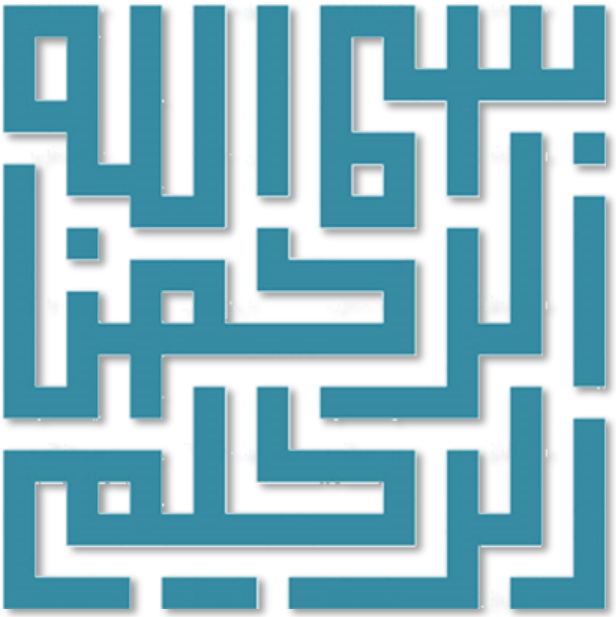
به‌نام خداوند جان و خرد

پروژه خدمات امنیت اطلاعات
ارتقاء امنیت با راه‌اندازی مرکز عملیات امنیت گروه صنعتی گلرنگ

جزوه و سوالات کارگاه تخصصی
ارزش گذاری دارایی ها

Workshop notes



مدیریت لاگ ها

مستند	جزوه و سوالات کارگاه تخصصی ارزش گذاری دارایی ها
طبقه‌بندی	عادی
تهیه کننده	شرکت فراکنش
تایید کننده	
تاریخ تایید	
کد مستند	FR-GIG-asset list-Workshop notes

نسخه	تاریخ تهیه	خلاصه تغییرات
۱.۰	۱۳۹۹/۰۷/۲۳	تهیه و تدوین نسخه اولیه

فهرست مطالب

مقدمه

این سند یکی از خروجی‌های پروژه «خدمات امنیت اطلاعات» با عنوان « سند فنی الزامات امنیتی جمع‌آوری لاگ از سامانه‌ها و سرویس‌های گروه صنعتی گلرنگ » است.

در این سند توضیح مختصری در رابطه با ارائه مفاهیم امنیت به مالکین دارایی های گلرنگ تحت جزوه آمده است. همچنین سوالاتی که جمع آوری آن ها نیاز به مصاحبه با مالکین دارایی دارد در بخش دیگری آمده است تا در قالب کارگاه از آنها پرسیده شود.

۱- مفاهیم امنیت اطلاعات

۱-۱ محرمانگی

در امنیت اطلاعات و ارتباطات، منظور از حفظ محرمانگی، حفاظت کردن از داده ها و فراداده ها در برابر هر گونه دسترسی غیرمجاز به آن ها است.

محرمانگی را باید در ابعاد مختلف آن در نظر گرفت. ممکن است داده ها و اطلاعات مرتبط با کسب و کار باشند. ممکن است اطلاعات مرتبط با مشتری باشند.

مثلا اطلاعاتی که سازمان در مورد آنها حق مالکیت معنوی دارد یا اسرار تجاری، محرمانه تلقی می شوند. فرمولهای شیمیایی یک شرکت یا حتی فرایندهای داخلی می توانند محرمانه باشند. اطلاعاتی که افشای آنها باعث تقویت رقبا، کاهش سهم بازار، کاهش سود نسبت به پیش بینی های پیشین و اثراتی ازین دست شود؛ باید محرمانه تلقی شوند.

