Як працювати віддалено і не пошитися в дурні

Минуло два з половиною роки відтоді, як вірус змусив людей полишити офіси. Робота з дому або звідки доведеться стала новою нормою. Але пристосування до цієї реальності було непростим, та й зараз залишаються проблеми.

Пандемія коронавірусу спричинилася до тектонічних зсувів у роботі компаній. За даними Gartner, наразі 60% інформаційних працівників у світі працюють віддалено, і принаймні 18% не планують повертатися до офісів. В Україні на це все наклалася війна, через яку багато людей були змушені покинути свої домівки. На щастя, існує Інтернет, завдяки якому в багатьох випадках можна працювати, знаходячись у будь-якій точці світу.

Водночас віддалена робота ставить свої виклики, адже зростає ризик кібератак і витоків даних. «МтБ» розбирався, як захищають віддалені робочі місця, які виклики та проблеми при цьому постають і які продукти у цій царині є на ринку.

Забудьмо про периметр

Європейський Центр досліджень економічної політики (CEPR) торік оприлюднив результати аналізу, згідно з якими у другому кварталі 2020 року 557 млн людей працювали вдома: це 17,4% світової робочої сили. Дослідницький центр ***Pew*** наприкінці 2020-го повідомляв, що з поміж опитаних працівників, чию роботу загалом можна виконувати з дому, 71% в цьому режимі і працювали, а також що 54% бажали б залишитися на такому режимі роботи й після пандемії. ***Acronis*** у своєму звіті Cyber Readiness Report 2020, в якому було проаналізовано перші

