Тренди кібербезпеки-2023:

Бойові дії в кіберпросторі між Росією та Україною — провідна тема в аналітичних звітах, проте старі «добрі» явища на кшталт фішингу, здирництва і DDoS теж ніде не поділися.

В Україні минулий рік розпочався з російських кібератак, і відтоді «бойові дії» в кіберпросторі не припиняються. Аналітики називають прикметним навіть не стільки саму кібервійну, як той факт, що на боці сторін виступають рядові, на позір не пов'язані з урядами держав хакери і активісти.

Війна в Україні посідає чільне місце в оцінках фахівців з кібербезпеки і профільних компаній, присвячених підсумкам 2022 року. Окрім того, у звітах фігурують все ті ж, що й останніми роками, наслідки пандемії і спричиненої нею форсованої цифрової трансформації, зростання кіберздирництва, атаки на IoT, використання обома сторонами інструментів машинного навчання.

«МтБ» вивчав, як оцінюють минулий рік експерти з кібербезпеки, і чого вони очікують від року 2023-го.

Російсько-українська кібервійна

Нині провідною темою для аналітиків кібербезпеки є російські атаки проти України, наша відповідь і вплив усіх цих подій на безпекову ситуацію у світі загалом. Усі погоджуються, що таких масштабних «бойових дій» у кіберпросторі досі не було.

Як писало у лютому видання Wired.com, дослідники з компаній ***ESET***, ***Fortinet*** і ***Mandiant*** (кібербезпекової фірми, що належить Google) незалежно встановили, що у 2022 році Україна зіткнулася з більшою кількістю різних програм-руйнівників (вайперів), ніж у будь-який рік кібервійни, яку веде Росія проти нашої держави. Дослідники порівнюють розмаїття зразків зловмисного коду в Україні з кембрійським вибухом. Вони знайшли зразки ПО, яке вражало машини не лише з Windows, але й з Linux, Solaris та FreeBSD, ці програми були написані різноманітними мовами і застосовували різні прийоми: псування таблиць розділів, використання команди SDelete, заміну вмісту файлів білим шумом тощо.

Компанія Fortinet за 12 місяців нарахувала в Україні 16 сімейств вайперів — раніше бувало по одному-два на рік. Такий обсяг може свідчити про те, що Росія кинула проти України величезну кількість розробників коду або ж сподівається створити масу нових варіантів, з якою не зможуть впоратися українські детектори. Fortinet також виявив, що це зростання числа вайперів, спрямованих проти України, може стати глобальною проблемою, адже зразки програм вже з'явилися у світових репозиторіях, і інструменти Fortinet зафіксували їх використання у 25 країнах.

Водночас дослідники зазначають, що, попри масштаб, кібератаки 2022 року проти України у деяких відношеннях були менш ефективними, ніж у минулі роки. Замість «шедеврів» зловмисного програмування, на створення яких ішли місяці, Кремль почав запускати грубі й примітивні інструменти знищення даних, позбавлені витончених механізмів самопоширення. Згідно з дослідженням ESET, у деяких випадках були навіть помічені ознаки поспіху. Наприклад, HermeticWiper, який було запущено перед самим вторгненням, використовував для проникнення вкрадений цифровий сертифікат, що є свідченням наперед спланованої операції, але пізніший його різновид, шифрувальних HermeticRansom, мав лише список з восьми імен і трьох простих паролів. За даними Mandiant, з травня минулого року ГРУ почало раз по раз засилати один і той же простий вайпер CaddyWiper, лише трохи змінюючи його код для обходу антивірусів.

Водночас продовжувалось нашестя нових різновидів вайперів — ESET лише з жовтня нарахував сім програм, які з'явились в Україні. Проте компанія не вбачає у цьому потоці якоїсь еволюції, скоріше йдеться про спроби продавити захист усіма можливими способами.

Check Point у своєму звіті *Cyber Security Trends* також зазначає, що, як у фізичній війні, росіяни вочевидь не готувалися до тривалої кіберкампанії. Їхні кібероперації, які на ранньому етапі включали ретельно сплановані високоточні атаки, практично припинились. Нині замість нових інструментів і вайперів кремлівські хакери запускають вже відомі інструменти і намагаються швидко використовувати будь-які можливості, які з'являються.

При цьому залучення обома сторонами фахівців, злочинців та інших цивільних осіб розмиває грань між державними акторами, кіберкриміналом і активістами. Зокрема, український уряд заснував армію хактивістів. Якщо раніше подібні утворення складалися просто з окремих хакерів, які ситуативно співпрацювали задля якоїсь мети, нині вони провадять вербування, навчання, розвідку, розподіл завдань і аналіз бойових дій, достоту як військові. Якщо досі напади на російські цілі вважалися табу, то нині Росія потерпає від безпрецедентної хвилі атак з боку державних груп, «політичних вояків» і злочинців. З іншого боку, численні угруповання хактивістів, які діють на боці Росії, атакують цілі не лише в Україні, а й у Європі, Північній Америці та Японії. Цікаво, що на мапі індексу загроз Check Point Україна має нижчий рівень небезпеки (40,9%), ніж Росія (43,9%).

