالیت پیش از ایجاد خسارت جدی متوقف شود.

دسترسی‌های فرد متخلف لغو و همکاری او با سازمان خاتمه یافت. همچنین برای کاهش ریسک‌های مشابه در آینده، استفاده از نرم‌افزارهای کنترل از راه دور غیرمجاز در کل مجموعه ممنوع شد و سیاست‌های دسترسی از راه دور بازنگری گردید. این پرونده نشان داد که تهدیدات داخلی همیشه از بیرون سازمان آغاز نمی‌شوند؛ گاهی یک فرد ناراضی همراه با یک حساب کاربری معتبر می‌تواند به اندازه یک حمله سایبری خارجی خطرناک باشد.

راهکارهای مؤثر در کشف و رسیدگی :


اطلاعات محرمانه رو
می فروشم ودرنهایت
استعفا میدم!
PAM Monitoring
ورود درساعات
غیرکاری
Cisco
ورود از طریق
Teamviewer
حدس رمز
کارمند خاطی اخراج شد!
استفاده از نرم افزار مدیریت
از راه دور ؟
Cancel

انتقام یک کارمند ناراضی

در جریان پایش مستمر رفتار کاربران، کارشناسان امنیت اطلاعات متوجه تغییرات قابل‌توجهی در عملکرد یکی از کارکنان شدند. او پس از بازگشت از یک مرخصی طولانی، تمرکز و بهره‌وری سابق را نداشت؛ تأخیرهای مکرر، صرف زمان زیاد برای سرگرمی‌های آنلاین و کاهش محسوس کیفیت کار، نشانه‌هایی بود که توجه مدیران را جلب کرد. پس از چندین تذکر و در نهایت حذف بخشی از مزایای تشویقی، این کارمند تصمیم گرفت نارضایتی خود را به شکلی دیگر نشان دهد.

سامانه‌های تحلیل رفتار کاربران (UBA) و سیاست‌های هوشمند DLP، نشانه‌هایی از رفتارهای پرریسک را شناسایی کردند. بررسی‌های تکمیلی نشان داد او از تصمیمات مدیریت به‌شدت انتقاد داشته و حتی برنامه ای برای ایجاد مشکل دارد. مدت زیادی طول نکشید تا این تهدید از مرحله حرف به عمل برسد. تنها یک روز بعد، تیم امنیت اطلاعات تلاش این کارمند برای کپی حجم گسترده‌ای از اطلاعات سازمان روی یک حافظه خارجی را شناسایی کرد. داده‌هایی که او قصد خروج آن‌ها را داشت، شامل اطلاعات تأمین‌کنندگان، سوابق فروش، فهرست مشتریان و اسناد مالی حساس شرکت بود. به لطف هشدارهای به موقع و واکنش سریع تیم مدیریت ریسک، خرابکاری پیش از خروج اطلاعات از ساختمان متوقف شد و کارمند فرصت استفاده از داده‌های سرقت‌شده را پیدا نکرد. برآوردهای انجام‌شده نشان می‌داد در صورت موفقیت این اقدام، سازمان با خسارتی بالغ بر ده هزار میلیارد تومان مواجه می‌شد؛ خسارتی که علاوه بر زیان مالی، می‌توانست روابط تجاری، اعتبار سازمان و مزیت رقابتی آن را نیز به خطر بیندازد.

این تجربه نشان داد که سامانه‌های امنیتی تنها برای مقابله با تهدیدها طراحی نشده‌اند؛ بلکه می‌توانند به ابزاری ارزشمند برای تصمیم‌گیری مدیریتی، حفظ سرمایه انسانی و افزایش بهره‌وری سازمان تبدیل شوند.

