سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

شرکت فناوری اطلاعات و ارتباطات رضوی

اتوماسیون اداری روان

نسخه ۱,۸

۱. فهرست

۲- الزامات امنیتی ۵
۲-۱- ممیزی امنیت ((Log ۵
۲-۲- رمزنگاری ۹
۲-۳- شناسایی و احراز هویت ۱۱
۲-٤- حفاظت از داده‌ی کاربری ۱۵
۲-۵- مدیریت امنیت ۱۹
۲-٦- حفاظت از توابع امنیتی محصول ۲۳
۲-۷- تخصیص منابع ۲۵
۲-۸- دسترسی به محصول ۲٦
۲-۹- کانال‌ها/مسیرهای مورد اعتماد ۲۸
۳- الزامات امنیتی مبتنی بر انتخاب ۳۹

الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه ۱,۱ نمایه[۱] حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر رده در نمایه‌ی حفاظتی مربوطه، یک دسته الزام بیان شده است.

۱- ممیزی امنیت (Log)

در این رده توانایی‌های محصول از نظر امکان تولید داده ممیزی (Log) مناسب برای فعالیت‌های مختلفی که در محصول صورت می‌گیرد، در شرایط مختلف سنجیده می‌شود.

شماره الزام	رده ممیزی امنیت (**Log**)			
۱	محصول باید برای موارد مشخص‌شده که در زیر آمده است، ثبت‌نشان[۲] تولید کند (**Log** ثبت نماید).			■
	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	شروع و اتمام توابع	■	
		تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها	■	
		خواندن اطلاعات از ثبت‌نشان‌ها	■	
		تمامی تغییرات در پیکربندی ثبت‌نشان‌ها	■	
		عملیات انجام‌شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه	■	
		عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها	■	
		تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	■	
		تمام کاربردهای سازوکار احراز هویت	■	
		نتایج نهایی عملیات احراز هویت	■	
		تلاش موفق و ناموفق هر گذرواژه بررسی‌شده توسط محصول	■	
		شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	■	
		تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی	■	
		تمامی درخواست‌ها (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	■	
		تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی)	■	
		همه تلاش‌ها برای خارج کردن اطلاعات از محصول	■	
		تمامی تغییرات در رفتارهای توابع کارکردی محصول	■	

[۱] Profile

[۲] Log

		استفاده از کارکردهای مدیریتی	■	
		تغییرات در گروه کاربران	■	
		شکست در کارکردهای امنیتی محصول	■	
		تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.	■	
		تلاش موفق یا ناموفق برای برقراری نشست.	■	
		ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)	■	
		خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	■	
		خاتمه به نشست غیرفعال توسط مدیر سیستم	■	
۲	محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.			■
	ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.	تاریخ و زمان رویداد	■	
		نوع رویداد	■	
		هویت ایجادکننده رویداد	■	
		نتیجه رویداد	■	
		آدرس IP ایجادکننده رویداد	■	
۳	محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.			■
۴	ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.			■
۵	محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.			■
۶	محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.			■
۷	محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.			■
۸	محصول باید توانایی تولید ثبت‌نشان (ثبت **Log**) هنگام از کار افتادن محصول و/یا پر شدن حافظه ثبت‌نشان‌ها را داشته باشد			■

۲- رمزنگاری

در این رده، توانایی محصول در پیاده‌سازی یا به‌کارگیری واحدهای[۳] رمزنگاری، بررسی می‌گردد. برای حفظ محرمانگی داده، از رمزنگاری استفاده می‌شود و این رمزنگاری‌ها می‌توانند به صورت متقارن و نامتقارن صورت گیرد.

شماره الزام	رده رمزنگاری	
۱	محصول باید قابلیت رمزنگاری یا واحد رمزنگاری بر اساس استانداردهای لازم را داشته باشد	■
۲	محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (**Hash**) را داشته باشد	■
۳	در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)	■
۴	در صورتی که امضای دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضای رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)	■

[۳] Modules

۳- شناسایی و احراز هویت

در این رده توانایی‌های محصول از نظر امکان شناسایی و احراز هویت کاربر در حالت‌های مختلف و اقدامات متقابل در راستای عدم برقراری آنها، بررسی می‌گردد.

شماره الزام	رده شناسایی و احراز هویت			
۱	محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.			■
۲	محصول باید هنگامی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین‌شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.			■
	روش استفاده شده برای پیچیده‌تر کردن احراز هویت	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	■	
		استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود)	■	
۳	محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید.			■
	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	شناسه کاربر	■	
		روش احراز هویت مورد استفاده	■	
		داده احراز هویت	■	
		وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	■	
		نقش کاربر	■	
۴	محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.			■
	موارد نیاز که باید در تعریف گذرواژه استفاده شوند.	استفاده از حروف کوچک	■	
		استفاده از حروف بزرگ	■	
		استفاده از اعداد	■	
		استفاده از کاراکترهای خاص («@»، «#»، «$»، «٪»، «^»، «!»، «&»، «*»، «(» , «)» و ...)	■	
		حداقل طول ۸ یا بیشتر (قابل تنظیم)	■	

۵	محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.			■
	اقدامات عمومی که کاربر می‌تواند قبل از احراز هویت انجام دهد، انتخاب شود.	مشاهده راهنمای نحوه ورود به سیستم	■	
		بازیابی گذرواژه	■	
۶	محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد).			■
	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	نام کاربری و گذرواژه	■	
		سامانه‌های احراز هویت مرکزی (مانند Active Directory و ...)	■	
		OTP یا توکن	■	
		احراز هویت دو فاکتوری	■	
۷	محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید.			■
۸	محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.			■
۹	محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.			■

۴- حفاظت از داده‌ی کاربری

داده کاربری در واقع هر نوع داده‌ای است که کاربر تولید می‌کند یا مالک آن است. در این رده، توانایی محصول در حفاظت از این داده‌ها مورد بررسی قرار می‌گیرد.

