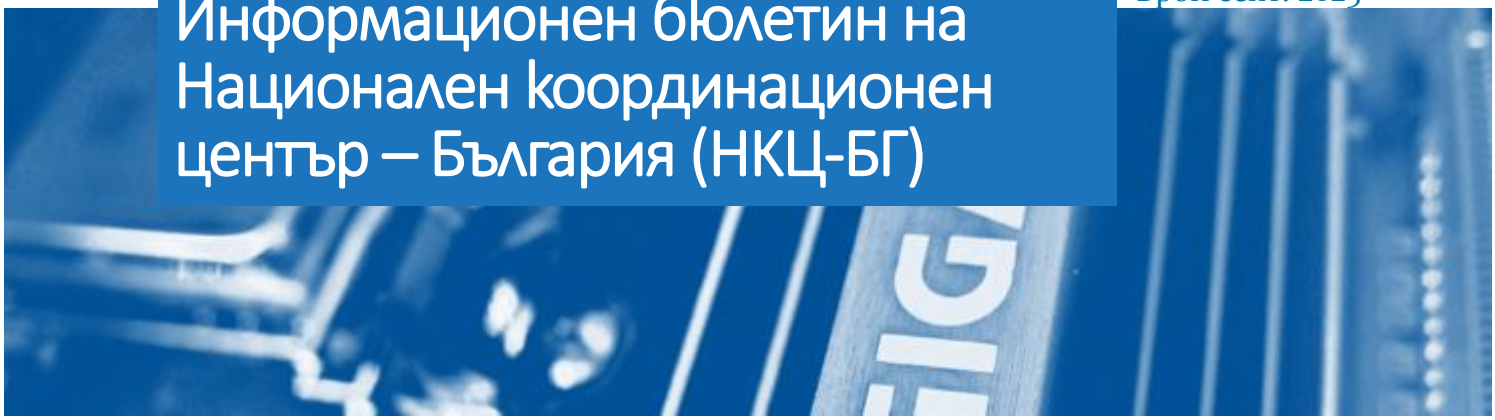
NCC-BG
NATIONAL COORDINATION CENTER
BULGARIA

Министерство на електронното управление

Съфинансирано от Европейския съюз

Информационен бюлетин на Национален координационен център – България (НКЦ-БГ)

Брой септ. 2025



63 БЪЛГАРСКИ ПРЕДПРИЯТИЯ ЩЕ ПОЛУЧАТ ФИНАНСИРАНЕ ЗА ПОВИШАВАНЕ НА КИБЕРСИГУРНОСТТА ИМ

63 български фирми ще получат безвъзмездна финансова помощ след приключване на оценката на качеството на проектните предложения по процедура DEP-1.001 „Подкрепа за подобряване на киберсигурността в малките и средни предприятия в Република България".

С наличния финансов ресурс се предлагат за финансиране 63 проектни предложения с общ размер на БФП 3 882 551,44 лева. Финансирането е 100% безвъзмездно и не се изисква съфинансиране от страна на кандидатите.

Процедурата се реализира от МЕУ в качеството му на Национален координационен център (NCC-BG) и се финансира със средства от програма „Цифрова Европа" 2021-2027 г. и от бюджета на министерството.

Основната цел на инициативата е да подпомогне микро, малки и средни предприятия в България при внедряването на съвременни решения за защита от киберзаплахи. Очакваният ефект е повишаване на устойчивостта на бизнеса в дигиталната среда, намаляване на риска от киберинциденти и подобряване на конкурентоспособността на българските компании.

ПРОЦЕДУРА DEP-001.1

Министерството на електронното управление обяви на 13.06.2025 г. процедура чрез подбор на проектни предложения „Подкрепа за подобряване на киберсигурността в малките и средни предприятия в Република България" по Програма „Цифрова Европа" 2021-2027



Резултатите от оценяването на проектните предложения са публикувани на 30.09.2025 г. тук.



Целта на процедурата е предоставяне на финансова подкрепа, която да позволи на малките и средни предприятия да въведат съвременни решения и мерки за намаляване на рисковете за киберсигурността им и за гарантиране на устойчивостта на икономиката на Република България.

МЕЖДУИНСТИТУЦИОНАЛНО ОТКРИВАЩО СЪБИТИЕ ЗА ЕВРОПЕЙСКИЯ МЕСЕЦ НА КИБЕРСИГУРНОСТТА 2025 Г.

Тази година Европейската комисия е домакин на Междуинституционалното откриващо събитие на 1 октомври 2025 г. в Брюксел и онлайн.



Месец Октомври 2025 г. ще бъде Европейски месец на киберсигурността *- ежегодна кампания на ЕС, посветена на повишаване на осведомеността за киберсигурността сред гражданите и организациите.*



Европейският месец на киберсигурността (ECSM) е ежегодната кампания на ЕС, посветена на повишаване на осведомеността за киберсигурността сред гражданите и организациите. Годишното събиране е възможност за насърчаване на иновациите, развиване на таланти и трансформиране на перспективите.