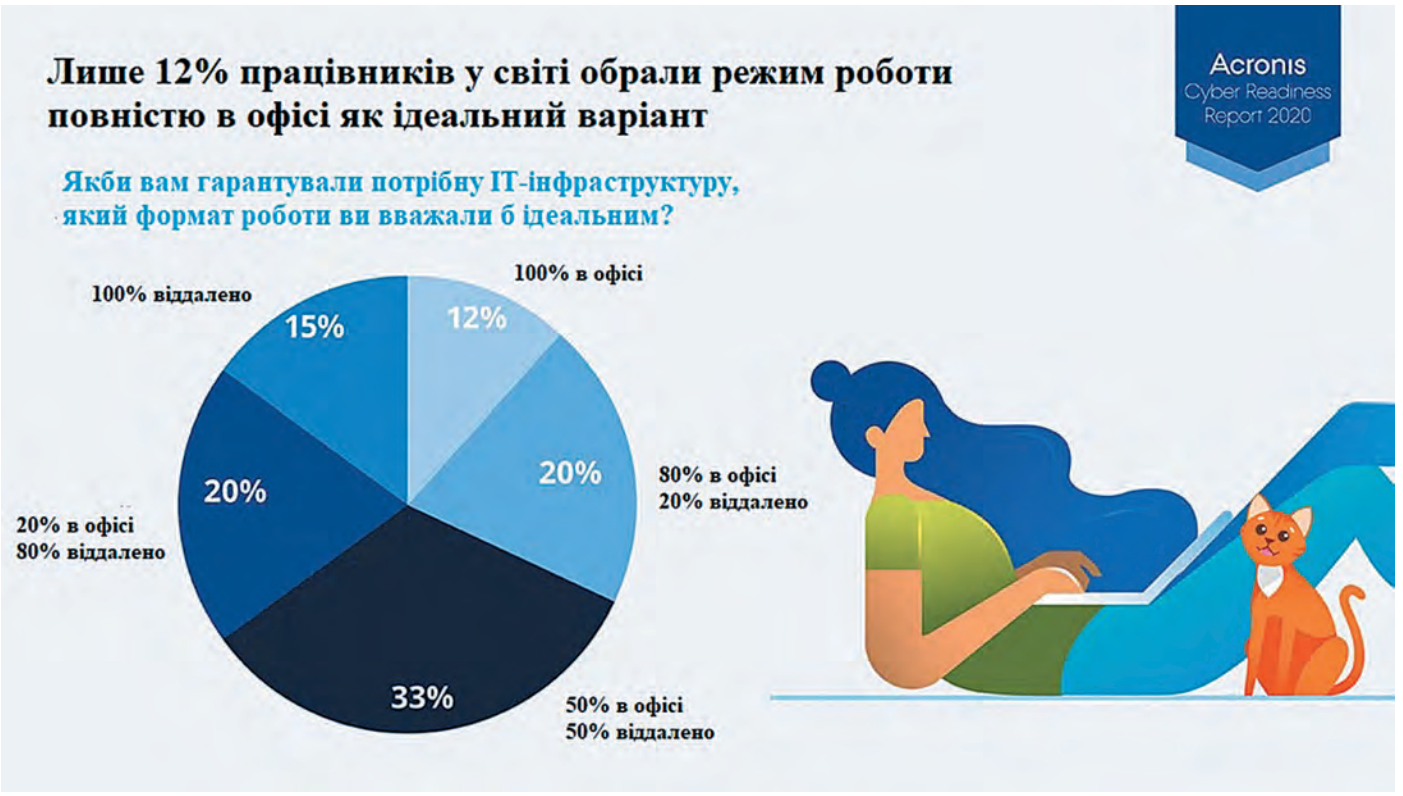

Рис. 1 Більшість працівників бажали б принаймні частину часу працювати вдома (джерело: Acronis)

півроку пандемії, зазначав, що глобально лише 12% працівників бажали б надалі працювати виключно в офісі, тоді як решта обрала б якусь форму гібридної роботи (**рис. 1**)

Цей, без перебільшення, грандіозний зсув відкрив нові можливості для кіберзлочинців. Перемістившись за межі периметру захисту, працівники опинились у ситуації, коли вони наражають на небезпеку себе самих і свої компанії. Хакери вчиняли атаки, використовуючи прийоми соціальної інженерії, про що наш журнал писав вже навесні того року *(«Коронавірус атакує комп'ютери», «МтБ» №2/2020)*. Зокрема, експлуатувалася тема коронавірусу: створювались тематичні сайти, заражені зловмисним ПО, яке збирало в користувачів інформацію про банківські рахунки та інші дані; розсилалися фішингові листи нібито від добропорядних організацій з вкладеннями знову-таки на тему вірусу і лікування від нього.

Інші атаки були розраховані просто на недосвідченість в інформаційній гігієні. Наприклад, у квітні 2020 року відбулась відома кампанія проти Twitter: зловмисники телефонували працівникам компанії, представляючись співробітниками IT-відділу, і просили підтвердити їхні паролі на підставному веб-сайті. Діставши цю інформацію, вони зламали рахунки 130 людей, у тому числі Ілона Маска, Джеффа Безоса і Барака Обами.

Forbes наводить слова директора з кіберуправління сінгапурської страху вальної компанії ***FWD Insurance*** Прітіша Пурохіта, який зауважує, що поза офісом фішингарям і здирникам легше обходити корпоративний кіберзахист. *«В обстановці традиційного офісу існує природний захист проти фішингу, адже співробітник може легко проконсультуватися з колегою, який сидить поруч»*. До пандемії менеджери, як і належить, ігнорували тестові фішингові повідомлення, оскільки знали, що відділ кіберзахисту вживає заходів проти шахрайства; але, працюючи віддалено, ті самі співробітники демонстрували більшу схильність відкривати фішингові листи.

Водночас, пише Forbes, якщо співробітник втрачає зв'язок з компанією, йому важко отримати допомогу від потрібних фахівців. Окрім того, багато працівників бояться, що вони «зробили щось не те», і вагаються звертатися по допомогу.

Організація ***Ponemon Institute*** у своєму звіті 2002 Cost of Insider Threats Global Report повідомляє, що з-поміж 6803 інцидентів, пов'язаних з діяльністю інсайдерів, 46% були спричинені недбалістю співробітників або контрагентів, причому збитки від інциденту в середньому становили майже $485 тис. Ще 18% інцидентів були пов'язані з крадіжкою облікових даних і коштували у середньому $805 тис. Згідно з опитуванням, 67% компаній мали протягом 2022 року від 21 до 40 таких інцидентів, порівняно з 60% у 2020-му і 53% у 2018-му. Можна здогадуватись, що немала їх частина була обумовлена саме віддаленим режимом роботи.

