

ارزیابی امنیت اطلاعات

-

نگاهی تحلیلی بر معیارهای سنجش امنیت

نویسندگان:

ابوذر عرب‌سرخی

فریبا غفاری

رضا کلانتری



انتشارات آوای قلم

پیشگفتار

اگر به دنیای اطراف خود بنگریم، شاید استفاده از ابزارهای ارتباطات و فناوری اطلاعات امری بسیار پایه‌ای در زندگی امروز به نظر برسد. در این شرایط دیگر نمی‌توانیم تصور کنیم که اگر برنامه‌های کاربردی امروزی و یا بسیاری از ابزارها نبودند، زندگی بشر در عصر ارتباطات چه شکلی به خود می‌گرفت. فناوری اطلاعات و ارتباطات، همان‌طور که بخشی جدایی‌ناپذیر از زندگی افراد است، به‌عنوان شرط بقاء سازمان‌ها در عصر حاضر به‌شمار می‌رود. هر ابزار و موجودیتی می‌تواند در کنار مزایایی که برای انسان فراهم کند، خطراتی را نیز برای او داشته باشد. در مورد ارتباطات و ابزارهای فناوری، این مشکلات فارغ از مشکلات اجتماعی -که مورد بحث این کتاب نبوده و از حوصله آن خارج است- مشکلات امنیتی را نیز دربر می‌گیرد. این مشکلات امنیتی می‌تواند در قالب افشاء داده‌های کاربران، کلاهبرداری‌ها و... نمایان شود. بنابراین سازمان‌ها تلاش می‌کنند تا امنیت خود را بهبود داده و از این طریق برای مشتریان خود اعتمادسازی نماید. ارزیابی امنیتی معرف روشی است که به سازمان‌ها این امکان را می‌دهد تا از شرایط امنیتی موجود اطمینان حاصل نموده و راه‌کارها و راهبردهای بهبود آن‌را به‌دست آورند. ارزیابی امنیتی به‌خودی خود موجودیت خوش‌تعریفی نیست و مشخص است که باید چیزی در سازمان وجود داشته باشد که ارزیابی شود. این موجودیت با عنوان معیار شناخته می‌شود. چنانچه بیشتر به این فرآیند بیاندیشیم مشخص می‌شود که هزاران و شاید میلیون‌ها موجودیت برای ارزیابی در سازمان‌ها وجود دارد. اما آیا تمامی آنها پاسخگوی نیاز یک ارزیاب است و سازمان را به هدف مشخص خود می‌رساند؟! بدیهی است که این‌طور نیست. از این‌رو در کتاب حاضر برآنیم تا سازمان‌ها را با معیارهایی آشنا کنیم که می‌تواند آنها را در راستای بهبود امنیت اطلاعات هدایت نماید.

در این راستا، دیدگاه‌ها و نگرش‌های مختلفی وجود دارد. مؤلف با بهره‌گیری از مجموعه این موارد در پی آدرس‌دهی به مسائل امنیتی موجود در سازمان‌ها از طریق ارزیابی امنیتی و معیارهای امنیتی است.