شماره الزام	رده حفاظت از داده‌ی کاربری	
۱	محصول باید برای موجودیت‌ها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.	■
۲	محصول باید بر اساس ویژگی‌های مشخص، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.	■
۳	محصول باید بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نماید	■
۴	محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.	■
۵	محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام تخصیص و یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.	■
۶	محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.	■
۷	محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفافی را بین داده کاربری دریافت‌شده و ویژگی‌های امنیتی آن فراهم و همچنین از شنود و گم‌شدن داده حین انتقال جلوگیری می‌کند.	■
۸	محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.	■
۹	محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.	■
۱۰	محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.	■

۱۱	محصول باید در صورت تشخیص خطای صحت در داده‌ها، ایجاد هشدار/اخطار برای نقش‌های مجاز را انجام دهد.	■

۵- مدیریت امنیت

در این رده توانایی‌های محصول در مدیریت (حذف، تغییر، فعال کردن و ...) کارکردهای امنیتی (جمع‌آوری داده‌های سیستم، پیکربندی‌ها و ...) مورد بررسی قرار می‌گیرد. همچنین توانایی محصول در مدیریت نقش‌ها و دسترسی آنها برای اعمال مدیریت بر روی کارکردهای امنیتی سنجیده می‌شود.

شماره الزام	رده مدیریت امنیت			
۱	محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیت‌های مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.			■
۲	محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام ۷ از رده (**Class**) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.			■
	عملیات بر روی ویژگی‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.	پرس‌وجو	■	
		تغییر	■	
		حذف	■	
		تغییر پیش‌فرض	■	
۳	محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.			■
	عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.	تغییر پیش‌فرض	■	
		حذف نمودن	■	
		پرس‌وجو	■	
		مقداردهی	■	
		ایجاد	■	
		مشاهده	■	
۴	محصول باید توانایی انجام کارکردهای زیر را داشته باشد.			■
		پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشان‌ها	■	
		پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها	■	
		پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشان‌ها	■	
		مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول	■	
		ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول	■	

		در نظر گرفتن یک عملیات از پیش تعیین‌شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد.	■	
		۱. مدیریت حد آستانه برای تلاش‌های ناموفق ۲. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.	■	
		مدیریت معیارها برای تنظیم گذرواژه‌ها	■	
		۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه ۲. مدیریت یک‌سری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند.	■	
		۱. مدیریت سازوکارهای احراز هویت ۲. مدیریت قوانین مرتبط با احراز هویت	■	
		مدیریت تغییرات و فرآیندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.	■	
		مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	■	
		مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول	■	
		مدیریت نقش‌ها در محصول	■	
		مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر	■	
		مدیریت شرایط آغاز نشست توسط مدیر مجاز	■	
		۱. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد. ۲. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.	■	
۵	محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.			■
	نقش‌هایی که در محصول پشتیبانی می‌شوند، مشخص گردد.	مدیر سیستم	■	
		کاربر پیشرفته	■	
		کاربر عادی	■	
۶	محصول باید قادر باشد کاربران را به نقش‌های تعریف‌شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.			■

۶- حفاظت از توابع امنیتی محصول

در این رده، توانایی محصول در حفظ وضعیت امن در زمان رخ دادن شکست و همچنین حفاظت از داده‌ها هنگام تبادل بین اجزای محصول یا تبادل با موجودیت‌های دیگر، مورد بررسی قرار گرفته است.

شماره الزام	رده حفاظت از توابع امنیتی محصول	
۱	محصول باید هنگام رخ دادن هرگونه خرابی، اشکال یا شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته، صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید.	■
۲	محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی جلوگیری از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.	■
۳	در صورتی که محصول از محصولات امن **IT** استفاده می‌کند، باید تفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک‌گذاری آن بین خود و دیگر محصولات امن **IT**، فراهم آورد.	■
۴	محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی[۴] معتبر را تولید یا از آن‌ها استفاده نماید.	■
۵	محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.	■

۷- تخصیص منابع

در این رده، به بررسی وضعیت عملکردهای محصول و منابع مورد استفاده توسط آن در زمانهای مختلف از جمله زمان شکست پرداخته می‌شود.

شماره الزام	رده تخصیص منابع	
۱	محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	■

[۴] Time stamp

۸- دسترسی به محصول

در این رده توانایی محصول در مدیریت نشست‌های صورت گرفته شده توسط کاربر، ارزیابی می‌شود.

شماره الزام	رده دسترسی به محصول	
۱	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.	■
۲	محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.	■
۳	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.	■
۴	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست باشد.	■
۵	در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.	■
۶	محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.	■
۷	محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.	■

۹- کانال‌ها/مسیرهای مورد اعتماد

در این رده به بررسی پروتکل‌های امنی که برای برقراری کانال/مسیر مورد اعتماد، بین محصول و موجودیت‌های IT خارجی، یا بین اجزای محصول، استفاده می‌شوند، پرداخته می‌شود.

شماره الزام	رده کانال‌ها/مسیرهای مورد اعتماد			
۱	محصول باید قادر باشد مسیر ارتباطی امنی بین خود، کاربران و دیگر محصولات **IT** فراهم نماید که به طور منطقی از دیگر کانال‌ها متمایز باشد. سپس از طریق این کانال احراز هویت را انجام دهد و از تغییر و افشای داده تبادلی حفاظت نماید و تغییرات را تشخیص دهد.			■
	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	HTTPS	■	
		TLS	■	
		SSH	■	
۲	محصول باید به کاربر/دیگر محصول **IT** معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.			■
۳	محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.			■