فصلنامه علمی-ترویجی پدافند غیرعامل

سال چهارم، شماره ۴، زمستان ۱۳۹۲، (پیاپی ۱۶)، صص ۱-۱۲

بررسی روش‌های نشت اطلاعات و راه‌کارهای جلوگیری از آن

محمدحسین حسن‌نیا[۱]، مهدی دهقانی[۲]

تاریخ دریافت: ۹۲/۰۷/۱۴
تاریخ پذیرش: ۹۲/۱۰/۱۶

چکیده

این روزها، دارائی‌های یک سازمان نه تنها بر حسب داشته‌های فیزیکی، بلکه براساس اطلاعاتی که دارند نیز سنجیده می‌شود. مانند هر دارایی دیگر سازمان، اطلاعات نیز در معرض تهدیدات است. این تهدیدات عبارت‌اند از حمله از جانب افرادی خارج و یا داخل سازمان که ممکن است بخواهند پدافند غیرعاملِ (امنیت، ایمنی و پایداری) دارایی‌های اطلاعاتی در دست سازمان را تحت تأثیر قرار دهند. یکی از تهدیداتی که دارایی‌های اطلاعاتی در معرض آن است نشت اطلاعات می‌باشد، تهدیدی که افشای غیرمجاز اطلاعات محرمانه را تشکیل می‌دهد.

روش‌های مختلفی برای نشت اطلاعات وجود دارد؛ بنابراین جهت کاهش خطرات ایجادشده توسط حوادث نشت اطلاعات که ممکن است تصادفی و یا با قصد خرابکاری باشد، ضروری است اطلاعات حساس شناسایی و به نحوی مناسب سازماندهی گردد و با ابزارهای امنیتی معروف به راه‌کارهای DLP که توسط تأمین کنندگان محصولات امنیتی تولید و توسعه داده شده است، محافظت گردد.

کلیدواژه‌ها: تهدید، پدافند غیرعامل، امنیت، نشت اطلاعات

۱- دانشجوی کارشناسی ارشد دانشگاه جامع امام حسین(ع) hassannia@ihu.ac.ir – نویسنده مسئول

۲- مربی و عضو هیئت علمی دانشگاه جامع امام حسین(ع) mdehghany@ihu.ac.ir

۱- مقدمه

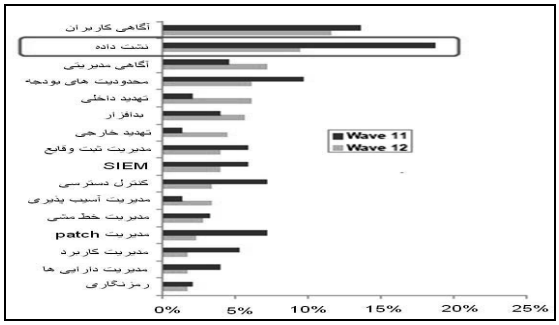
در حالی که سازمان‌ها، هزینه بالایی را برای امن نمودن سازمان خود در مقابل حمله‌کنندگان خارجی می‌پردازند و از انواع دیواره‌های آتش و نرم‌افزارهای ضدویروس استفاده می‌نمایند، می‌توانند در معرض خطر از دست دادن داده‌های حساس خود، به وسیله افراد درون سازمان باشند. اطلاعات مشتریان و محصولات، اطلاعات مالی، اداری و کارمندی هر لحظه می‌تواند بدون این که کسی با خبر باشد، از سازمان خارج شود. سارقین اطلاعات نه تنها نفوذگرها یا افراد بیگانه نبوده، بلکه کارمندان خود سازمان نیز می‌باشند. این کارمندان با ذخیره‌کردن اطلاعات حساس از رایانه شخصی خود به حافظه‌های USB، DVD، CD و انواع دیگر تجهیزات قابل حمل و یا با استفاده از رایانامه[1]، پیام‌رسان[2] یا وسایل بی‌سیمی هم‌چون Wi-Fi و بلوتوث می‌توانند عامل نشت اطلاعات شوند. به‌علاوه، کامپیوترهای شخصی کارمندان سازمان، ممکن است از طریق بدافزارهایی آلوده گردد و اطلاعات محرمانه با استفاده از کانال‌های پوششی[3] در پوشش کانال‌های مجاز و با پروتکل‌های پرکاربردی مانند HTTP و FTP به‌دست افراد متخاصم برسد [۱]. نشت اطلاعات به هر دلیلی (اتفاقی یا با اهداف سوء) می‌تواند هزینه‌های بسیاری را برای سازمان دربر داشته باشد و حتی باعث نابودی آن گردد.

در جهت ممانعت از فقدان داده‌ها[4] به‌وسیله تهدیدات داخلی[5]، سیستم‌های جلوگیری از نشت داده[6] یا جلوگیری از فقدان داده[7] طراحی شده است. با استفاده از این سیستم‌ها می‌توان برای نحوه دسترسی کاربران و انتقال اطلاعات توسط آنان، خط‌مشی‌هایی تعریف نموده و در سازمان اعمال نمود. به علاوه می‌توان گزارش‌های کاملی از فعالیت کاربران و نحوه دسترسی آنان به اطلاعات تهیه کرده و در نهایت، کنترل و نظارت کامل بر روی داده‌های سازمانی و نقل و انتقال آن‌ها داشت.

در این مقاله، ابتدا به بررسی چالش‌های امنیتی و سپس به بررسی روش‌های مربوط به نشت داده‌ها پرداخته می‌شود. در ادامه این بخش، انواع سیستم‌های DLP را معرفی کرده و امکانات و ویژگی‌های آنها را برمی‌شماریم و در نهایت، مقایسه‌ای بین سیستم‌های موجود انجام داده و جمع‌بندی می‌نماییم.

۲- نشت اطلاعات

فاش شدن اطلاعات محرمانه سازمان‌ها، به عنوان اولین تهدید امنیتی (تهدیدی بالاتر از ویروس‌ها، اسب‌های تروا و کرم‌ها) شناخته شده است. در مطالعه موردی، افراد معتبری در زمینه امنیت مورد پرسش قرار گرفته‌اند. این افراد در مورد دو حوزه از حوزه‌هایی که بیشترین توجه آن‌ها را به خود معطوف کرده بود مورد مصاحبه قرار گرفتند. نتایج بررسی‌های انجام‌شده، در شکل (۱) خلاصه گردیده است که *نشت داده* را به عنوان بزرگترین معضل امنیتی نشان می‌دهد [۲و۳].



شکل ۱- الویت حوزه‌های دردسرساز برای مدیران [۳ و ۲]

دلیل اینکه جلوگیری از نشت داده، جزء مهم‌ترین مسایل امنیتی سازمان‌ها مورد توجه قرار گرفته این است که با از دست رفتن داده‌ها، اعتبار سازمان دچار خدشه شده و مشتریان خود را از دست می‌دهد، هزینه بالایی را در جهت برطرف کردن خسارات باید بپردازد و این امر گاه منجر به نابودی سازمان خواهد گردید [۳]. در سال‌های اخیر، حوادث متعددی که منجر به از دست رفتن حجم وسیعی از داده‌های محافظت‌شده سازمان‌ها گزارش شده که هزینه‌های گزافی را برای سازمان‌ها دربر داشته است [۴]. نمونه‌هایی از این حوادث عبارت‌اند از:

- مفقود شدن اطلاعات شخصی ۱۰۰۰ مشتری بانک توسط یک کارمند بانک ایرلندی از طریق یک حافظه USB، بدون توجه به مسئله رمزنگاری اطلاعات (نوامبر ۲۰۰۸)
- سرقت بیش از ۴۰ میلیون شماره کارت اعتباری از ۹ خرده‌فروش آمریکایی با نفوذ به شبکه بی‌سیم توسط هکرها

۲-۱- اطلاعات به عنوان یک دارایی

امروزه سازمان‌ها حجم بالایی از دارایی‌ها را به اشکال و صورت‌های مختلف دارند که *اطلاعات*، به خاطر هزینه هنگفت و دشواری‌های تولید یا جایگزین کردن، یکی از ارزنده‌ترین این دارایی‌هاست. سازمان‌ها معمولاً دارای دو نوع مختلف از دارایی‌های اطلاعاتی هستند؛ دارایی‌های اطلاعات شخصی و دارایی‌های اطلاعات سازمانی. دارایی‌های اطلاعات شخصی به شکل هرگونه دارایی که شامل *اطلاعات قابل شناسایی قابل شخصی‌سازی*[8] باشد، و یا هر نوع

1- Email
2- Instant Messaging
3- Covert Channel
4- Data Loss
5- Insider Threat
6- Data Leakage Prevention
7- Data Loss Prevention

8- Personable Identifiable Information (PII)

اطلاعاتی که بتوان از آن برای شناسایی یک شخص واحد یا یافتن موقعیت او استفاده نمود، تعریف می‌شود. متأسفانه تعریف PII به قانونگذاری کشورها وابسته بوده و از کشوری به کشور دیگر متفاوت است.