У серпні минулого року сер Джеремі Флемінг, директор британського Центру урядового зв'язку, назвав український кіберзахист «імовірно, найбільш ефективною оборонною кібердіяльністю в історії». Check Point зазначає, що безперервні кібервійни між Росію та Україною зіграли роль тренувального періоду для обох сторін. Знання прийомів та інструментів супротивника є вкрай важливим, і хоча перше застосування того чи іншого вайпера може бути руйнівним, вдруге дія часто буває набагато слабшою. Наприклад, застосування програми Industroyer2 у березні 2022 року проти української енергосистеми мало обмежені наслідки порівняно з 2016 роком.

Вайпери, здирники, пенетратори

Атаки вайперів відбувалися не лише в рамках російсько-української війни. Check Point розслідував атаку на іранського державного телерадіомовника IRIB, яка сталася у січні минулого року. Тоді було вражено десятки комп'ютерів по всій країні, на телеекранах з'явилися портрети лідерів антиурядової організації MEK з побажаннями смерті аятоллі Хаменеї. У червні вайпер атакував металургійні заводи в Ірані, і були також інші інциденти, проте вони привернули менше уваги на тлі заворушень в країні.

У липні, за кілька днів до того, як MEK мала провести в Албанії «Світовий саміт вільного Ірану», місцева влада була змушена тимчасово закрити доступ до публічних сервісів та урядових сайтів через діяльність кіберзлочинців. Група хактивістів, яка взяла на себе відповідальність за атаки, дала зрозуміти, що це помста за акції проти Ісламської республіки. Саміт було скасовано, але це не завадило проіранським хакерам здійснити повторну атаку у вересні.

Загалом, пише Check Point, минулого року було застосовано більше вайперів, ніж за 30 попередніх, причому багатьом неурядовим угрупованням допомагають держави, аж до прямого управління і фінансування.

Що одним трендом є розвиток кіберздирництва і перетворення його на індустрію з багатьма учасниками, зокрема з використанням моделі «здирництво як послуга» (Ransomware-as-a-Service, RaaS). Розподіл ролей серед учасників ускладнює атрибуцію атаки і відстеження організаторів. Деякі здирники взагалі не використовують шифрування і вимагають гроші, шантажуючи просто витоком даних. Це дозволяє уникнути тривалої фази шифрування і зменшує ймовірність викриття. Також задля додаткового стимулювання вони можуть виходити на працівників, ділових партнерів і клієнтів своїх жертв (ці дії дістали назву «потрійне здирництво»). У жовтні минулого року, коли австралійська медична страхова компанія Medibank відмовилася сплатити викуп у розмірі $10 млн, здирники виклали в Інтернет масив конфіденційних даних, зокрема стосовно переривання вагітності, зловживання наркотиками та алкоголем, психічного здоров'я і т.д. Ще інші здирники замість шифрування даних просто знищують їх. Наприклад, угруповання Onyx, яке діє з квітня минулого року, видаляє усі файли, більші за 2 МБ.

Щоб уникати виявлення інструментами безпеки, злочинці вдаються до легітимних знарядь, зокрема використовують утиліти Windows для безфайлових атак. Іншим варіантом є спеціалізовані інструменти, які використовуються в тестах на проникнення (пентестах). Найпоширенішим з них є Cobalt Strike, вихідний код якого було злито у 2020 році, але оскільки засоби

ЗАМОВНИКИ ПОЧАЛИ УВАЖНІШЕ СТАВИТИСЬ ДО БЕЗПЕКИ

За останні роки, включно з роком широкомасштабного вторгнення, ми можемо бачити суттєве зростання кіберінцидентів у цілому, а також розповсюдження їх на усі сектори (державний; бізнес; об'єкти інфраструктури). Атаки стають більш складними та масштабними. З шаленим розвитком технологій ШІ, які можуть генерувати голос, зображення, відео і навіть код зловмисних програм, на нашу думку, збільшиться кількість спроб викрадення облікових даних та фішингових атак.

Помітна більшість замовників почала уважніше відноситись до безпеки в IT, тому що війна йде (і йде давно) в тому числі і в кіберпросторі. Замовники, які раніше категорично були проти хмарних рішень, почали більш лояльно ставитися до них. Крім цього, змінилось ставлення до загроз. Якщо до вторгнення було поширене більш формальне ставлення до систем безпеки («на папері» або з позиціонуванням «кому ми потрібні...».), то зараз є розуміння того, що загрози реальні і кожен може стати ціллю зловмисників. Через це замовники стали звертати більше уваги не лише на продукт як такий, а роблять акцент на такі якості продукту, як практичність використання, легкість роботи з ним, швидкість впровадження та якість підтримки.

Як компанія-дистриб'ютор продуктів та рішень кіберзахисту, ми бачимо запит в першу чергу на захист від DDoS-атак, інтенсивність яких значно зросла з початку широкомасштабного вторгнення.

Крім того, збільшилась зацікавленість до відстеження внутрішніх загроз. Бо, як би це не було прикро визнавати, в Україні до початку широкомасштабного вторгнення не було розуміння, що в нас є колаборанти та ті, хто «співчуває ворогу», і вони можуть завдавати шкоди зсередини компаній. На щастя, зараз це усвідомлює все більша кількість організацій. Саме тому ми бачимо підвищення інтересу до систем, що відслідковують внутрішні загрози. Особлива увага до рішень, що вимагають для обслуговування невеликої кількості персоналу. Через брак кваліфікованих спеціалістів ці рішення повинні бути максимально ефективними, автоматизованими та простими в використанні. Зараз такі рішення у своїй роботі використовують машинне навчання та штучний інтелект.