Европейският център за компетентност в киберсигурността (ECCC) също ще вземе участие в тазгодишната програма. Лука Талиарети, изпълнителен директор на ECCC, ще се включи в дискусиите на високо ниво, с акцент върху предизвикателствата и възможностите, свързани с ресурсите за киберсигурност.

Фокусът тази година е върху човешкия фактор в киберсигурността: укрепване на уменията, подкрепа на по-безопасни онлайн преживявания и изграждане на култура на готовност. Иновативен елемент от събитието ще изследва как игровите техники могат да доведат до промяна в поведението и да засилят осведомеността.

Събитието е отворено за всички чрез линк за стрийминг на живо, като не е необходима предварителна регистрация.

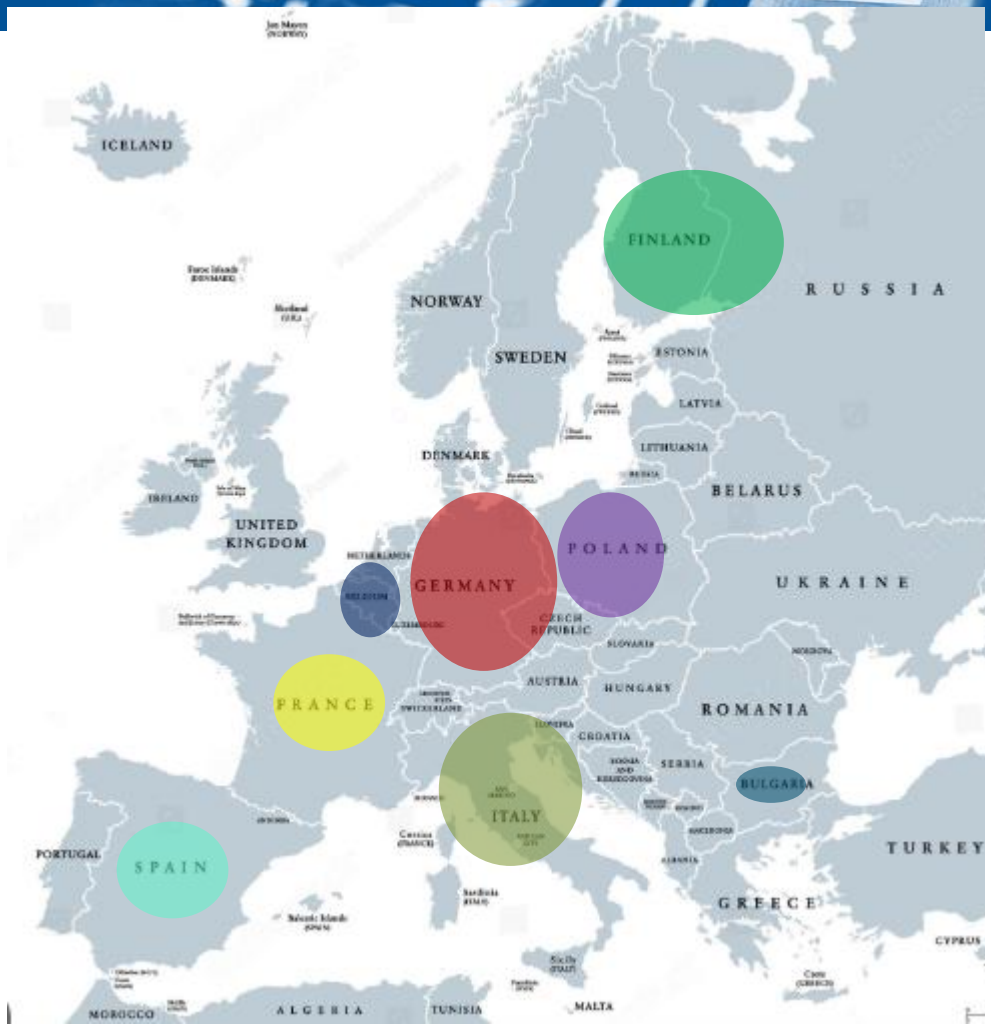
За повече информация, посетете официалната страница на събитието: https://commission.europa.eu/get-involved/events/interinstitutional-kick-event-european-cybersecurity-month-2025-2025-10-01_en

КИБЕРБЮЛЕТИН НА ДИРЕКЦИЯ „МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ“

По данни обработвани в Дирекция „Мрежова и информационна сигурност“ към Министерството на електронното управление за месец септември на ниво ЕС може са се изведе информацията, че най-активната заплаха са хактивистките атаки от типа „разпределен отказ от услуги“ (DDoS). Сред първите три целеви държави членки на ЕС са Германия, Италия, Финландия и Испания, към които по-специално са насочвани DDoS кампании. Наблюдава се повишаване на интереса на атакуващите към сектора на публичната администрация.

