УДК 007.3+331.108.45+331.445+658.5.011
DOI https://doi.org/10.32689/maup.it.2023.3.3

Станіслав ГОРБАЧЕНКО
доктор економічних наук, професор, завідувач кафедри кібербезпеки Національного університету "Одеська юридична академія", вул. Рішельєвська, 28, Одеса, Україна, індекс 65045 (stasgorbachenko@gmail.com)
ORCID: 0000-0001-8442-9581

Віктор БОЙКО
кандидат технічних наук, доцент кафедри кібербезпеки Національного університет "Одеська юридична академія", вул. Рішельєвська, 28, Одеса, Україна, індекс 65045 (boyko-work@ukr.net)
ORCID: 0000-0001-5929-657X

Stanislav HORBACHENKO
Doctor of Economic Science, Professor, Head of the Department of Cybersecurity at National university "Odesa Law Academy", 28 Rishelievskaya, Odesa, Ukraine, postal code 65045 (stasgorbachenko@gmail.com)

Victor BOYKO
Candidate of Technical Sciences, Senior Lecturer at the Department of Cybersecurity at National university "Odesa Law Academy", 28 Rishelievskaya, Odesa, Ukraine, postal code 65045 (boyko-work@ukr.net)

Бібліографічний опис статті: Горбаченко, С., Бойко, О. (2023). Тестування на проникнення як ефективний інструмент менеджменту кібербезпеки. *Інформаційні технології та суспільство*, 3, 23–29. DOI: https://doi.org/10.32689/maup.it.2023.3.3

Bibliographic description of the article: Horbachenko, S., Boyko, O. (2023). Testuvannya na proniknennya yak efectivniy instrument manajmentu kiberbezpeki [Penetration testing as an effective tool for cybersecurity management]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 3, 23–29. DOI: https://doi.org/10.32689/maup.it.2023.3.3

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ЯК ЕФЕКТИВНИЙ ІНСТРУМЕНТ МЕНЕДЖМЕНТУ КІБЕРБЕЗПЕКИ

Анотація. *В статті розглянуто теоретичні аспекти розбудови та функціонування системи управління, спрямованої на захист комп'ютерних систем, мереж, даних, та інформації підприємства чи організації від кіберзагроз. В кінцевому рахунку вказана система має трансформуватися у менеджмент кібербезпеки. Останню категорію визначено як процес планування, розробки, впровадження та керування заходами, які спрямовані на захист комп'ютерних систем, мереж і даних від наявних та потенційних кіберзагроз. Виявлено, що основні функції класичного менеджменту, а саме, планування, організування, мотивування та контроль, відповідають і завданням менеджменту кібербезпеки.*

Серед конкретних інструментів які має використовувати менеджмент кібербезпеки виокремлено моніторинг подій, моніторинг мережі, інтрузійне виявлення, системи виявлення аномалій, етичний хакінг тощо.

Зроблено висновок, що поряд з безпосередньо технічними питаннями, істотну частину проблем сучасного кіберзахисту підприємств та організацій спричиняє «людський фактор». Відтак однією з нагальних проблем у цій галузі, поряд із загальним підвищенням технічної грамотності та підготовленості персоналу, є підтримання високого рівня корпоративної пильності та алертності.

З огляду на це, як один з ефективних інструментів підвищення рівня пильності та алертності персоналу, в статті пропонується використовувати процедуру тестування на проникнення у формі Cyber Red Team, при якій тестування виконується зовнішньою командою. Доведено, що тестування на проникнення сприяє розумінню з боки персоналу факту, що вторгнення може здійснюватися різними шляхами, а кіберризики є об'єктивною реальністю. В результаті запропоновано практичні рекомендації щодо проведення пентестів, які мають забезпечити збільшення ефективності та результативності менеджменту кібербезпеки на рівні окремих підприємств та організацій.

