امنیت اطلاعات شبکه و بانک های اطلاعاتی

ارائه کننده: امیر حسین نریمانی موسسه حسابرسی هوشیار

بخش دوم

رویکردی به حسابرسی امنیت شبکه
(تلخیصی از مقالات ISACA)

امروزه ما در دنیای متصل بهم زندگی می کنیم، ارتباطات یکی از الزامات اساسی کلیه سیستمهاست افزایش یکپارچکی سیستمها، نیاز وقفه ناپذیر سازمان ها و معاملات تجاری آن ها را به استقرار سریع و قابل اعتماد ارتباطات در گستره جهانی می طلبد.

سیستمهای اطلاعاتی به برقراری ارتباط با استفاده کنندگان ، فروشندگان ، مشتریان و شرکاء (بدون توجه به فعالیت مکانی آنها) نیاز دارد تقریباً هر چیزی به هر چیز دیگری متصل است.

تمام اینها ما را به این نتیجه می رساند که اینکه سیستمی در داخل یک جعبه یا فضای بسته قرار دارد برای حصول اطمینان از امینت آن کافی نیست، واقعیت این است که تقریباً هر کامپیوتر درجهان می تواند (هم اکنون تقریباً در اغلب موارد هست) از طریق اینترنت با هر کامپیوتر دیگری ارتباط برقرار کند.

خوشبختانه، انبوهی از راه حل های فنی، که بسیاری از آنها استاندارد شده اند بیشتر شبکه ها و سیستمها را مجزا و محافظت شده نگه می دارد.

بنابراین بیائید ببینیم که چگونه نگرش حسابرسی شبکه ها و حصول اطمینان از این که آنها ایمنی هستند را شکل می دهیم.

همچنین خوب است در این مرحله تاکید کنیم که کلاً در چارچوب های حسابرسی سیستمهای اطلاعاتی، حسابرسی شبکه ها یکی از قطعات پازل است به همراه سایر قطعات قابل ذکر حسابرسی نرم افزارهای کاربردی، حسابرسی سیستم عامل ها و بانک های اطلاعاتی، حسابرسی امنیت فیزیکی و محیطی، حسابرسی تداوم فعالیت تجاری (که به اینها پیشتر نیز در اصول اساسی حسابرسی سیستمهای اطلاعاتی پرداخته شده است)

برای کسب یک اطمینان جامع درباره سیستمها تخمین و ارزیابی کلیه اجزا و قطعات اهیت دارد. در این بحث ما بر حسابرسی امنیت شبکه متمرکز می شویم.

یک شبکه می تواند به سادگی یک شبکه محلی، از اتصال چند کامپیوتر در یک اتاق یا ساختمان یا چیزی که کامپیوترهای کارخانجات و دفاتر را در تعدادی از شهرها یا حتی کشورها بهم مرتبط می کند؛ باشد. یک شبکه همچنین می تواند به سایر شبکه ها نظیر شبکه های مشتریان و فروشندگان یا یک شبکه عمومی نظیر اینترنت متصل باشد.

نقاط آسیب پذیر

آسیب پذیری های اصلی مرتبط با یک شبکه می تواند به ۳ دسته طبقه بندی شوند:

- دستبرد
- در دسترس بودن
- نقاط دسترسی و ورود

۱. دستبرد: اطلاعاتی که در شبکه منتقل می شود از برخی از واسطه ها عبور می کند که از یک حمل کننده و سایر تجهیزاتی که اغلب به صورت فیزیکی در اختیار اشخاص ثالث می باشند تشکیل می شود.

این اطلاعات می توانند مورد دستبرد واقع شوند و در این صورت، خطر افشای نامطلوب می توانند در مورد دستبرد واقع شوند و در این صورت، خطر افشای نامطلوب آنها وجود دارد، سرقت اطلاعات یا افشای اطلاعات دزیده شده نتیجتاً زیان از دست دادن جامعیت اطلاعاتی و زیان مادی را در بر خواهد داشت.