ابوذر عرب‌سرخی

فهرست مطالب

عنوان..... صفحه
فصل اول: مقدمه‌ای بر ارزیابی امنیتی ۱۹
۱-۱- مقدمه..... ۲۱
۱-۲- نگاهی گذرا بر مفاهیم پایه امنیت اطلاعات..... ۲۱
۱-۳- تعریف امنیت اطلاعات..... ۲۳
۱-۳-۱- تعریف مفاهیم پایه در امنیت اطلاعات..... ۲۴
۱-۳-۲- تعریف ویژگی‌های امنیتی اطلاعات..... ۲۷
۱-۴- مفهوم‌شناسی ارزیابی امنیتی..... ۳۰
۱-۵- اهمیت و جایگاه ارزیابی امنیتی..... ۳۲
۱-۵-۱- پاسخگویی به سوال‌های مدیریتی..... ۳۲
۱-۵-۲- بهبود امنیت اطلاعات به‌صورت نظام‌مند..... ۳۵
۱-۵-۳- تأمین اهداف تطابق و اطمینان..... ۳۶
۱-۵-۴- تأمین اهداف راهبردی، تاکتیکی و عملیاتی..... ۳۷
۱-۵-۵- پرکردن خلاءهای بوجود آمده بر اثر عدم توانایی ارزیابی امنیتی..... ۳۸
۱-۵-۶- افزایش سودآوری..... ۳۹
۱-۶- نقش معیارهای امنیتی در فرآیند ارزیابی و چگونگی انتخاب آن‌ها..... ۳۹
۱-۶-۱- فرامعیارهای کورِس..... ۴۱
۱-۶-۲- فرامعیارهای پرگمتیک..... ۴۲
۱-۶-۲-۱- پیشگویانه بودن..... ۴۲
۱-۶-۲-۲- مربوط بودن..... ۴۴
۱-۶-۲-۳- عملی بودن..... ۴۴
۱-۶-۲-۴- واقعی بودن..... ۴۵
۱-۶-۲-۵- معنی‌دار بودن..... ۴۶
۱-۶-۲-۶- دقیق بودن..... ۴۶
۱-۶-۲-۷- به‌موقع بودن..... ۴۷
۱-۶-۲-۸- مستقل بودن..... ۴۹
۱-۶-۲-۹- هزینه‌بر بودن..... ۴۹
فصل دوم: دیدگاه‌ها و نگرش‌های مختلف نسبت به ارزیابی امنیتی..... ۵۳
۲-۱- مقدمه..... ۵۵

عنوان..... صفحه

۲-۲- معرفی معیارهای امنیتی براساس نظر متخصصین یا مراجع امنیتی ۵۸
۲-۳- معیارهای ارزیابی امنیتی براساس سطح تعریف ۵۹
۲-۳-۱- معیارهای راهبردی، مدیریتی و عملیاتی ۶۰
۲-۳-۱-۱- معیارهای راهبردی ۶۲
۲-۳-۱-۲- معیارهای مدیریتی ۶۳
۲-۳-۱-۳- معیارهای عملیاتی ۶۳
۲-۳-۲- معیارهای ورودی-پردازش-خروجی ۶۴
۲-۳-۳- معیارهای بلوغ ۶۶
۲-۳-۴- معیارهای آمادگی ۶۷
۲-۴- معیارهای کارکردی و فرآیندی ۶۸
۲-۴-۱- معیارهای فرآیندی ۶۸
۲-۴-۱-۱- معیارهای مدیریت مخاطره ۶۸
۲-۴-۱-۲- معیارهای خط‌مشی/ عملی‌بودن امنیت اطلاعات ۶۹
۲-۴-۱-۳- معیارهای حکمرانی، مدیریت و سازماندهی امنیتی ۷۰
۲-۴-۱-۴- معیارهای مدیریت دارایی‌های اطلاعاتی ۷۳
۲-۴-۱-۵- معیارهای مدیریت تداوم کسب‌وکار ۷۳
۲-۴-۱-۶- معیارهای تطابق و اطمینان ۷۴
۲-۴-۱-۷- معیارهای کارایی و اثربخشی ۷۵
۲-۴-۱-۸- معیارهای صریح و مستقیم ۷۵
۲-۴-۱-۹- معیارهای پایداری ۷۶
۲-۴-۲- معیارهای کارکردی ۷۶
۲-۴-۲-۱- معیارهای امنیتی منابع انسانی ۷۷
۲-۴-۲-۲- معیارهای امنیت فیزیکی ۷۹
۲-۴-۲-۳- معیارهای امنیت فناوری اطلاعات ۸۰
۲-۴-۲-۴- معیارهای کنترل دسترسی ۸۱
۲-۴-۲-۵- معیارهای امنیت نرم‌افزار ۸۴
۲-۴-۲-۶- معیارهای مدیریت رخداد ۸۵
۲-۵- دسته‌بندی معیارها براساس قابلیت و نوع سنجش ۸۵
۲-۵-۱- معیارهای کمی ۸۶
۲-۵-۲- معیارهای کیفی ۸۷
۲-۵-۳- معیارهای ترکیبی ۸۷

