آزمایشگاه آپا

آگاهی‌رسانی، پشتیبانی و امداد در

حوزه امنیت سیستم‌عامل

دانشگاه صنعتی امیرکبیر

(با حمایت مرکز تحقیقات مخابرات ایران)

گروه مدیریت

جریانهای کاری مربوط به رویه حفاظت از زیرساختار در یک گروه پاسخگویی به حوادث کامپیوتری رسمی

FC_۸۷_۰۶_۰۳

تاریخ: ۸۷/۰۶

مشخصات سند			
نام سند: جریانهای کاری مربوط به رویه حفاظت از زیرساختار در یک گروه پاسخگویی به حوادث کامپیوتری رسمی			
کد فایل	**آخرین نسخه**	**تاریخ آخرین بازبینی**	**گروه**
FC_۸۷_۰۶_۰۳	۱،۱	۸۷/۰۸/۰۱۸	مدیریت

سابقه سندها			
نسخه	**تاریخ تنظیم**	**تنظیم‌کننده**	**توضیحات**
۱،۰	۸۷/۰۶/۰۴	خدیجه محمدزاده	ایجاد

چکیده

رویه محافظت در یک گروه پاسخگویی به حوادث کامپیوتری رسمی شامل رویه هایی در جهت جلوگیری از وقوع حملات و هم چنین رویه هایی در جهت کاهش اثر حملات در صورت بروز آنها است.در این گزارش، نمودارهای جریان کاری این رویه مورد بررسی قرار می گیرد.

فهرست مطالب

۱ حفاظت از زیرساختار ۱

۱-۱ نمودار جریان کاری رویه حفاظت از زیرساختار ۲

۲ منابع و مراجع ۸

فهرست شکلها

شکل ۱- نمودار جریان کاری حفاظت از زیرساختار ۲

فهرست جداول

جدول ۱-توضیح جریان کاری رویه حفاظت از یرساختار ۳

۱ حفاظت از زیرساختار

در دنیای امروز که ویروسها و کرمها به سرعت منتشر می‌شوند سازمان‌ها باید برای حفاظت از سیستم‌های خود از وقوع این فعالیتهای مخرب جلوگیری کنند. در مواردی همچون کرم Slammer یا Sobig در سال ۲۰۰۳ حملات قبل از آنکه یک پاسخ نرمال امکان پذیر باشد به وقوع پیوستند . در این موارد تنها پاسخ درست این است که از وقوع چنین اتفاقاتی جلوگیری شود.بعد از وقوع چنین اتفاقاتی باید از انتشار این کدهای مخرب جلوگیری شده و سیستم ترمیم گردد.

رویه محافظت شامل رویه‌هایی در جهت جلوگیری از وقوع حملات و هم‌چنین رویه‌هایی در جهت کاهش اثر حملات در صورت بروز آن‌ها است.

بخشی از پاسخ به یک حادثه مداوم و در حال پیشرفت و یا کاهش اثر یک حادثه، ایجاد تغییراتی در زیرساختار است این تغییرات شامل موارد زیر است:

- تغییر در فیلترهای دیوار آتش ، مسیریاب‌ها و سرورهای پست الکترونیک برای جلوگیری از ورود بسته های آلوده به زیرساختار
- به روزرسانی سیستم تشخیص نفوذ برای داشتن امضاهای جدید
- تغییر در پیکربندی سیستم برای قطع سرویس‌های پیش فرض
- نصب وصله‌هایی برای نرم افزارهای آسیب پذیر
- به روزرسانی نرم افزارهای پویش ویروس برای داشتن امضای حملات جدید

عملیات پیشگیرانه می‌تواند به شکلهای متفاوتی انجام شود از جمله:

- انجام بازرسیهای امنیتی برای تعیین آسیب‌پذیریها و دیگرارزیابی های زیر ساختار برای مشخص شدن هر گونه ضعف
- پیاده سازی بهترین استانداردها برای حفاظت مانند ISO۱۷۷۹۹ و یا استانداردهای دیگر

در زیر، لیستی از استانداردهایی که سازمان‌ها می‌توانند در جهت ایمن ساختن زیر ساختار خود از آن‌ها استفاده کنند آمده است:

