Киберпрестъпления срещу бизнеса в ЕС:

Предизвикателства при докладването в полицията

Policy Brief

През последните десетилетия цифровите технологии се превърнаха в неизменна част от ежедневието на гражданите и бизнеса в ЕС. Дигиталните иновации насърчиха социално-икономическото развитие в държавите-членки на ЕС, но същото така доведоха до увеличаване на рисковете от киберзаплахи и кибератаки. Киберсигурността се превърна в критично условие за съществуването на дигитализирана и взаимосвързана Европа, чийто просперитет и технологичен напредък все повече зависят от киберустойчивостта.

Избухването на пандемията COVID-19 ускори дигитализацията не само в Европа, но и в целия свят, но същевременно доведе до появата на редица нови предизвикателства. Наред с това, продължаващият конфликт в Украйна допълнително увеличи рисковете свързани с киберпрестъпления спрямо физически лица, фирми и публични институции. Противоепидемичните ограничения и работата от вкъщи предоставиха и продължават да предоставят нови възможности на киберпрестъпниците.[1] В периода 2021-2022 г. най-разпространените киберзаплахи са: рансъмуер, зловреден софтуер, социално инженерство (напр. фишинг), разпределени атаки за отказ на услуга (DDoS атаки), както и неразрешен достъп до данни и мрежи - включително атаки срещу хуманитарни организации и организации с нестопанска цел. Конфликтът между Русия и Украйна също доведе до множество проблеми за киберсигурността в ЕС. Кибервойната е неразделна част от руската инвазия, като има данни, че руските служби стоят зад много от атаките срещу компютърни мрежи и

Основни изводи

- Най-разпространени киберпрестъпления срещу малки и средни предприятия в ЕС-27 са **зловреден и шпионски софтуер и фишинг атаки с цел кражба на банкови сметки или самоличност**.
- През 2021 г. **44% от киберпрестъпленията**, с които са се сблъскали малките и средни предприятия в ЕС-27, **не са били докладвани**.
- Основните причини за недокладване на киберпрестъпления са:
  - инцидентът е разрешен вътрешно
  - инцидентът е твърде незначителен
  - липса на доверие в полицията и нейната дигититална компетентност
  - липса на единен механизъм за докладване
  - вероятност от прекъсване на бизнес процеси
  - пропуски при прилагане на мерките за киберсигурност
- **Сътрудничеството между публичния и частния сектор** следва да бъде насърчено чрез **хармонизиране** и **централизиране** на **механизмите за докладване** и **изграждане на партньорства основани на доверие**.

[1] Europol (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021.

Тази публикация е финансирана от Фонда за вътрешна сигурност на Европейския съюз - Полиция.
Съдържанието на публикацията отразява единствено възгледите на авторите и е тяхна изключителна отговорност.
Европейската комисия не поема никаква отговорност за използването на съдържащата се в нея информация.

информационни системи на публични и частни институции в ЕС.,[2] Засилващата се взаимовръзка между информационните технологии и традиционните (офлайн) престъпления също води до нарастване на криминалните заплахи. Престъпниците все по-често използват дигитални технологии, които им дават възможност за достъп до нови методи и инструменти за извършване на престъпления.

Въпреки че кибератаките и техните извършители поставят все по-голяма заплаха за сигурността, към днешна дата все още има малко информация за реалния обхват и въздействие на киберпрестъпността по отношение на бизнес сектора в ЕС . Липсата на информация се дължи най-вече на ниските нива на докладване. Много малка част от киберпрестъпленията попадат в полезрението на системата на наказателното правосъдие. Недостатъчното докладване е сред основните пречки за придобиване на ясна представа относно размера на проблема с киберпрестъпленията срещу бизнеса и допринася за липсата на ефективно сътрудничество между публичния и частния сектор. В крайна сметка това води до ограничени резултати в областта на наказателното правосъдие.

Фактори за недостатъчно докладване на киберпрестъпления

Недостатъчното подаване на сигнали остава едно от основните предизвикателства пред разбирането на реалните мащаби на киберпрестъпността. Ограниченото докладване оказва влияние върху регистрирането на киберпрестъпленията, а оттам и върху наличието на точни данни за киберпрестъпността. Неотдавнашно проучване на киберпрестъпленията срещу малки и средни предприятия (МСП) в държавите - членки на ЕС, потвърждава, че докладването към полицията продължава да е ниско, като 44 % от киберпрестъпленията по отношение на МСП, не са докладвани на никого.[3]

Няколко са най-често споделяните причини за недокладването на киберинциденти от предприятията. Една от най-често срещаните причини е свързана с възприятието, че инцидентът е твърде незначителен и/или не си струва да се докладва. Подобна често посочвана причина е, че случаят е бил разрешен вътрешно. Други причини се отнасят до страхове от увреждане на репутацията и липсата на доверие в полицията. В първия случай, предприятията се опасяват, че ако започне разследване и киберинцидентите станат публично известни, това може да има отрицателно въздействие върху доверието на клиентите и инвеститорите. Наред с това, фирмите често нямат доверие в дигиталната компетентност на полицейските органи и поради това не съобщават за киберинциденти.

