فاطمه طوسی ۹۸۱۳۲۰۰۰۴۸

۱- security policy یک سازمان مفروض را تا رسیدن به لایه عملیاتی ارائه دهید:

سیاست امنیتی برای یک سازمان پیام رسان، باید مراحل و فرآیندهای مختلفی را که برای حفظ امنیت اطلاعات و داده‌های محرمانه و شخصی سازمان لازم است، پوشش دهد. برای رسیدن به لایه عملیاتی یک سازمان پیام رسان، می‌توان سیاست امنیتی را به چندین لایه تقسیم کرد که در ادامه به توضیح آن‌ها می‌پردازیم:

لایه فیزیکی:

در این لایه، سیاست امنیتی باید مراحل و فرآیندهای لازم برای حفظ امنیت فیزیکی ساختمان، دفتر و تجهیزات را شامل شود. مثلاً استفاده از سیستم‌های نظارتی، اعمال محدودیت برای ورود و خروج افراد و تجهیزات و محدود کردن دسترسی به اتاق‌های حساس و غیره.

لایه شبکه:

در این لایه، سیاست امنیتی باید مراحل و فرآیندهای لازم برای حفظ امنیت شبکه سازمان را شامل شود. این شامل استفاده از فایروال، رمزنگاری اطلاعات حساس و محدود کردن دسترسی به سیستم‌هایی که به اطلاعات حساس دسترسی دارند و غیره می‌شود.

لایه سرویس:

در این لایه، سیاست امنیتی باید مراحل و فرآیندهای لازم برای حفظ امنیت سرویس‌های ارائه شده توسط سازمان را شامل شود. به عنوان مثال، محدودیت دسترسی به برنامه‌ها و سرویس‌هایی که به اطلاعات حساس دسترسی دارند، تأیید هویت کاربران و تأیید کدام کاربران دسترسی دارند، رمزنگاری اطلاعات حساس در هنگام ارسال پیام و...

بعد از تعریف و ارائه سیاست‌های امنیتی، باید این سیاست‌ها به یک برنامه عملیاتی واقعی تبدیل شوند که به تمامی بخش‌های سازمان پیام‌رسان اجرا شود. در این مرحله، می‌توان لایه‌های امنیتی مربوط به عملیاتی شدن سیاست‌های امنیتی را به شرح زیر تعریف کرد:

۱. لایه آموزش و پرورش: در این لایه، باید تمامی کارکنان سازمان پیام رسان آموزش دیده و پرورش داده شوند تا با سیاست‌های امنیتی آشنا شوند و بتوانند آن‌ها را اجرا کنند. علاوه بر آموزش، در این لایه باید از کارکنان سازمان خواسته شود که در مورد هر نوع تهدید امنیتی به گروه امنیتی اطلاع دهند.

۲. لایه مدیریت دسترسی: در این لایه، باید سطوح دسترسی به اطلاعات و سرویس‌های مختلف سازمان پیام‌رسان مدیریت شود. برای مثال، کارکنانی که به بخش پشتیبانی دسترسی دارند، نباید به اطلاعات کاربران دسترسی داشته باشند.

۳. لایه پیشگیری و شناسایی: در این لایه، باید اقداماتی برای جلوگیری از وقوع تهدیدات امنیتی انجام شود. این اقدامات شامل نصب و راه‌اندازی سیستم‌های ضد ویروس و فایروال، بروزرسانی نرم‌افزارها، رمزنگاری اطلاعات حساس و ایجاد مکانیزم‌های شناسایی و ردیابی نفوذکنندگان است.

۴. لایه حفاظت از اطلاعات: در این لایه، باید مکانیزم‌هایی برای حفاظت از اطلاعات مهم سازمان پیام رسان پیاده سازی شود.

در کل سیاست‌های امنیتی شرکت‌ها بسته به نوع فعالیت و حوزه کاری آن‌ها می‌تواند متفاوت باشد، اما برخی اصول عمومی سیاست‌های امنیتی عبارتند از:

رمزنگاری داده‌ها: شرکت‌های بزرگ باید داده‌های محرمانه و حساس را با استفاده از روش‌های رمزنگاری قوی محافظت کنند. این شامل رمزنگاری اطلاعات حساب بانکی، رمزنگاری فایل‌های شخصی و حساس کارمندان، مشتریان و ... می‌شود.

