نرم‌افزار پیشگیری از دست دادن داده‌ها

نرم افزار پیشگیری از دست دادن داده ، نقض احتمالی داده ها را تشخیص داده و با مانیتور کردن آنها ، [۱] شناسایی و مسدود کردن داده های حساس در هنگام *استفاده* (اقدامات نهایی) ، در *حرکت* (ترافیک شبکه) و در *حالت استراحت* (ذخیره سازی داده ها) مانع از آنها می شود. .

اصطلاحات " از دست دادن داده " و " نشت داده " مرتبط هستند و اغلب به‌صورت متقابل استفاده می شوند. [۲] حوادث از دست دادن داده ها در مواردی که رسانه های حاوی اطلاعات حساس، گم شده و متعاقبا توسط یک طرف غیرمجاز از بین می روند به حوادث نشت داده ها تبدیل می شوند. با این حال ، نشت داده ها بدون از دست دادن داده ها در طرف مبدا امکان پذیر است. سایر اصطلاحات مرتبط با پیشگیری از نشت داده ها عبارتند از: تشخیص و پیشگیری از نشت اطلاعات (ILDP) ، جلوگیری از نشت اطلاعات (ILP) ، نظارت و فیلتر کردن محتوا (CMF) ، محافظت و کنترل اطلاعات (IPC) و سیستم پیشگیری از اکستروژن (EPS) ، در مقابل سیستم پیشگیری از نفوذ .

دسته بندی ها

وسایل تکنولوژیکی استفاده شده برای مقابله با حوادث نشت داده ها را می توان به این دسته بندی ها تقسیم کرد: اقدامات امنیتی استاندارد ، اقدامات امنیتی پیشرفته / هوشمند ، کنترل دسترسی و رمزگذاری و سیستم های DLP تعیین شده. [۳]

اقدامات استاندارد

اقدامات امنیتی استاندارد مانند فایروال ها ، سیستم های تشخیص نفوذ (IDS) و نرم افزار آنتی ویروس معمولاً محصولات در دسترسی هستند که رایانه ها را در برابر حملات بیرونی و درونی محافظت می کنند. به عنوان مثال، استفاده از فایروال مانع از دسترسی افراد خارجی به شبکه داخلی می شود و یک سیستم تشخیص نفوذ، تلاش های نفوذ کردن توسط افراد خارجی را تشخیص می دهد.

اقدامات پیشرفته

اقدامات امنیتی پیشرفته از الگوریتم های یادگیری ماشین و الگوریتم های استدلال زمانی برای تشخیص دسترسی غیر طبیعی به داده ها (به عنوان مثال ، پایگاه داده ها یا سیستم های بازیابی اطلاعات) یا تبادل ایمیل غیرعادی ، و از هانی‌پات برای شناسایی کارمندان مجاز با اهداف مخرب و از نظارت بر فعالیت کاربر برای تشخیص دسترسی غیر طبیعی به داده ها استفاده می کند.

سیستم های تعیین شده

سیستم های تعیین شده ، تلاش های غیرمجاز برای کپی یا ارسال داده های حساس را، آگاهانه یا ناآگاهانه، عمدتاً توسط پرسنلی که مجاز به دسترسی به اطلاعات حساس هستند، شناسایی و از آنها جلوگیری می کنند و برای طبقه بندی اطلاعات معین به عنوان اطلاعات حساس، از مکانیزم هایی از قبیل تطبیق دقیق داده ها ، اثر انگشت ساختاری داده ها ، روش های آماری ، تطبیق قانون و عبارت های منظم ، واژگان منتشر شده ، تعاریف مفهومی ، کلمات کلیدی و اطلاعات متنی مانند منبع داده ها استفاده می کنند. [۴]

انواع

شبکه

فناوری شبکه (داده های در حال حرکت) معمولاً در نقاط خروجی شبکه در نزدیکی محیط نصب می شود و ترافیک شبکه را برای شناسایی داده های حساس که بر خلاف سیاست های امنیت اطلاعات ارسال می شوند تجزیه و تحلیل می کند.
چندین نقطه کنترل امنیتی ممکن است فعالیتها را جهت مورد تجزیه و تحلیل قرار گرفتن یک سرور مدیریت مرکزی گزارش دهند. [۲]

اطلاعات در حالت استراحت

"داده در حال استراحت" به طور خاص به اطلاعات بایگانی شده قدیمی اشاره دارد. این اطلاعات نگرانی زیادی را برای مشاغل و مؤسسات دولتی ایجاد می کند ، به این دلیل که هرچه داده ها مدت زمان طولانی تری در فضای ذخیره استفاده

نشده باقی بمانند ، با احتمال بیشتری توسط افراد غیرمجاز بازیابی می شود. محافظت از چنین داده هایی شامل روش هایی مانند کنترل دسترسی ، رمزگذاری داده ها است . [۲]

داده های در حال استفاده

"داده در حال استفاده" به داده هایی اطلاق می شود که کاربر در حال حاضر با آنها در تعامل است. سیستم های DLP که از داده های در حال استفاده محافظت می کنند ، می توانند فعالیتهای غیرمجاز را نظارت و نشانه گذاری کنند. [۲] این فعالیت ها شامل عملیات ضبط صفحه ، کپی / چسباندن ، چاپ و نمابر است که شامل داده های حساس است. این می تواند تلاش های عمدی یا غیر عمدی برای انتقال داده های حساس از طریق کانال های ارتباطی باشد.

داده های در حال حرکت

"داده در حال حرکت" داده هایی است که از طریق شبکه به یک نقطه انتهایی در حال عبور است. شبکه ها می توانند داخلی یا خارجی باشند. سیستم های DLP که از داده های در حال حرکت محافظت می کنند ، بر داده های حساس که از طریق کانال های مختلف ارتباطی از شبکه عبور می کنند، نظارت می کنند. [۲]

منابع

1. *Hayes, Read (2007), "Data Analysis" (https://dx.doi.org/10.1057/9780230598546_9), Retail Security and Loss Prevention, Palgrave Macmillan UK: 137–143, ISBN 978-1-349-28260-9, retrieved 2020-01-22*
2. *Asaf Shabtai, Yuval Elovici, Lior Rokach, A Survey of Data Leakage Detection and Prevention Solutions (https://www.springer.com/computer/security+and+cryptology/book/978-1-4614-2052-1), Springer-Verlag New York Incorporated, 2012*
3. *Phua, C., Protecting organisations from personal data breaches (http://www.sciencedirect.com/science/article/pii/S1361372309700119), Computer Fraud and Security, 1:13-18, 2009*
4. *Ouellet, E., Magic Quadrant for Content-Aware Data Loss Prevention, Technical Report, RA4 06242010, Gartner RAS Core Research, 2012*

آخرین ویرایش ۲ ماه پیش توسط **M4tinbeigi** انجام شده