۲. در دسترس بودن: هر چه شبکه ها، شاخه های بیشتری پیدا می کنند کاربران بیشتر و بیشتری از راه دور به برنامه های کاربردی آنها دسترسی پیدا می کنند از صدها و هزاران مایل دورتر . اگر ارتباطات شبکه ای در هم شکسته شود یا به هر دلیلی از دسترس خارج شود، موجب قطع جدی فعالیت تجاری می گردد و نتیجاً خساراتی به بار می آورد.

۳. نقاط دسترسی و ورود: یک شبکه، یک سیستم کامپیوتری را ورای یک جعبه به تمام جهان گسترش می دهد. شبکه امکان گسترش سیستم به کاربران ورای مرزهای جغرافیایی را فراهم آورده، موجب می شود راحتی و اثربخشی که در غیراینصورت ممکن نبود فراهم شود. در مقابل، همان شبکه امکان دسترسی به سیستم از هر جای دنیا را نیز فراهم می آورد. تنها یک نقطه ضعف در شبکه می تواند تمام دارایی های اطلاعاتی موجود در شبکه در معرض نفوذ قرار دهد. شبکه می تواند نقاط ورود بسیاری برای نفوذکنندگان، سارقان و ویروس های شبه-کد مخرب، کرم ها و اسب های تروژان فراهم کند. توانایی شبکه برای فراهم آوردن امکان دسترسی به یک سیستم از هرجا، جدی ترین آسیب پذیری یک شبکه است. با آگاهی از این حقیقت که یکی از مزایای عمده شبکه امکان فراهم آمدن دسترسی به سیستم از هرجاست، وظیفه کنونی کشف چگونگی به کارگیری بهترین کنترل ها حول این دسترسی است.

خوشبختانه، مسئله به آن دشواری که به نظر می رسد نیست. راه حل های کنترل دسترسی برای شبکه به اشکال مختلف و در محصولات مختلف وجود دارند که می توانند به شکلی موفقیت آمیز آزموده و به کار گرفته شوند.

کنترل ها

پس از شناسایی نقاط آسیب پذیر، اجازه دهید یک به یک نگاهی به کنترل های ممکن بیاندازیم.

۱. دستبرد- کنترل های دسترسی فیزیکی مناسب در مراکز داده و دفاتر و امنیت فیزیکی در تجهیزات ارتباطات می‌توانند نقشی بازدارنده داشته باشند. به عنوان گام اول، حسابرس می تواند امنیت فیزیکی، شامل تمام نقاطی که اتصالات ارتباطات در آن ها به پایان می رسند و نقاطی که سیم کشی ها و منابع توزیع شبکه در آن ها قرار گرفته اند، را ارزیابی کند. اثربخش ترین کنترل برای پیشگیری رمزگذاری است. وقتی داده ها رمزگزاری شوند، حتی اگر سرقت شدند، افشا یا اصلاح امکان پذیر نخواهد بود مگر اینکه داده های درهم رمزگشایی شوند. امروز، شیوه های زیادی برای رمزگذاری و ترکیب های متنوعی از انواع استفاده آن وجود دارد. رمزگذاری می تواند یا با یک برنامه کاربردی یا در سطح ارتباطات با استفاده از ابزاری نظیر مسیریاب اعمال شود. یک شبکه مجازی خصوصی (VPN) مثالی از استفاده رمزگذاری برای ایجاد کانالی برای انتقال داده به شکلی ایمن در یک شبکه عمومی یا مشترک است. استفاده از اسناد دیجیتال و امضاهای دیجیتال مثالی دیگر است.

