محمد مهدی واعظی نژاد

مجموعه راهنماهای امن‌سازی سیستم‌ها و سامانه‌ها

شماره سه

چک‌لیست ارزیابی امنیت پشتیبان‌گیری

به نام خداوندی که به انسان برخاسته از خاک، خرد بخشید؛ از روح خود در او دمید و او را خلیفه خویش در زمین قرار داد و پیامبرانش را با دلایل آشکار فرو فرستاد تا انسان‌ها را به سعادت و هدایت، بر پایه تفکر و تعقل رهنمون گردانند.

تلفن مرکز پخش: ۰۹۳۶۰۸۹۵۸۴۸

فهرست مطالب

۱- مقدمه

تهدیدهای امنیتی و شدت حملات سایبری که موجب از کار انداختن گسترده سیستم‌ها و سامانه‌های سازمانی شده و سازمان‌ها را در دستیابی به اهداف کسب و کاری‌شان می‌تواند با مخاطرات جدی مواجهه سازد، روز به روز در حال افزایش است. شدت این حملات گاهی به حدی است که سازمان‌هایی با بهترین زیرساخت‌های فناوری اطلاعات و امنیتی نیز نمی‌توانند در برابر آن مقاومت چندانی کنند. تهدیداتی که موجب از دست رفتن داده‌ها، تخریب یا دستکاری غیرمجاز آنها می‌شوند، در اوج این حملات قرار داشته و باعث خسارت‌های فراوانی به سازمان‌ها شده‌اند.

بنابراین با وجود این تهدیدهای گسترده سایبری، پشتیبان‌گیری ایمن و تهیه نسخه‌های پشتیبان امن از دارایی‌های اطلاعاتی سازمان، از اهمیت به سزایی برای تمامی سازمان‌ها و شرکت‌ها برخودار است. بگارگیری کنترل‌های ویژه به منظور ایجاد، حفظ و نگهداشت امن نسخه‌های پشتیبان حایز اهمیت بسیاری است که لازم است به صورت دوره‌ای یا موردی، ممیزی‌ها و ارزیابی‌های امنیتی لازم جهت اطمینان از صحت و کارایی این نسخه‌های پشتیبان به عمل آید.

هدف از تدوین و ارایه سند چک‌لیست ارزیابی امنیت پشتیبان‌گیری، بررسی وضعیت کنترل‌های امنیتی نسخه‌های پشتیبان موجود در سازمان‌ها و شرکت‌ها است. این سند می‌تواند ارزیابی بسیار دقیق و جامعی از میزان پیاده‌سازی کنترل‌های امنیتی مربوط به پشتیبان‌گیری از دارایی‌های اطلاعاتی سازمان ارایه کند. از این چک‌لیست می‌توان برای انجام هر گونه ارزیابی امنیتی درون سازمانی استفاده کرد و از طریق فرایند خودارزیابی، وضعیت امنیت پشتیبان‌گیری سازمان را همواره مورد ارزیابی قرار داد.

در پایان، از تمام کارشناسان امنیت اطلاعات و خوانندگان گرامی درخواست می‌کنم نظرها و پیشنهادهای اصلاحی یا تکمیلی خود را از طریق ایمیل Info@mvaezi.ir با اینجانب در میان گذارند تا در اصلاح‌های بعدی این سند مد نظر قرار گیرد.

خدایا چنان کن سرانجام کار، تو خشنود باشی و ما رستگار

محمد مهدی واعظی نژاد

تابستان ۱۳۹۶

۲- چک‌لیست ارزیابی امنیت پشتیبان‌گیری

سند چک‌لیست ارزیابی امنیت پشتیبان‌گیری که با هدف بررسی وضعیت فعلی امنیت نسخه‌های پشتیبان در شرکت‌ها و سازمان‌های ایرانی نگاشته شده است می‌تواند مبنایی برای شناسایی و برطرف‌سازی نقاط ضعف احتمالی و همچنین پیاده‌سازی کنترل‌های امنیتی آتی پشتیبان‌گیری قرار گیرد. این کتاب حاوی ۶ شاخص ارزیابی در زمینه‌های مختلف است که هر شاخص، خود شامل تعدای سؤال است که وضعیت امنیت پشتیبان‌گیری سازمان یا شرکت را در آن شاخص نشان خواهد داد. ماهیت و جنس سؤال‌هایی که در هر یک از این شاخص‌های ۶ گانه آمده است، سعی بر آن دارند که برآوردی کلی را از وضعیت امنیت پشتیبان‌گیری سازمان/شرکت مورد ارزیابی نشان دهند. پاسخ به این سؤال‌ها می‌تواند ضعیف، متوسط، خوب یا عالی باشد که باید در ستون مربوطه درج می‌شود. بعد از تکمیل پرسشنامه‌های این ۶ شاخص، شمای کلی از وضعیت امنیت پشتیبان‌گیری در هر یک از حوزه‌ها به دست می‌آید.

