

معرفی پروژه:

طراحی و استقرار سامانه مدیریت دسترسی‌های ویژه (PAM) در سازمان صنعت، معدن و تجارت

در راستای افزایش امنیت زیرساخت فناوری اطلاعات سازمان صنعت، معدن و تجارت (صمت)، پروژه طراحی و استقرار سامانه مدیریت دسترسی‌های ویژه (PAM) با هدف کنترل، نظارت و ثبت کامل فعالیت کاربران دارای دسترسی حساس اجرا گردید. این پروژه با هدف جلوگیری از سوءاستفاده از حساب‌های مدیریتی، کاهش ریسک نفوذ داخلی و خارجی، و ایجاد قابلیت ممیزی امنیتی مطابق الزامات امنیتی کشور طراحی و پیاده‌سازی شد.

چالش‌های موجود قبل از اجرا

قبل از استقرار سامانه PAM، سازمان با چالش‌های زیر مواجه بود:

- استفاده مستقیم از اکانت‌های Administrator
- نگهداری رمزهای عبور در فایل‌ها و یادداشت‌های شخصی
- عدم ثبت دقیق فعالیت مدیران سیستم
- نبود کنترل متمرکز بر دسترسی‌های حساس
- دشواری در ممیزی امنیتی
- افزایش ریسک نشت اطلاعات
- عدم امکان ردیابی دقیق تغییرات انجام‌شده در زیرساخت

تاریخ: ۱۴۰۴/۱۰/۲۸

شماره فایل: ۰۴۱۰۰۷

پیوست: دارد

دیدار داده محسن (سهامی خاص) شماره ی ثبت: ۱۴۰۱۴۹۶۸۹۸۶

آدرس: خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

اهداف پروژه

- مدیریت متمرکز حساب‌های سطح دسترسی بالا
- کنترل کامل دسترسی مدیران سیستم
- ثبت و ضبط فعالیت‌های کاربران ویژه
- کاهش ریسک نفوذ و تهدیدات داخلی
- ایجاد بستر ممیزی و گزارش‌دهی امنیتی
- افزایش انطباق با الزامات امنیتی و افتا

مراحل اجرای پروژه

فاز اول: تحلیل و شناسایی دارایی‌ها

در این مرحله کلیه دارایی‌های حیاتی سازمان شناسایی گردید:

- سرورها
- تجهیزات شبکه
- فایروال‌ها
- تجهیزات امنیتی
- ماشین‌های مجازی
- پایگاه‌های داده
- سرویس‌های حیاتی

شماره ی تماس: ۰۹۱۲۷۲۴۳۲۶۷

آدرس وب سایت: <https://www.sekkodata.com>

آدرس ایمیل: kaedi.mohsen@sekkodata.com

تاریخ: ۱۴۰۴/۱۰/۲۸

شماره فایل: ۰۴۱۰۰۷

پیوست: دارد

دیدار داده محسن (سهامی خاص) شماره ی ثبت: ۱۴۰۱۴۹۶۸۹۸۶

آدرس: خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

خروجی:

- لیست دارایی‌ها
- طبقه‌بندی سطح حساسیت
- شناسایی حساب‌های مدیریتی

فاز دوم: طراحی معماری PAM

معماری سامانه بر اساس نیازهای سازمان طراحی گردید.

اجزاء اصلی:

- PAM Server
- Password Vault
- Session Manager
- Audit Server
- Reporting Server

طراحی شامل:

- ساختار دسترسی کاربران
- سیاست‌های رمز عبور
- سیاست‌های ثبت وقایع
- فرآیند تأیید دسترسی

شماره ی تماس: ۰۹۱۲۷۲۴۳۲۶۷

آدرس وب سایت: <https://www.sekkodata.com>

آدرس ایمیل: kaedi.mohsen@sekkodata.com

فاز سوم: نصب و راه اندازی

در این بخش سامانه PAM بر روی زیرساخت مجازی سازمان پیاده سازی شد.

اقدامات:

- نصب سرور PAM
- راه اندازی پایگاه داده
- اتصال به Active Directory
- تعریف نقش های سازمانی
- تعریف حساب های حساس

فاز چهارم: مدیریت رمزهای عبور

کلیه رمزهای عبور حساس در خزانه امن ذخیره شدند.