دارایی‌های اطلاعاتی کسب‌وکار[1] را می‌توان به‌صورت هرگونه اطلاعاتی تعریف کرد که برای دستیابی به اهداف سازمان ضروری است. این اطلاعات شامل نقشه‌های پیش‌ساخته، کد منبع، طرح‌های مالی و سرمایه‌گذاری و غیره را دربر می‌گیرد. این نوع دارایی‌ها به‌شدت ناهمگن است، چرا که می‌توان آن‌ها را به اشکال مختلف یافت (فایل متنی، طراحی، ارائه) و قالب‌های (PDF، DOC، DOCX، PPT، OPT، CATIA و غیره) [۵].

۲-۲- شناسایی و طبقه‌بندی اطلاعات حساس

شناسایی اطلاعات حساس که در سازمان نگهداری می‌شود به عنوان گام اول برای *حفاظت از اطلاعات در برابر نشت آن* است. اگر این فعالیت به‌صورت دستی انجام شود می‌تواند به شدت کند و زمانگیر باشد. فنون شناسایی و طبقه‌بندی خودکار اطلاعات، شناسایی و طبقه‌بندی اطلاعات در زیرساخت سازمان را ممکن می‌سازد.

به‌علاوه، دارایی‌های اطلاعاتی ممکن است به خاطر فرایند کسب‌وکار و یا حمله توسط یک عامل داخلی خرابکار دچار تغییر گردد. در این صورت، فنون شناسایی باید برای شناسایی مؤثر دارایی‌های اطلاعاتی، این را نیز به حساب آورند که اطلاعات ممکن است دچار این‌گونه تغییرات شود. در بدترین شرایط، ممکن است یک دارایی اطلاعاتی با استفاده از پنهان‌نگاری در یک حامل عادی مخفی شده باشد. در این صورت، فنون شناسایی اطلاعات حساس غیرقابل استفاده خواهد بود. برای شناسایی این‌گونه فایل‌ها و اجتناب از سرقت اطلاعات، باید از فنون *تحلیل پنهان‌نگاری* استفاده کرد. استفاده از فنون زیر، با وجود اینکه به طور خاص برای شناسایی اطلاعات حساس طراحی نشده‌اند، در مقالات و محصولات تجاری مشاهده شده است [۵].

۲-۱-۱- فنون برابرسازی کلمات کلیدی و تشخیص الگو[2]

در برخی موارد، ممکن است دارایی‌های اطلاعاتی شامل کلمات یا خصوصیات ویژه‌ای باشد که بتواند شناسایی آن‌ها را به عنوان اسناد حساس از طریق برابرسازی کلمات کلیدی (نام، نام خانوادگی، کلمه محرمانه و غیره) ممکن سازد. بنابراین می‌توان از برابرسازی کلمات کلیدی برای جستجو در درون فرادادههای فایل به دنبال اطلاعات حساس نیز استفاده نمود. فنون تشخیص الگو، بخشی از نظریه اتوماتون و نظریه محاسباتی است که توسط «کلین» معرفی گردیده است. امروزه عبارات قاعده‌مند[3] برای شناسایی الگوها در درون فایل‌های متنی سازوکاری رایج است که در اکثر زبان‌های برنامه‌نویسی نیز پیاده‌سازی شده است.

در ضمن می‌توان از کلمات کلیدی و الگوها تنها زمانی استفاده کرد که دارایی‌های اطلاعاتی، حاوی اطلاعات حساس صریح باشند (نمی‌توان از آن‌ها برای دارایی‌های اطلاعاتی تغییر یافته یا مخفی استفاده نمود). با این حال، کلمات کلیدی و الگوها را باید با دقت انتخاب کرد، چرا که ممکن است اسنادی را که حساس نیستند حساس تشخیص دهد (اشتباهی مثبت[4]) [۵].

۲-۲-۲- انگشت‌نگاری سند[5]

انگشت‌نگاری، فنّی است که سعی می‌کند امضاهایی را از اسناد استخراج کند به نحوی که بعداً بتوان از این امضاها برای شناسایی نسخه و اسناد دیگر با محتوای مشابه استفاده نمود. از آنجا که هدف این نوع انگشت‌نگاری شناسایی اسناد مشابه است، معمولاً این نوع انگشت‌نگاری نیز انگشت‌نگاری تقریبی نامیده می‌شود. بنابراین از فنون انگشت‌نگاری می‌توان برای شناسایی اطلاعات حساس و همچنین تشخیص دارایی‌های اطلاعاتی واضح و دارایی‌های اطلاعاتی تغییر یافته استفاده نمود [۵].

۲-۲-۳- توابع درهم‌ریزی جرم‌شناختی[6]

توابع درهم‌ریزی جرم‌شناختی (درهم‌ریزی‌های فازی[7]) خانواده‌ای از توابع درهم‌ریزی هستند که هدف اصلی آن‌ها تعیین مشابهت یا رابطه متقابل میان قطعات اطلاعات است. با این‌که سازوکارهای شناسایی سند مشابه قبلاً توسط *"برین"* و دیگران پیشنهاد شده بود، به این سازوکارها اولین بار توسط *"کرن‌بلوم"* به عنوان یک ابزار جرم‌شناسی پرداخته شد. در رابطه با حفاظت در برابر نشت اطلاعات، این‌گونه فنون را می‌توان حتی بعد از تغییر یافتن، برای رهگیری اطلاعات حساس به‌کار برد [۵].

۳- فنون نشانه‌گذاری[8]

اگر اطلاعاتی درباره خود سند در درون آن جاسازی شود این روش را فنون نشانه‌گذاری می‌نامند. فنون نشانه‌گذاری به طور گسترده جهت حفاظت حقوق تکثیر محتوای چند رسانه‌ای، مورد کاوش قرار گرفته است. با این حال، نشانه‌گذاری در حوزه‌های دیگری نیز همچون طراحی CAD، کد اجرائی، فایل‌های XML و غیره مورد کاوش قرار گرفته است. با اینکه افزودن نشانه‌گذاری راه‌کار مناسبی برای شناسایی اسناد حساس نیست، می‌توان از آن برای نظارت بر اسناد

1- Business Information Assets
2- Keyword Matching and Pattern Recognition Techniques
3- Regular Expressions
4- False Positive
5- Document Fingerprinting
6- Forensic Hash Functions
7- Fuzzy Hashes
8- Watermarking

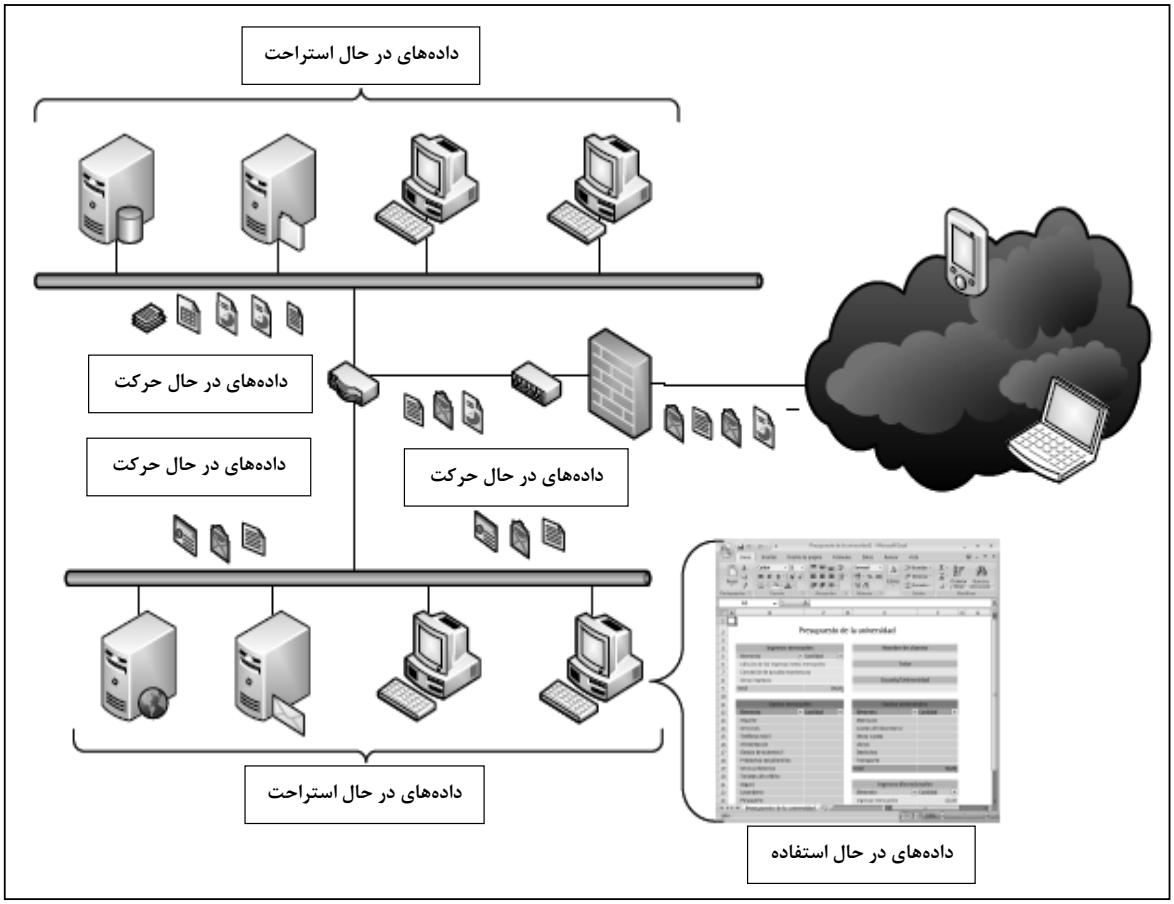
تغییریافته و تعریف خصوصیات سند همچون حساسیت، محرمانگی و غیره استفاده کرد. جدول (۱) مروری بر فنون شناسایی و طبقه‌بندی ارائه شده قبلی را نشان می‌دهد [۵].

