

ارائه الگوی مناسب برای استقرار CSIRT در شرکت مخابرات استانها

مورد مطالعاتی: شرکت مخابرات استان لرستان

علی ناصری^۱، سمیه حجازی^{۲*}، نبی‌اله شمس‌فر^۳

۱- استادیار دانشگاه جامع امام حسین (ع)، ۲- کارشناسی ارشد مهندسی فناوری اطلاعات-گرایش تجارت الکترونیک، دانشگاه شیراز

۳- کارشناسی ارشد مهندسی برق - گرایش مخابرات، دانشگاه آزاد اسلامی واحد نجف آباد

(دریافت: ۸۹/۱۱/۲۷، پذیرش: ۹۱/۱۱/۱۴)

چکیده

با مطالعه مفاهیم پاسخگویی به حوادث امنیت رایانه‌ای و مراحل پیشنهادی CERT/CC برای توسعه تیم‌های پاسخگویی به حوادث امنیت رایانه‌ای، به مدل‌سازی این تیم برای شرکت مخابرات استان‌ها که هدف آن ارائه خدمات پاسخگو، پیشگیرانه و مدیریت کیفیت در حوزه امنیت شبکه در داخل و خارج شرکت است، پرداخته‌ایم. در این مدل‌سازی تحلیل وضع موجود و نیازمندی‌های فضای تبادل اطلاعات شرکت مخابرات لرستان، مبنای تصمیم‌گیری در خصوص ساختار و طرح پیاده‌سازی TCL-CERT بوده و این طرح مبنای توسعه خط مشی‌ها، رویه‌ها، طرح‌ها، نقش‌ها، مسئولیت‌ها، جریان‌های کاری و ارتباطات آن با CERTهای ملی است.

واژه‌های کلیدی :

قابلیت پاسخگویی به حوادث امنیتی کامپیوتری، تیم پاسخگویی به حوادث امنیتی کامپیوتری، تیم پاسخگویی اورژانس رایانه‌ای، مدیریت حادثه

APPLYING A MODEL FOR IMPLEMENTATION OF CSIRT IN PROVINCES ICT

Case Study :Lorestan province ICT

Ali Naseri, Somayeh Hejazi*,Nabi alah Shamsifar

Abstract

Studying the concepts underlying reactions to computer security events and the steps proposed by CERT/CC for development of teams responding to computer security events, we have modeled teams for provinces ICT. These teams provide reactive, proactive and security quality management services in network security areas at both the inside and outside of the provinces ICT. In this modeling, current state analysis and requirements of information transaction space of the provinces ICT provide the basis for establishing vision and implementation plan of the TCL-CERT. This plan provides the basis for the development of TCL-CERT policies, procedures, roles, responsibilities, work flows and relationship with national CERTs.

Keywords: CSIRT, CERT, TCL-CERT, Incident management

* Corresponding Author Email: somayehejazi@gmail.com