



مدل‌های سازمانی برای تیم‌های پاسخگو به حوادث رایانه‌ای

مترجمان:

رضا انتظارشیشتری

حسن زاده جعفراسدی

امیر صمدی



گروه
صنایع
امنیت فاوا
صا ایران



انستیتو ایز ایران

عنوان و نام پدیدآور: مدل‌های سازمانی برای تیم‌های پاسخگو به حوادث رایانه‌ای (تألیف جورجیا کیلکرس... و دیگران) مترجمان: رضا انتظارشبهستری، حسن زاده جعفراسدی، امیر صمدی.
 مشخصات نشر: تهران: انستیتو ایز ایران، ۱۳۹۰.
 مشخصات ظاهری: ۱۴۲ ص: جدول.
 شابک: ۹۷۸-۹۶۴-۲۰۱-۰۴۸-۶
 وضعیت فهرست نویسی: فیا
 یادداشت: کتاب حاضر ترجمه مقاله‌ای با عنوان «Organizational models for computer security incident response teams (CSIRTs)» است.
 موضوع: کامپیوترها -- ایمنی اطلاعات
 موضوع: شبکه‌های کامپیوتری -- اقدامات امنیتی
 موضوع: جرایم کامپیوتری -- پی‌جویی
 شناسه افزوده: کیلکرس، جورجیا
 Killcrece, Georgia
 شناسه افزوده: زاده جعفراسدی، حسن، ۱۳۵۵ - مترجم
 شناسه افزوده: صمدی، امیر، ۱۳۵۸ - مترجم
 رده بندی کنگره: ۹۷۸/۹۶۴/۲۰۱/۰۴۸/۶ م ۳۶ ۱۳۹۰
 رده بندی دیویی: ۰۰۵۸۸
 شماره کتابشناسی ملی: ۲۴۰۴۲۸



- ۱ نام کتاب: مدل‌های سازمانی برای تیم‌های پاسخگو به حوادث رایانه‌ای
 ۲ مترجمان: رضا انتظارشبهستری، حسن زاده جعفراسدی، امیر صمدی
 ۳ نوبت چاپ: اول - پاییز ۱۳۹۰
 ۴ شمارگان: ۲۰۰۰ جلد
 ۵ قیمت: ۴۵۰۰ تومان
 ۶ شابک: ۹۷۸-۹۶۴-۲۰۱-۰۴۸-۶
 ۷ ناظر چاپ: علی نورا، اوغلی
 ۸ طراح جلد: مرتضی محمد صادقی

کلیه حقوق قانونی و شرعی برای ناشر محفوظ است.
 تکثیر تمام یا قسمتی از این اثر بصورت حرفه‌چینی و چاپ مجدد، چاپ افست، پلی‌کپی، فتوکپی و انواع دیگر چاپ ممنوع است. نقل مطالب به صورت معمول در مقاله‌های تحقیقاتی با ذکر نام کامل ناشر و کتاب آزاد است.

ناشر از همکاری گروه صنایع امنیت فاوا صالیران در چاپ این کتاب به منظور توسعه فناوری اطلاعات و ارتباطات در کشور قدردانی می‌کند.