Ключові слова: *кіберзахист, менеджмент кібербезпеки, контроль, алертність, тестування на проникнення.*

PENETRATION TESTING AS AN EFFECTIVE TOOL FOR CYBERSECURITY MANAGEMENT

Abstract. *In the modern information environment, special attention is paid to cyber security issues. The growing threat of cyber attacks and unauthorized access to computer systems, networks, data and information of enterprises and organizations presents them with the task of effective cyber security management. Accordingly, the article examines the theoretical aspects of the development and functioning of the management system aimed at protecting against cyber threats.*

One of the key concepts is the transformation of this system into cyber security management. It has been studied that the classical functions of management – planning, organization, motivation and control – are properly correlated with the tasks of cyber security. This allows for an integrated approach to cyber security management, providing effective protection against cyber threats.

Paradoxically, the cornerstone of modern cyber defense is the "human factor". It was found that, in addition to technical aspects, an important role in ensuring cyber security is played by the preparedness and awareness of personnel. Therefore, increasing technical literacy and corporate vigilance become extremely important tasks.

In this context, the article suggests the use of a penetration testing procedure known as the Cyber Red Team. According to this concept, an expert team conducts testing using external methods, carrying out attacks on the system, which allows identifying weak points and gaps in cyber defense.

Finally, the article provides practical recommendations for conducting pentests aimed at improving the effectiveness of cyber security management at the level of individual enterprises and organizations. These measures will contribute to improving the level of vigilance and alertness of personnel, which is an important step in ensuring a high degree of cyber security.

In conclusion, the article highlights the current aspects of the development of the cyber security management system, focusing on the importance of the "human factor" and proposing innovative approaches to increasing the level of cyber security at enterprises and organizations.

Key words: *cybersecurity, cybersecurity management, control, alertness, penetration testing.*

Постановка проблеми у загальному вигляді. Безпека, в різних її проявах, має для сучасного менеджменту велике значення, оскільки дозволяє зменшити ризики втрати активів, порушення операцій, втрати довіри клієнтів і репутації, а також може допомогти підприємству чи організації бути більш стійкими та успішними в непередбачуваних умовах. Серед складових безпеки чільне місце займає інформаційна безпека, тобто захист інформації, даних, конфіденційної інформації та інтелектуальної власності від несанкціонованого доступу, втрати або викрадення.

У свою чергу розвиток інформаційних технологій призвів до повноцінного відокремлення від інформаційної безпеки кола питань пов'язаних із захистом комп'ютерних систем, мереж, даних, програмного забезпечення та інформації від кіберзагроз, кібератак, зловмисних дій та несанкціонованого доступу, тобто, напряму кібербезпеки. На макрорівні кібербезпеку розглядають як найважливішу складову національної та економічної безпеки, адже від початку повномасштабної війни кіберзагрозам підлягають, в першу чергу, об'єкти критичної (промислової та міської) інфраструктури. Атаки таких об'єктів можуть завдавати значних збитків, до того ж часто їхнє технічне та організаційне оснащення або відстає, або знаходиться в процесі оновлення та перебудови.

В процесі побудови системи кіберзахисту суттєву роль завжди відіграє «людський фактор», оскільки будь-який недбалий і недосвідчений співробітник (або, ще гірше – управлінець) здатний звести нанівець заходи технічного характеру. З огляду на це серед інструментів менеджменту кібербезпеки, спрямованих на підготовку співробітників (та й всієї організації в цілому) до можливих вторгнень чи не найважливіше місце займає тестування на проникнення.

Аналіз останніх досліджень і публікацій. Навіть в умовах загального розуміння в науковому середовищі важливості досліджень в сфері забезпечення кіберзахисту, на практиці основна увага зосереджується на, так званій, SHN-тріаді («software-hardware-network»). В цьому сенсі можна, зокрема, виділити наукові праці Дж. Боема, П. Меррата, Л. Шентона, А. Самнера, Х. Алдавуда, Дж. Скіннера, В. Бенсона, Д. Боссарта, С. Ванга та інших. Деякі із зазначених авторів доречно вказували на зростання кількості випадків використання інструментів соціальної інженерії для здійснення вторгнень і важливість відповідної роботи з персоналом. Однак саме управлінському аспекту формування ефективної системи кіберзахисту все ще приділяється недостатньо уваги.

Формулювання мети статті. Мета даної статті полягає в аналізі та обгрунтуванні ефективності тестування на проникнення як ключового інструменту в області менеджменту кібербезпеки. Досліджено основні аспекти та переваги застосування тестування на проникнення, включаючи його вплив на виявлення потенційних вразливостей, забезпечення недоступності для зловмисників, та зниження ризиків кібератак. Також, стаття має на меті надати читачам практичні рекомендації щодо впровадження та оптимального використання тестування на проникнення для підвищення рівня кібербезпеки в організаціях.