سیاست‌های تعیین دسترسی کاربران: برای افزایش امنیت، شرکت‌های بزرگ باید دسترسی کاربران به سیستم‌ها و داده‌های حساس را مدیریت کنند. این شامل استفاده از مدل‌های دسترسی مبتنی بر نقش (Role-based access control)، اعمال محدودیت‌های دسترسی بر اساس اصل حداقل دسترسی ممکن (Principle of least privilege) و ... می‌شود.

آموزش و آگاهی: آموزش کارکنان شرکت‌ها در خصوص رفتار امن در استفاده از سیستم‌ها، شناسایی تهدیدات امنیتی، رعایت قوانین و مقررات امنیتی و استفاده از ابزارهای امنیتی اساسی است.

سیاست‌های بازبینی دسترسی: مرور دوره‌ای دسترسی‌های کاربران به داده‌ها و سیستم‌های شرکت، برای تشخیص هرگونه فعالیت ناشایست و غیرمجاز.

بروزرسانی نرم‌افزارها: برای جلوگیری از حملات به روز، شرکت‌های بزرگ باید به صورت دوره‌ای نرم‌افزارها و سیستم‌عامل‌های خود را بروزرسانی کنند.

سیاست‌های تعیین مدت زمان نگهداری داده‌ها: تعیین زمان نگهداری داده‌های حساس و اطلاعات شخصی مشتریان، برای جلوگیری از دسترسی به داده‌های منسوخ شده.

سیاست‌های پشتیبانی از داده‌ها: ایجاد پشتیبان‌گیری از داده‌ها و سیستم‌های شرکت، برای جلوگیری از دست رفتن اطلاعات در صورت وقوع حوادث امنیتی، مشکلات فنی و غیره.

سیاست‌های کنترل دسترسی به اینترنت: تعیین سیاست‌های مربوط به دسترسی کاربران به اینترنت، مانند فیلترینگ سایت‌های مشکوک و محدودیت دسترسی به سایت‌های حساس.

مانیتورینگ و شناسایی تهدیدات: شرکت‌های بزرگ باید از ابزارهای مانیتورینگ و شناسایی تهدیدات استفاده کنند تا بتوانند به سرعت اقدامات امنیتی لازم را در برابر تهدیدات تشخیص دهند.

سیاست‌های تعیین مدت زمان نگهداری داده‌ها بسیار مهم است و باید به دقت مدیریت شود. در این سیاست‌ها، تعیین مدت زمان نگهداری داده‌ها برای اهداف مختلف مانند رفع ابهامات حقوقی، حفظ حریم شخصی، پاسخ به درخواست‌های قضایی، ارائه خدمات بهتر به مشتریان و ... انجام می‌شود.

مدت زمان نگهداری داده‌ها باید بر اساس نوع داده و هدف از نگهداری آن‌ها تعیین شود. به طور مثال، در صورتی که داده‌ها به علت قوانین محاسباتی یا مالی نگهداری می‌شوند، باید مدت زمان لازم برای بررسی صحت و کارکرد داده‌ها تعیین شود. همچنین، در صورتی که داده‌ها حاوی اطلاعات حساس یا حریم شخصی هستند، باید مدت زمان نگهداری آن‌ها کوتاه و محدود باشد و پس از مدت زمان تعیین شده، باید به صورت دائمی از سامانه حذف شوند.

در ادامه، چند سیاست معمول در تعیین مدت زمان نگهداری داده‌ها را می‌توان ذکر کرد:

مدت زمان نگهداری داده‌های مالی: این سیاست برای تعیین مدت زمان نگهداری داده‌های مالی به کار می‌رود. برای مثال، برای پرداخت‌های مالی می‌توان به‌صورت دائمی داده‌ها را نگهداری کرد، اما برای تراکنش‌هایی که قابلیت بازپرداخت دارند، می‌توان مدت زمان نگهداری داده‌ها را برابر با دو ماه تعیین کرد.

