

سیستم مدیریت امنیت اطلاعات isms

مؤلف: مهندس سید محسن احمد پناه

سرشناسه : احمدپناه، سیدمحسن، ۱۳۵۹ -
عنوان و نام : /نویسنده سیدمحسن احمدپناه SMS؛ سیستم مدیریت امنیت اطلاعات
پدیدآور
مشخصات نشر : تهران: اندیشه طلایی، ۱۳۹۳.

مشخصات : ۵۲ص.: مصور.
ظاهری
شابک : ۹۷۸-۶۰۰-۹۴۵۹۷-۴-۲ : ۸۰۰۰۰ ریال
وضعیت فهرست : فیا

نویسی
موضوع : کامپیوترها -- ایمنی اطلاعات -- مدیریت
موضوع : کامپیوترها -- ایمنی اطلاعات -- استانداردها
موضوع : تکنولوژی اطلاعات -- تدابیر ایمنی
رده بندی کنگره : QA۹/۷۶/۳ ک ۹الف ۱۳۹۳

رده بندی دیویی : ۸/۰۰۵

شماره کتابشناسی : ۳۵۸۹۶۶۸
ملی

نام اثر: سیستم مدیریت امنیت اطلاعات isms

نویسنده: مهندس سیدمحسن احمدپناه

ناشر: انتشارات اندیشه طلایی www.andishetalae.ir

طراح جلد: سید اسماعیل احمدپناه

نوبت چاپ : اول ۱۳۹۳ تیراژ: ۱۰۰۰ جلد

شابک: 978-600-94597-4-2

مرکز پخش شماره : تهران- میدان انقلاب. تلفن: ۶۶۱۲۰۸۳۴

حق چاپ برای ناشر محفوظ می باشد

حرکت سریع کشورها به سوی جامعه اطلاعاتی، موجب رشد وسیع سیستم ها و سرویس های اطلاعاتی شده است. در این شرایط، بخشی وسیعی از خدمات در همین بستر ارائه شده و ارائه دهندگان و دریافت کنندگان خدمات را ناگزیر از پیوستن به این جامعه نموده است.

اطلاعات، گنجینه‌ای که تا چندی قبل در کمدی و پستوهای سازمان ها نگهداری می شد، از چند سال قبل وبا توسعه شبکه های محلی درون سازمانی، به شبکه داخلی سازمان ها راه یافت. در آن زمان، اطلاعات محدود کاربران شبکه و اعمال کنترل های مدیریتی، محافظت های فیزیکی و محدود نمودن تعداد افرادی که به سرویس ها و بویژه سرویس های حساس دسترسی داشتند، موجب می شد تا مشکل خاصی بروز نکند. اما اینک با اتصال شبکه های سازمانی به شبکه جهانی، همان گنجینه حساس در معرض دید و استفاده طیف وسیعی از مخاطبین در سراسر جهان قرار گرفته است. مخاطبینی که مجهز به انواع اطلاعات و ابزارهای اطلاعاتی می باشند. البته تهدید فقط از سوی مخاطبین خارج از سازمان نیست. بررسی های انجام شده نشان می دهد که امروزه عمده تهدیدهای موجود علیه اطلاعات

وسیستم های اطلاعاتی سازمان ها، منشاء داخلی داشته و خواسته یا ناخواسته توسط پرسنل سازمان ایجاد می شود.

در این شرایط تامین امنیت همان گنجینه گران مایه یعنی اطلاعات، بدون شک یکی از ضروریات هر سازمانی است. حاصل تجربه و اقدامات انجام شده در طول یک دهه گذشته در جهان، رویکردی است تحت عنوان سیستم مدیریت امنیت اطلاعات که در این کتاب به بررسی آن می پردازیم.