عنوان..... صفحه

فصل سوم: متخصصین حوزه امنیت و نگاه به معیارهای امنیتی..... ۸۹

۳-۱- مقدمه ۹۱

۳-۲- معیارهای امنیتی پِرگَمَتیک از منظر بروتبی ۹۱

۳-۲-۱- مدیریت مخاطره امنیت اطلاعات ۹۲

۳-۲-۱-۱- تعداد مخاطره‌های برطرف/ درمان‌نشده در سطوح مختلف ۹۲

۳-۲-۱-۲- انحراف بودجه امنیت اطلاعات ۹۳

۳-۲-۱-۳- آسیب‌پذیری یا شکنندگی فرآیند یا سیستم ۹۳

۳-۲-۱-۴- تعداد آسیب‌پذیری‌هایی که وصله امنیتی برای آن‌ها نصب نشده ۹۳

۳-۲-۱-۵- درجه مخاطره‌های امنیت اطلاعات ۹۴

۳-۲-۱-۶- میزان هزینه بالقوه برای مخاطره‌های برطرف نشده/ جنبی ۹۵

۳-۲-۱-۷- شاخص کوپلینگ ۹۵

۳-۲-۱-۸- تغییر در سطح کاوش‌های شبکه ۹۶

۳-۲-۱-۹- همگنی فنی و سازمانی ۹۶

۳-۲-۱-۱۰- درصد کنترل‌هایی که طبق تعریف درست کار می‌کنند ۹۷

۳-۲-۱-۱۱- میزان پوشش بیمه سازمان در مقابل حق‌بیمه سالانه ۹۷

۳-۲-۱-۱۲- تعداد حمله‌ها ۹۷

۳-۲-۲- معیارهای خط‌مشی امنیتی ۹۷

۳-۲-۲-۱- تعداد خط‌مشی‌ها، استانداردها، رویه‌ها و معیارهای امنیتی دارای مسئول مشخص ۹۸

۳-۲-۲-۲- قابلیت رصدخط‌مشی‌ها، کنترل‌ها، اهداف، استانداردها و رویه‌ها ۹۸

۳-۲-۲-۳- تعداد عملیات مهم که دارای رویه‌های امنیتی مستند و آزمون‌شده هستند ۹۹

۳-۲-۲-۴- فراگیر بودن پوشش خط‌مشی امنیتی ۹۹

۳-۲-۲-۵- پوشش خط‌مشی توسط چارچوب‌های امنیتی ۹۹

۳-۲-۲-۶- تعداد یا نسبت خط‌مشی‌های امنیتی که مخاطره‌های مانا را آدرس‌دهی می‌کند ۱۰۰

۳-۲-۲-۷- کیفیت خط‌مشی‌های امنیتی ۱۰۰

۳-۲-۲-۸- درصد خط‌مشی‌های امنیتی که به‌صورت شفاف به هدف‌های کنترلی نگاشت شده‌اند ۱۰۰

