868-050822 (дата звернення: 23.03.2024).

8. Українське суспільство в умовах війни. 2022: Колективна монографія / С.Дембіцький, О. Злобіна, Н. Костенко та ін.; за ред. член.-кор. НАН України, д. філос. н. Є. Головахи, д. соц. н. С. Макеєва. Київ: Інститут соціології НАН України, 2022. 410 с.

9. Я мрію про державу у смартфоні – Володимир Зеленський. *Офіційне інтернет-представництво Президента України*. 23 травня 2019. URL: https://www.president.gov.ua/news/ya-mriyu-pro-derzhavu-u-smartfoni-volodimir-zelenskij-55585 (дата звернення: 23.03.2024).

Кобус Олена Сергіївна
Кандидат фізико-математичних наук, доцент,
завідувач кафедри ТЗК ЦКБ ННІ ІБ СК.
Національна академія СБ України.
ORCID: 0000-0003-3130-6515
Бондаренко Степан Юрійович
Фахівець кафедри ТЗК ЦКБ ННІ ІБ СК.
Національна академія СБ України
ORCID: 0000-0001-8328-5117

НАСЛІДКИ ДИСТАНЦІЙНОЇ РОБОТИ ТА ПОЛІТИКИ BYOD ДЛЯ КІБЕРБЕЗПЕКИ

Стрімке поширення дистанційної роботи та політики використання власних пристроїв (BYOD) в організаціях зробило революцію на сучасному робочому місці, пропонуючи гнучкість, продуктивність та економію коштів. Однак ці тенденції також створюють значні виклики кібербезпеці, оскільки віддалені працівники отримують доступ до конфіденційних даних і корпоративних мереж з різних місць і пристроїв. Авторами розглядається вплив дистанційної роботи та політики BYOD на кібербезпеку. Завдяки науковому аналізу сучасних тенденцій, викликів, найкращих практик і новітніх технологій ця робота має на меті забезпечити організації знаннями і стратегіями, необхідними для зменшення ризиків кібербезпеки в епоху дистанційної роботи і BYOD.

Поява дистанційної роботи та політики принесення власних пристроїв (BYOD) трансформувала традиційне робоче місце, дозволивши працівникам працювати з будь-якого місця, використовуючи свої персональні пристрої для доступу до корпоративних ресурсів. Хоча ці тенденції пропонують численні

переваги з точки зору гнучкості, продуктивності та задоволеності працівників, вони також створюють значні ризики для кібербезпеки. З поширенням кіберзагроз, таких як шкідливе програмне забезпечення, фішингові атаки та витоки даних, організації повинні вживати проактивних заходів для захисту своєї конфіденційної інформації та мереж.

Впровадження політики дистанційної роботи та використання власних пристроїв (BYOD) прискорилося в останні роки завдяки технологічному прогресу, зміні робочих уподобань та необхідності забезпечення безперервності бізнесу під час пандемії COVID-19. Згідно з останніми опитуваннями, значний відсоток організацій дозволяє працівникам працювати віддалено принаймні частину часу, а політики BYOD стають все більш поширеними в різних галузях [2,5]. Ці тенденції відображають зростаючий попит на гнучкість і мобільність сучасної робочої сили, а також потенційну економію витрат, пов'язану з ініціативами BYOD. Однак вони також викликають складні проблеми кібербезпеки, пов'язані із захистом даних, мережевою безпекою та дотриманням нормативних вимог.

Дистанційна робота та BYOD створюють кілька викликів для кібербезпеки. Оскільки працівники використовують особисті пристрої для доступу до корпоративних мереж, організації стикаються з підвищеною вразливістю до шкідливого програмного забезпечення, програм-вимагачів та інших кіберзагроз, націлених на кінцеві точки. Передача конфіденційних даних між корпоративними та особистими пристроями підвищує ризик їх втрати або витоку, особливо якщо немає належного шифрування та контролю доступу. Віддалений доступ до корпоративних мереж створює потенційні точки входу для зловмисників, які можуть використовувати вразливості VPN-з'єднань або незахищених мереж Wi-Fi для отримання несанкціонованого доступу. Організації повинні переконатися, що політики віддаленої роботи та BYOD відповідають галузевим нормам і законам про захист даних, таким як GDPR, HIPAA і CCPA, щоб уникнути дорогих штрафів і юридичних наслідків. Пристрої, що належать співробітникам, можуть становити внутрішні загрози, якщо користувачі ненавмисно або зловмисно компрометують конфіденційну інформацію або корпоративні системи.