Виклад основного матеріалу. Вагомість проблематики кібербезпеки підтверджується тим, що протягом 2022 року на Україну було здійснено понад 7 тис. кібератак що у 2,8 разів більше, ніж у 2021 році. Серед опрацьованих протягом 2022 року фахівцями CERT-UA 2194 кіберінцидентів 120 стосувалися фінансового сектору, 156 – комерційних організацій та 92 – сектору телекомунікацій і розробки програмного забезпечення. Крім того за результатами 2022 р. Україна займає 2 місце серед найбільш атакованих країн світу після США [1].

В огляду на наявність вищевказаних проблем на державному рівні основним завданням кібербезпеки виступає захист життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2].

В той самий час для окремих підприємств та організацій кібербезпека – це сукупність заходів, процедур, стратегій та політик, спрямованих на захист від ризиків, загроз і небезпек, що спричиняються кіберсередовищем і можуть впливати на операції, активи, працівників, імідж, фінансовий стан, репутацію тощо.

Забезпечення ефективного кіберзахисту потребує не тільки сучасних технологічних рішень, а й відповідної управлінської складової. Адже основним джерелом загроз все частіше виступає «людський чинник». Як управлінська категорія менеджмент кібербезпеки – це процес планування, розробки, впровадження та керування заходами, які спрямовані на захист комп'ютерних систем, мереж і даних від наявних та потенційних кіберзагроз.

Робота з персоналом та зменшення впливу «людського фактору» має здійснюватися у відповідності з основними функціями менеджменту, які транслюються й на менеджмент кібербезпеки. Такими функціями є планування, організування, мотивування та контроль.

Планування, як функція менеджменту – це процес розробки системи заходів, спрямованих на досягнення певних цілей. Основною одиницею планування в менеджменті кібербезпеки найчастіше виступають задача (з такими характеристиками як: тип, пріоритет, компоненти, зміст, вартість, обмеження тощо) та подія (яка характеризується ймовірністю та можливими втратами).

Організаційна функція менеджменту кібербезпеки спрямована на забезпечення впорядкування процесу управління в цілому. З одного боку, менеджменту кібербезпеки не притаманні складні організаційні структури. Навпаки, в ньому превалює проєктний підхід, зокрема, в процесі управління розробкою та супроводу програмних продуктів. З іншого боку проєкти кібербезпеки є комплексними і відрізняються такими характеристиками як складність, масштабність і різноманітність [3, с. 107].

Мотивація передбачає управлінську діяльність, спрямовану на спонукання до вибору співробітниками того або іншого типу поведінки в залежності від сили впливу стимулів, мотивів і очікуваних результатів. Вона дозволяє розкрити потенційні можливості персоналу, в тому числі й креативні здібності, а також збільшити продуктивність праці. Це обумовлюється тим, що роботодавець усвідомлює свою залежність від фахових працівників, він готовий мотивувати і берегти команду, а тому враховує матеріальні, соціальні і кар'єрні запити [4]. При вирішенні питань кібербезпеки використовують такі інструменти мотивації як розуміння персоналом загальної мети захисту інформації, а також можливих втрат, у тому числі фінансових та репутаційних, створення відповідної корпоративної культури, забезпечення індивідуального підходу до окремих працівників.

І, нарешті, функція контролю передбачає управлінську діяльність, спрямовану на виявлення, виправлення та попередження відхилень досягнутих результатів від намічених параметрів та цілей. Для менеджменту кібербезпеки контроль передбачає постійний моніторинг об'єкту та процесів з метою перевірки відповідності поточного стану об'єкта його прогнозованому стану, згідно з вимогами клієнтів, технологічними можливостями та законодавчими обмеженнями. Щодо конкретних інструментів які використовує менеджмент кібербезпеки в процесі контролю слід, зокрема, відзначити моніторинг подій, моніторинг мережі, інтрузійне виявлення, системи виявлення аномалій, етичний хакінг тощо.

