شرکت بهپردازجهان

www.behpardaz.net

رزومه دپارتمان امنیت اطلاعات

فهرست مطالب

معرفی

دپارتمان امنیت شرکت بهپرداز جهان در سال ۱۳۸۸ از به هم پیوستن کارشناسان فنی توسعه نرم افزار با گرایش های کاری امنیت و نیز کارشناسان فنی علوم رمزنگاری و امنیت اطلاعات شرکت بهپرداز جهان، در قالب یک تیم فنی صرفا امنیتی، با هدف پوشش نیازهای امنیت در خدمات نرم افزاری، خدمات سخت افزاری و خدمات معماری سازمانی شرکت، در چارت سازمانی بهپرداز، ایجاد شده و طی سالهای اخیر توسعه یافته است.

دپارتمان امنیت بهپرداز مجهز به نیروهای متخصص در حوزه امنیت اطلاعات در سطوح کارشناس ارشد و کارشناس و نیز تجهیزات سخت افزاری و نرم افزاری پیشرفته ی امنیت اطلاعات است که به صورت مستقل ، کلیه فرایندهای تحقیق، تحلیل و طراحی و پیاده سازی ماژولها و نیازمندیهای امنیتی پروژه های شرکت بهپرداز و نیز اجرای پروژه های اختصاصی صرفا امنیتی را بر عهده دارد. طراحی و پیاده سازی سامانه های امنیتی در سطح پروژه های ملی کشور، از افتخارات دپارتمان امنیت بهپرداز جهان است.

رویکرد خدمات دپارتمان امنیت

از آنجایی که مهندسی امنیت اطلاعات در سطح یک سازمان بزرگ، نیازمند یک معماری امنیت سازمانی با پوشش کامل سازمان است، فراهم نمودن خدمت "ارائه معماری امنیت سازمانی یکپارچه" در دستور کار دپارتمان امنیت بهپرداز جهان قرار گرفته و با بررسی متدولوژی های استاندارد معماری امنیت سازمانی، و تجربیات گرانبهای تحلیل و طراحی معماری های امنیت، دانش مناسب و یک معماری پایه ای در این حوزه بدست آمده است.

معماری فوق، مجموعه ای از راهکارها . سامانه های امنیتی متعامل و یکپارچه سازی شده به همراه حجم وسیعی از چارچوب ها و سیاستگذاریهای مفهومی و منطقی است که باید تماما در سازمان هدف جاری شوند تا تضمین نیل به هدف بقاء در مقابل تهدیدات متداول فضای اطلاعات و داده ها، ایجاد گردیده و چرخه حیات خدمات سازمان مربوطه دچار مخاطره نگردد.

خدمت نوع دوم این دپارتمان، خدمت "ارائه راهکارهای امنیت اطلاعات" به صورت مستقل، موردی و محصول گراست. در این نوع خدمت، نیازهای امنیتی موردی سازمان هدف، بنابه اعلام نیاز آن سازمان مورد تحلیل و طراحی و اجرا قرار می گیرد و لزوما تمامی مدلهای چهارگانه ی امنیت منطقی، امنیت مفهومی، فناوری امنیت و امنیت عملیاتی ، به صورت همزمان اجرا نمی گردند. در واقع این مدل متناسب با نیاز سازمانها بر اساس بضاعت زیرساختی و فنی امنیت کنونی، و نیز با در نظر گرفتن فازهای اجرایی کوتاه مدت و ناهمگن ارائه می شود.

خدمات و سرویسهای فنی دپارتمان امنیت

طراحی معماری امنیت سازمانی:

با استفاده از تجربیات ناشی از بررسی مدلهای معماری امنیت سازمانی استاندارد، از قبیل SABSA ، TOGAF ، DODAF ، FEA و ساختار EISA ، متد طراحی معماری امنیت سازمانی دپارتمان امنیت بهپرداز، مجموعه ی سامانه ها، طرحها و زیرساختهای امنیتی را در قالب مدل مفهومی امنیت، مدل منطقی امنیت، مدل فناوری امنیت و مدل عملیاتی امنیت متناسب با ساختار و نیازهای بومی سازمان هدف ارائه می کند. در هر یک از مدل های فوق، مولفه ها، سامانه ها، ساختارها، سرویسها و خدمات امنیت برای سازمان فوق طراحی می شود که در صورت اجرا، با تعاملات یکپارچه مولفه های موجود در آن چهار مدل، معماری امنیت سازمانی در آن سازمان جاری خواهد شد.

