Политика за поверителност/защита на данните на „Колективно финансиране“ АД

I. Политика за предотвратяване на измами и за поверителност/защита на данните

1. Политика за предотвратяване на измами

Уеб платформата ще бъде хоствана на избран доставчик с доказани процедури за сигурност като: *ИНТЕГРИРАНА СИСТЕМА ЗА ЗАЩИТА ОТ DDOS, КОЯТО ПРЕДПАЗВА ХОСТИНГ УСЛУГИТЕ НА МРЕЖОВО НИВО. ТЯ ЗАПАЗВА НОРМАЛНАТА РАБОТА НА САЙТОВЕТЕ, КАТО НЕУТРАЛИЗИРА DDOS АТАКИ КЪМ ОБОРУДВАНЕТО.*

Интегрираната система за защита от DDoS е мощен механизъм за предпазване на хостинг услугите на мрежово ниво. Това е важно, тъй като DDoS атаките могат да доведат до сериозни проблеми за онлайн платформата, като недостъпност за потребителите и загуба на бизнес. Системата за защита от DDoS предлага автоматизирано откриване и нейтрализиране на DDoS атаки, като анализира трафика на мрежата и блокира необичайните заявки, които могат да предизвикат натоварване на оборудването. Освен това, системата може да разпознае и блокира различни типове атаки, като SYN flood, DNS amplification и HTTP GET flood.

Системата за защита от DDoS предлага и висока производителност и надеждност, като работи в реално време и може да издържа на големи натоварвания. Това я прави идеална за онлайн платформи с висока посещаемост, като платформи за колективно финансиране.

Като цяло, интегрираната система за защита от DDoS е необходима за онлайн платформите, които искат да осигурят непрекъсната достъпност и защита на потребителските данни, като същевременно гарантират нормалната работа на сайтовете при всякакви условия.

ДОСТЪПЪТ ДО ПРОФИЛА ЗА УПРАВЛЕНИЕ ЩЕ СЕ ОСЪЩЕСТВЯВА С КОНТАКТЕН ИМЕЙЛ АДРЕС И ПАРОЛА ЗА ПРОФИЛА. ЗА ДОПЪЛНИТЕЛНА ЗАЩИТА ЩЕ СЕ АКТИВИРА ДВУФАКТОРНА АУТЕНТИКАЦИЯ, КОЯТО ЕЛИМИНИРА ВЪЗМОЖНОСТТА ЗА ЗЛОВРЕДЕН ДОСТЪП ДО УСЛУГИТЕ ПРЕЗ ПРОФИЛА.

Двуфакторната аутентикация е изключително важна за осигуряване на допълнителна защита на профила за управление на платформата за колективно финансиране. При тази система за аутентикация, след въвеждане на потребителското име и парола, се изисква и въвеждане на допълнителен код за потвърждение, който се генерира от мобилно приложение или получава на потребителския телефон. Това значително повишава нивото на сигурност, тъй като зловредни

потребители няма да могат да имат достъп до профила, дори ако имат достъп до потребителското име и паролата.

ЗАЩИТА ПО IP АДРЕС И РАЗРЕШАВАНЕ НА ВХОДА В ПРОФИЛА САМО ЗА ОПРЕДЕЛЕНИ IP АДРЕСИ/МРЕЖА.

Защитата по IP адрес и разрешаването на входа в профила само за определени IP адреси/мрежа е една от най-ефективните мерки за защита на профилите за управление. Тази мярка може да бъде използвана за ограничаване на достъпа до профила за управление само до определени компютри или мрежи, които са доверени и които потребителят може да идентифицира като сигурни. Това е важно, защото може да се предотврати входът в профила от зловредни компютри или мрежи.

За да се реализира тази мярка за сигурност, системата за управление на платформата за колективно финансиране може да използва IP-базирани списъци за разрешаване на входа на потребителите. Това означава, че само потребителите, които идват от доверени IP адреси или мрежи, ще имат достъп до профилите за управление. За да се улесни процесът на добавяне на нови IP адреси или мрежи, системата може да предостави интерфейс за администриране на списъка с доверени IP адреси. Това ще позволи на администраторите да добавят или премахнат IP адреси или мрежи, които са разрешени да влизат в профилите за управление.