На мікрорівні суб'єктом менеджменту кібербезпеки виступає будь-яка організація або підприємство, незалежно від розміру або сфери діяльності. Головною ознакою є те, що вони використовують комп'ютерні системи, мережі та залежать від цифрових технологій та мережі Інтернет, а також потребують захисту інформації, активів та інфраструктури від кіберзагроз і кібератак відразу з декількох вимірів.

Перший вимір – це категоріальний розподіл заходів щодо кіберзахисту. Адже ефективний кіберзахист будується як комплексне поєднання кількох підсистем з різними «зонами відповідальності». Зазвичай виділяють три основні зони відповідальності: фізичну, зовнішній периметр, внутрішній простір.

Системи, задіяні у фізичній зоні, визначають що робити, щоб не допустити противника фізичної присутності противника чи зловмисника на території організації або його доступу до матеріальних ресурсів та носіїв організації. Це може включати як очевидні (фізична охорона периметра, системи сигналізації та відеоспостереження), так і неочевидні аспекти, наприклад, охорону та захист комунікацій між філіями організації, питання використання співробітниками фізичних носіїв інформації.

Сюди має входити захист від вардрайвінгу (wardriving) та інших варіантів злому бездротових мереж. З одного боку, їх можна було б віднести до інформаційних атак, на зовнішній периметр, які відбуваються без матеріального підключення до мережі. Однак, вони не можуть бути зроблені без підключення до точок бездротового доступу, яке в більшості випадків обмежено фізичною відстанню, а отже, вимагає присутності на території або в околиці периметра організації.

Кошти та системи захисту зони відповідальності зовнішнього інформаційного периметра націлені на запобігання проникненню зловмисника через зовнішній інформаційний периметр організації. Найбільш поширеним, але не єдиним засобом захисту такого класу зазвичай є система фаєрволів (firewall) або брандмауерів (brandmauer), яка дозволяє фільтрувати інформаційний трафік, що проходить через задані заздалегідь точки периметра.

Захист внутрішнього простору спрямовано зменшення втрат, або повне їх виняток у припущенні, що фізичний чи зовнішній інформаційний периметр був компрометований і зловмисник виявився "всередині" периметра. До засобів захисту насамперед відносять політику поділу прав та ролей, засоби резервного копіювання даних тощо.

Перераховані вище зони відповідальності з одного боку дозволяють розподілити ресурси та засоби при організації кіберзахисту, з іншого слід розуміти, що як захист, так і атака може бути комплексною – наприклад, у класичному випадку хробака Stuxnet були задіяні способи атаки одночасно через фізичну (заражений флешдрайв) і внутрішню (прохід крізь захисні системи Windows) зони безпеки [5].

Комплексний підхід можна розглядати з погляду іншої категорії системи. Насамперед – поділ заходів на технічні та організаційні. Відповідно, категоріями аналізованого захисту може з одного боку виступати інформаційно-комунікаційна система як апаратно-програмний комплекс, а з іншого – користувачі та оператори цих систем.

У внутрішній зоні захисту користувачі можуть ігнорувати рекомендації щодо резервного копіювання (особливо, якщо не впроваджено автоматизовану систему бекапів), обмінюватися паролями «бо так зручніше», залишати собі шпаргалки зі складними паролями поруч із робочим місцем. Відповідно до досліджень витоків паролів – досі досить поширена хрестоматійна помилка, коли як пароль використовується слово «пароль», «qwerty» та ще кілька занадто простих та розповсюджених варіантів паролів [6].

У зовнішньому периметрі захисту частою помилкою є неправильна конфігурація фаєрволла, або повна його відсутність – оскільки оператору не вистачає кваліфікації для його налаштування та тестування. Оборотною стороною непрофесіоналізму можуть бути занадто закриті політики ланцюжків (chains), що ускладнюють функціонування організації. Також часто зустрічається стереотип мислення, що передбачає, що «air gap» – повна відсутність провідного підключення до зовнішніх мереж – забезпечує надійний захист від зовнішнього вторгнення. Як показує приклад описаного вище хробака Stuxnet, що цілком успішно подолав захист такого типу, це досить небезпечна помилка.

