Изх. № А 580-00/23.03.2017 г.

ВСС-2642/

ДО
Г- Н РУМЕН ГЕОРГИЕВ

ПРЕДСЕДАТЕЛ НА КОМИСИЯ
"ПРОФЕСИОНАЛНА КВАЛИФИКАЦИЯ,
ИНФОРМАЦИОННИ ТЕХНОЛОГИИ И
СТАТИСТИКА"
ВИСШ СЪДЕБЕН СЪВЕТ

ОТНОСНО: Отговор на Ваше писмо с изх. № ВСС-2642/17 от 13.03.2017 г. по изпълнение на договор № 45-06-027/15.06.2015 г. във връзка със запитване отправено към ВСС от страна на Българския институт за правни инициативи /БИПИ/

УВАЖАЕМИ ГОСПОДИН ГЕОРГИЕВ,

В отговор на Ваше писмо изх. № ВСС-2642/17 от 13.03.2017 г. и съответно наш вх. № 316/15.03.2017 г. Ви изпращаме разяснение по зададените от Българския институт за правни инициативи /БИПИ/ въпроси по отношение на разработената от нас система за избор на членове на Висшия съдебен съвет, част от Единния портал на електронното правосъдие:

ВЪПРОС 1: Практиката при конструирането на подобен тип системи е данните за удостоверяване на потребителите (т. нар. log in credentials) да не се получават по един и същ канал. В тази връзка как ще бъде елиминиран рискът от злоупотреба с тези данни?

- *Въпрос 1:* Моля, вижте по-долу отговора на въпрос номер 5.

ВЪПРОС 2: Предвижда ли се да бъдат извършени външни проверки на първичните кодове на модула за електронно гласуване (voting system) и модула за управление на избирателните списъци (electors system), осъществени от различни и несвързани помежду си експерти и ако не, какви са причините за това? Смисълът от такава насрещна външна проверка се състои в това, че тайната на разработчика ще бъде запазена, като едновременно с това много от евентуалните съмнения за пропуски в системата ще отпаднат.

• *Въпрос 2:* Системата беше представена и одитирана пред външни независими ИТ експерти по време на пробните тестови избори през 2016 г. Сорс кодовете на системата се пазят, подписани с времеви електронен печат при специални условия. Предвид важността и чувствителността им, както и от опасността от опити за блокиране и манипулиране на системата, те са защитени и с парола, съхраняваща се отделно от тях. В момента от съображения за сигурност непосредствено преди и по време на изборите не се предвижда тяхната проверка или демонстрация. Те са на разположение за експертиза в случай на възникнал спор.

ВЪПРОС 3: Съгласно чл. 54 от Правилника за провеждане на избори на членове на Висшия съдебен съвет от съдиите, прокурорите и следователите, след влизане в сила на решението, с което избирателната комисия се произнася за резултата от избора, всички данни в информационната система се архивират и се пазят 5 години от деня на избора. Какъв набор данни обхваща този архив, с оглед ограниченията на разпоредбите на чл. 52, ал. 1 - 3?

• *Въпрос 3:* Във връзка с изискването на чл. 54 е предвидено запазване на самите виртуални машини и съдържащите се в тях логове и бази данни, така че при необходимост в последствие да могат да се направят съответните експертизи по отношение на сигурност и външно вмешателство. **В тези логове, бази данни и модули, съгласно чл. 51 от правилата не се съдържа**

информация за това кой избирател за кой кандидат е гласувал. Единственото, което може да се проследи за определен избирател е това, дали си е упражнил правото на вот чрез електронно гласуване. Възможност за проверка, която съществува и при гласуването с хартиена бюлетина – аналога на хартиения списък, в който се отбелязват гласуващите на място.

Поради известна неточност на чл. 54 от правилата за провеждане на избор, в момента има предложение за изменението му така:

> „**Чл. 54.** След влизане в сила на решението, с което избирателната комисия се произнася за резултата от избора, всички виртуални машини и бази данни на модулите „Избирателни списъци“, „Административен модул“ и „Електронен избор“ се архивират и се пазят 5 години от деня на избора.“

ВЪПРОС 4: Ще бъде ли публикувана диаграмата (flow-chart), която показва отношенията „администратори-машина“ във всеки един етап от протичане на изборния процес, въз основа на която става ясно кой субект на какъв етап се включва и каква е неговата отговорност по отношение верификацията на процеса?

- *Въпрос 4:* Не, непосредствено преди провеждането на изборите и по време на самите избори с цел сигурност и опасност от злонамерени действия не се предвижда публикуването на техническа информация, включително и организационна. Всички машини и бази данни на физическо, логическо, мрежово, системно и приложно ниво са с предвидени и включени логове и при необходимост в последствие могат да бъдат одитирани.

ВЪПРОС 5: Как се подава информацията за валидните и невалидни талони? Как е осигурена системата срещу изтичане на информация при електронния обмен на данни?

• *Въпрос 5:* Генерираните от системата кодове на талони за гласуване по подразбиране са невалидни (не са активни). Непосредствено преди гласуването се активират и се променят на „валидни“ само раздадените за електронно гласуване талони с изключение на тези, които са обявени за изгубени или унищожени, в тази връзка са въведени и поредните номера на талони. Кои талони са раздадени, съответно кои трябва да бъдат активирани („валидни“), е видно от хартиените декларации за получен талон за електронно гласуване, които декларации се попълват индивидуално от всеки магистрат и сканирани се съдържат в информационната система.

След гласуване, системата не позволява повторно влизане в модула за Електронно гласуване, което от своя страна предотвратява възможността за опит да се влезе в системата и да се гласува с чужд талон без за това да се разбере от истинския собственик на талона. Т.е. ако потребител, притежаващ талон, не бъде допуснат от модула за гласуване със съобщение за това, че талонът вече е бил използван, това води до извод, че с неговия талон вече е гласувано и потребителят може да сигнализира за злоупотреба с талона му. В системата с избирателните списъци може да се направи справка дали лицето, което се е оплакало, е действителният притежател на съответният номер талон. При неправомерно използване и при необходимост, в последствие на системно и мрежово ниво може да се направи справка за точния адрес, от който е гласувано и случаят да се разследва. Ако пък лице, различно от собственика на

талона, намери или неправомерно се опита да го използва последствие (след като вече с талона е гласувано), системата отново няма да го допусне и фактически този талон няма да може да се използва. Това важи преди всичко за случаите, в които избирател след използване изхвърля своя талон и той бива намерен от друго лице.

В обобщение:

- с чужд талон не може да се гласува, без за това да разбере истинският му притежател;
- с талон, с който вече е гласувано, не може да се гласува повторно или да се разбере за кой кандидат е гласувано преди това със същия този талон.

Освен това системата поддържа функционалност за незабавно блокиране на талон за електронно гласуване, вкл. и в деня на избор за случаите в които талона е съобщен за загубен или унищожен.

На техническо ниво електронният обмен на данни между системите и модулите е защитен с електронни сертификати по криптирани канали за връзки. Самите модули и връзки между системи са в осигурени специални вътрешни мрежови зони, които не са достъпни през интернет и през други вътрешни мрежи.

Оставаме на разположение при необходимост от допълнителна информация или съдействие от наша страна.

С уважение:

Иван Иванов
Изпълнителен директор
„АБАТИ" АД

София, 21.03.2017 г.