به عنوان مثال در مورد اطلاعات مشتریان سایت فروش اینترنتی Okala، باید در نظر داشت که اطلاعات مشتریان محرمانه فرض می شوند و نباید افشا شوند. این اطلاعات بر روی هر دارایی که ذخیره می شوند یا با استفاده از هر دارایی که منتقل می شوند، حفاظت از محرمانگی در مورد آن دارایی ها معنادار خواهد بود.

۱-۲ دسترس پذیری

در محرمانگی گفتیم حفاظت در برابر دسترسی غیرمجاز. اما برخی دسترسی ها مجاز هستند. دسترس پذیری به معنای در دسترس بودن اطلاعات در زمان مورد نیاز برای حالات مجاز است. پس لازم است سامانه های ذخیره و پردازش اطلاعات و راه های ارتباطی مورد استفاده برای دسترسی به اطلاعات به درستی فعالیت نمایند.

دسترس پذیری را نیز باید در ابعاد مختلف آن در نظر گرفت. مثلا مشتری انتظار دارد که به سرویس خاصی دسترسی داشته باشد. اختلال در دسترسی می تواند باعث از دست رفتن اعتبار برند در ذهن مشتری شود. یا همکاران باید به داده ها و سرویس هایی دسترسی داشته باشند تا بتوانند وظایف شغلی خود را انجام دهند.

۱-۳ صحت

حفظ صحت یعنی جلوگیری از تغییر داده‌ها به طور غیرمجاز و تشخیص تغییر غیرمجاز در صورت وقوع. داده ها در تمام مراحل چرخه حیات خود از ایجاد تا امحا باید در برابر تغییرات غیرمجاز محافظت شوند. در حین پردازش، در حین انتقال، در ذخیره سازی و ...

مثلا مشتری وقتی وارد حساب کاربری خود در یک سایت می شود، اگر اطلاعات اشتباهی درباره حساب خود مشاهده نماید ممکن است اعتماد خود را به برند یا شرکت یا حتی هلدینگ از دست بدهد.

یا به عنوان مثالی دیگر، از دست رفتن صحت در داده های مالی یک سازمان می تواند خسارات سنگینی ایجاد نماید. شاید منجر به ناتوانی در پرداخت های درون یا برون سازمانی، یا از دست دادن بخشی از سود برای جبرات خسارت گردد. یا حتی ممکن است منجر به افزایش اجباری ساعات کاری همکاران و نارضایتی سازمانی شود.

۲- پرسش‌های مصاحبه‌ای

پرسش های قابل مصاحبه در ادامه آمده است:

۱. آیا نیاز به دسترسی به سرور از داخل شبکه به شکل ریموت وجود دارد؟

a. بله

b. خیر

۲. آیا نیاز به دسترسی به سرور از طریق اینترنت وجود دارد؟

a. بله

b. خیر

۳. آدرس IP معتبر سرور از بیرون شبکه (اینترنت) چیست؟ (در صورت وجود)

۴. کدام یک از دستگاه های زیر ممکن است به سرور متصل باشند؟

a. Wireless Dongle

b. Printer

c. USB

d. GPS

e. Hardware Auth. Token

f. other

۵. چه پایگاه داده هایی روی این سرور وجود دارد؟ (در صورت وجود)

۶. آیا لازم است قابلیت به روزرسانی خودکار این سرور فعال باشد؟

a. بله

b. خیر

۷. از نظر مفهوم امنیت، امتیاز صحت را وارد کنید.

۸. از نظر مفهوم امنیت، امتیاز دسترس پذیری را وارد کنید.

۹. از نظر مفهوم امنیت، امتیاز محرمانگی را وارد کنید.

۱۰. چه سرویس هایی با این دارایی مرتبط است؟

۱۱. اولویت سرور را تعیین کنید. (توسط واحد امنیت پاسخ داده شود)

a. حاد

b. بالا

c. متوسط

d. پایین

۱۲. آیا این سرور مورد انتظار گزارش گیری لاگ می باشد؟ (توسط واحد امنیت پاسخ داده شود)

a. بله

b. فعلا خیر

c. خیر