طراحی و پیاده سازی راهکارهای امنیت اطلاعات

طراحی ، پیاده سازی، استقرار و راه اندازی زیرساخت کلید عمومی(PKI):

امروزه زیرساخت کلید عمومی (Public Key Infrastructure) زیربنایی ترین زیرساخت لازم برای استفاده از تکنولوژیها، پروتکل ها و فریم ورک های روز امنیت اطلاعات به شمار می آید. دپارتمان امنیت بهپرداز، کلیه چرخه حیات و مولفه های یک زیرساخت کلید عمومی را طراحی و پیاده سازی کرده که در حال حاضر یکی از تجربیات PKI این دپارتمان در یکی از سامانه های حساس کشور در حال سرویس دهی است. کلیه فازهای تحلیل و طراحی و پیاده سازی مولفه های این زیر ساخت تحت عنوان سامانه های مرکز صدور گواهی (CA) ، مرکز ثبت نام(RA) ، مرکز نشر (PKD) ، سرویس استعلام برخط وضعیت گواهی (OCSP Server)، سامانه مدیریت کلید مرکزی، طرح های معماری امنیت فیزیکی، سیاست نامه ها و دستورالمل های اجرایی به صورت بومی و مستقل از محصولات جانبی در دپارتمان امنیت بهپرداز جهان اجرا گردیده است.

تجهیز سامانه ها به کاربردهای PKI:

کلیه سامانه هایی که نیاز به اجرای فرایندهای امن سازی و کنترل های تضمین اطلاعات هستند، باید از قابلیت ها و کاربردهای PKI بهره مند شوند یا به اصطلاح PK Enabled گردند. طراحی و پیاده سازی مولفه ها و ابزارهای امنیتی که از محصولات PKI استفاده کرده و سرویسهای امنیتی سازمان ها را بوجود می آورند از خدمات فنی ویژه دپارتمان امنیت بهپرداز می باشند.

تضمین اطلاعات:

تضمین اطلاعات مفهوم پایه ای است که شاخه های گوناگون امنیت اطلاعات زیرمجموعه ای از آن هستند. تحلیل و طراحی و پیاده سازی مولفه ها و سیستم های حصول تضمین اطلاعات اصلی ترین گرایش و رویکرد فنی دپارتمان امنیت بهپرداز جهان می باشد. این دپارتمان ارائه کننده انواع مولفه های متضمن خصیصه تضمین اطلاعات بوده و آماده ی سرویس دهی در تمامی مباحث حوزه تضمین اطلاعات در سطح بالایی از کیفیت و استحکام می باشد.

ماژول های رمزنگاری:

طراحی و پیاده سازی ماژول های رمز، API، SDK، سرویس ها و نرم افزارهای رمزنگاری با پوشش کلیه الگوریتمهای رمزنگاری متقارن و نامتقارن به عنوان Crypto Engine پایه ای ترین تکنولوژی مورد نیاز درتمامی روشها، پروتکل ها و راهکارهای تضمین اطلاعات هستند که در زمره تجربیات موفق و فنی واحد امنیت بهپرداز قرار دارند. پشتیبانی ازالگوریتمهای استاندارد، غیر استاندارد و ترکیبی، متناسب با پارامترهای فنی و امنیتی گوناگون در دو مدل پیاده سازی نرم افزاری و نیز پیاده سازی سخت افزاری به صورت Embed در سخت افزارهای رمزنگاری پیشرفته ، نظیر HSM و TOKEN ارائه می شود. در این راهکار، کلیه مراحل چرخه حیات برنامه نویسی، Initialization و استقرار سخت افزارهای فوق، تحت انواع مدل استقرار مرکزی توزیع شده واختصاصی WorkStation قابل ارائه است.

