پائیز ۱۳۹۹

مستند امن سازی – بستر ذخیره سازی اندیشه نگار پارس

امن سازی و سخت سازی چیست

با توجه به این‌که امروزه تهدیدهای متعددی متوجه دارایی‌ها و سرمایه‌های سازمانی هستند، برای هدفمند و قانونمند شدن فرآیند امن سازی، کارشناسان شرکت اندیشه نگار پارس ، با تکیه‌بر استانداردهای امن سازیCIS ، مستندات امن سازی ارائه‌شده توسط vendor هایی چونCisco ، Micrososftو... و توصیه‌ها و مستندات افتای ریاست جمهوری اقدام به امن سازی در هر بخش از تجهیزات شبکه و زیرساخت به‌عنوان مرجعی کامل و مفید که مورد تائید اغلب کارشناسان این حوزه می‌باشد، نموده‌اند.

امن سازی به فراهم نمودن و ارائه ابزارهای مختلف به‌منظور حفاظت از یک سیستم کامپیوتری اشاره دارد. به‌عبارت‌دیگر حفاظت در لایه‌های مختلفی ارائه‌شده و اغلب به‌عنوان دفاع در عمق شناخته می‌شود. منظور از حفاظت در لایه‌های مختلف، حفاظت در سطح میزبان، سطح برنامه کاربردی، سطح سیستم‌عامل، سطح کاربر، سطح فیزیکی و تمامی سطوح پایینی آن می‌باشد. هر یک از سطوح نیازمند روش منحصربه‌فردی از امن سازی می‌باشد.

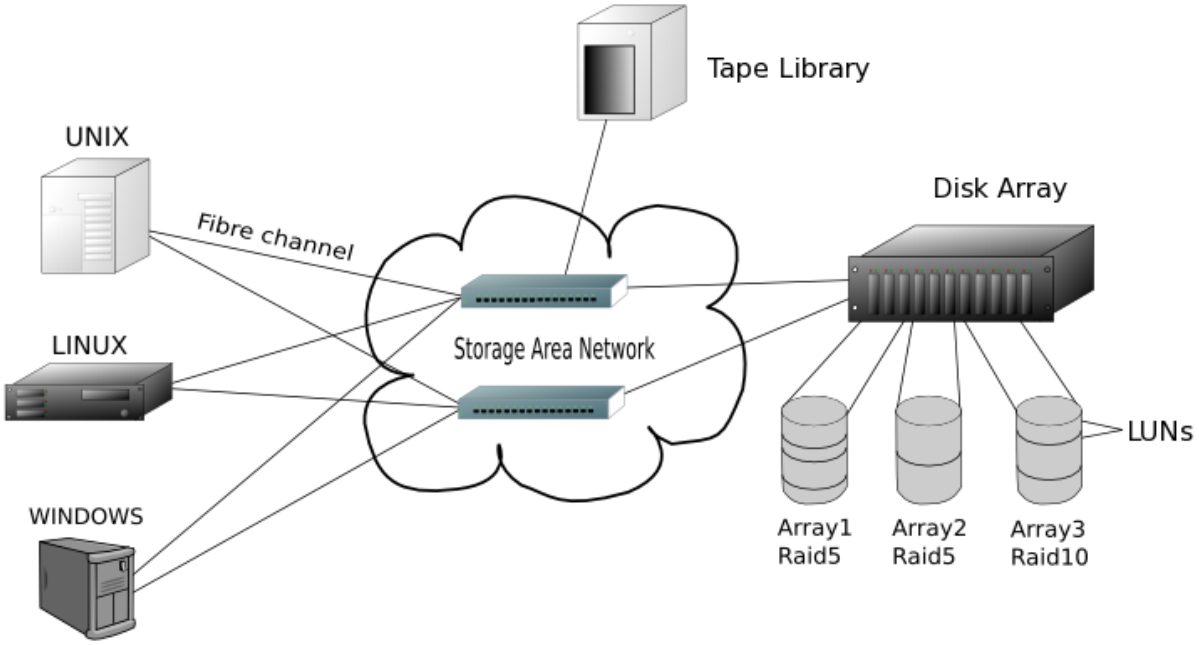
معرفی مستند

در مستند فوق ، اقدامات موردنیاز پیرامون امن سازی بستر ذخیره‌سازی که از طریق بهروش‌های شرکت‌های سازنده ، مقالات و مستندات افتای ریاست جمهوری و تجربه‌های موفق شرکت اندیشه نگار پارس می‌باشد بیان می‌گردد.