۲-۳- حالت و سازماندهی اطلاعات

زیرساخت فناوری اطلاعات یک سازمان معمولاً از سرورها، کامپیوترهای رومیزی و دستگاه‌های همراه (لپ‌تاپ‌ها و گوشی‌های هوشمند) تشکیل می‌یابد که توسط شبکه سازمان به یکدیگر متصل می‌شوند. همان طور که در شکل (۲) نشان داده شده است، همه‌روزه دارایی‌های اطلاعات از درون شبکه سازمان جریان می‌یابد (اطلاعات در حال حرکت) و در هر یک از سیستم‌های سازمان ذخیره می‌گردد (اطلاعات در حال استراحت). از آنجا که می‌توان اطلاعات را در هر یک از این حالات یافت و سیستم‌های اطلاعاتی با هر یک از این حالات به گونه‌ای متفاوت رفتار می‌کنند، کنترل‌ها و اقدامات متقابل متفاوتی باید پیاده‌سازی شود تا از نشت اطلاعات جلوگیری به عمل آید [۵].

جدول ۱- مروری بر فنون شناسایی و طبقه‌بندی اطلاعات [۵]

فن	کشف محتوای متغیر	ردگیری تغییرات	تغییر محتوا
برابرسازی کلمات کلیدی	خیر	خیر	خیر
تشخیص الگو	بله	خیر	خیر
انگشت‌نگاری سند	بله	بله	خیر
توابع درهم‌ریزی جرم‌شناختی	بله	بله	خیر
نشانه‌گذاری	بله	بله	بله



شکل ۲- انواع اطلاعات درون یک سازمان [۵]

۲-۳-۱- اطلاعات در حال استراحت

دارایی‌های اطلاعاتی که در زیرساخت سازمان ذخیره‌سازی شده ولی مورد استفاده نیستند، *اطلاعات در حال استراحت* تلقی می‌شوند. دارایی‌های اطلاعاتی در این حالت معمولاً در دیسک‌های سخت[1]، کارت‌های حافظه[2]، دیسک‌های حالت جامد[3] و وسایل دیگر پشتیبانی فیزیکی داده‌های دیجیتال ذخیره می‌گردند. به لحاظ منطقی، این اطلاعات در سرورها در پایگاه‌های داده[4]، مخازن فایل[5]، انبارهای داده[6] و غیره ذخیره می‌گردد. بر روی کامپیوترهای رومیزی و دستگاه‌های همراه (لپ‌تاپ‌ها، گوشی‌های هوشمند و درایوهای قابل حمل) معمولاً به طور مستقیم به‌صورت اسناد (PDF، Word، Excel، OpenOffice، و غیره)، طرح‌های گرافیکی (CAD، Catia و غیره)، فایل‌های متنی (کد منبع و غیره) و فایل‌های دودویی (تصاویر و غیره) در فایل‌سیستم ذخیره می‌گردد[۵].

۲-۳-۲- اطلاعات در حال استفاده

هر دارایی اطلاعاتی که در حال استفاده در یک ایستگاه کاری یا یک سرور باشد، *اطلاعات در حال استفاده* تلقی می‌گردد. با اینکه اطلاعات در حال استفاده نیز در اکثر موارد در یک دستگاه ذخیره‌سازی ذخیره می‌گردد، اطلاعات در حال استفاده توسط برنامه کامپیوتری در حافظه سیستم ذخیره می‌گردد و تهدیدات جدیدی را به وجود می‌آورد که باید به آن‌ها پرداخته شود. به‌علاوه، احتمال دستیابی و دستکاری برنامه‌هایی که از این اطلاعات استفاده می‌کنند باید در هنگام طراحی سازوکارهای حفاظت برای اجتناب از نشت اطلاعات، به حساب آورده شود. این برنامه‌ها نیز ممکن است دارایی‌های اطلاعاتی جدیدی را به وجود آورند که قبل از ذخیره‌سازی صحیح در حافظه سیستم ذخیره می‌شود [۵].

۲-۳-۳- اطلاعات در حال حرکت

هر دارایی اطلاعاتی که از درون شبکه سازمان عبور می‌کند *اطلاعات در حال حرکت* تلقی می‌گردد. با این که این دارایی‌ها در موقعیت دیگری نیز ذخیره شده‌اند (و بدین ترتیب اطلاعات در حال استراحت تلقی می‌شوند)، می‌توان آن‌ها را از طریق شبکه ارسال کرد و (اگر اطلاعات، بدون سازوکارهای محافظتی صحیح، به یک دستگاه غیرمجاز یا کنترل‌نشده برسد) احتمال تولید یک رونوشت کنترل‌نشده از یک سند حساس به وجود می‌آید. یکی از چالش‌های کنترل اطلاعات در حال حرکت، توانایی کنترل تعداد زیادی از پروتکل‌ها از قبیل HTTP، HTTPS، SMTP، P2P، FTP و غیره است که می‌توان از آنها برای ارسال اطلاعات استفاده کرد [۵].

۲-۴- روش‌های نشت اطلاعات

به زبان علوم کامپیوتر، *روش‌های نشت* را می‌توان به عنوان وسیله‌ای تعریف کرد که توسط آن، یک دارایی اطلاعاتی برای کاربران غیرمجاز افشا می‌گردد. با وجود این که دارایی‌های اطلاعاتی در طول تاریخ با وسایل فیزیکی نشت داده شده و ربوده شده است، استفاده گسترده از فناوری اطلاعات، راه‌های کپی‌برداری و ارسال اطلاعات را آسان کرده و طرق جدیدی را برای نشت ممکن ساخته است. در سطور بعدی، شرحی از هر دو نوع روش‌های نشت، با تمرکز بر نشت‌هایی که توسط سیستم اطلاعاتی تولید می‌شود، ارائه خواهد شد. این روش‌های نشت باید وقتی که فنونی همچون پنهان‌نگاری برای مخفی کردن تلاش برای سرقت اطلاعات مورد استفاده قرار می‌گیرد نیز به کار رود [۵].

۲-۴-۱- نشت فیزیکی

با این که این روزها اکثر اطلاعات داخل سازمان به‌صورت الکترونیکی ذخیره می‌شود، رسانه‌های این اطلاعات (درایوهای سخت، درایوهای USB، CDها و غیره) ابزارهای فیزیکی هستند که احتمال سرقت فیزیکی آنها وجود دارد. مخزن دارایی اطلاعاتی دیگر که از همه مهم‌تر است کاغذ است که می‌توان آن را به راحتی به سرقت برد، چرا که پیاده کردن محدودیت بر روی زیرساخت سازمان برای کنترل جریان اطلاعات در قالب چاپی به لحاظ عملی امکان‌پذیر نیست.

جلوگیری از نشت با این وسایل نیازمند پیاده‌سازی اقدامات امنیتی فیزیکی است که به استخراج تجهیزات سازمان اجازه نمی‌دهند. با این وجود، برای اعمال امنیت اطلاعاتی که از سازمان خارج می‌شود، سازوکارهایی همچون رمزگذاری دیسک سخت را می‌توان بر روی سیستم‌های اطلاعاتی پیاده کرد [۵].

۲-۴-۲- نشت سیستم‌های اطلاعاتی

همان سازوکارهایی که خودی‌ها از آن برای انجام وظایف کسب‌وکار معمول خود استفاده می‌کنند می‌توانند برای سرقت دارایی‌های اطلاعاتی نیز مورد استفاده قرار گیرند. فنونی که اطلاعات حساس را با هدف آشکار نشدن تبدیل می‌کنند روش‌های نشت تلقی نمی‌شوند. برای جلوگیری از نشت و سرقت اطلاعات، باید از سازوکارها و اقدامات حفاظتی در برابر این روش‌ها استفاده کرد [۵].

