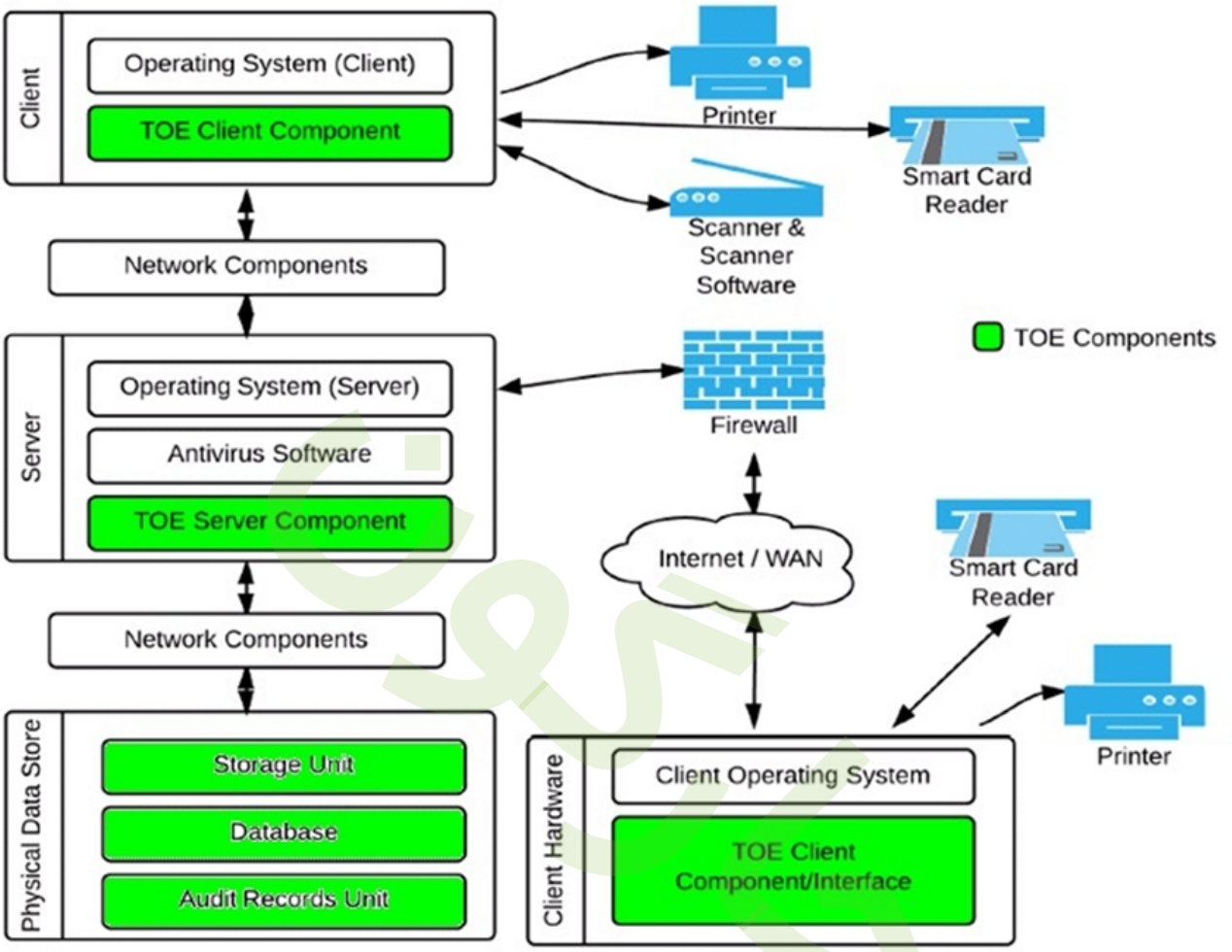
امنیت محصول (Product Security)

معماری امنیتی نرم‌افزار

تیم زیرساخت چارگون، بیشترین زمان خود را بر روی توسعه امکانات جدید متناسب دیدگاه با آخرین استانداردهای به‌روز امنیتی در سطح کشور، صرف کرده و Kernel اصلی دیدگاه زاگرس دارای مجوزهای امنیتی است.