۳-۲-۲-۹- عامل ضربه ۱۰۱

۳-۲-۲-۱۰- تعداد خط‌مشی‌هایی که در زمان مقرر بازبینی نشده‌اند ۱۰۱

۳-۲-۲-۱۱- رتبه خوانایی فِلِش-کین‌ساید برای خط‌مشی‌های امنیت ۱۰۲

۳-۲-۲-۱۲- تعداد یا نسبت خط‌مشی‌های امنیتی شفاف ۱۰۲

۳-۲-۲-۱۳- درصد خط‌مشی‌های امنیتی مبتنی بر استانداردهای مستندسازی ۱۰۲

عنوان..... صفحه

۳-۲-۲-۱۴- تعداد خط‌مشی‌های ناسازگار با سایر خط‌مشی‌ها ۱۰۳
۳-۲-۳- حکمرانی، مدیریت و سازماندهی امنیت ۱۰۳
۳-۲-۳-۱- کیفیت معیارهای امنیتی مورد استفاده ۱۰۳
۳-۲-۳-۲- درصد کنترل‌های امنیتی که به‌درستی عمل نمی‌کنند ۱۰۴
۳-۲-۳-۳- امنیت اطلاعات در سطوح بالا ۱۰۴
۳-۲-۳-۴- درصد کنترل‌های امنیتی که به‌طور شفافی به هدف‌های امنیتی نگاشت شده‌اند ۱۰۵
۳-۲-۳-۵- تعداد کنترل‌هایی که اهداف تعریف‌شده خود را به‌درستی انجام می‌دهند ۱۰۵
۳-۲-۳-۶- نسبت کنترل‌های حیاتی سازگار با خط‌مشی‌های امنیتی ۱۰۵
۳-۲-۳-۷- وضعیت اقتصادی سازمان ۱۰۶
۳-۲-۳-۸- درصد کنترل‌های افزونه یا اضافی ۱۰۶
۳-۲-۳-۹- هدف‌های کنترلی که با اهداف خاص کسب‌وکار ارتباط تنگاتنگی دارند ۱۰۶
۳-۲-۳-۱۰- زمان سپری‌شده از آخرین حادثه مهم امنیتی ۱۰۷
۳-۲-۳-۱۱- هزینه سالانه کنترل‌های امنیت اطلاعات ۱۰۷
۳-۲-۳-۱۲- تعداد کنترل‌های مختلف ۱۰۸
۳-۲-۳-۱۳- گستردگی حسابرسی دارایی‌های اطلاعاتی ۱۰۹
۳-۲-۳-۱۴- هزینه امنیت اطلاعات ۱۰۹
۳-۲-۳-۱۵- قانون بِنفورد ۱۰۹
۳-۲-۳-۱۶- ارزش خالص فعلی ۱۱۱
۳-۲-۳-۱۷- بازگشت سرمایه ۱۱۲
۳-۲-۳-۱۸- نرخ بازده داخلی ۱۱۲
۳-۲-۳-۱۹- دوره بازگشت سرمایه ۱۱۳
۳-۲-۳-۲۰- نرخ رضایت مشتریان مدیریت امنیت اطلاعات ۱۱۳
۳-۲-۳-۲۱- میزان پوشش کنترل‌های امنیت اطلاعات ۱۱۴
۳-۲-۳-۲۲- سطح وضعیت دفاعی ۱۱۴
۳-۲-۳-۲۳- سازگاری کنترل‌ها ۱۱۵
۳-۲-۳-۲۴- حدود و ثغور کارکردهای امنیت اطلاعات ۱۱۵
۳-۲-۳-۲۵- ارزش در معرض خطر ۱۱۵
۳-۲-۳-۲۶- بازگشت سرمایه‌گذاری امنیت ۱۱۶
۳-۲-۳-۲۷- بودجه امنیت به نسبت بودجه فناوری اطلاعات یا برعکس ۱۱۶
۳-۲-۴- معیارهای مدیریت دارایی اطلاعاتی ۱۱۷
۳-۲-۴-۱- تعداد دارایی‌هایی که صاحب ندارند ۱۱۷

عنوان..... صفحه

۳-۲-۴-۲- سهم دارایی‌های اطلاعاتی که طبقه‌بندی نشده‌اند ۱۱۷
۳-۲-۴-۳- مدت زمانی‌که دارایی‌های اطلاعاتی بدون متولی بوده‌اند ۱۱۸
۳-۲-۴-۴- جامعیت فهرست دارایی‌های اطلاعاتی ۱۱۸
۳-۲-۴-۵- ارزش دارایی‌های اطلاعاتی که صاحب آن‌ها مشخص است ۱۱۸
۳-۲-۴-۶- درصد دارایی‌های اطلاعاتی که -براساس طبقه‌بندی- برچسب زده نشده‌اند ۱۱۹
۳-۲-۵- معیارهای امنیت منابع انسانی ۱۱۹
۳-۲-۵-۱- سطح آگاهی امنیتی ۱۱۹
۳-۲-۵-۲- نرخ استعفاء یا غیبت کارمندان ۱۲۰
۳-۲-۵-۳- میزان انگیزه و روحیه کارمندان ۱۲۱
۳-۲-۵-۴- میزان تبعیت مدیران از قوانین ۱۲۲
۳-۲-۵-۵- فرهنگ امنیتی سازمان ۱۲۲
۳-۲-۵-۶- نسبت حساب‌های‌کاربری به کارمندان ۱۲۲
۳-۲-۵-۷- مشاهده مستقیم یا جمع‌آوری پرسشنامه در مورد فرهنگ سازمان ۱۲۳
۳-۲-۵-۸- میزان ترافیک امنیتی در فضای میز پشتیبان ۱۲۴
۳-۲-۵-۹- فرهنگ/ جهان‌بینی سازمان ۱۲۵
۳-۲-۵-۱۰- تغییر کارمندان در مقابل ریزش حساب‌های‌کاربری ۱۲۵
۳-۲-۵-۱۱- اختلال عملکردی سازمانی ۱۲۶
۳-۲-۵-۱۲- روان‌سنجی ۱۲۷
۳-۲-۶- معیارهای امنیت فیزیکی ۱۲۸
۳-۲-۶-۱- مصرف انرژی در واحد رایانه به نسبت ظرفیت تهویه هوا ۱۲۸
۳-۲-۶-۲- فاصله مابین مکان فیزیکی و مکان دسترسی منطقی ۱۲۹
۳-۲-۶-۳- تعداد نقاط دسترسی ناامن ۱۲۹
۳-۲-۶-۴- تعداد مخاطره‌های فیزیکی غیرقابل قبول ۱۳۰
۳-۲-۶-۵- فاصله مابین پارکینگ کارمندان و میهمانان ۱۳۰
۳-۲-۶-۶- درصد سازه‌هایی که نور خارجی مناسبی دارند ۱۳۰
۳-۲-۷- معیارهای امنیت فناوری اطلاعات ۱۳۱
۳-۲-۷-۱- تعداد سیستم‌های آزمون‌شده و منطبق بر استانداردهای امنیتی ۱۳۱
۳-۲-۷-۲- زمان مابین تأیید تغییر تا اعمال تغییر ۱۳۲
۳-۲-۷-۳- همبستگی بین سیستم/ رخدادنگاری‌های پیکربندی با درخواست تغییر مجاز ۱۳۳
۳-۲-۷-۴- تعداد سیستم‌های اطلاعاتی با پیکربندی ناامن ۱۳۳