توانایی تحلیل، طراحی، برنامه نویسی، شخصی سازی، مکان یابی ، استقرار و یکپارچه سازی سخت افزارهای امن به عنوان پردازشگرهای اصلی سامانه های امنیتی از ویژگی های برجسته این دپارتمان است که با بهره گیری از تجارب گوناگون تجهیز سامانه های ملی به سخت افزارهای امنیتی، دانش و تجربه بومی و مطمئن را به ارمغان آورده است. طراحی، ساخت و توسعه سرورهای Appliance که انواع پروتکل امنیتی را در درون خود نگهداری و سرویس دهی می کنند، طراحی و پیاده سازی نرم افزارهای شخصی سازی توکن های رمزنگاری و احراز هویت، طراحی و پیاده سازی نرم افزارهای شخصی سازی کارت های هوشمند گوناگون، طراحی و پیاده سازی و استقرار PCI کارت های HSM در معماری سامانه های Enterprise و ملی، طراحی و پیاده سازی و استقرار سرورهای HSM در معماری سامانه های امنیتی سازمانی، نظامی، بانکی ، طراحی و پیاده سازی ماژولهای احراز هویت وشناسایی سخت افزاری، همگی خدمات سخت افزار امن این دپارتمان هستند.

شناسایی و احراز هویت:

طراحی و پیاده سازی راهکارهای هویت شناسی، کنترل دسترسی وممیزی هویتی در قالب انواع روشهای سخت افزاری و نرم افزاری در سطح نرم افزارهای وب، رومیزی و سرویسها با معماری سرویس دهنده/مشتری (Client/Server) تحت فریم ورک های گوناگون صورت گرفته و قابل ارائه است. طراحی و اجرای سامانه های مجهز به انواع تکنولوژی در این حوزه، از قبیل گواهی های دیجیتال، توکن، کارت هوشمند تماسی و غیر تماسی، زیست سنج ها(بیومتریک)، گذرواژه های مدت دار و یکبار مصرف (OTP) ، انواع دایرکتوری LDAP/AD ، پروتکل های AAA، SSL/TLS ، سامانه SSO، RBAC، MAC ، امضای دیجیتال و احراز هویت چند عاملی از تجربیات موفق دپارتمان امنیت بهپرداز می باشد.

امنیت نرم افزار:

طراحی و پیاده سازی انواع راهکار محافظت و امن سازی نرم افزار، در قالب تکنولوژیها و روشهای سخت و نرم افزاری برای انواع نرم افزار تحت وب، رومیزی، Standalone و Client/Server از تواناییهای دیگر دپارتمان امنیت بهپرداز جهان به حساب می آیند. روش های محافظت نرم افزار با هدف محافظت از کد و منابع نرم افزار و نیز کنترل توزیع نسخ آن با حفظ منافع تولید کننده ی آن و جلوگیری از سوء استفاده و کاربری غیر مجاز به صورت ارائه تکنولوژیهایی از قبیل تست های نفوذ امنیتی، قفل های سخت و نرم افزاری، License، Activation Code، امن سازی سورس، توزیع نسخ منحصربفرد و مولدهای HW Unique ID در انواع سامانه های حساس طراحی و اجرا گردیده که تجارب فنی فوق قابل ارائه در دپارتمان امنیت بهپرداز قابل ارائه می باشند.

تبادلات امن:

در فضای داده ها و اطلاعات، انتقال و تبادل متعامل داده های حساس و غیر حساس نیازمند مجهز بودن به ملاحظات امنیتی هستند تا اعتماد پذیری و قابلیت اتکاء بدون وجود مخاطره و ریسک برای طرفین تبادل وجود داشه باشد. از اینرو دپارتمان امنیت بهپرداز مجموعه ای از پروتکل ها و زیر ساختهای لازم برای برقراری تبادل امن را طراحی و پیاده سازی کرده است که کلیه نیازهای یک دامنه تبادل امن با تعداد نامحدود شرکا را پشتیبانی می کند. راهکارهای فنی پوشش دهنده فضای اعتماد و اتکاپذیر فوق در قالب طراحی و پیاده سازی دامنه های معتمد شرکا، امنیت نقطه به نقطه، تبادلات امن برخط و برون خط، تبادل کلید، توافق کلید، تجهیز به کاربردهای کلید عمومی، نقطه اعتماد سوم، انتشار و توزیع امن و اشتراک امن ارائه می گردند.