در حال حاضر استانداردهای امنیتی کشوراز سخت‌گیرانه‌ترین Protection Profileهای مورد استفاده در دنیا، مانند ISO 15408 و Common Credit Aria است و تنها نهادی که در دنیا از این پروتکل‌ها استفاده می‌کند، پنتاگون در آمریکاست. در ایران هم تمامی سازمان‌هایی که موضوع امنیتشان از سطحی بالا برخوردار است، ملزم به استفاده و تبعیت از این Protection Profileها هستند.



امنیت توسعه نرم‌افزار (Secure SDLC)

چرخه توسعه نرم‌افزار در چارگون شامل کنترل‌های امنیتی مشخص است؛ از جمله بازبینی کد، کنترل وابستگی‌ها، مدیریت نسخه و آزمون‌های امنیتی پیش از انتشار. حداکثر تلاش‌ها می‌شود تا آسیب‌پذیری‌ها در همان مراحل اولیه توسعه شناسایی و اصلاح شوند تا هزینه اصلاح در محیط عملیاتی کاهش یابد.

امکانات و قابلیت‌های امنیتی محصول (Security Capabilities)

فهرست امکانات و قابلیت‌ها

- هویت‌سنجی پیشرفته
- احراز هویت چندعامله (Two Factor Authentication)
- احراز هویت با استفاده از توکن سخت‌افزاری
- احراز هویت با استفاده از رمز یک‌بارمصرف (SMS)
- احراز هویت بر اساس Active Directory
- الزام ورود صحیح Captcha در زمان ورود به سیستم
- هماهنگی با مکانیزم‌های SSO
- پشتیبانی کامل از پروتکل Oauth
- پشتیبانی کامل از پروتکل CAS
- ایجاد محدودیت در ورود کاربران به سیستم
- امکان محدودسازی براساس IP Address
- حراست از اطلاعات هویت‌سنجی
- جلوگیری از ذخیره‌سازی اطلاعات تصدیق هویت کاربر بر روی مرورگر
- رمزنگاری رمزهای عبور در بانک اطلاعاتی
- رمزنگاری رمزهای عبور در انتقال اطلاعات در شبکه
- عدم دسترسی به اطلاعات هویت‌سنجی رمز شده در سیستم
- مدیریت تلاش‌های ناموفق

- توقف فعالیت کاربر (User Lock) پس از چند تلاش ناموفق در ورود به سیستم
- تنظیم تعداد تلاش ناموفق برای توقف ورود کاربر به سیستم
- عدم نمایش جزئیات کاربر (نام کاربری و سایر جزئیات) در تلاش‌های ناموفق ورود به سیستم
- رویدادنگاری تلاش‌های ناموفق ورود به سیستم و امکان گزارش‌گیری از آن
- تنظیم سیاست‌های رمزعبور
- تنظیم الزام تغییر رمز عبور اولیه بعد از اولین ورود کاربر به سیستم
- تنظیم سیاست‌های الزام‌آور جهت تعیین رمز عبور پیچیده
- عدم پذیرش رمز عبور خالی
- حفاظت از اطلاعات و کنترل دسترسی (User Data Protection)
- در ادامه لیستی از اهداف امنیتی مرتبط با User data protection که پیاده‌سازی شده ذکر می‌شود:
  - رمزنگاری اطلاعات حساس
  - رمزنگاری تمام اطلاعات حساس هنگام ذخیره‌سازی
  - مکانیزم انکارناپذیری
  - بهره‌گیری از مکانیزم‌های امضای دیجیتالی برای جلوگیری از انکار
  - استفاده از فناوری‌های هویت‌سنجی قوی‌تر از نام و گذرواژه برای اعمال حساس (هویت‌سنجی دو عاملی – پشتیبانی از ورود با توکن سخت‌افزاری)
  - عدم دسترسی به منابع با دور زدن واسط کاربر
  - مستند بودن تمام واسطهای دسترسی به برنامه (مانند اینترنت، شبکه محلی) و