راهکارهای مؤثر در کشف و رسیدگی :

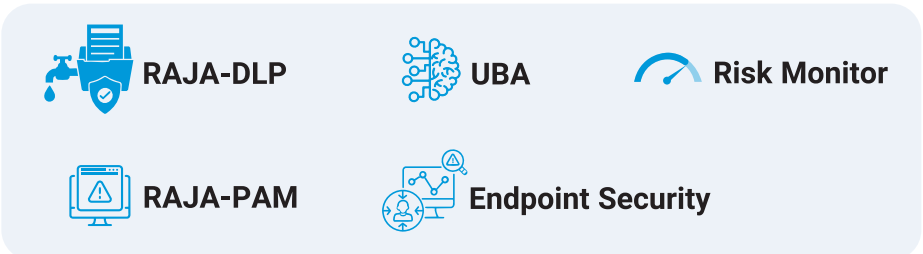

هیچ پاداشی نداری!
انتقامم رو ازشون میگیرم
مدیریت
دانلود
پایگاه داده

کارکنان پرتلاش؛ سرمایه‌های ارزشمند یا ریسکی پنهان؟

در بسیاری از سازمان‌ها، حجم کار به‌صورت متوازن میان کارکنان توزیع نمی‌شود. مدیران معمولاً مسئولیت‌های بیشتری را به افرادی واگذار می‌کنند که عملکرد بهتری دارند، سریع‌تر نتیجه می‌گیرند و قابل‌اعتمادتر هستند. در کوتاه‌مدت این رویکرد منطقی به نظر می‌رسد، اما در بلندمدت می‌تواند به یک تهدید جدی برای سازمان تبدیل شود. افزایش مداوم فشار کاری، به‌تدریج موجب خستگی، فرسودگی شغلی و کاهش تمرکز کارکنان می‌شود. در چنین شرایطی احتمال بروز خطاهای انسانی افزایش می‌یابد؛ خطاهایی که می‌توانند از یک اشتباه ساده در پردازش اطلاعات تا افشای ناخواسته داده‌های حساس یا ناتوانی در تشخیص حملات فیشینگ را شامل شوند. در یکی از بانک های کشور، تیم امنیت اطلاعات با استفاده از داده‌های جمع‌آوری‌شده توسط سامانه‌های PAM,DLP، الگوهای رفتاری غیرعادی را در میان برخی کارکنان شناسایی کرد. بررسی‌ها نشان داد تعدادی از نیروهای کلیدی شرکت به‌طور مستمر تا ساعات پایانی شب مشغول کار هستند، به‌ندرت مرخصی می‌گیرند و حجم کاری آن‌ها به‌مراتب بیشتر از سایر اعضای تیم است.

این تحلیل به مدیران کمک کرد تا تصویری دقیق از وضعیت واقعی نیروی انسانی به دست آورند. در نتیجه، بخشی از وظایف میان سایر کارکنان توزیع شد و فشار کاری از روی نیروهای کلیدی کاهش یافت. این اقدام نه‌تنها احتمال بروز خطاهای ناشی از خستگی را کاهش داد، بلکه از فرسودگی و از دست رفتن تعدادی از ارزشمندترین متخصصان بانک نیز جلوگیری کرد. علاوه بر این، داده‌های رفتاری جمع‌آوری‌شده امکان شناسایی کارکنان با عملکرد برتر را نیز فراهم کرد. مدیریت بانک از این اطلاعات برای برنامه‌ریزی نظام پاداش، توسعه مسیرهای شغلی و شناسایی استعدادهای کلیدی استفاده کرد. این تجربه نشان داد که سامانه‌های امنیتی تنها برای مقابله با تهدیدها طراحی نشده‌اند؛ بلکه می‌توانند به ابزاری ارزشمند برای تصمیم گیری مدیریتی، حفظ سرمایه انسانی و افزایش بهره‌وری سازمان تبدیل شوند.

راهکارهای مؤثر در کشف و رسیدگی :




می توانید این اسناد را
دوباره بررسی کنید لطفا؟
اینها قرار است بخشی از
گزارش مالی سالانه باشند.
بله، خودم انجامش میدم
گزارش
شنبه
ظهر ۳:۲۶

▪ امنیت، نتیجه شانس نیست؛

حاصل دیدن تهدیدها پیش از وقوع آن‌هاست. اگر می‌خواهید داستان سازمان شما متفاوت باشد، زمان اقدام همین امروز است.

فناوری اطلاعات رجاء
اپراتور امنیت سایبری

دفترمرکزی

تهران، بلوارکریمخان، آبان جنوبی، ساختمان رجاء

۰۲۱- ۵۷ ۲۶۱

دفترفنی و مرکز داده

خیابان قائم مقام، خیابان خدری، پلاک ۵۹

۰۲۱ - ۸۸۹۱ ۸۱ ۳۶

Rajaco.com