

روایاتی از کابوسهای امنیتی

امنیت اطلاعات

الهام مسجدیان
سیده فاطمه موالی زاده

انتشارات خایره

سیرشناسه	الهام مسجدیان ، ۱۳۶۱
عنوان و پدیدآور	روایاتی از کابوسهای امنیتی : امنیت اطلاعات / مولف : الهام مسجدیان ، سیده فاطمه موالی زاده
مشخصات نشر	تهران : نایره ، ۱۳۹۰
مشخصات ظاهری	۲۲۸ ص : مصور ، نمودار .
شابک	978-964-95423-7-9
موضوع	کامپیوترها - امنیتی اطلاعات شبکه های کامپیوتری - اقدامات تأمینی
شناسه افزوده	موالی زاده ، سیده فاطمه ، ۱۳۶۶
رده بندی کنگره	1390 5 9 ک / 9 / 76 QA
رده بندی دیوینی	۰۰۵/۸
شماره کتابشناسی ملی	۲۴۲۲۴۷۵



● روایاتی از کابوسهای امنیتی : امنیت اطلاعات

- مولفان : الهام مسجدیان ، سیده فاطمه موالی زاده
- ناشر : انتشارات نایره
- چاپ اول : تابستان ۱۳۹۰
- تیراژ : ۲۰۰۰ جلد
- قیمت : ۱۰۰۰۰ تومان
- صفحه آرایی : گروه مهندسی - پژوهشی ساحر
- چاپ : فناوری اطلاعات پارسه
- صحافی : فناوری اطلاعات پارسه
- شابک : 978-964-95423-7-9

مراکز پخش:

۶۶۹۱۹۲۶۷ ۶۶۰۶۵۹۹۶ - ۰۹۱۲۳۴۴۷۳۵۸

۷۷۲۶۳۶۵۹ - ۰۹۱۲۲۰۷۳۰۸۴

www.paarseh.com

✓ گروه مهندسی - پژوهشی ساحر

✓ انتشارات پارسه

www.saaheer.com

بنام خدا

آنچه در تقابل انسان و اطلاعات اهمیت می‌یابد، دسترسی سریع به دریایی از اطلاعات جامع و کامل است که برای نیل به این مهم نیاز به اتخاذ تدابیری می‌باشد تا نتیجه مطلوب حاصل گردد.

در این راستا، هدف **گروه مهندسی - پژوهشی ساحر** این است تا با عنایت پروردگار و همت و همکاری استادان و دانشجویان متعهد و دلسوز، به مطالعات و تحقیقات لازم پرداخته و به تألیف و ترجمه منابع دروس اصلی، فرعی و جنبی علوم کامپیوتر اقدام نماید و صداخته دشواری چنین کاری بر دانشمندان و صاحبان نظر پوشیده نیست و به همین جهت مرحله کمال مطلوب آن، باید بتدریج و پس از انتقادات و یادآوری‌های پیاپی بدست آید و انتظار می‌رود که این بزرگواران از این همکاری دریغ نورزند.

در این میان از استادان و دانشجویان ارجمند تقاضا می‌شود تا با همکاری، راهنمایی و پیشنهادهای اصلاحی خود، این گروه را در جهت ارائه دیگر آثار مورد نیاز جامعه دانشگاهی یاری دهند.

در خاتمه جای دارد تا از همکاری تمامی اعضاء گروه مهندسی - پژوهشی ساحر بخصوص برادر گرامی مهندس سعید هراتیان، مهندس آرتین هنرجیان و همچنین سرکار خانم مهندس عاطفه شیخ‌پوری که در این حرکت و تلاش ما را همراهی نمودند، تشکر و قدردانی نمایم.

مدیر گروه مهندسی - پژوهشی ساحر
مهرداد توانا

فهرست

۱۵	۱ پاسخ به حملات
۱۶	کابوس پاسخ به وقایع
۱۷	روز اول: دستیابی غیرمجاز
۱۸	روز دوم: مشکل حل شد
۱۸	روز سوم: دوباره شکافی در امنیت ایجاد شد
۱۹	روزهای چهارم تا هفتم: گزارش واقعه به مقامات رده بالا
۱۹	روز هشتم: برای بدست آوردن شواهد، بسیار دیر شده است
۱۹	روز نهم: آدم بده چه کسی بود؟
۲۰	خلاصه: حملات درونی
۲۱	کاری کنیم به آنجا نرسیم که
۲۱	تمرکز روی پیشگیری
۲۴	خود را برای بدترین حالت آماده کنید
۲۸	به سرعت و با تصمیم گیری، واکنش نشان دهید
۳۰	لیست پرسشها
۳۱	کلام آخر