Интегрирана защита при вход в клиентския профил и при засечени определени критерии се изиска въвеждане на допълнителен код, който да се изпраща само на контактния имейл адрес за услугите.

ЗАЩИТА СРЕЩУ BRUTE FORCE НА CMS ПЛАТФОРМИ И ИМЕЙЛИ

Brute Force атаките са кибератаки, при които злоумишленникът се опитва да получи достъп до система, като пробва множество комбинации от потребителски и паролни имена. За да се предотвратят тези атаки, е необходимо да се приложат подходящи мерки за защита, като например:

- Силни пароли: Изискването за силни пароли може да намали риска от успешни Brute Force атаки. Паролите трябва да са дълги и да включват различни видове знаци.
- Лимитиране на опитите за влизане: Може да се ограничи броят на опитите за влизане на потребителите до системата. Например, системата може да блокира опитите за влизане след определен брой грешни опити за парола.
- CAPTCHA: Добавянето на CAPTCHA може да предотврати автоматизираните Brute Force атаки, като изисква от потребителя да реши капча преди да получи достъп до системата.
- IP блокиране: Може да се блокират IP адресите на атакуващия, след като те бъдат засечени при опити за влизане в системата. Това може да се осъществи чрез инструменти като firewall и security plugins.

- Мониторинг на логовете: Редовният мониторинг на логовете на системата може да помогне да се открият Brute Force атаки и да се предприемат подходящи мерки за защита.

За защита срещу Brute Force на CMS платформи и имейли може да се използват специализирани security plugins, като например Login LockDown за WordPress, Brute Force Login Protection за Joomla и т.н. Тези инструменти могат да блокират IP адреси след определен брой опити за влизане, както и да наблюдават логовете на системата за подозрителна активност.

BACKUP

Backup е изключително важен елемент в сигурността на всяка система за управление на съдържанието. Той позволява да се възстанови информацията в случай на неочаквана загуба или повреда на данните.

За да се гарантира правилната работа на системата за управление на съдържанието и да се предотвратят евентуални проблеми, е необходимо да се правят редовни и пълни резервни копия на данните. Различни платформи за управление на съдържанието предоставят различни инструменти за създаване на резервни копия, като някои от тях могат да се настроят да правят автоматични копия на редовни интервали.

Важно е да се запазят резервни копия на всички данни, включително на базата данни, конфигурационните файлове и всички медийни файлове (картинки, видеа, аудио и т.н.). Копията трябва да се пазят на сигурно място, където няма да бъдат изложени на опасност от хакерски атаки или други събития, които могат да доведат до загуба на данни.

За да се гарантира, че резервните копия са пълни и валидни, е препоръчително да се извършва периодична проверка на тяхното състояние. Това може да се направи чрез възстановяване на една от копията на тестова система, за да се уверите, че данните са налични и могат да бъдат използвани.

2. Поверителност и защита на данните

2.1 ОБРАБОТКА НА ЛИЧНИ ДАННИ

Дружеството се задължава да третира личните данни, предоставени от потребителите в съответствие с разпоредбите на действащото законодателство по въпроса и с необходимата поверителност.

2.2 ВИДОВЕ ЛИЧНИ ДАННИ, КОИТО СЕ СЪБИРАТ И ОБРАБОТВАТ ОТ ДРУЖЕСТВОТО

Навигацията на потребител през Уебсайта се извършва анонимно, с изключение на тези частни секции, ограничени до регистрирани потребители, които се осъществяват при поискване на техния идентификационен код. Ние не събираме лични данни, освен когато потребителят изрично ни предостави тази информация.

Дружеството събира онези лични данни, които потребителят на уебсайта предоставя при регистрация или при извършване на инвестиция през Дружеството, както и тези, които се генерират по време на навигацията им през уебсайта и при използването на продуктите / услугите / съдържанието / абонаменти на уебсайта.

Потребителят декларира на своя отговорност, че данните, предоставени на Дружеството, са верни и принадлежат на него. Всяко невярно или неточно твърдение, което възниква в резултат на представената информация и данни, както и щетите, които тази информация може да причини, ще бъдат отговорност на потребителя. Потребителят, който предостави неверни данни, може да бъде изключен от услугите на уебсайта, към който принадлежи.

2.3 МЯСТО НА СЪХРАНЕНИЕ НА ЛИЧНИТЕ ДАННИ НА ПОТРЕБИТЕЛИТЕ И ПЕРИОД НА СЪХРАНЕНИЕ.

