سازمان بورس و اوراق بهادار
SECURITIES & EXCHANGE ORGANIZATION

الزامات ثبت لاگ

مرکز نظارت بر امنیت اطلاعات بازار سرمایه (مکنا)

طبقه بندی محرمانگی: عادی

ویرایش ۱,۲

آبان ۱۳۹۷

فهرست

پیشگفتار ۳
تعریف واژگان ۵
ساختار ارتباطی الزامات مرکز نظارت بر امنیت اطلاعات بازار سرمایه ۶
۱- ثبت لاگ ۷
۱-۱- نکات عمومی ۷
۱-۲- امنیت شبکه و ارتباطات ۸
۱-۳- سیستم‌عامل‌ها ۱۱
۱-۴- نرم‌افزارها ۱۳
۱-۵- سرویس‌ها ۱۴
۱-۶- سرویس پایگاه داده‌ها ۱۵
۲- منابع ۱۷

پیشگفتار

ثبت و نگهداری رویدادها و وقایع در تمام سطوح فناوری هم به لحاظ فنی و هم به لحاظ قانونی و مقرراتی جزو ضروریات هر زیر ساخت و سامانه‌ای می‌با شد. ذخیره و نگهداری کامل رویدادها و وقایع در حوزه فناوری، کاربردهای گوناگونی می‌تواند داشته باشد. به عنوان مثال در صورتی که اختلالی در عملکرد سیستم ایجاد شود، مراجعه به رویدادها و وقایع ذخیره شده می‌تواند ردیابی ریشه و منشأ اختلالات را نشان دهد و در عیب‌یابی سیستم‌ها بسیار کمک‌کننده باشد. در موضوعاتی که به امنیت سیستم‌ها یا جرائم رایانه‌ای مرتبط می‌شوند، ذخیره رویدادها و وقایع به نحوی که بتوان به عنوان ادله الکترونیکی استنادپذیر به آن‌ها رجوع نمود، می‌تواند گره‌گشا باشد.

از زاویه قانونی و مقرراتی نیز بر ضرورت تولید و نگهداری رویدادها و وقایع در تمام سطوح فناوری تأکید شده است. ازجمله می‌توان به موارد ذیل اشاره نمود:

- فصل دوم و سوم آئین‌دادرسی، قانون جرائم رایانه‌ای مصوب ۱۱ بهمن ۱۳۸۹ مجلس شورای اسلامی
- آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، مصوب ۱۳۹۳/۵/۱۲ قوه محترم قضاییه
- سند الزامات امنیت اطلاعات بازار سرمایه (کنترل‌های امنیتی بخش ۹)

لازم به ذکر است که در استانداردهای بین‌المللی امنیت اطلاعات نیز بر ضرورت تولید و نگهداری رویدادها و وقایع زیر ساخت‌ها و سیستم‌ها تأکید شده است. حتی در این زمینه، استاندارد بین‌المللی مختص تولید و نگهداری رویدادها تدوین شده است. استانداردهایی مانند NIST 800-92 و SANS Information Logging Standard از جمله این موارد می‌باشند.

این سند، الزامات نگهداری رویدادها و وقایع را در حوزه‌های ذیل پوشش داده است:

- شبکه و ارتباطات
- تجهیزات امنیتی
- سیستم‌عامل‌ها
- سرویس‌ها

- پایگاه داده‌ها
- نرم‌افزارها

باید به این نکته اشاره شود که رویدادها و وقایع ذخیره شده در حوزه فناوری، زمانی سودمند خواهند بود که به صورت جامع رویدادهای همه ابعاد فناوری از پایین‌ترین لایه تا بالاترین لایه را به شکل مناسبی پوشش داده باشند.

تعریف واژگان

لاگ: یک رکورد از فعالیت رخ داده (رویدادها و وقایع) در سطح یک سیستم، سامانه یا سرویس، لاگ[۱] نامیده می‌شود. به دلیل درک بهتر و برقراری ارتباط معنایی برای افراد فنی، لاگ به فارسی ترجمه نشده است و عبارت لاگ عیناً با معنی فوق در این مستند به کار رفته است.