عنوان..... صفحه

۳-۲-۷-۵- نرخ درخواست‌های تغییر فوری/ اضطراری ۱۳۳
۳-۲-۷-۶- تعداد کاربران یا توابعی که حقوق دسترسی بالایی دارند ۱۳۴
۳-۲-۷-۷- بی‌نظمی محتوای رمزشده ۱۳۴
۳-۲-۷-۸- درصد تغییرهای ناموفقی که به دلایل امنیتی رخ داده‌اند ۱۳۵
۳-۲-۷-۹- شاخص آسیب‌پذیری ۱۳۵
۳-۲-۷-۱۰- تأخیرها و ناسازگاری‌ها در نصب وصله‌های امنیتی ۱۳۶
۳-۲-۷-۱۱- نرخ شهودی تغییر در فناوری اطلاعات ۱۳۶
۳-۲-۷-۱۲- پیروی از خط‌مشی‌های نصب وصله امنیتی ۱۳۶
۳-۲-۷-۱۳ تعداد تغییرها ۱۳۶
۳-۲-۷-۱۴- تعداد ویروس‌های کشف‌شده در فایل‌های کاربران ۱۳۷
۳-۲-۷-۱۵- تعداد تغییرها در قوانین دیواره‌آتش ۱۳۷
۳-۲-۷-۱۶- نرخ آلودگی داده‌های مشتریان ۱۳۷
۳-۲-۸- معیارهای کنترل دسترسی ۱۳۸
۳-۲-۸-۱- تعداد پیام‌های دریافتی در سیستم اعلام هشدار/ رخدادنگاری مرکزی ۱۳۸
۳-۲-۸-۲- مدت‌زمان سپری‌شده از آخرین بازبینی ماتریس کنترل دسترسی سیستم‌ها ۱۳۹
۳-۲-۸-۳- تعداد حساب‌های‌کاربری که براساس خط‌مشی‌ها غیرفعال شده‌است ۱۳۹
۳-۲-۸-۴- نرخ تشخیص ناهنجاری‌های دسترسی ۱۳۹
۳-۲-۸-۵- پوشش و جزئیات ماتریس کنترل دسترسی منطقی برای برنامه‌های کاربردی ۱۴۰
۳-۲-۸-۶- وضعیت توسعه ماتریس‌های کنترل دسترسی منطقی برای برنامه‌های کاربردی ۱۴۰
۳-۲-۸-۷- کیفیت کنترل‌های شناسایی و احراز هویت ۱۴۰
۳-۲-۸-۸- نسبت واحدهای کسب‌وکار که روش‌های شناسایی و احراز هویت خود را آزمایش نموده‌اند ۱۴۱
۳-۲-۸-۹- تعداد دفعه‌هایی که دارایی‌ها بدون احراز هویت در دسترس افراد/ سیستم‌های غیرمجاز قرار گرفته‌اند ۱۴۱
۳-۲-۹- معیارهای امنیت نرم افزار ۱۴۱
۳-۲-۹-۱- درصد کنترل‌هایی که به‌صورت واقعی آزمون شده‌اند ۱۴۱
۳-۲-۹-۲- سطح تضمین کیفیت نرم‌افزار ۱۴۲
۳-۲-۹-۳- کیفیت امنیت سیستم که از طریق آزمون مشخص شده‌است ۱۴۳
۳-۲-۹-۴- سطح امنیت اطلاعات موجود در تضمین کیفیت نرم‌افزار ۱۴۳
۳-۲-۹-۵- سطح تضمین کیفیت نرم‌افزار موجود در امنیت اطلاعات ۱۴۴
۳-۲-۹-۶- درصد پیکربندی‌هایی که در راستای خدمات کارایی و امنیت اعمال می‌شوند ۱۴۴
۳-۲-۹-۷- درصد کنترل‌های فنی که به‌طور امن شکست می‌خورند ۱۴۴