۳۵	۲ امنیت Out-of-the-Box
۳۶	بعداً با امنیت برخورد کنید
۳۷	روز اول: حسن اشتباه امنیت داشتن
۳۷	دو سال بعد: متوجه حمله شدند
۳۸	+ دو هفته بعد: نفوذ گر برگشته است
۳۸	+ سه سال بعد: اصلاح کردن امنیت
۴۰	داستان ادامه دارد: شبکه همچنان در معرض خطر قرار دارد
۴۱	خلاصه: آیا شما از این ISP استفاده خواهید کرد؟
۴۲	کاری کنیم به آنجا نرسیم که
۴۲	ریسکهای خود را بشناسید
۴۳	از نصیهای بدون امنیت خودداری کنید
۴۳	شبکه خود را امتحان کنید
۴۴	افرادی که از داده های شما خبر دارند را بشناسید
۴۵	بودجه لازم را برای امنیت اختصاص دهید یا بدست آورید
۴۶	به همه مجوز خواندن اتوشتن ندهید
۴۶	Accountهای قدیمی را حذف کنید

فهرست
مطالب

۴۷	 کلمات عبور را امتحان کنید.
۴۷	 Patch های امنیتی را بکار ببرید.
۴۷	 از سیاستها و رویه ها پیروی کنید.
۴۸	 با کارشناسان کار کنید.
۴۸	 از آموزش استفاده کنید.
۴۹	 لیست پرسشها.
۵۰	 کلام آخر.

۵۳	 ۳ پشتیبانی اجرایی
۵۴	 تعهد اجرایی
۵۵	 روز اول: سیستمهای ایمن نشده.
۵۶	 یک سال بعد: دستیابی غیرمجاز ادامه می یابد.
۶۱	 خلاصه: روش فعالی را در پیش بگیرید.
۶۲	 کاری کنیم به آنجا نرسیم که
۶۲	 تعهد به امنیت از بالا به پایین
۶۲	 امنیت را محول نکنید
۶۲	 سطوح مدیریت را به حداقل برسانید.
۶۳	 به مدیریت اجرایی گزارش دهید.
۶۴	 امنیت را بتوان یکی از اهداف شرکت معرفی کنید.
۶۴	 در صورت لزوم، آموزش دهید یا آموزش ببینید.
۶۶	 اطمینان حاصل کنید که تمام مدیران، امنیت را درک کرده اند.
۶۶	 بصورت شفاف و روشن با مدیریت ارتباط برقرار کنید.
۶۶	 لیست پرسشها.
۶۷	 کلام آخر.

۷۱	 ۴ دستیابی به شبکه
۷۲	 اتصالاتهای شریک تجاری
۷۳	 روز اول: معماری امنیت.
۷۳	 چند هفته بعد: سیاست نصب امنیت.
۷۳	 روز بعد: چه کسی مسئول امنیت است.
۷۳	 ۲۹ روز بعد: یک نفوذگر کنترل را بدست می گیرد.
۷۴	 + در طی یک ماه: یک تست امنیتی زمان بندی نشده.
۷۵	 روز اول بررسی: نقشه های شبکه مطالب زیادی را بازگو می کنند.
۷۷	 روز دوم بررسی: سیاستهای اجرا نشده.
۷۸	 آخرین روز بررسی: پذیرفتن مسئولیت امنیت.
۸۰	 خلاصه: از رقابت دوری کنید.
۸۱	 کاری کنیم به آنجا نرسیم که
۸۱	 از طراحی های معماری استاندارد استفاده کنید.