Микола МОЙСАК,
директор з продажів та розвитку бізнесу NWU

В цій сфері, на нашу думку, є ще простір для розвитку, бо до широкомасштабного вторгнення ця область була досить погано охоплена.

кіберзахисту дедалі частіше вміють його виявляти, у 2022-му хакери почали переходити на іншу програму — Brute Ratel. Зламана версія цього інструменту почала поширюватись у вересні 2022 року, що викликає особливе занепокоєння, адже Brute Ratel був розроблений колишнім пентестером з глибокими знаннями про інструменти виявлення і усунення загроз на кінцевих пристроях (EDR), а тому «заточений» для обходу EDR.

Загалом Check Point у 2022 році фіксував зростання числа кібератак проти цілей з усіх сфер економіки. Більшість були спрямовані проти освітніх та дослідницьких установ (2314 атак щотижня, на 43% більше проти 2021 року). На другому місці державний сектор і збройні сили (1661 атака на тиждень, + 46%). Найбільшого приросту атак (74%) зазнав сектор охорони здоров'я, де було 1643 атаки на тиждень; злочинці тримають цей напрям у фокусі уваги від початку пандемії COVID-19, і у минулому році 89% медичних організацій (клінік, лікарень і наукових інститутів) повідомили, що зазнали кібератак.

Це далеко не всі актуальні кіберзагрози. У березні компанія ***Lookout*** оприлюднила результати дослідження мобільного фішингу. Як з'ясувалося, минулого року він був на рекордному рівні: половина власників мобільних телефонів у світі кожного кварталу стикалася зі спробою фішингу. І це є продовженням тренду, який почався три роки тому. Мобільний фішинг є одним з найефективніших способів викрадення облікових даних, зазначає Lookout, додаючи, що, ймовірно, тут зіграв свою роль перехід до віддаленої роботи, який змусив роботодавців пом'якшити політику використання персональних пристроїв. Окрім того, доля мобільних користувачів, які у корпоративному середовищі переходять щороку по більш ніж шістьох шкідливих посиланнях, зросла з 1,6% у 2020-му до 11,8% у 2022-му, тобто стає все важче відрізнити зловмисні листи від легітимних.

Deloitte, опитавши понад 1100 топ-менеджерів та інших представників організацій, повідомляє: 34,5% респондентів впродовж 12 місяців зафіксували атаки кіберзлочинців на фінансові та бухгалтерські дані їхніх організацій. В межах цієї групи 22% зазнали принаймні одного кіберінциденту, і 12,5% зазнали двох. Майже половина (48,8%) респондентів очікують, що впродовж нинішнього року число і масштаб кібератак зросте, водночас лише 20,3% оцінили, що їхні бухгалтерські та фінансові служби тісно співпрацюють з відділами кібербезпеки.

Кіберзахист потрібен усім

Щоб дізнатися на ситуацію з кібербезпекою в Україні на другий рік великої війни, ми зробили власне міні-опитування, звернувшись до дев'ятьох компаній — дистриб'юторів, системних інтеграторів і дата-центрів. Зокрема, ми поцікавилися, як вони зустріли російське вторгнення і як змінилися потреби замовників. Як з'ясувалося, компанії виявилися більш-менш готовими до форс-мажору, бо пристосувалися до віддаленого режиму роботи за час пандемії. І хоча певна частина була змушена призупинити роботу, вже за місяць вони повернулися до більш-менш звичної діяльності. Чотири компанії повідомили, що насправді вони навіть збільшили штат.

Отже, компанія ***iIT Distribution*** (***iITD***) відновила роботу в березні. Багато виробників, з якими вона співпрацює, погодились надавати свої рішення безплатно для компаній державного

СЛІД ЧЕКАТИ ПОСИЛЕННЯ КІБЕРВІЙНИ

На початку війни відбувались масові DDoS-атаки на бізнес та інфраструктуру. А наприкінці 2022 року переважали цілеспрямовані та синхронізовані атаки на критичну інфраструктуру та енергетичну систему. Загалом атаки розпочинаються за день до ракетних обстрілів. Також вони здійснюються у вихідні дні, коли бізнес менш готовий. Тобто вони характеризуються системністю: ворог поєднує «фізичні» удари з DDoS-атаками на інфраструктуру, аби завдати якомога більшої шкоди певному сектору економіки.

На початку війни зловмисники приховували напрямки атак. Вони здійснювалися, як правило, з Венесуели, Бразилії та Індії. Сьогодні зловмисники перестали шифрувати шляхи атак. Крім того, значна частина DDoS-атак припадає на український сегмент – UA IX. До атак почали приєднуватися бот-мережі та заражені комп'ютери всередині України.

У 2022 році Україна зазнала великої кількості атак на критичну інфраструктуру та бізнес. Лише через три дні після російського вторгнення кількість кібератак на державно-військовий сектор зросла на 196% в порівнянні з 2021 роком. «Антирекордом» окупантів стали 275 DDoS-атак на день.