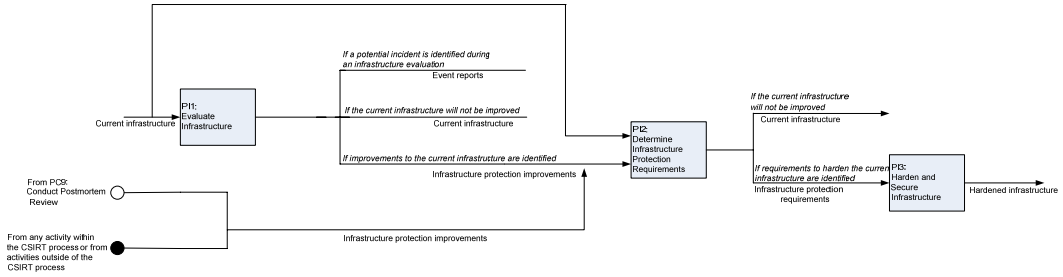
- ISO ۱۷۷۹۹/British Standard Institue ۷۷۹۹ part ۲
- Control Objectives for Information and related Technology (COBIT)
- Federal Financial Institutions Examination Council (FFIEC) Handbooks
- International Information Systems Security Certification Consortium ((ISC)) Certified Information Systems Security Professional (CISSP) Body of Knowledge
- Information Security Forum Best Practices
- Information Systems Security Association; Generally Accepted Information Security Principles (ISSA GAISP)
- Information Technology Governance Institute (ITGI) sources
- Information Technology Infrastructure Library (ITIL)

- National Institute of Standards and Technology (NIST) (selected SP ۸۰۰ series); Federal Information Processing Standards (FIPS) ۱۹۹
- National CyberSummit Task Force reports (draft)
- SEI body of work including Capability Maturity Model (CMM), Capability Maturity Model Integration (CMMI), OCTAVE, the Security Knowledge in Practice (SKiPSM) method, CERT Security Practices

به هر گروه پاسخگویی به حوادث کامپیوتری می‌توان به عنوان یک فراهم کننده معتبر اطلاعات ریسک ، با توجه به اطلاعاتی که از آنالیز انواع حملات در زیرساختار به دست می آورد ، نگاه کرد. از این اطلاعات می‌توان برای مشخص کردن استراتژیهایی حفاظتی استفاده نمود.پس کسانی که مسئولیت توسعه و نگهداری زیرساختار را بر عهده دارند می‌توانند از این اطلاعات استفاده کنند و این کار را با توجه به ریسکهاو حملات موجود انجام دهند.

رویه حفاظت که در دیاگرام نشان داده شده است شامل زیر رویه‌هایی برای ارزیابی زیر ساختار موجود (PI۱) و دریافت پیشنهاداتی برای پیشرفت رویه حفاظت، از جانب هر رویه ای در مدیریت حوادث یا در خارج از آن است. زمانی که پیشنهادات پیشرفت حفاظت مورد بررسی قرار گرفتند تغییراتی که باید اعمال شوند مشخص می گردند (PI۲) و پیاده سازی می‌شوند (PI۳). پیاده سازی شامل اعمالی در جهت ایمن ساختن زیر ساختار است. این اعمال می‌تواند شامل اضافه یا تغییر استحکاماتی نظیر دیوار آتش و سیستم تشخیص نفوذ؛ تغییرات پیکربندی کامپیوترهای میزبان، سرورها، مسیریاب‌ها؛ یا تغییر در سیاستهای مربوط به مدیریت حساب کاربران، امنیت فیزیکی، منابع انسانی و موارد مشابه باشد .

۱-۱ نمودار جریان کاری رویه حفاظت از زیرساختار



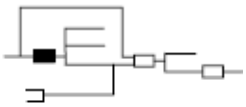
شکل ۱- نمودار جریان کاری حفاظت از زیرساختار

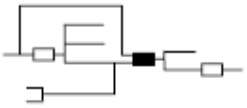
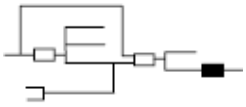
جدول ۱-توضیح جریان کاری رویه حفاظت از یرساختار

معیارهای اتمام	سیاستها و قوانین	نیازهای عمومی
• زمانی که امنیت زیرساختار کامپیوتری بهبود یافت.	• سیاستهای گروه پاسخگویی به حوادث کامپیوتری/ فناوری اطلاعات • معیارها، استانداردها، راهنماها، قوانین و دستورات مربوط به امنیت • سیاستهای امنیتی سازمان • سیاستهای سازمان که بر اعمال گروه پاسخگویی به حوادث کامپیوتری تاثیر گذار است.	• در زمانی که به بررسی امن اطلاعات حوادث نیاز است از رویه‌ها و تکنولوژیهای مناسب استفاده می شود. • نیروهای معین آموزشهای لازم در ارتباط با شغلی که می خواهند آن را انجام دهند دریافت می‌کنند. • نیروهای معینی، نتایج را مطابق با سیاستهای سازمان، مستندسازی می‌کنند. • نیروهای معینی با استفاده از متدها، ابزار و تکنولوژیهای موجود به حفاظت از زیرساختار می پردازند.

