

## ДОКЛАД

До	Висшия адвокатски съвет
От	Адв. Асен Георгиев, член на ВАДвС и председател на Комисията по въпросите на електронното правосъдие и електронните адвокатски регистри
Относно	Тестове за сигурност на Единните адвокатски регистри
Дата	03.11.2023 г.

### УВАЖАЕМИ КОЛЕГИ,

С Решение № 967/21.09.2023 г. на ВАДвС беше създадена Работна група („РБ“), в която освен членовете на Комисията по въпросите на електронното правосъдие и електронните адвокатски регистри („Комисията“), бяха включени адвокатите Жана Кисьова, Христо Хинов, Стефан Марчев и Венелина Фотева.

Сред задачите на РБ е извършване на анализ и приоритизиране на установените неотстранени недостатъци и затруднения в работата на ЕАР, изготвяне на предложение за тяхното отстраняване и преодоляване, като работи по поставените задачи във взаимодействие с изпълнителя по договора за извънгаранционна поддръжка на ЕАР - Кроссроуд.

Успоредно с това, както добре е известно на всички, ВАДвС партнира на Министерство на правосъдието в неговото участие в проект „Намери адвокат“ (Find a lawyer) по хоризонтална програма „Правосъдие-2022-Е-Правосъдие“ на Европейската комисия. В хода на изпълнението на този проект изпълнителят по договора с Министерство на правосъдието с предмет: „Анализ на нормативната уредба и съществуващите европейски практики“ изготви междинен доклад, съдържащ анализ на и препоръки към ЕАР, в който наред с други изводи, се съдържат констатации за състоянието на съществуващата система по отношение на киберсигурност, като поставената оценка от авторите на доклада е незадоволителна.

Макар тази оценка да служи единствено за сведение и ВАДвС официално да изрази пред Министерство на правосъдието своето несъгласие с тези констатации, РБ си дава сметка, че киберсигурността е изключителна важна тема в нашето съвремие и е от първостепенно значение тя бъде максимално осигурена.

Провеждането на ежегодни тестове за сигурност на регистрите е задължително по всички стандарти и най-добри практики, а такива тестове на ЕАР в новия му вид не са правени.

Ето защо РБ определи като приоритет провеждането в рамките на настоящата календарна година на тестове за информационна сигурност на уеб базиран регистър, като това включва<sup>1</sup>:

- Провеждане на уеб пенетрейшън тест по методологията „черна кутия“ (black-box testing);
- Сканиране за уязвимости;
- Изготвяне на доклад с резултатите;
- Провеждане на повторни тестове след отстраняване на открити уязвимости, при установена необходимост от такива.

Членовете на РБ, които имат опит с фирми, предоставящи тази услуга или имат препоръки за такива, бяха приканени да отправят до такива фирми искане за оферти, съдържащо основна/базова информация за регистъра и имащи еднакво съдържание.

В резултат на това и в рамките на определения срок, постъпиха три оферти, а извън него – още една.

С цел постигане на сравнимост на офертите, до кандидатите бяха отправени допълнителни, уточняващи офертите въпроси, на които те отговориха в поставения им срок. Офертите, поставените допълнителни въпроси и техните отговори бяха предоставени на Кроссроуд за експертен анализ.

Сравнителна таблица с основните параметри на всички постъпили оферти, изготвена от Кроссроуд, се съдържа в Приложение 1 към този Доклад.

След разглеждането на получените оферти, РБ, като взе предвид репутацията на всеки един от кандидатите и препоръките за тях, както и мнението на Кроссроуд, че (i) работата би била свършена добре от всеки един от кандидатите; и че (ii) най-подходящо е офертите да бъдат преценявани спрямо предложени цена и срокове, взе решение всеки един член на РБ да гласува „за“ кой да бъде избран и на база на събраните брой гласове за всеки кандидат, да бъде подредено класиране.

РБ реши още да не определя „кворум“ при гласуването и отчитането на резултата.

РБ определи срок, до който да приключи гласуването, който бе еднократно удължен, с цел постигане на по-висока активност при гласуването.

След проведеното гласуване в рамките на удължения срок, бяха отчетени 9 гласа, а тяхното разпределение между кандидатите е посочено в Приложение 2 към този Доклад.

От него е видно, че кандидатът „Лайън Гейт Секюрити“ ООД, ЕИК 206972328 получи 5 гласа, кандидатът „Телелинк Бизнес Сървисис“ ЕАД, ЕИК 130545438 получи 4 гласа, а останалите двама кандидати не получиха гласове.