سوییچ دسترسی سرورها: به سوییچی که مستقیم به سرورها متصل شده است، سوییچ دسترسی سرورها گویند.

سوییچ هسته: به سوییچی که ارتباط کلیه اجزای شبکه را به هم پیوند می‌زند، سوییچ هسته شبکه گویند.

[۱] Log

ساختار ارتباطی الزامات مرکز نظارت بر امنیت اطلاعات بازار سرمایه

ارتباط بین "سند الزامات امنیت اطلاعات بازار سرمایه"، "سند الزامات ثبت لاگ" و پیوست الف سند الزامات ثبت لاگ با عنوان "راهنمای تولید و نگهداری لاگ و سوابق تراکنش‌ها در سامانه‌های معاملات برخط" به شکل زیر می باشد.

۱- ثبت لاگ

در این بخش نکات عمومی که باید بطور کلی در تهیه لاگ‌ها در تمام سطوح مدنظر قرار گیرد و همچنین حداقل لاگ‌هایی که باید در حوزه‌های شبکه و ارتباطات، تجهیزات امنیتی، سیستم‌عامل‌ها، سرویس‌ها، پایگاه‌داده‌ها و نرم‌افزار نگهداری شوند مشخص شده است.

۱-۱- نکات عمومی		
ردیف	عنوان	توضیحات
۱	تنظیمات تاریخ و زمان	تاریخ و زمان تمامی‌تجهیزات و سرویس‌هایی که از آن‌ها لاگ‌گیری انجام می‌شود باید بر اساس کنترل شماره ۹-۷ سند الزامات امنیت اطلاعات بازار سرمایه با یک مرجع زمانی مشترک در شبکه همگام‌سازی شوند و صحت توالی زمانی لاگ‌ها حفظ شود.
۲	سرویس مدیریت لاگ مرکزی	جهت ذخیره‌سازی و پردازش تمامی لاگ‌ها می‌بایست سرویس مدیریت لاگ مرکزی (یا حداقل به ازای هر سطح لاگ یک سرویس لاگ مرکزی مجزا؛ مانند لاگ امنیت شبکه و ارتباطات، لاگ سیستم‌عامل، لاگ سرویس پایگاه‌داده و ...) راه‌اندازی شود. تمامی لاگ‌های بیان شده در این سند می‌بایست به سمت این سرویس(ها) ارسال و نگهداری گردند.
۳	زمان نگهداری لاگ‌ها	تمام لاگ‌ها حداقل به مدت شش ماه با رعایت سایر قوانین بالادستی در این خصوص نگهداری شوند.
۴	آدرس IP کاربران	تمامی کاربران و راهبران در شبکه داخلی شرکت می‌بایست دارای آدرس IP مشخص و مستند شده باشند و در صورت تغییر با اطلاع نماینده امنیت شرکت مستندات به‌روز رسانی گردد.
۵	اقلام اطلاعاتی ضروری لاگ‌ها	تمام لاگ‌های تولید شده باید تمامی نیازمندی‌های کنترل شماره ۹-۲ سند الزامات امنیت اطلاعات بازار سرمایه را پوشش دهد.
۶	مدیریت حجم لاگ‌های تولیدی	انجام هرگونه اقدامی که بدون از دست رفتن لاگ‌های این دستورالعمل، منجر به کاهش حجم لاگ‌ها شود (از قبیل عدم ذخیره‌سازی لاگ‌های تکراری یا فشرده‌سازی لاگ‌ها و ...) منعی نخواهد داشت.