Помилки у фізичному захисті на перший погляд цілком очевидні – наприклад відсутність контролю доступу (вахти) на вході, недбале ставлення до замків і ключів, проте, коли йдеться про контроль інформаційних ресурсів, можливі помилки іншого роду, оскільки фізичні системи вторгнення іноді дозволяють «вторгатися не вторгаючись» – наприклад, шляхом злому бездротового роутера, доступ до якого є за межами фізичних кордонів, контрольованих організацією.

При цьому слід розуміти, що механічне ускладнення та посилення заходів безпеки, наприклад, шляхом введення додаткових заходів захисту у вигляді ускладнення паролів та завдання двофакторної автентифікації найчастіше не призводить до поліпшення ситуації. Наприклад, за оцінками [7] на 2018 рік близько 16 мільйонів пар паролів (включаючи 30% змінених після витоку паролів) можуть бути зламані лише за 10 спроб. Дослідження 2022 [8] виявило використання в паролі особистої інформації (56%), повторне використання пароля (69%), використання поширених шаблонів (81,3%). Ці цифри можуть відрізнятися від дослідження до дослідження, однак загальний зміст той самий – низька поінформованість і недостатня технічна кваліфікація користувачів тягне за собою появу вразливостей навіть у найдосконаліших системах [9].

Ступінь і надійність заходів безпеки (наприклад, складність використовуваних паролів) часто входить у конфлікт із зручністю використання системи (необхідністю частої авторизації), тому таке механічне посилення заходів безпеки зазвичай працює лише до певної (найчастіше – недостатньої) межі, за якою користувачі починають обходити систему, спрощуючи собі життя. Наприклад, є приклади підприємств та організацій, в яких система поділу прав і ролей була нівельована тим, що використовувався один обліковий запис користувача і один пароль на всю організацію – таким чином зловмисник отримав доступ до одного облікового запису, отримував доступ відразу до всієї системи.

Таким чином, для управління людським фактором, як складовою системи кібернетичного захисту організації, потрібен особливий підхід і впровадження правил і політик роботи організації тут є лише одним із аспектів проблеми.

Однією з очевидних і нагальних проблем у цій галузі, поряд із загальним підвищенням технічної грамотності та підготовленості персоналу, є підтримка високого рівня пильності (vigilance) та алерт-

ності (alertness) організації. У тому числі – культивування серйозного ставлення до заходів безпеки та уваги до різноманітних інцидентів, які на перший погляд можуть бути незначними (наприклад, вхід до системи під логіном співробітника, який зараз перебуває у відпустці).

Складність підтримки такого рівня пов'язана по-перше з тим, що з одного боку такі якості (режим роботи мозку) можуть вимагати витрат з погляду ресурсів [10] і можуть вступати в конфлікт із прямими обов'язками співробітника з виконання основних завдань у створенні, і навіть із загальними особливостями сучасного життя. Як приклад – у роботах [11],[12] розглянуто дію депривації сну (sleep deprivation) на загальну алертність працівників організації.

Другим джерелом складності підтримки пильності та алертності є загальна властивість адаптивності психіки людини [13], [14]. Завдяки цій властивості будь-який стимул так чи інакше «втрачає новизну», що знижує рівень алертності та уваги при його пред'явленні. Наслідком вказаної ситуації є неможливість постійно підтримувати пильність на максимально високому рівні.

Також слід брати до уваги, що обидва ефекти (кількість доступного ресурсу та загальний рівень «новизни» стимулів) досить складно оцінюються, особливо в умовах повсякденного функціонування підприємства чи організації.

В цьому сенсі ефективним управлінським інструментом перевірки рівня кіберзахисту є тестування на проникнення або pentesting. Воно може проводитись різними засобами та різними командами і відігравати велику роль не тільки в суто технічному аспекті, як розглянуто у багатьох наукових працях [15], [16], але й як інструмент менеджменту кібербезпеки.

Періодичне проведення тестування на проникнення може виконувати у тому числі функцію ефективної підтримки комплексної готовності персоналу. При цьому слід виділити кілька різних форм вказаного тестування – ручний, автоматизований, виконуваний власним персоналом, виконуваний фахівцями, залученими із боку і таке інше.