۲-۴-۲-۱- نشت از طریق شبکه سازمان

شبکه‌های سازمان، یکی از قسمت‌های ضروری از زیرساخت فناوری اطلاعات سازمان است. از شبکه سازمان می‌توان برای ارتباط داخل به داخل، خارج به داخل و داخل به خارج استفاده نمود.

1- Hard Disk
2- Memory Card
3- Solid State Disk
4- Databases
5- File Repositories
6- Data Warehouses

ارتباطات داخل به داخل، تمام ارتباطاتی را که در داخل شبکه سازمان اتفاق می‌افتد پوشش می‌دهد. با این که این نوع ارتباطات معمولاً نشت اطلاعات را نه تولید کرده و نه افزایش می‌دهد، اطلاعاتی که توسط این سازوکارها انتقال داده می‌شود می‌تواند به دریافت کنندگان غیرمجاز در داخل سازمان ارسال شود و نشت اطلاعاتی را در داخل سازمان به وجود آورد.

ارتباطات خارج به داخل، هر ارتباطی را که خارج از سازمان آغاز شده و مقصد آن نقطه‌ای در داخل زیرساخت شبکه سازمان است، پوشش می‌دهد. این نوع ارتباطات، مستعد تولید نشت اطلاعات است، چرا که ممکن است اطلاعات حساس، به اشتباه بر روی یک سرور دسترسی عمومی قرار گیرد. به‌علاوه، ممکن است نفوذگرهای[1] بیرونی به این سرورها نفوذ کرده و دسترسی به اطلاعات ذخیره شده بر روی آن‌ها را به دست آورند. ابزارهای امنیتی از قبیل سیستم تشخیص و جلوگیری از نفوذ[2]، دیواره‌های آتش و ضدویروس‌ها از سیستم‌ها در برابر این نوع تهدیدات خارجی محافظت می‌کنند.

ارتباطات داخل به خارج، دربرگیرنده هر گونه ارتباطی است که در داخل مرزهای سازمان آغاز شده و مقصدش خارج از سازمان است. این‌ها معمولاً گستره وسیعی از خدمات را دربر می‌گیرند که کارکنان برای ارتباط با جهان خارج مورد استفاده قرار می‌دهند. از تمام این خدمات می‌توان برای سرقت اطلاعات استفاده کرد، چرا که یک عامل داخلی می‌تواند اطلاعات حساسی را به یک شبکه اجتماعی ارسال کند، یک فایل حساس را از طریق رایانامه ارسال کرده و یا آن را به یک سرور FTP انتقال دهد. به‌علاوه، یک عامل داخلی خرابکار می‌تواند دارایی اطلاعاتی حساس را از طریق یک شبکه P2P پخش کند. علاوه‌بر این، یک عامل خرابکار می‌تواند با استفاده از یک روش پنهان‌نگاری که از یک کانال مخفی شبکه سوء استفاده می‌کند، اطلاعات را به سرقت ببرد [۵].

۲-۴-۲-۲- نشت از طریق چاپگر سازمان

چاپ کردن، اطلاعات یک فایل الکترونیکی را به یک تکه کاغذ حساس تبدیل می‌کند. در این رابطه، نباید خود چاپ کردن را یک روش نشت قلمداد کرد، بلکه یکی از رویه‌های اصلی است که ممکن است برای تبدیل اطلاعات دیجیتال به یک ظرف فیزیکی همچون کاغذ مورد استفاده قرار گیرد و استخراج فیزیکی آن را ممکن سازد که در اکثر موارد ممکن است شواهد و مدارکی را بر جای بگذارد [۵].

۲-۴-۲-۳- نشت از طریق رسانه‌های قابل حمل سازمان

استفاده از دیسک‌های سخت بیرونی[3]، درایوهای USB و غیره در سال‌های اخیر افزایش یافته است، چرا که حمل‌ونقل آسان فایل‌ها، پشتیبان‌ها و غیره را ممکن می‌سازند. علاوه بر گم شدن این‌گونه ابزارها که می‌تواند منجر به نشت اطلاعات شود، این ابزارها می‌توانند با ذخیره کردن رونوشت فایل‌های حساس بر روی سیستم‌های ذخیره‌سازی نظارت نشده، برای سرقت اطلاعات از سازمان، مورد استفاده خودی‌ها قرار گیرند. معمولاً این درایوهای قابل حمل[4] را می‌توان از طریق درگاه‌های USB به کامپیوتر وصل کرد؛ هم‌چنین هر روش دیگری نیز همچون Bluetooth، مادون قرمز[5] و غیره نیز ممکن است مورد استفاده قرار گیرد [۵].

۲-۴-۲-۴- نشت از طریق دستگاه‌های همراه شخصی

استفاده از گوشی‌های هوشمند و سایر دستگاه‌های همراه شخصی به شدت در طی سال‌های گذشته افزایش یافته است. این دستگاه‌ها قابلیت انجام عملیات‌های پیچیده را داشته و حتی می‌توان آن‌ها را از حیث توان محاسباتی با برخی کامپیوترهای شخصی مقایسه کرد. با این که این دستگاه‌ها امکان بهبود بخشیدن به بهره‌وری کارکنان را فراهم می‌کنند، روش‌های نشت تازه‌ای را نیز به‌وجود می‌آورند. این دستگاه‌ها معمولاً برای دسترسی به زیرساخت سازمان پیکربندی می‌شوند (حتی اگر ابزارهای شخصی باشند)؛ اما بر طبق سیاست امنیتی سازمان پیکربندی نمی‌شود (به طور مثال، ممنوع کردن استفاده از دوربین). بدین ترتیب، این روش نشت، روش نشت جدیدی می‌باشد که باید به حساب آورده شود [۵].

جدول (۲) خلاصه‌ای از روش‌های نشت را که قبلاً شرح داده شد نشان می‌دهد. هم محققین و هم تأمین کنندگان امنیت اطلاعات جهت توسعه سیستم‌ها و فنونی برای کاهش مخاطرات[6] از طریق این روش‌های نشت، کوشش‌های بسیاری را انجام داده‌اند.

جدول ۲- خلاصه روش‌های نشت سیستم‌های اطلاعاتی

	شبکه	چاپگر	رسانه قابل حمل	دستگاه همراه
امکان رمزگذاری	بله	خیر	بله	بله
نیاز به دسترسی فیزیکی	خیر	بله	بله	خیر
شیء موضوع نشت	داده	کاغذ	داده	داده
نظارت شده	بله	بله	بله	به‌طور جزئی
قابل قفل کردن	بله	بله	بله	به‌طور جزئی

1- Hackers
2- Intrusion Detection Prevention System (IDPS)
3- External Hard Drives
4- Removable Drives
5- Infrared
6- Risk Reduction

همان‌گونه که مشاهده می‌گردد، راه‌های متعددی برای نشت داده وجود دارد. شکل (۳) دید جامعی از انواع روش‌های نشت داده ارائه می‌دهد. این نمودار راه‌های مختلف نشت داده‌های در *حال حرکت*[1] و داده‌های در *حال استراحت*[2] و هم‌چنین روش‌های مختلف نشت داده در *نقاط پایانی*[3] یا راه‌های نشت داده که با استفاده از وسایل فیزیکی و یا مهندسی اجتماعی می‌تواند صورت گیرد را دسته‌بندی می‌کند [۶].