شرکت‌های مطرح ارائه‌کننده ذخیره‌ساز

- Hitachi
- HPE
- Dell EMC

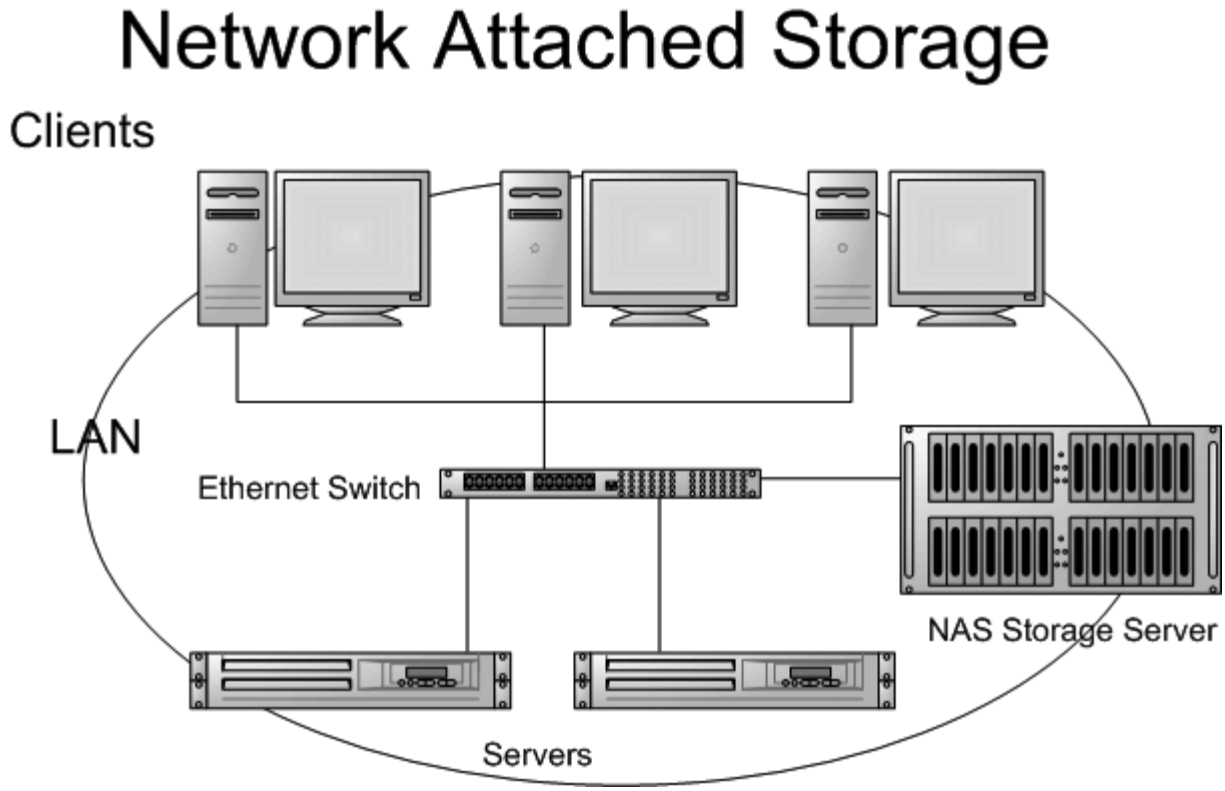
معرفی SAN



سرویس‌دهنده ذخیره‌سازی یا (Storage Server) دارای حجم زیادی از اطلاعات می‌باشد بطوریکه برای انتقال داده‌ها و ارائه خدمات مناسب نیاز به پهنای باند بالا می‌باشد . از مشخصات این نوع شبکه می‌توان داشتن بازده بالا برای انتقال حجم زیادی از داده‌ها، در دسترس بوده همیشگی سرویس‌دهنده‌ها حتی در فاصله‌های دور و طولانی و گستردگی زیاد در ابعاد شبکه‌های محلی یا شبکه‌های شهری یا جهانی می‌باشد .