Функціонал тестування на проникнення корисно розглядати, як частину спільної задачі, спрямованої на підвищення організаційно-соціального аспекту кіберзахисту організації: підтримання високого рівня пильності та алертності персоналу організації, підвищення технічної грамотності персоналу, впровадження безпечних практик тощо; увагу в першу чергу на соціальну складову (фішинг, соціальна інженерія, доксинг, OSINT), які набувають все більшого значення: велика кількість інформації, яку можна отримати в сучасних мережах, технології підробки та імітації особистості (зокрема – deepfake), які можна реалізувати в атаці тощо.

У практиці тестування на проникнення склалося своє найменування команд – за аналогією з військовими навчаннями: «своя команда» – сині (CBT – Cyber Blue Team), «чужі» – червоні (CRT – Cyber Red Team). При цьому для CRT виділяють основні напрямки вектора атаки, що частково збігаються і перетинаються з описаними вище: фізична атака – на фізичні ресурси та матеріальні об'єкти обмеження – проникнення в будівлю, приміщення і таке інше; вектор атак «ззовні», спрямований на впровадження в інформаційні системи організації зовні; внутрішні атаки припускають, що атака «ззовні» пройшла успішно і доступ всередину периметра вже отримано; гібридна атака, що поєднує всі перелічені види атак у різних пропорціях.

Імітація атаки реальних зловмисників крім інших своїх переваг дозволяє тримати персонал у формі – розуміння факту, що вторгнення може йти різними шляхами дозволяє робити його значущим психологічно, що у свою чергу позначається на пильності та алертності персоналу. Узагальнена загроза кібератаки – це «звичний ворог», який не викликає необхідної віддачі та сприймається як незначний. При цьому інформація про те, що відбувається реальне тестування з реальними атаками, буде свіжою і сприймається психологічно по-іншому, що також безпосередньо впливає на персонал організації.

Як інструмент менеджменту кібербезпеки CRT pentesting характеризується наступними перевагами:

– використання CRT дозволяє виявляти та ідентифікувати слабкі місця та вразливості організації на всіх рівнях – у тому числі організаційно-соціальному;

– дозволяє проводити незалежне тестування;

– дозволяє виявляти потенційні ризики, які в іншому випадку залишилися б поза увагою (навіть zero day, якщо CRT є достатньо кваліфікованою) і дає можливість скасувати або змінити потенційно небезпечні рішення (наприклад, винесення чутливих даних у потенційно небезпечний хмарний сервіс);

– тренує команду «від захисту» CBT в умовах, максимально наближених до реальних, дозволяє організовувати та підтримувати творчу та здорову конкурентну атмосферу;

– дозволяє уникнути рутинних атак і застою у плануванні заходів кіберзахисту, оскільки CRT зазвичай не обмежені (або слабко обмежені) у виборі заходів, сценаріїв та інструментів;

– впливає на пильність і алертність всього персоналу організації, адже наслідки та висновки з тестування мають не тільки впливати на суто технічні рішення, а й змінювати організаційні підходи менеджменту кібербезпеки і формувати відповідну корпоративну культуру.

Однак, за всієї привабливості «повноконтактного пентесту», слід обмежувати та планувати заздалегідь діяльність CRT – пентестери схильні захоплюватися і можуть навмисно чи ненавмисно завдати організації шкоди. Повинні вживатися заходи безпеки для того, щоб позитивний результат тестування на проникнення не виявився «надто хорошим» і не призвів до виникнення проблем (наприклад, блокування робочого процесу, або витоку конфіденційної інформації).

Планування процесів тестування на проникнення має виконуватися з максимальним залученням всіх стейкхолдерів, а результати проведення пентесту, хоча б частково, мають ставати предметом обговорень та розбору не лише CBT, а й усього колективу за участю вищого керівництва.

Паралельно із цим слід правильно підбирати частоту та серйозність проведення тестувань. Занадто рідкісне проведення пентестів не дозволяє виконати достатню кількість перевірок, хоча все одно краще ніж повна відсутність тестів на проникнення. З іншого боку, занадто часте проведення пентесту пов'язане із втратами продуктивності та простоями основного робочого процесу. Тобто, воно призводить до перевитрати ресурсів, а також до звикання та перетворення пентесту на «знайому загрозу», що знищує всі організаційно-соціальні переваги від проведення таких процедур.