عنوان..... صفحه

۳-۲-۹-۸- تعداد انحراف‌های شناسایی‌شده مابین فایل پیکربندی و پیکربندی واقعی دارایی‌ها ۱۴۵
۳-۲-۱۰- معیارهای مدیریت حوادث ۱۴۵
۳-۲-۱۰-۱- زمان صرف‌شده برای ترمیم حادثه‌های امنیتی ۱۴۶
۳-۲-۱۰-۲- فاصله زمانی مابین وقوع و تشخیص حادثه ۱۴۶
۳-۲-۱۰-۳- درصد حادثه‌هایی که مقصر اصلی آن کشف شده‌است ۱۴۶
۳-۲-۱۰-۴- هزینه‌های تجمیعی حادثه‌های امنیت اطلاعات ۱۴۷
۳-۲-۱۰-۵- تعداد کل رویدادها و حادثه‌های امنیت اطلاعات ۱۴۸
۳-۲-۱۰-۶- تعداد حادثه‌های امنیتی که قابلیت کنترل، پیش‌گیری یا مقابله با آن‌ها وجود دارد ۱۴۸
۳-۲-۱۰-۷- تأثیرهای غیرمالی حادثه‌های امنیتی ۱۴۹
۳-۲-۱۱- معیارهای تداوم کسب‌وکار ۱۴۹
۳-۲-۱۱-۱- میزان پوشش تحلیل پیامدهای کسب‌وکار ۱۴۹
۳-۲-۱۱-۲- درصد فعالیت‌های مهم دارای سازمان‌دهی مناسب در حوزه تداوم کسب‌وکار ۱۴۹
۳-۲-۱۱-۳- درصد رویه‌های کسب‌وکار که هدف‌های زمان بازیابی و نقطه بازیابی تعریف‌شده‌ای دارند ۱۵۰
۳-۲-۱۱-۴- وضعیت نگه‌داری برنامه‌های تداوم کسب‌وکار ۱۵۱
۳-۲-۱۱-۵- نتایج آزمون بازیابی بلایا ۱۵۱
۳-۲-۱۱-۶- زمان روشن‌بودن ۱۵۲
۳-۲-۱۱-۷- ظرفیت و کارایی فناوری اطلاعات ۱۵۳
۳-۲-۱۱-۸- نگاشت فرآیندهای حیاتی به برنامه‌های بازیابی بلایا و تداوم کسب‌وکار ۱۵۳
۳-۲-۱۱-۹- هزینه تداوم کسب‌وکار ۱۵۴
۳-۲-۱۱-۱۰- تعداد سیستم‌های حساس منطبق بر الزام‌های کنترلی امنیت ۱۵۴
۳-۲-۱۲- معیارهای انطباق و اطمینان امنیت ۱۵۵
۳-۲-۱۲-۱- تفکیک استثناءها و تبصره‌ها ۱۵۵
۳-۲-۱۲-۲- تعداد و میزان فاجعه‌بار بودن یافته‌های ممیزی، گزارش‌ها، بازبینی‌ها و ارزیابی‌ها ۱۵۵
۳-۲-۱۲-۳- وضعیت پیروی از قوانین امنیت اطلاعات که از خارج به سازمان تحمیل شده‌اند ۱۵۶
۳-۲-۱۲-۴- سوابق جریمه‌های عدم انطباق ۱۵۷
۳-۲-۱۲-۵- تعداد سیستم‌های اعتبارسنجی‌شده امنیتی ۱۵۷
۳-۲-۱۲-۶- وضعیت پیروی از الزام‌های اجباری داخلی ۱۵۷
۳-۲-۱۲-۷- تعداد نرم‌افزارهای بدون مجوز نصب‌شده بر روی دستگاه‌ها ۱۵۸
۳-۲-۱۲-۸- درصد خط‌مشی‌های امنیتی پشتیبانی‌شده توسط فعالیت‌های تطابقی مناسب ۱۵۸
۳-۲-۱۲-۹- الگوی تطابق در مواجهه با شرکاء ۱۵۸