В съответствие с действащото законодателство за защита на личните данни, данните, които потребителят изрично се съгласява да сподели с Дружеството или които предоставя в бъдеще, ще бъдат включени за обработка в съответния автоматизиран файл, собственост на Дружеството. Тези данни ще се съхраняват, докато потребителят не изрази желание да бъдат изтрити.

Дружеството е приело изискваните от закона нива на сигурност на защита на личните данни, като е предприела необходимите правни и технически мерки за предотвратяване на загуба, злоупотреба, промяна, неоторизиран достъп и кражба на предоставените лични данни. Въпреки това, потребителят трябва да е наясно, че мерките за сигурност в интернет пространството не са непреодолими.

2.4 УПРАЖНЯВАНЕ НА ПРАВАТА НА ПОТРЕБИТЕЛЯ НА ДОСТЪП, КОРИГИРАНЕ, ЗАЛИЧАВАНЕ И ПРЕНОСИМОСТ НА ЛИЧНИТЕ ДАННИ И ОГРАНИЧАВАНЕ ИЛИ ОТКАЗ ОТ ТЯХНОТО ОБРАБОТВАНЕ.

По всяко време регистрираният потребител може да упражни правото си на достъп, коригиране, заличаване, ограничаване и отказ от обработването на личните му данни чрез писмено, подписано по надлежния ред искане ка, като приложи копие от своя документ за самоличност или друга документация, която го идентифицира, адресирани до “Колективно финансиране” АД на адреса, посочен по-горе, или по имейл, адресиран до contact@spacecrowd.bg

2.5 ИЗПОЛЗВАНЕ НА ЛИЧНИТЕ ДАННИ НА ПОТРЕБИТЕЛИТЕ ОТ ДРУЖЕСТВОТО

Данните, предоставени от потребителя, могат да бъдат използвани от Дружеството, за да подобри функционалностите на уебсайта, да го идентифицира и да му предложи продуктите и услугите, от които се интересува, за статистически цели, както и да изпраща всякакви вид търговска, техническа и оперативна информация за промоции, продукти и услуги, предлагани от Дружеството и от трети страни – компании, търсещи финансиране, партньори на Дружеството.

По всяко време потребителят може да възрази срещу използването на личните му данни за търговски цели чрез имейл на contact@spacecrowd.bg

2.6 СПОДЕЛЯНЕ НА ЛИЧНИ ДАННИ НА ПОТРЕБИТЕЛИТЕ

Личните данни на потребителя могат да бъдат споделяни по следните начини:

- Тези данни, които изрично изберете да бъдат част от публичния профил, ще бъдат видими за потребителите, които са регистрирани на Дружеството, когато потребителя избере да следва новините на дадена компания, търсеща финансиране или да инвестирате в нея чрез Дружеството. Потребителят избира дали публичният му профил да е видим и кои данни от него да са публични.

- Когато потребителят обменя информация с компания, която е в кампания за набиране на средства, и с други потребители чрез Дружеството или участва във форума за коментари в Дружеството, тази информация може да бъде видима за други потребители, които са регистрирани в Дружеството.

- Когато потребителят извърши инвестиция в компания чрез Дружеството, Дружеството предоставя лични данни на компанията, която получава финансиране, и на други лица, участващи във формализирането на инвестицията (например нотариус, длъжностни лица на търговски регистар, централен регистър на ценни книжа).

- Ако потребителят промени собствеността или контрола върху всички или част от услугите или активите, Дружеството ще прехвърли цялата информация на профила на новия собственик.

- Личните данни на потребителя могат да бъдат предоставяни в съответствие с действащата нормативна уредба и на регулаторни органи (напр. КФН)

2.7 ПРОМЯНА В ПОЛИТИКАТА ЗА ПОВЕРИТЕЛНОСТ

Дружеството може да приеме промяна в установените практики и/или политика за поверителност, които може да засегнат личните данни на потребителите. Задължение на потребителя за достъп до уебсайта е да се запознае с Политиката за поверителност на Дружеството. Дружеството ще уведоми по електронна поща потребителя за всяка актуализация в Политиката за поверителност на всички потребители, регистрирани в Дружеството, като отговорността на потребителя е да ги прочете и приеме.