۲. در دسترس بودن: کنترل برای حصول اطمینان از در دسترس بودن و قابل اتکا بودن یک شبکه از طریق معماری و پایشِ خوب و مناسب شبکه است. طراحی شبکه باید اطمینان دهد که بین هر منبع و نقطه دسترسی مسیرهای فراوان وجود دارد و مسیریابی اتوماتیک برای انتقال ترافیک به مسیر مناسب موجود، بدون اتلاف داده یا زمان، وجود دارد. هر جزء شبکه باید تحمل خطا را داشته باشد یا با فراوانی مناسب ساخته شده باشد. شبکه های پیچیده و گسترده باید پایش و مدیریت شوند. این امر معمولاً با استفاده از نرم افزار مدیریت شبکه انجام می شود. استقرار مرکز عملیات شبکه (NOC) با ابزار نرم افزاری و میز خدماتی که ۲۴ ساعته و در ۷ روز هفته کارمندی برای آن تامین شده این قابلیت را تامین می کند. چنین ابزاری داده ها را برای مدیریت ظرفیت فراهم می کنند. این ابزار، همچنین، اطمینان می دهند که شبکه ها پهنای باند کافی برای حرکت داده ها، بدون قرار گرفتن در تنگنا و با سرعت مورد نیاز کاربر و برنامه های کاربردی، فراهم می کنند. مرور حسابرسی سیستم های اطلاعاتی (IS) باید تمام این ابعاد را در برگیرد.

۳. اکسس پوینت ها: اکثر کنترل ها در یک شبکه در نقاطی اعمال می شوند که شبکه با شبکه های خارجی/برون‌سازمانی ارتباط می‌یابد. این کنترل ها به دنبال این هستند که نوع ترافیکی که می تواند وارد یا خارج شود و، همچنین، مبدا و مقصد ترافیک را محدود کند. برای مثال، برای تامین دسترسی به وب سروری که درون شبکه قرار دارد برای مشتریانی که در سراسر جهان قرار دارند و قصد ثبت سفارش دارند، شبکه باید تنها نوع مشخصی از ترافیک را قبول کند (HTTP) و نه نوع ترافیکی را که قصد نفوذ به سرور را دارد (telnet). در موقعیتی دیگر، جایی که یک شریک یا فروشنده، برای مثال، خدمات توسعه یا حفظ و نگهداری سیستم را از طریق یک شبکه اختصاصی (dedicated network) از مکانی ثابت تامین می کند، شبکه باید تنها ترافیک آمده از آن سیستم ها با آدرس مشخص را مجاز بداند. چنین کنترل هایی از طریق پیکربندی هایی مناسب از پایگاه قوانین در فایروال و/یا از طریق لیست های کنترل دسترسی در مسیریاب ها اجرا می‌شوند. نرم افزارهای آنتی ویروس و سیستم های کشف نفوذ (IDS) می توانند ویروس ها و سایر کدهای مخرب در نقاط ورودی شناسایی کنند و اقدامات کشف کننده و اصلاحی را پیش بگیرند.