خیابان میرداماد - خیابان شهید حساری (رازان جنوبی) پ ۳۶

تلفن: ۲۲۲۵۴۰۷۸، شماره: ۲۲۲۵۲۶۵

www.isishop.ir

www.isibook.ir

نمایندگان پخش

۰۲۱-۶۶۴۴۰۹۲۲
 ۰۲۱-۶۶۹۷۳۱۷۵
 ۰۲۱-۸۸۲۰۰۹۷۲
 ۰۶۱۰-۲۲۱۷۰۰۰

انتشارات آگاه
 مهریان
 مرکز تحقیقات صنعتی
 رشد امواز

۰۲۱-۶۶۵۶۵۳۳۶
 ۰۲۱-۶۶۴۰۱۵۴۳
 ۰۲۱-۶۶۵۶۹۸۸۱
 ۰۲۱-۸۸۹۴۰۳۰۳

انتشارات آتی نگر
 به نشر آستان قدس
 سپا دانش
 پکتا

معرفی گروه صافاوا

در بهار ۱۳۸۶ به دنبال انتزاع دو مجموعه صنعت امنیت مخابرات از شرکت صنایع مخابرات با بیش از ۲۰ سال سابقه طراحی و تولید انواع رمز کننده‌های صوت و دیتا در حوزه امنیت مخابرات و مراکز امنیت نرم افزار و سخت افزار از شرکت ایزایران با سابقه ۵ ساله در تأمین و ارائه خدمات امن‌سازی بومی نرم افزارها، سخت افزارها و امنیت شبکه‌های رایانه‌ای در حوزه امنیت فناوری اطلاعات و تجمع این دو، مجموعه‌ای تحت عنوان گروه صنایع امنیت فناوری اطلاعات و ارتباطات (صافاوا) به عنوان ششمین مجموعه وابسته به صایران ایجاد گردید.

این الحاق موجب رشد هر دو صنعت، ادغام و تقویت متمرکز برخی امور و مأموریت‌های موازی و نیز بهره‌مندی متقابل از توانمندی‌های یکدیگر و نهایتاً ارتقای جایگاه و مأموریت امنیت در بین شرکتهای صایران را فراهم ساخته است.

محصولات و خدمات این گروه در پنج حوزه تکنولوژی امنیت ارتباطات، امنیت فناوری اطلاعات، رمزنگاری، کنترل امنیت و ارزیابی سامانه‌های نرم افزاری به متقاضیان عرضه می‌گردد.

معرفی مرکز مهار

باتوجه به گسترش شبکه‌های رایانه‌ای حوادث، آسیب پذیریها و بدافزارها به صورت چشم‌گیری افزایش یافته است. با بروز یکی از موارد فوق مهمترین دغدغه سازمان‌ها داشتن قابلیت تشخیص، تحلیل و پاسخگویی سریع و موثر به آن، محدود کردن دامنه خرابی‌ها و بازیافت کم هزینه اطلاعات است. یکی از راهکارهایی که بسیاری از سازمان‌ها در راهبردهای امنیتی خود منظور نموده‌اند، ایجاد تیم‌های پاسخگویی به حوادث امنیت رایانه‌ای (CERT) است. لذا گروه صنایع امنیت فواصاایران در راستای ایجاد یک نقطه کانونی در سطح وزارت دفاع و پشتیبانی نیروهای مسلح اقدام به ایجاد مرکزی با عنوان «مقابله هماهنگ امنیت رایانه‌ای» یا به اختصار «مهار» نموده است.

مرکز مهار گروه صافاوا با بهره‌گیری از دانش روز دنیا قادر به تشخیص، تحلیل و پاسخگویی به حوادث، آسیب‌پذیری‌ها و بدافزارهای رایانه‌ای است، همچنین توانایی ایجاد و راه‌اندازی تیم‌های پاسخگویی به حوادث امنیت رایانه‌ای را در سازمان‌های مختلف داراست و ضمن نظارت، قادر به پشتیبانی از آن نیز می‌باشد.

فهرست مطالب

پیشگفتار..... ۱

فصل اول: درباره کتاب

مقدمه.....	۳
۱-۱- هدف این کتاب.....	۵
۲-۱- مخاطبین کتاب.....	۶
۳-۱- این کتاب چگونه باید مورد استفاده قرار بگیرد.....	۷
۴-۱- فصول کتاب.....	۸

فصل دوم: ایجاد توانمندی CSIRT

۱-۲- خلاصه.....	۱۱
۲-۲- موانع در ایجاد یک تیم جدید.....	۱۲
۳-۲- مثال‌هایی از تیم‌های موجود.....	۱۴
۴-۲- نام‌ها چه هستند؟.....	۱۵
۵-۲- تعیین جامعه قلمرو CSIRT.....	۱۷
۶-۲- تعریف مأموریت CSIRT.....	۱۸
۷-۲- تعیین خدمات CSIRT.....	۱۸
۱-۷-۲- خدمات واکنشی.....	۲۱
۲-۷-۲- خدمات پیشگیرانه.....	۲۶
۳-۷-۲- خدمات هسته CSIRT.....	۳۳
۴-۷-۲- پیشنهاد توسعه خدمات.....	۳۴
۱-۵-۷-۲- ایجاد خدمات جدید روی خدمات موجود.....	۳۶
۲-۵-۷-۲- ایجاد جوامع قلمرو جدید مطابق با خدمات موجود.....	۳۹