Проте відповідь української кіберармії потужна. Кількість DDoS-атак на інфраструктуру окупантів у 2022 рік перевищила показники 2021 року на 700%. Загалом було зафіксовано 1,26 мільйона DDoS-атак на критичні об'єкти окупантів. Для порівняння: це 8,4% від усієї кількості DDoS-атак у світі. В результаті Росія зайняла четверте місце в рейтингу найбільш атакованих країн світу за результатами 2022 року.

На початку кібервійни зловмисники зазвичай застосовували атаки рівня L3 та L4 – тобто на рівні інфраструктур. Метою таких атак є перевантаження пропускної спроможності мережі чи застосунків. Також часто вдавалися до large DDoS-атак, тобто атак з великим обсягом трафіку. Починаючи з другого півріччя 2022 року і до сьогодні війна на кіберфронті стала більш «витонченою». Хакери почали частіше застосовувати атаки рівня L7 – інтелектуальні атаки. Вони направлені на знаходження «слабких» місць в IT-інфраструктурі компанії. Ймовірно, що така тенденція збережеться і надалі.

За нашими прогнозами, кількість DDoS-атак зростатиме, особливо в кінці першого та другому кварталі 2023 року. Зловмисники будуть посилювати «кіберудари», зважаючи на невдачі на фізичному фронті.

Назарій КУРОЧКО,
засновник групи компаній GIGAGROUP

Ту саму тенденцію вбачають і західні ЗМІ. Нещодавно американська медіаорганізація Politico закликала Україну готуватися до нового етапу кібервійни з Росією. На думку експертів, нова фаза розпочнеться в період поновлення контрнаступу на східні регіони України.

Цілями атак залишатиметься критична IT-інфраструктура, в тому числі державні органи. На нашу думку, ймовірне зростання кіберзагроз з використанням malware, атак вірусами-шифрувальниками, що призведе до зростання витоків корпоративних та персональних даних. Також не варто забувати про традиційні типи мережевих DDoS-атак, зокрема TCP та UDP-флуд.

та приватного секторів, зокрема замовники мали можливість отримати пробні ліцензії рішення анти-DDoS від A10 Networks на необхідний термін. Хоча деякі компанії неохоче приймали допомогу, побоюючись невідповідності вимогам, більшість привітала цю пропозицію, розуміючи, що перед лицем величезних кіберможливостей ворога не час думати про відповідність.

Компанія ***NWU*** змогла зберегти структуру офісу і швидко налагодити віддалену роботу. В перші місяці після вторгнення дистриб'ютор зосередився на допомозі країні: організовував «безкоштовні» поставки, вів перемовини з виробниками щодо допомоги українським замовникам тощо. Повноцінну роботу було відновлено влітку минулого року.

Ще один дистриб'ютор, ***«Оберіг IT»***, з 25 лютого 2022 року також активно займається волонтерством, допомагаючи замовникам з державного та комерційного секторів за підтримки виробників, які «без розмов» надають можливість безкоштовно активувати рішення ІБ та IT-моніторингу та повноцінно їх використовувати на необхідний час в інфраструктурах кінцевих користувачів. Компанія повідомила, що хоча одразу після вторгнення було певне «замороження» ринку, вже за кілька тижнів запитів стало більше, ніж будь-коли раніше, адже всі усвідомили нову реальність і навіть «відкладені потреби» почали реалізовуватись підвищеним темпом.

Дистриб'ютор ***ELKO Ukraine*** відновив роботу з кінця березня 2022 року, зберігши всю команду спеціалістів. Завдяки досвіду, набутому під час пандемії COVID-19, компанія була технічно готовою до віддаленого формату роботи у складних умовах, які змінювалися кожного дня, і мала налагоджені інфраструктуру та процеси. Що цікаво, компанія зауважує: у замовників кібербезпека була на особливому, але не головному місці, бо українські компанії перш за все дбали про безпеку своїх працівників, а збереження матеріальних цінностей було на другому плані.

«Мегатрейд» також зауважує, що для багатьох компаній виникла необхідність перевести офіси та/або склади до інших регіонів країни, а також деякі з них були змушені переводити дані за кордон, оскільки забезпечення безпеки даних в Україні було ризикованим або неможливим. У зв'язку з переходом на дистанційну роботу підвищилось усвідомлення необхідності кібербезпеки, набагато більше уваги було приділено навчанню працівників знанням про кібербезпеку, впровадженню процедур реагування на кібератаки та інших заходів для забезпечення безпеки даних.

Підвищений попит на рішення з кібербезпеки після початку широкомасштабного вторгнення зафіксувала і компанія-інтегратор ***Wise IT***, яка також змогла швидко

НАЙБІЛЬША ЗАГРОЗА — ЛЮДСЬКИЙ ФАКТОР

У найближчому майбутньому технології кіберзахисту та підходи до нього будуть продовжувати розвиватись і змінюватися. Це пов'язано з динамічними змінами у загрозах, які виникають у сфері кібербезпеки.

По-перше, зростають ризики кібератак та злочинної діяльності в онлайн-середовищі. У зв'язку з цим компанії, уряд та інші організації мають забезпечити надійний захист своїх мереж та інформації від кіберзлочинців. Це вимагає розробки та впровадження новітніх технологій кіберзахисту, щоб виявляти та відбивати кібератаки швидше та ефективніше.