Зокрема, тому, що — як з'ясувалося — бізнес був не надто готовий до змін. Acronis за результатами свого опитування підрахував, що у 2020 майже половина працівників у світі не отримала адекватних інструкцій від свого IT-департаменту щодо налаштування віддаленої роботи, і 16% не отримали взагалі жодних, тоді як 33% одержали кілька електронних листів

(відтоді ситуація покращилась). З іншого боку, відсутність IT-підтримки було названо останньою серед проблем, з якими зіткнулися працівники: 37% респондентів на перше місце поставили труднощі з покриттям Wi-Fi, на другому місці взагалі сама необхідність користуватися VPN та іншими засобами безпеки, на третьому — недоступність корпоративної мережі та програм.

Сайт ***CIO&Leader*** навесні минулого року опублікував дослідження, згідно з яким загалом для 78% працівників технічні питання на кшталт безпечного доступу до корпоративних ресурсів виявилися серйозною проблемою. 67% зізналися, що аби не зменшувати продуктивність праці і вправлятися зі своїми обов'язками, вони знаходили способи оминати корпоративну політику безпеки: надсилали робочі документи на персональні поштові адреси, використовували однакові паролі, встановлювали сторонні програми на робочі пристрої.

Безпеку периметра викинуто у вікно, а «роботу з дому» скоро замінить «робота звідусіль» (Work from Anywhere), зазначає Acronis серед своїх висновків. Захищати треба не просто мережу. На наступному етапі треба попіклуватися про те, щоб можна було безпечно працювати навіть у незахищеному середовищі. Люди будуть надалі працювати і наймати інших людей віддалено, і це стане новою нормальністю.

Захист своїми силами

То що робити? По-перше, працівники мають самі попіклуватися про свою захищеність. Фахівці пропонують різні поради, які є не такими вже складними і взагалі-то (здебільшого) актуальними незалежно від режиму роботи.

Ось, наприклад, рекомендації від компанії ***NordLayer***, яка зокрема займається убезпеченням віддаленої роботи. Потрібно мати надійний антивірус і підтримувати його в найновішій версії, а також встановити VPN. Використовувати паролі, які неможливо вгадати, і регулярно їх міняти. Не нехтувати безпекою своєї мережі Wi-Fi: ставити надійний пароль та ідентифікатор мережі, який ніяк не асоціюється з користувачем, використовувати WAP2-шифрування, задавати MAC-адреси пристроїв, яким дозволено доступ до мережі, і завжди мати останню версію ПО маршрутизатора. Дуже обережно ставитись до електронної пошти: перевіряти автентичність адреси, не відкривати листів від неочікуваних відправників, а також не чіпати вкладень, якщо нема цілковитої певності в тому, чому ті файли надіслано і що вони містять. Задля більшої надійності можна перейти до провайдера шифрованої пошти.

Важливо використовувати двофакторну автентифікацію, причому отримання паролю через SMS не є найбезпечнішим способом; можна послуговуватись USB-ключами чи мобільними застосунками. Дуже небезпечно використовувати один і той самий пристрій в робочих і особистих цілях, тому варто попрохати в компанії окремий ноутбук, а якщо це неможливо — поміркувати про самостійне його придбання. (Acronis повідомляв, що 49% людей, почавши працювати віддалено, купили щонайменше один додатковий пристрій — комп'ютер чи телефон). Якщо доводиться працювати на ноутбуці в публічних місцях, на випадок крадіжки доцільно шифрувати увесь вміст.

Іноді зловмисники зламують веб-камеру, щоб збирати інформацію, записувати переговори через месенджери чи програми конференцзв'язку, а в деяких випадках і щоб вимагати гроші в жертв. Тут важко щось вдіяти, але можна закривати або навіть заклеювати камеру, коли вона не використовується, або мати зовнішню і вмикати її лише за потреби.

