دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

مقدمه

در دنیای امروز، امنیت اطلاعات دیگر صرفاً به استقرار تجهیزات امنیتی محدود نمی‌شود؛ بلکه توانایی مشاهده، تحلیل و پاسخ سریع به تهدیدات، به یکی از مهم‌ترین الزامات سازمان‌های مدرن تبدیل شده است. با افزایش حجم حملات سایبری، پیچیده‌تر شدن تهدیدات و رشد روزافزون زیرساخت‌های فناوری اطلاعات، وجود یک سامانه متمرکز برای جمع‌آوری، تحلیل و مدیریت رخدادهای امنیتی ضرورتی اجتناب‌ناپذیر است.

سازمان صنعت، معدن و تجارت به عنوان یکی از دستگاه‌های اجرایی راهبردی کشور، دارای زیرساخت‌های متنوع فناوری اطلاعات، سامانه‌های عملیاتی، پایگاه‌های داده، سرویس‌های شبکه و اطلاعات ارزشمندی است که حفاظت مؤثر از آن‌ها نیازمند ایجاد دید جامع و متمرکز نسبت به وضعیت امنیتی سازمان می‌باشد.

شرکت دیدار داده محسن با تکیه بر دانش تخصصی در حوزه امنیت سایبری، زیرساخت، مانیتورینگ و تحلیل رخدادهای امنیتی، این طرح را با هدف طراحی، استقرار و بهره‌برداری از سامانه مدیریت و تحلیل رویدادهای امنیتی (SIEM) ارائه نموده است.

هدف از اجرای این پروژه ایجاد یک مرکز هوشمند پایش امنیتی است که بتواند اطلاعات و لاگ‌های تولیدشده توسط سرورها، تجهیزات شبکه، فایروال‌ها، ماشین‌های مجازی، سرویس‌های حیاتی و سامانه‌های کاربردی را به‌صورت متمرکز جمع‌آوری، تحلیل و همبسته‌سازی نموده و تهدیدات امنیتی را در کوتاه‌ترین زمان ممکن شناسایی نماید.

در معماری پیشنهادی این پروژه، تمامی رویدادهای امنیتی از منابع مختلف شامل فایروال FortiGate ، زیرساخت VMware ، سرورهای Windows و Linux ، سرویس‌های Active Directory ، پایگاه‌های داده، تجهیزات شبکه و سایر سامانه‌های سازمان جمع‌آوری شده و پس از تحلیل و همبستگی رویدادها، هشدارهای امنیتی دقیق و قابل اقدام در اختیار کارشناسان فناوری اطلاعات قرار خواهد گرفت.

پیاده‌سازی این سامانه علاوه بر افزایش سطح امنیت سایبری سازمان، امکان شناسایی سریع تهدیدات، کاهش زمان کشف رخدادها، تسریع فرآیند پاسخگویی، مدیریت متمرکز لاگ‌ها، تولید گزارش‌های مدیریتی، تحلیل رفتار کاربران و تجهیزات، مدیریت آسیب‌پذیری‌ها و ارتقای تاب‌آوری سایبری سازمان را فراهم خواهد نمود.

شرکت دیدار داده محسن با بهره‌گیری از تجربه اجرایی در حوزه امنیت اطلاعات، مجازی‌سازی، مدیریت زیرساخت و سامانه‌های مانیتورینگ، متعهد است این پروژه را بر اساس بهترین رویه‌های بین‌المللی و با رویکردی عملیاتی، پایدار و قابل توسعه اجرا نموده و بستری امن برای پایش و مدیریت امنیت اطلاعات سازمان فراهم آورد.

این سند در ادامه ضمن معرفی اهداف، معماری فنی، الزامات اجرایی، روش استقرار، فرآیندهای عملیاتی و الزامات نگهداری سامانه SIEM ، نقشه راه اجرای پروژه را تشریح می‌نماید.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل ۱: مقدمه و کلیات

- مقدمه
- اهداف
- دامنه
- تعاریف

فصل ۲: حاکمیت امنیت اطلاعات

- ساختار سازمانی
- نقش‌ها
- کمیته امنیت
- مسئولیت‌ها

فصل ۳: مدیریت دارایی‌ها

- شناسایی دارایی
- مالکیت دارایی
- طبقه‌بندی اطلاعات
- ارزش‌گذاری

فصل ۴: مدیریت ریسک

- روش تحلیل ریسک
- ماتریس ریسک
- برنامه مقابله

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل ۵: کنترل‌های امنیتی

- کنترل دسترسی
- امنیت شبکه
- امنیت سرورها
- امنیت VMware
- امنیت فیزیکی
- رمزنگاری

فصل ۶: مدیریت رخداد امنیتی

- Incident Management
- پاسخ به رخداد
- Playbookها
- گزارش‌دهی

فصل ۷: مدیریت آسیب‌پذیری

- اسکن
- Patch Management
- ارزیابی امنیت
- تست نفوذ

فصل ۸: تداوم کسب‌وکار و بازیابی بحران

- BCP
- DRP
- Backup
- Recovery

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- سناریوهای بحران

فصل ۹: سامانه SIEM وSOC

- معماری SIEM
- Wazuh
- FortiAnalyzer
- SOC
- Use Caseها
- Ruleها
- Dashboardها

فصل ۱۰: ممیزی، آموزش و بهبود مستمر

- ممیزی
- KPI
- آموزش
- بازنگری مدیریت
- بهبود مستمر

پیوست‌ها

- Asset Register
- Risk Register
- فرم‌ها
- چک‌لیست‌ها
- SoA
- RACI
- SLA

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

- برنامه زمان‌بندی
- دیاگرام‌ها

فصل اول: مقدمه و کلیات پروژه

۱-۱ مقدمه

در عصر تحول دیجیتال، اطلاعات به عنوان یکی از مهم‌ترین دارایی‌های راهبردی سازمان‌ها شناخته می‌شوند. توسعه روزافزون فناوری اطلاعات، گسترش خدمات الکترونیکی، افزایش وابستگی فرآیندهای سازمانی به سامانه‌های اطلاعاتی و رشد تهدیدات سایبری، اهمیت حفاظت از اطلاعات و زیرساخت‌های فناوری اطلاعات را بیش از پیش آشکار ساخته است.

سازمان‌ها امروزه با طیف گسترده‌ای از مخاطرات امنیتی شامل حملات سایبری، بدافزارها، باج‌افزارها، نشت اطلاعات، نفوذهای غیرمجاز، خطاهای انسانی و اختلالات زیرساختی مواجه هستند. وقوع هر یک از این مخاطرات می‌تواند منجر به خسارات مالی، عملیاتی، اعتباری و حقوقی قابل توجهی گردد.

از این رو ایجاد یک چارچوب مدیریتی و فنی جهت شناسایی، ارزیابی، کنترل و پایش ریسک‌های امنیت اطلاعات به یکی از نیازهای اساسی سازمان‌های دولتی و خصوصی تبدیل شده است.

سیستم مدیریت امنیت اطلاعات (ISMS) مجموعه‌ای از سیاست‌ها، فرآیندها، ساختارهای مدیریتی، کنترل‌های فنی و مکانیزم‌های نظارتی است که با هدف حفظ محرمانگی، صحت و دسترس‌پذیری اطلاعات طراحی و پیاده‌سازی می‌شود.

استقرار ISMS علاوه بر ارتقاء سطح امنیت سازمان، زمینه انطباق با الزامات قانونی، استانداردهای ملی و بین‌المللی و همچنین الزامات مراجع حاکمیتی را فراهم می‌نماید.

این سند با هدف تبیین چارچوب استقرار سیستم مدیریت امنیت اطلاعات، سامانه مدیریت رخدادها و اطلاعات امنیتی (SIEM)، فرآیندهای مدیریت ریسک، مدیریت رخداد، تداوم کسب‌وکار و بازیابی بحران تدوین گردیده است.

۱-۲ ضرورت اجرای پروژه

با توجه به گسترش زیرساخت‌های فناوری اطلاعات، افزایش تعداد سامانه‌ها و سرویس‌های سازمانی، و همچنین پیچیده‌تر شدن تهدیدات سایبری، استفاده از روش‌های سنتی مدیریت امنیت پاسخگوی نیازهای فعلی سازمان نمی‌باشد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بررسی‌های انجام شده در سطح ملی و بین‌المللی نشان می‌دهد که بخش عمده‌ای از رخدادهای امنیتی ناشی از موارد زیر می‌باشد:

- نبود مدیریت متمرکز امنیت اطلاعات
- ضعف در فرآیندهای مدیریت ریسک
- نبود سامانه‌های مانیتورینگ امنیتی
- ضعف در مدیریت دسترسی‌ها
- نبود رویه‌های پاسخگویی به رخداد
- عدم آگاهی کاربران
- ضعف در مستندسازی فرآیندهای امنیتی

اجرای این پروژه بستری را فراهم خواهد نمود تا سازمان بتواند با رویکردی ساختاریافته نسبت به شناسایی تهدیدات، مدیریت مخاطرات و افزایش تاب‌آوری سایبری اقدام نماید.

۳-۱ اهداف کلان پروژه

اهداف کلان این پروژه عبارتند از:

حفاظت از دارایی‌های اطلاعاتی

شناسایی و حفاظت از اطلاعات، سامانه‌ها، تجهیزات و زیرساخت‌های حیاتی سازمان.

تضمین محرمانگی اطلاعات

اطمینان از دسترسی اطلاعات صرفاً توسط افراد مجاز.

تضمین صحت اطلاعات

جلوگیری از تغییر یا تخریب غیرمجاز اطلاعات.

تضمین دسترس‌پذیری اطلاعات

تضمین دسترسی مستمر کاربران مجاز به اطلاعات و خدمات.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

مدیریت ریسک‌های امنیتی

شناسایی، ارزیابی و کنترل مخاطرات امنیت اطلاعات.

افزایش تاب‌آوری سایبری

افزایش توان سازمان در پیشگیری، شناسایی و مقابله با تهدیدات.

انطباق با الزامات قانونی

رعایت الزامات نهادهای نظارتی و حاکمیتی.

ارتقاء فرهنگ امنیت

افزایش آگاهی کارکنان نسبت به مخاطرات امنیتی.

۱-٤ اهداف اختصاصی پروژه

اهداف اجرایی پروژه شامل موارد زیر می‌باشد:

- شناسایی دارایی‌های اطلاعاتی سازمان
- طبقه‌بندی اطلاعات
- تحلیل ریسک امنیتی
- تدوین سیاست‌های امنیت اطلاعات
- استقرار فرآیند مدیریت رخداد
- استقرار فرآیند مدیریت تغییرات
- استقرار مدیریت آسیب‌پذیری
- طراحی و راه‌اندازی SIEM
- طراحی سناریوهای امنیتی
- آموزش کاربران
- تدوین برنامه تداوم کسب‌وکار

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- تدوین برنامه بازیابی بحران
- ایجاد نظام ممیزی امنیت اطلاعات

۵-۱ دامنه پروژه

دامنه این پروژه کلیه زیرساخت‌ها، سامانه‌ها، تجهیزات، کاربران و فرآیندهای مرتبط با فناوری اطلاعات سازمان را در بر می‌گیرد.

موارد تحت پوشش عبارتند از:

زیرساخت شبکه

- سوئیچ‌ها
- روترها
- تجهیزات ارتباطی
- لینک‌های ارتباطی

تجهیزات امنیتی

- FortiGate
- سامانه‌های مانیتورینگ
- سامانه‌های تحلیل لاگ

زیرساخت مجازی‌سازی

- VMware ESXi
- VMware vCenter
- ماشین‌های مجازی

سرورها

- Windows Server
- Linux Server

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- File Server
- Database Server

کاربران

- مدیران
- کارشناسان
- کاربران عادی
- پیمانکاران

۶-۱ ذی‌نفعان پروژه

ذی‌نفعان اصلی پروژه عبارتند از:

مدیریت ارشد سازمان

مسئول تصویب سیاست‌ها و تخصیص منابع.

واحد فناوری اطلاعات

مسئول اجرای کنترل‌های فنی.

مسئول امنیت اطلاعات

مسئول پایش و ارزیابی امنیت.

کاربران سازمان

مسئول رعایت الزامات امنیتی.

پیمانکار پروژه

مسئول طراحی، پیاده‌سازی، آموزش و انتقال دانش.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱-۷ فرضیات پروژه

این پروژه بر اساس فرضیات زیر تدوین شده است:

- زیرساخت شبکه سازمان عملیاتی می‌باشد .
- تجهیزات امنیتی سازمان فعال هستند .
- همکاری واحدهای مختلف سازمان فراهم خواهد بود .
- دسترسی لازم جهت ارزیابی زیرساخت‌ها فراهم می‌شود .
- اطلاعات موردنیاز در اختیار تیم پروژه قرار خواهد گرفت .

۱-۸ محدودیت‌های پروژه

محدودیت‌های احتمالی شامل:

- محدودیت زمانی
- محدودیت بودجه
- محدودیت منابع انسانی
- محدودیت دسترسی به برخی سامانه‌ها
- الزامات قانونی و حاکمیتی

۱-۹ روش اجرای پروژه

اجرای پروژه در شش فاز انجام خواهد شد:

فاز اول: شناخت وضع موجود

بررسی وضعیت فعلی امنیت اطلاعات سازمان.

فاز دوم: تحلیل ریسک

شناسایی دارایی‌ها، تهدیدات و آسیب‌پذیری‌ها.

فاز سوم: طراحیISMS

تدوین سیاست‌ها، رویه‌ها و مستندات.

فاز چهارم: استقرارSIEM

پیاده‌سازی سامانه جمع‌آوری و تحلیل رخدادها.

فاز پنجم: آموزش و انتقال دانش

آموزش مدیران، کارشناسان و کاربران.

فاز ششم: ارزیابی و تحویل نهایی

ممیزی، رفع نواقص و تحویل پروژه.

۱۰-۱ ساختار سند

این سند در قالب ده فصل اصلی و مجموعه‌ای از پیوست‌های فنی و مدیریتی تدوین گردیده است و کلیه الزامات موردنیاز جهت استقرارISMS ، SIEM و فرآیندهای مرتبط را تشریح می‌نماید.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل دوم: حاکمیت امنیت اطلاعات(Information Security Governance)

۲-۱ مقدمه

حاکمیت امنیت اطلاعات مجموعه‌ای از ساختارها، سیاست‌ها، فرآیندها، نقش‌ها و مسئولیت‌هایی است که جهت هدایت، کنترل و پایش امنیت اطلاعات در سطح سازمان طراحی و اجرا می‌گردد.

هدف از حاکمیت امنیت اطلاعات، اطمینان از هم‌راستایی فعالیت‌های امنیتی با اهداف راهبردی سازمان، مدیریت ریسک‌های امنیتی و استفاده بهینه از منابع می‌باشد.

در این چارچوب، مدیریت ارشد سازمان مسئولیت نهایی امنیت اطلاعات را بر عهده داشته و تمامی واحدها موظف به همکاری در اجرای الزامات امنیتی می‌باشند.

۲-۲ اهداف حاکمیت امنیت اطلاعات

اهداف اصلی عبارتند از:

- ایجاد ساختار مدیریتی امنیت اطلاعات
- تعیین مسئولیت‌ها و اختیارات
- هم‌راستاسازی امنیت با اهداف سازمان
- مدیریت ریسک‌های امنیتی
- افزایش پاسخگویی
- افزایش سطح بلوغ امنیتی
- نظارت بر اجرای کنترل‌های امنیتی
- بهبود مستمر وضعیت امنیت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲-۳ اصول حاکمیت امنیت اطلاعات

اصل اول: مسئولیت‌پذیری

کلیه افراد سازمان در قبال امنیت اطلاعات مسئول هستند.

اصل دوم: شفافیت

فرآیندها و مسئولیت‌ها باید مستند و شفاف باشند.

اصل سوم: مدیریت ریسک

تصمیمات امنیتی باید مبتنی بر تحلیل ریسک باشند.

اصل چهارم: بهبود مستمر

فرآیندهای امنیتی باید به صورت دوره‌ای بازنگری شوند.

اصل پنجم: انطباق

سازمان باید الزامات قانونی، قراردادی و استانداردهای مرتبط را رعایت نماید.

۲-۴ ساختار حاکمیتی امنیت اطلاعات

ساختار پیشنهادی شامل:

مدیریت ارشد سازمان

کمیته امنیت اطلاعات

مسئول امنیت اطلاعات

واحد فناوری اطلاعات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

کاربران

پیمانکاران

۲-۵ مدیریت ارشد سازمان

مدیریت ارشد مسئول نهایی امنیت اطلاعات بوده و وظایف زیر را بر عهده دارد:

- تصویب خطمشی امنیت
- تأمین منابع
- بررسی گزارش‌های امنیتی
- تصویب برنامه‌های امنیتی
- حمایت از اجرای کنترل‌ها

۲-٦ کمیته امنیت اطلاعات

اهداف کمیته

- هدایت راهبردی امنیت
- تصویب سیاست‌ها
- بررسی ریسک‌ها
- ارزیابی رخدادها
- نظارت بر پروژه‌های امنیتی

اعضای کمیته

- مدیر ارشد
- مدیر فناوری اطلاعات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- مسئول امنیت اطلاعات
- نماینده منابع انسانی
- نماینده امور حقوقی
- نماینده واحدهای عملیاتی

جلسات

حداقل هر سه ماه یکبار برگزار می‌شود.

۲-۷ مسئول امنیت اطلاعات

مسئول امنیت اطلاعات به عنوان متولی اصلی امنیت سازمان وظایف زیر را انجام می‌دهد:

برنامه‌ریزی امنیتی

- تدوین برنامه سالانه
- تدوین سیاست‌ها

نظارت

- پایش کنترل‌ها
- بررسی لاگ‌ها
- ارزیابی ریسک‌ها

گزارش‌دهی

- گزارش به مدیریت
- گزارش رخدادها
- گزارش ممیزی‌ها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲-۸ واحد فناوری اطلاعات

واحد IT مسئول اجرای کنترل‌های فنی می‌باشد.

مسئولیت‌ها:

- مدیریت سرورها
- مدیریت VMware
- مدیریت Backup
- مدیریت شبکه
- مدیریت تجهیزات امنیتی

۲-۹ مسئولیت کاربران

کاربران موظف‌اند:

- محرمانگی اطلاعات را حفظ نمایند .
- رمز عبور خود را محافظت کنند .
- رخدادهای امنیتی را گزارش دهند .
- از نصب نرم‌افزار غیرمجاز خودداری نمایند .

۲-۱۰ مدیریت پیمانکاران

پیمانکاران قبل از دریافت دسترسی باید:

- توافقنامه محرمانگی امضا کنند .
- آموزش امنیتی دریافت نمایند .
- سطح دسترسی آن‌ها تعریف شود .

۲-۱۱ خط مشی امنیت اطلاعات

خط مشی امنیت اطلاعات باید:

- توسط مدیریت ارشد تصویب شود .
- به کلیه کارکنان ابلاغ گردد .
- سالانه بازنگری شود .
- در دسترس ذی‌نفعان قرار گیرد .

۲-۱۲ فرآیند بازنگری مدیریت

مدیریت ارشد حداقل سالی یک بار موارد زیر را بررسی می‌کند:

- وضعیت ریسک‌ها
- وضعیت رخدادها
- نتایج ممیزی
- عملکرد KPI ها
- میزان تحقق اهداف

۲-۱۳ شاخص‌های حاکمیت امنیت

KPI-۰۱

درصد اجرای مصوبات کمیته امنیت

هدف: ۹۰%

KPI-۰۲

درصد کنترل‌های پیاده‌سازی شده

هدف: ۹۵%

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

KPI-۰۳

تعداد رخدادهای بحرانی

هدف: روند کاهشی

KPI-۰٤

درصد کارکنان آموزش دیده

هدف: ۱۰۰%

۲-۱٤ ماتریس مسئولیت(RACI)

فعالیت	مدیریت	امنیت	IT	کاربران
تحلیل ریسک	A	R	C	I
مدیریت رخداد	I	R	C	I
Backup	I	C	R	I
آموزش	A	R	C	I
ممیزی	A	R	C	I

تعاریف:

- R = Responsible
- A = Accountable
- C = Consulted
- I = Informed

۲-۱۵ ممیزی حاکمیت امنیت

ممیزی‌های داخلی حداقل سالی یک بار انجام خواهند شد.