عنوان..... صفحه

۳-۲-۱۲-۱۰- تعداد یا نرخ عدم انطباق کشف‌شده خط‌مشی‌ها ۱۵۹
۳-۲-۱۲-۱۱- عامل شرم ۱۵۹
۳-۲-۱۲-۱۲- درصد خرید نرم‌افزارهای غیرمجاز ۱۵۹
۳-۲-۱۲-۱۳- نسبت هزینه خرج‌شده برای امنیت بر حاصل‌ضرب تأثیر بالقوه در احتمال وقوع خطر ۱۵۹
۳-۲-۱۲-۱۴- تعداد لایسنس‌های خریداری‌شده بلااستفاده ۱۶۰
۳-۲-۱۲-۱۵- درصد دارایی‌های حیاتی موجود بر روی سیستم‌هایی که به‌صورت کامل از الزام‌های تعیین‌شده پیروی نموده‌اند ۱۶۰
۳-۳- معیارهای مدیریت امنیت اطلاعات از منظر بروتبی ۱۶۰
۳-۳-۱- معیارهای کارایی عمومی امنیت ۱۶۱
۳-۳-۱-۱- تعداد بسته‌هایی که توسط دیواره‌آتش دور ریخته شده‌اند ۱۶۱
۳-۳-۱-۲- میزان مصرف پردازشگر یا پهنای‌باند ۱۶۱
۳-۳-۱-۳- ظرفیت باقی‌مانده از انباره ۱۶۲
۳-۳-۱-۴- تغییر در سایز فایل‌ها ۱۶۲
۳-۳-۱-۵- فایل‌های اضافی موجود بر روی سرور ۱۶۲
۳-۳-۱-۶- تعداد تلاش‌های ناموفق برای ورود به سیستم ۱۶۳
۳-۳-۱-۷- دسترسی غیرمجاز به وب‌سایت ۱۶۳
۳-۳-۱-۸- تخلف سرپرست ۱۶۳
۳-۳-۱-۹- تعداد نفوذهای موفق به سیستم‌ها ۱۶۳
۳-۳-۲- معیارهای کارایی فنی امنیت ۱۶۴
۳-۳-۲-۱- میزان استفاده از/ بهره‌وری سیستم ۱۶۴
۳-۳-۲-۲- زمان خاموشی ۱۶۴
۳-۳-۲-۳- میزان پیروی از توافقنامه‌های سطح سرویس ۱۶۴
۳-۳-۲-۴- میزان کارامدی پالایش هرزنامه ۱۶۵
۳-۳-۲-۵- تعداد حمله‌های مقابله‌شده ۱۶۵
۳-۳-۲-۶- زمان‌های پاسخ به حادثه ۱۶۵
۳-۳-۲-۷- فاصله‌های زمانی مابین کشف آسیب‌پذیری و رفع آن ۱۶۵
۳-۳-۲-۸- نرخ شکست در کنترل ۱۶۶
۳-۳-۲-۹- اثربخشی کنترل‌ها ۱۶۶
۳-۳-۲-۱۰- هزینه عملیاتی کنترل‌ها ۱۶۶
۳-۳-۲-۱۱- هزینه نگه‌داری کنترل‌ها ۱۶۶
۳-۳-۲-۱۲- تأثیر کنترل‌ها بر روی کسب‌وکار ۱۶۷