---

<sup>1</sup> Предметът е формулиран от Кроссроуд

**Въз основа на гореизложеното, предлага се следния проект за решение на ВАДвС:**

**Одобрява сключването на договор за провеждане на тестове за информационна сигурност на ЕАР в рамките на 2023 г. с „Лайън Гейт Секюрити“ ООД, ЕИК 206972328, съобразно представената от това дружество оферта.**

**Възлага работата по изготвяне и съгласуване с кандидата на проект на договор и организацията по неговото подписване на председателя на ВАДвС – Ивайло Дерменджиев, главния секретар на ВАДвС - Красимир Краев и председателя на Комисията - Асен Георгиев.**

**Определя краен срок за сключване на договора до 20.11.2023 г.**

**В случай, че по причини, дължащи се на „Лайън Гейт Секюрити“ ООД, ЕИК 206972328, договор не бъде сключен в рамките на така определения срок или преди крайния срок стане ясно, че такъв не може да бъде сключен, незабавно да се премине към сключване на договор за провеждане на тестове за информационна сигурност на ЕАР в рамките на 2023 г. с „Телелинк Бизнес Сървисис“ ЕАД, ЕИК 130545438, съобразно представената от този кандидат оферта.**

**ПРИЛОЖЕНИЯ:**

1. Таблица с основните параметри на постъпилите оферти;
2. Таблица с разпределение на гласовете „за“ постъпилите оферти.

---

**Асен Георгиев, адв.**

## Приложение 1

Анализ на получени оферти към ВАДВС за провеждане на тестове за сигурност на <https://bar-register.bg>

Descriptions	Lion Gate Security – EUR 2 500,00 (without VAT)	Telelink BS – EUR 5 287,00 (without VAT)	Mnemonic – EUR 5 760,00 (without VAT)	MV Consulting USD 3 200,00 (without VAT)
<b>Детайли за теста</b>				
<p>Web Application penetration test (<i>real-world attacks from external sources, identifying vulnerabilities without prior knowledge of systems</i>)</p> <p>of:</p> <ul style="list-style-type: none"> <li>• <a href="https://bar-register.bg">https://bar-register.bg</a></li> <li>• <a href="https://private.bar-register.bg">https://private.bar-register.bg</a></li> </ul>	<p><b>Yes</b></p> <p><i>(Web Application penetration test of <a href="https://bar-register.bg">https://bar-register.bg</a> and <a href="https://private.bar-register.bg">https://private.bar-register.bg</a></i></p> <p><i>Black Box Penetration Testing real-world attacks from external sources, identifying vulnerabilities without prior knowledge of your systems.)</i></p>	<p><b>Yes</b></p> <p><i>(TBS включва два подхода – започваме с black-box, но след като направим това тестване преминаваме към тестване от типа gray-box, при което ще извършим тест на двете приложения навътре, след автентикационния процес и по този начин ще можем да изследване цялата структура на уеб приложенията и така да открием всички възможни уязвимости.)).</i></p>	<p><b>Yes</b></p> <p><i>Only <b>Black Box</b> Penetration testing will be performed.</i></p> <p><i>(“Grey box” and “White box” are <b>not part of the current scope of the proposal</b>)</i></p> <p><i>Public web site (<a href="https://public.bar-register.bg">https://public.bar-register.bg</a>).</i></p> <p><i>Officiary access (<a href="https://private.bar-register.bg">https://private.bar-register.bg</a>).</i></p> <p><i>Vulnerability assessment and Black-box penetration</i></p>	<p><b>Yes</b></p> <p><i>The black-box web application penetration test will evaluate the security of VAS public and private web site from the point of view of an external threat actor without prior access. The test will include web-based attacks that are applicable to the web site's technology stack.</i></p>

		<p>Тест за проникване на следните уеб приложения:  <a href="https://public.bar-register.bg">https://public.bar-register.bg</a>;  <a href="https://private.bar-register.bg">https://private.bar-register.bg</a>.</p>	<p>test of two web sites,  Comprehensive report generation, Retesting</p>	
Vulnerability Scanning	<p><b>Yes</b></p> <p><i>(Vulnerability Scanning. evaluates network infrastructure to identify weaknesses and provides actionable recommendations for fortifying your defenses)</i></p>	<p><b>Yes</b></p> <p>Сканиране на уязвимости на същите</p>	<p><b>Yes</b></p> <p><i>Vulnerability assessment and Black-box penetration test of two web sites, Comprehensive report generation, Retesting</i></p>	<p><b>Yes</b></p>
Pentest report	<p><b>Yes</b></p> <p><i>(Pentest report full report with all identified vulnerabilities will be provided Remediation steps will be described as part of the process for mitigation the risk of the service.)</i></p>	<p><b>Yes</b></p> <p><i>(TBS ще предостави доклад, съдържащ резюме и технически подробности, описващи откритите уязвимости и констатации от теста за проникване.)</i></p>	<p><b>Yes</b></p> <p><i>Reporting will be generated at the end of the testing.</i></p> <p><i>Vulnerability assessment and Black-box penetration test of two web sites, Comprehensive report generation, Retesting</i></p>	<p><b>Yes</b></p> <p><i>The service will produce a comprehensive penetration testing report that describes the discovered vulnerabilities and our recommendations for remediation.</i></p> <p><i>Preparing a final report (after re-test phase) - Issuing a follow-up report to confirm the</i></p>