دامنه ممیزی:

- سیاست‌ها
- فرآیندها
- کنترل‌ها
- مستندات
- سوابق

منابع و مراجع فصل دوم

استانداردها

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- ISO ۳۱۰۰۰

چارچوب‌ها

- NIST Cybersecurity Framework
- COBIT

مراجع فنی

- SANS Institute
- Center for Internet Security

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل سوم: مدیریت دارایی‌ها و طبقه‌بندی اطلاعات

۳-۱مقدمه

دارایی‌های اطلاعاتی از مهم‌ترین سرمایه‌های هر سازمان محسوب می‌شوند. این دارایی‌ها شامل اطلاعات، نرم‌افزارها، سخت‌افزارها، زیرساخت‌های شبکه، تجهیزات امنیتی، منابع انسانی و خدمات پشتیبان می‌باشند.

شناسایی، ثبت، ارزش‌گذاری و حفاظت مناسب از دارایی‌ها یکی از الزامات اصلی سیستم مدیریت امنیت اطلاعات بوده و نقش اساسی در مدیریت ریسک و پیاده‌سازی کنترل‌های امنیتی ایفا می‌کند.

هدف از این فصل ایجاد چارچوبی جهت شناسایی، طبقه‌بندی، مدیریت و حفاظت از دارایی‌های اطلاعاتی سازمان می‌باشد.

۳-۲ اهداف مدیریت دارایی

اهداف اصلی عبارتند از:

- شناسایی کلیه دارایی‌ها
- تعیین مالکیت دارایی‌ها
- ارزش‌گذاری دارایی‌ها
- طبقه‌بندی اطلاعات
- حفاظت متناسب با ارزش دارایی
- کاهش ریسک‌های امنیتی
- تسهیل مدیریت رخدادها
- بهبود فرآیند ممیزی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳-۳ تعریف دارایی

دارایی به هر چیزی اطلاق می‌گردد که برای سازمان ارزش داشته و از دست رفتن، تخریب یا افشای آن موجب ایجاد خسارت گردد.

دارایی‌ها می‌توانند فیزیکی، منطقی یا انسانی باشند.

۳-٤ دسته‌بندی دارایی‌ها

دارایی‌های اطلاعاتی

شامل:

- بانک‌های اطلاعاتی
- اسناد سازمانی
- اطلاعات پرسنلی
- اطلاعات مالی
- اطلاعات قراردادها
- مکاتبات اداری
- اطلاعات مشتریان

دارایی‌های نرم‌افزاری

شامل:

- سیستم عامل‌ها
- نرم‌افزارهای کاربردی
- سامانه‌های سازمانی
- سیستم‌های ERP
- نرم‌افزارهای مالی
- نرم‌افزارهای مانیتورینگ

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

دارایی‌های سخت‌افزاری

شامل:

- سرورها
- Workstationها
- لپ‌تاپ‌ها
- تجهیزات ذخیره‌سازی
- چاپگرها
- تجهیزات امنیتی

دارایی‌های شبکه

شامل:

- روترها
- سوئیچ‌ها
- فایروال‌ها
- تجهیزات بی‌سیم
- لینک‌های ارتباطی

دارایی‌های انسانی

شامل:

- مدیران
- کارشناسان
- کاربران
- پیمانکاران

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

دارایی‌های خدماتی

شامل:

- اینترنت
- برق
- سامانه پیامک
- سرویس‌های ابری
- مراکز داده

۳-۵ فهرست دارایی‌ها(Asset Register)

برای تمامی دارایی‌ها باید اطلاعات زیر ثبت گردد:

توضیح	فیلد
شناسه یکتا	کد دارایی
نام تجهیز	نام دارایی
سخت‌افزار، نرم‌افزار و...	نوع دارایی
مسئول دارایی	مالک دارایی
مکان فیزیکی	محل استقرار
کم، متوسط، زیاد	سطح اهمیت
فعال یا غیرفعال	وضعیت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

نمونه ثبت دارایی

مالک	دارایی	کد
واحدIT	Active Directory	AST-۰۰۱
واحدIT	VMware Cluster	AST-۰۰۲
واحد امنیت	FortiGate	AST-۰۰۳
واحد فناوری	SQL Server	AST-۰۰٤
واحدIT	Backup Server	AST-۰۰۵

۳-٦ مالکیت دارایی‌ها

برای هر دارایی باید یک مالک مشخص گردد.

مسئولیت‌های مالک:

- تعیین سطح طبقه‌بندی
- تأیید دسترسی‌ها
- بازبینی دوره‌ای
- مدیریت تغییرات

۳-۷ ارزش‌گذاری دارایی‌ها

ارزش هر دارایی بر اساس سه شاخص تعیین می‌شود:

محرمانگی

آسیب ناشی از افشای اطلاعات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

صحت

آسیب ناشی از تغییر اطلاعات

دسترس‌پذیری

آسیب ناشی از عدم دسترسی

مقیاس امتیازدهی

سطح	امتیاز
کم	۱
متوسط	۲
زیاد	۳
خیلی زیاد	۴
بحرانی	۵

نمونه ارزش‌گذاری

دارایی	C	I	A
Active Directory	۵	۵	۵
VMware	۴	۵	۵
FortiGate	۴	۵	۵
Email Server	۴	۴	۴

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳-۸ طبقه‌بندی اطلاعات

اهداف

- حفاظت مناسب
- کنترل دسترسی
- جلوگیری از افشای اطلاعات

سطح اول: عمومی

اطلاعات قابل انتشار

نمونه:

- بروشورها
- اطلاعات وب‌سایت

سطح دوم: داخلی

مخصوص کارکنان

نمونه:

- دستورالعمل‌ها
- فرم‌ها

سطح سوم: محرمانه

دارای حساسیت بالا

نمونه:

- قراردادها
- اطلاعات مالی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

سطح چهارم: بسیار محرمانه

بالاترین سطح حساسیت

نمونه:

- تنظیمات فایروال
- رمزهای مدیریتی
- اطلاعات زیرساخت حیاتی

۳-۹ برچسب‌گذاری اطلاعات

تمام اسناد باید دارای برچسب باشند.

نمونه:

- عمومی
- داخلی
- محرمانه
- بسیار محرمانه

۳-۱۰ مدیریت چرخه عمر دارایی

ایجاد

ثبت دارایی

بهره‌برداری

استفاده عملیاتی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

نگهداری

به‌روزرسانی و تعمیر

خروج از سرویس

حذف یا امحا

۱۳-۱۱ محای امن اطلاعات

روش‌های مجاز:

- Secure Erase
- Disk Wipe
- Degaussing
- Shredding

۳-۱۲ کنترل‌های امنیتی دارایی‌ها

کنترل فیزیکی

- اتاق سرور
- کنترل دسترسی
- دوربین

کنترل منطقی

- MFA
- ACL
- RBAC

کنترل مدیریتی

- سیاست‌ها
- رویه‌ها
- ممیزی

۳-۱۳ شاخص‌های عملکرد

KPI -۰۱

دارایی‌های ثبت‌شده

هدف: ۱۰۰%

KPI -۰۲

دارایی‌های دارای مالک

هدف: ۱۰۰%

KPI -۰۳

دارایی‌های طبقه‌بندی‌شده

هدف: ۱۰۰%

KPI -۰٤

بازبینی سالانه دارایی‌ها

هدف: ۱۰۰%

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳-۱۴ ممیزی مدیریت دارایی

موارد ممیزی:

- کامل بودن Asset Register
- مالکیت دارایی
- طبقه‌بندی اطلاعات
- وضعیت دارایی‌ها
- انطباق با سیاست‌ها

۳-۱۵ خروجی‌های مورد انتظار

- فهرست کامل دارایی‌ها
- طبقه‌بندی اطلاعات
- تعیین مالک دارایی
- ارزش‌گذاری دارایی‌ها
- ماتریس CIA
- مستندات ممیزی

منابع و مراجع فصل سوم

استانداردهای بین‌المللی

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- ISO/IEC ۲۷۰۰۵

چارچوب‌های امنیتی

- NIST SP ۸۰۰-۵۳

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- NIST SP ۸۰۰-٦۰
- Center for Internet Security

مستندات تخصصی

- Wazuh Documentation
- Fortinet Security Best Practices
- VMware Security Configuration Guide

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل چهارم: مدیریت ریسک امنیت اطلاعات

٤-١ مقدمه

مدیریت ریسک امنیت اطلاعات فرآیندی نظام‌مند برای شناسایی، تحلیل، ارزیابی، کنترل و پایش ریسک‌های مرتبط با دارایی‌های اطلاعاتی سازمان است.

هدف اصلی مدیریت ریسک، کاهش احتمال وقوع رخدادهای امنیتی و به حداقل رساندن اثرات ناشی از آن‌ها بر فعالیت‌های سازمان می‌باشد.

ریسک امنیت اطلاعات زمانی ایجاد می‌شود که یک تهدید بتواند از یک آسیب‌پذیری موجود سوءاستفاده نموده و به یک دارایی ارزشمند آسیب وارد نماید.

فرآیند مدیریت ریسک در این پروژه بر اساس الزامات:

- ISO/IEC ۲۷۰۰۵
- ISO ۳۱۰۰۰
- ISO/IEC ۲۷۰۰۱:۲۰۲۲

طراحی و اجرا می‌گردد.

٤-٢ اهداف مدیریت ریسک

اهداف اصلی عبارتند از:

- شناسایی دارایی‌های حیاتی
- شناسایی تهدیدات
- شناسایی آسیب‌پذیری‌ها
- تعیین میزان ریسک
- اولویت‌بندی اقدامات امنیتی
- کاهش خسارات احتمالی
- افزایش تاب‌آوری سازمان
- بهبود تصمیم‌گیری مدیریتی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳-٤ تعاریف

دارایی(Asset)

هر چیزی که برای سازمان ارزش داشته باشد.

نمونه:

- سرورها
- اطلاعات
- تجهیزات شبکه
- کاربران
- نرم‌افزارها

تهدید(Threat)

هر عامل بالقوه که بتواند به دارایی آسیب برساند.

نمونه:

- هکر
- بدافزار
- باج‌افزار
- خطای انسانی
- قطع برق

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

آسیب‌پذیری(Vulnerability)

ضعفی که امکان سوءاستفاده از دارایی را فراهم کند.

نمونه:

- رمز عبور ضعیف
- Patchنشدن
- تنظیمات اشتباه

ریسک(Risk)

احتمال بهره‌برداری تهدید از آسیب‌پذیری و ایجاد خسارت.

٤-٤ چارچوب مدیریت ریسک

فرآیند مدیریت ریسک شامل مراحل زیر است:

۱ - تعیین دامنه

۲ - شناسایی دارایی‌ها

۳ - شناسایی تهدیدات

٤ - شناسایی آسیب‌پذیری‌ها

٥ - تحلیل ریسک

٦- ارزیابی ریسک

۷- انتخاب روش برخورد

۸ - پایش مستمر

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

٤-٥ تعیین دامنه ارزیابی

دامنه این ارزیابی شامل:

زیرساخت مجازی سازی

- VMware ESXi
- vCenter
- Virtual Machines

تجهیزات امنیتی

- FortiGate ۱۰۰F
- FortiAnalyzer
- Wazuh

سرورها

- Active Directory
- DNS
- DHCP
- SQL Server
- File Server

تجهیزات شبکه

- Switch
- Router
- Wireless

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

کاربران

- مدیران
- کارشناسان
- پیمانکاران

٤-٦ شناسایی دارایی‌ها

دارایی‌ها بر اساس ارزش کسب‌وکاری شناسایی می‌شوند.

دارایی‌های حیاتی

دارایی	شناسه
Active Directory	A-۰۱
VMware Cluster	A-۰۲
FortiGate	A-۰۳
SQL Server	A-۰٤
Backup Server	A-۰٥
File Server	A-۰٦
Internet Link	A-۰۷
کاربران	A-۰۸

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۴-۷ شناسایی تهدیدات

تهدیدات انسانی

- نفوذگر خارجی
- کاربر ناراضی
- خطای کاربر
- پیمانکار غیرمجاز

تهدیدات فنی

- بدافزار
- باج‌افزار
- حملات DDoS
- Exploit

تهدیدات محیطی

- آتش‌سوزی
- زلزله
- سیل
- قطع برق

تهدیدات مدیریتی

- نبود مستندات
- نبود Backup
- نبود آموزش

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸-٤ شناسایی آسیب‌پذیری‌ها

نمونه آسیب‌پذیری‌های رایج:

Active Directory

- رمز عبور ضعیف
- Administratorمشترک
- عدم MFA

VMware

- Snapshotطولانی
- Patchنشدن
- دسترسی زیاد

FortiGate

- Firmwareقدیمی
- Ruleاضافی
- NATاشتباه

کاربران

- فیشینگ
- رمز عبور ضعیف
- نصب نرم‌افزار غیرمجاز

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹-٤ روش محاسبه ریسک

ریسک از رابطه زیر محاسبه می‌شود:

$$Risk = Likelihood \times Impact$$

احتمال وقوع

شرح	امتیاز
بسیار کم	۱
کم	۲
متوسط	۳
زیاد	۴
بسیار زیاد	۵

میزان اثر

شرح	امتیاز
ناچیز	۱
کم	۲
متوسط	۳
زیاد	۴
بحرانی	۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۴-۱۰ ماتریس ریسک

اثر / احتمال	۱	۲	۳	۴	۵
۵	۵	۱۰	۱۵	۲۰	۲۵
۴	۴	۸	۱۲	۱۶	۲۰
۳	۳	۶	۹	۱۲	۱۵
۲	۲	۴	۶	۸	۱۰
۱	۱	۲	۳	۴	۵

۴-۱۱ سطح‌بندی ریسک

سطح	امتیاز
پایین	۱تا ۵
متوسط	۶تا ۱۰
بالا	۱۱تا ۱۵
بحرانی	۱۶تا ۲۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۲-٤ ثبت ریسک‌ها

R -۰۰۱

دارایی:

Active Directory

تهدید:

نفوذ

آسیب‌پذیری:

رمز ضعیف

احتمال:

۴

اثر:

۵

ریسک:

۲۰

وضعیت:

بحرانی

R -۰۰۲

دارایی:

VMware

تهدید:

باج افزار

آسیب‌پذیری:

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

Patchنشدن

احتمال:

۳

اثر:

۵

ریسک:

۱۵

R - ۰۰۳

دارایی:

FortiGate

تهدید:

دسترسی غیرمجاز

آسیب‌پذیری:

تنظیمات اشتباه

احتمال:

۳

اثر:

۴

ریسک:

۱۲

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

R -۰۰٤

دارایی:

SQL Server

تهدید:

نشت اطلاعات

آسیب‌پذیری:

دسترسی بیش از حد

احتمال:

۴

اثر:

۵

ریسک:

۲۰

R-۰۰۵

دارایی:

Backup Server

تهدید:

خرابی سخت‌افزار

احتمال:

۲

اثر:

۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک:

۱۰

۱۳-٤ روش‌های برخورد با ریسک

اجتناب(Avoid)

حذف کامل فعالیت پرریسک

کاهش(Mitigate)

پیاده‌سازی کنترل‌های امنیتی

انتقال(Transfer)

بیمه یا قرارداد

پذیرش(Accept)

پذیرش آگاهانه ریسک

۱٤-٤ برنامه کاهش ریسک

اقدام	ریسک
MFA	نفوذAD
Backup + EDR	باج افزار
DLP	نشت اطلاعات
آموزش کاربران	حمله فیشینگ
HA	خرابیVMware

۴-۱۵ پایش و بازنگری

بازبینی ریسک‌ها در شرایط زیر انجام می‌شود:

- سالانه
- تغییر زیرساخت
- وقوع رخداد
- تغییر قوانین
- تغییر سرویس‌ها

۴-۱۶ شاخص‌های عملکرد

KPI -۰۱

ریسک‌های بحرانی رفع شده

هدف:

۹۰٪

KPI -۰۲

آسیب‌پذیری‌های بحرانی رفع شده

هدف:

۹۵٪

KPI -۰۳

زمان رفع ریسک

هدف:

کمتر از ۳۰ روز

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۷-٤ خروجی‌های فصل

- Asset Register
- Threat Register
- Vulnerability Register
- Risk Register
- Risk Treatment Plan
- گزارش تحلیل ریسک

منابع و مراجع فصل چهارم

- ISO/IEC ۲۷۰۰۵
- ISO ۳۱۰۰۰
- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- NIST SP ۸۰۰-۳۰
- NIST SP ۸۰۰-۳۷
- Center for Internet Security
- MITRE ATT&CK Framework
- OWASP Risk Rating Methodology

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل پنجم: کنترل‌های امنیتی و مدیریت دسترسی

۵-۱ مقدمه

کنترل‌های امنیتی مجموعه‌ای از اقدامات مدیریتی، فنی، عملیاتی و فیزیکی هستند که با هدف حفاظت از دارایی‌های اطلاعاتی سازمان در برابر تهدیدات و کاهش ریسک‌های امنیتی طراحی و پیاده‌سازی می‌شوند.

هدف از این فصل، تشریح چارچوب کنترل‌های امنیتی مورد نیاز جهت حفاظت از اطلاعات، سامانه‌ها، کاربران و زیرساخت‌های فناوری اطلاعات سازمان می‌باشد.

کنترل‌های این فصل بر اساس الزامات:

- ISO ۲۷۰۰۱:۲۰۲۲
- ISO ۲۷۰۰۲:۲۰۲۲
- NIST Cybersecurity Framework
- CIS Controls v۸

تعریف گردیده‌اند.

۵-۲ اهداف کنترل‌های امنیتی

اهداف اصلی عبارتند از:

- حفاظت از محرمانگی اطلاعات
- حفظ صحت اطلاعات
- تضمین دسترس‌پذیری اطلاعات
- کاهش ریسک‌های امنیتی
- جلوگیری از دسترسی غیرمجاز
- کنترل فعالیت کاربران
- افزایش تاب‌آوری سایبری
- انطباق با الزامات قانونی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳-۵ دسته‌بندی کنترل‌ها

کنترل‌ها در چهار گروه اصلی طبقه‌بندی می‌شوند:

کنترل‌های مدیریتی

Policy
Procedure
Guideline

کنترل‌های فنی

Firewall
SIEM
EDR
Access Control

کنترل‌های فیزیکی

Door Control
CCTV
UPS

کنترل‌های عملیاتی

Backup
Monitoring
Patch Management

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

٤-٥ کنترل دسترسی(Access Control)

هدف

اطمینان از دسترسی افراد مجاز به منابع مورد نیاز و جلوگیری از دسترسی غیرمجاز.

اصول کنترل دسترسی

Least Privilege

هر کاربر صرفاً به منابع مورد نیاز خود دسترسی خواهد داشت.

Need To Know

اطلاعات صرفاً در اختیار افراد نیازمند قرار می‌گیرد.

Separation Of Duties

وظایف حساس میان افراد مختلف توزیع می‌شود.

Accountability

تمامی فعالیت‌ها قابل ثبت و رهگیری خواهند بود.

۵-۵ مدیریت حساب‌های کاربری

برای هر کاربر:

- شناسه منحصر به فرد
- مالک مشخص
- سطح دسترسی مشخص

تعریف می‌شود.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

انواع حساب‌ها

User Account

کاربران عادی

Privileged Account

مدیران سیستم

Service Account

سرویس‌ها

Temporary Account

پیمانکاران

۶-۵ چرخه عمر دسترسی

ایجاد دسترسی

بر اساس درخواست رسمی

تغییر دسترسی

با تأیید مالک سامانه

لغو دسترسی

پس از تغییر شغل یا خروج کاربر

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بازبینی دسترسی

حداقل هر شش ماه یکبار

۵-۷ سیاست رمز عبور

حداقل طول

۱۲کاراکتر

پیچیدگی

- حرف کوچک
- حرف بزرگ
- عدد
- نماد

انقضا

۹۰روز

جلوگیری از تکرار

حداقل ۵ رمز قبلی

قفل حساب

۵تلاش ناموفق

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵-۸ احراز هویت چندعاملی(MFA)

برای سامانه‌های حساس الزامی است.

شامل:

- VPN
- FortiGate
- VMware
- Email
- Remote Access

۵-۹ مدیریت دسترسی مدیران

حساب‌های مدیریتی باید:

- نام اختصاصی داشته باشند
- لاگ شوند
- محدود شوند
- تحت MFA باشند

استفاده از Administrator مشترک ممنوع است.