Так само й питання «звикання та адаптації» робить бажаною ротацію CRT, адже коли персонал CRT вичерпає свої можливості він має передати максимум досвіду та порад CBT. Цінною в цьому сенсі є практика purple teaming – поєднання фахівців із CRT/CBT, які працюють разом. Фахівці CBT, що беруть участь в атаці зможуть краще вчитися працювати на захист. Аналогічно для CRT розуміння процесів захисту та логіки дій CBT дозволяє більш креативно підходити до процесів тестування на проникнення. І саме правильно побудована взаємодія та обмін досвідом, знаннями та інформацією взаємно збагачуватиме обидві команди.

Висновки. Більшу частину проблем кіберзахисту будь-якого підприємства чи організації ще й досі спричиняє «людський фактор», оскільки технічна неграмотність і недбалість персоналу може звести нанівець ефект від будь-яких технічних засобів захисту. Як один з ефективних інструментів підвищення рівня пильності та алертності персоналу, мотивуючого фактору для впровадження ефективних політик та практик безпеки пропонується використовувати тестування на проникнення, яке дотепер розглядається швидше як чисто технічний інструмент контролю кібербезпеки.

Найбільш ефективною процедурою тестування на проникнення є CRT, або purple teaming, що проводиться відповідно до запропонованих вище рекомендацій. Використання означеного інструменту дозволяє зменшити кіберризики в основі яких знаходиться «людська складова» та, одночасно, збільшити загальну ефективність всієї системи менеджменту кібербезпеки.

Список використаних джерел:

1. У 2022 році кількість кібератак на Україну зросла майже втричі. 2023. URL: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454

2. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 р. № 2163-VIII / Верховна Рада України. 2017. URL: http://zakon3.rada.gov.ua/laws/show/2163-19

3. Сметанюк О.А., Бондарчук А. В. Особливості системи управління проєктами в it-компаніях. *Агросвіт*. 2020. № 10. С. 105–111.

4. Орлова О.М. Особливості управління персоналом в IT-сфері. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/11_2017ua/28.pdf

5. Barzashka I. Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme. *The RUSI Journal. Taylor & Francis*. 2013. Vol. 158, № 2. P. 48–56.

6. Jaeger D., et al. Analysis of Publicly Leaked Credentials and the Long Story of Password. 2016. P. 1–19.

7. Wang C., et al. The Next Domino to Fall */ Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. CODASPY18 The 8th ACM Conference on Data; Application Security; Privacy March 19 – 21.* 2018. Tempe, AZ, USA. P. 196–203.

8. Tanni T., et al. Is My Password Strong Enough? : A Study on User Perception in The Developing World. EAI Endorsed Transactions on Creative Technologies. *European Alliance for Innovation n.o*. 2022. Vol. 9, № 30. P. 1–12.

9. Hitchcock K. Linux System Administration for the 2020s : The Modern Sysadmin Leaving Behind the Culture of Build and Maintain. Apress, 2022. P. 328.

10. Aston-Jones G. Brain structures and receptors involved in alertness. *Sleep Medicine. Elsevier BV*. 2005. Vol. 6. P. 3–7.

11. Caldwell J.A., Caldwell J.L., Schmidt R.M. Alertness management strategies for operational contexts URL: https://pubmed.ncbi.nlm.nih.gov/18359253/

12. Niu S.F., Chung M.H., Chen C.H., Hegney D., OBrien A., Chou K.R. The Effect of Shift Rotation on Employee Cortisol Profile, Sleep Quality, Fatigue, and Attention Level. *Journal of Nursing Research. Ovid Technologies (Wolters Kluwer Health)*. 2011. Vol. 19. № 1. P. 68–81.

13. Oken B., et al. Vigilance state fluctuations and performance using braincomputer interface for communication. *Brain-Computer Interfaces. Informa UK Limited*. 2018. Vol. 5, № 4. P. 146–156.

14. Langner R., Eickhoff S. B. Sustaining attention to simple tasks: A meta-analytic review of the neural mechanisms of vigilant attention. *Psychological Bulletin. – American Psychological Association (APA).* 2013. Vol. 139, № 4. P. 870–900.

15. Zakaria M. N., et al. Review of Standardization for Penetration Testing Reports and Documents. *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS).* 2019. P. 1–5.

