الزامات احراز هویت چند عاملی

مرکز نظارت بر امنیت اطلاعات بازار سرمایه (مکنا)

طبقه بندی محرمانگی: عادی

ویرایش ۱,۰

مهر ۱۳۹۸

فهرست

مقدمه

اولین گام برای معرفی یک کاربر به یک سامانه، تعریف هویت کاربر در سامانه و سپس تعیین دسترسی‌های مجاز برای آن هویت می‌باشد. هر کاربر با اطلاعاتی منحصربفرد در سامانه ثبت و شناسایی می‌شود. بنابراین زمانی که کاربر بخواهد وارد سامانه شده و به اطلاعات سامانه دسترسی پیدا کند، باید ابتدا با ارائه اطلاعاتی هویت خود را اثبات کند. احراز هویت به فرایندی گفته می‌شود که طی آن درستی هویت یک کاربر تایید می‌شود.

مکانیزم‌های مختلفی برای احراز هویت کاربران وجود دارد که بطور کلی می‌توان آنها را به سه دسته زیر تقسیم کرد:

۱- مکانیزم‌های احراز هویت بر اساس چیزی که کاربر می‌داند؛ مانند رمز عبور
۲- مکانیزم‌های احراز هویت بر اساس چیزی که کاربر دارد مانند پیامک، توکن
۳- مکانیزم‌های احراز هویت بر اساس چیزی که کاربر هست؛ مانند اثر انگشت

بطور کلی هر یک از مکانیزم‌های ذکر شده دارای نواقصی می‌باشند که می‌تواند امنیت اطلاعات سامانه‌ها و کاربران آنها را به خط بیندازد. به منظور بهبود امنیت اطلاعات سامانه‌ها و کاربران آنها در مرحله احراز هویت، احراز هویت چند عاملی پیشنهاد می‌گردد. احراز هویت چند عاملی به معنی احراز هویتی است که حداقل از دو عامل در آن استفاده شود و این عوامل باید از دسته‌های متفاوت باشند تا سطح مطلوب امنیت تأمین شود.

در این مستند ابتدا عامل اول احراز هویت که استفاده از رمز عبور است معرفی شده و الزامات آن شرح داده شده است. پس از آن چند مکانیزم به همراه الزامات آنها به عنوان عامل دوم ارائه شده است که شرکت‌ها می‌توانند هر یک از این روش‌ها را به عنوان عامل دوم انتخاب و در سامانه‌های خود پیاده سازی نمایند.

۱- عامل اول – رمز عبور

ساده ترین مکانیزم احراز هویت، استفاده از نام‌کاربری و رمز عبور است. مکانیزم رمز عبور باید به عنوان عامل اول جهت احراز هویت در تمام سامانه‌ها مورد استفاده قرار گیرد.

این مکانیزم بر مبنای "چیزی که کاربر می‌داند" است. این مکانیزم از جمله ضعیف ترین مکانیزم‌های احراز هویت محسوب می‌شود زیرا از یک طرف اگر چیزی را که کاربر می‌داند، شخص دیگری بداند پس آن شخص می‌تواند به جای آن کاربر احراز هویت شود. از طرف دیگر بسیاری از کاربران در انتخاب، استفاده و نگهداری از رمز عبور خود نکات امنیتی را رعایت نمی کنند که این امر منجر به افشای رمز عبور آنها (چیزی که کاربر می‌داند) می‌شود.

حداقل الزاماتی که به منظور بهبود امنیت این مکانیزم باید در سامانه‌ها لحاظ شود به شرح زیر می‌باشد.

۱- خط‌مشی رمزهای عبور باید از نظر طول، پیچیدگی، زمان انقضا و از این قبیل به شیوه‌های امنیتی صحیح، مطابق با مراجع SANS یا NIST الزام و مستند شود.

۲- طول رمز عبور باید حداقل ۸ کاراکتر باشد.

۳- پیچیدگی رمز عبور باید حداقل شامل حروف و اعداد باشد.

۴- باید تنظیمات لازم به گونه ای اعمال گردد که کاربر به صورت سیستمی ملزم به رعایت خط مشی رمز عبور گردد.

۵- رمز عبور یا باید از ابتدا توسط خود کاربر تعریف شود و یا به صورت امن توسط یک الگوریتم تصادفی به صورت غیرتکراری و با لحاظ کردن خط مشی رمزهای عبور تولید شده و به گونه ای به کاربر تحویل داده شود که قابل مشاهده توسط هیچ فرد دیگری نباشد (به عنوان مثال با استفاده از کاغذ رمز). تعیین رمز عبور توسط اپراتور مجاز نمی باشد.

۶- در صورتی که رمز عبور توسط خود کاربر تعریف نشده باشد، کاربر باید به صورت سیستمی ملزم به تغییر رمز عبور در اولین ورود باشد.