۵-۱۰ مدیریت نشست‌ها

نشست‌های کاربران باید:

- Timeoutداشته باشند
- ثبت شوند
- کنترل شوند

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵-۱۱ کنترل دسترسی شبکه

Network Segmentation

تفکیک:

- کاربران
- سرورها
- مدیریت
- DMZ

VLAN

ایجاد VLAN مجزا برای:

- کاربران
- سرورها
- VoIP
- تجهیزات امنیتی

ACL

تعریف قوانین دسترسی

۵-۱۲ امنیت تجهیزات شبکه

تمام تجهیزات باید:

- Backup Configurationداشته باشند .
- Firmwareبروزرسانی شود .
- دسترسی مدیریتی محدود باشد .
- لاگ ارسال کنند .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۳-۵ امنیت فایروال

مدیریت Rule ها

Ruleها باید:

- مستند باشند .
- شماره داشته باشند .
- مالک داشته باشند .

بازبینی

هر ۶ ماه

حذف Rule های بلااستفاده

الزامی است.

۱۴-۵ امنیتVMware

دسترسی

فقط مدیران مجاز

vCenter

MFAفعال

Snapshot

بیش از ۷۲ ساعت مجاز نیست.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ESXi

Patch Managementفعال

لاگ

ارسال بهSIEM

۵-۱۵ امنیت سیستم عامل

Windows

- Windows Defender
- Audit Policy
- GPO
- Patch

Linux

- SSH Hardening
- Sudo Control
- Log Monitoring

۵-۱۶ امنیت پایگاه داده

کنترل دسترسی

Role Based Access

رمزنگاری

Encryption At Rest

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

لاگ

Audit Logging

Backup

روزانه

۵-۱۷ امنیت ایستگاه‌های کاری

آنتی ویروس

الزامی

USB Control

کنترل شده

Screen Lock

حداکثر ۱۰ دقیقه

Software Installation

صرفاً توسط IT

۵-۱۸ امنیت ایمیل

Anti Spam

فعال

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

Anti Phishing

فعال

Attachment Control

فعال

SPF

فعال

DKIM

فعال

DMARC

فعال

۱۹-۵ امنیت ارتباطات

VPN

رمزنگاری شده

TLS

نسخه‌های قدیمی غیرفعال

Remote Access

کنترل شده.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵-۲۰ مدیریت تغییرات امنیتی

هر تغییر باید:

- ثبت شود
- تأیید شود
- تست شود
- مستندسازی شود

۵-۲۱ مدیریت وصله‌های امنیتی

Critical

کمتر از ۷ روز

High

کمتر از ۳۰ روز

Medium

کمتر از ۶۰ روز

Low

کمتر از ۹۰ روز

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵-۲۲ ثبت وقایع و لاگ‌ها

تمام سامانه‌های حیاتی باید لاگ تولید نمایند.

شامل:

- Active Directory
- VMware
- FortiGate
- Database
- Linux
- Windows

۵-۲۳ مانیتورینگ امنیتی

مانیتورینگ باید شامل:

- کاربران
- سرورها
- تجهیزات شبکه
- فایروال
- ماشین‌های مجازی

باشد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵-۲٤ کنترل‌های فیزیکی

اتاق سرور

- قفل مناسب
- دوربین
- کنترل ورود

برق

- UPS
- ژنراتور

اطفاء حریق

سامانه اطفاء مناسب

۵-۲۵ مدیریت تجهیزات قابل حمل

شامل:

- لپ‌تاپ
- هارد اکسترنال
- فلش

الزامات:

- رمزنگاری
- ثبت دارایی
- کنترل استفاده

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۶-۵ شاخص‌های عملکرد

KPI -۰۱

درصد حساب‌های دارایMFA

هدف: ۱۰۰%

KPI -۰۲

Patch Compliance

هدف: ۹۵%

KPI -۰۳

غیرفعال‌سازی حساب‌های بلااستفاده

هدف: ۱۰۰%

KPI -۰٤

پوشش لاگ‌گیری

هدف: ۱۰۰%

KPI-۰۵

موفقیتBackup

هدف: ۹۸%

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵-۲۷ ممیزی کنترل‌های امنیتی

موارد ممیزی:

- دسترسی‌ها
- حساب‌ها
- فایروال
- VMware
- Backup
- Patch
- MFA
- لاگ‌ها

۵-۲۸ خروجی‌های فصل

- Access Control Policy
- Password Policy
- Network Security Policy
- Firewall Policy
- Patch Management Policy
- Logging Policy
- MFA Policy
- Change Management Policy

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

منابع و مراجع فصل پنجم

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- NIST SP ۸۰۰-۵۳ Rev.۵
- NIST SP ۸۰۰-٦۳
- Center for Internet Security
- Fortinet Security Best Practices
- VMware Security Configuration Guide
- OWASP Foundation Security Guidelines

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل ششم: مدیریت رخدادهای امنیتی(Incident Management)

۶-۱ قدمه

هیچ سازمانی در دنیا وجود ندارد که صد درصد امن باشد. حتی بزرگ‌ترین شرکت‌ها و سازمان‌های دولتی نیز ممکن است با حملات سایبری، خطاهای انسانی، خرابی تجهیزات یا نشت اطلاعات مواجه شوند.

بنابراین هدف امنیت اطلاعات فقط جلوگیری از حمله نیست، بلکه توانایی **تشخیص سریع، واکنش سریع و بازگرداندن سریع سرویس‌ها** است.

مدیریت رخدادهای امنیتی فرآیندی است که به سازمان کمک می‌کند:

- حملات را زودتر تشخیص دهد .
- خسارت را محدود کند .
- سرویس‌ها را سریع‌تر بازیابی کند .
- از تکرار رخداد جلوگیری کند .

٦-۲ چرا صمت به این بخش نیاز دارد؟

فرض کنید :

سناریو اول

یک کارمند روی فایل آلوده کلیک می‌کند.

باج‌افزار وارد شبکه می‌شود.

اگر هیچ فرآیندی وجود نداشته باشد:

- فایل سرورها رمز می‌شوند .
- سیستم اتوماسیون می‌خوابد .
- خدمات سازمان متوقف می‌شود .
-

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

اما اگر فرآیند مدیریت رخداد وجود داشته باشد:

- Wazuhهشدار می‌دهد .
- مسئول IT مطلع می‌شود .
- سیستم آلوده قرنطینه می‌شود .
- خسارت محدود می‌شود .

سناریو دوم

رمز عبور مدیر شبکه لو می‌رود.

هکر وارد VPN می‌شود.

اگر هیچ مانیتورینگی نباشد:

ممکن است هفته‌ها داخل شبکه بماند.

اما SIEM می‌گوید:

ورود غیرعادی از IP ناشناس انجام شده است.

و تیم امنیت وارد عمل می‌شود.

۳-٦ اهداف مدیریت رخداد

هدف فقط پیدا کردن حمله نیست.

اهداف اصلی:

- کاهش خسارت
- کاهش زمان تشخیص
- کاهش زمان بازیابی
- حفظ شواهد
- جلوگیری از تکرار حادثه

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۴-۶تعریف رخداد امنیتی

رخداد امنیتی هر اتفاقی است که:

محرمانگی یا صحت یا دسترس‌پذیری اطلاعات را تهدید کند.

٦-۵ نمونه رخدادها

دسترسی غیرمجاز

ورود فرد غیرمجاز به سیستم

باج‌افزار

رمز شدن فایل‌ها

بدافزار

آلودگی سیستم‌ها

فیشینگ

سرقت رمز کاربران

نشت اطلاعات

خروج اطلاعات محرمانه

اختلال سرویس

قطع سامانه‌های حیاتی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

٦-٦ چرخه مدیریت رخداد

فرآیند شامل شش مرحله است:

۱- شناسایی

۲- ثبت

۳- تحلیل

٤- مهار

٥- رفع

٦- گزارش نهایی

٦-٧ مرحله شناسایی

رخدادها از طریق موارد زیر شناسایی می‌شوند:

Wazuh

مثلاً:

۱۰بار Login ناموفق

FortiAnalyzer

مثلاً:

IPS Attack

کاربران

گزارش رفتار غیرعادی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

واحدIT

گزارش خرابی سرویس

۶-۸ مرحله ثبت

تمام رخدادها باید ثبت شوند.

اطلاعات ثبت شده:

- تاریخ
- ساعت
- سیستم درگیر
- فرد گزارش دهنده
- سطح اهمیت

۶-۹ مرحله تحلیل

هدف:

تشخیص علت اصلی

بررسی:

- چه اتفاقی افتاده؟
- از کجا شروع شده؟
- چه سیستم‌هایی درگیر هستند؟
- میزان خسارت چقدر است؟

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۰-۶ مرحله مهار

هدف:

جلوگیری از گسترش خسارت

مثال:

باج افزار

قطع ارتباط سیستم

نفوذ

مسدودسازی حساب

بدافزار

قرنطینه سیستم

۱۱-٦ مرحله رفع

پس از مهار:

- حذف بدافزار
- اصلاح تنظیمات
- Patch
- تغییر رمزها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۶-۱۲ مرحله بازیابی

بازگرداندن سرویس‌ها

مثلاً:

- Restore Backup
- راه‌اندازی VM
- بازگردانی دیتابیس

٦-۱۳ گزارش نهایی

پس از پایان رخداد:

- علت
- خسارت
- اقدامات انجام شده
- درس آموخته‌ها

مستند می‌شود.

۶-۱۴ طبقه‌بندی رخدادها

سطح ۱

کم اهمیت

نمونه:

قفل شدن حساب کاربر

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

سطح ۲

متوسط

نمونه:

خرابی سرویس محدود

سطح ۳

بالا

نمونه:

آلودگی چند سیستم

سطح ۴

بحرانی

نمونه:

باج افزار
نفوذ گسترده
نشت اطلاعات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۵-۶ نقش Wazuh در پروژه

چرا Wazuh می‌خواهیم؟

زیرا:

- لاگ همه سرورها را جمع می‌کند .
- حملات را تشخیص می‌دهد .
- هشدار تولید می‌کند .
- داشبورد ارائه می‌دهد .

مثال:

کاربری ساعت ۳ صبح وارد سرور شود.

Wazuhهشدار می‌دهد.

۱۶-۶ نقشFortiAnalyzer

چرا FortiAnalyzer می‌خواهیم؟

چون FortiGate روزانه هزاران لاگ تولید می‌کند.

خواندن دستی این لاگ‌ها غیرممکن است.

FortiAnalyzer:

- لاگ‌ها را ذخیره می‌کند .
- تحلیل می‌کند .
- گزارش می‌دهد .
- حملات را نمایش می‌دهد .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۶-۱۷ نقش SIEM

قبل از SIEM:

هر دستگاه جداگانه لاگ دارد.

بعد از SIEM:

همه لاگ‌ها یکجا جمع می‌شوند.

مثلاً:

FortiGate

Windows Server

VMware

Active Directory

همزمان بررسی می‌شوند.

۶-۱۸ مثال واقعی برای صمت

سناریو:

کاربر VPN وصل می‌شود.

↓

وارد Domain می‌شود.

↓

فایل زیادی دانلود می‌کند.

↓

به SQL وصل می‌شود.

↓

داده استخراج می‌کند.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بدون:SIEM

هیچ کس متوجه نمی‌شود.

با:SIEM

تمام این رویدادها به هم مرتبط می‌شوند.

هشدار تولید می‌شود.

۱۹-۶ KPI ها

زمان تشخیص

(MTTD)

هدف:

کمتر از ۱۵ دقیقه

زمان پاسخ

(MTTR)

هدف:

کمتر از ۳۰ دقیقه

رخدادهای بحرانی

هدف:

کاهش سالانه

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۶-۲۰ خروجی‌های این فصل

پس از اجرای این بخش سازمان دارای:

- فرآیند پاسخ به رخداد
- تیم پاسخگویی
- Playbookها
- Wazuh
- FortiAnalyzer
- داشبورد امنیتی
- گزارش‌های مدیریتی

خواهد بود.

منابع و مراجع

- ISO/IEC ۲۷۰۳۵
- NIST SP ۸۰۰-۶۱ Rev.۲
- NIST Cybersecurity Framework
- SANS Institute
- Wazuh Documentation
- FortiAnalyzer Documentation

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل هفتم: مدیریت آسیب‌پذیری(Vulnerability Management)

۷-۱ مقدمه

امروزه بخش عمده‌ای از حملات سایبری از طریق سوءاستفاده از آسیب‌پذیری‌های شناخته شده صورت می‌گیرد.
بسیاری از سازمان‌ها قربانی هک نمی‌شوند چون هدف قرار گرفته‌اند؛ بلکه قربانی می‌شوند چون یک ضعف شناخته شده را برطرف نکرده‌اند.

آسیب‌پذیری می‌تواند در:

- سیستم عامل
- نرم‌افزار
- فایروال
- پایگاه داده
- تجهیزات شبکه
- تنظیمات امنیتی
- فرآیندهای سازمانی

وجود داشته باشد.

مدیریت آسیب‌پذیری فرآیندی مستمر برای شناسایی، ارزیابی، اولویت‌بندی، رفع و پایش نقاط ضعف امنیتی سازمان است.

۷-۲ چرا سازمان به مدیریت آسیب‌پذیری نیاز دارد؟

فرض کنید:

FortiGateسازمان سه سال آپدیت نشده است.

هکر یک Exploit عمومی پیدا می‌کند.

در عرض چند دقیقه می‌تواند کنترل فایروال را به دست بگیرد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

یا:

یکی از سرورهای ویندوز دارای آسیب‌پذیری RDP است.

Patchنصب نشده است.

مهاجم از اینترنت وارد می‌شود.

کل شبکه آلوده می‌شود.

در بسیاری از رخدادهای امنیتی علت اصلی:

- ضعف در Patch Management
- ضعف در پیکربندی
- ضعف در بروزرسانی

است.

۳-۷ اهداف مدیریت آسیب‌پذیری

اهداف عبارتند از:

- کشف ضعف‌های امنیتی
- کاهش سطح حمله
- اولویت‌بندی ریسک‌ها
- کاهش احتمال نفوذ
- بهبود وضعیت امنیتی
- افزایش تاب‌آوری سایبری

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۷-۴ تعریف آسیب‌پذیری

آسیب‌پذیری هر نقطه ضعف فنی، مدیریتی یا عملیاتی است که توسط تهدیدات قابل سوءاستفاده باشد.

نمونه آسیب‌پذیری‌های فنی

- سیستم عامل قدیمی
- Firmwareقدیمی
- رمز عبور ضعیف
- سرویس‌های غیرضروری
- پورت‌های باز

نمونه آسیب‌پذیری‌های مدیریتی

- نبود سیاست امنیتی
- نبود آموزش
- نبود مدیریت تغییر

نمونه آسیب‌پذیری‌های عملیاتی

- Backupنامناسب
- نبود مانیتورینگ
- مستندسازی ضعیف

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۷-۵ فرآیند مدیریت آسیب‌پذیری

فرآیند شامل مراحل زیر است:

۱ - شناسایی دارایی‌ها

۲- اسکن آسیب‌پذیری

۳- تحلیل نتایج

۴- اولویت‌بندی

۵- اصلاح

۶- اعتبارسنجی

۷- پایش مستمر

۷-٦ شناسایی دارایی‌های هدف

دارایی‌های زیر باید تحت ارزیابی قرار گیرند:

تجهیزات امنیتی

- FortiGate
- FortiAnalyzer

زیرساخت مجازی سازی

- VMware ESXi
- vCenter

سرورها

- Active Directory
- DNS
- DHCP
- SQL
- File Server

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

سیستم‌های کاربران

- Desktop
- Laptop

تجهیزات شبکه

- Router
- Switch

۷-۷ روش‌های شناسایی آسیب‌پذیری

اسکن خودکار

ابزارها:

- Wazuh Vulnerability Detection
- Nessus
- OpenVAS
- Greenbone

بررسی دستی

بررسی:

- تنظیمات
- سرویس‌ها
- Ruleها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

تست نفوذ

شبیه‌سازی حمله واقعی

ممیزی امنیتی

بررسی انطباق با استانداردها

Wazuh ۷-۸ و مدیریت آسیب‌پذیری

یکی از دلایل مهم انتخاب Wazuh قابلیت Vulnerability Detection است.

Wazuhمی‌تواند:

- نسخه سیستم عامل را بررسی کند .
- نرم‌افزارهای نصب شده را شناسایی کند .
- CVEهای مرتبط را پیدا کند .
- هشدار صادر کند .

مثال

سرور۲۰۱۹ Windows Server

دارای:

CVE-۲۰۲۵-XXXX

باشد.

Wazuhهشدار می‌دهد:

Severity: High

Asset: Server-۰۱

Status: Unpatched

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹-۷ امتیازدهیCVSS

برای تعیین شدت آسیب‌پذیری از استاندارد CVSS استفاده می‌شود.

Critical

امتیاز:

۹تا ۱۰

رفع:

حداکثر ۷ روز

High

امتیاز:

۷تا ۸.۹

رفع:

حداکثر ۳۰ روز

Medium

امتیاز:

۴تا ۶.۹

رفع:

حداکثر ۶۰ روز

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

Low

امتیاز:

۰تا ۳.۹

رفع:

حداکثر ۹۰ روز

۷-۱۰ Patch Management

مقدمه

Patch Management فرآیند نصب وصله‌های امنیتی و بروزرسانی‌ها می‌باشد.

اهداف

- رفع آسیب‌پذیری‌ها
- افزایش پایداری
- کاهش ریسک نفوذ

۷-۱۱ چرخه مدیریت وصله

شناسایی Patch

ارزیابی

بررسی اثرات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

تست

در محیط آزمایشی

استقرار

در محیط عملیاتی

اعتبارسنجی

اطمینان از نصب موفق

۷-۱۲ مدیریت آسیب‌پذیری VMware

موارد کنترل:

- Patch ESXi
- Patch vCenter
- Snapshotهای قدیمی
- دسترسی Root
- تنظیمات Host

ریسک‌های رایج

- Host Compromise
- VM Escape
- Credential Theft

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۳-۷مدیریت آسیب‌پذیری FortiGate

موارد بررسی:

- Firmware
- SSL VPN
- Admin Access
- Policy Review
- IPS Status

نمونه ریسک

فعال بودن SSL-VPN آسیب‌پذیر

اقدام اصلاحی

Firmware Upgrade

۱۴-۷ مدیریت آسیب‌پذیری Active Directory

موارد بررسی:

- Password Policy
- Kerberos Settings
- Domain Admin Accounts
- Delegation

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

تهدیدات رایج

- Pass The Hash
- Kerberoasting
- Privilege Escalation

۷-۱۵ مدیریت آسیب‌پذیری پایگاه داده

بررسی:

- دسترسی‌ها
- رمزنگاری
- Audit Logging
- Backup

۷-۱۶ مدیریت آسیب‌پذیری کاربران

کاربران نیز یک دارایی پرریسک محسوب می‌شوند.

موارد ارزیابی:

- آگاهی امنیتی
- فیشینگ
- استفاده از رمز عبور ضعیف

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۷-۱۷ تست نفوذ

هدف:

ارزیابی عملی امنیت

دامنه:

- External
- Internal
- Web Application

خروجی:

- یافته‌ها
- شدت ریسک
- پیشنهادات اصلاحی

۷-۱۸ شاخص‌های عملکرد

KPI-۰۱

درصد آسیب‌پذیری‌های بحرانی رفع شده

هدف:

۹۵٪

KPI-۰۲

زمان رفع آسیب‌پذیری بحرانی

هدف:

کمتر از ۷ روز

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

KPI-۰۳

نرخ انطباقPatch

هدف:

۹۵٪

KPI-۰٤

پوشش اسکن آسیب‌پذیری

هدف:

۱۰۰٪

۷-۱۹ گزارش‌های مدیریتی

گزارش ماهانه شامل:

- تعداد آسیب‌پذیری‌ها
- روند تغییرات
- وضعیت اصلاح
- ریسک‌های بحرانی
- وضعیت Patch

۷-۲۰ ارتباط باSIEM

SIEMرخداد را تشخیص می‌دهد.

Vulnerability Managementعلت رخداد را پیدا می‌کند.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

مثال:

SIEM :

نفوذ تشخیص داده شد.

↓

تحلیل:

سرور Patch نشده بود.

↓

Vulnerability Management:

علت اصلی مشخص می‌شود.

۷-۲۱ خروجی‌های فصل

پس از اجرای این فصل سازمان دارای:

- برنامه مدیریت آسیب‌پذیری
- فرآیند Patch Management
- چرخه اسکن امنیتی
- گزارش‌های مدیریتی
- داشبوردهای امنیتی
- فرآیند تست نفوذ

خواهد بود.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۷-۲۲ مزیت برای سازمان صمت

اجرای این فصل باعث می‌شود:

- ضعف‌ها قبل از مهاجم کشف شوند .
- ریسک نفوذ کاهش یابد .
- هزینه رخدادها کاهش یابد .
- آمادگی ممیزی افزایش یابد .
- سطح امنیت زیرساخت ارتقا پیدا کند .
- داده‌های سازمان بهتر محافظت شوند .

