بسم الله الرحمن الرحیم

مدل‌های سازمانی برای تیم‌های پاسخگو به حوادث رایانه‌ای

مترجمان:

رضا انتظارشبستری

حسن زاده‌جعفراسدی

امیر صمدی

انستیتوایزایران

گروه صنایع امنیت فاوا صاایران

عنوان و نام پدیدآور: مدل‌های سازمانی برای تیم‌های پاسخگو به حوادث رایانه‌ای/[تالیف جورجیا کیلکرس ...[و دیگران] ؛ مترجمان- رضا انتظارشبستری،حسن زاده‌جعفراسدی،امیر صمدی.
مشخصات نشر: تهران: انستیتو ایز ایران، ۱۳۹۰.
مشخصات ظاهری: ۱۴۲ص.: جدول.
شابک : ۶-۴۸-۰۲۰۱-۹۶۴-۹۷۸
وضعیت فهرست نویسی: فیپا
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 تامینی
موضوع: جرایم کامپیوتری — پی‌جویی
شناسه افزوده: کیلکرس، جورجیا
شناسه افزوده: Killcrece, Georgia
شناسه افزوده: زاده‌جعفر اسدی، حسن، ۱۳۵۵ - ، مترجم
شناسه افزوده: صمدی، امیر، ۱۳۵۸ - ، مترجم
رده بندی کنگره: QA۷۶/۹/ک۹ م۳۶ ۱۳۹۰
رده بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی: ۲۴۰۴۴۲۸

انتشارات انستیتو ایز ایران

- **نام کتاب:** ..... مدل‌های سازمانی برای تیم‌های پاسخگو به حوادث رایانه‌ای
- **مترجمان:** ..... رضا انتظارشبستری، حسن زاده‌جعفراسدی، امیر صمدی
- **نوبت چاپ:** ..... اول - پاییز ۱۳۹۰
- **شمارگان:** ..... ۲۰۰۰ جلد
- **قیمت:** ..... ۴۵۰۰ تومان
- **شابک:** ۹۷۸-۹۶۴-۲۰۱-۰۴۸-۶
- **ناظر چاپ:** ..... علی نورا... اوغلی
- **طراح جلد:** ..... مرتضی محمد صادقی

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

خیابان میرداماد- خیابان شهید حصاری (رازان جنوبی) پ ۳۶
تلفن: ۲۲۲۵۴۰۷۸ نمابر: ۲۲۲۲۵۲۶۵
www.isibook.ir www.isishop.ir

□نمایندگان پخش

○انتشارات آتی نگر	۰۲۱-۶۶۵۶۵۲۳۶	○انتشارات آگاه	۰۲۱-۶۶۴۶۰۹۳۲
○به نشر آستان قدس	۰۲۱-۶۶۴۰۱۵۴۳	○مهریان	۰۲۱-۶۶۹۷۳۱۷۵
○سها دانش	۰۲۱-۶۶۵۶۹۸۸۱	○مرکز تحقیقات صنعتی	۰۲۱-۸۸۳۰۰۹۷۲
○پکتا	۰۲۱-۸۸۹۴۰۳۰۳	○رشد اهواز	۰۶۱۱-۲۲۱۷۰۰۰

معرفی گروه صافاوا

در بهار۱۳۸٦ 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 تجمیع این دو، مجموعه‌ای تحت عنوان گروه صنایع امنیت فناوری اطلاعات و ارتباطات (صافاوا) به عنوان ششمین مجموعه وابسته به صاایران 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 صاایران 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 فاواصاایران 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

فصل چهارم: تیم امنیتی

فصل پنجم: CSIRT توزیع شده داخلی

فصل ششم: CSIRT متمرکز شده داخلی

فصل هفتم: CSIRT ترکیبی

فصل هشتم: مدل CSIRT هماهنگ کننده

فصل نهم: انتخاب مدل صحیح CSIRT برای یک سازمان

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. باتوجه 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 برنیاز 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 صاایران

بهمن آصفی