عنوان ..... صفحه

۳-۳-۲-۱۳- شاخص‌های کلیدی عملکرد ۱۶۷
۳-۳-۲-۱۴- شاخص‌های کلیدی هدف ۱۶۸
۳-۳-۳- معیارهای ارزیابی مالی ۱۶۹
۳-۳-۳-۱- برآورد خسارت واحد مورد انتظار ۱۶۹
۳-۳-۳-۲- برآورد خسارت سالانه مورد انتظار ۱۷۰
۳-۳-۳-۳- تحلیل مقرون‌به‌صرفه بودن ۱۷۰
۳-۳-۳-۴- تحلیل هزینه-منفعت ۱۷۰
۳-۳-۴- تجزیه و تحلیل درخت خطا ۱۷۱
۳-۳-۵- چارچوب ارزش رقابتی ۱۷۱
۳-۳-۶- ساختار سازمانی ۱۷۳
۳-۴- معیارهای امنیتی از منظر جاکوس ۱۷۳
۳-۴-۱- معیارهای امنیتی محیطی ۱۷۴
۳-۴-۲- معیارهای امنیتی کنترل و پوشش ۱۷۶
۳-۴-۳- معیارهای دسترس‌پذیری و اطمینان ۱۸۱
۳-۴-۴- مخاطره‌های برنامه‌کاربردی ۱۸۲
۳-۴-۵- معیارهای کارآمدی فرآیندها ۱۸۴
فصل چهارم: معیارهای امنیتی مبتنی بر بهترین تجربه‌های منتشرشده ۱۹۳
۴-۱- مقدمه ۱۹۵
۴-۲- بهترین تجربه‌ها و جایگاه آن‌ها در تعریف معیارهای امنیتی ۱۹۵
۴-۳- معیارهای امنیتی مبتنی بر چارچوب سابسا ۱۹۵
۴-۳-۱- مشخصه‌های کاربر ۱۹۷
۴-۳-۲- مشخصه‌های مدیریتی ۱۹۹
۴-۳-۳- مشخصه‌های عملیاتی ۲۰۱
۴-۳-۴- مشخصه‌های مدیریت مخاطره‌ها ۲۰۲
۴-۳-۵- مشخصه‌های حکمرانی و تنظیم مقررات ۲۰۵
۴-۳-۶- مشخصه‌های راهبرد فنی ۲۰۶
۴-۳-۷- مشخصه‌های راهبرد کسب‌وکار ۲۰۸
۴-۴- معیارهای امنیتی مبتنی بر دیدگاه مؤسسه ملی استانداردها و فناوری ۲۱۱
۴-۴-۱- بودجه بخش امنیت ۲۱۱
۴-۴-۲- نرخ مدیریت آسیب‌پذیری ۲۱۱

عنوان..... صفحه
۴-۴-۳- وضعیت کنترل دسترسی ۲۱۲
۴-۴-۴- وضعیت آموزش و آگاهی بخشی ۲۱۲
۴-۴-۵- وضعیت ممیزی و حسابرسی ۲۱۲
۴-۴-۶- وضعیت گواهینامه، اعتبارنامه و ارزیابی امنیتی ۲۱۳
۴-۴-۷- وضعیت مدیریت پیکربندی ۲۱۳
۴-۴-۸- وضعیت برنامه‌ریزی اقتضایی ۲۱۳
۴-۴-۹- وضعیت شناسایی و احراز هویت ۲۱۴
۴-۴-۱۰- وضعیت پاسخ به رخداد ۲۱۵
۴-۴-۱۱- وضعیت نگه‌داری ۲۱۵
۴-۴-۱۲- وضعیت محافظت از رسانه ۲۱۵
۴-۴-۱۳- وضعیت امنیت محیطی و فیزیکی ۲۱۶
۴-۴-۱۴- وضعیت برنامه‌ریزی ۲۱۶
۴-۴-۱۵- وضعیت امنیت کارمندان ۲۱۷
۴-۴-۱۶- وضعیت ارزیابی مخاطره‌ها ۲۱۷
۴-۴-۱۷- وضعیت خرید خدمات و سیستم‌ها ۲۱۷
۴-۴-۱۸- وضعیت محافظت از سیستم‌ها و ارتباط‌ها ۲۱۸
فصل پنجم: جمع‌بندی معیارهای ارزیابی امنیتی ۲۲۱
۵-۱- مقدمه ۲۲۳
۵-۲- نمایه‌ای انتزاعی از معیارهای امنیتی ۲۲۴
پیوست الف ۲۵۱
مروری اجمالی بر روش‌های ارزیابی مخاطره ۲۵۱
فهرست واژگان ۲۶۳
مراجع ۲۸۱