مدت زمان نگهداری داده‌های مشتری: این سیاست برای تعیین مدت زمان نگهداری داده‌های مشتری به کار می‌رود. برای مثال، اگر یک شرکت بخواهد اطلاعات مشتریان خود را نگهداری کند، باید مدت زمان نگهداری را برای هر دسته از اطلاعات تعیین کند. مثلاً، برای اطلاعات شخصی مشتریان مانند نام، نام خانوادگی، شماره تلفن، آدرس و ... می‌توان مدت زمان نگهداری داده‌ها را تا یک سال تعیین کرد. در ضمن، باید توجه داشت که اگر مشتری درخواست حذف اطلاعات خود را داد، باید بلافاصله اطلاعات مربوط به او از سامانه حذف شود. همچنین، برای اطلاعات حساس مشتریان مانند اطلاعات بانکی، شماره کارت، رمز عبور و ... باید مدت زمان نگهداری داده‌ها را به حداقل ممکن محدود کرد و پس از اتمام آن‌ها را به صورت دائمی حذف کرد

۲- نرم افزارهای بکاپ گیری:

در زمینه نرم‌افزارهای بکاپ‌گیری داده‌ها، تعداد زیادی ابزار وجود دارد. برخی از معروف‌ترین نرم‌افزارهای بکاپ‌گیری داده‌ها عبارتند از:

Acronis True Image

EaseUS Todo Backup

Macrium Reflect

Backup and Sync by Google

Backblaze

Carbonite

Veeam Backup and Replication

Veritas Backup Exec

NovaBackup

CrashPlan

لازم به ذکر است که انتخاب نرم‌افزار مناسب برای بکاپ‌گیری داده‌های شما، به میزان مهمی از سطح حساسیت و اهمیت اطلاعات شما و نیز امکانات و ویژگی‌های هر نرم‌افزار بستگی دارد. قبل از استفاده از هر نرم‌افزاری، بهتر است امکانات و قابلیت‌های آن را با دقت بررسی کنید.

۳- Incremental Backup

در فرایند بکاپ گیری، دو روش متداول بکاپ گیری کامل (Full Backup) و بکاپ گیری افزایشی (Incremental Backup) وجود دارد. بکاپ گیری کامل، تمامی داده ها و اطلاعات موجود در یک سیستم را به صورت کامل به یک دستگاه دیگر یا در محیط ذخیره سازی دیگر کپی می کند. این روش، به دلیل زمان بر بودن برای بکاپ گیری کامل، برای برخی سیستم ها و داده ها مناسب نیست.

بکاپ گیری افزایشی به جای بکاپ گیری کامل، فقط اطلاعات جدیدی که در دوره زمانی بعدی تغییر کرده اند، به عنوان یک بکاپ افزایشی ذخیره می شوند. به عبارت دیگر، در این روش، در زمان بکاپ گیری اول، تمامی داده ها به عنوان بکاپ کامل ذخیره می شوند و در بعدی، تنها تغییرات اعمال شده را به عنوان بکاپ افزایشی ذخیره می کند. به این ترتیب، زمان بکاپ گیری بسیار کوتاه تر می شود و فضای ذخیره سازی نیز به طور قابل توجهی کاهش می یابد.

در بکاپ گیری incremental، بکاپ های افزایشی به ترتیب زمانی اعمال تغییرات به سیستم، تولید می شوند و برای بازگرداندن داده ها، ابتدا باید بکاپ کامل و سپس بکاپ های افزایشی به ترتیب زمانی اعمال تغییرات برگردانده شوند. به عبارت دیگر، در بکاپ گیری incremental، با توجه به تعداد بکاپ های افزایشی، زمان بازگرداندن داده ها ممکن است زمان بر باشد.

به طور خلاصه، در بکاپ گیری incremental، تمامی تغییرات ایجاد شده از زمان آخرین بکاپ گیری، با فایل های بکاپ گیری قبلی ترکیب شده و در یک فایل بکاپ ذخیره می شوند.