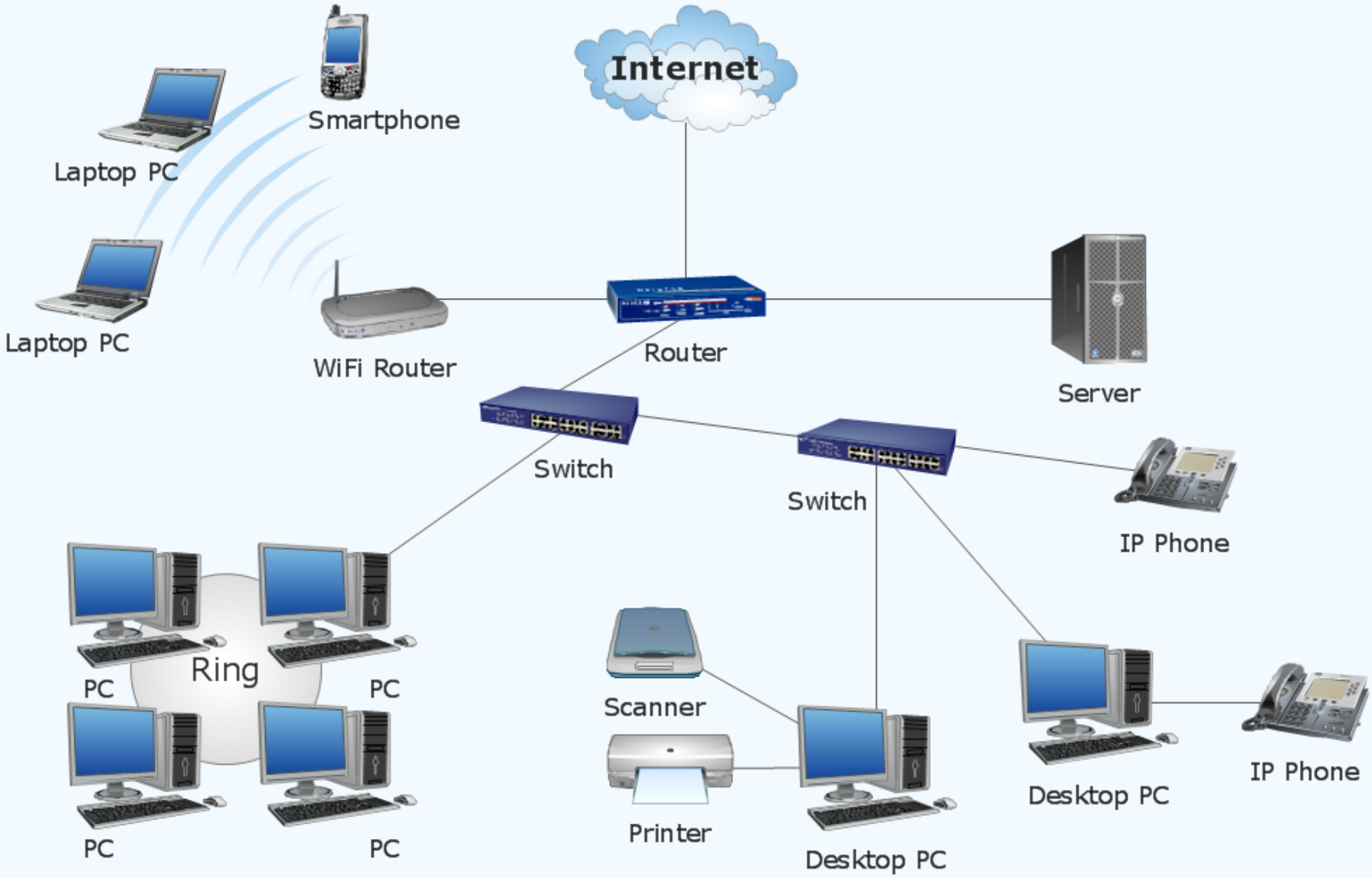
استقرار و جاسازی استراتژیک چنین ابزار و نرم افزارهای کنترل در هاست ها و بخش های حیاتی، علاوه بر دروازه ها، می‌تواند امنیت را، براساس الزامات تعیین شده در ارزیابی ریسک، بیشتر ارتقا دهد. سیستم های عاملِ سرورها، در جایی که منابع حیاتی نگهداری می شوند، باید سخت شوند (harden) و کنترل های دسترسی در برنامه های کاربردی نیز باید کنترل شده و به شکلی ایمن حفظ شوند.

حسابرسی امنیت شبکه

حسابرس باید اطلاعات و درک و شناخت مشخصی از شبکه ای که تحت بررسی وی است بدست آورد تا در راستای حسابرسی امنیت شبکه پیش رود. این جمع آوری اطلاعات باید طبق گام های زیر و به همین ترتیب صورت گیرد.

شبکه چیست؟- گام اول تعیین گستره شبکه است. این گام عموماً از طریق بررسی دایاگرام/طرح و نمایه شبکه صورت می گیرد. دایاگرام شبکه، اساساً، نقشه ای است که تمام مسیرهای موجود در شبکه را نشان می دهد. عامل کلیدی درباره دایاگرام که حسابرس باید نگرانش باشد دقت آن است. شبکه های بزرگ مدام، به همراه نیازهای کسب و کار، در حال تغییر و ارتقا هستند و دایاگرامی که به روز نباشد بلااستفاده است. حسابرس سیستم های اطلاعاتی باید اطمینان حاصل کند که چه فرایندهایی در سازمان وجود دارند تا دایاگرام شبکه را به دقت به روز کرده و به روز نگه دارد. استفاده از ابزار نرم افزاری برای تولید دایاگرام درجه ای از دقت را تضمین می کند.