خروجیها			
تصمیم	**خروجی**	**توضیح**	**شکل**
زیرساختار موجود بهبود یافته است.	زیرساختار مستحکم	این مرحله شامل اعمال تغییراتی به گروه پاسخگویی به حوادث کامپیوتری است. حاصل این مرحله زیرساختاری است که در برابر حملات، آسیب‌پذیری کمتری دارد. این زیرساختار مستحکم	افراد، رویه‌ها و تکنولوژیها

		تمام نیازهای حفاظت از زیرساختار را برآورده می‌کند.	
زیرساختارموجود بهبود نیافته است	زیرساختار موجود	این مرحله، زیرساختار موجود را حفظ می‌کند.زیرساختار موجود شامل افراد، رویه‌ها و تکنولوژیها است.	افراد، رویه‌ها و تکنولوژیها
یک حادثه بالقوه از طریق بازبینی زیرساختار مشخص شده است.	گزارشات حادثه	این مرحله شامل گزارشات فعالیتهای غیرعادی یا مشکوک است که به رویه تشخیص حوادث ارسال می شود.	شفاهی، الکترونیکی یا فیزیکی

زیررویه	نیازمندیهای زیررویه	رویه‌های نوشته شده
PI۱ : ارزیابی زیرساختار 	• نیروهای معینی، زیرساختار کامپیوتری را ارزیابی می‌کنند و تصمیم می گیرند که چه کاری انجام دهند. (زیرساختار موجود را بهبود ببخشند، تغییری در زیرساختار موجود ندهند، یا زمانی که یک حادثه بالقوه تعیین شد گزارشی به رویه تشخیص حوادث ارسال کنند). ورودیها: زیرساختار موجود خروجیها: پیشرفت حفاظت از زیرساختار زیرساختار موجود گزارشات حوادث	• نیروهای معینی، رویه‌ها و متدلوژیهای سازمان را برای تعیین ریسکها و آسیب‌پذیریها دنبال می‌کنند. • نیروهای معینی راهنماها، رویه‌ها و قوانین حفاظت و ایمن سازی زیرساختار مربوط به سازمان‌های دیگر را مطالعه می‌کنند. • نیروهای معینی، راهنماها و رویه‌های مدیریت تغییرات سازمان یا گروه پاسخگویی به حوادث کامپیوتری را دنبال می‌کنند.

PI۲: تعیین نیازمندیهای حفاظت از زیرساختار 	• نیروهای معینی تغییرات پیشنهاد شده را مطالعه می‌کنندو تصمیم می گیرند که چه عملی باآن‌ها انجام دهند (تغییرات پیشنهاد شده را اعمال کنند یا کاری انجام ندهند.) ورودیها: زیرساختار موجود، پیشرفت حفاظت از زیرساختار خروجیها: زیرساختار موجود، نیازمندیهای حفاظت از زیرساختار	• نیروهای معینی رویه‌های سازمان برای مستندسازی نیازمندیهای حفاظت از زیرساختار را دنبال می‌کنند. • نیروهای معینی راهنماها، رویه‌ها و قوانین حفاظت و ایمن سازی زیرساختار مربوط به سازمان‌های دیگر را مطالعه می‌کنند. • نیروهای معینی ، راهنماها و رویه‌های مدیریت تغییرات سازمان یا گروه پاسخگویی به حوادث کامپیوتری را دنبال می‌کنند. • نیروهای معینی، معیارهای سازمان برای الویت دهی نیازمندیهای زیرساختار را دنبال می‌کنند.
PI۳: استحکام و ایمن سازی زیرساختار 	• نیروهای معینی نیازمندیهای حفاظت از زیرساختار را تامین می‌کنند تا امنیت زیرساختار موجود ارتقا یابد. ورودی: نیازمندیهای حفاظت از زیرساختار خروجی: زیرساختار مستحکم	• نیروهای معینی رویه‌های سازمان برای پیکربندی و نگهداری زیرساختار را دنبال می‌کنند. • نیروهای معینی راهنماها، رویه‌ها و قوانین حفاظت و ایمن سازی زیرساختار مربوط به سازمان‌های دیگر را مطالعه می‌کنند. • نیروهای معینی ، راهنماها و رویه‌های مدیریت تغییرات سازمان یا گروه پاسخگویی به حوادث

		کامپیوتری را دنبال می‌کنند • نیروهای معینی راهنماها و رویه‌های سازمان برای مدیریت پروژه را دنبال می‌کنند.