По-друге, зростає значущість кібербезпеки в глобальному масштабі. Кібератаки стають все більш проникливими та витонченими, що може призвести до серйозних наслідків для економіки та безпеки держав. У зв'язку з цим міжнародні організації та уряди шукають нові шляхи співпраці та координації в галузі кібербезпеки, в тому числі створення міжнародних стандартів та спільних стратегій.

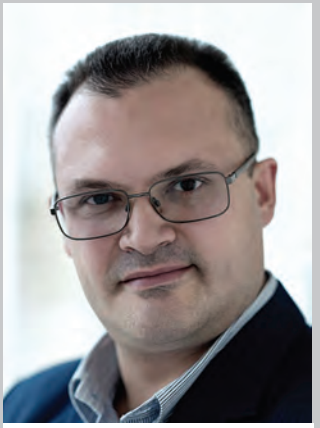
Третє — але, на мою думку, чи не найважливіше, — зростає значущість ролі людини у кіберзахисті. Багато кібератак починаються зі спаму, фішингу та інших соціально-інженерних методів, що використовують людські помилки. Тому компанії та уряди повинні вдосконалювати свої програми навчання та обізнаності про кібербезпеку, щоб знизити ризик успішної кібератаки через помилки персоналу.

Основними напрямки розвитку технологій кіберзахисту я бачу:

1. Біометричні технології. Сканери відбитків пальців, розпізнавання обличчя, клавіатурний почерк тощо можуть забезпечити точнішу ідентифікацію користувачів та більшу безпеку для даних, забезпечити захист від кібератак, що базуються на викраденні або підробленні паролів та інших форм аутентифікації.

2. Zero trust. Розширення застосування облікових записів з багатофакторною аутентифікацією. Багатофакторна аутентифікація зменшує ризик несанкціонованого доступу до даних.

3. Розробка кіберзахисту на основі хмарних технологій: вони дозволяють розгортати інфраструктуру кібербезпеки та управляти нею, що забезпечує більш ефективний та безпечний захист даних та інформації.



Павло ЛІСОВСЬКИЙ,
керівник напрямку дистриб'юції ПЗ «Мегатрейд»

4. Розробка кіберзахисту для Інтернету речей: з поширенням IoT потрібні більш потужні заходи безпеки, щоб запобігти кібератакам на пристрої з підключенням до Інтернету, які використовуються в побутовій електроніці, медичній техніці, автомобілях тощо.

5. Розвиток захисту від розподілених атак (DDoS): зростання кількості DDoS-атак за останні кілька років вимагає нових технологій для виявлення та захисту від них.

6. Застосування штучного інтелекту та машинного навчання для виявлення загроз. Це дозволить швидко виявляти та реагувати на нові загрози та атаки, а також зменшувати кількість людських помилок. Машинне навчання дозволяє аналізувати великі обсяги даних та знаходити закономірності, що можуть вказувати на аномальну поведінку в мережі.

перелаштуватись і зберегти штат, а згодом і збільшити його.

ТОВ «АМ Інтегратор Груп» вже пройшло через одну релокацію, у 2014 році переїхавши з Донецька до Маріуполя, тому 24 лютого не заскочило компанію зненацька. На той час більшість корпоративних даних давно було перенесено в хмарне середовище з забезпеченням функцій захисту, контролю доступу, резервування тощо. На початку великої війни компанія вирішувала два завдання: врятувати співробітників, які опинилися в окупації (у тому числі в Маріуполі) та допомогти персоналові психологічно повернуться до робочого стану.

«АМ Інтегратор Груп» повідомляє, що багато клієнтів впровадили режим економії до кінця війни, проте ті, які все ж провадять закупівлі, роблять значно більший наголос на кібербезпеку. За минулий рік компанії довелось як відновлювати пошкоджені об'єкти, так і допомагати партнерам з переміщенням IT-інфраструктури окремих філій та цілих підприємств, локалізованих на окупованих територіях (у тому числі з використанням ЦОДів в мобільному та модульному виконанні), організовувати захищений віддалений доступ для співробітників, які були переміщені або виїхали з країни, закривати вразливості інформаційної інфраструктури.

Група компаній ***GIGAGROUP***, до складу якої входять телеком-оператор GigaTrans, дата-центр GigaCenter та хмарний оператор GigaCloud, мала план безперервності бізнесу (business continuity planning), що допомогло спланувати і скоригувати дії. В перші місяці війни здійснено релокацію на захід України, хоча частина фахівців лишилася в Києві, щоб обслуговувати IT-інфраструктуру клієнтів та самої компанії. На сьогодні 85–90% персоналу повернулися до столиці.

GIGAGROUP зауважує, з посиланням на результати власного опитування, що серед клієнтів дата-центру GigaCenter понад 58% компаній приділили увагу резервуванню та захисту корпоративних даних (завдяки хмарним сервісам, бекапуванню інформації в іншому ЦОДі та моніторингу трафіку). З початку 2022 року близько 60% клієнтів хмарного оператора GigaCloud зробили або перемістили резервні копії своїх проєктів до західних зон доступності — Львова та Варшави. Завдяки дата-центрам у ЄС та на заході України, а також наявності кількох майданчиків у Києві фахівці будують хмарні рішення без єдиних точок відмови, а клієнти створюють зарезервовану інфраструктуру, рознесену географічно.