مهندس سیدمحسن احمدپناه

پاییز ۱۳۹۳

فهرست

۳	 مقدمه
۱۷	 فصل اول: تعریف
۱۷	 ISMS چیست؟
۱۷	 رویکرد فرآیندی:
۱۷	 هدف از تدوین استانداردهای ISMS:
۱۸	 طرحی کلی از سیستم مدیریت امنیت اطلاعات ISMS Plan
۲۰	 طراحی و مستند سازی ISMS:
۲۴	 کنترل اثر بخشی سیستم امنیت اطلاعات
۲۵	 نگهداری و ارتقای سیستم مدیریت امنیت اطلاعات:
۲۶	 فصل دوم: استانداردهای مدیریت امنیت اطلاعات
۲۸	 بررسی استاندارد BS۷۷۹۹

بخش اول استاندارد 1999: 2 bs7799: ۲۹

بخش دوم استاندارد 1999: 2 BS 7799: ۳۵

تعریف سیاست امنیت اطلاعات ۳۶

شکل چارچوب ایجاد مدیریت امنیت اطلاعات ۳۸

فصل سوم: تدوین اهداف، راهبردها و سیاست های امنیتی ۴۰

اهداف امنیت اطلاعات ۴۰

سرمایه های مرتبط با اطلاعات سازمان ۴۱

الف: اهداف کوتاه مدت امنیت اطلاعات ۴۲

ب: اهداف میان مدت امنیت اطلاعات: ۴۲

راهبردهای تامین امنیت ۴۳

اجرای طرح ها و برنامه های امنیت اطلاعات ۴۶

پشتیبانی امنیت اطلاعات ۴۶

شرح وظایف تشکیلات امنیت فناوری ۴۸

- ۴۹..... شرح وظایف پشتیبانی حوادث امنیتی:
- ۵۰..... انجام اقدامات پیشگیرانه و به منظور کنترل دامنه تاثیر و بروس
- ۵۱..... تشخیص و پشتیبانی حوادث فیزیکی
- ۵۲..... شرح وظایف نظارت و بازرسی امنیتی
- ۵۴..... شرح وظایف مدیریت تغییرات
- ۵۵..... شرح وظایف نگهداری امنیت
- ۵۶..... فصل چهارم: سیاست های امنیت اطلاعات در محیط های سخت افزاری
- ۵۶..... مدیریت تجهیزات:
- ۵۷..... رویدادنگاری:
- ۵۸..... تشخیص و خنثی نمودن حملات:
- ۵۸..... سخت افزار تجهیزات:
- ۵۸..... محافظت فیزیکی:
- ۵۹..... بازرسی امنیتی تجهیزات:

- فصل پنجم: نیازمندی های امنیتی نرم افزارهای کاربردی در سازمان ۶۴
- نیازمندی های تامین محرمانگی اطلاعات : ۶۴
- نیازمندی های تامین صحت اطلاعات : ۶۴
- نیازمندی های تعیین هویت کاربران: ۶۵
- نیازمندی های ثبت اقدامات انجام شده توسط کاربر : ۶۵
- نیازمندی های تامین امنیت ارتباط : ۶۶
- استاندارد طراحی نرم افزار : ۶۶
- استاندارد پیاده سازی نرم افزار : ۶۷
- استاندارد تست نرم افزار : ۶۷
- سیاست های امنیتی دسترسی کاربران به نرم افزارها ۶۷
- درخواست استفاده از سرویس : ۶۷
- سفارش خرید نرم افزار: ۶۸
- درخواست تغییر نرم افزار : ۶۹
- خرید نرم افزار : ۶۹
- تست و تحویل نرم افزار : ۶۹

۷۰..... پیکر بندی نرم افزار :

۷۰..... نصب نرم افزار:

۷۱..... پشتیبانی نرم افزار :

۷۱..... سیاست های امنیتی اطلاعات

۷۱..... سطوح طبقه بندی اطلاعات رایانه ای :

۷۲..... طبقه بندی اطلاعات رایانه ای :

۷۳..... فصل ششم: نیازمندی های امنیتی اطلاعات طبقه بندی شده

۷۳..... محرمانگی :

۷۳..... صحت :

۷۴..... تشخیص هویت کاربران در دسترسی به اطاعات :

۷۴..... سیاست های امنیتی اطلاعات

۷۴..... سطوح طبقه بندی اطلاعات رایانه ای :

۷۷..... بخش های مختلف :

۷۸..... ارتباطات مجاز و غیرمجاز داخلی :