این سند در تمام محدوده فیزیکی سازمان‌ها و شرکت‌ها و نیز در حوزه تعریف شده در دامنه مورد ارزیابی، قابل اجرا است. توصیه می‌شود ممیزان و ارزیابانی که با استفاده از مفاد این سند اقدام به ارزیابی امنیت پشتیبان‌گیری می‌کنند، با رعایت اصول بی‌طرفی و استقلال کامل، یافته‌های خود را بر اساس مشاهده، مصاحبه و بررسی مستندات در قسمت مربوطه یادداشت کرده و از تحت تأثیر قرار نگرفتن یا دستکاری آنها توسط مالکان اطلاعات و فرایندها اطمینان حاصل کنند. همچنین لازم است منابع کافی برای انجام فعالیت‌های ضروری اندازه‌گیری همچون جمع‌آوری داده‌ها، تحلیل، ذخیره‌سازی، گزارش‌دهی و توزیع آن را در نظر گرفته و از آموزش، آگاهی‌رسانی و صلاحیت لازم برخوردار باشند.

۲-۱- مفاد چک‌لیست

در جدول شماره ۱، سؤال‌های چک‌لیست ارزیابی امنیت پشتیبان‌گیری در حوزه‌های ۶ گانه آورده شده است.

*نکته مهم: این چک‌لیست پس از تکمیل هر بخش از آن، به وضعیت **خیلی محرمانه** تغییر می‌کند. بنابراین لازم است اقدام‌های لازم برای حفظ محرمانگی و جلوگیری از دسترسی غیرمجاز به آن انجام شود.*

جدول ۱: چک‌لیست ارزیابی پشتیبان‌گیری

شماره	سؤال ارزیابی	ضعیف	متوسط	خوب	عالی	توضیحات
A01	**مدیریت طرح‌ها و خط‌مشی‌های پشتیبان‌گیری امن**					
هدف	ایجاد و حفظ طرح‌ها و خط‌مشی‌های پشتیبان‌گیری که برای مدیریت، برنامه‌ریزی راهبردی و حمایت از فعالیت‌های سایبری و همچنین تدوین اسناد تداوم کسب و کار سازمان/شرکت از آن استفاده شود.					
A0101	آیا یک سند خط‌مشی پشتیبان‌گیری، مربوط به سیستم‌های اطلاعاتی و خاص سازمان وجود دارد؟					
A0102	آیا در تدوین خط‌مشی‌ها و طرح‌های پشتیبان‌گیری، از تجربیات مستندی همچون استانداردها یا سندهای راهنما استفاده می‌شود؟					
A0103	آیا الزامات امنیتی سازمان، در هنگام تدوین طرح‌ها و خط‌مشی‌های پشتیبان‌گیری در نظر گرفته و لحاظ شده است؟					
A0104	آیا منابع لازم و کافی (شامل افراد، بودجه و ابزارها) برای ایجاد و استفاده از طرح‌ها و خط‌مشی‌های پشتیبان‌گیری تخصیص داده شده است؟					
A0105	آیا خط‌مشی پشتیبان‌گیری به صورت ساده، مختصر، روشن و در سطح بالا که به خوبی بیانگر اهداف امنیتی سازمان باشد، تدوین شده است؟					
A0106	آیا سازوکاری برای پیاده‌سازی طرح‌ها و خط‌مشی‌های پشتیبان‌گیری و اجباری کردن آنها وجود دارد؟					
A0107	آیا خط‌مشی و طرح‌های پشتیبان‌گیری، توسط مدیریت تصویب، منتشر و به اطلاع کارکنان مربوطه و طرف‌های ذینفع بیرونی رسیده است؟					
A0108	آیا خط‌مشی و طرح‌های پشتیبان‌گیری بیانگر تعهد مدیریت و رویکرد سازمان نسبت به امنیت اطلاعات و حفظ تداوم کسب و کار است؟					
A0109	آیا طرح‌ها و خط‌مشی‌های پشتیبان‌گیری، اهداف و فعالیت‌های مربوط به تهیه نسخه‌های پشتیبان امن از دارایی‌های سازمانی را توصیف می‌کنند؟					
A0110	آیا خط‌مشی‌ها و طرح‌های پشتیبان‌گیری و اولویت‌های آن، مستندسازی شده و همراستا با اهداف راهبردی و مخاطرات سازمان هستند؟					
A0111	آیا سندی برای تنظیم شرایط، مسئولیت‌ها و رویه‌های اعمال شده به منظور حفاظت از سوابق پشتیبان‌گیری وجود دارد؟					
A0112	آیا مسئولیت‌های پشتیبان‌گیری نسبت داده شده، برای پوشش همه امور و جلوگیری					