SAN-Storage Area Networkیک شبکه بر پایه FC ، FCOE و... می‌باشد که امکان ذخیره‌سازی مشترک اطلاعات را بین تمامی اجزای شبکه ممکن می‌سازد. این ماشین که مجموعه‌ای از دیسک‌های ذخیره‌سازی اطلاعات است به کمکHBA و بهره گیری از SAN Switch با دیگر اجزای شبکه همچون سرور ها ارتباط برقرار می‌کند و اطلاعات را به‌صورت بلوکی Block-Level Access در اختیار دیگر اجزا شبکه قرار می‌دهد. به‌طورکلی چهار روش برای ایجاد ارتباط بین SAN و دیگر اجزا شبکه موجود است.

معرفی NAS



ابزارهایی که برای ذخیره‌سازی در شبکه به کار می‌رود بر اساس ساختارهای شبکه‌ای، زیرساخت‌های سخت‌افزاری، سیستم‌عامل، نرم‌افزارهای موردنیاز و کاربردی دسته بندی می‌شوند. یکی از انواع روش‌های ذخیره‌سازی شبکه Network Attached Storageیا NAS نامیده می‌شود.

در این روش ، تمامی هارد ها بر روی سخت‌افزار ذخیره‌ساز قرارگرفته و با استفاده از تکنولوژی موجود بر روی ذخیره‌ساز ، اقدام به اشتراک گزاری فضاهای ساخته‌شده بر بستر شبکه میگردد.

درواقع از طریق پروتکل TCP/IP به استوریج متصل می‌شویم و از آن سرویس می‌گیریم. این استوریج‌ها به‌سادگی، فضایی مرکزی، محلی و بسیار در دسترس را برای ذخیره‌سازی فایل‌ها و فولدرهای حیاتی برای هر سازمانی را فراهم می‌کنند.

دلایل امن سازی بستر ذخیره‌سازی

همواره یکی از ارزشمندترین دارایی های سازمانها ، اطلاعات آن‌ها می‌باشد که به همین دلیل ، همیشه درخطر از بین رفتن ، مخدوش شدن و یا سرقت آن‌ها هستند. با امن سازی بستر ذخیره‌ساز ، مخاطرات موجود در زمینه اطلاعات از بین رفته و دسترسی‌پذیری و حفاظت از آن‌ها برای سازمان فراهم می‌گردد.

- محافظت از اطلاعات در برابر نفوذها و حمله‌های خارج از سازمان
- محافظت از اطلاعات در برابر رخنه‌های امنیتی داخلی و خارجی
- محافظت از محتوی اطلاعات در برابر ایجاد تغییرات

از مزایای امن سازی بستر ذخیره‌ساز می‌باشد.

لایه‌های بستر ذخیره‌سازی و مخاطرات آن‌ها

همان‌گونه که در مستند فوق به آن اشاره شد ، لایه ذخیره‌سازی بر اساس سخت‌افزاری به ۲ دسته SAN و NAS تقسیم می‌گردد که هر دو آن‌ها به‌صورت مشترک از ۴ لایه جهت ارائه سرویس های خود استفاده می کنند.

۱- تجهیزات موجود در شبکه
۲- دسترسی به اطلاعات
۳- ارتباطات
۴- مدیریت

بررسی لایه‌های NAS و مخاطرات آن

- لایه شماره ۱ ، تجهیزات موجود در شبکه

ذخیره ساز های NAS ، سرویس های خود را بر اساس به اشتراک گزاری اطلاعات در شبکه TCP/IP ارائه می دهند که این روش دارای مخاطرات ذیل می‌باشد