Щоб вирішити проблеми кібербезпеки, пов'язані з віддаленою роботою та власними пристроями, організації можуть впровадити наступні найкращі практики: 1) створення комплексної політики дистанційної роботи та використання власних пристроїв, яка визначатиме вимоги безпеки, рекомендації щодо прийнятного використання та процедури звітування про інциденти безпеки; 2) впровадження надійних рішень для захисту кінцевих точок, такі як антивірусне програмне забезпечення, засоби виявлення та реагування на загрози на кінцевих точках (EDR) та рішення для управління

мобільними пристроями (MDM), щоб захиститися від шкідливого програмного забезпечення та несанкціонованого доступу; 3) впровадження багатофакторної автентифікації (MFA) і політики надійних паролів, щоб гарантувати, що тільки авторизовані користувачі можуть отримати доступ до корпоративних ресурсів з віддалених пристроїв; 4) шифрування даних як під час передачі, так і в стані спокою, щоб захистити їх від перехоплення або несанкціонованого доступу, особливо під час передачі файлів між корпоративними та особистими пристроями.

Нами пропонується розглянути можливості впровадження декількох нових технологій і тенденцій обіцяють посилити кібербезпеку в контексті віддаленої роботи та BYOD, зокрема: 1) прийняття підходу нульової довіри, який передбачає, що жодному пристрою або користувачеві не можна довіряти за замовчуванням, може допомогти організаціям зменшити ризики, пов'язані з віддаленим доступом і принесеними з собою пристроями (BYOD); 2) розглянути безпечний доступ до сервісів, де ці рішення об'єднують мережеву безпеку і контроль доступу в єдину хмарну платформу, пропонуючи масштабований і гнучкий захист для віддалених користувачів і пристроїв; 3) розглянути передові рішення для віддаленого доступу, такі як програмно-визначений периметр (SDP) і альтернативи віртуальних приватних мереж (VPN), забезпечують безпечне з'єднання і гнучкий контроль доступу для віддалених працівників; розглянути рішення EDR, які дозволяють організаціям проактивно виявляти та реагувати на сучасні загрози, націлені на кінцеві точки, забезпечуючи видимість в режимі реального часу та можливості виправлення.

Дійсно, сучасне робоче місце зазнало сейсмічних змін. Під впливом технологічного прогресу та глобалізації економіки дистанційна робота стає все більш поширеною. Ця зміна парадигми, пропонуючи гнучкість і економічні переваги, створює унікальний набір викликів для кібербезпеки. Інтеграція політики використання власних пристроїв (BYOD) ще більше ускладнює ситуацію, створюючи безліч потенційних вразливостей. Традиційний периметр безпеки – чітко визначена межа навколо фізичної офісної мережі – застарів в епоху віддаленої роботи. Коли співробітники отримують доступ до корпоративних даних і додатків з географічно віддалених місць за допомогою персональних пристроїв, поверхня атаки – сукупність вразливих точок, які можуть бути атаковані – різко розширюється.

Віддалені працівники часто покладаються на публічні мережі Wi-Fi, які за своєю суттю є незахищеними. Зловмисники можуть легко перехоплювати конфіденційні дані, що передаються через ці мережі, ставлячи під загрозу конфіденційність і цілісність. Як правило, IT-відділи мають менший контроль над станом безпеки персональних пристроїв, що використовуються в угодах BYOD [1]. Застаріле програмне забезпечення та невиправлені операційні

системи створюють вразливості, якими хакери можуть скористатися для отримання доступу до корпоративних систем. Віддалені працівники можуть бути більш вразливими до фішингових атак через відсутність контролю. Вони можуть з більшою ймовірністю натискати на шкідливі посилання або відкривати заражені вкладення. Впровадження заходів із запобігання втраті даних (DLP) стає більш складним у віддаленому середовищі [4]. Конфіденційна інформація може бути ненавмисно збережена або передана на персональних пристроях, що збільшує ризик витоку даних.