افراد مورد نیاز	تکنولوژیها
• از نیروهای زیر برای ارزیابی زیرساختار می‌توان استفاده کرد: - کارکنان فناوری اطلاعات (کارکنان مرکز اطلاعات شبکه [۱]، مرکز عملکردشبکه[۲] و مرکز عملکرد امنیت[۳] ، سرپرست سیستم و شبکه) - ماموران بازرسی، کارکنان مدیریت ریسک - ارزیابی کننده هایی از سازمان‌های دیگر - کارکنان گروه پاسخگویی به حوادث کامپیوتری	• این افراد می‌توانند از تکنولوژیهای زیر استفاده کنند: - ابزارهای پویش و تشخیص آسیب‌پذیریها (پویشگرهای شبکه) - ابزارهای تعیین ریسک - سیستم پایگاه داده - کانالهای ارتباطی (پست الکترونیک، ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب)
• نیروهای لازم برای تعیین نیازمندیهای حفاظت از زیرساختار می‌تواند شامل موارد زیر باشد: - کارکنان فناوری اطلاعات (کارکنان مرکز اطلاعات شبکه، مرکز عملکردشبکه و مرکز عملکرد امنیت، سرپرست سیستم و شبکه) - سازمان‌های دیگر(شرکتهای ثالث فراهم کننده سرویس امنیت، فراهم کنندگان سرویس اینترنت) - ماموران بازرسی، کارکنان مدیریت	• این افراد می‌توانند از تکنولوژی زیر استفاده کنند: - کانالهای ارتباطی (پست الکترونیک، ویدئو کنفرانس ،نرم‌افزارهای مورد استفاده گروه و وب)

[۱] Network Information Center (NIC)

[۲] Network Operations Center (NOC)

[۳] Security Operations Center (SOC)

ریسک - ارزیابی کننده هایی از سازمان‌های دیگر - کارکنان گروه پاسخگویی به حوادث کامپیوتری	
• از نیروهای زیر برای استحکام و ایمن سازی زیرساختار می‌توان استفاده کرد: - کارکنان فناوری اطلاعات (کارکنان مرکز اطلاعات شبکه، مرکز عملکردشبکه و مرکز عملکرد امنیت، سرپرست سیستم و شبکه) - سازمان‌های دیگر(شرکتهای ثالث فراهم کننده سرویس امنیت، فراهم کنندگان سرویس اینترنت ها) - کارکنان گروه پاسخگویی به حوادث کامپیوتری	• این افراد می‌توانند از تکنولوژیهای زیر برای استحکام و ایمن سازی زیرساختار استفاده کنند: - ابزارهای مدیریت سیستم و شبکه - سیستم پایگاه داده/بایگانی - کانالهای ارتباطی (پست الکترونیک، ویدئو کنفرانس، نرم‌افزارهای مورد استفاده گروهو وب)

۲ منابع و مراجع

۱. *A STEP-BY-STEP APPROACH ON HOW TO SET UP A CSIRT*. ۲۰۰۶, European Network and information Security Agency (ENISA). Available at www.enisa.europa.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA.pdf

۲. Albert,C , Dorofee,A ,Killcrece, G, Ruefle, R,Zajicek, M. *Defining Incident Management Processes for CSIRTS:A Work in Progress*. Available at www.cert.org/archive/pdf/۰۴tr۰۱۵.pdf

۳. Grance, T,Karent, k,Kim, B., *Computer Security Incident Handling Guide*.

۴. Killcrece, G.,Kossakowski ,K., Ruefle ,R.,Zajicek ,M., *State of the Practice of Computer Incident Response Teams (CSIRTs).* p. ۲۹۱.Available at www.cert.org/archive/pdf/۰۳tr۰۰۱.pdf

۵. Stikvoort, D,Kossakowski, K,Killcrece, G,Ruefle, R,Zajicek, M. *Handbook for Computer Security Incident Response Teams(CSIRTs)*.Available at www.cert.org/archive/pdf/csirt-handbook.pdf