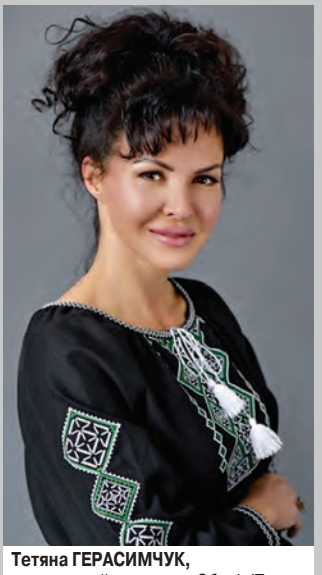
Дата-центр ***«Парковий»*** «з фундаменту» спроєктований у відповідності з рівнем захисту TIER III від Uptime institute, тож минулий рік також виявився стрес-перевіркою алгоритмів на випадок екстреної ситуації. У перші півроку після вторгнення з'явилася хвиля запитів на катастрофостійкі рішення, такі як захист від DDoS-атак, Firewall, WAF, бекапування (BaaS), аварійне відновлення послуг (DRaaS). Ці запити компанія задовольняє по сей день. Для державного сектору на базі меморандуму з НКЦК компанія

ВОРОГ ГОТУВАВ КІБЕРАТАКИ ЗАЗДАЛЕГІДЬ

Кіберпростір розвивається дуже динамічно. Постійно виникають нові сервіси та високотехнологічні рішення, які надають споживачам нові можливості. Але чим складніша система, тим більше у неї може бути вразливостей або недокументованих функцій, котрі можна використати для реалізації кібератаки. І це не якісь навмисно залишені «бекдори» – мова саме про те, що через високу складність і розгалуженість дуже складно зробити «абсолютно безпечний» продукт, все одно може знайтись помилка... Тому дуже важливим питанням була і залишається саме реалізація комплексного, системного підходу до забезпечення кібербезпеки.

Атаки стали більш продуманими і заздалегідь спланованими. Якщо кілька років тому достатньо було використовувати стандартні методи захисту, такі як антивірусний захист кінцевих користувачів, серверів, захист поштового та веб-трафіку, то зараз цього вкрай недостатньо. Зважаймо й на те, що зараз відбувається тенденція зміни підходу роботи з інформацією – міграція даних та сервісів у хмарне середовище, відповідно змінюються й підходи до захисту.

Під час війни насамперед слід очікувати атак, спрямованих на шпигування, на порушення працездатності критичної інфраструктури і фінансового сектору, онлайн-сервісів компаній. Відбувається закономірне зміщення акцентів кіберзагроз на безпосереднє завдання шкоди, без будь-яких «комерційних» складових. Стрімко зросла кількість і потужність досить простих, але небезпечних DDoS-атак (тобто на відмову в обслуговуванні), атак вірусів-шифрувальників. Зараз Україна доволі успішно протистоїть усім викликам у кіберпросторі, і хоча інциденти все одно трапляються, загалом кібербезпека і державних установ, і приватних компаній була «на висоті». І надалі лише продовжує посилюватись.



Тетяна ГЕРАСИМЧУК,
генеральний директор «Оберіг ІТ»

Ми впевнені, що так само, як і повномасштабне вторгнення, плани кібератак готувались ворогом заздалегідь, і тому найбільша активність таких атак припала на перші дні нападу. Використовуючи DDoS як відволікаючий маневр, зловмисники намагалися проникати в інфраструктури компаній, щоб заподіяти максимальної шкоди. На жаль, неможливо провести об'єктивну оцінку щодо того, «вдало чи не вдало» відбиваються атаки, без детального обстеження стану справ в тій чи іншій компанії після нападу: все залежить від співвідношення рівня і ресурсів злочинців до рівня захисту і використання технологій та внутрішніх процесів структур інформаційної безпеки компаній-жертв.

проводить роботи з провадження Security-рішень та організовує захист даних у тісній кооперації з РНБО та партнерами з системної інтеграції.

З кінця 4 кварталу 2022 року та на початку першого кварталу 2023-го, під час загострення атак на енергетичну інфраструктуру України компанія фіксувала значне зростання числа запитів на розміщення серверного обладнання у дата-центрі. «Парковий» мав змогу працювати безперебійно з максимальним завантаженням до 10 днів до першої зовнішньої заправки дизель-генераторів, при цьому витрати на пальне та обслуговування ДГУ не додавались до рахунків абонентів.

Український кіберландшафт: загрози і засоби захисту

Ми запитали у компаній, як змінився ландшафт кіберзагроз в Україні з початком широкомасштабного російського вторгнення і які типи загроз нині домінують **(рис. 1)**. Майже всі респонденти, виходячи з запитів своїх клієнтів, згадали про DDoS-атаки, яких стало набагато більше. Вони спрямовані на державні органи, енергетичну та іншу критичну інфраструктуру, а також на бізнес. По чотири компанії відзначили застосування фішингу та інших прийомів соціальної інженерії, а також спроби крадіжки та руйнування даних. Три компанії віднесли до поширених загроз атаки шифрувальників (кіберздирників). Згадувались і загрози, які можна назвати характерними саме для воєнного часу: небезпека з боку власних співробітників, які можуть співчувати ворогу, кібероперації з метою збору даних (не лише про Україну, але й про наших союзників), а також дії з метою поширення дезінформації.