۱-۲- امنیت شبکه و ارتباطات		
ردیف	عنوان	توضیحات
۱	لاگ سوییچ هسته شبکه	تنظیمات Syslog بر روی سوییچ هسته مرکزی شبکه به صورتی تنظیم شود که تمامی دسته‌بندی‌های زیر را ثبت نماید و برای سرویس مدیریت لاگ مرکزی ارسال نماید. • Emergencies • Alerts • Critical • Errors • Warnings • Notifications • Information
۲	لاگ سوییچ دسترسی سرورها	تنظیمات Syslog بر روی سوییچ دسترسی سرورها به صورتی تنظیم شود که تمامی دسته‌بندی‌های زیر را ثبت نماید و برای سرویس مدیریت لاگ مرکزی ارسال نماید. • Emergencies • Alerts • Critical • Errors • Warnings • Notifications • Information
۳	لاگ سیاست‌های دسترسی	در صورتی که در تجهیزات شبکه مانند روترها و سوییچ‌ها سیاست‌های دسترسی[۲] ایجاد شده باشد، لازم است لاگ‌های ذیل دریافت و به سرویس مدیریت لاگ مرکزی ارسال گردد. • لاگ Permit • لاگ Deny
۴	لاگ ترافیک فایروال‌های شبکه	لاگ‌های مربوط به ترافیک‌های عبوری از فایروال با تنظیم Deny و Allow می‌بایست ذخیره گردد.
۵	لاگ سرویس‌های IPS/IDS	لاگ IPS/IDS تحت شبکه، باید به صورت استاندارد در سرویس مدیریت لاگ مرکزی ذخیره شود.

[۲] Access Policy (Access List)

۱-۲- امنیت شبکه و ارتباطات		
ردیف	عنوان	توضیحات
		لازم به ذکر است منظور از لاگ‌های سرویس IPS/IDS موارد زیر می‌باشد. • High Priority Attack • Medium Priority Attack • Low Priority Attack
۶	لاگ آنتی‌ویروس	لاگ پیکربندی و رخدادهای شناسایی شده توسط آنتی‌ویروس باید ثبت و نگهداری شود. در اینجا منظور از آنتی‌ویروس، هم سیستم مدیریت آنتی‌ویروس سیستم‌عامل‌ها و هم آنتی‌ویروس تجهیزات UTM می‌باشد.
۷	لاگ تجهیز Proxy	در صورت وجود سرویس Web Proxy تمامی‌ترافیک‌های عبوری از این سرویس می‌بایست ذخیره گردد. • Web Post Log • Web Get Log لازم به ذکر است لاگ مربوط به سرویس‌های webی که ترافیک آنها از Proxy عبور نمی‌کند می‌بایست توسط وب سرور مربوطه ذخیره گردد؛ در غیر اینصورت ذخیره سازی آنها در وب‌سرور ضروری نمی‌باشد.
۸	لاگ تجهیز WAF	تمامی‌لاگ‌های مربوط به موارد زیر باید در سرویس مدیریت لاگ مرکزی ذخیره گردد. • Web Firewall Log • Attack Log • Access Log • Audit Log • System Log • Traffic Log
۹	لاگ رویدادهای[۳] تجهیزات	اعمال تنظیمات زیر بر روی تمامی تجهیزات و سرویس‌های شبکه باید لاگ شود. • Login Fail/Login Success • Enable and Disable Service • Set Access List • Enable and Disable Network Port • Any Configuration system رویدادهایی که بر روی تجهیزات و سرویس‌های شبکه بدون اعمال نیروی انسانی انجام می‌گیرد مانند: • Enable/Disable Network Card • Traffic Flow • Port Block

[۳] Event Log

۱-۲- امنیت شبکه و ارتباطات		
ردیف	عنوان	توضیحات
		• RAM/CPU Alert • Power Information
۱۰	لاگ شبکه LAN	تمامی‌رویدادهای مربوط به ارتباطات سیستم کاربران با شبکه مانند : • MAC سیستم‌های متصل به سوییچ • شماره پورت سوییچ مربوط به هر کاربر • لاگ‌های مربوط به PortSecurity • لاگ‌های مربوط به حملاتی مانند ARP Spoofing • لاگ‌های Dynamic ARP inspection