منابع و مراجع فصل هفتم

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- ISO/IEC ۲۷۰۰۵
- NIST SP ۸۰۰-٤۰
- NIST SP ۸۰۰-۱۱۵
- MITRE
- FIRST
- Wazuh Vulnerability Detection Documentation
- OpenVAS Documentation

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل هشتم: تداوم کسب‌وکار و بازیابی بحران(Business Continuity & Disaster Recovery)

۸-۱ مقدمه

وابستگی سازمان‌ها به سامانه‌های فناوری اطلاعات روزبه‌روز افزایش یافته است. از کار افتادن سرورها، تجهیزات شبکه، سامانه‌های نرم‌افزاری یا مراکز داده می‌تواند موجب توقف خدمات، اختلال در فرآیندهای سازمانی، از دست رفتن اطلاعات و خسارات مالی و اعتباری شود.

هدف از این فصل، ایجاد سازوکارهایی جهت حفظ تداوم خدمات حیاتی و بازیابی سریع سامانه‌ها در شرایط بحران می‌باشد.

۸-۲ اهداف

اهداف اصلی عبارتند از:

- حفظ تداوم ارائه خدمات
- کاهش زمان توقف سرویس‌ها
- حفاظت از اطلاعات حیاتی
- افزایش تاب‌آوری سازمان
- آمادگی در برابر بحران‌ها
- کاهش خسارات مالی و عملیاتی
- انطباق با الزامات پدافند غیرعامل و امنیت اطلاعات

۸-۳ تعاریف

تداوم کسب‌وکار(BCP)

مجموعه برنامه‌ها و فرآیندهایی که امکان ادامه فعالیت سازمان را در شرایط بحرانی فراهم می‌نماید.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بازیابی بحران(DRP)

مجموعه اقدامات فنی و عملیاتی برای بازگرداندن سامانه‌ها و اطلاعات پس از وقوع بحران.

بحران(Disaster)

هر رویدادی که موجب توقف یا اختلال جدی در فعالیت‌های سازمان شود.

نمونه‌ها:

- آتش‌سوزی
- قطعی برق طولانی
- خرابی سرور
- حمله باج‌افزاری
- از دست رفتن داده‌ها
- خرابی تجهیزات ذخیره‌سازی
- اختلال لینک ارتباطی

۸-٤ ضرورت اجرای طرح

در بسیاری از سازمان‌ها اطلاعات مهم‌تر از تجهیزات هستند.

یک سرور قابل جایگزینی است اما اطلاعات از دست رفته ممکن است هرگز قابل بازگشت نباشد.

پیاده‌سازی برنامه تداوم کسب‌وکار باعث می‌شود:

- خدمات حیاتی متوقف نشوند .
- اطلاعات از بین نروند .
- زمان بازیابی کاهش یابد .
- اعتماد کاربران حفظ شود .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵-۸تحلیل تأثیر کسب‌وکار(BIA)

در این مرحله فرآیندها و سامانه‌های حیاتی سازمان شناسایی می‌شوند.

نمونه:

سامانه	اهمیت
اتوماسیون اداری	بسیار بالا
سامانه مالی	بسیار بالا
پایگاه داده	بسیار بالا
ایمیل سازمانی	بالا
فایل سرور	بالا

هدف این تحلیل مشخص کردن اولویت بازیابی سرویس‌ها است.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸-٦ سناریوهای بحران

سناریوهای مورد بررسی شامل:

خرابی سرور

از کار افتادن فیزیکی سرور

خرابی ذخیره‌ساز

از دست رفتن داده‌ها

حمله باج‌افزاری

رمز شدن فایل‌ها

خطای انسانی

حذف اطلاعات

قطعی برق

از دسترس خارج شدن تجهیزات

خرابی تجهیزات شبکه

قطع ارتباطات

بلایای طبیعی

زلزله، آتش‌سوزی و سیل

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸-۷ راهبردهای تداوم خدمات

برای هر سرویس حیاتی راهبرد مناسبی تعیین می‌شود.

شامل:

- Backup
- Replication
- High Availability
- Failover
- Site Recovery

۸-۸ High Availability (HA)

هدف:

جلوگیری از توقف سرویس

در ساختار HA:

در صورت خرابی یک تجهیز، تجهیز دوم به‌صورت خودکار سرویس را ادامه می‌دهد.

مزایا:

- کاهش Downtime
- افزایش پایداری
- افزایش دسترس‌پذیری

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

نمونه‌ها:

- VMware HA
- FortiGate HA
- SQL Cluster

۸-۹ پشتیبان‌گیری(Backup)

Backupیکی از مهم‌ترین کنترل‌های امنیتی و عملیاتی است.

اهداف:

- حفاظت از اطلاعات
- بازیابی داده‌ها
- مقابله با باج‌افزار

انواع:Backup

Full Backup

نسخه کامل

Incremental Backup

فقط تغییرات

Differential Backup

تغییرات نسبت به آخرین نسخه کامل

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸-۱۰ سیاست پشتیبان‌گیری

حداقل الزامات:

- Backupروزانه
- نگهداری نسخه‌های متعدد
- ذخیره خارج از سرور اصلی
- تست بازیابی دوره‌ای

۸-۱۱ قانون ۳-۲-۱

پیشنهاد می‌شود:

- ۳نسخه از اطلاعات
- ۲رسانه متفاوت
- ۱نسخه خارج از سایت

نگهداری شود.

۸-۱۲ بازیابی اطلاعات

بازیابی باید شامل:

- فایل‌ها
- پایگاه داده
- ماشین‌های مجازی
- تنظیمات تجهیزات

باشد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸-۱۳ مجازی‌سازی و تداوم خدمات

زیرساخت VMware نقش کلیدی در بازیابی سریع سرویس‌ها دارد.

مزایا:

- مهاجرت سریع VM ها
- Snapshot
- Replication
- HA

۸-۱٤ مراکز جایگزین

در صورت نیاز، سازمان می‌تواند از:

- سایت پشتیبان
- مرکز داده جایگزین
- سرویس ابری

استفاده نماید.

۸-۱۵ اهداف بازیابی

RTO

Recovery Time Objective

حداکثر زمان قابل قبول برای بازگشت سرویس

مثال:

۴ساعت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

RPO

Recovery Point Objective

حداکثر میزان داده قابل از دست رفتن

مثال:

۱ساعت

۸-۱۶ آزمون و مانور

طرح بازیابی باید حداقل سالی یکبار آزمون شود.

نمونه آزمون‌ها:

- Restore Backup
- Failover Test
- Recovery Test

۸-۱۷ نقش Wazuh وSIEM

در شرایط بحران:

- تشخیص رخداد
- شناسایی علت
- ارائه هشدار
- ثبت شواهد

توسط سامانه‌های مانیتورینگ انجام می‌شود.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸-۱۸ نقش FortiAnalyzer

در رخدادهای امنیتی:

- تحلیل لاگ
- شناسایی منبع حمله
- مستندسازی رویداد

انجام می‌شود.

۸-۱۹مسئولیت‌ها

مدیریت ارشد

تصویب سیاست‌ها

واحد فناوری اطلاعات

اجرای برنامه بازیابی

واحد امنیت اطلاعات

مدیریت رخدادهای امنیتی

کاربران

رعایت رویه‌ها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸-۲۰ شاخص‌های عملکرد

KPI -۰۱

موفقیتBackup

هدف:

بیش از ۹۸%

KPI -۰۲

موفقیت بازیابی

هدف:

۱۰۰٪

KPI -۰۳

زمان بازیابی

کمتر از RTO تعریف شده

KPI -۰٤

تعداد مانورهای سالانه

حداقل ۱ بار

۸-۲۱ خروجی‌های مورد انتظار

پس از اجرای این بخش سازمان دارای موارد زیر خواهد بود:

- برنامه تداوم کسب‌وکار (BCP)
- برنامه بازیابی بحران (DRP)

- سیاست Backup
- رویه بازیابی اطلاعات
- سناریوهای بحران
- برنامه آزمون و مانور
- اهداف RTO و RPO
- مستندات پایداری سرویس

مزیت برای سازمان صمت

اجرای این بخش باعث می‌شود:

- خرابی یک سرور کل سازمان را متوقف نکند .
- اطلاعات حیاتی قابل بازیابی باشند .
- زمان توقف سرویس‌ها کاهش یابد .
- اثر حملات باج‌افزاری محدود شود .
- الزامات پدافند غیرعامل و امنیت اطلاعات بهتر پوشش داده شوند .
- سطح تاب‌آوری زیرساخت افزایش یابد .

منابع

- ISO ۲۲۳۰۱
- ISO/IEC ۲۷۰۳۱
- NIST SP ۸۰۰-۳٤
- ISO/IEC ۲۷۰۰۱:۲۰۲۲

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل نهم : مدیریت لاگ ، SIEM و پایش امنیتی (Security Monitoring & SIEM)

۹-۱مقدمه

در زیرساخت‌های امروزی، تجهیزات مختلفی از جمله فایروال‌ها، سرورها، ماشین‌های مجازی، تجهیزات شبکه، پایگاه‌های داده و سامانه‌های کاربردی به‌صورت مداوم رویدادهای مختلفی را ثبت می‌کنند.

این رویدادها که تحت عنوان Log شناخته می‌شوند، یکی از مهم‌ترین منابع تشخیص تهدیدات، تحلیل رخدادها و مدیریت امنیت اطلاعات هستند.

بدون وجود یک سامانه متمرکز مدیریت لاگ وSIEM ، تشخیص حملات و تحلیل رخدادهای امنیتی عملاً بسیار دشوار خواهد بود.

۹-۲ اهداف پروژهSIEM

هدف از پیاده‌سازی سامانه SIEM در سازمان عبارت است از:

- جمع‌آوری متمرکز لاگ‌ها
- تحلیل رخدادهای امنیتی
- تشخیص تهدیدات
- کشف رفتارهای مشکوک
- هشداردهی خودکار
- تولید گزارش‌های مدیریتی
- کاهش زمان تشخیص حملات
- افزایش سطح نظارت امنیتی

۹-۳وضعیت سنتی سازمان‌ها

در بسیاری از سازمان‌ها:

- FortiGate لاگ خودش را دارد .
- VMware لاگ خودش را دارد .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- Windows Server لاگ خودش را دارد .
- SQL لاگ خودش را دارد .

هیچ ارتباطی بین این رویدادها برقرار نمی‌شود.

نتیجه:

ممکن است مهاجم هفته‌ها در شبکه حضور داشته باشد و کسی متوجه نشود.

٤-٩ مفهوم SIEM

SIEMمخفف:

Security Information and Event Management

می‌باشد.

وظیفه: SIEM

- جمع‌آوری لاگ
- نرمال‌سازی
- همبستگی رخدادها
- تحلیل امنیتی
- هشداردهی
- گزارش‌گیری

است.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹-۵ معماری پیشنهادی پروژه

در این پروژه معماری زیر پیشنهاد می‌شود:

FortiGate
|
Windows Servers
|
Linux Servers
|
VMware ESXi
|
Database Servers
|
Network Devices
|
Wazuh
|
Elastic Stack
|
Dashboard
|
Security Team

۹-۶ اجزای اصلی راهکار

Wazuh Manager

هسته مرکزی تحلیل امنیت

وظایف:

- جمع‌آوری رویدادها
- تحلیل
- تولید هشدار
- مدیریتAgent ها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

Wazuh Agent

روی سرورها نصب می‌شود.

نمونه:

- Windows Server
- Linux Server
- Domain Controller

وظایف:

- ارسال لاگ
- بررسی فایل‌ها
- تشخیص تغییرات
- پایش فرآیندها

Indexer

ذخیره اطلاعات

Dashboard

نمایش اطلاعات

FortiAnalyzer

تحلیل تخصصی لاگ‌هایFortiGate

۹-۷ منابع تولید لاگ

تجهیزات امنیتی

- FortiGate
- IPS
- VPN

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

زیرساخت مجازی

- VMware ESXi
- vCenter

سیستم عامل

- Windows Server
- Linux

اکتیودایرکتوری

- Login
- Group Changes
- Privilege Changes

پایگاه داده

- Login
- Query
- Permission Changes

تجهیزات شبکه

- Switch
- Router

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹-۸ انواع رویدادهای قابل مانیتور

Login موفق و ناموفق- تغییر رمز عبور- ساخت کاربر جدید- حذف کاربر- تغییر گروه‌ها

نصب نرم افزار- اجرای فایل مشکوک - اتصال USB - تغییر فایل‌های حیاتی-تغییر Rule فایروال

حملات IPS - حملات VPN

۹-۹ Use Case های امنیتی

این بخش مهم‌ترین قسمت SIEM است.

Use Case شماره ۱

Brute Force Attack اگر: بیش از ۱۰ Login ناموفق در ۵ دقیقه رخ دهد

هشدار صادر شود.

Use Case شماره ۲

Privilege Escalation اگر: کاربر عادی عضو Domain Admin شود

هشدار بحرانی صادر شود.

Use Case شماره ۳

VPN Suspicious Loginn اگر: ورود از کشور یا IP غیرمعمول رخ دهد

هشدار صادر شود.

Use Case شماره ۴

Ransomware Activity

اگر :تعداد زیادی فایل در زمان کوتاه تغییر کند

هشدار صادر شود.

Use Case شماره ۵

Disabled Antivirus در صورت غیرفعال شدن آنتی‌ویروس **هشدار صادر شود.**

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹-۱۰ همبستگی رخدادها(Correlation)

قلب SIEM همین قسمت است.

مثال:

کاربر وارد VPN می‌شود

↓

وارد Domain می‌شود

↓

به SQL متصل می‌شود

↓

داده استخراج می‌کند

↓

فایل‌ها را حذف می‌کند

به صورت جداگانه طبیعی هستند.

اما کنار هم نشانه حمله هستند.

۹-۱۱ مانیتورینگ FortiGate

موارد پایش:

- VPN
- IPS
- Antivirus
- Web Filter
- Application Control
- Admin Login

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹-۱۲ مانیتورینگVMware

موارد پایش:

- خاموش شدن VM
- Snapshot Creation
- حذف VM
- تغییرات Host
- ورود مدیران

۹-۱۳ مانیتورینگ Active Directory

موارد پایش:

- Login
- Failed Login
- User Creation
- Group Modification
- Domain Admin Changes

۹-۱۴مانیتورینگ پایگاه داده

پایش:

- Login
- Failed Login
- Permission Change
- Data Export
- Sensitive Query

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹-۱۵ File Integrity Monitoring

یکی از قابلیت‌های مهم Wazuh

پایش:

- فایل‌های سیستمی
- فایل‌های تنظیمات
- فایل‌های امنیتی

در صورت تغییر : هشدار صادر می‌شود.

۹-۱۶ Vulnerability Detection

Wazuh به صورت مستمر:

- CVE
- Patch Status
- Software Inventory

را بررسی می‌کند.

۹-۱۷ گزارش‌های مدیریتی

گزارش‌های روزانه -گزارش‌های هفتگی-گزارش‌های ماهانه-گزارش‌های مدیریتی-گزارش‌های ممیزی

۹-۱۸ داشبوردهای مدیریتی نمایش:

- حملات
- وضعیت سرورها
- آسیب‌پذیری‌ها
- کاربران
- VPN
- فایروال

۹-۱۹ نقشSOC

SOC یا مرکز عملیات امنیت مسئول:

- پایش ۲۴ ساعته
- بررسی هشدارها
- تحلیل رخدادها
- پاسخ به حملات

در این پروژه، زیرساخت لازم برای ایجاد SOC سازمانی فراهم می‌شود.

۹-۲۰ شاخص‌های عملکرد

MTTD

زمان تشخیص رخداد

هدف:

کمتر از ۱۵ دقیقه

MTTR

زمان پاسخ

هدف:

کمتر از ۳۰ دقیقه

پوشش لاگ

هدف:

۱۰۰درصد

پوشش دارایی‌ها

هدف:

۱۰۰درصد

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹-۲۱ خروجی‌های پروژه

پس از اجرای پروژه، سازمان دارای موارد زیر خواهد بود:

- سامانه SIEM
- سامانه مدیریت لاگ
- داشبورد مدیریتی
- Use Case های امنیتی
- هشدارهای امنیتی
- گزارش‌های مدیریتی
- فرآیند مانیتورینگ
- مستندات فنی

۹-۲۲ معماری پیشنهادی برای صمت

با توجه به اطلاعات فعلی:

- حدود ۲۰ ماشین مجازی
- ۶سرور فیزیکی
- FortiGate ۱۰۰F
- VMware
- Active Directory
- SQL Server

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

معماری پیشنهادی:

- ۱عدد Wazuh Manager
- ۱عدد Wazuh Indexer
- ۱عدد Wazuh Dashboard
- Agentروی تمامیVM ها
- اتصال FortiGate به Wazuh و FortiAnalyzer
- نگهداری لاگ حداقل ۶ تا ۱۲ ماه
- داشبورد مدیریتی برای مدیران و واحد فناوری اطلاعات

منابع

- Wazuh
- FortiAnalyzer
- Splunk Enterprise Security
- Elastic Stack
- NIST SP ۸۰۰-۹۲
- ISO/IEC ۲۷۰۰۱:۲۰۲۲

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل دهم: آموزش، ممیزی، پایش و بهبود مستمر

۱۰-۱ مقدمه

امنیت اطلاعات یک محصول یا نرم‌افزار نیست که یک بار خریداری و برای همیشه حل شود. امنیت یک فرآیند مستمر است که نیازمند آموزش، پایش، ارزیابی و بهبود دائمی می‌باشد.

حتی پیشرفته‌ترین تجهیزات امنیتی نیز در صورت عدم آگاهی کاربران، عدم نظارت و نبود فرآیندهای کنترلی، نمی‌توانند از اطلاعات سازمان حفاظت نمایند.

هدف این فصل ایجاد سازوکارهای لازم برای حفظ اثربخشی سیستم مدیریت امنیت اطلاعات در طول زمان است.

۱۰-۲ اهداف

اهداف اصلی این بخش عبارتند از:

- ارتقای فرهنگ امنیت اطلاعات
- افزایش آگاهی کارکنان
- سنجش اثربخشی کنترل‌های امنیتی
- شناسایی نقاط ضعف
- بهبود مستمر فرآیندها
- انطباق با استانداردهای امنیتی
- حفظ آمادگی سازمان در برابر تهدیدات جدید

۱۰-۳ آموزش و آگاهی امنیتی

کاربران یکی از مهم‌ترین دارایی‌های سازمان و در عین حال یکی از مهم‌ترین منابع ایجاد ریسک هستند.

بخش قابل توجهی از رخدادهای امنیتی ناشی از:

- خطای انسانی
- عدم آگاهی

- مهندسی اجتماعی
- فیشینگ
- استفاده نادرست از تجهیزات

می‌باشد.

۴-۱۰ برنامه آموزش امنیت اطلاعات

برنامه آموزشی سازمان شامل موارد زیر خواهد بود:

آشنایی با امنیت اطلاعات

مفاهیم پایه امنیت

امنیت رمز عبور

- انتخاب رمز مناسب
- مدیریت رمزها
- MFA

فیشینگ و مهندسی اجتماعی

- تشخیص ایمیل‌های جعلی
- لینک‌های مخرب
- حملات تلفنی

امنیت تجهیزات سازمانی

- لپ‌تاپ
- موبایل
- حافظه‌های جانبی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

امنیت اینترنت

- دانلود ایمن
- وب‌سایت‌های مشکوک
- نرم‌افزارهای غیرمجاز

گزارش‌دهی رخدادها

نحوه اعلام مشکلات امنیتی

۱۰-۵ گروه‌های آموزشی

آموزش‌ها متناسب با نقش افراد ارائه می‌شود.

مدیران ارشد

تمرکز بر:

- ریسک
- حاکمیت
- تصمیم‌گیری

کارشناسان IT

تمرکز بر:

- زیرساخت
- امنیت فنی
- رخدادها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

کاربران عادی

تمرکز بر:

- فیشینگ
- رمز عبور
- استفاده ایمن

۱۰-٦ ارزیابی اثربخشی آموزش

برای اطمینان از اثربخشی آموزش:

- آزمون
- مصاحبه
- مانور
- شبیه‌سازی حملات

انجام می‌شود.

۱۰-۷ ممیزی داخلی

ممیزی داخلی فرآیندی است برای بررسی انطباق وضعیت موجود با الزامات تعیین شده.