Рис. 1. Кіберзагрози, що набули найбільшого поширення з початком широкомасштабного російського вторгнення

Респонденти розділилися в питанні, чи вдало Україна відбиває ворожі кібератаки: 4 компанії відповіли, що вдало, 3 — що наша країна не є повністю захищеною і в цьому напрямку ще є куди розвиватися.

Щодо ландшафту загроз загалом у розрізі останніх кількох років, то тут відповіді були більш розмаїтими **(рис. 2)**. Чотири компанії назвали загрозою саме по собі збільшення числа кібератак, їх складності та масштабу, зростання різноманітності шкідливого ПО, а також те, що атаки стають більш продуманими, і для захисту від них стандартного набору інструментів вже недостатньо. Також чотири компанії відзначили вдосконалення здирницьких програм

ДЕЛЕГУВАННЯ КІБЕРБЕЗПЕКИ ДАТА-ЦЕНТРАМ — НЕОБХІДНІСТЬ У 2023 РОЦІ

Впродовж останніх декількох років нами фіксуються такі патерни кіберзлочинів, як DDoS-атаки (які з часом тільки посилюються), DoS-атаки, фішинг, атаки на web-застосунки. На додачу простежується тенденція переходу від простих DoS-атак і програм-вимагачів, які застосовуються з метою отримання фінансової вигоди, до замаскованих під звичайних вимагачів програм, покликаних зруйнувати усі дані та IT-інфраструктуру підприємства або отримати внутрішні дані клієнтів для їх подальшого продажу.

Зараз зрозуміло, що кількість кіберзагроз будь-якого рівня в Європі та в післявоєнній Україні буде тільки зростати. А з ними і бюджети на забезпечення роботи цього напряму бізнесу. До майбутніх загроз вже сьогодні слід бути готовим компаніям-провайдерам програмного забезпечення та систем зберігання даних, які надають свої послуги урядовому сектору, банківській та телеком-індустріям.

У перші дні повномасштабного вторгнення державі та компаніям допомогла IT-стратегія, яка передбачала переведення даних у хмару та партнерство із західними компаніями. Також у лютому минулого року Україна разом з урядовим сектором перенесла в резервні копії стільки даних, скільки було можливо організаційно. На цьому важливому етапі основними завданнями для «Паркового» були бекапи клієнтів на партнерський майданчик країн ЕС, копіювання хмари та інфраструктури, налаштування гібридної інфраструктури вже існуючим клієнтам, які розміщували на зберігання своє обладнання, резервні копії (BaaS) та аварійне відновлення послуг (DRaaS). Це дає змогу компаніям-партнерам протистояти кіберзагрозам на найвищому рівні.

Нами прогнозується збільшення зацікавленості від урядового сектору у хмарних сервісах українських дата-центрів, оскільки європейські дата-центри від західних партнерів цього року закінчать свою грантову програму на безкоштовне обслуговування українських компаній.

Володимир ПОКАТІЛОВ,
директор дата-центру «Парковий»

Також логічно припустити, що через постійну загрозу нових кібератак дані урядового сектору, телекому, ритейлу та банків будуть у перманентній небезпеці. Це, в свою чергу, є каталізатором для переосмислення діючих інструментів кіберзахисту та запровадження додаткових механізмів захисту корпоративних даних, надійними провайдерами яких є і будуть найбільші українські дата-центри.

Вже зараз зрозуміло, що клієнтам з урядового і приватного сегментів економічно та організаційно не вигідно тримати штат спеціалістів з кіберзахисту. Перед усе більшою кількістю компаній постає вибір делегування кіберзахисту провайдерам, які на цьому спеціалізуються. Тому «Парковий» має в арсеналі модель SECaaS (Security as a service), яка буде й надалі мати попит у різного рівня клієнтів.

і поширення таких, що шифрують не лише дані, а й їхні резервні копії, і розповсюдження явища RaaS. По три компанії назвали серед загроз зростання фішингу та DDoS-атак. Стільки ж вказали на кібершпигунство і атаки з боку хакерів, спонсорованих державами, і атаки на критичну інфраструктуру та фінансовий сектор. Зміни, спричинені COVID-19, призвели до зростання атак на користувачів, що працюють віддалено, а цифрова трансформація — атак на хмарні сервіси і розподілені системи. Також відзначають використання штучного інтелекту в злочинних цілях — для підготовки фішингових повідомлень, а також для підготовки більш складних і ефективних кібератак.

Рис. 2. Кіберзагрози, які набули найбільшого поширення впродовж останніх 2–3 років, і яких слід очікувати у найближчому майбутньому

Ми поцікавились, які технології та рішення кіберзахисту найбільш популярні серед українських замовників **(рис. 3)**. Вони в цілому корелюють з ландшафтом найпоширеніших загроз. Тут на першому місці традиційні антивірусні програми, але не лише вони, а й інструменти EDR і їхня розширена версія XDR, які також збирають дані в мережі і у хмарі. Так само респонденти виділили рішення для захисту від DDoS. Три компанії назвали рішення для захисту від витоків даних (DLP). На такому

ж рівні популярності технології для контролю доступу (Access Control Management — ACM) і управління привілеями доступу (Privileged Access Management — PAM), які регулюють дії, що їх користувачі можуть виконувати в системі.

