ویکی‌پدیا

مدیریت ریسک بر پروژه‌های فناوری اطلاعات

این مقاله نیازمند ویکی‌سازی است. لطفاً با توجه به راهنمای ویرایش و شیوه‌نامه، محتوای آن را بهبود بخشید.

بیشتر بدانید

این مقاله نیازمند بررسی توسط متخصص است.

بیشتر بدانید

مدیریت ریسک بر پروژه‌های فناوری اطلاعات

چکیده: ریسک یکی از مهم‌ترین عوامل تأثیرگذار بر روند پروژه‌ها است که با یک مدیریت ریسک جامع و اصولی می‌توان آن را به نحو گسترده ای کنترل نمود. این پروسه خود از چندین بخش کوچکتر تشکیل شده که پس از اجتماع به دستاوردهای مورد نظر جامه عمل می پو شاند.[۱]

مقدمه: مدیریت ریسک پروسه ای است که به مدیران IT اجازه می‌دهد تا از سیستم‌ها و داده‌های سازمان خود حفاظت کرده، هزینه‌های اقتصادی و عملی سنجش‌های حفاظتی را متعادل نموده و به دستاوردهای مورد نظر در مأموریت دست یابند. مدیران IT هزینه‌های بسیاری را به حفاظت فناوری اطلاعات اختصاص می‌دهند که با یک متدولوژی خوش ساخت که به‌طور مؤثر به خدمت گرفته شودT می‌توان مدیریت در جهت شناخت کنترل‌های مناسب برای قابلیت‌های حفاظتی مهیا شده را به‌طور محسوسی بهینه نمود. «کمینه کردن تاثیرهای منفی سازمان و نیاز به یک پایه در تصمیم گیری»، دلایل اساسی است که سازمان‌ها را به ایجاد یک پروسه مدیریت ریسک برای سیستم‌های IT سوق داده است.[۲]

ریسک پروژه

یک رخداد یا شرایط غیر قطعی است که اگر رخ دهد تأثیری مثبت یا منفی بر روی یکی از اهداف پروژه می‌گذارد. ریسک ممکن است دارای یک یا چند دلیل باشد که اگر رخ دهد یک یا چند اثر به همراه داشته باشد.

پروسه مدیریت ریسک پروژه

به قصد کمک مؤثر به مدیریت ریسک‌های پروژه، تهدیدها و موقعیت‌ها اعمال می‌شود. پروسه سیستماتیک طرح‌ریزی برای شناسایی، تجزیه و تحلیل، واکنش نشان دادن و نظارت بر ریسک‌های پروژه است. مدیریت ریسک پروسه ای است که به مدیران IT اجازه می‌دهد تا از سیستم‌ها و داده‌های سازمان شان حفاظت کرده، هزینه‌های اقتصادی و عملی سنجش‌های حفاظتی را متعادل نموده و به دستاوردهای مورد نظر در مأموریت دست یابند. باید توجه داشت که *سیکل حیات پیشرفته سیستم* دارای ۵ فاز است:

۱- گشایش

۲- پیشرفت یا اکتساب

۳- پیاده‌سازی

۴- عملیات یا نگه داری

۵- مصرف

ارزیابی ریسک

برای تعیین مقدار بالقوه تهدید و ریسک مرتبط با یک سیتم IT در چرخه حیات نه گام در نظر گرفته شده‌است:

۱) مشخصات سیستم ۲) شناسایی تهدید ۳) شناسایی قابلیت آسیب‌پذیری ۴) تجزیه و تحلیل کنترل ۵) تعیین درست نمایی (Likelihood) ۶) تجزیه و تحلیل برخورد ۷) تعیین ریسک ۸) پیشنهادها کنترلی ۹) مستندسازی نتایج

قابل ذکر است که مراحل ۶،۴،۳،۲ می‌تواند از تمام مرحله تحت به صورت موازی اجرا شوند.