  - دسترسی های ناخواسته به دلیل وجود گذرواژه ها ی ضعیف و یا استفاده از گذرواژه ها ی پیش فرض در ذخیره‌ساز یکی از دلایل بروز رخنه‌های امنیتی در ذخیره‌ساز می‌باشد ، از طرفی ایجاد امنیت تنها به واسطه کلمه کاربری و گذرواژه نیز یکی دیگر از حفره های امنیتی در ذخیره سازهای NAS است.
  - نفوذپذیری‌های سیستم عامل در ذخیره سازهای NAS نیز یکی دیگر از حفره های امنیتی رایج می‌باشد که با استفاده از حفره های متعددی همچون Certificate های قدیمی و یا DNS های Buffer شده امکان نفوذ به ذخیره‌ساز میسر می‌شود که تعدادی از این حفره ها با اعمال بسته های امنیتی از بین خواهند رفت.

- لایه شماره ۲ ، دسترسی به اطلاعات

ذخیره اطلاعات در ذخیره سازهای NAS با استفاده از تکنولوژی CIFS ، SMB و NFS می‌باشد که دسترسی ناخواسته و رخنه‌های امنیتی به آن‌ها از طرق ذیل صورت می‌گیرد.

  - استفاده از کلمات کاربری یکسان و گذرواژه ها ی ساده برای دسترسی به اطلاعات به اشتراک قرار داده شده
  - استفاده از دسترسی های کاربری بر محتوی CIFS با استفاده از متد غیر امن LanMan
  - تبادل در NFS بر پایه Clear Text که امکان Sniff کردن تبادل اطلاعات را فراهم می کند.
  - ایجاد اشتراک برای سرویس های NFS به‌صورت یکپارچه و عمومی
  - از دست رفتن اطلاعات و یکپارچگی آن‌ها به دلیل ویروس ها ، بد افزارها ، Worm ها و حمله‌های DoS

- لایه شماره ۳ ، ارتباطات

همان‌گونه که اشاره شد ، سرویس های NAS بر پایه IP می باشند و مخاطراتی همچون حملات DoS ، Session Hijacking و IP-spoofing در انتظار این گونه از سرویس ها می‌باشد.

- لایه شماره ۴ ، مدیریت

مدیریت ذخیره سازهای NAS ، شامل نظارت و پیکر بندی تجهیز ، ایجاد سرویس و اختصاص آن‌ها به سرویس گیرندگان می‌باشد.

  - رخنه‌های امنیتی به واسطه Sniff کردن گذرواژه ها بر اساس ارتباطات بر پایه Text همانند Telnet و HTTP
  - رخنه‌های امنیتی بر اساس استفاده از گذرواژه ها ی ضعیف و یا پیش فرض
  - ایجاد دسترسی های موقت و یا در اختیار قرار دادن دسترسی های Admin به کاربران

بررسی لایه‌های SAN و مخاطرات آن

- لایه شماره ۱ ، تجهیزات موجود در شبکه

تمامی سرور های موجود در شبکه SAN به اطلاعات موجود بر روی ذخیره‌ساز ها دسترسی دارند که مخاطرات ذیل در زمینه اطلاعات برای سازمان ایجاد می‌گردد

  - دسترسی های ناخواسته به واسطه استفاده از گذرواژه ها ی سست و غیر امن در سیستم عامل های موجود در شبکه SAN
  - حفره ها و رخنه‌های امنیتی بر اساس سرویس ها و نرم افزار های Publish شده بر روی سرور های موجود در شبکه SAN که شامل سرویس های DNS ، Gateway و نرم افزار هایی مانند Oracle ، Exchange و SAP و ... می‌باشد.

- لایه شماره ۲ ، دسترسی به اطلاعات

نگهداری اطلاعات در ذخیره ساز های SAN ، به‌صورت مستقیم و بلاک می‌باشد که در این حالت ، سرور ها ، سرویس ها و نرم افزار ها به‌صورت مستقیم قابلیت فعالیت بر روی فضای ایجاد شده بر روی ذخیره‌ساز را دارا می باشند.