Ще три голоси набрали рішення класу Deception (приманки), які відволікають зловмисників від реальних цілей і дозволяють швидко виявляти спроби реалізації загроз, а також пісочниці, які створюють ізольоване середовище і запобігають прориву всередину мережі. Також важливі інструменти автоматизації кіберзахисту, зокрема SIEM/SOAR, які дозволяють не лише прискорити процеси і скоротити кількість людських помилок, а й зменшити ризики, спричинені віддаленою роботою і втратою персоналу. Респонденти відзначили важливість збільшення обізнаності користувачів щодо кібербезпеки і навчання персоналу на гіперреалістичних імітованих атаках.

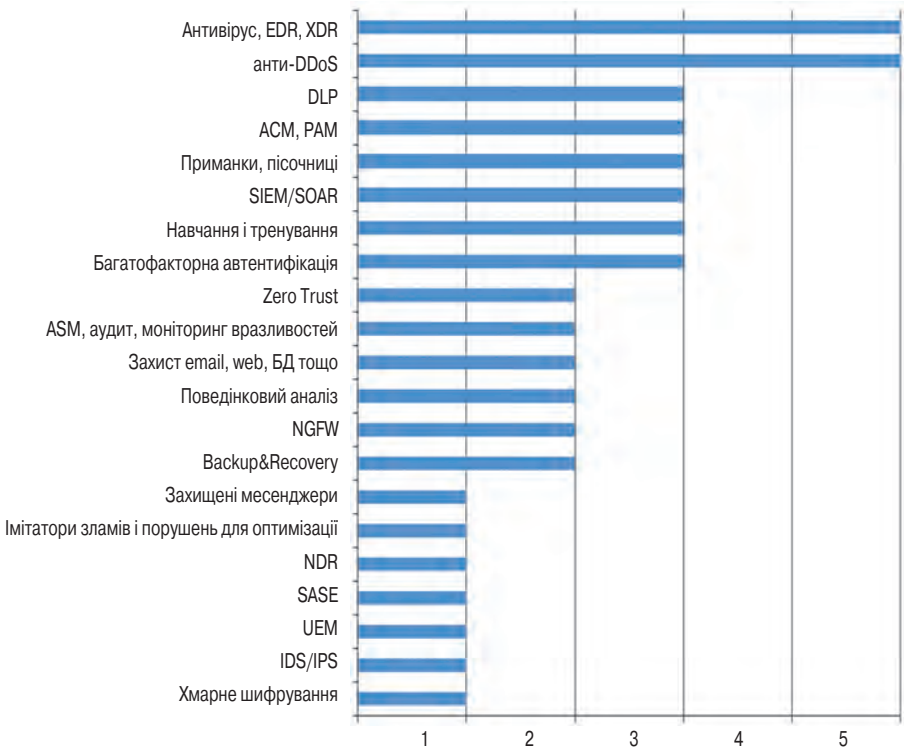


Рис. 3. Технології кіберзахисту, найбільш затребувані серед українських компаній

Відповідаючи на питання про те, як зміняться технології та підходи до кіберзахисту в найближчому майбутньому **(рис. 4)**, респонденти насамперед вказали на впровадження штучного інтелекту, машинного навчання та Big Data, адже ці механізми здатні швидко виявляти та знешкоджувати нові загрози, зменшують кількість людських помилок, а загалом дозволяють автоматизувати процеси або й навіть замінити людей. Чотири компанії вважають, що розвиватиметься напрямок захисту хмарних та гібридних середовищ, а також, навпаки, інструменти кіберзахисту на основі хмарних технологій. З одного боку, оскільки все більше організацій переміщують свої IT-активи до хмари, їм потрібні механізми захисту цих активів, а з іншого, хмарні технології забезпечують ефективніший захист інформації.

Рис. 4. Технології та підходи кіберзахисту, які будуть актуальними у найближчому майбутньому

Дві компанії вказали на важливість захисту пристроїв IoT (побутової техніки, автомобілів, медичного обладнання тощо). Зокрема, цей тренд чекає і на нас з появою мереж 5G, оскільки в країнах, де вже є зв'язок п'ятого покоління, загрози таким пристроям вже вважаються повсякденною реальністю. Також дві компанії згадали концепцію «нульової довіри» (Zero Trust) і багатофакторної автентифікації.

Якщо ж поглянути, які тренди розвитку технологій кіберзахисту розглядають у світі, то тут, окрім AI/ML і Zero Trust, називають ще цікаві речі. По-перше, це апаратна автентифікація за допомогою смартфона чи будь-якого іншого пристрою, що належить користувачу. Апаратна автентифікація усуває потребу мати логін і пароль, хоча з'являється інша небезпека — втрати чи крадіжки пристрою. Блокчейн для розподіленого зберігання даних, поведінковий аналіз для відстеження підозрілих дій, контекстуальний захист для забезпечення доступу на основі багатьох даних, — ці технології вже використовуються або набуватимуть поширення в кіберзахисті найближчим часом.

Василь ТКАЧЕНКО, **МтБ**