هدف ممیزی:

- شناسایی عدم انطباق‌ها
- ارزیابی کنترل‌ها
- بهبود فرآیندها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸-۱۰ دامنه ممیزی

ممیزی شامل:

- زیرساخت فناوری اطلاعات
- امنیت شبکه
- مدیریت دسترسی
- مدیریت رخداد
- پشتیبان‌گیری
- SIEM
- Wazuh
- FortiGate
- VMware

خواهد بود.

۹-۱۰ فرآیند ممیزی

برنامه‌ریزی - جمع‌آوری شواهد- مصاحبه- بررسی مستندات- تهیه گزارش- اقدامات اصلاحی

۱۰-۱۰ مدیریت عدم انطباق

در صورت مشاهده هرگونه ضعف یا عدم انطباق:

- ثبت می‌شود .
- تحلیل می‌شود .
- مسئول تعیین می‌شود .
- زمان اصلاح مشخص می‌شود .
- مجدداً بررسی می‌شود .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۰-۱۱ شاخص‌های عملکرد امنیتی

برای ارزیابی وضعیت امنیت سازمان شاخص‌هایی تعریف می‌شود.

شاخص مدیریت رخداد

تعداد رخدادهای امنیتی

شاخص زمان پاسخ

میانگین زمان پاسخگویی

شاخص آسیب‌پذیری

تعداد آسیب‌پذیری‌های بحرانی

شاخص وصله‌های امنیتی

درصد سیستم‌های بروزرسانی شده

شاخص آموزش

درصد کارکنان آموزش دیده

۱۰-۱۲ پایش مستمر

وضعیت امنیتی سازمان به صورت مداوم از طریق:

- Wazuh
- FortiAnalyzer
- SIEM
- گزارش‌های مدیریتی

پایش می‌شود.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۰-۱۳ بازنگری مدیریت

مدیریت ارشد باید حداقل سالی یک بار وضعیت ISMS را بررسی نماید.

موارد بررسی:

- نتایج ممیزی
- ریسک‌ها
- رخدادها
- وضعیت کنترل‌ها
- وضعیت پروژه‌های امنیتی

۱۰-۱٤ بهبود مستمر

این پروژه بر اساس چرخه بهبود مستمر طراحی شده است.

مراحل شامل:

۱. برنامه‌ریزی
۲. اجرا
۳. ارزیابی
٤. اصلاح

این چرخه به صورت زیر تعریف می‌شود:

Plan
↓
Do
↓
Check
↓
Act
↓
Plan

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۰-۱۵ برنامه نگهداری و پشتیبانی

پس از استقرار سامانه‌ها فعالیت‌های زیر انجام خواهد شد:

پایش روزانه

بررسی هشدارها

پایش هفتگی

تحلیل وضعیت امنیت

پایش ماهانه

گزارش مدیریتی

پایش فصلی

ممیزی کنترل‌ها

پایش سالانه

بازنگریISMS

۱۰-۱۶ خدمات پشتیبانی پیشنهادی

پشتیبانی می‌تواند شامل:

- پشتیبانی Wazuh
- پشتیبانی FortiAnalyzer
- پشتیبانی SIEM
- پشتیبانی VMware
- پشتیبانی FortiGate
- مشاوره امنیت
- بازبینی دوره‌ای

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۰-۱۷ دستاوردهای نهایی پروژه

با اجرای کامل پروژه، سازمان به قابلیت‌های زیر دست خواهد یافت:

حوزه مدیریتی

- چارچوب ISMS
- مدیریت ریسک
- سیاست‌های امنیتی

حوزه فنی

- SIEM
- Wazuh
- FortiAnalyzer
- مدیریت لاگ

حوزه عملیاتی

- مدیریت رخداد
- مدیریت آسیب‌پذیری
- Patch Management

حوزه تاب‌آوری

- Backup
- HA
- BCP
- DRP

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

حوزه نظارتی

- ممیزی
- گزارش‌گیری
- پایش مستمر

۱۰-۱۸ جمع‌بندی نهایی پروژه

این پروژه با هدف استقرار یک نظام جامع مدیریت امنیت اطلاعات طراحی شده است تا ضمن انطباق با الزامات استانداردهای امنیتی، سطح بلوغ امنیتی سازمان را ارتقا داده و امکان مدیریت مؤثر تهدیدات، رخدادها و ریسک‌های امنیتی را فراهم نماید.

خروجی نهایی پروژه صرفاً نصب چند نرم‌افزار یا تهیه چند مستند نخواهد بود، بلکه ایجاد یک زیرساخت مدیریتی، فنی و عملیاتی پایدار برای حفاظت از دارایی‌های اطلاعاتی سازمان خواهد بود.

منابع

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- ISO/IEC ۲۷۰۰٤
- ISO ۱۹۰۱۱
- NIST Cybersecurity Framework

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

فصل یازدهم: نقشه راه اجرا و زمان‌بندی پروژه

۱۱-۱ فاز اول: شناخت وضع موجود

مدت زمان: ۲ تا ۳ هفته

فعالیت‌ها:

- جلسات اولیه
- جمع‌آوری اطلاعات
- بررسی زیرساخت
- بررسی VMware
- بررسی FortiGate
- بررسی Active Directory
- بررسی سیاست‌های موجود

خروجی:

- گزارش وضعیت موجود
- Gap Analysis

۱۱-۲ فاز دوم: تحلیل ریسک

مدت زمان: ۸ هفته

فعالیت‌ها:

- شناسایی دارایی‌ها
- شناسایی تهدیدات
- شناسایی آسیب‌پذیری‌ها
- تحلیل ریسک

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

خروجی:

- Asset Register
- Risk Register

۳-۱۱ فاز سوم: طراحی ISMS

مدت زمان: ۸ هفته

فعالیت‌ها:

- تدوین سیاست‌ها
- تدوین فرآیندها
- تدوین رویه‌ها

خروجی:

- مستندات ISMS

۴-۱۱فاز چهارم: پیاده‌سازی SIEM

مدت زمان: ۴ هفته

فعالیت‌ها:

- نصب Wazuh
- نصب Dashboard
- اتصال لاگ‌ها
- تعریف Use Case ها

خروجی:

- سامانه SIEM عملیاتی

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵-۱۱فاز پنجم: استقرارFortiAnalyzer

مدت زمان: ۱ هفته

فعالیت‌ها:

- نصب
- اتصال FortiGate
- گزارش‌گیری

خروجی:

- سامانه تحلیل لاگ

۱۱-۶ فاز ششم: مدیریت آسیب‌پذیری

مدت زمان: ۲ هفته

فعالیت‌ها:

- اسکن
- تحلیل
- اصلاح

خروجی:

- گزارش آسیب‌پذیری

۱۱-۷ فاز هفتم: آموزش

مدت زمان: ۱ هفته

فعالیت‌ها:

- آموزش مدیران
- آموزش کارشناسان

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- آموزش کاربران

۸-۱۱ فاز هشتم: آزمون و تحویل

مدت زمان: ۱ هفته

فعالیت‌ها:

- تست نهایی
- تحویل مستندات
- ارائه گزارش

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوستA

سیاست امنیت اطلاعات(Information Security Policy)

شماره سند

ISP-۰۰۱

نسخه ۱,۰

تاریخ اجرا

پس از تصویب مدیریت ارشد

۱- مقدمه

اطلاعات یکی از مهم‌ترین دارایی‌های سازمان محسوب می‌شود و حفاظت از آن برای تداوم فعالیت‌های سازمانی، حفظ اعتماد ذی‌نفعان، رعایت الزامات قانونی و جلوگیری از خسارات مالی و اعتباری ضروری است.

این سند با هدف ایجاد چارچوبی جامع برای حفاظت از دارایی‌های اطلاعاتی و ارتقاء سطح امنیت اطلاعات در سازمان تدوین شده است.

۲ - هدف

اهداف اصلی این سیاست عبارتند از:

- حفاظت از اطلاعات سازمان
- حفظ محرمانگی اطلاعات
- حفظ صحت اطلاعات
- حفظ دسترس‌پذیری اطلاعات
- کاهش ریسک‌های امنیتی
- افزایش سطح آگاهی امنیتی
- ایجاد چارچوب حاکمیت امنیت اطلاعات
- رعایت الزامات قانونی و مقرراتی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳ -دامنه کاربرد

این سیاست شامل تمامی موارد زیر می‌گردد:

- کارکنان
- مدیران
- پیمانکاران
- مشاوران
- تجهیزات فناوری اطلاعات
- سامانه‌های نرم‌افزاری
- اطلاعات فیزیکی و الکترونیکی
- مراکز داده
- تجهیزات شبکه
- زیرساخت‌های مجازی سازی

۴- اصول بنیادین امنیت اطلاعات

سیاست امنیت اطلاعات سازمان بر سه اصل اساسی استوار است:

۴-۱ محرمانگی(Confidentiality)

اطلاعات فقط در اختیار افراد مجاز قرار خواهد گرفت.

نمونه اقدامات:

- کنترل دسترسی
- رمزنگاری
- مدیریت کاربران
- طبقه‌بندی اطلاعات

٤-۲ صحت اطلاعات(Integrity)

اطلاعات باید صحیح، کامل و بدون تغییر غیرمجاز باقی بماند.

نمونه اقدامات:

- ثبت وقایع
- کنترل تغییرات
- مدیریت نسخه‌ها
- نظارت بر تغییرات

٤-۳ دسترس‌پذیری(Availability)

اطلاعات و سامانه‌ها باید در زمان مورد نیاز در دسترس کاربران مجاز باشند.

نمونه اقدامات:

- Backup
- High Availability
- Disaster Recovery
- مانیتورینگ

۵- مسئولیت‌ها

مدیریت ارشد

مسئول:

- تصویب سیاست‌ها
- تأمین منابع
- حمایت از برنامه امنیت اطلاعات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

واحد فناوری اطلاعات

مسئول:

- اجرای کنترل‌های امنیتی
- نگهداری تجهیزات
- پایش زیرساخت

مسئول امنیت اطلاعات

مسئول:

- مدیریت ریسک
- نظارت بر اجرای ISMS
- بررسی رخدادهای امنیتی

کاربران

مسئول:

- رعایت سیاست‌ها
- حفاظت از اطلاعات
- گزارش رخدادهای مشکوک

۶- مدیریت دارایی‌های اطلاعاتی

تمام دارایی‌های اطلاعاتی باید:

- شناسایی شوند .
- ثبت شوند .
- طبقه‌بندی شوند .
- مالک مشخص داشته باشند .

دارایی‌ها شامل:

- سرورها
- تجهیزات شبکه
- نرم‌افزارها
- اطلاعات
- مستندات
- پایگاه‌های داده

می‌باشند.

۷- طبقه‌بندی اطلاعات

اطلاعات سازمان در چهار سطح طبقه‌بندی می‌شوند:

عمومی

قابل انتشار برای عموم

داخلی

فقط برای استفاده سازمانی

محرمانه

مخصوص واحدهای مشخص

خیلی محرمانه

محدود به افراد دارای مجوز ویژه

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸- کنترل دسترسی

دسترسی به اطلاعات بر اساس:

- نیاز شغلی
- اصل حداقل دسترسی
- تأیید مدیر مربوطه

اعطا خواهد شد.

الزامات

- حساب اشتراکی ممنوع است .
- دسترسی‌ها ثبت می‌شوند .
- بازبینی دوره‌ای انجام می‌شود .
- MFAبرای سامانه‌های حساس الزامی است .

۹- مدیریت رمز عبور

کاربران موظف هستند:

- از رمز عبور قوی استفاده نمایند .
- رمز خود را در اختیار دیگران قرار ندهند .
- رمز را در مکان‌های ناامن ذخیره نکنند .

حداقل طول رمز:

۱۲کاراکتر

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۰ - استفاده از تجهیزات سازمانی

تمام تجهیزات سازمانی صرفاً برای امور کاری استفاده خواهند شد.

موارد زیر ممنوع است:

- نصب نرم‌افزار غیرمجاز
- اتصال تجهیزات ناشناس
- استفاده شخصی نامتعارف
- دور زدن کنترل‌های امنیتی

۱۱ -استفاده از اینترنت و ایمیل

کاربران موظفند:

- از وب‌سایت‌های معتبر استفاده کنند .
- فایل‌های مشکوک را باز نکنند .
- لینک‌های ناشناس را بررسی نمایند .

موارد زیر ممنوع است:

- دانلود نرم‌افزارهای غیرمجاز
- انتشار اطلاعات سازمان
- ارسال فایل‌های محرمانه بدون مجوز

۱۲ -مدیریت رخدادهای امنیتی

تمام کارکنان موظفند هرگونه:

- نفوذ احتمالی
- بدافزار
- فیشینگ

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- نشت اطلاعات
- رفتار غیرعادی

را فوراً گزارش نمایند.

۱۳-پشتیبان‌گیری از اطلاعات

اطلاعات حیاتی سازمان باید:

- به صورت منظم پشتیبان‌گیری شوند .
- در محل امن نگهداری شوند .
- به صورت دوره‌ای بازیابی آزمایشی شوند .

١٤ -مدیریت تغییرات

هرگونه تغییر در:

- سرورها
- تجهیزات شبکه
- فایروال
- سامانه‌های نرم‌افزاری

باید ثبت و تأیید گردد.

۱۵ – آموزش و آگاهی امنیتی

تمام کارکنان باید به صورت دوره‌ای در برنامه‌های آموزشی امنیت اطلاعات شرکت نمایند.

۱۶- انطباق و ممیزی

رعایت این سیاست برای تمامی کاربران الزامی است.

سازمان مجاز است:

- ممیزی انجام دهد .
- دسترسی‌ها را بررسی کند .
- گزارش‌های امنیتی را ارزیابی نماید .

۱۷ -تخلفات

نقض این سیاست می‌تواند منجر به:

- محدودسازی دسترسی
- اقدامات انضباطی
- پیگیری قانونی

گردد.

۱۸ -بازنگری سیاست

این سند حداقل سالی یک بار یا در صورت وقوع تغییرات اساسی مورد بازنگری قرار خواهد گرفت.

۱۹-تأییدیه

این سیاست پس از تأیید مدیریت ارشد سازمان لازم‌الاجرا خواهد بود.

مراجع

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- NIST Cybersecurity Framework
- ISO ۲۲۳۰۱

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوستB

سیاست کنترل دسترسی(Access Control Policy)

شماره سند

ACP-۰۰۱

نسخه ۱.۰

تاریخ اجرا

پس از تصویب مدیریت ارشد

۱- مقدمه

کنترل دسترسی یکی از مهم‌ترین کنترل‌های امنیت اطلاعات است که هدف آن اطمینان از دسترسی افراد مجاز به منابع مورد نیاز و جلوگیری از دسترسی غیرمجاز به اطلاعات، سامانه‌ها و تجهیزات سازمان می‌باشد.

این سیاست چارچوب مدیریت هویت، احراز هویت، اعطای دسترسی، بازبینی دسترسی‌ها و حذف دسترسی‌های غیرضروری را مشخص می‌کند.

۲- هدف

اهداف این سیاست عبارتند از:

- حفاظت از اطلاعات سازمان
- جلوگیری از دسترسی غیرمجاز
- پیاده‌سازی اصل حداقل دسترسی
- کاهش ریسک نشت اطلاعات
- مدیریت چرخه عمر دسترسی کاربران
- افزایش قابلیت ردیابی فعالیت‌ها
- انطباق با الزامات امنیتی و ممیزی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳- دامنه کاربرد

این سیاست شامل تمامی موارد زیر می‌گردد:

- کاربران عادی
- کارشناسان فناوری اطلاعات
- مدیران
- پیمانکاران
- مشاوران
- سامانه‌های نرم‌افزاری
- Active Directory
- VMware
- FortiGate
- پایگاه‌های داده
- سرورها
- تجهیزات شبکه

٤- اصول کنترل دسترسی

اصل حداقل دسترسی(Least Privilege)

هر کاربر صرفاً باید به منابع مورد نیاز برای انجام وظایف شغلی خود دسترسی داشته باشد.

اصل نیاز به دانستن(Need To Know)

کاربر تنها به اطلاعاتی دسترسی خواهد داشت که برای انجام وظایف وی ضروری است.

اصل تفکیک وظایف(Segregation of Duties)

هیچ فردی نباید به تنهایی امکان انجام تمام مراحل یک فرآیند حساس را داشته باشد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

اصل مسئولیت‌پذیری

تمام فعالیت‌ها باید قابل انتساب به یک فرد مشخص باشند.

۵- مدیریت هویت کاربران

تمام کاربران باید دارای شناسه کاربری یکتا باشند.

موارد زیر ممنوع است:

- استفاده از حساب‌های اشتراکی
- استفاده از حساب افراد دیگر
- ایجاد حساب بدون مجوز

۶- چرخه عمر حساب کاربری

ایجاد حساب

ایجاد حساب صرفاً با درخواست رسمی و تأیید مدیر واحد انجام می‌شود.

تغییر دسترسی

در صورت تغییر سمت یا مسئولیت:

سطح دسترسی بازبینی می‌شود.

غیرفعال‌سازی

در زمان:

- پایان همکاری
- انتقال واحد
- تعلیق دسترسی

حساب باید غیرفعال گردد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

حذف حساب

حساب‌های بلااستفاده پس از دوره مشخص حذف می‌شوند.

۷- سطوح دسترسی

سطح یک: کاربران عادی

دسترسی به:

- سامانه‌های کاری
- ایمیل
- فایل‌های واحد مربوطه

سطح دو: کارشناسان

علاوه بر سطح یک:

- مدیریت سامانه‌های تخصصی
- دسترسی محدود مدیریتی

سطح سه: مدیران سیستم

دسترسی مدیریتی به:

- سرورها
- Active Directory
- تجهیزات شبکه

سطح چهار: مدیران ارشد

دسترسی به:

- گزارش‌ها
- داشبوردهای مدیریتی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- اطلاعات مدیریتی

۸- سیاست رمز عبور

حداقل طول رمز عبور:

۱۲کاراکتر

الزامات:

- حروف بزرگ
- حروف کوچک
- اعداد
- نمادها

ممنوع:

- رمزهای ساده
- تاریخ تولد
- شماره تلفن
- نام سازمان

۹- احراز هویت چندعاملی(MFA)

برای سامانه‌های حساس استفاده از MFA الزامی است.

از جمله:

- VPN
- FortiGate
- VMware
- ایمیل سازمانی
- سامانه‌های مدیریتی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۰- مدیریت دسترسی‌های ممتاز(Privileged Access)

حساب‌های دارای دسترسی مدیریتی باید:

- محدود باشند .
- مستند شوند .
- دوره‌ای بازبینی شوند .

نمونه:

- Domain Admin
- Enterprise Admin
- VMware Administrator
- FortiGate Administrator
- SQL Administrator

۱۱- مدیریت دسترسی Active Directory

تمام کاربران باید از طریق Active Directory مدیریت شوند.

الزامات:

- استفاده از Group Policy
- مدیریت گروه‌ها
- ثبت رویدادها
- بازبینی دوره‌ای

۱۲- مدیریت دسترسی VMware

دسترسی به VMware باید مبتنی بر نقش باشد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

نمونه نقش‌ها:

Read Only

فقط مشاهده

Operator

عملیات محدود

Administrator

مدیریت کامل

تمام ورودها باید ثبت شوند.

۱۳- مدیریت دسترسی FortiGate

دسترسی مدیریتی به فایروال باید:

- محدود باشد .
- ثبت شود .
- از MFA استفاده کند .

دسترسی مستقیم از اینترنت ممنوع است مگر با مجوز رسمی.

۱٤- مدیریت دسترسی پایگاه داده

تمام دسترسی‌های پایگاه داده باید:

- مبتنی بر نقش
- مستند
- قابل ردیابی

باشند.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۵- مدیریت دسترسی VPN

کاربران دورکار فقط از طریق VPN مجاز خواهند بود.

الزامات:

- MFA
- ثبت لاگ
- محدودیت زمانی
- محدودیت IP در صورت امکان

۱۶- مدیریت دسترسی پیمانکاران

پیمانکاران باید:

- حساب جداگانه داشته باشند .
- مدت دسترسی مشخص داشته باشند .
- پس از پایان همکاری حذف شوند .

۱۷- بازبینی دسترسی‌ها

تمام دسترسی‌ها باید به صورت دوره‌ای بازبینی شوند.

حداقل:

هر شش ماه یکبار

موارد بررسی:

- کاربران فعال
- دسترسی‌های مدیریتی
- حساب‌های بلااستفاده
- دسترسی پیمانکاران

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۸- ثبت و پایش فعالیت‌ها

تمام فعالیت‌های حساس باید ثبت شوند.