16. Shebli H.M.Z.A., Beheshti B.D. A study on penetration testing process and tools. 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT). 2018. P. 1–7.

References:

1. U 2022 rotsi kilkist kiberatak na Ukraini zrosla mayje vtichi. [In 2022, the number of cyberattacks on Ukraine increased almost threefold]. Retrieved from https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 [in Ukrainian].

2. Pro osnovni zasadi zabezpechennya kiberbezpeki Ukraini : zakon Ukraini vid 05.06.2017 r. № 2163-VIII / Verhovna Rada Ukraini. [On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated 05.10.2017 No. 2163-VIII / Verkhovna Rada of Ukraine]. 2017. Retrieved from http://zakon3.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

3. Smetaniuk, O.A., Bondarchuk, A.V. (2020). *Osoblivosti sistemi upravlinnya proyektami v it-companiyah. Agrosvit. [Peculiarities of the project management system in IT companies. Agroworld].* № 10. P. 105–111. Ukraine. [in Ukrainian].

4. Orlova, O.M. Osoblivosti upravlinnya personalom v IT-sferi. [Peculiarities of personnel management in the IT sphere]. Ukraine. Retrieved from http://www.visnyk-econom.uzhnu.uz.ua/archive/11_2017ua/28.pdf [in Ukrainian].

5. Barzashka, I. (2013). Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme. USA: The RUSI Journal. Taylor & Francis. Vol. 158, № 2. P. 48–56.

6. Jaeger, D., Pelchen, C., Graupner, H., Cheng, F., Meinel, C. (2016). Analysis of Publicly Leaked Credentials and the Long Story of Password (Re-)use. USA. P. 1–19.

7. Wang, C., Jan, S.TK., Hu, H., Bossart, D., Wang, G. (2018). The Next Domino to Fall / *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. CODASPY18 The 8th ACM Conference on Data; Application Security; Privacy March 19 – 21*. USA: Tempe, AZ. P. 196–203.

8. Tanni, T., Taharat, T., Parvez, M., Rumee, S., Zaber, M. (2022). Is My Password Strong Enough?: A Study on User Perception in The Developing World. USA: EAI Endorsed Transactions on Creative Technologies. – European Alliance for Innovation n.o. Vol. 9, № 30. P. 1–12.

9. Hitchcock, K. (2022). Linux System Administration for the 2020s: The Modern Sysadmin Leaving Behind the Culture of Build and Maintain. Apress. USA. P. 328.

10. Aston-Jones, G. (2005). Brain structures and receptors involved in alertness. USA: Sleep Medicine. Elsevier BV. Vol. 6. P. S3–S7.

11. Caldwell, J.A., Caldwell, J.L., Schmidt, R.M. Alertness management strategies for operational contexts. USA. Retrieved from https://pubmed.ncbi.nlm.nih.gov/18359253/.

12. Niu, S.F., Chung, M.H., Chen, C.H., Hegney, D., OBrien, A., Chou, K.R. (2011). The Effect of Shift Rotation on Employee Cortisol Profile, Sleep Quality, Fatigue, and Attention Level. USA: *Journal of Nursing Research. Ovid Technologies (Wolters Kluwer Health)*. Vol. 19. № 1. P. 68–81.

13. Oken, B., Memmott, T., Eddy, B., Wiedrick, J., Fried-Oken. M. (2018). Vigilance state fluctuations and performance using braincomputer interface for communication. United Kingdom: Brain-Computer Interfaces. Informa UK Limited. Vol. 5 № 4. P. 146–156.

14. Langner, R., Eickhoff, S. B. (2013). Sustaining attention to simple tasks: A meta-analytic review of the neural mechanisms of vigilant attention. USA: *Psychological Bulletin. American Psychological Association (APA).* Vol. 139, no. 4. P. 870–900.

15. Zakaria, M.N., Phin, P.A., Mohmad, N., Ismail, S.A., Kama, M.N., Yusop, O.A. (2019). Review of Standardization for Penetration Testing Reports and Documents. *USA: 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*. P. 1–5.

16. Shebli, H.M.Z.A., Beheshti, B.D. (2018). A study on penetration testing process and tools. USA: 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT). P. 1–7.