  - دسترسی ناخواسته بر اساس استفاده از گذرواژه ها ی سست و غیر استاندارد
  - دسترسی ناخواسته به اطلاعات از طریق عدم رعایت امنیت اطلاعات
  - از بین رفتن اطلاعات به واسطه ویروس ها ، Worm ها و حملات DoS
  - سرقت اطلاعات به واسطه دسترسی به سرور های موجود در شبکه SAN

- لایه شماره ۳ ، ارتباطات

ارتباطات در ذخیره ساز های SAN عموماً به واسطه استفاده از HBA در سرور ها و SAN Switch ها در شبکه برقرار می‌شود که بستر این نوع ارتباط عموماً Fiber Channel می‌باشد. استفاده از این روش به‌صورت معمول امن تر از روش های دیگر است ولی جهت دستیابی به بالاترین میزان امنیت ، نیاز به استفاده از راهکارهای مختلفی می‌باشد.

  - تمامی تجهیزات در بستر SAN جهت برقراری ارتباط با یکدیگر از World Wide Name (WWN) استفاده میکنند ، یکی از راه های دستیابی به اطلاعات در زیرساخت SAN ، Spoof کردن WWN و استفاده از آن‌ها می‌باشد ، از طرفی استفاده از Snoop و به واسطه آن سرقت اطلاعات نیز یکی دیگر از روش های ایجاد خلل و رخنه در اطلاعات سازمان می‌باشد.
  - ها
  - عدم پیکربندی مناسب SAN Switch ها

- دسترسی به اطلاعات به وسیله Man in The Middle و سرقت اطلاعات
- استفاده از پیکربندی‌های پیش فرض در ذخیره‌ساز

- لایه شماره ۴ ، مدیریت
  - رخنه‌های امنیتی به واسطه Sniff کردن گذر واژه ها بر اساس ارتباطات بر پایه Text همانند Telnet و HTTP
  - رخنه‌های امنیتی بر اساس استفاده از گذرواژه ها ی ضعیف و یا پیش فرض
  - ایجاد دسترسی های موقت و یا در اختیار قرار دادن دسترسی های Admin به کاربران

امن سازی NAS

اقدامات ذیل جهت امن سازی در ذخیره ساز های NAS انجام می‌گیرد

- لایه شماره ۱ ، تجهیزات موجود در شبکه NAS
  - استفاده از Two-Factor Authentication مانند Biometric ها ، Token ها یا SSL جهت مدیریت دسترسی
  - دسترسی توسط (Access Control List (ACL جهت ایجاد دسترسی های مختلف
  - استفاده از گذرواژه ها ی قوی و با حداکثر کاراکتر های قابل استفاده و تعویض دوره ای آن‌ها
  - تغییر گذرواژه ها ی پیش فرض
  - نظارت بر سیستم عامل ها و سرویس های آن‌ها
  - نظارت بر پیغام های خطای ذخیره‌ساز
  - استفاده از بروز رسانی ها و بسته های امنیتی مربوط به ذخیره‌ساز
  - استفاده از ابزارهای Scanner مانند Nessus ، SAINT و ...
  - ایمن سازی سیستم عامل های موجود در بستر NAS
- لایه شماره ۲ ، دسترسی به اطلاعات
  - دسته بندی اطلاعات بر اساس سیاست های سازمان
  - ایجاد دسترسی های مختلف بر اساس دسته بندی های انجام شده
  - رمزنگاری اطلاعات به واسطه استفاده از ابزارهای موجود
  - رمزنگاری ذخیره‌ساز به واسطه استفاده از لایسنس های مربوطه
  - استفاده از CIFS NTLMv2 جهت ایجاد دسترسی به کاربران
  - استفاده از IP Address مربوط به سرویس گیرندگان جهت اختصاص فضای موجود بر روی ذخیره‌ساز NAS
  - محافظت از اطلاعات با استفاده از ابزارهای ضدویروس و Malicious
- لایه شماره ۳ ، ارتباطات

امن سازی در بستر NAS ، همانند امن سازی بستر شبکه می‌باشد که به تعدادی از آن‌ها در این مستند اشاره می‌گردد

  - استفاده از تجهیزات Firewall در شبکه NAS
  - استفاده از VLAN جهت جداسازی ترافیک NAS
  - نظارت بر ترافیک موجود