عدم دسترسی به هر گونه منبع برنامه غیر از مسیر واسطها

- اعتبارسنجی فعالیت‌های برنامه
- عدم وجود منابعی (مانند فایل) خارج از برنامه که بتوان آن‌ها را تغییر داده و یا ایجاد کرد
- عدم پذیرش ورود مستقیم URL جهت دسترسی به منابع غیرمجاز
- عدم نمایش فهرست پوشه‌ها با ورود یک آدرس URL نامعتبر
- عدم استفاده از کاربری‌های تعریف‌شده در پایگاه داده به‌عنوان راهکار مکانیزم کنترل دسترسی
- امکان تفکیک وظایف و حداقل مجوزها
- امکان تعیین نقش‌های کاربران و مدیران بر اساس دو اصل تفکیک وظایف و حداقل مجوزها
- امکان انقضای دسترسی حساب‌ها توسط مدیر سیستم
- اجرای برنامه در حداقل سطح اعتباری
- رویدادنگاری و ممیزی اطلاعات (Event Log / Audit Log)
- در ادامه لیستی از اهداف امنیتی مرتبط با رویدادنگاری و ممیزی اطلاعات پیاده‌سازی‌شده، ذکر می‌شود:
  - تولید رکورد ممیزی رویداد برای فعالیت‌ها و توابع نرم‌افزار
  - تمام کاربردهای سازوکار احراز هویت
  - نتایج نهایی عملیات احراز هویت
  - تغییرات بر روی مقادیر مشخصه‌های امنیتی

- ایجاد و تغییر در مشخصات تنظیماتی نرم‌افزار
- شروع و پایان توابع اصلی نرم‌افزار
- خواندن، درج و ویرایش اطلاعات
- پایان دادن یا شکست در ایجاد نشست کاربری
- تولید رویدادهای ممیزی با مشخصات دقیق
- تاریخ و زمان رویداد
- هویت ایجادکننده رویداد
- نوع و نتیجه رویداد
- آدرس شناسه شبکه (IP) ایجادکننده رویداد
- حفاظت از رویدادها و رکوردهای ممیزی اطلاعات
- قابلیت تعیین مجوزهای دسترسی جهت مشاهده رویدادها و رکوردهای ممیزی اطلاعات
- قابلیت فهم و بهره‌برداری سریع و آسان از رویدادها
- مرتب‌سازی و دسترسی‌پذیری رکوردهای اطلاعاتی برحسب نوع، تاریخ و هویت ایجادکننده
- امکان تعریف آستانه ایجاد رکوردهای اطلاعات و مکانیزم اطلاع به راهبر
- امکان جداسازی محل ذخیره‌سازی رویدادها جهت کنترل حجم و نگهداری سوابق
- پشتیبانی کامل از استاندارد syslog و ارسال تمامی logهای مورد انتظار owasp به log systemهای خارج external که از این استاندارد تبعیت

کنند.

- مکانیزم خدشه‌ناپذیری تشخیص حذف یا تغییر در رویدادها

- مدیریت خطاها و استثناها (Exception Handling)
- لیستی از اهداف امنیتی مرتبط با مدیریت خطاها و استثناهایی که پیاده‌سازی‌شده، ذکر می‌شود:
  - مدیریت مناسب خطاها و استثناها
  - تعبیه زیرسیستم متمرکز در برابر خطا و استثناء
  - عدم وجود اطلاعات قابل سوءاستفاده در مورد پایگاه داده، شبکه یا برنامه کاربردی در پیغام خطا
  - رویدادنگاری صحیح و کامل خطاها
  - وضعیت امن پس از وقوع خطا
  - عدم اجازه دسترسی‌های غیرمعمول در شرایط پس از خطا در سیستم
  - وجود روال‌های پیش‌بینی‌شده پس از شکست یا خطا در هر بخش از سیستم
- مقاومت در برابر حملات و نفوذها (Security Function Protect)
- مقاوم‌سازی در برابر آسیب‌پذیری (Broken Authenticating)
- با استفاده از راهکارهایی مانند استفاده از احراز هویت چندمنظوره، مدیریت صحیح آغاز و پایان sessionها، استفاده از کوکی‌های امن، عدم درج اطلاعات حساس در کد منبع و... از امکان جعل و سوءاستفاده از هویت کاربران جلوگیری می‌شود.
- مقاوم‌سازی در برابر آسیب‌پذیری (Injection)