А що робити, зі свого боку, компанії? Тут багато чого зводиться навчання персоналу. Оскільки домашні працівники повинні більше знати про загрози, ніж ті, що знаходяться всередині периметра, доцільно започаткувати навчальні курси, у тому числі для керівників. NordLayer радить мати у штаті співробітника, відповідального за віддалену роботу, який має пояснювавати найкращі практики, протоколи використання паролів та інформацію щодо автентифікації. До нього ж працівники мають звертатись, якщо в них виникають питання. Зокрема, треба довести до персоналу інформацію про те, як робити сильні паролі, наскільки часто їх міняти, які застосунки для управління паролями використовувати і якими можуть бути наслідки недбальства. Загалом роботодавцеві важливо піклуватись про те, щоб люди дотримуватися корпоративних політик безпеки і не втрачали пильності, водночас проявляти розуміння у разі помилок.

Якщо компанія має якісь корпоративні інструменти захисту типу VPN, антивірусів тощо, не варто резервувати їх використання лише для головного офісу або окремих працівників. Часто дешевше купити ліцензії для всіх працівників, ніж покладатися на те, що вони самі забезпечать себе відповідними інструментами. Взагалі варто надати працівникам робочі ноутбуки і встановити двофакторну автентифікацію, що дозволить мати кращий контроль доступу до корпоративних ресурсів, а також убезпечить від проникнення зловмисного ПО.

Компанія ***Critical Insight***, яка надає послуги кіберзахисту, наголошує: зберігати дані виключно на робочих комп'ютерах важливо тому, що на них IT-відділ робить регулярні оновлення ПЗ, проводить сканування на віруси, блокує зловмисні сайти тощо. Сам працівник, імовірно, того робити не буде. На додачу, компанія може забезпечувати віддалений контроль робочого комп'ютера. При цьому, щоб знизити ризики, багато компаній скасували політику, яка дозволяла використовувати робочі пристрої для власних цілей.

А ось ще кілька думок від Алмога Апріона, засновника і CEO ізраїльського стартапу ***Cyolo***. Він зазначає, що VPN не є найкращим варіантом, адже більшість цих продуктів сконфігуровані таким чином, щоб надавати або повний доступ, або жодного. Хоча адміністратори можуть обмежувати доступ до певних програм або для окремих користувачів, це потребує надто великої роботи, що просто не практично. Це поєднання замалого контролю і завеликих прав є рецептом катастрофи, наголошує фахівець, тим більше коли привілеї VPN