نمونه:

- Login
- Failed Login
- ایجاد کاربر
- حذف کاربر
- تغییر گروه
- تغییر رمز
- تغییر سیاست‌ها

۱۹- مانیتورینگ امنیتی

ثبت وقایع باید در سامانه SIEM تجمیع شود.

نمونه سامانه‌ها:

- Wazuh
- FortiAnalyzer
- SIEM مرکزی

۲۰- مدیریت حساب‌های اضطراری

حساب‌های اضطراری باید:

- محدود باشند .
- رمز نگهداری امن داشته باشند .
- استفاده از آن‌ها ثبت شود .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۱- مدیریت حساب‌های سرویس

Service Accountها باید:

- مستندسازی شوند .
- مالک مشخص داشته باشند .
- بازبینی شوند .
- حداقل دسترسی را داشته باشند .

۲۲- الزامات ممیزی

سازمان باید امکان ارائه شواهد زیر را داشته باشد:

- لیست کاربران
- سطح دسترسی‌ها
- لاگ ورود و خروج
- تغییرات دسترسی
- گزارش بازبینی دسترسی‌ها

۲۳- شاخص‌های عملکرد

KPI -۰۱

تعداد حساب‌های بلااستفاده

هدف: صفر

KPI-۰۲

تعداد حساب‌های مشترک

هدف: صفر

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

KPI-۰۳

درصد استفاده ازMFA

هدف: ۱۰۰%

KPI-۰٤

بازبینی دسترسی‌ها

هدف: ۱۰۰%

۲٤- تخلفات

موارد زیر تخلف محسوب می‌شوند:

- اشتراک‌گذاری رمز عبور
- استفاده از حساب دیگران
- ایجاد حساب غیرمجاز
- دور زدن کنترل‌های امنیتی

۲۵- بازنگری

این سیاست حداقل سالی یک بار یا پس از تغییرات اساسی بازبینی خواهد شد.

۲٦- تأییدیه

این سند پس از تأیید مدیریت ارشد لازم‌الاجرا خواهد بود.

مراجع

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- NIST SP ۸۰۰-۵۳
- NIST SP ۸۰۰-٦۳

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوستC

سیاست رمز عبور و احراز هویت(Password & Authentication Policy)

شماره سند

PAP-۰۰۱

نسخه : ۱.۰

تاریخ اجرا

پس از تصویب مدیریت ارشد

۱- مقدمه

احراز هویت اولین خط دفاعی سازمان در برابر دسترسی‌های غیرمجاز محسوب می‌شود. بخش عمده‌ای از رخدادهای امنیتی در دنیا ناشی از استفاده از رمزهای عبور ضعیف، افشای اطلاعات هویتی کاربران و ضعف در فرآیندهای احراز هویت می‌باشد.

این سیاست با هدف افزایش امنیت حساب‌های کاربری، کاهش احتمال نفوذ و حفاظت از اطلاعات سازمان تدوین شده است.

۲- هدف

اهداف این سیاست عبارتند از:

- افزایش امنیت حساب‌های کاربری
- کاهش احتمال نفوذ
- جلوگیری از سرقت هویت
- کاهش حملات Brute Force
- حفاظت از اطلاعات سازمان
- الزام استفاده از روش‌های احراز هویت امن

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳- دامنه کاربرد

این سیاست شامل موارد زیر می‌شود:

- Active Directory
- Windows Server
- Linux Server
- VMware
- FortiGate
- VPN
- ایمیل سازمانی
- پایگاه‌های داده
- سامانه‌های تحت وب
- کاربران داخلی
- پیمانکاران
- مدیران سیستم

٤- اصول کلی

تمام کاربران موظف هستند:

- رمز عبور خود را محرمانه نگه دارند .
- از رمزهای پیچیده استفاده کنند .
- رمز عبور خود را در اختیار دیگران قرار ندهند .
- از ذخیره رمز روی کاغذ یا فایل‌های ناامن خودداری کنند .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵- استاندارد رمز عبور

حداقل طول رمز عبور:

کاربران عادی

۱۲کاراکتر

کاربران مدیریتی

۱۵کاراکتر

حساب‌های حساس

۱۸کاراکتر

٦- پیچیدگی رمز عبور

رمز عبور باید شامل حداقل:

- یک حرف بزرگ
- یک حرف کوچک
- یک عدد
- یک نماد

باشد.

نمونه قابل قبول

M۰hsen@۲۰۲٦#Net

نمونه غیرقابل قبول

۱۲۳۴۵۶
password
admin۱۲۳
qwerty

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۷- ممنوعیت استفاده از اطلاعات شخصی

استفاده از موارد زیر در رمز عبور ممنوع است:

- نام فرد
- نام سازمان
- شماره تلفن
- تاریخ تولد
- کد ملی
- نام کاربری

۸- تاریخ انقضای رمز عبور

کاربران عادی

۹۰روز

کاربران مدیریتی

۶۰روز

حساب‌های حساس

۴۵روز

۹- تاریخچه رمز عبور

کاربران نباید از ۱۰ رمز قبلی خود مجدداً استفاده نمایند.

۱۰- قفل شدن حساب کاربری

برای جلوگیری از:Brute Force

اگر:

۵بار ورود ناموفق

ثبت شود

حساب کاربری به مدت ۱۵ دقیقه قفل خواهد شد.

۱۱- مدیریت رمز اولیه

در زمان ایجاد حساب:

- رمز اولیه تصادفی ایجاد می‌شود .
- کاربر در اولین ورود ملزم به تغییر رمز است .

۱۲- بازنشانی رمز عبور

Reset Passwordصرفاً از طریق:

- واحد فناوری اطلاعات
- سامانه مدیریت هویت

انجام خواهد شد.

۱۳- حساب‌های مدیریتی

تمام مدیران سیستم باید دارای دو حساب باشند.

حساب عادی

برای فعالیت‌های روزمره

حساب مدیریتی

برای امور مدیریتی

استفاده روزمره از Domain Admin ممنوع است.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۴- حساب‌های سرویس(Service Accounts)

الزامات:

- مالک مشخص
- مستندسازی
- بازبینی دوره‌ای
- حداقل دسترسی

۱۵- احراز هویت چند عاملی(MFA)

استفاده از MFA برای سامانه‌های حیاتی الزامی است.

VPN

الزامی

FortiGate

الزامی

VMware

الزامی

ایمیل سازمانی

الزامی

پنل‌های مدیریتی

الزامی

۱۶- روش‌های مجازMFA

روش‌های مورد تأیید:

- OTP
- Authenticator Application

- Push Notification
- Hardware Token

۱۷- مدیریت نشست‌ها(Session Management)

جهت جلوگیری از سوءاستفاده:

کاربران عادی

۳۰دقیقه عدم فعالیت

قطع نشست

مدیران سیستم

۱۵دقیقه عدم فعالیت

قطع نشست

۱۸- دسترسی از راه دور

تمام دسترسی‌های راه دور باید از طریق:

- VPN
- MFA
- رمزنگاری

انجام شوند.

دسترسی مستقیم RDP از اینترنت ممنوع است.

۱۹- مانیتورینگ ورود کاربران

رویدادهای زیر ثبت و پایش خواهند شد:

- Login Success
- Login Failure
- Password Change

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- Password Reset
- Account Lockout
- MFA Failure

۲۰- تحلیل رفتار کاربران

سامانه SIEM باید موارد زیر را تشخیص دهد:

- ورود در ساعات غیرعادی
- ورود از موقعیت جغرافیایی غیرمعمول
- تلاش‌های مکرر ناموفق
- تغییرات غیرعادی دسترسی

۲۱- الزامات Active Directory

حداقل سیاست‌های پیشنهادی:

Minimum Password Length

۱۲

Password History

۱۰

Maximum Password Age

۹۰روز

Lockout Threshold

۵ Attempt

Lockout Duration

۱۵ Minute

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۲- الزامات VPN

تمام کاربران VPN باید:

- حساب شخصی داشته باشند .
- MFAفعال داشته باشند .
- لاگ فعالیت آن‌ها ثبت شود .

۲۳- الزامات VMware

حساب Root و Administrator باید:

- محدود شوند .
- MFAداشته باشند .
- لاگ کامل آن‌ها ثبت شود .

۲۴- الزامات FortiGate

حساب‌های مدیریتی:

- MFA
- Trusted Host
- ثبت لاگ

الزامی است.

۲۵- آموزش کاربران

تمام کاربران باید آموزش ببینند:

- انتخاب رمز قوی
- تشخیص فیشینگ
- حفاظت از اطلاعات ورود
- استفاده از MFA

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۶- شاخص‌های عملکرد

KPI -۰۱

کاربران دارایMFA

هدف:

۱۰۰٪

KPI-۰۲

حساب‌های اشتراکی

هدف:

۰

KPI-۰۳

ورودهای ناموفق

پایش ماهانه

KPI-۰٤

حساب‌های قفل شده

تحلیل ماهانه

۲۷- تخلفات

موارد زیر تخلف محسوب می‌شوند:

- اشتراک‌گذاری رمز عبور
- ذخیره رمز در مکان ناامن
- غیرفعال کردن MFA
- استفاده از حساب دیگران

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۸- بازنگری

این سیاست حداقل سالی یک بار بازبینی خواهد شد.

۲۹- تأییدیه

این سند پس از تصویب مدیریت ارشد لازم‌الاجرا می‌باشد.

مراجع

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- NIST SP ۸۰۰-۶۳B
- CIS Controls v۸

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوستD

سیاست پشتیبان‌گیری و بازیابی اطلاعات(Backup & Recovery Policy)

شماره سند

BRP -۰۰۱

نسخه : ۱.۰

تاریخ اجرا

پس از تصویب مدیریت ارشد

۱- مقدمه

اطلاعات یکی از ارزشمندترین دارایی‌های سازمان محسوب می‌شود و از دست رفتن آن می‌تواند منجر به توقف فعالیت‌های سازمان، خسارات مالی، از بین رفتن سوابق، اختلال در ارائه خدمات و آسیب به اعتبار سازمان گردد.

به همین دلیل لازم است فرآیندهای پشتیبان‌گیری و بازیابی اطلاعات به صورت ساختاریافته، مستمر و قابل آزمون طراحی و اجرا شوند.

این سند الزامات مربوط به پشتیبان‌گیری، نگهداری، حفاظت و بازیابی اطلاعات را تشریح می‌نماید.

۲- هدف

اهداف این سیاست عبارتند از:

- حفاظت از اطلاعات حیاتی
- کاهش ریسک از دست رفتن داده‌ها
- آمادگی در برابر خرابی تجهیزات
- مقابله با حملات باج‌افزاری
- تضمین تداوم خدمات
- تسریع فرآیند بازیابی اطلاعات
- رعایت الزامات پدافند غیرعامل و امنیت اطلاعات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳- دامنه کاربرد

این سیاست شامل کلیه دارایی‌های اطلاعاتی سازمان می‌باشد:

- VMware Infrastructure
- Virtual Machines
- Windows Servers
- Linux Servers
- SQL Server
- Active Directory
- File Servers
- Application Servers
- FortiGate Configuration
- تجهیزات شبکه
- مستندات الکترونیکی

٤- اصول حاکم بر پشتیبان‌گیری

فرآیند Backup باید:

- منظم باشد .
- مستند باشد .
- قابل بازیابی باشد .
- دوره‌ای آزمون شود .
- مستقل از سیستم اصلی نگهداری شود .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵- اهداف بازیابی

Recovery Time Objective (RTO)

حداکثر زمان قابل قبول برای بازیابی سرویس

اهداف پیشنهادی:

سرویس	RTO
Active Directory	۴ساعت
VMware	۴ساعت
SQL Server	۴ساعت
File Server	۸ساعت
سامانه‌های کاربردی	۸ساعت

Recovery Point Objective (RPO)

حداکثر میزان داده قابل از دست رفتن

اهداف پیشنهادی:

سرویس	RPO
SQL Server	۱ساعت
Active Directory	۴ساعت
File Server	۲۴ساعت
سامانه‌های کاربردی	۴ساعت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۶- طبقه‌بندی اطلاعات

سطح بحرانی

- پایگاه‌های داده
- سامانه‌های مالی
- سامانه‌های عملیاتی

سطح مهم

- فایل سرورها
- ایمیل‌ها
- مستندات اداری

سطح عادی

- اطلاعات عمومی
- فایل‌های غیرحساس

۷- انواع پشتیبان‌گیری

Full Backup

نسخه کامل از تمامی اطلاعات

مزایا:

- بازیابی سریع
- ساده

معایب:

- حجم زیاد
- زمان طولانی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

Incremental Backup

فقط تغییرات از آخرینBackup

مزایا:

- حجم کم
- سرعت بالا

معایب:

- بازیابی پیچیده‌تر

Differential Backup

تغییرات نسبت به آخرین Full Backup

مزایا:

- بازیابی آسان‌تر

۸- برنامه پشتیبان‌گیری

ماشین‌های مجازیVMware

Daily Incremental

Weekly Full

Monthly Archive

SQL Server

Backup ساعتی Transaction Log

Backupروزانه Database

Backupهفتگی Full

Active Directory

Backup روزانه

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

System State Backup

File Server

Daily Incremental

Weekly Full

۹- قانون ۳-۲-۱

سازمان باید حداقل:

- ۳ نسخه از اطلاعات
- ۲رسانه متفاوت
- ۱نسخه خارج از سایت

نگهداری نماید.

۱۰- محل نگهداری نسخه‌های پشتیبان

نسخه‌ها باید در مکان‌های زیر نگهداری شوند:

Primary Backup Storage

ذخیره‌ساز اصلی

Secondary Backup Storage

ذخیره‌ساز دوم

Offsite Storage

مکان فیزیکی دیگر

(Cloud Backup)در صورت مجاز بودن

فضای ابری

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۱- حفاظت از Backup ها

نسخه‌های پشتیبان باید:

- رمزنگاری شوند .
- دسترسی محدود داشته باشند .
- در برابر حذف محافظت شوند .

Backup نباید در همان سرور اصلی ذخیره شود.

۱۲- حفاظت در برابر باج‌افزار

برای مقابله با:Ransomware

- Offline Backup
- Immutable Backup
- Air-Gap Backup

توصیه می‌شود.

۱۳-

Backup زیرساخت VMware

موارد زیر باید Backup شوند:

- VMها
- vCenter
- ESXi Configuration
- Distributed Switch Configuration

۱٤-

Backup پایگاه داده

شامل:

- Full Backup

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- Transaction Log Backup
- Differential Backup

تمام Backup ها باید به صورت دوره‌ای آزمایش شوند.

۱۵-

Backup Active Directory

باید شامل:

- System State
- Domain Controller
- Group Policy
- DNS

باشد.

۱۶-

Backup تجهیزات امنیتی

پیکربندی تجهیزات زیر باید Backup شود:

- FortiGate
- FortiAnalyzer
- Switches
- Routers

۱۷- **نگهداری نسخه‌ها**

روزانه

۳۰روز

هفتگی

۳ماه

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ماهانه

۱۲ماه

سالانه

حداقل ۳ سال

۱۸- فرآیند بازیابی اطلاعات

مراحل بازیابی:

تشخیص حادثه

درخواست بازیابی

تأیید بازیابی

Restore

اعتبارسنجی

بازگشت به سرویس

۱۹- آزمون بازیابی

تمام Backup ها باید حداقل:

هر شش ماه یکبار

تست شوند.

نمونه تست:

- بازیابی VM
- بازیابی SQL
- بازیابی فایل
- بازیابی Active Directory

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۰- سناریوهای بازیابی

خرابی یکVM

بازیابی از Snapshot یاBackup

خرابیHost

انتقال سرویس به Host دیگر

حذف فایل

Restoreفایل

خرابیSQL

Restore Database

حمله باج‌افزاری

Restoreاز نسخه سالم

۲۱- مسئولیت‌ها

مدیریت ارشد

تأمین منابع

واحد فناوری اطلاعات

اجرایBackup

مسئول امنیت اطلاعات

نظارت بر فرآیند

مدیر سامانه‌ها

اعتبارسنجیBackup

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۲- مانیتورینگBackup

موارد زیر باید روزانه بررسی شوند:

- موفقیت Backup
- فضای ذخیره‌سازی
- خطاها
- سلامت Backup Repository

۲۳- گزارش‌گیری

گزارش‌های زیر تولید می‌شود:

- Backup Success Rate
- Failed Backup
- Restore Test Result
- Storage Utilization

۲۴- شاخص‌های عملکرد

KPI -۰۱

موفقیتBackup

هدف:

بیش از ۹۸%

KPI -۰۲

موفقیتRestore

هدف:

۱۰۰٪

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

KPI -۰۳

انجام تست بازیابی

هدف:

حداقل دو بار در سال

KPI -۰٤

رعایتRTO

هدف:

۱۰۰٪

KPI -۰۵

رعایتRPO

هدف:

۱۰۰٪

۲۵- ممیزی

فرآیند Backup باید در ممیزی‌های داخلی و دوره‌ای بررسی گردد.

موارد بررسی:

- صحت Backup
- وضعیت نگهداری
- تست Restore
- امنیت نسخه‌ها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۶- تخلفات

موارد زیر تخلف محسوب می‌شوند:

- عدم انجام Backup
- حذف Backup بدون مجوز
- ذخیره Backup روی سرور اصلی
- عدم انجام تست Restore

۲۷- بازنگری

این سیاست حداقل سالی یک بار بازبینی خواهد شد.

۲۸- تأییدیه

این سند پس از تأیید مدیریت ارشد لازم‌الاجرا خواهد بود.

مراجع

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۳۱
- ISO ۲۲۳۰۱
- NIST SP ۸۰۰-۳٤
- NIST SP ۸۰۰-۲۰۹

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوستE

سیاست مدیریت رخدادهای امنیتی(Information Security Incident Management Policy)

شماره سند

IRP-۰۰۱

نسخه ۱.۰

تاریخ اجرا

پس از تصویب مدیریت ارشد

۱- مقدمه

با توجه به افزایش تهدیدات سایبری، حملات هدفمند، باج‌افزارها، نفوذهای غیرمجاز و سوءاستفاده از آسیب‌پذیری‌ها، هیچ سازمانی مصون از وقوع رخدادهای امنیتی نیست.

هدف این سند ایجاد یک فرآیند ساختاریافته برای شناسایی، ثبت، تحلیل، مهار، رفع و مستندسازی رخدادهای امنیتی به منظور کاهش خسارات و افزایش آمادگی سازمان می‌باشد.

۲- اهداف

اهداف اصلی این سیاست عبارتند از:

- تشخیص سریع رخدادها
- کاهش خسارات ناشی از حملات
- افزایش سرعت پاسخگویی
- حفظ شواهد دیجیتال
- جلوگیری از تکرار رخدادها
- افزایش بلوغ امنیتی سازمان
- ایجاد فرآیند پاسخگویی استاندارد

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳- دامنه کاربرد

این سیاست شامل تمامی دارایی‌های اطلاعاتی سازمان می‌شود:

- سرورها
- VMware Infrastructure
- Active Directory
- FortiGate
- FortiAnalyzer
- Wazuh
- تجهیزات شبکه
- پایگاه‌های داده
- سیستم‌های کاربران
- سامانه‌های کاربردی

٤- تعریف رخداد امنیتی

رخداد امنیتی هر رویدادی است که:

- محرمانگی اطلاعات را تهدید کند .
- صحت اطلاعات را تهدید کند .
- دسترس‌پذیری خدمات را تهدید کند .

٥- نمونه رخدادهای امنیتی

نفوذ غیرمجاز

دسترسی غیرمجاز به سیستم‌ها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بدافزار

آلودگی سیستم‌ها

باج‌افزار

رمز شدن فایل‌ها

حملات فیشینگ

سرقت اطلاعات هویتی

نشت اطلاعات

خروج اطلاعات سازمان

سوءاستفاده از دسترسی‌ها

استفاده غیرمجاز از مجوزها

حملات شبکه

- Port Scan
- Brute Force
- DoS
- DDoS

۶- ساختار پاسخگویی به رخداد

مدیریت ارشد

تصمیم‌گیری در رخدادهای بحرانی

مدیر فناوری اطلاعات

هماهنگی عملیات پاسخ

مسئول امنیت اطلاعات

مدیریت رخداد

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

کارشناسان فنی

تحلیل و رفع مشکل

کاربران

گزارش رویدادهای مشکوک

۷- طبقه‌بندی رخدادها

سطح ۱(Low)

رخدادهای کم اهمیت

نمونه:

قفل شدن حساب کاربری

سطح ۲(Medium)

اختلال محدود

نمونه:

بدافزار روی یک سیستم

سطح ۳(High)

اختلال گسترده

نمونه:

آلودگی چندین سیستم

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

سطح ۴(Critical)

بحرانی

نمونه:

- باج‌افزار
- نفوذ گسترده
- نشت اطلاعات
- توقف سرویس حیاتی

۸- فرآیند مدیریت رخداد

فرآیند پاسخگویی شامل مراحل زیر است:

۱. شناسایی
۲. ثبت
۳. تحلیل
٤. مهار
٥. رفع
٦. بازیابی
۷. گزارش نهایی

۹- شناسایی رخداد

رخدادها می‌توانند از طریق منابع زیر شناسایی شوند:

Wazuh

FortiAnalyzer

SIEM

کاربران

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

واحد فناوری اطلاعات

سامانه‌های مانیتورینگ

۱۰- ثبت رخداد

هر رخداد باید دارای شناسه یکتا باشد.