آسیب‌پذیری

ضعف‌هایی می‌تواند به صورت تصادفی به منابع و اطلاعات صدمه برساند. انواع آسیب‌پذیری‌های در سیکل حیات پیشرفته سیستم عبارت است از:

- اگر طراحی IT آغاز نشده‌است، جستجو برای آسیب‌ها باید بر سیاست‌های امنیتی سازمان، روال‌های امنیتی مطرح، تعاریف مورد نیاز سیستم و غیره متمرکز شود.

- در صورتی که سیستم IT در حال اجرا است، شناخت این آسیب‌ها باید برای توسعه اطلاعات مشخص بیشتر مانند مشخصه‌های امنیتی طرح و تعریف شده در سند طراحی امنیتی و نتایج تست تأیید سیستم و ارزیابی توسعه یابد.

- اگرسیتم IT عملی باشد، پروسه شناسایی آسیب باید شامل یک تجزیه و تحلیل جنبه‌های امنیت و کنترل‌های امنیت سیستم IT باشد.[۳]

روش‌های تست

-ابزارهای خودکار وارسی آسیب‌پذیری که برای وارسی یک گروه از میزبان‌ها و شبکه جهت شناسایی سرویس‌های آسیب‌پذیر (مانند سیستم‌هایی که به پروتکل تبادل فایل (FTP) بی نام اجازه عمل می‌دهند و غیره)

- ارزیابی و تست امنیت (ST & E) شامل پیشرفت و اجرای تست (برای نمونه متن سند تست، روال‌های تست و نتایج تست مورد نظر) است. هدف از این تست، تست کارا بودن کنترل‌های امنیت یک سیستم IT که در یک محیط عملیاتی به کار گرفته می‌شود است . به عبارت دیگر هدف، تضمین آن است که کنترلی که به کار گرفته شده با مشخصات امنیتی تصویب شده برای نرم‌افزار و سخت‌افزار سازش داشته باشد و اجرای سیاست امنیت سازمان یا بدست آوردن استانداردهای صنعتی است.[۴]

کاهش ریسک

دومین پروسه مدیریت ریسک شامل اولیت بندی، ارزیابی واجرای پیشنهادهای کنترلی جهت کاهش ریسک مناسب از پروسه ارزیابی ریسک است. به دلیل آن که نابود کردن تمامی ریسک‌ها معمولاً غیر عملی یا نزدیک به محال است، برعهده مدیر ارشد، عملیاتی یا تجاری است که از این رهیافت‌های حداقل هزینه، سود برد و مناسب‌ترین کنترل‌ها را برای کاهش ریسک مأموریت به سطحی قابل قبول با حداقل برخورد زیان بار منابع و مأموریت سازمان اجرا کند.[۲]

تجزیه و تحلیل سود و زیان

برای اختصاص دهی منابع و اجرای کنترل‌های کارا بر روی هزینه، سازمان‌ها پس از شناخت تمامی کنترل‌های ممکن و ارزیابی امکان‌پذیری و کارای آن‌ها باید یک تجزیه و تحلیل سود و زیان برای هر کنترل پیشنهاد شده انجام دهند تا تضمین شود کدام کنترل‌ها مناسب و مورد نیاز شرایط آن‌ها است.[۴]

ریسک باقیمانده

سازمان‌ها می‌توانند مقدار کاهش ریسک تولید شده توسط کنترل‌های جدید یا افزوده را بر حسب برخورد یا درست نمایی تهدید - دو عامل اساسی که سطح مأموریت سازمانی را تعیین می‌کند- کاهش داده، تجزیه و تحلیل نمایند.

منابع

1. *Risk Analysis and Management for Projects. Thomas Telford, RAMP (Institute of Civil Engineers and the Faculty and Institute of Actuaries).London. 1998*
2. *NIST Special Publication 800-14. Generally Accepted Principles and Practices for Securing Information Technology Systems. September 1996. Co-authored with Barbara Guttman.*
3. *NIST Interagency Reports 4749. Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out. December 1991.*
4. *NIST Special Publication 800-12. An Introduction to Computer Security: The NIST Handbook. October 1995.*

آخرین ویرایش ۳ سال پیش **توسط Yazdanpanahaskari انجام شده**

ویکی‌پدیا