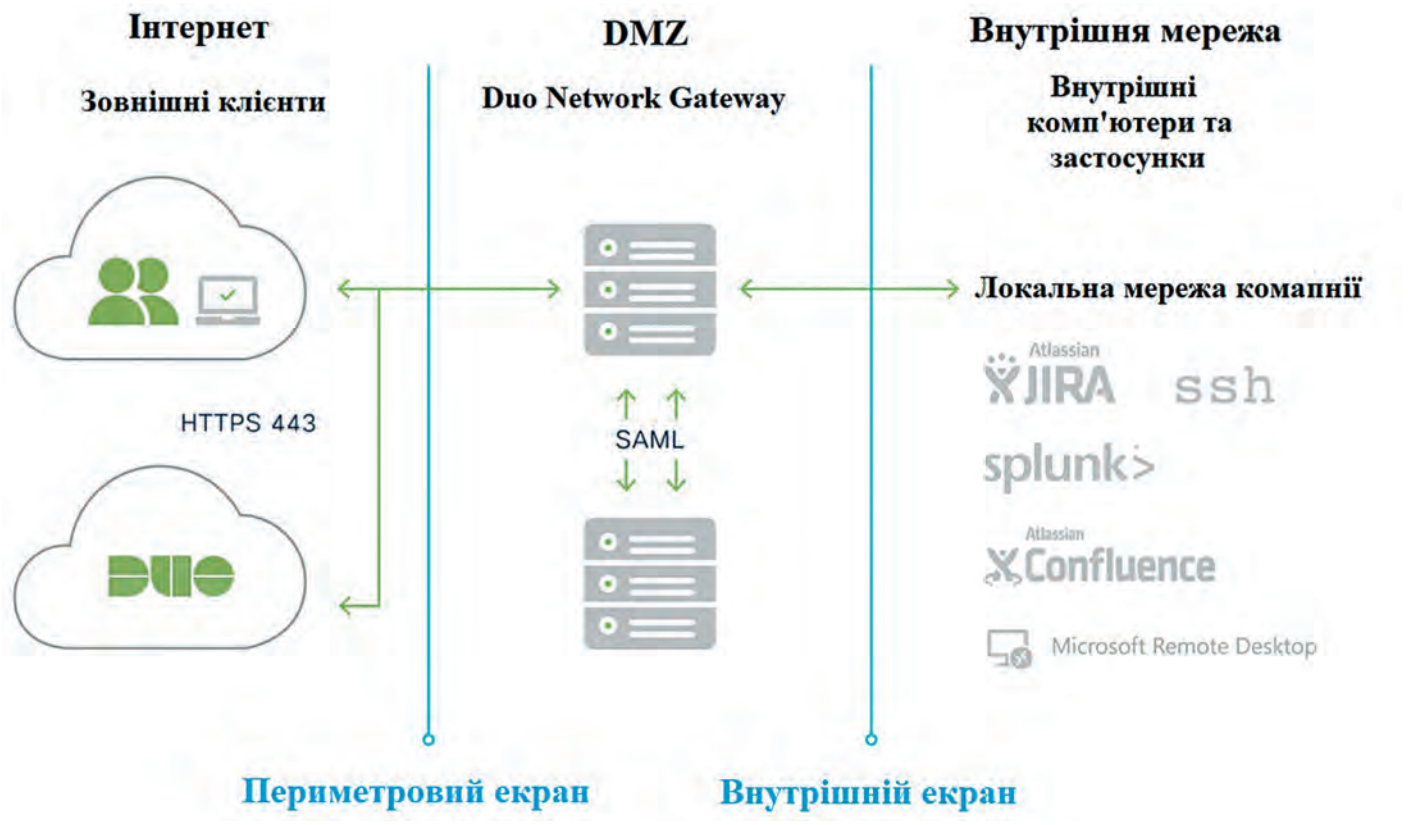

Рис. 2 Доступ до корпоративних ресурсів через Cisco Duo Network Gateway

потрібно надавати підрядникам або постачальникам.

По-друге, не можна обійти увагою того факту, що людям властиво помилятися, і тому захисні рішення, які не враховують можливості помилки, просто не спрацюють. Наприклад, розробникам ПО властиве прагнення негайно виправляти знайдені помилки в коді або, і програміст може увійти в систему з першої-ліпшої доступної мережі. За такого сценарію хтось неминуче забуде вийти і цим самим відкриє доступ злочинцям, які завжди того чатують.

Саме тут буде корисною архітектура з нульової довірою (ZTNA), адже в ній доступ надається за принцом постійної авторизації, а моніторинг сесій забезпечує додатковий рівень контролю. Також компаніям варто визначати найбільш уразливі точки і убезпечувати їх насамперед: наприклад, замість надавати постачальникам повний доступ через VPN, краще відкрити лише ту частину мережі, яка їм потрібна для роботи. Пан Апріон тут промовляє зі своєї дзвіниці, адже його компанія спеціалізується на ZTNA; проте зараз усі виробники так чи інакше пропонують ZTNA у своїх розробках.

Професійний захист віддалених працівників

Концепція «роботи звідусіль» передбачає три режими, у яких працівник може провадити свою діяльність. Звичайно, в офісі він перебуває за периметром корпоративної мережі. Працюючи вдома, він користується Інтернетом від найближчого провайдера і простим бездротовим маршрутизатором, до якого також можуть бути підключені інші користувачі в помешканні, але, принаймні, може налаштувати захист домашньої мережі. Тоді як мобільні працівники користуються незахищеними мережами (наприклад, в кав'ярні чи в готелі), чим наражають корпоративні ресурси на ще більшу небезпеку, адже існує багато способів перехопити трафік (наприклад, за допомогою фальшивої точки доступу).