اطلاعات ثبت شده:

- تاریخ
- زمان
- سیستم درگیر
- گزارش‌دهنده
- سطح رخداد
- شرح رخداد

۱۱- تحلیل رخداد

موارد بررسی:

- علت اصلی
- دامنه تأثیر
- سیستم‌های آسیب دیده
- میزان خسارت
- روش حمله

۱۲- مهار رخداد

هدف:

جلوگیری از گسترش خسارت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

نمونه اقدامات:

قطع دسترسی کاربر

قرنطینه سیستم

مسدودسازیIP

غیرفعال‌سازی سرویس آسیب‌پذیر

جداسازی شبکه

۱۳- رفع رخداد

اقدامات اصلاحی:

- حذف بدافزار
- نصب Patch
- اصلاح تنظیمات
- تغییر رمزها
- حذف حساب‌های مخرب

۱٤- بازیابی سرویس

پس از رفع رخداد:

- Restore Backup
- بازگردانی VM
- فعال‌سازی سرویس‌ها
- اعتبارسنجی عملکرد

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۵- جمع‌آوری شواهد

در رخدادهای مهم باید موارد زیر حفظ شوند:

- لاگ‌ها
- تصاویر سیستم
- فایل‌های مشکوک
- اطلاعات شبکه

هدف:

امکان تحلیل و بررسی بعدی

۱۶- مدیریت شواهد دیجیتال

شواهد باید:

- تغییر نکنند .
- ثبت شوند .
- دارای زمان‌بندی باشند .
- در محل امن نگهداری شوند .

۱۷-

Escalation Matrix

سطح پایین

واحد فناوری اطلاعات

سطح متوسط

مدیر فناوری اطلاعات

سطح بالا

مسئول امنیت اطلاعات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

سطح بحرانی

مدیریت ارشد

۱۸- مدیریت رخدادهای باج‌افزاری

در صورت مشاهده:

۱. جداسازی سیستم
۲. قطع ارتباط شبکه
۳. تحلیل دامنه آلودگی
٤. بررسی Backup
٥. بازیابی اطلاعات
٦. گزارش نهایی

۱۹- مدیریت رخدادهای فیشینگ

اقدامات:

- مسدودسازی فرستنده
- اطلاع‌رسانی
- تغییر رمز کاربران
- بررسی لاگ‌ها

۲۰- مدیریت رخدادهای نفوذ

اقدامات:

- مسدودسازی مهاجم
- تحلیل مسیر نفوذ
- جمع‌آوری شواهد

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- اصلاح آسیب‌پذیری

۲۱- نقش SIEM در مدیریت رخداد

سامانه SIEM مسئول:

- تجمیع لاگ‌ها
- همبستگی رویدادها
- هشداردهی
- تحلیل اولیه

می‌باشد.

۲۲- نقش Wazuh

Wazuhمسئول:

- File Integrity Monitoring
- Vulnerability Detection
- Threat Detection
- Log Analysis

است.

۲۳- نقش FortiAnalyzer

FortiAnalyzer مسئول:

- تحلیل لاگ FortiGate
- گزارش حملات
- گزارش VPN
- تحلیل تهدیدات

می‌باشد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۴- زمان پاسخگویی

سطح رخداد	زمان پاسخ
Low	۸ساعت
Medium	۴ساعت
High	۲ساعت
Critical	۱ساعت

۲۵- شاخص‌های عملکرد

KPI -۰۱

MTTD

Mean Time To Detect

هدف:

کمتر از ۱۵ دقیقه

KPI -۰۲

MTTR

Mean Time To Respond

هدف:

کمتر از ۳۰ دقیقه

KPI -۰۳

درصد رخدادهای ثبت شده

هدف:

۱۰۰٪

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

KPI -۰٤

درصد رخدادهای تحلیل شده

هدف:

۱۰۰٪

۲٦- آموزش تیم پاسخگویی

اعضای تیم باید آموزش ببینند در:

- تحلیل لاگ
- Wazuh
- FortiAnalyzer
- مدیریت رخداد
- پاسخ به حملات

۲۷- مانورهای امنیتی

حداقل سالی یکبار:

- مانور باج‌افزار
- مانور نفوذ
- مانور بازیابی

انجام خواهد شد.

۲۸- گزارش نهایی رخداد

گزارش نهایی باید شامل:

- علت
- دامنه تأثیر
- خسارت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- اقدامات انجام شده
- درس آموخته‌ها

باشد.

۲۹- ممیزی و بازنگری

این سیاست حداقل سالی یکبار بازبینی می‌شود.

۳۰- تأییدیه

این سند پس از تصویب مدیریت ارشد لازم‌الاجرا خواهد بود.

مراجع

- ISO/IEC ۲۷۰۳۵
- NIST SP ۸۰۰-٦١ Rev.۲
- NIST Cybersecurity Framework
- SANS Institute

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوستF

فرم‌ها، رویه‌ها و Playbook های مدیریت رخداد امنیتی

شماره سند

IRF -۰۰۱

نسخه ۱.۰

هدف

ایجاد قالب‌های استاندارد جهت:

- ثبت رخداد
- تحلیل رخداد
- پاسخ به رخداد
- مستندسازی
- درس‌آموخته‌ها
- ممیزی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بخش اول

فرم ثبت رخداد امنیتی

Incident Report Form

اطلاعات پایه

شماره رخداد:

IR-YYYY-XXXX

تاریخ:

ساعت:

نام گزارش دهنده:

واحد سازمانی:

شماره تماس:

اطلاعات رخداد

نوع رخداد:

□ بدافزار

□ باج افزار

□ فیشینگ

□ نفوذ

□ نشت اطلاعات

□ حمله شبکه

□ اختلال سرویس

□سایر

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

سیستم درگیر:

IP:

نام سرور:

شرح رخداد:

.....

.....

.....

سطح اهمیت

□ Low

□ Medium

□ High

□ Critical

وضعیت فعلی

□ باز

□ در حال بررسی

□ مهار شده

□ رفع شده

□ بسته شده

تأیید

کارشناس امنیت:

مدیر فناوری اطلاعات:

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بخش دوم

فرم تحلیل ریشه‌ای رخداد

Root Cause Analysis

شماره رخداد:

نوع رخداد:

علت اصلی

☐ خطای انسانی

☐ ضعف تنظیمات

☐ آسیب‌پذیری

☐ بدافزار

☐ نقص نرم‌افزار

☐ نقص سخت‌افزار

☐ حمله خارجی

شرح علت:

.....

.....

عوامل مؤثر

- عامل اول
- عامل دوم
- عامل سوم

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

اقدامات اصلاحی

- مورد اول
- مورد دوم
- مورد سوم

مسئول اجرا

زمان اجرا

تأیید نهایی

بخش سوم

فرم درس‌آموخته‌ها

Lessons Learned Report

شماره رخداد:

تاریخ:

نوع رخداد:

چه اتفاقی افتاد؟

.....

چه چیزی خوب انجام شد؟

.....

چه چیزی نیاز به بهبود دارد؟

.....

پیشنهادات آینده

.....

تصمیمات مدیریتی .....

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بخش چهارم

Playbook پاسخ به باج افزار

Ransomware Response Playbook

مرحله ۱

شناسایی

نشانه‌ها:

- تغییر نام فایل‌ها
- رمز شدن فایل‌ها
- پیام باج خواهی
- افزایش مصرف CPU

مرحله ۲

مهار

اقدامات:

- قطع شبکه سیستم
- غیرفعال کردن WiFi
- جداسازی VM
- مسدودسازی دسترسی

مرحله ۳

تحلیل

بررسی:

- نقطه ورود
- دامنه آلودگی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- حساب آلوده

مرحله ۴

حذف

- حذف فایل مخرب
- پاکسازی سیستم
- نصب Patch

مرحله ۵

بازیابی

- Restore Backup
- بررسی صحت اطلاعات
- راه‌اندازی مجدد سرویس

مرحله ۶

گزارش نهایی

بخش پنجم

Playbook پاسخ به فیشینگ

Phishing Response Playbook

شناسایی

نشانه‌ها:

- ایمیل مشکوک
- لینک جعلی
- صفحه Login تقلبی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

مهار

- حذف ایمیل
- مسدودسازی دامنه
- اطلاع‌رسانی

اصلاح

- تغییر رمز کاربران
- فعال‌سازی MFA
- بررسی لاگ‌ها

گزارش

مستندسازی کامل

بخش ششم

Playbookنفوذ غیرمجاز

Unauthorized Access Playbook

مرحله اول

شناسایی

منابع:

- Wazuh
- SIEM
- FortiAnalyzer

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

مرحله دوم

جمع‌آوری شواهد

- لاگ‌ها
- IPمهاجم
- زمان رخداد

مرحله سوم

مهار

- مسدودسازی IP
- غیرفعال‌سازی حساب

مرحله چهارم

تحلیل

- مسیر نفوذ
- آسیب‌پذیری مورد سوءاستفاده

مرحله پنجم

اصلاح

- نصب Patch
- تغییر تنظیمات
- اصلاح Rule ها

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

بخش هفتم

Playbookخرابی سرور

Server Failure Playbook

نشانه‌ها:

- عدم پاسخگویی
- خاموش شدن VM
- خرابی Host

اقدامات:

- بررسی وضعیت Host
- بررسی Storage
- Restore Backup
- فعال‌سازی HA

بخش هشتم

Playbookنشت اطلاعات

Data Leakage Playbook

شناسایی:

- دانلود غیرعادی
- ارسال فایل مشکوک
- خروج اطلاعات

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

اقدامات:

- قطع دسترسی
- بررسی لاگ‌ها
- حفظ شواهد
- گزارش به مدیریت

بخش نهم

ماتریسEscalation

مسئول	سطح
کارشناسIT	Low
مدیرIT	Medium
مسئول امنیت	High
مدیریت ارشد	Critical

بخش دهم

چک لیست بستن رخداد

قبل از بسته شدن هر رخداد باید تأیید شود:

□ علت اصلی مشخص شده

□ خسارت مشخص شده

□ اصلاح انجام شده

□ مستندات تکمیل شده

□ درس‌آموخته ثبت شده

□ مدیریت تأیید کرده

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوستG

متدولوژی ارزیابی ریسک، فرم‌های ارزیابی ریسک وRisk Register

شماره سند

RMP-۰۰۱

نسخه ۱.۰

۱- مقدمه

ریسک امنیت اطلاعات به احتمال وقوع یک تهدید و میزان خسارت ناشی از آن گفته می‌شود.

هدف از مدیریت ریسک حذف کامل ریسک نیست؛ بلکه شناسایی، ارزیابی و کاهش آن تا سطح قابل قبول سازمان است.

بر اساس الزامات ISO/IEC ۲۷۰۰۱:۲۰۲۲ و ISO ۳۱۰۰۰ تمامی دارایی‌های اطلاعاتی باید مورد ارزیابی ریسک قرار گیرند.

۲- اهداف مدیریت ریسک

اهداف این فرآیند عبارتند از:

- شناسایی تهدیدات
- شناسایی آسیب‌پذیری‌ها
- تعیین سطح ریسک
- اولویت‌بندی اقدامات امنیتی
- تخصیص صحیح منابع
- کاهش احتمال رخدادهای امنیتی
- پشتیبانی از تصمیم‌گیری مدیریت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳- دامنه ارزیابی ریسک

این فرآیند شامل کلیه دارایی‌های سازمان می‌شود:

- سرورهای فیزیکی
- VMware Infrastructure
- ماشین‌های مجازی
- Active Directory
- SQL Server
- File Server
- FortiGate
- FortiAnalyzer
- Wazuh
- تجهیزات شبکه
- اطلاعات سازمانی
- کاربران
- پیمانکاران
- لینک‌های ارتباطی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

٤- فرآیند مدیریت ریسک

فرآیند شامل مراحل زیر است:

شناسایی دارایی
↓
شناسایی تهدید
↓
شناسایی آسیب پذیری
↓
محاسبه ریسک
↓
تصمیم گیری
↓
اجرای کنترل
↓
بازبینی

٥- شناسایی دارایی‌ها

دارایی هر چیزی است که برای سازمان ارزش دارد.

دارایی‌های اطلاعاتی

- پایگاه داده‌ها
- اسناد مالی
- اطلاعات کارکنان
- اطلاعات مشتریان

دارایی‌های نرم‌افزاری

- سامانه‌ها
- نرم‌افزارهای کاربردی

- سیستم عامل‌ها

دارایی‌های سخت‌افزاری

- سرورها
- سوئیچ‌ها
- روترها
- فایروال‌ها

دارایی‌های انسانی

- مدیران
- کارشناسان
- کاربران

۶- تعیین ارزش دارایی

برای هر دارایی ارزش تعیین می‌شود.

ارزش	امتیاز
بسیار کم	۱
کم	۲
متوسط	۳
زیاد	۴
بسیار زیاد	۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

نمونه

ارزش	دارایی
۵	Domain Controller
۵	SQL Server
۴	File Server
۲	PCکاربر

۷- شناسایی تهدیدات

نمونه تهدیدات:

انسانی

- خطای کاربر
- سوءاستفاده داخلی
- مهندسی اجتماعی

فنی

- نفوذ
- بدافزار
- باج افزار
- Exploit

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

محیطی

- آتش‌سوزی
- سیل
- زلزله

زیرساختی

- قطعی برق
- خرابی UPS
- خرابی Storage

۸- شناسایی آسیب‌پذیری‌ها

نمونه:

- Patchنصب نشده
- رمز عبور ضعیف
- عدم MFA
- Backupنامناسب
- تنظیمات اشتباه Firewall
- عدم مانیتورینگ

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹- احتمال وقوع(Likelihood)

احتمال	امتیاز
بسیار کم	۱
کم	۲
متوسط	۳
زیاد	۴
بسیار زیاد	۵

۱۰- میزان اثر(Impact)

اثر	امتیاز
ناچیز	۱
کم	۲
متوسط	۳
زیاد	۴
فاجعه‌آمیز	۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۱- محاسبه ریسک

فرمول محاسبه:

مثال

احتمال وقوع:

۴

اثر:

۵

ریسک:

۲۰

۱۲- ماتریس ریسک

وضعیت	ریسک
کم	۱تا ۵
متوسط	۶تا ۱۰
زیاد	۱۱تا ۱۵
بحرانی	۱۶تا ۲۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۳- معیار پذیرش ریسک

ریسک کم

پذیرش

ریسک متوسط

پایش

ریسک زیاد

اصلاح

ریسک بحرانی

اقدام فوری

۱٤- روش‌های برخورد با ریسک

پذیرش

Accept

کاهش

Mitigate

انتقال

Transfer

نمونه:

بیمه

حذف

Avoid

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۵- فرم ارزیابی ریسک

Risk Assessment Form

کد ریسک:

R-۰۰۱

دارایی:

مالک دارایی:

تهدید:

آسیب‌پذیری:

احتمال:

۱تا ۵

اثر:

۱تا ۵

امتیاز ریسک:

وضعیت:

کنترل پیشنهادی:

مسئول:

تاریخ بازبینی:

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۶- نمونه Risk Register

کد	دارایی	تهدید	احتمال	اثر	ریسک
R۰۰۱	AD	باج افزار	۴	۵	۲۰
R۰۰۲	VMware	خرابیHost	۳	۵	۱۵
R۰۰۳	FortiGate	تنظیمات اشتباه	۳	۴	۱۲
R۰۰٤	SQL	نشت اطلاعات	۳	۵	۱۵
R۰۰۵	File Server	حذف اطلاعات	۴	۴	۱۶

۱۷- نمونه کنترل‌های پیشنهادی

Active Directory

- MFA
- Backup
- Monitoring

VMware

- HA
- Backup
- Patch Management

FortiGate

- Rule Review
- MFA
- Log Monitoring

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

SQL

- Encryption
- Backup
- Access Control

۱۸- بازبینی ریسک

ریسک‌ها باید:

حداقل هر شش ماه یا در شرایط زیر بازبینی شوند:

- تغییر زیرساخت
- خرید تجهیزات
- رخداد امنیتی
- تغییر قوانین

۱۹- ارتباط باSIEM

سامانه SIEM می‌تواند در شناسایی ریسک‌های زیر کمک کند:

- Login Failure
- Brute Force
- Malware
- Unauthorized Access

۲۰- ارتباط باWazuh

Wazuhدر شناسایی موارد زیر نقش دارد:

- آسیب‌پذیری‌ها
- تغییر فایل‌ها
- رفتار مشکوک
- Compliance Monitoring

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۱- ارتباط باFortiAnalyzer

کمک در شناسایی:

- حملات شبکه
- VPN Abuse
- Threat Detection

۲۲- شاخص‌های عملکرد

KPI -۰۱

ریسک‌های بحرانی اصلاح شده

هدف:

۱۰۰٪

KPI -۰۲

ریسک‌های بازبینی شده

هدف:

۱۰۰٪

KPI -۰۳

ریسک‌های بدون مالک

هدف:

۰

KPI -۰٤

ریسک‌های پذیرش شده

پایش مستمر

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۳- گزارش‌دهی به مدیریت

گزارش ریسک باید شامل:

- تعداد ریسک‌ها
- ریسک‌های بحرانی
- وضعیت اصلاح
- روند تغییرات

باشد.

۲۴- تأییدیه

این سند پس از تأیید مدیریت ارشد لازم‌الاجرا خواهد بود.

مراجع

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO ۳۱۰۰۰
- ISO/IEC ۲۷۰۰۵
- NIST SP ۸۰۰-۳۰

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوستH

مدیریت دارایی‌های اطلاعاتی وAsset Register

شماره سند

ASM -۰۰۱

نسخه ۱,۰

۱- مقدمه

تمام دارایی‌های اطلاعاتی سازمان دارای ارزش بوده و باید شناسایی، ثبت، طبقه‌بندی و محافظت شوند.

عدم آگاهی از دارایی‌های موجود یکی از مهم‌ترین دلایل شکست پروژه‌های امنیت اطلاعات است؛ زیرا سازمان نمی‌تواند از چیزی که نمی‌شناسد محافظت کند.

این سند چارچوب مدیریت دارایی‌های اطلاعاتی سازمان را مشخص می‌کند.

۲- هدف

اهداف این سند عبارتند از:

- شناسایی کامل دارایی‌ها
- تعیین مالک دارایی
- تعیین سطح اهمیت دارایی
- طبقه‌بندی اطلاعات
- تسهیل مدیریت ریسک
- تسهیل ممیزی
- پشتیبانی از فرآیند ISMS

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳- دامنه کاربرد

این سند شامل تمامی دارایی‌های زیر می‌شود:

اطلاعات

- اطلاعات مالی
- اطلاعات پرسنلی
- اطلاعات قراردادها
- اطلاعات سامانه‌ها

نرم‌افزارها

- Windows Server
- Linux
- VMware
- SQL Server
- FortiAnalyzer
- Wazuh

سخت‌افزارها

- سرورها
- ذخیره‌سازها
- سوئیچ‌ها
- روترها
- فایروال‌ها
- UPS

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

خدمات

- اینترنت
- VPN
- ایمیل
- سرویس‌های ابری

منابع انسانی

- مدیران
- کارشناسان
- پیمانکاران

٤- تعاریف

Asset

هر چیزی که برای سازمان ارزش ایجاد می‌کند.