۱-۳- سیستم‌عامل‌ها		
ردیف	عنوان	توضیحات
۱	لاگ حسابرسی امنیتی[۴]	تمامی رویدادهای امنیتی در سیستم‌عامل از جمله موارد ذیل، می‌بایست تولید و ذخیره گردد. • لاگ‌های مربوط به مدیریت حساب‌های کاربری • لاگ‌های مربوط به ورود و خروج کاربر (موفق و ناموفق) • لاگ‌های مربوط به دسترسی به objectهای مهم از قبیل ○ فایلهای مربوط به Application[۵] و تنظیمات آنها ○ فایل‌های پایگاه‌داده‌ها و تنظیمات آنها ○ رجیستری ویندوز • لاگ‌های مربوط به تغییر در خط‌مشی‌ها از قبیل ○ تغییر در خط‌مشی حقوق دسترسی کاربر ○ تغییر در خط‌مشی‌های فایروال سیستم‌عامل ○ تغییر در خط‌مشی‌های Audit • لاگ رویدادهای سیستم (مانند startup و shutdown) • نصب سرویس • فعال و یا غیرفعال شدن سرویس‌ها • Start، Stop و Restart شدن سرویس‌ها • لاگ مربوط به پاک شدن لاگ‌ها **نکته:** ❖ جهت اعمال این تنظیمات در سیستم‌عامل‌های لینوکسی نیاز به نصب بسته Audit می‌باشد. ❖ جهت اعمال این تنظیمات در سیستم‌عامل‌های ویندوزی از طریق تنظیمات Group Policy به صورت زیر اقدام شود: Windows Settings → Security Settings → Advanced Audit Policy Configuration → System Audit Policies

[۴] Security Audit Log

[۵] در خصوص فایل‌های مربوط به Application لازم است ابتدا دسترسی‌های لازم بر اساس اصل حداقل دسترسی بر روی این فایل‌ها تنظیم گردد و پس از آن، دسترسی‌های ناموفق کاربر Application و تمام دسترسی‌های سایر کاربران به این فایل‌ها لاگ شود.

۱-۴- نرم‌افزارها

ردیف	عنوان	توضیحات
۱	لاگ برنامه کاربردی	در سمت برنامه کاربردی حداقل بایستی رویدادهای ذیل تولید و ذخیره شود. • (تلاش برای) دسترسی به صفحات غیرمجاز (فاقد دسترسی لازم) توسط کاربران • تلاش برای ورودهای (موفق و ناموفق) کاربران • ایجاد، ویرایش و حذف کاربر (کاربر آنلاین / راهبر) • خروج کاربران از سامانه • تغییر کلمات عبور کاربران • خطاها و استثنائات • سایر رویدادهایی که باید در سامانه‌های معاملات برخط تولید و ذخیره شود در پیوست "راهنمای تولید و نگهداری لاگ و سوابق تراکنش‌ها در سامانه‌های معاملات برخط" ارائه شده است.
۲	پارامترهای لاگ	به ازای تمامی رویدادها حداقل بایستی موارد ذیل لاگ شوند. • نوع رویداد • شناسه کاربر جاری • آدرس IP کاربر جاری • زمان رویداد (تاریخ – ساعت) • وضعیت (موفق یا ناموفق بودن) • مقدار درهم سازی شده رکورد جاری که بدین صورت محاسبه می‌شود که مقدار درهم سازی شده رکورد قبلی با استفاده از الگوریتم SHA-256 با رکورد فعلی در کنار هم قرار گرفته (concatenate) و مجدداً با استفاده از الگوریتم SHA-256 درهم سازی شده است. ○ $Hash_{(n)} = SHA\text{-}256\ (Hash_{(n-1)} \mid n)$