فصل سوم: پیاده سازی CSIRTs

۱-۳- مرور کلی.....	۴۳
۲-۳- مدل‌های سازمانی معمول برای CSIRTs.....	۴۳

۴۶	۳-۳- سایر موضوعات
۴۶	۳-۳-۱- غربالگری (Triage)
۴۹	۳-۳-۲- اختیارات
۵۱	۳-۳-۳- تیمهای موجود در یک سازمان
۵۲	۳-۴- مقایسه مدل‌های سازمانی
۵۲	۳-۴-۱- مرور کلی
۵۲	۳-۴-۲- جوامع قلمرویی که مدل پشتیبانی میکند
۵۲	۳-۴-۳- ساختار سازمانی
۵۳	۳-۴-۴- غربالگری
۵۳	۳-۴-۵- خدمات موجود
۵۳	۳-۴-۶- منابع
۵۳	۳-۴-۷- نقاط قوت و ضعف مدل

فصل چهارم: تیم امنیتی

۵۵	۴-۱- مرور کلی
۵۶	۴-۲- جامعه قلمرویی که این مدل پشتیبانی می‌کند
۵۷	۴-۳- ساختار سازمانی
۵۸	۴-۴- غربالگری
۵۹	۴-۵- خدمات موجود
۵۹	۴-۵-۱- خدمات اصلی (هسته)
۶۴	۴-۵-۲- خدمات اضافی
۶۷	۴-۶- منابع
۶۷	۴-۶-۱- نیروی انسانی
۶۷	۴-۶-۲- تجهیزات
۶۸	۴-۶-۳- زیرساخت
۶۸	۴-۷- نقاط قوت و ضعف این مدل

فصل پنجم: CSIRT توزیع شده داخلی

۷۱	۵-۱- مرور کلی
----	---------------

۷۲	۲-۵- جامعه قلمرو این مدل
۷۲	۳-۵- ساختار سازمانی
۷۷	۴-۵- غربالگری
۷۷	۵-۵- خدمات موجود
۷۸	۱-۵-۵- خدمات اصلی
۸۱	۲-۵-۵- خدمات اضافی
۸۶	۶-۵- منابع
۸۶	۱-۶-۵- کارکنان
۸۸	۲-۶-۵- تجهیزات
۸۸	۳-۶-۵- زیرساخت
۸۹	۷-۵- نقاط قوت و ضعف این مدل

فصل ششم: CSIRT متمرکز شده داخلی

۹۱	۱-۶- مرور کلی
۹۲	۲-۶- جامعه قلمرو این مدل
۹۳	۳-۶- ساختار سازمانی
۹۴	۴-۶- غربالگری
۹۴	۵-۶- خدمات موجود
۹۴	۱-۵-۶- خدمات اصلی
۹۹	۲-۵-۶- خدمات اضافی
۱۰۱	۶-۶- منابع
۱۰۱	۱-۶-۶- کارکنان
۱۰۳	۲-۶-۶- تجهیزات
۱۰۳	۳-۶-۶- زیرساخت
۱۰۴	۷-۶- نقاط قوت و ضعف این مدل

فصل هفتم: CSIRT ترکیبی

۱۰۵	۱-۷- مرور کلی
۱۰۶	۲-۷- جامعه قلمرو این مدل

- ۳-۷- ساختار سازمانی ۱۰۷
- ۴-۷- غربالگری ۱۰۸
- ۵-۷- خدمات موجود ۱۰۹
- ۱-۵-۷- خدمات اصلی ۱۰۹
- ۲-۵-۷- خدمات اضافی ۱۱۳
- ۶-۷- منابع ۱۱۵
- ۱-۶-۷- کارکنان ۱۱۵
- ۲-۶-۷- تجهیزات ۱۱۶
- ۳-۶-۷- زیرساخت ۱۱۶
- ۷-۷- نقاط قوت و ضعف این مدل ۱۱۷