۷- کاربران باید به صورت سیستمی ملزم به تغییر رمز عبور خود در بازه حداکثر ۹۰ روزه باشند. کاربر در هنگام تغییر رمز عبور نباید بتواند آخرین رمز عبور خود را مجدد استفاده نماید.

۸- رمزهای عبور نباید به صورت متن واضح در پایگاه‌های داده ذخیره شوند، بلکه باید حتی‌الامکان به صورت درهم‌سازی شده (رمز یکطرفه و غیر قابل بازگشت) ذخیره شوند.

۹- رمزهای عبور حتی به صورت درهم‌سازی شده نباید در لاگ‌ها ذخیره شوند.

۱۰-مکانیزم‌های جلوگیری از حملات Brute Force بر روی نام‌های کاربری و رمزهای عبور باید در سامانه پیاده سازی شود.

۱۱-جهت تغییر رمز عبور توسط کاربر، باید عامل دوم نیز از کاربر درخواست شود و در صورتی که رمز فعلی و عامل دوم هر دو صحیح باشد تغییر رمز انجام شود.

۲- عامل دوم

مکانیزم‌های متفاوتی را می‌توان به عنوان عامل دوم احراز هویت اســتفاده نمود اما عامل دوم احراز هویت باید از دســته ای متفاوت از دســته عامل اول باشــد تا بتواند ســطح امنیت فرایند احراز هویت را ارتقا دهد. هر یک از مکانیزم‌های زیر می‌تواند به عنوان عامل دوم احراز هویت در سامانه‌ها مورد استفاده قرار گیرد.

۱- استفاده از پیامک
۲- استفاده از نرم افزار Authenticator
۳- استفاده از توکن سخت‌افزاری

در ادامه توضیحات و الزامات مربوط به هر یک از این روش‌ها ارائه شده است.

لازم به ذکر است که در صورتی که راهکار دیگری علاوه بر راهکارهای مذکور مدنظر باشد، راهکار مورد نظر باید به مرکز نظارت بر امنیت اطلاعات بازار سرمایه اعلام و در صورت تایید توسط این مرکز قابل استفاده می‌باشد.

۲-۱- مکانیزم اول – استفاده از پیامک

این مکانیزم از دسته "چیزی که کاربر دارد" می باشد. در این مکانیزم، پس از وارد کردن نام کاربری و رمز عبور صحیح (عامل اول) تو سط کاربر، پیامکی حاوی یک کد به شماره موبایل ثبت شده کاربر در سامانه ار سال شده و کاربر پس از دریافت این کد باید آن را در قسمت مربوطه در سامانه وارد نماید. در صورت صحیح بودن کد وارد شده توسط کاربر، هویت کاربر تایید می‌شود. بدین ترتیب پیامک به عنوان عامل دوم احراز هویت در سامانه مورد استفاده قرار می‌گیرد.

حداقل الزاماتی که به منظور بهبود امنیت این مکانیزم باید در سامانه‌ها لحاظ شود به شرح زیر می‌باشد.

۱- کد پیامک شده باید حداقل ۵ کاراکتر باشد.
۲- کد پیامک شده به کاربر جهت ورود به سامانه باید حداکثر به مدت ۵ دقیقه معتبر باشد. در غیر اینصورت کاربر باید جهت دریافت مجدد کد اقدام نماید.

۳- در صورت ورود اشتباه کد پیامک شده بعد از سه مرتبه تکرار (در یک فرایند ۵ دقیقه‌ای) توسط کاربر، این کد باید منقضی شود و کاربر ملزم به درخواست مجدد کد گردد.

۴- شماره موبایل ثبت شده کاربر به یکی از روش‌های زیر قابل تغییر می‌باشد:

أ. تغییر شماره موبایل توسط کاربر در صورت در دسترس بودن شماره موبایل فعلی:

در زمان تغییر شماره موبایل توسط کاربر باید یک کد با رعایت الزام بند ۱ الزامات همین بخش به شماره موبایل فعلی ثبت شده کاربر ارسال گردد و در صورت صحیح بودن کد وارد شده توسط کاربر با رعایت الزامات بند ۲ و ۳ الزامات همین بخش، شماره موبایل کاربر تغییر یابد.

ب. تغییر شماره موبایل توسط کاربر در صورت در دسترس نبودن شماره موبایل فعلی و یا تغییر شماره موبایل توسط راهبر سامانه بنا به درخواست مستند کاربر باید به یکی از سه روش زیر امکان پذیر باشد:

۱) استعلام از سامانه شاهکار جهت اثبات مالکیت شماره موبایل جدید کاربر و تطابق آن با هویت کاربر

۲) استعلام شماره موبایل جدید کاربر از سامانه سجام

۳) در صورت عدم امکان اجرای دو روش قبل با استدلال موجه، شماره موبایل باید با مراجعه شخص و ثبت درخواست مستند و مثبته به کارگزاری تغییر یابد.

۴) در صورت وجود عامل سومی جهت احراز هویت (به غیر از عامل استفاده از پیامک)، این عامل از کاربر دریافت و در صورت صحیح بودن آن تغییر شماره موبایل انجام شود.