۱-۵- سرویس‌ها		
ردیف	عنوان	توضیحات
۱	لاگ وب‌سرور (مانند IIS یا Apache)	حداقل موارد زیر باید در سطح وب‌سرور ثبت گردد: • تمام درخواست‌های دریافتی توسط وب‌سرور که باید حداقل فیلدهای زیر را پوشش دهد: ○ تاریخ ○ زمان ○ آدرس IP مبدأ ○ مقدار سرآیند X-Forwarded-For (لاگ‌ها باید به گونه‌ای باشد که آدرس IP کلاینت درخواست کننده در آن ثبت گردد.) ○ آدرس پورت مبدأ ○ آدرس IP مقصد ○ شماره پورت مقصد ○ متد HTTP ○ آدرس URL ○ پارامترهای Query String (در صورت استفاده از متد GET) ○ مقادیر POST Data (در صورت وجود) ○ مقدار سرآیند UserAgent ○ مقدار سرآیند Referer ○ کد Status پاسخ • لاگ Start، Stop و Restart شدن سایت‌ها
۲	لاگ سرویس‌های زیرساختی	در خصوص سرویس‌های زیر ساختی مانند DNS، DHCP، ESX،WSUS و هرگونه سرویس زیر ساختی دیگر می‌بایست حداقل لاگ‌های زیر ثبت و نگهداری شوند. • لاگ تغییر در پیکربندی سرویس‌های زیرساختی • لاگ Start، Stop و Restart شدن سرویس‌های زیرساختی

۱-۶- سرویس پایگاه‌داده‌ها

ردیف	عنوان	توضیحات
۱	لاگ پایگاه‌داده‌ها	در سطح پایگاه‌داده‌ها باید حداقل موارد زیر لاگ شوند: ۱. اضافه نمودن، تغییر، تعلیق و حذف User Accountها ۲. تغییر حقوق دسترسی در user Accountها ۳. تغییر مالکیت Objectها ۴. Login ها و Logout ها و تلاش های ناموفق Administrator Accountهـا، Application Credentialها و Credentialهای مورد ا ستفاده برای د ستر سی مستقیم به پایگاه‌داده ۵. تغییر رمزهای عبور ۶. تغییر در پیکربندی و یا خط مشی‌های امنیتی پایگاه‌داده، شامل: o Authentication modeها o Password Controlها o فعال یا غیرفعال شدن Remote Access o فعال یا غیرفعال شدن Auditing Database ۷. تغییر در پیکربندی Audit system و تلاش‌های انجام شـده برای حذف کردن، ویرایش کردن یا پاک نمودن Audit trailها یا Database logها. ۸. تغییر در Database Schema و بطور کلی دستورات DDLی اجرا شده ۹. دسـتورات DMLی اجرا شـده توسـط تمام User Accountها (به جز کاربر application) ۱۰. عملیات Backup و Restore پایگاه‌داده ۱۱. عملیات Startup و Shutdown پایگاه‌داده‌ها ۱۲. تلاش برای دسترسی به عملکردهای سیستم‌عامل از طریق پایگاه‌داده‌ها (اجرای دستورات، خواندن/ویرایش فایل‌ها و تنظیمات) ۱۳. در رکورد لاگ باید اطلاعات کافی برای تعیین اینکه چه رویدادهایی رخ داده و چه چیزی یا چه کسی باعث آن شده وجود داشته باشد: o نوع رویداد o زمان وقوع رویداد o User credentialهای مربوط به رویداد o برنامه‌ها و یا د ستورات ا ستفاده شده برای راه اندازی رویداد (Exact SQL) o نام جداولی که مورد دسترسی قرار گرفته است (در صورت کاربرد) o Host name یا آدرس IP کاربر مبدأ o وضعیت (موفق یا ناموفق بودن)

۱-۶- سرویس پایگاه‌داده‌ها		
ردیف	عنوان	توضیحات
		علاوه بر موارد ذکر شـــده، در مورد پایگاه‌داده‌های اوراکل و Microsoft SQL Sever از موارد زیر نیز باید لاگ گرفته شود: ○ **اوراکل:** ثبت دستورات listener: Service، Status، version، Stop ○ **MSSQL:** ثبت دستورات DBCC (Transact SQL)

۲- منابع

۱. سند الزامات امنیت اطلاعات بازار سرمایه

2. NIST 800-92_ Guide to Computer Security Log Management
3. SANS_data-center-physical-security-checklist-416
4. Database Security Logging and Monitoring Program
5. SANS Institute

سازمان بورس و اوراق بهادار
SECURITIES & EXCHANGE ORGANIZATION

مرکز نظارت بر امنیت اطلاعات بازار سرمایه (مکنا)

تهران، خیابان ملاصدرا، سازمان بورس و اوراق بهادار
Email: MAKNA@SEO.IR