در هر شبکه، جاهایی هستند که تمرکز منابع در آن ها بیشتر است، از قبیل مرکز داده که سرورهای ERP، سرورهای میل و غیره در آن ها هاست شده اند و بسیاری نقاط از قبیل کارخانه های تولیدی، دفاتر فروش و غیره که این منابع از آن ها قابل دسترس اند. در حالی که شبکه های کوچک تر ممکن است تنها یک نقطه با این شرایط داشته باشند، شبکه های پیچیده ممکن است نقاط هاست فراوانی داشته باشند که منابع حیاتی در آن ها واقع شده اند. دایاگرام شبکه، همچنین، می تواند دروندادی مرتبط با انواع ابزار و پروتکل های استفاده شده در شبکه ارائه کند. دایاگرام شبکه و جزئیات آن مهمترین درونداد را برای حسابرس فراهم می کنند و حسابرس باید به طور مداوم، طی حسابرسی، به آن ها مراجعه کند.


Internet
Smartphone
Laptop PC
Laptop PC
WiFi Router
Router
Server
Switch
Switch
IP Phone
Ring
PC
PC
PC
PC
Scanner
Printer
Desktop PC
Desktop PC
IP Phone

دارایی های اطلاعاتی حیاتی در شبکه چه چیزهایی هستند؟- اصل بنیادی امنیت اطلاعات و حسابرسی این است که محافظت با ریسک های مرتبط با دارایی ها، آنگونه که در ارزیابی معنایی ریسک تعیین شده است، مرتبط است. حسابرس باید شناخت خوبی از دارایی ها، سیستم ها و خدمات حیاتی که باید ایمن نگاه داشته شوند داشته باشد. معمولاً، شرکت ها خواستار حفظ امنیت سیستم های سازمانی هستند، شامل ERP ها، سرورهای میل و سایر برنامه های کاربردی داخلی، ، وب سرورها هایی که میزبان برنامه های کاربردی ای هستند که در دسترس مشتریان و فروشندگان قرار دارند و شبکه و اجزای آن. در این زمینه، امنیت و مکانیسم دسترسی احاطه کننده برنامه های کاربردی و سرورها (شامل سیستم عامل و پایگاه داده) نیز باید سخت گیرانه باشد.

چه کسی دسترسی دارد؟ گام بعدی تعیین افرادی است که دسترسی به سیستم های روی شبکه دارند و همچنین چگونگی این دسترسی نیز اهمیت دارد. آیا سیستم فقط در دسترس کارمندان است؟ آیا مشتریان و فروشندگان نیز باید به سیستم دسترسی داشته باشند؟ آیا کارمندان از خارج از دفتر نیز به سیستم دسترسی دارند؟ آیا مشتریان تنها به وب سرور، از طریق اینترنت، دسترسی دارند یا از راه دور امکان ورود (login) به سیستم های سازمانی را دارند؟ پاسخ به این پرسش ها می تواند تاثیر عمده ای بر امنیت داشته باشد.

ارتباطات با شبکه های خارجی چگونه اند؟- با وجود اینکه این بخش در حقیقت بخشی از گام یک است و با مطالعه دایاگرام شبکه تعیین می شود، گامی مهم است که باید جداگانه با آن برخورد شود. امروزه، هر شبکه، حداقل، از طریق یک تامین کننده خدمات اینترنتی به اینترنت متصل است. دلیل اولیه برای وصل شدن به اینترنت فراهم آوردن امکان دریافت و ارسال میل و مرور و جستجو توسط کارمندان است. سازمان ها ممکن است دلایل دیگری برای اتصال به اینترنت داشته باشند، از قبیل وب سایت های تجارت الکترونیک که فروشندگان، مشتریان و شرکای شرکت با هم همکاری کرده، سفارشات خود را ثبت کرده یا اطلاعات دیگری را تبادل می کنند. اتصالات اختصاصی به شبکه های سایر شرکا نیز ممکن است وجود داشته باشند. دروازه هایی که هر یک از این ارتباطات از طریق آن ها برقرار می شوند نقاط ورودی بالقوه ای برای ورود دنیای خارجی/برون سازمانی است.