فصل هشتم: مدل CSIRT هماهنگ کننده

- ۱-۸- مرور کلی ۱۱۹
- ۲-۸- جامعه قلمرو این مدل ۱۲۰
- ۳-۸- ساختار سازمانی ۱۲۱
- ۴-۸- غربالگری ۱۲۲
- ۵-۸- خدمات موجود ۱۲۲
- ۱-۵-۸- خدمات اصلی ۱۲۲
- ۲-۵-۸- خدمات اضافی ۱۲۶
- ۶-۸- منابع ۱۲۷
- ۱-۶-۸- کارکنان ۱۲۷
- ۲-۶-۸- تجهیزات ۱۲۸
- ۳-۶-۸- زیرساخت ۱۲۸
- ۷-۸- نقاط قوت و ضعف این مدل ۱۲۹

فصل نهم: انتخاب مدل صحیح CSIRT برای یک سازمان

- ۱-۹- آیا تیم شما در این کتاب توضیح داده شده است؟ ۱۳۲
- ۲-۹- آیا شما یک تیم امنیتی هستید؟ ۱۳۲
- ۳-۹- آیا شما یک CSIRT هماهنگ کننده هستید؟ ۱۳۳

۹-۴- آیا شما یک CSIRT داخلی هستید؟ ۱۳۳

فصل دهم: ملاحظات نهایی

فصل یازدهم: خلاصه خدمات پشتیبانی

منابع و مواخذ ۱۴۲

www.ketab.ir

پیشگفتار

امروزه، توانایی پاسخگویی به حوادث امنیتی به صورت متمرکز در بسیاری از سازمان‌ها وجود ندارد و هر قسمت، حوادث امنیتی را که به طور خاص برای آن قسمت اتفاق می‌افتد رسیدگی می‌کند. با توجه به افزایش حوادث امنیت رایانه‌ای و نبود یک رویکرد هماهنگ و سریع برای پاسخگویی به این حوادث، نیاز به یک تیم رسمی برای مقابله با اینگونه حوادث احساس می‌شود. دیگر انگیزه‌هایی که منجر به ایجاد تیم پاسخگو به حوادث امنیتی رایانه‌ای (CSIRT) می‌شود، عبارتند از:

- افزایش تعداد و نوع سازمان‌هایی که تحت تأثیر حوادث امنیتی رایانه‌ای قرار می‌گیرند.
- آگاهی سازمان‌ها در مورد نیاز به سیاست‌های امنیتی و پرداختن به آن به عنوان بخشی از استراتژی کلی خود در مدیریت ریسک.
- قوانین و مقررات جدید که بر نیاز سازمان‌ها برای حفاظت از دارایی‌های اطلاعاتی خود اثر می‌گذارد.
- درک این مهم که مدیران شبکه و سیستم به تنهایی قادر به محافظت از سیستم‌ها و دارایی‌های سازمانی نیستند.

کتاب «مدل‌های سازمانی برای تیم‌های پاسخگو به حوادث رایانه‌ای (CSIRTs)» به عنوان یکی از منابع اصلی در زمینه ایجاد قابلیت پاسخگویی به حوادث در سازمان‌ها و مدیریت CSIRTs مورد استفاده قرار گرفته است. نسخه اصلاح شده این کتاب در سال ۲۰۰۳ منتشر گردید، اما بسیاری از مطالب این کتاب به طور عمیق پوشش داده نشده است. یکی از این مطالب که نیاز به بررسی بیشتری دارد، انتخاب مدلی صحیح برای قابلیت پاسخگویی به حوادث در یک سازمان است که موضوع اصلی کتاب «مدل‌های سازمانی برای CSIRTs» می‌باشد.

این کتاب بر ساختارهای سازمانی مختلف جهت ایجاد یک CSIRT صرف نظر از حوزه فعالیت (تجاری، آموزشی، دولتی و یا نظامی) یا وسعت فعالیت (درون سازمانی یا برون سازمانی) تمرکز دارد. علاوه بر این جهت طراحی و ایجاد یک CSIRT مفید بوده و به منظور ارتقاء فعالیت‌های یک CSIRT نیز می‌تواند مورد استفاده قرار بگیرد.

رئیس گروه صنایع امنیت فاوا صایران

بهمن آصفی