- با استفاده از راهکارهای استاندارد از قبیل کدگذاری، فیلتر کردن برچسب‌های HTML و... از به وجود آمدن آسیب‌پذیری XSS جلوگیری می‌شود. همچنین با استفاده از راهکارهایی از قبیل فیلتر کردن کاراکترهای خاص، استفاده از APIهای امن و پرس‌وجوهای پارامتریک و... از به وجود آمدن آسیب‌پذیری تزریق کد SQL جلوگیری می‌شود.
- مقاوم‌سازی در برابر استفاده از مؤلفه‌هایی با آسیب‌پذیری‌های شناخته‌شده (Vulnerable and Outdated Components)
- جهت جلوگیری از سوءاستفاده از حفره‌های امنیتی مؤلفه‌ها یا کامپوننت دارای‌های آسیب‌پذیری، با استفاده از کامپونت‌های دارای لیسانس و همچنین به‌روز نگهداری چارچوب‌های برنامه‌نویسی و کتابخانه‌ها تا حد امکان از سوءاستفاده از این نوع آسیب‌پذیری‌ها جلوگیری می‌شود.
- مقاوم‌سازی برابر آسیب‌پذیری شنود و سرقت اطلاعات (Cryptographic Failures)
- با استفاده از الگوریتم‌های رمزنگاری قوی برای اطلاعات حساس و همچنین پیکربندی آخرین نسخ TLS از امکان شنود و سرقت اطلاعات در حین جابه‌جایی جلوگیری می‌شود.
- مقاوم‌سازی در برابر تنظیمات امنیتی نادرست (Security misconfigurations)
- جهت جلوگیری از سوءاستفاده از پیکربندی‌های نادرست امنیتی، اقداماتی از جمله عدم استفاده از کلمات عبور ضعیف و گذرواژه پیش‌فرض، عدم استفاده از اسکریپت‌های پیش‌فرض ذخیره‌شده در سرورها، عدم پیکربندی نرم‌افزار در

دایرکتوری‌های پیش‌فرض، خاموش کردن پیام‌های پیش‌فرض خطا و... مورد استفاده قرار خواهد گرفت.

- مقاوم‌سازی در برابر آسیب‌پذیری (Broken Access control)
- با استفاده از راهکارهایی مانند استفاده از Authorization Token مدیریت صحیح Log in و Log out از امکان دورزدن فرایند احراز هویت و سوءاستفاده از نقش‌ها و دسترسی‌های بالاتر توسط کاربر فاقد صلاحیت دسترسی جلوگیری می‌شود.
- مقاومت در برابر خرابی و تسهیل در نگهداری از نرم‌افزار (Resistance to Failure)
- قابلیت پیاده‌سازی در دسترس‌پذیری (High Availability) در سطح سرورهای بانک اطلاعاتی و سرورهای وب جهت انتقال سرویس به وضعیت امن و تداوم سرویس
- قابلیت پشتیبان‌گیری به‌ویژه از داده‌های حساس و بازاریابی نسخه‌های پشتیبان از طریق نرم‌افزار SQL Server
- مستند بودن روش تهیه نسخه‌های پشتیبان و مانور بازیابی اطلاعات
- وجود طرح خروج از بحران
- کنترل تغییرات و نسخه نرم‌افزار
- امکان به‌روزرسانی خودکار
- رمزنگاری اطلاعات دوطرفه
- پنهان‌نگاری