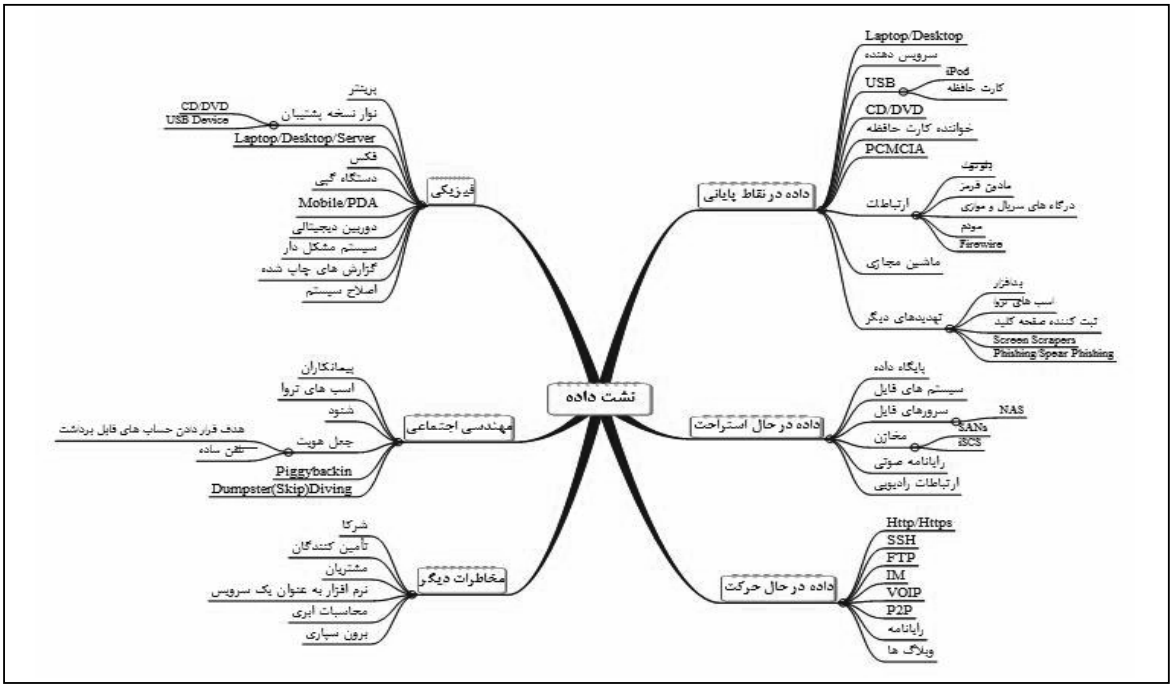
۳- راه‌کارهای جلوگیری از نشت اطلاعات

راه‌کارهای جلوگیری از نشت اطلاعات که سعی در پوشش دادن مسئله نشت اطلاعات را دارند، نه تنها تشخیص نشت‌های احتمالی، بلکه فراهم آوردن آموزش برای کارکنان، مدارک جرم‌شناسی، سیستم‌های مدیریت و رویه‌های عکس‌العمل را نیز دربر می‌گیرد. این راه‌کارها در مرحله اول، اطلاعات حساسی را که سازمان دارد شناسایی می‌کنند. وقتی پیکربندی انجام شد، روش‌های نشت را تحت نظارت می‌گیرند تا از ارسال اطلاعاتی که قبلاً به عنوان اطلاعات حساس شناسایی شده است جلوگیری کنند. در این‌باره، هر گاه داده‌ای در یک روش نشت قرار گیرد، در مقابل پایگاه داده اطلاعات حساس بررسی می‌شود. این بررسی عبارت از برابرسازی کلمات کلیدی، تشخیص الگو و انگشت‌نگاری می‌باشد. اگر هر کدام از این‌ها اطلاعات را حساس علامت‌گذاری کند، راه‌کار DLP جلوی ارسال اطلاعات را می‌گیرد. به‌علاوه، برخی از آنها امکان محدود کردن مجموعه برنامه‌هایی را که عامل داخلی می‌تواند اجرا کند، نیز فراهم می‌آورد و تنها به برنامه‌هایی که مورد اعتماد سازمان هستند اجازه اجرا می‌دهد. همچنین این راه‌کارها معمولاً شامل وسائل کشف اطلاعات نیز می‌شود که برای تحلیل و تشخیص خودکار اطلاعات حساس در سرورها و ایستگاه‌های کاری سازمان به کار می‌رود [۵].

۳-۱- استفاده از استانداردها و پیشنهادهای بین‌المللی

مدیریت امنیت اطلاعات امری پیچیده است که نه تنها کنترل‌های فنی بلکه مدیریت فرایند و سایر حوزه‌های سازمان را نیز دربر گرفته و در استاندارد ISO/IEC 27001 مجموعه‌ای از توصیه‌ها، فرایندها، روش‌شناسی‌ها و کنترل‌ها را مشخص می‌کند.

فعالیت‌های مختلفی را متناسب با استاندارد ISO/IEC 27001 برای مدیریت تهدیدات خودی تحلیل کرده‌اند. این فعالیت‌ها، سرقت اطلاعات را به طور خاص مورد تحلیل قرار نمی‌دهند، بلکه تمام تهدیداتی را که یک فرد خودی برای امنیت سیستم‌های اطلاعاتی سازمان شکل می‌دهد، تحلیل می‌کنند [۵].



شکل ۳- راه‌های نشت داده [۶]

1- Data in Motion 2- Data at Rest 3- End Point

۳-۲- سیستم‌های تشخیص خودی خرابکار

هدف از تحقیق درباره خودی‌های خرابکار، یافتن سازوکارها، رویه‌ها و فنونی برای تشخیص خودی‌های خرابکار در حیطه یک سازمان است. خودی‌های خرابکار ممکن است از سیستم‌های فناوری اطلاعات سوء استفاده کنند، اطلاعات را به سرقت ببرند، دست به تخریب و یا هرگونه عملی که برای منافع سازمان زیان‌آور است بزنند. تشخیص خودی، یک حوزه امنیت اطلاعات است که در سال‌های اخیر محبوبیت بسیاری یافته است. در واقع، حوزه‌ای است با تحقیقات گسترده که پیشنهادهای متعددی را برای سروکار داشتن با خودی‌ها ارائه کرده است. در حالی که گروهی از پیشنهادها بر تلاش برای هشدار از خطر خودی پیش از هرگونه نقض امنیتی ممکن تمرکز دارند، پیشنهادهای دیگر، حوادث خودی را در همان زمانی که اتفاق می‌افتد کشف می‌کنند. در حالی که برخی پیشنهادها می‌توانند یک تهدید خودی خاص را کشف کنند، پیشنهادهای دیگر خودیِ خرابکار را به عنوان یک تهدید عام تشخیص می‌دهند. پیشنهادهای تحلیل‌شده با استفاده از مشخصه‌های ارائه‌شده و خصوصیت زمانی طبقه‌بندی شده‌اند. این سازماندهی امکان ارائه پیشنهادهایی را که بر تشخیص تهدید نشت اطلاعات تمرکز دارند، با جزئیات بیشتر فراهم می‌کند [۵].

۳-۲-۱- پیشنهادهای پیش‌گویانه

فنون پیش‌گویانه سعی در شناسایی خودی‌های خرابکار قبل از این که بتوانند دست به عملی بزنند که برای سازمان زیان‌آور است، دارند. پیشنهادهای مرور شده در این‌باره، تهدید نشت اطلاعات به عنوان بخشی از تهدید خودیِ خرابکار را دربر می‌گیرند. یعنی تهدید بخصوصی را که توسط خودی به‌وجود می‌آید شناسایی نمی‌کنند. خروجی این فنون را می‌توان برای بهبود بخشیدن به کنترل‌های امنیتی در سازمان، تغییر امتیازات تخصیص داده‌شده یا کمک به منابع انسانی در طی فرایندهای استخدام به کار برد. «*شولتس*» و دیگران مجموعه‌ای از شاخص‌ها را (بیشتر رفتاری) برای ارزیابی خطر ایجادشده توسط خودی‌ها، تعریف می‌کنند. این شاخص‌ها از جمله رفتار لفظی، خصائص شخصیتی و ... که به وضوح تعریف نشده است را نمی‌توان بدون دخالت نظر فردی کمّی نمود؛ بنابراین با اعمال وزن به هر یک از شاخص‌ها، می‌توان برای هر یک از کارکنان یک ارزیابی خطر ارائه داد [۵].

۳-۲-۲- پیشنهادهای واکنشی

فنون واکنشی، خودیِ خرابکار را در همان لحظه‌ای که حمله را در برابر سازمان صورت می‌دهد آشکار می‌کند. این سیستم‌ها را می‌توان نوعی سیستم تشخیص ورود غیرمجاز در نظر گرفت به نحوی که حوادث امنیتی محتمل را که سیاست امنیتی سازمان را نقض می‌کند، آشکار می‌کنند. با وجود این که برخی از پیشنهادهای بررسی شده تفاوتی میان تهدیدات به وجود آمده توسط خودی‌های خرابکار قائل نمی‌شوند، برخی به طور مستقیم به تهدید نشت اطلاعات می‌پردازند. در واقع راه‌کارهای محافظت در برابر نشت اطلاعات که توسط تأمین کنندگان امنیت اطلاعات توسعه داده می‌شود در این دسته از پیشنهادها می‌گنجد [۵].

۳-۲-۳- پیشنهادهای تشخیص نشت اطلاعات

علاوه بر مطالعه تهدید *خودیِ خرابکار*، محققین به تهدیداتی که توسط *خودی‌ها* تحمیل می‌شود نیز پرداخته‌اند. این بخش به طور اخص، مطالعات مربوط به نشت اطلاعات را تحلیل می‌کند. کارهایی که بر تهدیدات خودی تمرکز دارند نه شرح داده شده و نه تحلیل می‌شوند؛ چرا که خارج از حوزه این مقاله می‌باشد.