Виробники, що працюють у сфері кібербезпеки, мають свої пропозиції для убезпечення віддаленої та гібридної роботи. Як правило, це вже відомі продукти, які закривають ті чи інші потреби віддаленого працівника, адже завдання залишаються більш-менш тими самими. Зрештою, віддаленому працівникові так само треба захищатися від різних векторів атак: через веб, електронну пошту, хмарні сервіси, мобільну мережу тощо.

Зокрема, ***Cisco*** пропонує рішення для багатофакторної автентифікації Duo, яке при кожній спробі входу в мережу контролює захищеність пристрою і створює безпечне підключення до корпоративних ресурсів навіть без VPN. Для цього використовується зворотній проксі-сервер Duo Network Gateway (**рис. 2**). Водночас Duo інтегрується з безпековими рішеннями Cisco та інших виробників.

Cisco має сервіс VPN — AnyConnect, який, окрім надання захищеного доступу, забезпечує видимість поведінки пристроїв та користувачів у всій мережі з попередженням про загрози, блокування доступу до мережі пристроям, що не відповідають політиці безпеки, і багатофакторну автентифікацію у взаємодії з Duo. Рішення Cisco Secure Endpoint бере на себе захист робочих станцій, а також виявлення загроз і реагування на них. Також Cisco має окреме апаратне рішення — мережеві екрани серії 3100, розраховані на підтримку віддалених працівників зі швидким VPN-з'єднанням; окрім того, вони вміють ідентифікувати за стосунки і потенційні загрози в зашифрованому трафіку.

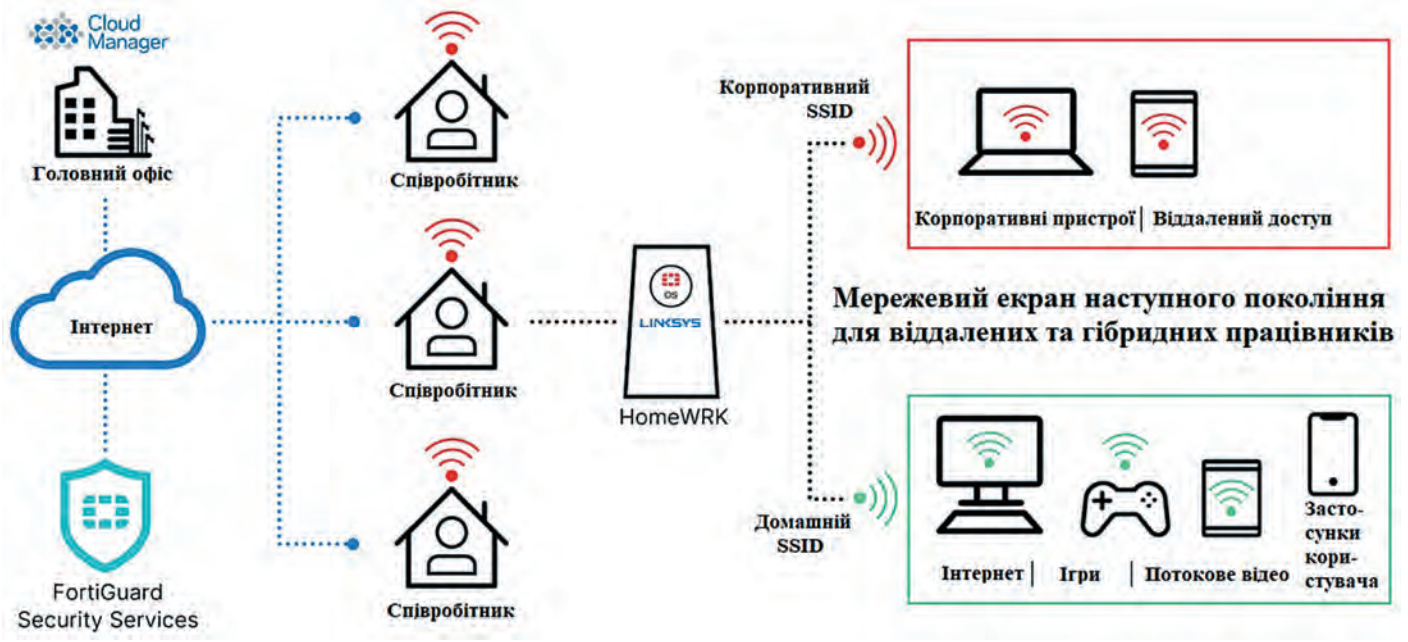

Рис. 3 Linksys HomeWRK for Business | Secured by Fortinet і створення корпоративної мережі на базі домашньої.