2.8 ПОЛИТИКА ЗА БИСКВИТКИ

Какво представляват бисквитките?

„Бисквитката“ е малък файл с данни, който се изтегля на компютъра/смартфона/таблета на потребителя при достъп до определени уеб страници, за да съхранява и извлича информация за навигацията, която се извършва от съответното устройство.

Тези файлове се съхраняват на устройството на потребителя и съдържат анонимни данни, които не са вредни за самото устройство. Те се използват за запомняне на потребителски предпочитания, като избран език, данни за достъп или персонализиране на страницата. Бисквитките могат също да се използват за записване на анонимна информация за това как посетител използва даден уебсайт. Например от коя уеб страница сте отворили или дали сте използвали рекламен „банер“, за да стигнете до там.

Какви бисквитки използва Дружеството

Дружеството използва следните бисквитки на уебсайта:

- бисквитки, строго необходими за осигуряване на навигацията на потребителя през уебсайта и за предоставяне на определени услуги, изрично заявени от потребителя: ако тези бисквитки са деактивирани, потребителят няма да може да получава или правилно да осъществява достъп до съдържанието и услугите на Дружеството; и

- Аналитични бисквитки (за наблюдение и статистически анализ на поведението на всички потребители): ако тези бисквитки са деактивирани, уебсайтът може да продължи да функционира, без да се засяга фактът, че информацията, уловена от тези бисквитки при използването на Дружеството, позволява на Дружеството да подобри предлаганите услуги.

Потребителят сам решава дали да приеме бисквитки или не, когато конфигурира своя уеб браузър.

Уебсайтът може да съдържа връзки към социални мрежи (като Facebook или Twitter). Дружеството не контролира бисквитките, използвани от тези външни мрежи.

II. Местоположенията, методите и политиките за архивиране на документация, включително използването на облаци

1. Тези правила регламентират реда и отговорностите на Дружеството, свързани с действия при резервиране (архивиране) на информацията и мерките за защита на данните в системата на платформата, както и мерките за защита на обработваните от Дружеството лични данни, съгласно изискванията на член 32 на Регламент 2016/679 (GDPR).

Правилата са разработени, за да се осигури запазване на информацията в Дружеството, гарантирайки, че не може да бъде загубена и че може да бъде възстановена във всеки един момент, при срив на системата или при всякаква друга ситуация.

2. Всички ключови компоненти, обслужващи работоспособността на платформата, ще са дублирани: най-малко два сървъра за приложения, два маршрутизатори за достъп, резервирано мрежово оборудване и др. Двата маршрутизатора за достъп до платформата ще работят автономно, независими един от друг, и ще и се намират в сградата на БФБ АД, а трети – в резервния център на Борсата.

3. Целта на ежедневния архив да съхрани и осигури бързо частично възстановяване на информационната система платформата при всякакъв вид срив на система за време по-малко от 2 часа. Ежедневният архив се извършва всяка вечер от 01.00 часа от понеделник до неделя в автоматичен режим.

4. Архивните файлове се съхраняват на следните физически места: сървърно помещение на БФБ АД на ул. Три Уши 6, и Резервен център, както и в облачното пространство на първокласен доставчик на облачни услуги.

5. Целта на седмичния архив е да съхрани и осигури пълно възстановяване на информационната система на Дружеството при срив на базата данни**.** Седмичният архив се извършва всеки петък в 22.00 часа в автоматичен режим.

6. Отговорността по проверката за цялостност на извършения архив и съхране-нието в охранявани места се носи от Функционално звено „Информационни технологии“. Промени в графика за извършване на архивите се определя и регулира от Функционално звено „Информационни технологии“.

7. Необходим хардуер:

- препоръчва се поне 10% свободно дисково пространство на сървъра;
- външен носител за съхраняване на копие от архивите на физически защитено място извън сградата – в Резервен център.

8. Проверка и тестване на архивите:

- всяка сутрин след извършен архив, в Функционално звено „Информационни технологии“ проверяват логовете на архивите на база нотификейшъни, които получават.
- периодично Функционално звено „Информационни технологии“ прави пробен тест за възстановяване на резервно копие, с цел да се установи дали данните ще бъдат възстановени правилно при евентуален срив.

Тези Правила са приети с Решение на Съвета на директорите на „КОЛЕКТИВНО ФИНАНСИРАНЕ“АД.