- نمایش Watermark
- پشتیبانی از فایل‌های PDF
- امکان پیاده‌سازی نرم‌افزار دیدبان و پشتیبانی پیشگیرانه
- امکان استفاده از قابلیت HTTPS و امن‌ترین پروتکل TLS
- حذف Cipher Suiteهای خطرناک بر روی سیستم‌عامل سرورهای وب و بانک اطلاعاتی
- حذف verbهای غیرضروری
- امن‌سازی کوکی‌ها
- اعمال موارد امنیتی در Headerها
- اعمال موارد امنیتی در View State Encryption
- غیرفعال بودن ASP.Net Debugging
- امکان جلوگیری از حملات Brute Force
- جلوگیری از انتقال و آپلود extensionهای مخرب
- امکان Rate Limit برای استفاده از Apiها
- امکان محدود کردن به احراز هویت جهت استفاده از Apiها
- فهرست خدمات
  - نصب و راه‌اندازی با معماری امن سرورهای محصول
  - سخت‌سازی سیستم‌عامل سرورهای محصول (OS Hardening)
  - سخت‌سازی نرم‌افزار بانک اطلاعاتی محصول (Database Server Hardening)

- اعمال دستورالعمل سخت‌سازی و ارتقاء امنیت محصول (Didgah Hardening)
- راه‌اندازی HTTPS و فعال کردن پروتکل‌های TLS امن
- نصب و راه‌اندازی سرورهای محصول در بیشترین حالت پایداری (High Availability)
- نصب و راه‌اندازی سرورهای محصول در کمترین حالت از دست رفتن اطلاعات (Disaster Recovery Site)
- انجام مانور و شبیه‌سازی حالت بحران
- آزمایش بازیابی نسخ پشتیبان بانک‌های اطلاعاتی
- راه‌اندازی آرشیو فایل‌های بانک‌های اطلاعاتی حجیم
- ممیزی تخصصی و انتقال بهترین تجربیات فنی و امنیتی
- نصب و راه‌اندازی مدیریت نشست‌های پیشرفته
- نصب و راه‌اندازی احراز هویت دوعاملی
- نصب و راه‌اندازی (LogApi) انتقال رویدادها (Logs) به سامانه SIEM

امنیت احراز هویت و دسترسی

سامانه‌های چارگون از مدل کنترل دسترسی مبتنی بر نقش (RBAC) پشتیبانی می‌کنند و امکان تعریف سطوح دسترسی تفکیک‌شده برای کاربران وجود دارد. قابلیت یکپارچه‌سازی سامانه‌های احراز هویت متمرکز و یا Active Directory و اعمال سیاست‌های رمز عبور سازمانی علاوه بر مدیریت کاربران داخلی محصول فراهم است.

مدیریت نشست‌ها به‌صورت امن انجام شده و امکان اعمال محدودیت زمانی، خاتمه نشست‌های غیرمجاز و ثبت رویدادهای ورود و خروج وجود دارد.

امنیت داده

تمام تبادلات داده در بستر شبکه با استفاده از پروتکل‌های امن مانند TLS انجام می‌شود. داده‌های سازمان در پایگاه داده مستقر در زیرساخت مشتری ذخیره می‌شود و شرکت چارگون دسترسی پیش‌فرض به اطلاعات عملیاتی مشتریان ندارد. سیاست‌های پشتیبان‌گیری، نگهداری و بازیابی اطلاعات بر اساس مستندات فنی به مشتری ارائه می‌شوند.

سخت‌سازی در نصب On-Premise

با توجه به مدل استقرار On-Premise، چارگون راهنمای فنی سخت‌سازی برای IIS، SQL Server، Windows Server و مجموعه نرم‌افزاری دیدگاه و محصولات خود را ارائه می‌دهد. این راهنماها و مستندات شامل ارتقاء تنظیمات امنیتی پیشنهادی، محدودسازی پورت‌ها، تفکیک شبکه، استقرار در DMZ (در صورت نیاز) و اعمال سیاست‌های امنیتی است. اجرای این کنترل‌ها بخشی از مسئولیت مشتری در مدل مسئولیت مشترک محسوب می‌شود.