۳-۲-۳-۱ پیشنهادهای جامعه تحقیقاتی

با این که پیشنهادهایی که تهدیدات خودیِ خرابکار را تحلیل می‌کنند، تهدید نشت اطلاعات را می‌پذیرند، میزان تحقیقاتی که به طور اخص به آن بپردازد امروزه بسیار کم است. محققین معماری‌ای را برای پیاده‌سازی چندین فن تحلیل پنهان‌نگاری جهت تشخیص محتوای پنهان‌نگاری که بلادرنگ از طریق پروتکل‌های شبکه ارسال می‌شود پیشنهاد می‌کنند. معماری پیشنهاد شده به سه لایه تقسیم می‌شود. لایه اول، مسئول استخراج ترافیک شبکه و طبقه‌بندی آن بسته به برنامه استفاده شده برای تولید آن (پروتکل شبکه) می‌باشد. لایه دوم، با توجه به یک پایگاه داده محتوا، محتوا را از بسته‌های شبکه استخراج می‌کند. هم‌چنین این لایه می‌تواند بررسی کند که آیا بعضی از محتواهای استخراج‌شده با پایگاه داده انبار بحرانی (اطلاعات حساس) مطابقت دارد یا خیر. در نهایت، محتوای استخراج‌شده از یک فرایند تحلیل پنهان‌نگاری عبور داده می‌شود. اگر محتوای مخفی یافت شود، این لایه تلاش می‌کند آن را از پوشش استخراج کرده و با پایگاه داده انبار بحرانی مقایسه کند [۵].

۳-۲-۳-۲- راه‌کارهای تجاری

صنعت امنیت اطلاعات، اهمیت تهدید نشت اطلاعات را با توسعه راه‌کارهای اختصاصی برای مبارزه با آن پذیرفته است. راه‌کارهای *جلوگیری یا محافظت از نشت اطلاعات*[1] محصولاتی تجاری هستند که از مجموعه‌ای از مؤلفه‌ها تشکیل می‌شوند (حسگرها، عامل‌های کشف اطلاعات، عامل‌های فیلتر کردن محتوا و غیره) که برای جلوگیری از نشت اطلاعات در زیرساخت سازمان عملیاتی می‌شود. راه‌کارهای DLP نه‌تنها برای جلوگیری از نشت اطلاعات ناشی از

1- Data Leakage Prevention/ Protection

خودی‌های خرابکار، بلکه برای جلوگیری از نشت‌های تصادفی که ممکن است به علت اشتباه افراد داخلی به وجود آید نیز مورد استفاده قرار می‌گیرد. جدول (۳) فهرستی از راه‌کارهای برتر را که توسط گارتنر[1] طبقه‌بندی شده است نشان می‌دهد [۵].

جدول ۳- لیست مهم‌ترین فروشندگان DLP توسط گارتنر [۵]

فروشنده	نام راه‌کار
Websense	Data Security Suite
Trend Micro	Leak Proof 5.0
RSA	Data Loss Prevention Suite
Symantec	Data Loss Prevention 9
McAfee	Total Protection
Palisade Systems	Palisade DLP
Verdasys	Digital Guardian 5
Computer Asociates	CA DLP v6
Fidelis Security Systems	Fidelis XPS
GTB Technologies	GTB Data Loss Platform
Safend	Safend Data Protection Suite
Trustwave	Trustwave DLP

۴- سامانه‌های جلوگیری از نشت اطلاعات

هم‌اکنون، سامانه‌های جامعی وجود دارند که از نشت داده به روش‌های مختلف جلوگیری می‌کنند و هم‌چنان نیز تلاش می‌کنند که به امکانات خود افزوده و راه‌های دیگر نشت داده را نیز پوشش دهند.

۴-۱- انواع سامانه‌های جلوگیری از نشت اطلاعات

سیستم‌های جلوگیری از نشت داده، داده‌های در حال استفاده، داده‌های در حرکت (داده‌های ارسالی در شبکه) و داده‌های ذخیره شده در دستگاه‌های ذخیره‌سازی داده را پایش و بررسی نموده و در صورتی که خط‌مشی‌های امنیتی تعریف شده را نقض کنند، دسترسی به آن‌ها را مسدود می‌نمایند. بر اساس نوع داده‌ها و به عبارتی کانال‌هایی که سیستم‌های DLP کار بررسی، تحلیل و مراقبت را انجام می‌دهند، می‌توان راه‌حل‌های DLP را به سه دسته زیر تقسیم نمود [۷و۸].

DLP مبتنی بر میزبان[2] (نقطه پایانی): سیستم‌های مبتنی بر میزبان، بر روی کامپیوترهای کاربران پایانی و یا سرورهای درون سازمان اجرا می‌شوند. این سیستم‌ها، ارتباطات درونی و بیرونی را پوشش می‌دهند و بنابراین می‌توانند برای کنترل جریان اطلاعات[3] بین گروه‌ها و یا انواع کاربران مورد استفاده قرار گیرند. به علاوه، DLPهای مبتنی بر میزبان، می‌توانند دستگاه‌های فیزیکی مانند دستگاه‌های همراه که قابلیت ذخیره داده را دارند را نیز بررسی نمایند. این سیستم‌ها می‌بایست بر روی کامپیوترهای همه کاربران شبکه نصب شوند که این امر یکی از معایب آن‌ها به شمار می‌رود. با استفاده از این سیستم‌ها، می‌توان بر کارمندانی که اطلاعات حساس را در iPod، لپ‌تاپ، USB، CD و یا هر وسیله همراه خود ذخیره می‌کنند تا در مکان دیگر بر روی آن‌ها کار کنند، کنترل کاملی اعمال نمود. می‌توان گفت که هدف اصلی فن‌آوری‌های مبتنی بر میزبان (نقطه پایانی) حفاظت از دارایی‌های معنوی و داده‌های ارزشمند سازمان‌ها از سرقت‌های درون‌سازمانی و نشت‌های اتفاقی داده می‌باشد.

DLP مبتنی بر شبکه[4]: DLPهای شبکه که با نام DLPهای مبتنی بر دروازه[5] نیز شناخته می‌شوند در محل اتصال سازمان به اینترنت نصب می‌شوند و ترافیک شبکه را برای یافتن ارسال اطلاعات غیرمجاز از طریق کانال‌های ارتباطی مانند رایانامه، پیام‌رسان، HTTP، FTP و HTTPS تحلیل می‌کنند (سادگی نصب این سیستم‌ها از مزیت آن‌ها به شمار می‌رود).

DLP کشف داده‌های در حال استراحت[6]: DLPهای کشف داده‌های در حال استراحت (داده ذخیره‌شده) را برای شناسایی نواحی مخاطرات، یعنی جاهایی که داده‌های محرمانه در مکان‌های نامناسب و ناامن ذخیره شده‌اند، بررسی می‌نماید. این سیستم‌ها در بسیاری موارد به‌صورت جداگانه و مستقل نبوده بلکه به‌عنوان قسمتی از DLPهای شبکه موجود می‌باشند. ارزش راه‌حل‌های شبکه و کشف داده با توجه به دیدی که از نحوه جریان اطلاعات به‌دست می‌دهند، بیشتر کمک به مدیران برای شناسایی داده و اصلاح نمودن فرایندهای کسب وکار نادرست، شناسایی و جلوگیری از افشای داده‌های حساس و فراهم نمودن روشی برای پشتیبانی از فعالیت‌های بازرسی می‌باشد.

۴-۲- امکانات یک سامانه جلوگیری از نشت اطلاعات جامع

یک راه‌حل جامع DLP، با مدیریت و کنترل خط‌مشی‌های تعریف شده برای سازمان، از نشت اطلاعات با استفاده از کانال‌های مختلف ارتباطی جلوگیری می‌کند که در ادامه به‌صورت فهرست‌وار بیان می‌شود [۹].

تعریف خط‌مشی: یک راه‌حل DLP خوب باید بتواند امکان تعریف و مدیریت خط مشی‌ها را به راحتی فراهم آورد.

شناسایی داده: سیستم‌های DLP از روش‌های مختلفی برای شناسایی داده‌های (در حال حرکت، درحال استراحت یا در حال

1- Gartner
2- Endpoint DLP
3- Information Flow
4- Network DLP
5- Gateway-Based DLP
6- Embedded DLP

استفاده) حساس و محرمانه استفاده می‌کنند. این سیستم‌ها، روش‌های مختلفی برای تحلیل دقیق محتوا بر اساس کلمات کلیدی، لغت‌نامه، عبارات منظم یا انطباق سند[1] به کار می‌برند (مثلا روش‌های آماری مانند بیزی[2]، یادگیری ماشین و انگشت‌نگاری[3]). قدرت موتور تحلیل و شناسایی داده DLPها، دقیقاً متناظر با میزان صحت آن در شناسایی داده‌ها است که با نتیجه اشتباهی مثبت یا نتیجه اشتباهی منفی[4] آنها ارتباطی مستقیم دارد.

پاسخ به حوادث: سازمان باید بتواند سریعاً به حادثه‌ای که اتفاق می‌افتد، پاسخ دهد.

پایش شبکه: قابلیت پایش شبکه در راه‌حل‌های DLP، امکان بازرسی ترافیک شبکه را فراهم می‌آورند و در نتیجه، دید مناسبی از انواع داده‌های موجود در ترافیک شبکه در اختیار ما قرار می‌دهند. وجود این نگاه، برای تحلیل و گزارش و نیز ایجاد خط‌مشی‌های مناسب، حیاتی است

امنیت وب: حملات وب برای دزدیدن اطلاعات حساس و محرمانه، ارتباط تنگاتنگی بین امنیت وب و ابزارهای جلوگیری از نشت داده ایجاد می‌کنند.