- لایه شماره ۴ ، مدیریت
  - غیرفعال سازی Telnet و HTTP
  - فعال سازی SSH و HTTPS
  - ایجاد کاربران مختلف با سطوح دسترسی مختلف
  - استفاده از مکانیزم قوی جهت اعتبار سنجی کاربران همانند Two-Factor ، Token و Biometric
  - استفاده از گذرواژه ها ی مستحکم و تغییر گذرواژه ها ی پیش فرض
  - تغییر گذرواژه ها به‌صورت زمان بندی شده
  - استفاده از Access Control List (ACL) برای ایجاد سطوح مختلف کاربری
  - ایجاد سطوح مختلف دسترسی برای سرور ها و سرویس گیرندگان مختلف

امن سازی SAN

اقدامات ذیل جهت امن سازی در ذخیره ساز های SAN انجام می‌گیرد

- لایه شماره ۱ ، تجهیزات
  - استفاده از کلیدهای عمومی و خصوصی در سیستم عامل های موجود در شبکه SAN
  - استفاده از Two-Factor Authentication ، Token و Biometric جهت اعتبار سنجی کاربران
  - استفاده از Access Control List (ACL)
  - استفاده گذرواژه ها ی قوی و تغییر گذرواژه ها ی پیش فرض
  - تغییر گذرواژه ها ی به‌صورت زمان بندی شده
  - نظارت بر سیستم عامل های موجود با استفاده از ابزارهای مربوطه
  - استفاده از بروز رسانی ها و بسته های امنیتی ارائه شده توسط شرکت سازنده
  - استفاده از Scanner های موجود مانند Nessus ، SAINT و ....
  - غیرفعال کردن سرویس های غیر ضروری بر روی سیستم عامل های موجود
  - استفاده از ابزارهایی مانند Tripwire جهت افزایش امنیت سرور ها

لایه شماره ۲ ، دسترسی به اطلاعات

  - دسته بندی اطلاعات بر اساس سیاست های سازمان
  - ایجاد کاربران مختلف و دسترسی آن‌ها بر اساس دسته بندی اطلاعات
  - استفاده از ابزار رمزنگاری بر روی سرور ها و سیستم عامل های مختلف
  - استفاده از قابلیت رمزنگاری بر روی هارد دیسک های ذخیره‌ساز به واسطه لایسنس های موجود
  - استفاده از CIFS NTLMv2 جهت ایجاد دسترسی های مختلف
  - ایجاد امنیت به واسطه استفاده از LUN Masking
  - ایجاد امنیت به واسطه استفاده از Logical Unit Number
  - اختصاص فضای موردنیاز بر اساس WWN و Logical Unit Number
  - نظارت بر سرور ها و نرم افزارهای آن‌ها
  - استفاده از ضد ویروس ها بر روی سیستم عامل های موجود

لایه شماره ۳ ، ارتباطات

  - ایجاد Zoning جهت جداسازی و مدیریت ارتباطات میان ذخیره‌ساز SAN و سرور ها

- استفاده از روش Port و WWN در ایجاد Zoning جهت بالا بردن امنیت
- استفاده از قابلیت Port Binding جهت جلوگیری از Spoof شدن WWN ها
- استفاده از بهروش های شرکت سازنده
- جداسازی شبکه مدیریتی موجود از شبکه اصلی سازمان
- استفاده از Firewall و IDS جهت امنیت شبکه SAN
- نظارت بر ترافیک موجود بر روی شبکه

لایه شماره ۴ – مدیریت

- غیرفعال سازی Telnet و HTTP
- فعال سازی SSH و HTTPS
- ایجاد کاربران مختلف با سطوح دسترسی مختلف
- استفاده از Two-Factor Authentication ، Token یا Biometric جهت اعتبار سنجی کاربران
- استفاده از گذرواژه ها ی قدرتمند و تغییر آن‌ها به‌صورت زمان بندی شده
- تغییر گذرواژه ها ی پیش فرض
- مدیریت متمرکز ذخیره‌ساز ها بر روی یک میزبان

منابع و مآخذ

- بهروش‌های شرکت سازنده
- توصیه ها و مستندات ارائه شده توسط افتا ریاست جمهوری
- تجربه های موفق قبلی