عنوان مقاله:
ایجاد و مدیریت تیم واکنش به حوادث امنیتی رایانه ای

محل انتشار:
هشتمین کنفرانس ملی فرماندهی و کنترل ایران (C4I) (سال: 1393)

تعداد صفحات اصل مقاله: 4

نویسندگان:
پژمان غلام نژاد - *دانشگاه هوایی شهید ستاری دانشکده مهندسی رایانه و فناوری اطلاعات*

احمد پاشایی - *دانشگاه هوایی شهید ستاری دانشکده مهندسی رایانه و فناوری اطلاعات*

خلاصه مقاله:
تیم واکنش به حوادث امنیتی رایانه ای یک سازمان خدماتی است که مسئولیت دریافت بررسی و واکنش به گزارش حادثه های امنیت کامپیوتر و فعالیت های مربوط به آن ها را برعهده دارد.خدمات انها معمولا برای حوزه تعریف شده است که می تواند یک منشاء نمونه و پیشرو برای یک بخش یا سازمان دولتی و یا به صورت یک نهاد و سازمان آموزشی برای یک منطقه یا کشور و یا حتی بصورت یک شبکه پژوهشی باشد تیم واکنش به حوادث امنیتی رایانه می تواند یک تیم رسمی و یا یک تیم موقتی باشد یک تیم رمی کار پاسخ واقعه را به عنوان وظیفه اصلی کار خود انجام می دهد.در این مقاله به نکات کلیدی در ایجاد و مدیریت یک تیم واکنش به حوادث امنیتی رایانه که در بعضی مواقع به عنوان یک تیم واکنش به حوادث رایانه ای و یا یک تیم واکنش اضطراری رایانه ای نامیده می شوند.بصورت خلاصه می پردازیم برخی از دسته بندی های کلی تیم واکنش به حوادث امنیتی رایانه شامل موارد زیر است:تیم واکنش به حوادث امنیتی رایانه داخلی که بررسی حوادث و ارائه حادثه خدمات به سازمان متبوع و مادر خود را برعهده دارد.که این می تواند یک تیم واکنش به حوادث امنیتی رایانه داخلی برای یک بانک یک شرکت تولیدی و یا کارخانه یک دانشگاه و یا یک آژانس بین المللی در یک کشور باشد.بعضی از نمونه هاعبارتند از مرکز هماهنگی و تیم مرکزی واکنش اضطراری رایانه ای ژاپن هماهنگ کننده یا تیم واکنش اضطراری رایانه ای سنگاپور.

کلمات کلیدی:
تیم واکنش به حوادث امنیتی رایانه ای ، تیم واکنش به حوادث رایانه ای ، تیم واکنش اضطراری رایانه ای ، مرکز هماهنگ کننده تیم واکنش اضطراری رایانه ای