امنیت رایانامه: رایانامه، یکی از ساده‌ترین روش‌های ارسال اطلاعات محرمانه و حساس است. اطلاعات محرمانه در بدنه رایانامه و یا به‌صورت ضمیمه آن قرار می‌گیرند.

کشف داده: کشف مکان داده‌های حساس در سرورها، پایگاه داده‌ها، نقاط پایانی و دیگر مکان‌ها که آیا داده مطابق با خط‌مشی سازمان در مکان امنی ذخیره شده است یا خیر، یکی از قابلیت‌های سیستم‌های DLP می‌باشد. کشف داده به‌طور پیوسته، ذخیره‌سازی داده‌های حساس را پایش می‌نماید و در صورت لزوم آن‌ها را حذف و یا رمزنگاری می‌کند. هم‌چنین پویش مکان‌های دوردست با پهنای باند کم ممکن باشد

امنیت نقاط پایانی: نقاط پایانی یا لپ‌تاپ‌ها در سیستم‌های DLP نیاز به توجه خاصی دارند زیرا این وسایل دارای چندین روش برای انتقال اطلاعات هستند. کاربران در نقاط پایانی می‌توانند داده‌ها را در رسانه داخلی آن ذخیره کنند و یا به‌وسیله رسانه‌های قابل حمل مانند حافظه USB، CD، چاپ مستقیم و یا شبکه‌ای منجر به نشت اطلاعات گردند.

۴-۳- مقایسه سامانه‌های جلوگیری از نشت اطلاعات شناخته‌شده

بازار فعلی سیستم‌های جلوگیری از نشت داده در سال‌های اخیر با توجه به رکود جهانی اقتصاد، رشد قابل ملاحظه‌ای داشته است.

1- Document Matching
2- Baysian
3- Finger Printing
4- False Negative

سیستم‌های DLP مختلفی از طرف شرکت‌های مختلف عرضه شده‌اند که در اندازه، قابلیت‌ها و کانال‌های ارتباطی که پوشش می‌دهند با یکدیگر متفاوت هستند. بازار این محصولات را می‌توان به دوشاخه اصلی ارائه‌دهندگان DLP برای سازمان‌های بزرگ که دارای امکانات و قابلیت‌های فراوانی می‌باشند و ارائه‌دهندگان راه‌حل‌های DLP برای کسب‌وکارهای کوچک که قابلیت‌های حداقلی را دارا می‌باشند، تقسیم نمود. در نتیجه، سازمان‌ها با هر ابعاد و اندازه‌ای، با گزینه‌های مختلفی برای انتخاب روبرو هستند.

از تغییرات عمده‌ای که اخیراً در روند تولید این محصولات صورت گرفته است، اضافه کردن امکانات بیشتر برای پاسخ به نیازمندی‌های سازمان‌های بزرگ و ایجاد یک سیستم جامع، بومی‌سازی این محصولات و قابل استفاده کردن آن برای همگان و یکپارچه نمودن امکانات و قابلیت‌های DLP با محصولات و ابزارهای امنیتی قدیمی را می‌توان نام برد.

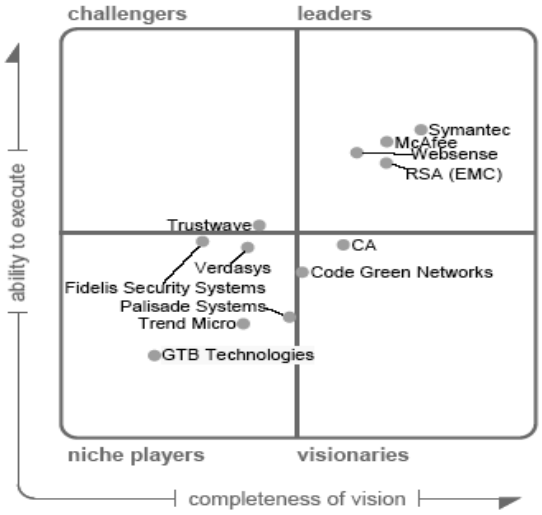
بر اساس گزارش گارتنر، بسیاری از سیستم‌های DLP که امکانات حداقلی مانند امنیت رایانامه، دریچه وب امن و سیستم حفاظت نقطه پایانی را فراهم می‌کنند، برای پاسخگویی به نیازمندی‌های DLP شرکت‌های کوچک و متوسط (بیشتر ۷۰٪ سازمان‌ها)، کافی می‌باشند.

یکی از دلایل بلوغ این بازار را می‌توان خریداری شرکت‌های کوچک این حوزه، توسط شرکت‌های امنیتی بزرگ دانست که با توجه به فروش بالایی که دارند، می‌توانند بازار این محصولات را در بین خریداران خود باز کنند. شرکت‌های بزرگی همچون Symantec، McAfee، RSA و Websense شرکت‌های ارائه‌دهنده DLP را خریداری نموده و توانسته‌اند با گسترش آن‌ها، به عنوان پیشگامان این محصولات در بازار قرار بگیرند. نمونه‌هایی از خریداری شرکت‌های کوچک در جدول (۴) نمایش داده شده است [۸].

جدول ۴- نمونه‌هایی از خریداری شرکت‌های کوچک ارائه‌دهنده DLP

سال	شرکت خریداری‌شده	شرکت خریداری‌کننده
2007	Vontu	Symantec
2006 2008	Onigma Reconnex	McAfee
2007	PortAuthority	Websense
2007	Tablus	RSA

شرکت گارتنر که هر ساله فعالان بازار محصولات رایانه‌ای در بخش‌های مختلف را بررسی می‌کند، در گزارشی در سال ۲۰۱۰ انواع شرکت‌های ارائه‌دهنده DLP را بررسی نموده و در مربع جادویی خود در شکل (۴) جای داده است.



شکل ۴- مربع جادویی گارتنر برای مقایسه محصولات DLP [۸]

در نمودار گارتنر، محور افقی برای نمایش میزان درک شرکت‌ها از بازار و قدرت اجرایی چشم‌اندازهای آنان می‌باشد. هرچه شرکت‌ها در این محور جلوتر قرار بگیرند، به این معنی است که این شرکت‌ها، بازار محصول و نیازمندی‌های مشتریان بازار را بهتر می‌شناسند.

در محور عمودی نمودار، قدرت اجرایی ایده‌های شرکت به شکل کمّی نشان داده می‌شود. این محور، شرکت‌ها را بیشتر بر اساس توانایی ارائه سه دسته قابلیت شبکه، نقطه‌پایانی و کشف داده و اینکه تا چه حد یکپارچگی با شرکای داخلی (مثلا شرکت DLP خریداری‌شده) و یا خارجی وجود دارد، رتبه‌بندی می‌کند. برای اندازه‌گیری این پارامتر، به مواردی مانند تنوع محصولات و خدمات شرکت، سیاست‌های فروش و قیمت‌گذاری، بازخورد و تجربیات مشتریان شرکت، حجم عملیات شرکت و سرعت پاسخ‌گویی به تغییرات بازار، توجه می‌شود.

شرکت‌هایی که در این نمودار در یک چهارم بالا و سمت راست قرار می‌گیرند رهبران[1] بازار محسوب می‌شوند. چرا که محصولات آنها از یک سو بیشترین سازگاری را با نیازهای مشتریان فعلی دارد و از سویی دیگر امکان ایجاد تغییرات سریع و اعمال نوآوری در محصولات، برای آن‌ها فراهم است. این گروه که در جداول (۵، ۶، ۷ و ۸) قرار دارند قابلیت‌های وسیعی را در هر سه حوزه ارائه داده‌اند، دورنما و چشم‌انداز بلندی دارند. در این دسته شرکت‌هایSymantec، McAfee، Websense و RSA قرار دارند و سهم بزرگی از بازار را به خود اختصاص داده‌اند.

