Лукомська А. А., курсант
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Мирошниченко В. О.,
професор кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

КІБЕРБЕЗПЕКА ВІДДАЛЕНОЇ РОБОТИ У СФЕРІ БІЗНЕСУ ПІД ЧАС ПАНДЕМІЇ COVID-19

Декілька років тому віддалена робота була рідкісним явищем на ринку праці. Зараз в умовах пандемії COVID-19 це практично єдина можливість зберегти працездатність бізнесу.

Захист інформації в комп'ютерних мережах являє собою комплексну систему, що містить апаратно-програмні засоби і методи, а також організаційно-правові заходи, які дозволяють запобігти або максимально ускладнити можливість реалізації загроз інформації. Для оцінки ефективності такої системи необхідно мати інструмент її формального подання, в ролі якого є модель захисту інформації [1, 2].

Для оперативної організації віддаленої роботи співробітників недостатньо одного рішення керівництва: потрібна підготовлена інфраструктура, яка є не у всіх компаній. Тому настає час інформаційно-технічних відділів та служб інформаційної безпеки, які покликані забезпечити безперервність і, що важливо, безпеку бізнес-процесів компанії. Цим службам необхідно швидко розробляти захисні заходи для технологій віддаленого доступу для співробітників своїх компаній та організацій.

Як показує практика, не всі сервіси організації безпечні, витоки інформації з бізнес-систем найбільших корпорацій трапляються із завидною регулярністю, і навіть VPN може виявитися ненадійним інструментом і бути зламаний. Через відсутність часу на аналіз і підбір додаткових засобів захисту ті компанії, які раніше фокусувалися переважно на обороні периметра, виявляться найбільш уразливими, оскільки тепер жодного периметра не існує.

Потребує вирішення і проблема забезпечення безпеки під час використання особистих пристроїв, якими користуються співробітники для організації віддаленого доступу. Не всі компанії можуть собі дозволити забезпечити співробітників робочими своїми технічними засобами. Непідконтрольні службі інформаційної безпеки пристрої з домашніх мереж Wi-Fi будуть масово підключатися до внутрішніх корпоративних ресурсів. Зобов'язати всіх співробітників ставити прийняті в компанії засоби захисту на

особисті комп'ютери, поширити туди прийняту в організації політику безпеки – теоретично можливо, але не в режимі переведення всього персоналу на віддалений формат роботи. Крім того, це спричинюватиме не тільки технічні, а й юридичні та організаційні складнощі. Тому ризики з найбільшою ймовірністю зростуть у компаній, які активно захищають лише кінцеві робочі станції, залишаючи без уваги корпоративну інфраструктуру загалом.

У цій ситуації службам безпеки компанії варто звернути увагу на такі рекомендації:

Необхідно скласти політику безпеки під час віддаленої роботи. Політика повинна бути короткою, зрозумілою, описувати основні ризики, заходи захисту та обмеження, що можуть виникнути під час віддаленої роботи.

Провести позапланове експрес-навчання і підготувати коротку пам'ятку, яка містить основи кіберграмотності. Це допоможе співробітникам не розслаблятися і не допускати помилок, вбереже від специфічних для віддаленої роботи неприємностей.

У разі термінового впровадження захисних рішень треба віддавати перевагу відомим на ринку компаніям зі сфери кібербезпеки. Довіра до таких постачальників знизить ймовірність зробити помилку, ціна якої для реального бізнесу зараз зросла в кілька разів. Якщо немає упевненості відповісти на питання про те, які процеси відбуваються в інформаційній інфраструктурі компанії, то для наведення порядку і встановлення контролю, в тому числі для інформаційно-технічних відділів, це зараз – головне завдання. Підключення до ресурсів через неврахований VPN, масове використання одного облікового запису, перебір паролів, дивні сплески певних типів внутрішнього трафіку за відсутності користувачів в мережі – далеко не повний список загроз безпеки, які особливо часто виникають під час віддаленої роботи співробітників компанії. Використання систем внутрішнього моніторингу в додаток до периметрового захисту набуває актуальності саме зараз.

Важливо сфокусуватися на захисті від тих видів атак, які стають актуальними в нових умовах, навіть якщо раніше їх не було в моделі загроз компанії. Зараз службі безпеки необхідно оперативно переглянути модель загроз, не забуваючи про засоби протидії DDoS-атакам і зовнішнім вторгненням, оскільки кількість точок проникнення і способів порушення конфіденційності, цілісності та доступності інформації стало більше. Це створює нові можливості для кіберзлочинців щодо навіть найконсервативніших в плані IT-інфраструктури компаній.

Захист і контроль особистих пристроїв – непросте завдання, тому необхідно сфокусуватися на забезпеченні безпеки на стороні важливих бізнес-систем і сервісів. Це дозволить не тільки контролювати легітімність роботи власних користувачів в них, але і більш ефективно виявляти вторгнення зовнішніх зловмисників.

Впровадження концепції Zero Trust (нульової довіри до користувачів і пристроїв), або хоча б її окремих елементів, стане хорошим рішенням саме

зараз. Незважаючи на те, що на старті процесу можливі деякі незручності для користувачів, комфортом доведеться пожертвувати. Допускати людей в корпоративну інфраструктуру ззовні, не впевнившись у застосуванні всіх необхідних процедур з погляду безпеки – рішення, яке може обійтися дорожче. Корисним рішенням може бути впровадження контролю внутрішнього трафіку (клас NTA – Network. Traffic Analysis). При цьому інциденти виявлятимуться автоматично, не потребуючи навіть перенастроювання наявної політики безпеки, не кажучи вже про додаткову покупку ще будь-яких безпекових рішень.

Як видно, вимушена дистанційна робота ставить перед співробітниками і організаціями нові проблеми щодо забезпечення безпеки інформації. Наведений вище список рекомендацій можна продовжувати довго, і він все одно може виявитися неповним. Його складання для конкретної компанії залежить від особливостей сфери бізнесу і прийнятої стратегії захисту інформації. Віддалений доступ співробітників до інфраструктури компанії – це завжди питання якісної настройки системи забезпечення інформаційної безпеки та застосування інструментів, здатних контролювати роботу співробітників з будь-якого місця, з метою максимально нівелювати ризики витоку конфіденційної інформації та порушення роботи корпоративних ресурсів.

Бібліографічні посилання

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : затв. наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

2. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методи та засоби захисту інформації : в 2 т. *Т. 2. Інформаційна безпека*. Київ : Арий, 2008. 344 с.

Масоха В. О., курсант 2-го курсу
факультету підготовки фахівців для
підрозділів стратегічних розслідувань
Науковий керівник – Паршин Ю. І.,
професор кафедри фінансових
та стратегічних розслідувань,
доктор економічних наук, професор
*(Дніпропетровський державний
університет внутрішніх справ)*

СТРАХОВІ РЕЗЕРВИ ТА ЇХ ЗБЕРЕЖЕННЯ

Будь-які підприємства, торгівельні чи промислові, створюють певну систему економічних показників, щоб бачити реальний фінансовий результат своєї діяльності. Там містяться лише дані про сукупність доходів та витрат страховика. На відміну від підприємств, страхові компанії з метою забезпечення майбутніх виплат страхових сум створюють ще й страхові