Друг важен фактор, особено за малките фирми и тези, които не взаимодействат често с полицията, е липсата на единен централизиран механизъм за подаване на сигнали. Липсата на централизиран механизъм означава наличие на множество канали и различни задължения за докладване, които в крайна сметка намаляват мотивацията и броят на подадените сигнали като цяло.

Докладването на киберпрестъпления често е възпрепятствано и от притеснения на фирмата, че определени бизнес процеси ще бъдат прекъснати, тъй като след кибератака приоритетите на фирмата и правоприлагащите органи могат да се различават значително. От гледна точка на фирмите, приоритет след киберинцидент е да се запази и продължи дейността на предприятието. Това предполага бързо възстановяване на достъпа до данните и мрежата след атаката, както и избягване на загуба на време и финансови щети. Така например, през 2021 г. загубеният бизнес (напр. нереализирани приходи, пропуснатите ползи или загубени клиенти) съставлява най-голямата част от разходите възникнали вследствие на пробив в сигурността на данните на компаниите в световен мащаб. Поради това, свързването с външни ИТ консултанти, решаването на технически проблеми и възстановяването на данни и услуги често са с по-висок приоритет за фирмите от запазването на доказателствата за престъпление.

[2] CSIS. (2022, June 16). Cyber War and Ukraine.

[3] European Commission. (2022). Flash Eurobarometer 496 SMEs and cybercrime.

Слабата осведоменост относно значението на киберсигурността и непознаването на задълженията за докладване към висшето ръководство и компетентните органи, също допринасят за ниското ниво на докладване към полицията. Някои предприятия, особено МСП, често не знаят, че са станали жертва, тъй като не разполагат с обучен персонал или ресурси за засичане на кибератаки. В някои случаи, дори и при успешно засечена кибератака, фирмите може да не съобщят за нея, защото подценяват нейната сериозност.[4]

Факторите за недокладване като предизвикателство на европейско равнище

Киберпрестъпността и цялостната бизнес среда в различните държави членки оказват по-скоро ограничено влияние върху причините за недокладване на информация. Добър пример за това е по-внимателното разглеждане на контекста в три различни държави-членки на ЕС, а именно България, Нидерландия и Испания. Трите държави имат много различна структура на икономиката като дял на големите предприятия и МСП и дигиталната грамотност. Докато в Нидерландия се намират сравнително голям брой големи компании, в Испания и България бизнесът се състои от голям брой МСП. Освен това, трите държави имат различни нива на развитие на цифровизацията и трансформацията на бизнеса, включително политиките по отношение на неприкосновеност на личния живот в дигиталното пространство и киберсигурността. Въпреки това, и трите са изправени пред сходни предизвикателства по отношение на факторите за недокладване от страна на фирмите. Например, приблизително една от десет компании във всяка от трите държави членки посочва липсата на информираност за работата на полицията с киберпрестъпления като често срещана причина за недокладване.

България

Информацията за инциденти в областта на киберсигурността и киберпрестъпленията в страната се събира от националния екип за реагиране при инциденти с компютърната сигурност (CERT) и от Главна дирекция "Борба с организираната престъпност" (ГДБОП) в България. Съгласно данни на CERT-България, през 2020 г. Са регистрирани приблизително 2100 киберинцидента, повечето от които са свързани с фишинг и атаки със зловреден софтуер. Според Българската асоциация за киберсигурност, през 2021 г. е имало 70% увеличение на кибератаките срещу МСП в България в сравнение с предходната година. Наред с това, по данни споделени от експерти на ГДБОП, специализираното звено за борба с киберпрестъпленията получава средно около десет сигнала за опити или извършени киберпрестъпления дневно. Най-разпространените видове киберпрестъпления срещу фирми, според ГДБОП, са а таки с компроментиране на бизнес електронна поща,[5] фишинг атаки, рансъмуер атаки, разпределени атаки за отказ на услуги и кибератаки от бивши служители. По-специално, атаките с компроментирана бизнес електронна поща най-често засягат фирми, работещи в областта на външната търговия.

По отношение на факторите за недостатъчно докладване, най-разпространените включват:

- непознаване на нормативната уредба, изискваща докладване на кибератаки (Закон за киберсигурността);
- ниско доверие в правоприлагащите органи;
- липса на осведоменост за значението на киберсигурността, включително за ролята, която фирмите могат да играят при предотвратяването и докладването на киберпрестъпления;
- неподготвеност за кибератаки поради липса на експертен опит в областта на киберсигурността, инвестиции в ИТ, обучение на служителите и мерки за киберзащита;
- страхът от увреждане на репутацията, особено при големите компании.[6]

[4] Williamson, J. (2016, February 10). Cyber-attack impact severely underestimated by SMEs. The Manufacturer.

[5] Business Email Compromise (BEC)

[6] Интервюта с експерти от правоохранителните органи, центъра CERT, асоциациите за киберсигурност и академичните среди.