1- Leaders

جدول ۵- بررسی ویژگی‌های محصول DLP شرکت Symantec [۸]

نام محصول	Symantec
خریداری شرکت	Vontu، ۲۰۰۷
قابلیت‌های DLP شبکه	عالی
قابلیت‌های DLP نقطه پایانی	خوب (دارای برخی محدودیت‌ها)
قابلیت‌های DLP کشف داده	عالی
شبکه VAR[2]	دارای شبکه قوی
محصول Enterprise بودن	بله
یکپارچگی	بله
قیمت	دارای بیشترین قیمت لیسانس
میدان حضور	جهانی
اندازه سازمان	سازمان‌های بزرگ
پشتیبانی از کاراکترهای دوبایتی	پشتیبانی می‌کند و برای ۲۵ زبان در سیستم‌های عامل مایکروسافت محلی شده است
مشکل یا ملاحظه لازم	پیچیدگی در پیاده‌سازی و کار با آن، برای جاهایی پیشنهاد می‌شود که از دیگر ابزارهای نقاط پایانی Symantec، مانند ضدویروس آن استفاده می‌شود
خصوصیات دیگر	قویترین راه‌حل DLP است، قابلیت‌های شبکه و جریان‌کاری[3] آن در صنعت هدایت کننده است، مدل متدولوژی ساخت به بلوغ رسیده‌ای دارد که در این بازار یکتا است

جدول ۶- بررسی ویژگی‌های محصول DLP شرکت McAfee [۸]

نام محصول	McAfee
خریداری شرکت	Reconnex، ۲۰۰۸
قابلیت‌های DLP شبکه	عالی
قابلیت‌های DLP نقطه پایانی	عالی
قابلیت‌های DLP کشف داده	عالی
شبکه VAR	دارای شبکه قوی
محصول Enterprise بودن	بله
یکپارچه‌سازی	بله (قبلاً یکپارچگی کامل بین انواع DLP آن و یکپارچگی با دیگر محصولاتش وجود نداشت ولی اکنون یکپارچگی خوبی ایجاد نموده است)
میدان حضور	جهانی
اندازه سازمان	سازمان‌های بزرگ
مشکل یا ملاحظه لازم	DLP آن بیشترین سازگاری را با نقاط پایانی که از ضدویروس McAfee و یا دیگر محصولات آن استفاده می‌کنند، دارد
خصوصیات دیگر	مدیریت خط‌مشی متمرکز با استفاده از ابزار راهبری[4]، با ارائه رمزنگاری بر روی رسانه نقاط پایانی و کنترل وسیله‌های قابل حمل، مزیت‌های رقابتی برای خود ایجاد کرده است، این محصول برای کاربران دیگر ابزارهای McAfee بسیار ارزشمند بوده است

2- Value Added Reselers
3- Workflow
4- ePolicy Orchestrator

جدول ۷- بررسی ویژگی‌های محصول DLP شرکت WebSense [۸]

نام محصول	WebSense
خریداری شرکت	PortAuthority، ۲۰۰۷
قابلیت‌های DLP شبکه	خوب
قابلیت‌های DLP نقطه پایانی	خوب
قابلیت‌های DLP کشف داده	خوب
شبکه VAR	-
محصول Enterprise بودن	بله
یکپارچگی	بله یکپارچه‌سازی با Websense Security Gateway
میدان حضور	جهانی
اندازه سازمان	سازمان‌های بزرگ، توزیع شده از نظر جغرافیایی و کمتر از ۵۰۰۰ کاربر
خصوصیات دیگر	دارای جریان کاری مناسب، یکپارچه‌سازی قابلیت‌های DLP با دروازه امنیتی وب WebSense[1]، راه‌اندازی DLP را برای مشتریان فعلی WebSense ساده نموده است، خط سیر تکاملی آن قوی است و اجرای قوی‌ای در سال ۲۰۰۷ و ۲۰۰۸ داشته است

جدول ۸- بررسی ویژگی‌های محصول DLP شرکت RSA(EMC) [۸]

نام محصول	RSA(EMC)
خریداری شرکت	Tablus، ۲۰۰۷
قابلیت‌های DLP شبکه	عالی
قابلیت‌های DLP نقطه پایانی	خوب (قابلیت‌های شبکه‌ای آن مشکل دارد، وقتی از شبکه شرکت خارج می‌شود، نمی‌تواند کنترل کند)
قابلیت‌های DLP کشف داده	عالی
شبکه VAR	-
محصول Enterprise بودن	بله
یکپارچه‌سازی	یکپارچه‌سازی با SIEM [2]
میدان حضور	جهانی و پراکنده از نظر جغرافیایی
اندازه سازمان	سازمان‌های بزرگ که نیازمندی‌های پیچیده کشف داده برای هزاران نقطه پایانی دارند
بهترین حوزه کاربرد	مشتریان مختلف در همه بخش‌ها و حوزه‌ها
پشتیبانی از کاراکترهای دوبایتی	محدویت‌های دو بایتی
مشکل یا ملاحظه لازم	نقطه پایانی آن هنوز احتیاج به بهبود دارد تا با محصولات شرکت‌های ضدویروس و شرکت‌هایی که متمرکز بر ارائه DLP نقطه پایانی هستند، قابل رقابت باشد
خصوصیات دیگر	قابلیت‌های محتوای توصیف شده قوی آن بوسیله فرایندهای مهندسی دانش فرمال، توانایی شناسایی داده مناسبی فراهم می‌کند که مکمل قابلیت شناسایی محتوای انگشت‌نگاری سند می‌باشد

1- WebSense Web Security Gateway
2- Security Information and Event Management (SIEM)

۵- نتیجه‌گیری

علاوه بر عوامل خارجی که امنیت سازمان‌ها را تهدید می‌کنند، بیشتر حوادث نشت اطلاعات منشاء داخلی دارند. کارمندانی که بدون توجه به خط‌مشی‌های امنیتی سازمان، اطلاعات محرمانه را از طریق کانال‌های ارتباطی مختلف مانند وب و رایانامه ارسال می‌کنند یا داده‌های حساس را در وسایل قابل حمل کپی می‌کنند، ناخواسته منجر به نشت اطلاعات سازمان می‌شوند. در این میان تعداد بسیار اندکی از کارمندان سازمان نیز یافت می‌شوند که با نیّت‌های سوء، داده‌های حساس را در اختیار افراد خارج از سازمان قرار می‌دهند. نشت اطلاعات، هم‌چنین می‌تواند در اثر آلوده شدن کامپیوترهای شخصی کاربران و ارسال داده‌های محرمانه به خارج آن و یا با استفاده از کانال‌های پوششی در پوشش کانال‌های مجاز به وقوع بپیوندد.

نشت اطلاعات به هر دلیل، خسارات سنگین و گاه جبران‌ناپذیری در پی دارد. هم‌چنین قوانین و الزامات دولتی و بازرگانی، برخی از سازمان‌ها را ملزم به فراهم آوردن کنترل امنیتی مناسب می‌کنند. در نتیجه، سازمان‌های بزرگ تلاش می‌کنند که با فراهم آوردن یک لایه امنیتی دیگر در پدافند غیرعامل (امنیت، ایمنی و پایداری)، از نشت داده به خارج از سازمان جلوگیری کنند. سیستم‌های DLP با هدف پایش و جلوگیری از نشت داده‌های سازمان این نیاز را برآورده می‌کنند. این سیستم‌ها خط‌مشی‌های امنیتی تعریف‌شده در سازمان را اعمال نموده و در صورت نقض آن‌ها اقدامات مناسب انجام می‌دهند و در نهایت، کنترل مناسبی بر روی داده‌های سازمان فراهم می‌کنند.

مراجع

1. Dehghani, M., Saleh Esfahani, M., Network Covert Channels: An Information Leakage Flow, Passive Defence Quarterly, Serial No. 9, (**2012**) (in Persian).
2. Research Report of IDC, Information Protection and Control Survey: Data Loss Prevention and Encryption Trends, Doc # 211109, March (**2008**).
3. Research Report of TheInfoPro Analyst, 2009, Top Pain Points, February (**1999**).
4. Cluley, G., Second Man Pleads Guilty In Hhuge Data Breach Case, Online Article Of Sophos, September 23, (**2008**), http://nakedsecurity.sophos.com/2008/09/23/second-tjx/.
5. Blasco Alis, J., Information Leakage and Steganography: Detecting and Blocking Covert Channels, Computer Science Department, May 21, (**2012**).
6. Bunker, G., Fraser-King, G., Data Leaks for Dummies, Book, (**2009**).
7. Web-based Encyclopedia WikiPedia, (**2011**), http://en. wikipedia.org/.
8. Ouellet, E., Paul, E., Magic Quadrant for Content-Aware Data Loss Prevention, Gartner Research, June 22, (**2009**).
9. A Buyer's Guide to Data Loss Protection Solutions, WebSense White Paper, August (**2010**).

Examining the Methods of Information Compromise and its Countermeasures Techniques

M. H. Hasan Nia[1]
M. Dehghani[2]

Abstract

Nowadays, the assets of an organization are assessed not only through physical possessions but also by the information they have. Information is prone to threat as are the other assets of every organization. These threats include attack from outsiders or insiders who may intend to affect the passive defense (security, safety and survivability) of the information assets an organization possesses. One of the threats to which information assets are exposed to is information compromise, the threat that causes unauthorized disclosure of confidential information. There are various ways for information compromise, therefore; it is necessary to identify and properly organize sensitive information in order to reduce the threats made by the information compromise events. The sensitive information should be protected using security tools known as DLP methods that are developed by security providers.

Key Words: *Threat, Passive Defense, Security, Information Compromise*

1- M.S Candidate of Imam Hussein Comprehensive University (hassannia@ihu.ac.ir) - Writer in Charge
2- Instructor and Academic Member of Imam Hussein Comprehensive University (mdehghany@ihu.ac.ir)