Asset Owner

فرد یا واحد مسئول دارایی

Asset Custodian

فرد مسئول نگهداری دارایی

Asset Classification

سطح اهمیت دارایی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۵- طبقه‌بندی دارایی‌ها

اطلاعاتی

Data Assets

نرم‌افزاری

Software Assets

سخت‌افزاری

Hardware Assets

ارتباطی

Network Assets

انسانی

Human Assets

خدماتی

Service Assets

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۶- فرآیند مدیریت دارایی

شناسایی

↓

ثبت

↓

طبقه بندی

↓

تخصیص مالک

↓

پایش

↓

بازبینی

۷- شناسایی دارایی‌ها

دارایی‌ها از طریق:

- بازدید میدانی
- مصاحبه
- مستندات
- Active Directory
- VMware
- CMDB
- اسکن شبکه

شناسایی می‌شوند.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸- مالکیت دارایی

هر دارایی باید دارای:

- مالک
- مسئول نگهداری
- مسئول فنی

باشد.

مثال

دارایی:

SQL Server

مالک:

مدیر فناوری اطلاعات

مسئول نگهداری:

کارشناس زیرساخت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۹- ارزش‌گذاری دارایی‌ها

معیارهای ارزش‌گذاری:

محرمانگی

Confidentiality

صحت

Integrity

دسترس‌پذیری

Availability

هر کدام از ۱ تا ۵ امتیاز می‌گیرند.

۱۰- سطح اهمیت دارایی

سطح	امتیاز
بسیار کم	۱
کم	۲
متوسط	۳
زیاد	۴
بحرانی	۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۱- طبقه‌بندی اطلاعات

عمومی

Public

داخلی

Internal

محرمانه

Confidential

خیلی محرمانه

Restricted

۱۲-

Asset Register

نمونه فرم

کد دارایی:

AST-۰۰۱

نام دارایی:

VMware Cluster

نوع:

Virtualization

مالک:

مدیر IT

مکان:

مرکز داده

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

سطح اهمیت:

بحرانی

طبقه‌بندی:

محرمانه

۱۳- نمونه Asset Register زیرساخت

کد	دارایی	نوع	اهمیت
AST۰۰۱	VMware Cluster	Virtualization	۵
AST۰۰۲	Domain Controller	Server	۵
AST۰۰۳	SQL Server	Database	۵
AST۰۰٤	File Server	Server	۴
AST۰۰۵	FortiGate	Security Device	۵

۱٤- نمونه دارایی‌های محیط صمت

سرورهای فیزیکی

- HPE G۱۰
- HPE G۹
- HPE G۸

مجازی‌سازی

- VMware ESXi
- vCenter

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ماشین‌های مجازی

تقریباً VM۲۰

تجهیزات امنیتی

- FortiGate ۱۰۰F

سامانه‌های امنیتی

- Wazuh
- FortiAnalyzer
- SIEM

۱۵- مدیریت چرخه عمر دارایی

خرید

بهره‌برداری

نگهداری

بازنشستگی

امحا

۱۶- الزامات دارایی‌های سخت‌افزاری

تمام تجهیزات باید:

- شماره سریال داشته باشند .
- ثبت شوند .
- برچسب‌گذاری شوند .

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۷- الزامات دارایی‌های نرم‌افزاری

تمام نرم‌افزارها باید:

- دارای مجوز باشند .
- ثبت شوند .
- نسخه مشخص داشته باشند .

۱۸- مدیریت دارایی‌های مجازی

برای VMware باید موارد زیر ثبت شود:

- نام VM
- IP
- سیستم عامل
- مالک
- کاربرد
- سطح اهمیت

نمونه

کاربرد	VM
Active Directory	VM-AD۰۱
Database	VM-SQL۰۱
File Server	VM-FILE۰۱
SIEM	VM-WAZUH۰۱

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۹- مدیریت دارایی‌های شبکه

ثبت اطلاعات:

- Switch
- Router
- Firewall
- VPN Gateway

اطلاعات ثبت شده:

- IP
- مدل
- Firmware
- مکان

۲۰- مدیریت دارایی‌های اطلاعاتی

اطلاعات زیر باید ثبت شوند:

- پایگاه داده‌ها
- فایل‌ها
- اسناد
- قراردادها

۲۱- مدیریت دارایی‌های انسانی

ثبت:

- مدیران
- کارشناسان
- پیمانکاران ، به عنوان دارایی‌های کلیدی سازمان

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۲- ارتباط Asset Register باRisk Register

هر ریسک باید به یک دارایی متصل باشد.

مثال:

دارایی:

SQL Server

ریسک:

نشت اطلاعات

کنترل:

Encryption

۲۳- ارتباط باSIEM

سامانه SIEM باید بتواند:

- دارایی‌های حیاتی را شناسایی کند .
- رخدادها را به دارایی مرتبط نماید .

۲۴- ارتباط با Wazuh

Wazuh می‌تواند:

- Asset Discovery
- Vulnerability Discovery
- Inventory Collection

را انجام دهد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۵- شاخص‌های عملکرد

KPI -۰۱

دارایی‌های ثبت شده

هدف:

۱۰۰٪

KPI -۰۲

دارایی‌های دارای مالک

هدف:

۱۰۰٪

KPI -۰۳

دارایی‌های طبقه‌بندی شده

هدف:

۱۰۰٪

KPI-۰٤

دارایی‌های بازبینی شده

هدف:

۱۰۰٪

۲۶- بازبینیAsset Register

حداقل:

هر شش ماه

یکبار

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

یا در صورت:

- خرید تجهیزات جدید
- حذف تجهیزات
- تغییر زیرساخت

۲۷- ممیزی

در ممیزی موارد زیر بررسی می‌شود:

- کامل بودن Asset Register
- تعیین مالک
- طبقه‌بندی
- ارزش‌گذاری

۲۸- تأییدیه

این سند پس از تصویب مدیریت ارشد لازم‌الاجرا خواهد بود.

مراجع

- ISO/IEC ۲۷۰۰۱:۲۰۲۲
- ISO/IEC ۲۷۰۰۲:۲۰۲۲
- ISO ۵۵۰۰۰
- NIST SP ۸۰۰-۵۳

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوست I

نمونه Risk Register و برنامه مدیریت ریسک سازمان

شماره سند

RRG-۰۰۱

نسخه : ۱.۰

۱- مقدمه

این پیوست نمونه‌ای از ریسک‌های محتمل در زیرساخت فناوری اطلاعات سازمان را ارائه می‌نماید.

هدف این سند کمک به شناسایی اولیه ریسک‌ها، اولویت‌بندی اقدامات اصلاحی و برنامه‌ریزی امنیتی می‌باشد.

توجه :ریسک‌های نهایی پس از بازدید میدانی، مصاحبه، Asset Discoveryو ارزیابی تفصیلی تعیین خواهند شد.

۲- مقیاس امتیازدهی

احتمال وقوع

توضیح	امتیاز
بسیار کم	۱
کم	۲
متوسط	۳
زیاد	۴
بسیار زیاد	۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

میزان اثر

توضیح	امتیاز
ناچیز	۱
کم	۲
متوسط	۳
زیاد	۴
بحرانی	۵

سطح ریسک

سطح	امتیاز
کم	۱-۵
متوسط	۶-۱۰
زیاد	۱۱-۱۵
بحرانی	۱۶-۲۵

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۳-

- **Risk Register**

ریسک شماره۰۰۱ - R

دارایی

Active Directory

تهدید

باج‌افزار

آسیب‌پذیری

عدم جداسازی دسترسی‌ها

احتمال : ۴

اثر ۵

امتیاز ریسک

۲۰

سطح

بحرانی

کنترل پیشنهادی

- MFA
- Backup
- Wazuh
- Patch Management

مسئول

مدیر زیرساخت

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره۰۰۲-R

دارایی

VMware Cluster

تهدید

خرابیHost

آسیب‌پذیری

نبودHA

احتمال

۳

اثر

۵

امتیاز

۱۵

سطح

زیاد

کنترل

- VMware HA
- Backup
- مانیتورینگ

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره۰۰۳ - R

دارایی

SQL Server

تهدید

نشت اطلاعات

آسیب‌پذیری

سطح دسترسی نامناسب

احتمال

۳

اثر

۵

امتیاز

۱۵

کنترل

- Encryption
- Access Control
- Audit Logging

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره R -۰۰٤

دارایی

FortiGate ۱۰۰F

تهدید

نفوذ

آسیب‌پذیری

Ruleهای اشتباه

احتمال

۳

اثر

۵

امتیاز

۱۵

کنترل

- Rule Review
- MFA
- Log Monitoring

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره۰۰۵ - R

دارایی

VPN

تهدید

سرقت اعتبارنامه

آسیب‌پذیری

عدمMFA

احتمال

۴

اثر

۴

امتیاز

۱۶

سطح

بحرانی

کنترل

- MFA
- Password Policy
- Monitoring

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره R - ۰۰۶

دارایی

File Server

تهدید

حذف اطلاعات

آسیب‌پذیری

نبود نسخه پشتیبان

احتمال

۴

اثر

۴

امتیاز

۱۶

سطح : بحرانی

کنترل

- Backup
- Snapshot
- Restore Testing

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره R -۰۰۷

دارایی

Wazuh Server

تهدید

از کار افتادن مانیتورینگ

آسیب‌پذیری

Single Point of Failure

احتمال

۳

اثر

۴

امتیاز

۱۲

کنترل

- Backup
- Redundancy
- Monitoring

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره R - ۰۰۸

دارایی

کاربران سازمان

تهدید

فیشینگ

آسیب‌پذیری

کمبود آموزش

احتمال

۵

اثر

۴

امتیاز

۲۰

کنترل

- Security Awareness
- Phishing Campaign
- MFA

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره R - ۰۰۹

دارایی

Storage

تهدید

خرابی دیسک

آسیب‌پذیری

نبود افزونگی

احتمال

۳

اثر

۵

امتیاز

۱۵

کنترل

- RAID
- Backup
- Monitoring

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

ریسک شماره R - ۰۱۰

دارایی

اینترنت سازمان

تهدید

قطع ارتباط

آسیب‌پذیری

Single ISP

احتمال

۴

اثر

۴

امتیاز

۱۶

کنترل

- لینک پشتیبان
- Failover

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۴- برنامه مدیریت ریسک

مرحله اول

شناسایی ریسک

مرحله دوم

تحلیل ریسک

مرحله سوم

اولویت‌بندی

مرحله چهارم

انتخاب کنترل

مرحله پنجم

پیاده‌سازی کنترل

مرحله ششم

بازبینی اثربخشی

۵- برنامه اصلاح ریسک‌های بحرانی

ریسک	زمان اصلاح
MFA VPN	۱ماه
Backup	۱ماه
آموزش کاربران	۲ماه
HA VMware	۳ماه
SIEM	۳ ماه

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۶:

Risk Treatment Plan

برای هر ریسک باید فرم زیر تکمیل گردد:

فیلد	مقدار
شناسه ریسک	R-۰۰۱
شرح ریسک	باج افزار
کنترل انتخابی	Backup
مسئول	مدیرIT
مهلت اجرا	۳۰روز
وضعیت	باز

۷- گزارش دوره‌ای ریسک

گزارش مدیریت باید شامل:

- تعداد کل ریسک‌ها
- ریسک‌های بحرانی
- ریسک‌های اصلاح شده
- ریسک‌های باز
- روند تغییرات

باشد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۸- داشبورد مدیریتی ریسک

شاخص‌های کلیدی:

تعداد ریسک‌های بحرانی

درصد ریسک‌های اصلاح شده

میانگین زمان اصلاح

تعداد ریسک‌های جدید

۹- ارتباط با پروژهSIEM

سامانه SIEM کمک می‌کند:

- ریسک‌های فعال سریع‌تر شناسایی شوند .
- هشدارها تولید شوند .
- شاخص‌های امنیتی استخراج شوند .

۱۰- ارتباط با پروژهISMS

این سند یکی از مهم‌ترین خروجی‌های ISMS است و مبنای:

- انتخاب کنترل‌ها
- تخصیص بودجه
- تصمیم‌گیری مدیریتی
- ممیزی‌ها

قرار می‌گیرد.

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

مراجع

- ISO/IEC ۲۷۰۰۵
- ISO ۳۱۰۰۰
- NIST SP ۸۰۰-۳۰
- NIST Cybersecurity Framework

شماره ی تماس : ۰۹۱۲۷۲۴۳۲۶۷
آدرس وب سایت : https://www.sekkodata.com
آدرس ایمیل : kaedi.mohsen@sekkodata.com

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

پیوست J

معماری فنی و نقشه اجرایی پروژه ISMS و SIEM

شماره سند

ARC-۰۰۱

نسخه

۱.۰

۱- مقدمه

این پیوست نمای کلی معماری فنی پروژه را ارائه می‌کند و نشان می‌دهد اجزای مختلف زیرساخت، امنیت، مانیتورینگ، SIEM، پشتیبان‌گیری و تداوم کسب‌وکار چگونه در کنار یکدیگر عمل خواهند کرد.

هدف اصلی این معماری:

- افزایش امنیت
- افزایش دیدپذیری (Visibility)
- افزایش تاب‌آوری
- کاهش ریسک
- تسهیل ممیزی
- تسریع پاسخگویی به رخدادها

می‌باشد.

۲- وضعیت هدف پروژه

در پایان پروژه سازمان دارای اجزای زیر خواهد بود:

لایه کاربران

- کاربران داخلی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- مدیران
- کارشناسان
- پیمانکاران

لایه دسترسی

- Active Directory
- MFA
- VPN

لایه امنیت مرزی

- FortiGate ۱۰۰F

لایه مجازی‌سازی

- VMware ESXi
- vCenter

لایه سرورها

- Active Directory
- SQL Server
- File Server
- Application Server

لایه امنیت

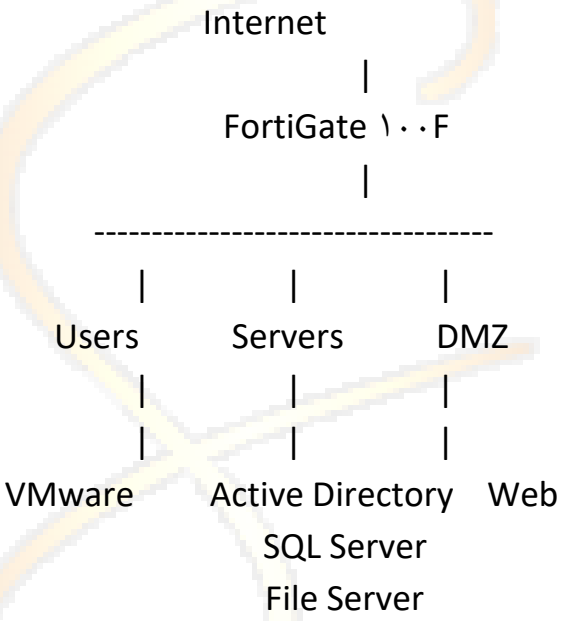
- Wazuh
- FortiAnalyzer
- SIEM

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

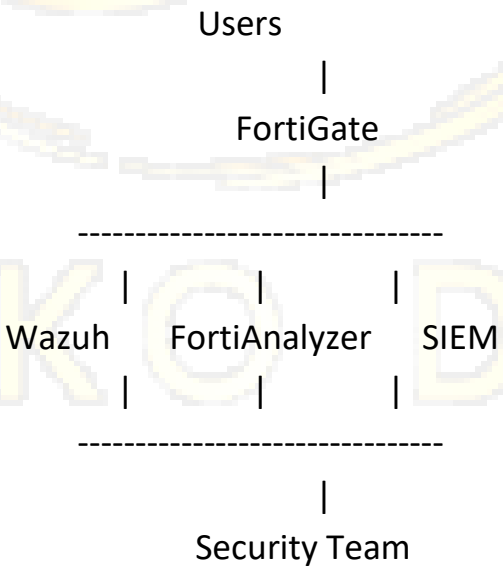
لایه تداوم کسب‌وکار

- Backup
- Restore
- HA
- DR

۳- معماری منطقی شبکه



۴- معماری امنیتی



دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

هدف:

تجمیع کامل رخدادهای امنیتی

۵- معماری SIEM

منابع لاگ:

FortiGate

Windows Server

Linux Server

VMware

Active Directory

SQL Server

Application Servers

VPN

همگی لاگ‌های خود را به SIEM ارسال می‌کنند.

Windows Server ----\
Linux Server -------\
VMware ---------- \
FortiGate ----------> SIEM
VPN ---------- /
Database ----------/

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۶- معماری Wazuh

عامل‌های Wazuh روی تمامی سرورها نصب می‌شوند.

وظایف:

Log Collection

File Integrity Monitoring

Vulnerability Assessment

Compliance Monitoring

Malware Detection

VM۰۱ --------\
VM۰۲ ---------\
VM۰۳ ----------\
VM۰٤ ----------> Wazuh Server
VM۰۵ ----------/
VM۰٦ ---------/
VM۰۷ --------/

۷- معماری FortiAnalyzer

FortiAnalyzer مسئول تحلیل لاگ تجهیزات امنیتی خواهد بود.

منابع:

- FortiGate
- VPN
- IPS
- Antivirus
- Web Filter

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

FortiGate
|
FortiAnalyzer
|
Security Reports

۸- معماری مانیتورینگ

هدف:

مشاهده وضعیت امنیتی سازمان در یک داشبورد واحد

شاخص‌ها:

- Login Failure
- Malware
- VPN Activity
- Resource Usage
- Threats
- Vulnerabilities

۹- معماری VMware

Vmware Cluster

| | |
ESXi۰۱ ESXi۰۲ ESXi۰۳
| | |

Shared Storage

مزایا:

- HA
- Migration
- Fault Tolerance

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

- مدیریت متمرکز

۱۰- معماری High Availability

پیشنهاد پروژه

Host ۱
|
|
Shared Storage
|
|
Host ۲

در صورت خرابی Host:

VMها روی Host دوم اجرا می‌شوند.

۱۱- معماری Backup

Production
|
Backup Server
|
Secondary Storage
|
Offsite Storage

سیاست:

- Daily Backup
- Weekly Backup
- Monthly Archive

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۲- معماری Disaster Recovery

سناریو:

از دست رفتن کامل سایت اصلی

Primary Site
|
|
Replication
|
|
DR Site

اهداف:

- کاهش زمان توقف
- بازیابی سریع خدمات

۱۳- جریان لاگ‌ها

Users
|
Servers
|
Applications
|
FortiGate
|
|----> Wazuh
|
|----> FortiAnalyzer
|
|----> SIEM

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۴- معماری مدیریت آسیب‌پذیری

Wazuh
|
Vulnerability Scan
|
Risk Analysis
|
Remediation

خروجی:

- CVEها
- سطح ریسک
- اقدامات اصلاحی

۱۵- معماری کنترل دسترسی

Users
|
Active Directory
|
Role Based Access Control
|
Applications

هدف:

پیاده‌سازیRBAC

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۶- معماری VPN

Remote User
|
|
VPN + MFA
|
|
FortiGate
|
|
Internal Resources

هدف:

دسترسی امن کاربران راه دور

۱۷- معماری پاسخگویی به رخداد

Threat
|
Detection
|
SIEM / Wazuh
|
Alert
|
Security Team
|
Containment
|
Recovery

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۸- نقشه راه فنی اجرا

فاز اول

شناخت وضع موجود

فاز دوم

Asset Discovery

فاز سوم

Risk Assessment

فاز چهارم

استقرارISMS

فاز پنجم

استقرارWazuh

فاز ششم

استقرارFortiAnalyzer

فاز هفتم

راه‌اندازیSIEM

فاز هشتم

آموزش

فاز نهم

ممیزی

فاز دهم

تحویل نهایی

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۱۹- خروجی‌های نهایی پروژه

پس از اتمام پروژه سازمان دارای موارد زیر خواهد بود:

مدیریتی

- ISMS
- Risk Management
- Asset Management

امنیتی

- SIEM
- Wazuh
- FortiAnalyzer

زیرساختی

- VMware HA
- Backup
- Monitoring

عملیاتی

- Incident Management
- Vulnerability Management

پدافندی

- تداوم خدمت
- تاب‌آوری
- Disaster Recovery

دیدار داده محسن (سهامی خاص) شماره ی ثبت : ۱۴۰۱۴۹۶۸۹۸۶
آدرس : خرم آباد کارخانه ی نوآوری پارک علم و فن آوری لرستان

۲۰- جمع‌بندی نهایی معماری

این معماری با هدف ایجاد یک زیرساخت یکپارچه امنیت اطلاعات طراحی شده است که بتواند:

- الزامات ISMS را پوشش دهد .
- نیازهای پدافند غیرعامل را پاسخ دهد .
- قابلیت پایش و تحلیل امنیتی متمرکز ایجاد کند .
- ریسک‌های عملیاتی و امنیتی را کاهش دهد .
- تاب‌آوری زیرساخت فناوری اطلاعات سازمان را افزایش دهد .