				<i>existence or lack of previously identified vulnerabilities</i>
Reassessment after remediation	<b>Yes</b> <i>(Reassessment after remediation –After fixing the vulnerability we will perform reassessmenttoensure that identifiedissuesare patched)</i>	<b>Yes</b> <i>(Penetration Testing and retest.  при открити уязвимости и предприети коригиращи действие от страна на клиента, ще бъде извършен повторен /ретест/ за конкретните уязвимости. )</i>	<b>Yes</b> <i>(Retesting will be performed after vulnerabilities are fixed (the retesting should be in shortest possible time after the initial tests).</i>	<b>Yes</b> <i>The service also includes one remediation validation test (retest) within 90 days of the penetration test completion.</i>
Време за извършване на уеб тест за проникване & Сканиране на уязвимости	<b>5 работни дни</b>	<b>5 работни дни</b>	<b>8 business days</b>	<b>5 days</b>
Време за изготвяне на доклад	<b>5 дни</b> <i>(5 дни след приключването на теста, като при намирането на критична уязвимост тя ще бъде комуникирана</i>	<b>до 3 дни</b>	<i>Reporting will be generated at the end of the testing</i>	<i>The tester will notify the team to any ongoing critical or live threats, internally or externally, during the tests. Documentation will be performed with the</i>

	<i>веднага. Това е с цел да се намали времето, в което системата е уязвима.)</i>			<i>upmost importance, at which the information will be transferred to the client's team for further analysis and implementation of necessary secure measures.</i>
<b>Условия на доставка и начин на плащане</b>				
Delivery:	<i>The services shall be delivered within 30 business days as of the receipt of payment of the total amount specified above unless parties agree otherwise.</i>	<i>до 10 дни след подписване на приемо-предавателен протокол за доставка/ услуги и издаване на оригинална фактура.  Срок и начин на плащане: до 10 дни след подписване на приемо-предавателен протокол за доставка/услуги и издаване на оригинална фактура</i>		
Offer Validity:	<i>30 days as of issue date.</i>	<i>30 дни от датата на издаване, посочена в офертата (20.10.2023)</i>	<i>till 31.10.2023</i>	<i>30 days as of the issue date (25/10/2023)</i>
Prices:	<i>Lion Gate Security Ltd prices shall be understood,</i>			<i>MV Consulting prices shall be understood,</i>

	<i>unless otherwise agreed upon, as net price in the currency specified, not including possible value-added tax. All applicable bank charges or other fees shall be the responsibility of the Client.</i>			<i>unless otherwise agreed upon, as net price in the currency specified, not including possible value-added tax. All applicable bank charges or other fees shall be the responsibility of the Client.</i>
Payment Method:	<i>Wire transfer</i>	<i>Банков превод</i>	<i>50 % advance payment upon signing a contract, 50% final payment upon signing a handover protocol after a report has been submitted</i>	
Payment Conditions:	<i>All payments shall be made in Bulgarian Levs, as per the official exchange rate of the Bulgarian National Bank on the day of the payment. In case of delayed payment Lion Gate Security Ltd reserves the right to calculate an appropriate interest.</i>	<i>EUR - Цената в лева се формира по курсът на БНБ в деня на приемане на доставката/ услугите</i>		
Withholding:	<i>Customer may not offset or retain the due payment in</i>			



	<i>respect of any of its counterclaims if they are not chargeable and proved by grounds and amount through an effective court decision.</i>			
Приемане на доставката/услугите:	<p><b>Доклади</b></p> <p><i>След извършването на тестовете ще се изготвят два доклада.</i></p> <ul style="list-style-type: none"> <li>- <i>Executive summary, където са представени общите уязвимости.</i></li> <li>- <i>Detailed report - пълен доклад, където са описани всички детайли за откритите уязвимости и пълна информация за извършените тестове (Обхват на тестването; Методология на тестване; Детайлни резултати; Описание на уязвимостта; Локация или местоположение на</i></li> </ul>	<p><i>С подписването на <b>приемо - предавателен протокол</b> за доставка/ услуги от упълномощени представители от двете страни.</i></p> <p><i>Доставката и услугите се приемат с отделни приемо - предавателни протоколи</i></p>	<ul style="list-style-type: none"> <li>- <i>Verbal reporting.</i></li> <li>- <i>Final reporting. (Project Description; Executive Summary of Findings; General Recommendations; Mitigation Plan; Detailed Vulnerability Descriptions; Validation Results; Recommended Mitigation Actions)</i></li> </ul>	

	<i>уязвимостта; Метод за експлоатация; Въздействие и потенциален риск; Снимки на екрана или други доказателства; Препоръки; Оценка на риска; Приложения и Заключение).</i>			
--	--	--	--	--

## Приложение 2

Класиране на получени оферти  
за провеждане на тестове за сигурност през 2023 г. на <https://bar-register.bg>

	<b>Lion Gate Security – EUR 2 500,00 (without VAT)</b>	<b>Telelink BS – EUR 5 287,00 (without VAT)</b>	<b>Mnemonic – EUR 5 760,00 (without VAT)</b>	<b>MV Consulting USD 3 200,00 (without VAT)</b>
1.	Христо Хинов	Албена Пискова		
2	Венелина Фотева	Стефан Марчев		
3	Валя Гигова	Златимир Жечев		
4.	Асен Георгиев	Красимир Краев		
5.	Жана Кисьова			