Тенденція до дистанційної роботи залишається, а політики принесення власних пристроїв продовжуватимуть розвиватися. Організації повинні застосовувати проактивний підхід до кібербезпеки, постійно адаптуючи свої стратегії до нових загроз. Розвиваючи культуру обізнаності з питань кібербезпеки серед співробітників, інвестуючи в надійні рішення для забезпечення безпеки та встановлюючи чіткі політики, компанії можуть зменшити ризики та створити надійний фундамент для успішної віддаленої роботи. Віртуальні приватні мережі (VPN) часто є наріжним каменем безпечного віддаленого доступу. Однак неправильні конфігурації, слабкі протоколи шифрування та вразливості в самому програмному забезпеченні VPN можуть створювати вразливі точки входу для зловмисників. Віддалене робоче середовище вимагає надійних рішень для захисту кінцевих точок, що включають антивірусне програмне забезпечення, системи виявлення вторгнень (IDS), а також засоби виявлення та реагування на кінцеві точки (EDR) [3]. Технічна ефективність цих рішень залежить від моніторингу в режимі реального часу, оновлення сигнатур та ефективних алгоритмів виявлення загроз. Шифрування даних захищає конфіденційну інформацію як у стані спокою (зберігається на пристроях), так і під час передачі (передається мережею). Надійні алгоритми шифрування, такі як AES-256, мають вирішальне значення для того, щоб зробити дані нерозбірливими у випадку злому.

Приплив персональних пристроїв – ноутбуків, смартфонів, планшетів – від різних виробників і з різними операційними системами створює неоднорідне середовище. Підтримка узгоджених конфігурацій безпеки і застосування політик безпеки в цьому різноманітному середовищі є значним викликом. ІТ-відділи мають обмежений контроль над технічною гігієною персональних пристроїв, що використовуються для роботи. Застарілі операційні системи з невиправленими вразливостями, слабкі практики використання паролів і наявність шкідливого або шпигунського програмного забезпечення на цих пристроях можуть слугувати шлюзами для кібератак. Технічні рішення DLP використовують дактилоскопію даних, перевірку контенту та методи запобігання втраті даних для запобігання несанкціонованому витоку даних. Однак їхня ефективність залежить від

здатності адаптуватися до різних типів даних, каналів зв'язку та методів витоку, що розвиваються.

Список використаних джерел

1. 10 Keys to an Effective BYOD and Remote Access Policy. Phelps. URL: https://www.phelps.com/insights/10-keys-to-an-effective-byod-and-remote-access-policy.html (дата звернення: 01.04.2024).
2. BYOD cybersecurity risks: How to protect a remote workforce. Roebuck Technologies. URL: https://www.roebucktech.com/it-blog/byod-cybersecurity-risks-how-to-protect-a-remote-workforce/ (дата звернення: 01.04.2024).
3. Singh G. Cybersecurity in the era of remote work: security risks & best practices. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/pulse/cybersecurity-era-remote-work-security-risks-best-practices-singh (дата звернення: 01.04.2024).
4. Amaxra. A Guide to BYOD Security: Policies, Pros & Cons and Best Practices. Microsoft Expertise to Accelerate Your Business - Amaxra. URL: https://amaxra.com/articles/byod-security (дата звернення: 01.04.2024).
5. The impact of remote work on cybersecurity. TeamViewer. URL: https://www.teamviewer.com/pl/insights/the-impact-of-remote-work-on-cybersecurity/ (дата звернення: 01.04.2024).

Талаш Валерія Юріївна
Здобувач другого рівня вищої освіти,
спеціальність «Публічне управління та адміністрування».
Донецький національний університет імені Василя Стуса

ФУНКЦІОНУВАННЯ МОБІЛЬНИХ ЦНАП ПІД ЧАС ВІЙНИ В УКРАЇНІ

Особливо важливим питанням є забезпечення доступу до базових адміністративних послуг громадян України, які опинилися в складних життєвих обставинах через війну. Тому функціонування мобільних ЦНАП у воєнний час змогло частково вирішити проблему доступу до адміністративних послуг для вразливих верст населення, зокрема, внутрішньо переміщених осіб та мешканців деокупованих та прифронтових територій.

Інноваційним рішенням в сфері децентралізації стало запуск проєкту організації надання адміністративних послуг у форматі «мобільного офісу» ще в листопаді 2017 року. Завдяки європейському досвіду та програми «U-LEAD з Європою» стало можливим надання якісних та своєчасних адміністративних