قابلیت ها:

- رمز گذاری اطلاعات
- چرخش خودکار رمزها
- حذف رمزهای ثابت
- دسترسی کنترل شده

تاریخ: ۱۴۰۴/۱۰/۲۸

شماره فایل: ۰۴۱۰۰۷

پیوست: دارد

دیدار داده محسن (سهامی خاص) شماره ی ثبت: ۱۴۰۱۴۹۶۸۹۸۶

آدرس: خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فاز پنجم: کنترل نشست‌های مدیریتی

تمام نشست‌های مدیریتی تحت کنترل قرار گرفت.

موارد تحت پوشش:

- RDP
- SSH
- Telnet
- Console Access
- Web Management

قابلیت‌ها:

- ضبط ویدئویی جلسات مدیریتی
- ثبت دستورات
- امکان بازبینی کامل فعالیت‌ها

فاز ششم: ثبت وقایع و مانیتورینگ

تمام رویدادهای امنیتی ثبت و تحلیل شدند.

نمونه رویدادها:

- ورود مدیران
- تغییر تنظیمات

- دسترسی خارج از ساعات اداری

شماره ی تماس: ۰۹۱۲۷۲۴۳۲۶۷

آدرس وب سایت: <https://www.sekkodata.com>

آدرس ایمیل: kaedi.mohsen@sekkodata.com

تاریخ: ۱۴۰۴/۱۰/۲۸

شماره فایل: ۰۴۱۰۰۷

پیوست: دارد

دیدار داده محسن (سهامی خاص) شماره ی ثبت: ۱۴۰۱۴۹۶۸۹۸۶

آدرس: خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- تلاش ناموفق ورود

- تغییر رمز عبور

فاز هفتم: تست امنیتی و تحویل

انجام تست‌های نهایی:

- تست عملکرد

- تست دسترسی

- تست ثبت وقایع

- تست بازیابی اطلاعات

پس از تأیید نهایی، سامانه تحویل کارفرما گردید.

دستاوردهای پروژه

افزایش امنیت

کاهش چشمگیر احتمال سوءاستفاده از حساب‌های سطح بالا.

قابلیت ممیزی

ثبت صددرصدی فعالیت مدیران سیستم.

مدیریت متمرکز

حذف دسترسی‌های پراکنده و غیرقابل کنترل.

شماره ی تماس: ۰۹۱۲۷۲۴۳۲۶۷

آدرس وب سایت: <https://www.sekkodata.com>

آدرس ایمیل: kaedi.mohsen@sekkodata.com

تاریخ: ۱۴۰۴/۱۰/۲۸

شماره فایل: ۰۴۱۰۰۷

پیوست: دارد

دیدار داده محسن (سهامی خاص) شماره ی ثبت: ۱۴۰۱۴۹۶۸۹۸۶

آدرس: خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

انطباق با الزامات امنیتی

پوشش بخش مهمی از الزامات:

- افتا
- پدافند غیرعامل
- ISMS
- استاندارد ISO ۲۷۰۰۱

فناوری‌های مورد استفاده

- Microsoft Active Directory
- VMware ESXi
- Windows Server
- Linux Server
- SQL Server
- PAM Solution
- Syslog
- SIEM Integration

خدمات قابل ارائه توسط شرکت دیدار داده محسن

- مشاوره و طراحی PAM
- استقرار سامانه PAM

شماره ی تماس: ۰۹۱۲۷۲۴۳۲۶۷

آدرس وب سایت: <https://www.sekkodata.com>

آدرس ایمیل: kaedi.mohsen@sekkodata.com

تاریخ: ۱۴۰۴/۱۰/۲۸

شماره فایل: ۰۴۱۰۰۷

پیوست: دارد

دیدار داده محسن (سهامی خاص) شماره ی ثبت: ۱۴۰۱۴۹۶۸۹۸۶

آدرس: خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

• اتصال به Active Directory

• ضبط و مانیتورینگ نشست‌های مدیریتی

• ممیزی امنیتی دسترسی‌ها

• آموزش کارشناسان سازمان

• پشتیبانی و نگهداری سامانه

نتیجه پروژه

با اجرای پروژه PAM، تمامی دسترسی‌های سطح بالا در سازمان تحت کنترل و نظارت متمرکز قرار گرفت و امکان ردیابی، ثبت و ممیزی کامل فعالیت‌های مدیریتی فراهم شد. این پروژه گامی مؤثر در افزایش امنیت زیرساخت و کاهش ریسک‌های ناشی از دسترسی‌های ویژه محسوب می‌شود.

SEKKO DATA

شماره ی تماس: ۰۹۱۲۷۲۴۳۲۶۷

آدرس وب سایت: <https://www.sekkodata.com>

آدرس ایمیل: kaedi.mohsen@sekkodata.com