АКЦЕНТИ НА КИБЕРБЮЛЕТИНА

• Обобщение на установените събития през месец септември и изобразяването им на карта;



Най-силно засегнати сектори в ЕС (от Ransomware и други видове заплахи)

Най-силно засегнати сектори в ЕС от Ransomware и други видове заплахи са сектор „публична администрация“, сектор „транспорт“, сектор „цифрова инфраструктура“ и сектор „енергетика“.

• Засегнати сектори и основни видове атаки;

• Секторно наблюдение, мониторинг на вида заплаха, докладвани Ransomware в ЕС

• Терминология и оценяване на събитията

• Най-често срещани кибератаки в България за месец септември.

• Заключение

На ниво ЕС се запазва тенденцията основната част от атаките да са от типа DDoS.

Според CERT BG, в България основно преобладават phishing атаките като се забелязва лек спад спрямо предходния месец.



Секторно наблюдение

Отчита се ръст на докладваните събития във всички сектори спрямо предходния месец от годината, с изключение на сектор „публична администрация“, където бройката се запазва и сектор „транспорт“, където се забелязва спад на докладваните събития.

Основни видове атаки в ЕС

Основните видове атаки в ЕС са DDoS атаки и Ransomware, като DDoS е основният тип атака през месец септември.

Мониторинг на вида заплахи

През месец септември, анализът показва драстичен ръст на докладваните събития към организации на държавите членки на ЕС спрямо месец август. Забелязва се още лек спад единствено в категорията Ransomware.

Ransomware докладвани в ЕС

Отчита се, че най-много на брой са ransomware атаките/инцидентите от типа qilin. На второ и трето място са Akira и DragonForce.

Qilin е активна ransomware заплаха от 2022 г., използваща двойно изнудване – криптиране на данни и заплаха за публичното им разкриване. Групата работи по модела Ransomware-as-a-Service (RaaS), като атаките често започват чрез phishing, уязвимости в публични услуги или компрометирани акаунти. След пробива се използват инструменти като PowerShell, PsExec и Cobalt Strike за придвижване и деактивиране на защити.

Qilin таргетира организации от различни сектори особено в Западна и Централна Европа и е известна с агресивен натиск върху жертвите чрез собствен сайт за публикуване на компрометирани данни в тъмната мрежа.

На второ място са инцидентите от типа Malicious Code (зловреден код).

Не са докладвани и регистрирани атаки от типа Ransomware и типа DDoS.



„The Gentlemen“ (или „The Gentleman“) е име, с което се свързва хакерска група, извършваща т.нар. двойно изнудване – първо криптиране на данните на жертвата чрез рансъмуер, а след това заплаха за публично изтичане на откраднатата информация, ако не бъде платен откуп. Групата обикновено получава достъп до системите чрез фишинг имейли, пробити RDP връзки, уязвимости в софтуера или чрез закупуване на достъп от други хакери (т.нар. „initial access brokers“). След проникване, киберпрестъпниците извличат чувствителни данни, криптират файлове и оставят откупно съобщение с инструкции за плащане и краен срок. За да увеличат натиска върху жертвата, те често публикуват част от откраднатите данни в сайтове за публикуване на компрометирани данни в тъмната мрежа. Признаци на подобна атака включват внезапна поява на файлове с непознато разширение, откупни бележки, нетипичен мрежов трафик и подозрителна активност на администраторски акаунти.

SafePay е нов и агресивен рансъмуер оператор, идентифициран за първи път през септември 2024 г., който през 2025 г. се утвърждава като една от най-активните групи с над 200 потвърдени жертви по света. Групата SafePay прилага тактика „двойно изнудване“ (double extortion): криптира данните на жертвата (.safepay разширение), като преди това ги ексфилтрира, и заплашва с публично разкрие информацията, ако откупът не бъде платен. Един от известните такива случаи е атаката срещу Ingram Micro през юли 2025 г., при която бяха откраднати 3.5 TB чувствителни данни, като групата е проникнала чрез VPN (GlobalProtect), оставила е бележка за искане на откуп и заплашва да публикува изтеклите материали.

Сектори, засегнати от Ransomware в ЕС

Спрямо предходния месец се забелязва драстичен ръст в сектор „Производство“ и сектор „Публична администрация“ по отношение на Ransomware атаки.

Регистрирани кибератаки в CERT България

През месец септември най-важните докладвани и регистрирани в CERT България атаки в България са Malicious Code (зловреден код) и Phishing.



Заключение

След извършения анализ е установено, че в ЕС се запазва тенденцията от предходния месец основната част от атаките да са от типа DDoS. Според предоставените данни от CERT BG прави впечатление, че в България основно преобладават phishing атаките като се забелязва лек спад спрямо предходния месец. На второ място са инцидентите от типа Malicious Code (зловреден код). Не са докладвани и регистрирани атаки от типа Ransomware и типа DDoS.





Министерство на електронното управление

ул. „Ген. Гурко“ № 6

Гр. София 1000

Ел. поща: bnccc@egov.government.bg

Ел. адрес: https://ncc.egov.bg/