حسابرس در این نقطه می تواند نسبت به شناسایی علامت ها میان شبکه داخلی و شبکه خارجی/برون سازمانی اقدام کند. براساس گام دو، حسابرس سیستم های اطلاعاتی باید از پیش آگاهی داشته باشد که کدام سیستم ها فقط در دسترس کاربران داخلی هستند، کدام سیستم ها در دسترس دنیای برون سازمانی یا اینترنت قرار دارند و کدام سیستم ها تنها در دسترس کاربران برون سازمانی هستند. چنین دسته بندی ای به حسابرس کمک می کند

ارزیابی مکانیسم محافظت

گام اول بررسی دروازه ها به عنوان نقاط بالقوه ای است که امکان ورود از آن ها، با استفاده از مجوز یا به شکل مخرب وجود دارد. کنترل ها از طریق معماری ایمن و درست طراحی شدهٔ شبکه، انتخاب پروتکل ها و مکانیسم های رمزگذاری، انتخاب و پیکربندی ابزار شبکه از قبیل مسیریاب ها و سایر اقدامات دفاعی از قبیل فایروال ها، آنتی ویروس ها و سیستم های تشخیص نفوذ اجرا می شوند.

ارزیابی هر یک از این موارد مستلزم دانش تخصصی است و حسابرس باید اطمینان حاصل کند که تیم حسابرسی کارشناسانی را نیز در اختیار دارد که از دانش خاص مربوط به پروتکل ها، ابزار شبکه و نرم افزارهای به کار گرفته شده در شبکه نیز برخوردارند. تمرکز این مقاله این بوده است که طرحی اولیه از رویکردی نسبت به حسابرسی امنیت شبکه ارائه کند و قصد ارائه رهنمودی فنی و مختص حسابرسی نداشته است.

کتاب ها و جستجوها در اینترنت می تواند چک لیست هایی مربوط به ارزیابی و پیکربندی رایج ترین ابزار و محصولات امنیتی را بدست دهد. محصولات امنیتی مدام در حال ارتقا و بهبود اند. بسیاری از آن ها قابلیت هایی چندگانه را توسعه داده و شکل محصولات هیبریدی/پیوندی/دورگه را به خود می گیرند که می توانند امکانات فایروال، آنتی ویروس، سیتسم های تشخیص نفوذ و اصلاحات را یکجا فراهم آورند. هنگامی که حسابرسی سیستم های اطلاعاتی از نیازها، نقش و محدودیت های هر یک از این موارد آگاه باشد، دانش تخصصی مرتبط با آن ها می توان کسب یا استخدام کرد.

ضروری است که حسابرس سیستم های اطلاعاتی فرایندهای مرتبط با مدیریت تمام این اجزای امنیتی را ارزیابی کند. پیکربندی ها باید از طریق تغییر فرایندهای مدیریتی حفظ شوند، تاریخچه عمکردها (Log) باید موشکافی شوند و در صورت لزوم اقدام لازم صورت پذیرد، رویدادها باید مدیریت شوند و یادگیری ها و اقدامات پیشگیرانه باید مستند شوند. امنیت خوب تنها با سرمایه گذاری در ابزار و نرم افزارهای پیچیده و گرانقیمت بدست نمی آید، بلکه مستلزم وجود یک حسابرسی سیستم های اطلاعاتی توانمند است که مدیریت سیستماتیک ابزار امنیتی را از طریق فرایندهای درست تعریف شده بررسی کند.

پایان