Нидерландия

Нидерландското централно статистическо бюро (CBS) посочва, че броят на киберинцидентите в страната е намалял през периода 2016-2020 г. През 2016 г. почти 40% от нидерландските дружества са преживели някакъв вид инцидент, свързан с киберсигурността. През 2019 г. този показател е по-малко от 20% за големите компании.[7] Освен това, инцидентите, свързани с разпределени атаки за отказ на услуга са 1610 през 2020 г., което е със 75% повече в сравнение с 2019 г.

Според неотдавнашно проучване на Европейската комисия, анкетираните нидерландски МСП съобщават, че през последните 12 месеца се сблъскват най-вече с фишинг атаки, атаки за превземане на акаунти или кражба на самоличност (21% от МСП), следвани от вируси, шпионски или зловреден софтуер (17%) и неоторизиран достъп до файлове или мрежи (6%). Най-сериозните инциденти са извършени чрез измами (34%) и зловреден софтуер (21%).[8] Тези констатации са в съответствие с предишни проучвания, според които зловредния софтуер, онлайн измамите, фишингът и хакерството са най-разпространените форми на киберпрестъпления срещу МСП в Нидерландия.[9]

Когато става въпрос за докладване на киберпрестъпления, около 5-10% от нидерландските компании, които са станали жертва на външна кибератака, впоследствие я докладват.[10] Съществуват различни причини за недокладване на киберпрестъпленията, но най-често срещаните са:

- компанията се е справила с инцидента вътрешно;
- усещането, че полицията не може да направи нищо по въпроса;
- ограниченото доверие в полицията и нейната киберкомпетентност;
- киберинцидентът или кибератаката не са били толкова важни и/или не си е струвало да бъдат докладвани [11]

Испания

В Испания информацията за киберпрестъпленията и киберинцидентите се събира от Испанския национален институт за киберсигурност (INCIBE) на Министерството на вътрешните работи. Последните данни за частните компании сочат, че през 2021 г. INCIBE-CERT е работил по общо 109 126 инцидента, свързани с киберсигурността в Испания. Двете най-разпространени форми на киберпрестъпления са били зловреден софтуер (29,88%) и измама (28,60%), следвани от атаки срещу уязвими системи (18,9%) и непозволен достъп до данни (6,5%)).[12]

[7] CBS. (2021). Cybersecuritymonitor 2020. Central Bureau of Statistics.

[8] European Commission. (2022). *Op. cit.*

[9] Veenstra et al. (2015). Cybercrime among companies. Lectoraat Cybersafety: Leeuwarden

[10] CBS. (2021). Op. cit.; see also Veenstra et al. (2015). *Op. cit.*

[11] European Commission. (2022). *Op. cit.*; van de Weijer, S. et al (2021). Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context: The human factor in victimization, offending, and policing (pp. 303–325). Springer.*

[12] López Gutiérrez et al. (2022). Informe sobre la cibercriminalidad en España 2021. Ministry of Interior: Government of Spain.

Какво трябва да се предприеме

Познания в областта на киберсигурността е сред основните компетентности, които частните субекти (включително и физическите лица) следва да придобият с активната подкрепа на публичните институции и най-вече на правоприлагащите органи. Това е необходимо не само с цел повишаване на дигиталната грамотност, но и за подобряване на знанията на фирмите за това кои са компетентните органи, към които да се обърнат в случай на киберинциденти. Ефективните стратегии за поощряване на докладването на киберпрестъпления и оперативното сътрудничество следва да:

- обърнат внимание на общите причини за недокладване, сред които са липсата на доверие в полицията, сложността на механизмите за докладване, както и страховете на фирмите от прекъсване на бизнес процесите и приоритетизирането им за сметка на запазването на доказателствени материали за извършено киберпрестъпление.
- да се възползват от съществуващите инициативи и така да продължи прилагането и надграждането на съществуващите добри практики. Добър пример за такава практика е порталът No More Ransom, стартиран през 2016 г. от Европол и други партньори, за да подпомогне жертвите при декриптирането на техните устройства или електронни файлове. Подобна платформа и нейният набор от инструменти за декриптиране имат за цел да прекъснат бизнес модела на киберпрестъпниците, които предлагат на жертвите декриптиране срещу заплащане на откуп.
- насърчат докладването на киберпрестъпленията като основен елемент в борбата срещу киберпрестъпленията. Повишаването на докладването ще позволи да се хвърли светлина върху реалните мащаби на киберпрестъпността и в крайна сметка да се ограничи нейното (икономическо) въздействие върху частните субекти.
- въведат единен централизиран механизъм за докладване на киберинциденти и киберпрестъпления.

Първа стъпка за въвеждането на единен механизъм за докладване на киберинциденти следва да бъде хармонизиране на съществуващите механизми за докладване и установените публично-частни партньорства (ПЧП) за обмен на информация. Поощряването на докладването следва да е процес на изграждане на доверие, основан на ПЧП, сигурни и централизирани канали за комуникация, както и стандартизирани протоколи и формати за данни. Доверието между фирмите и правоприлагащите органи е от решаващо значение за насърчаването на съществуващи и нови партньорства и надеждни механизми за обмен на информация (включително защитени платформи), които в крайна сметка да засилят сътрудничеството между различните участници в борбата с киберпрестъпността.

.