۲-۲- مکانیزم دوم - استفاده از نرم‌افزار Authenticator

این مکانیزم از دسته "چیزی که کاربر دارد" است. در این مکانیزم، یک نرم افزار Authenticator در اختیار کاربر قرار می‌گیرد. نرم افزارهای Authenticator یک مقدار اولیه[۱] به عنوان ورودی از کاربر دریافت می‌کنند و بر اساس این مقدار اولیه در بازه‌های زمانی مشخص یک کد جدید (OTP[۲]) تولید و به کاربر نمایش می‌دهند. پس از وارد کردن نام کاربری و رمز عبور صحیح (عامل اول)، مقدار OTP تولید شده توسط این نرم افزار نیز باید توسط کاربر به سامانه ارائه شود. در صورت صحیح بودن مقدار OTP، هویت کاربر تایید می‌شود.

در صورت انتخاب نرم‌افزار Authenticator به عنوان عامل دوم لازم است الزامات زیر رعایت شود:

۱- نرم افزار Authenticator باید بر اساس RFC6238[۳] پیاده سازی شده باشد.

---

[۱] Seed

[۲] OTP: One Time Password

[۳] TOTP: Time-Based One-Time Passsword Algorithm

۲- مقدار اولیه (Seed) باید به صورت تصادفی و بر اساس RFC4086[۴] تولید شود.

۳- مقدار اولیه (Seed) باید به صورت امن ذخیره گردد. پیشنهاد می‌شود بدین منظور از دستگاه‌های HSM[۵] استفاده شود.

۴- مقدار اولیه (Seed) مورد استفاده جهت نرم‌افزار Authenticator به منظور ایجاد کد صرفا می‌بایست از طریق پیامک به شماره موبایل ثبت شده کاربر ارسال گردد.

۵- کد تولید شده توسط نرم افزار Authenticator باید حداقل ۶ کاراکتر باشد.

۶- اعتبار کد تولید شده باید حداکثر ۶۰ ثانیه باشد و بعد از گذشت این زمان کد جدیدی تولید گردد.

۷- در صورت ورود اشتباه کد توسط کاربر پس از سه مرتبه تکرار (در یک فرایند۶۰ ثانیه‌ای) کد فعلی باید منقضی شده و کاربر تا زمان تولید کد جدید منتظر بماند.

۸- در صورت تغییر شماره موبایل ثبت شده کاربر، الزامات زیر باید مدنظر قرار گیرد.

أ. الزامات بند ۴ بخش ۲-۱ مکانیزم اول- استفاده از پیامک رعایت شود.

ب. به محض تغییر شماره موبایل کاربر مقدار اولیه (Seed) ثبت شده برای شماره موبایل قبلی کاربر منقضی شود و یک مقدار اولیه جدید تولید و به شماره موبایل جدید کاربر پیامک شود.

۲-۳- مکانیزم سوم- استفاده از توکن سخت‌افزاری

این مکانیزم نیز از دسته "چیزی که کاربر دارد" است. در این مکانیزم، کاربر دارای یک توکن سخت‌افزاری است. این توکن می‌تواند یکی از انواع زیر باشد:

۱) توکن OTP[۶] سخت‌افزاری

۲) توکن PKI مورد تایید مرکز دولتی صدور گواهی الکترونیکی ریشه حاوی گواهی الکترونیکی صادر شده توسط مرکز صدور گواهی الکترونیکی میانی بازار سرمایه

---

[۴] Randomness Requirements for Security

[۵] Hardware Security Module

[۶] One Time Password

در صورتی که کاربر دارای توکن OTP سخت‌افزاری باشد، پس از وارد کردن نام کاربری و رمز عبور صحیح (عامل اول)، کد تولید شده توسط این توکن نیز باید توسط کاربر به سامانه ارائه شود. در صورت صحیح بودن کد وارد شده توسط کاربر، هویت کاربر تایید می‌شود.

در صورت انتخاب استفاده از توکن OTP به عنوان عامل دوم احراز هویت چندعاملی الزامات زیر باید رعایت شود:

أ. کد تولید شده باید حداقل ۶ کاراکتر باشد.

ب. اعتبار کد تولید شده باید حداکثر ۶۰ ثانیه باشد و بعد از گذشت این زمان کد جدیدی تولید گردد.

ج. در صورت ورود اشتباه کد توسط کاربر پس از سه مرتبه تکرار (در یک فرایند۶۰ ثانیه‌ای) کد فعلی باید منقضی شده و کاربر تا زمان تولید کد جدید منتظر بماند.

سازمان بورس و اوراق بهادار
SECURITIES & EXCHANGE ORGANIZATION

مرکز نظارت بر امنیت اطلاعات بازار سرمایه (مکنا)

تهران، خیابان ملاصدرا، سازمان بورس و اوراق بهادار
Email: MAKNA@SEO.IR