Check Point пропонує для віддаленої роботи комплексну систему Harmony, яка поєднує захист робочих станцій, захищений Інтернет-доступ, архітектуру нульової довіри для доступу до корпоративних застосунків, безпеку електронної пошти і захист від мобільних загроз.

Зокрема, рішення для Інтернет-з'єднань доступне в двох варіантах: Harmony Connect Internet Access (хмарний веб-шлюз) і Browse (у вигляді нано-агента, який працює всередині браузера). Browse за технології Content Disarm&Reconstruction (CDR) аналізує завантажені файли і надає користувачеві знешкоджену версію, якщо там був зловмисний контент, а також інспектує SSL-трафік і блокує доступ до фішингових сторінок.

Рішення для захисту доступу до застосунків Harmony Connect Remote Access також є в двох варіантах: безклієнтному (через веб-браузер) і клієнтному (з VPN-агентом). Цікаве рішення Harmony E-Mail&Office, яке розгортається з хмари і захищає від загроз поштові скриньки і програми колективної роботи на кшталт Microsoft Office 365, Google Drive тощо. А Harmony Mobile забезпечує захист мобільних пристроїв, блокуючи завантаження шкідливих застосунків. Усі продукти інтегруються між собою через портал управління, де відбувається керування політиками безпеки, виводиться інфографіка подій і зберігаються усі дані. Таким чином створюється багатошаровий захист, який убезпечує віддалених користувачів від відомих загроз і атак нульового дня.

Fortinet пропонує рішення для «роботи звідусіль» в рамках своєї системи безпеки Security Fabric. Вони забезпечують захист на рівні мережі, робочих точок та доступу до ресурсів. Торік спільно з ***Linksys*** виведено на ринок маршрутизатор Linksys HomeWRK for Business, який дозволяє на базі домашньої мережі створити робоче середовище з окремим ідентифікатором. Компанія може віддалено конфігурувати цю другу мережу і керувати нею, тоді як домашні користувачі зберігають повний контроль над своїм власним сегментом (**рис. 3**).

Пристрій забезпечує захист корпоративного рівня для робочого сегмента — антивірус, веб-фільтрацію, запобігання вторгненням, контроль застосунків і бот-мереж, VPN, — і окремо локальний захист для домашньої мережі. Водночас він приорітизує виділення смуги пропускання для онлайн-конференцій. Через панель управління можна відслідковувати характеристики роботи усіх підключених пристроїв.

Palo Alto звертає увагу на те, що традиційна побудова VPN-тунелів, які з'єднують віддалених та мобільних користувачів з корпоративним дата-центром, застаріла через поширення хмарних сервісів та Інтернет-застосунків. Хмарний трафік мусить проходити через головний офіс, що є добре з точки зору безпеки, якщо там відбувається його інспекція, але погіршує якість послуги, тому користувачі намагаються за можливості уникати VPN, через що організація втрачає контроль за доступом до застосунків і можливість підтримувати політику безпеки.

Тому Palo Alto пропонує рішення Prisma Access, яке саме є хмарним сервісом на базі AWS і Google Cloud. Prisma Access інспектує трафік та виконує інші функції безпеки: мережевий-екран-як послуга (FWaaS), брокер доступу до хмарних сервісів (CASB), захищений веб-шлюз (SWG) тощо. Доповнює його GlobalProtect — застосунок для ноутбуків, смартфонів і планшетів, —, який автоматично під'єднується до Prisma Access і забезпечує видимість трафіку, користувачів, пристроїв та програм, а також дозволяє застосовувати політики безпеки до всіх користувачів.

Є ще багато інших продуктів від різних виробників, які можна використати для віддаленої роботи, тож в нових умовах є чим захистити свій бізнес якщо не від фізичних, то принаймні від кіберзагроз.

Василь ТКАЧЕНКО, **МтБ**