فهرست مطالب

۸۲	اتصالهای خارجی را ردیابی کنید
۸۲	مسئولیت قلمرو خود را بعهده بگیرید
۸۳	کاری کنید که اتصالهای خارجی تأیید بخواهند
۸۳	سیاستها و رویه‌ها را اجرا کنید
۸۳	سرویسهای غیر ضروری را غیر فعال کنید
۸۴	بر اهمیت آموزش تأکید کنید
۸۴	پیگیری کنید
۸۴	سیستمهای ایمن نشده را به اینترنت وصل نکنید
۸۵	لیست پرسشها
۸۵	کلام آخر

۵ آموزش امنیت

۹۰	دست‌کم گرفتن آموزش
۹۱	تماس اولیه: تست امنیت
۹۱	روز اول: جمع‌آوری اطلاعات
۹۳	روز دوم: تست کردن سیستمها
۹۶	روز سوم: آموزش امنیت از بودجه خارج شد
۹۷	خلاصه: حتماً در مورد آموزش سرمایه‌گذاری کنید
۹۸	کاری کنیم به آنجا نرسیم که
۹۹	آموزش به مدیریت اجرایی
۹۹	محافظت از بودجه آموزش امنیتی
۹۹	تبدیل امنیت به یک ضرورت مدیریتی
۹۹	تبدیل امنیت به یک ضرورت برای مدیر سیستم
۱۰۰	شرکت در سمینارهای امنیتی
۱۰۰	کنفرانس در هنگام صرف غذا
۱۰۰	انتشار اطلاعات امنیتی
۱۰۱	ملحق شدن به لیستهای امنیتی
۱۰۱	نوشتن مقاله
۱۰۱	نوشتن خبرنامه‌ها
۱۰۱	ابزارهایی را در داخل محصولات خود بگنجانید
۱۰۱	لیست پرسشها
۱۰۲	کلام آخر

۶ امنیت طرح‌ریزی نشده

۱۰۵	طرح‌گذر
۱۰۶	روز اول: بررسی امنیت
۱۰۸	شناخت خطر
۱۰۹	فاز اول: امنیت فیزیکی

فهرست مطالب

۱۱۰	فاز دوم: در دست گرفتن کنترل‌های فیزیکی پیشین
۱۱۱	فاز سوم: دسترسی غیرمجاز
۱۱۲	روز دوم: اطلاعات شخصی در خطر قرار دارند
۱۱۴	خلاصه: در ارائه پلان کاری خود به دیگران ماقب باشید
۱۱۵	کاری کنیم به آنجا نرسیم که ...
۱۱۵	ارزیابی خطرات
۱۱۵	طبقه‌بندی سیستمها
۱۱۶	از نصبهایی که در آنها امنیت لحاظ نشده است، جلوگیری کنید
۱۱۶	از ایجاد اعتمادهای بیش از حد ممانعت کنید
۱۱۶	از تجربیات گذشتگان استفاده نمایید
۱۱۶	بودجه اختصاص داده شده را کم نکنید
۱۱۷	بررسی‌های امنیتی را اعمال نمایید
۱۱۷	مدیریت را پاسخگو نگهدارید
۱۱۷	خودتان را بزرگتر از آنچه که هستید نشان ندهید
۱۱۸	بودجه‌ای را برای آموزش تعیین کنید
۱۱۸	بالا بردن امتیاز
۱۱۸	لیست پرسشها
۱۱۹	کلام آخر

۷ (حفظ) نگهداری امنیت

۱۲۳	مسئول امنیت
۱۲۴	روز اول: دور نگه داشتن افراد بد
۱۲۵	روز دوم: مدیر دیواره آتش
۱۲۶	امنیت موقت
۱۲۷	مدیریت و امنیت
۱۲۸	جدی بودن درباره پشتیبانی از امنیت
۱۲۹	آخرین روز کار من: عادت‌ها می‌توانند حرف‌های زیادی را بزنند
۱۳۰	خلاصه: نرسید که امنیت شرکت شما چه منفعتی برای شما دارد
۱۳۱	کاری کنیم به آنجا نرسیم که ...
۱۳۲	تعریف وظایف و مسئولیتها
۱۳۳	سیاستها و رویه‌های دیواره آتش را توسعه دهید
۱۳۳	دیواره آتش خود را تغذیه نمایید
۱۳۳	Audit log های خود را بخوانید
۱۳۴	از نرم‌افزار اکتشاف (detection) استفاده نمایید
۱۳۴	به سرعت واکنش نشان دهید
۱۳۵	نیازمندیهای امنیتی را لحاظ کنید
۱۳۵	نظارت‌ها را هدایت نمایید
۱۳۵	اطلاعات به روز را کسب کنید