۷۹..... سیاست های امنیت ارتباطات داخلی

تعیین بخشهای مختلف داخلی: ۷۹

دسترسی های مدیریتی مجاز در بخش داخلی: ۸۰

امنیت ارتباطات در بخش های مختلف داخلی: ۸۰

سیاست های امنیتی دسترسی به اینترنت: ۸۱

بخشهای مختلف دسترسی به اینترنت: ۸۱

دسترسی های مجاز کاربران داخلی و راه دور: ۸۲

دسترسی های مدیریتی مجاز در دسترسی به اینترنت: ۸۲

فصل هفتم: نیازمندی امنیتی اطلاعات کاربران ۸۴

کاربران سازمان: ۸۴

کاربران داخلی: ۸۴

شرایط و محدودیتهای کاربران: ۸۵

سیاست های تعیین هویت و کنترل دسترسی کاربران: ۸۵

تشخیص هویت کاربران: ۸۵

حدود اختیارات کاربران: ۸۶

پاسخ گویی کاربران: ۸۶

سیاست های حریم خصوصی کاربران: ۸۶

۸۷		حیطه حریم خصوصی کاربران:
۸۷		ضوابط بر حریم خصوصی کاربران:
۸۸		رعایت حریم خصوصی کاربران:
۸۸		سیاست های آگاهی رسانی امنیتی به کاربران:
۸۹		اعلام دوره ای (با تعیین دوره) موارد فوق به کاربران:
۸۹		سیاست های مدیریت رمز عبور:
۹۲		بازرسی امنیتی:
۹۳		فصل هشتم: ارائه طرح امنیتی
۹۳		بررسی مخاطرات و تهدیدات ونحوه رفع آن:
۹۵		مخابرات امنیتی محتمل در خصوص مکانیزم های مدیریتی:
۹۷		مخاطرات تشکیلات و روش های امنیت:
۹۸		تشکیلات امنیت:
۹۹		اهداف امنیت:

۹۹.....	راهبردهای ایجاد و تداوم امنیت
۱۰۰.....	سیاست های امنیتی
۱۰۰.....	تدوین طرح ها و برنامه های امنیتی
۱۰۰.....	اجرای طرح ها و برنامه های امنیتی
۱۰۰.....	پشتیبانی امنیت
۱۰۱.....	ارزیابی و رفع اشکالات
۱۰۲.....	اهداف طرح امنیت شبکه
۱۰۴.....	روش های تامین امنیت در طرح امنیت
۱۰۴.....	معماری ، ساختار و مشخصات سیستم امنیتی
۱۰۴.....	معماری امنیت
۱۰۷.....	مشخصات فنی ابزارهای امنیت
۱۰۷.....	مشخصات فنی فایروال
۱۰۹.....	مشخصات فنی سیستم ضد ویروس
۱۱۵.....	فصل نهم: ارائه طرح پشتیبانی حوادث

۱۱۵	مقدمه :
۱۱۶	بررسی طرح پشتیبانی حوادث
۱۱۸	ساختار تیم پشتیبانی حوادث
۱۱۸	دسته بندی حوادث
۱۱۸	پاسخ به حوادث
۱۱۹	سیاست های و روال های پشتیبانی حوادث
۱۱۹	ساختار تیم پشتیبانی حوادث
۱۲۰	سرویسهای تیم پشتیبانی حوادث
۱۲۱	توصیه ها
۱۲۲	فازهای مختلف چرخه پشتیبانی حوادث
۱۲۴	تشخیص و تحلیل حوادث
۱۲۵	تدوین روال هایی برای قطعی سازی وقوع حوادث :
۱۲۵	تعیین ابزار [های] تشخیص حوادث:
۱۲۶	تحلیل حوادث و روش های آن :

۱۲۷.....	گزارش دهی حوادث :
۱۲۷.....	اولویت دهی به حوادث:
۱۲۸.....	هشدار حوادث:
۱۲۹.....	محدود سازی ، ترمیم و ریشه کنی.....
۱۳۱.....	فعالیت های بعد از ترمیم حوادث.....
۱۳۳.....	فصل دهم: برنامه آگاهی رسانی، تربیت نیروی انسانی و آموزش امنیت
۱۳۳.....	اهداف
۱۳۴.....	مخاطبین
۱۳۶.....	ابعاد
۱۳۶.....	سیاست
۱۳۶.....	وظایف و مسؤولیت ها
۱۳۸.....	آگاهی رسانی امنیتی
۱۳۹.....	تربیت نیروی انسانی.....

آموزش امنیت ۱۳۹

طراحی ۱۴۰

مخاطرات موجود در سازمان و تأثیر آن ها ۱۴۳

توسعه ۱۴۴

منابع ۱۵۱

www.ketab.ir