امنیت بانکهای اطلاعاتی:

طراحی و پیاده سازی انواع راهکار امن سازی بانک اطلاعاتی با روشهای Embed در بانک و روش های بیرونی از قبیل رمزنگاری و نیز اتصال بانکها با سرورهای سخت افزاری امن مدیریت کلید از دیگر تواناییهای فنی دپارتمان امنیت بهپرداز می باشند. اجرای چک لیست های استاندارد امنیت دیتابیس در سطح Engine و نیز سطح داده و Initialize کردن Wallet ها، VPD ها و تنظیمات امنیتی دیگر از تجربیات موجود در این دپارتمان است.

استاندارد و سیاست نامه:

تدوین استاندارد های امنیتی و سیاست نامه های امنیت، پایه ترین و اساسی ترین محور در تقید و راهبری سامانه های امنیت و مفید واقع شدن خدمات آنها است که تدوین چنین اسنادی متناسب با مختصات بومی سازمانها در زمره خدمات امنیتی دپارتمان امنیت بهپرداز می باشد. تدوین اسناد بومی در کنار جاری سازی استاندارد های نسل 27000 و ISMS برای صورت مسئله های خاص سازمان ها از تجربیات این دپارتمان است.

ابزارهای ActivX/Aplet/Browser Plugin:

طراحی و پیاده سازی انواع ماژولهای امنیت وب در قالب تکنولوژیهای ActivX ، Aplet و Plugin برای مرورگرهای وب، تحت جاوا و C/C++ از تجربیات فنی و استراتژیک در دپارتمان امنیت بهپرداز می باشد. کاربردهای امضای دیجیتال فرم ها و صفحات وب و نیز رمزنگاری داده ها در وب از کاربردهای این تکنولوژی ها است.

امنیت سرویس:

طراحی و پیاده سازی انواع ماژولهای امنیت سرویس از قبیل ثبت نام، احراز هویت سرویس و صدا زننده سرویس، کنترل فراخوانی، امنیت داده ها و پارامترهای آنها، در معماری های سرویس گرا با پیاده سازی کلیه استاندارد های موجود و قابلیت تجهیز به سخت افزارهای امنیتی مدیریت کلید از تجربیات دیگر این دپارتمان می باشد.

امنیت اسناد الکترونیک:

پیاده سازی استانداردهای امنیت اسناد الکترونیک با پوشش انواع قالب سند به صورت سامانه های مولد شناسه امن، امضا و رمزنگار سند ونیز ارزیاب و بررسی کننده سمت سرور سند کلیه روشهای امنیت سند با خواص محرمانگی، دستنخوردگی، احراز هویت و عدم انکار فراهم آورده و مختصات یک سند امن را ایجاد می کند. این خدمات در قالب نرم افزار، API و سرویس قابل ارائه می باشند.

پروتکل امنیت:

طراحی و پیاده سازی پروتکل های استاندارد و بومی امنیت، متناسب با سناریوهای گوناگون استاندارد و بومی سازمان، در جهت امن سازی یک فرایند از خدمات فنی و حساس دپارتمان امنیت بهپرداز در سطوح پروژهای ملی در سطح سازمانها بوده است. با طراحی و اجرای پروتکل های ترکیبی امنیت، سناریوهای مجرد و نامتداول در سامانه های مختلف مجهز به خصیصه های امنیتی می گردند.

پلتفرم ها و ابزارهای توسعه و تولید:

پیاده سازی سامانه ها و سرویس های ارائه شده در این دپارتمان تحت پلتفرم ها و ابزارهای برنامه نویسی و واسط های توسعه ی زیر صورت می گیرد.