فهرست مطالب

لیست پرسشها	۱۳۶
کلام آخر	۱۳۶

۸ امنیت شبکه داخلی

شبکه ناامن	۱۴۲
در ابتدا: دور زدن (bypass) شبکه رسمی	۱۴۳
روز اول: جمع آوری اسناد	۱۴۳
روز دوم: مدیران سیستم در برابر تیم امنیتی	۱۴۶
چه کسی مالک امنیت است	۱۴۷
انتقال مسئولیت	۱۴۷
خلاصه: امنیت لازمه هر جنگی است	۱۴۸
شخصی را عهده دار سیاستها و رویه ها نمایید	۱۴۹
طرح پشتیبانی امنیتی میان سازمانی	۱۴۹
منتظر معجزه نباشید	۱۴۹
فرایند سوال	۱۵۰
زمان تسلیم شدنتان را بدانید	۱۵۰
مسئولیت بپذیرید	۱۵۰
لیست پرسشها	۱۵۱
کلام آخر	۱۵۱

۹ وضعیت امنیت در صورت محول کردن وظایف به یک شرکت طرف سوم (third-party)

سوم (third-party)	۱۵۵
آیا باید امنیت را فراموش نمود	۱۵۶
روز اول: نگاهی به کنترلهای امنیتی	۱۵۷
روز دوم: اتصالات شبکه	۱۵۸
اشتباهات امنیتی حیرت آور	۱۵۹
پشتیبانی آموزش داده نشده و تجربه نشده	۱۶۱
روزهای سوم و چهارم: آیا مدیریت می فهمد	۱۶۲
خلاصه: سیستمهای واگذار شده (outsourced) باید ایمن گردند	۱۶۲
کاری کنیم به آنجا نرسیم که	۱۶۳
هدایت ارزیابیهای امنیتی	۱۶۳
نظارت را بدرستی انجام بدهید	۱۶۳
نظارت را به طور منظم انجام دهید	۱۶۳
مسائلی را که می یابید تصحیح نمایید	۱۶۴
از روش آزمون و خطا استفاده نکنید	۱۶۴
لیست پرسشها	۱۶۵
کلام آخر	۱۶۶

فهرست
مطالب

فهرست مطالب

۱۶۹	۱۰ ایمیل ناامن (Unsecure Email)
۱۷۰	Email یا See Mail ؟
۱۷۰	دسترسی به داده های شخصی
۱۷۱	خلاصه: حق برخورداری از حریم خصوصی را دارید
۱۷۲	کاری نکنید به آنجا برسیم که
۱۷۳	استفاده از رمزنگاری!
۱۷۳	شرکت خود را تشویق به رمزنگاری نمایید
۱۷۳	رمزنگاری را به بودجه امنیتی خود اضافه کنید
۱۷۳	مواظب خطرات دیگر ایمیل باشید
۱۷۴	کلام آخر
۱۷۷	۱۱ نگرستن به گذشته: دیدن آینده
۱۷۸	به خطر انداختن شرکت
۱۸۰	وظایف قانونی مربوط به حفاظت از اطلاعات و شبکه ها
۱۸۶	نوآوری های تجاری و اهداف شرکتی
۱۸۷	تهدیدات نیازمند عکس العمل می باشند
۱۹۳	۱۲ یک نفوذگر در داخل شبکه به گشت وگذار می پردازد
۱۹۴	اطلاعات شخصی یک نفوذگر
۱۹۵	نفوذگرهای واقعی
۱۹۶	مطالبی درباره ابزارهای نفوذگرها
۱۹۷	قدم زدن با یک نفوذگر
۱۹۸	نفوذگر چه کاری را انجام می دهد
۲۲۸	نتیجه گیری
۲۲۹	ضمیمه A شناخت مردم و محصولات
۲۲۹	سازمانهای مرتبط با امنیت
۲۳۳	منابع امنیتی
۲۳۳	آرشیوهای آسیب پذیری امنیت (Security Vulnerability Archives)
۲۳۴	لیستهای پستی محبوب
۲۳۴	بنگاه های مشورتی
۲۳۶	تحقیق در مورد جرایم امنیتی
۲۳۷	بیمه کردن تکنولوژی اطلاعات
۲۳۷	نرم افزارهایی که شما باید درباره آنها مطالبی را بدانید
۲۴۲	عرضه کنندگان محصولات

توانائی کشف کردن، جلوگیری کردن و از ریشه درآوردن حوادث بد در خیلی موارد همانند خنثی کردن بمب می باشد - هرچقدر زودتر و بهتر این کار را انجام دهید، اثرات مخرب امنیتی کمتری ایجاد خواهد شد.

Gene Schultz، مهندس ارشد

www.ketab

پند
استاد