C/C++

VC++/MFC

C#

Java (J2ME/J2SE/J2EE)

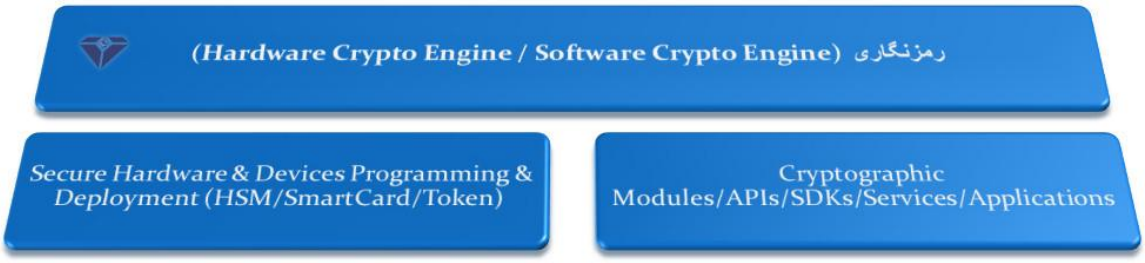
JS

PCSC/Serial Com, MsCAPI, PKCS#N(All)

Oracle -PL/SQL

Windows /Linux


تواناییها، تجربیات و فناوری های قابل ارائه در دپارتمان امنیت بهپرداز
C/C++, VC++/MFC, C#, Java (J2ME/J2SE/J2EE), JS, PCSC/Serial Com, MsCAPI, PKCS#N(All), Oracle/PL/SQL, Windows/Linux
زیرساخت کلید عمومی (PKI)
CA/RA/PKD(Ldap/AD)/OCSP Server/TS Server/KM
تجهیز سامانه ها به کاربردهای زیرساخت کلید عمومی و گواهی (PKE)
تضمین اطلاعات (IA)
امنیت اسناد الکترونیک
تبادل امن
امنیت وب سرویس
امنیت نرم افزار
شناسایی و احراز هویت
امنیت بانک اطلاعاتی
طراحی پروتکل امن
استاندارد و سیاست نامه
ActiveX / Applet / Browser Plugin
E-Docs Support
محرمانگی
تمامیت
عدم انکار
احراز هویت و شناسایی
ماژولهای سخت افزاری
ماژول های نرم افزاری
Partners Trusted Domain
Peer To Peer Security
Secure Channel
OnLine/OffLine Exchange
Key Agreement
Key Exchange
PKE Trusty Exchange
PKI TTP Trust Anchor
Secure Publication & Distribution
Secret Sharing
Full WS Sec
امنیت برنامه وب
امنیت برنامه رومیزی
تست ضعف امنیتی
قفل سخت افزاری
قفل نرم افزاری
License
Activation Code
امنیت سورس
توزیع منحصربفرد نسخ
HW Unique ID
SSO
SSL/TLS
Digital Certs
Tokens
OTPs
SmartCards
بیومتریک ها
Ldap/AD
Authentication
Digital Signatures
RBAC/MAC
احراز هویت چند عاملی
AAA
روش های نرم افزاری امنیت بانک اطلاعات
روش های سخت افزاری امنیت بانک اطلاعات
پروتکل های استاندارد امنیت
پروتکل های بومی امنیت
پروتکل های ترکیبی امنیت
پروتکل های مبتنی بر رمزنگاری
استانداردها
سیاست نامه امنیت
دستور العمل اجرایی امنیت
امضای تحت وب
رمزنگاری MAC
Generator
احراز هویت


رمزنگاری (Hardware Crypto Engine / Software Crypto Engine)
Secure Hardware & Devices Programming & Deployment (HSM/SmartCard/Token)
Cryptographic Modules/APIs/SDKs/Services/Applications

❖ تماس با ما:

تلفکس: ۴۴۴۸۷۱۰۰ – ۴۴۴۸۷۰۹۷ – ۴۴۴۸۷۰۹۸

پست الکترونیک: info@behpardaz.net

نشانی: تهران، خیابان اشرفی اصفهانی، جنب مرکز خرید تیراژه، کوچه شهید زمانی، شماره ۴۵

مدیر دپارتمان: مهندس مهدی شعبانی

security@behpardaz.net

www.behpardaz.net