KPMG

COVID-19 та нові кіберзагрози

Пандемія COVID-19 вже зараз має значний вплив на країни, організації та громадян. Люди розгублені і хочуть дізнатися більше, мати більше інформації та підтримки, вони хочуть бути захищеними. Організовані злочинні групи користуються ситуацією, невпевненістю та сумнівами, які приносить COVID-19, та винаходять нові способи для створення загроз у сфері IT та кібербезпеки.

Експерти KPMG наразі визначають наступні ключові ризики кібербезпеки, пов'язані з віддаленою роботою через COVID-19:

Спроби фішингу, пов'язані з COVID-19

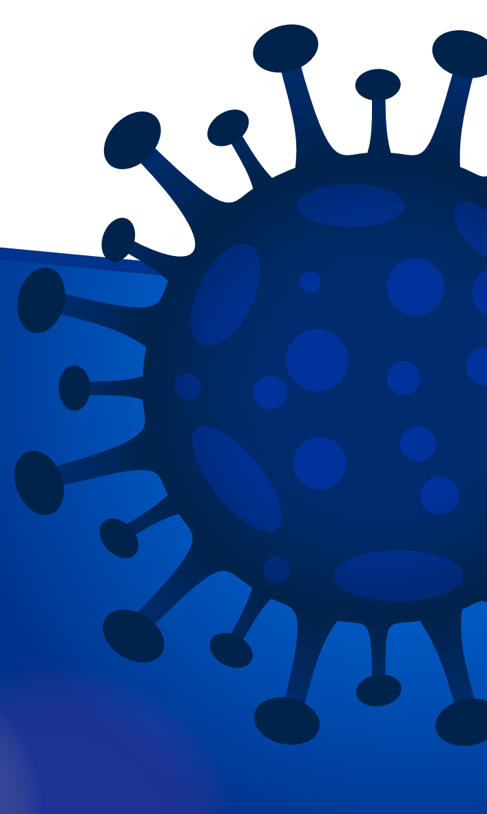
Існує багато прикладів підроблених електронних листів від нібито органів охорони здоров'я, які заманюють людей на веб-сайти для спроби зараження комп'ютера відвідувача. З 23 лютого ми бачимо, що для полегшення таких атак реєструється збільшена кількість веб-сайтів, пов'язаних із COVID-19.

Недостатньо захищені віддалені з'єднання з офісом.

Не всі організації технічно готові забезпечити у великій кількості захищені з'єднання для можливості віддаленої роботи співробітників. IT спеціалісти в умовах браку часу можуть придбати та запропонувати не ті рішення, які будуть найбільш захищеними.

Підвищене використання офісного обладнання для особистих цілей

Працюючи з дому, співробітники мають спокусу використовувати офісне обладнання (наприклад, ноутбук чи телефон) також в особистих цілях. Це може підвищити ризики зараження цих пристроїв вірусами або іншими зловмисними програмами під час відвідування менш захищених веб-сайтів для задоволення особистої зацікавленості. Останнім часом, як відомо, особливо реклама на таких веб-сайтах поширює зловмисне програмне забезпечення.



Чим KPMG може допомогти?

KPMG пропонує великий набір консультаційних послуг у сфері IT та інформаційної безпеки. Проте зважаючи на збільшення кіберзагроз у зв'язку з епідемією COVID-19, ми вважаємо, що наступні пропозиції можуть бути для вас найбільш цікавими:

Перегляд та адаптація планів забезпечення безперервності та відновлення діяльності (BCP та DRP)

Компаніям вкрай важливо продовжувати вести бізнес навіть в умовах кризових ситуацій, надавати безперервно сервіси своїм клієнтам. KPMG пропонує допомогу у перегляді та адаптації поточних BCP/DRP планів, враховуючи взаємозв'язки між компонентами IT-інфраструктури/архітектури, персоналу та процесів компанії в умовах віддаленого доступу до IT сервісів та обмеженого доступу до робочих місць.

Аналіз захищеності мережевої інфраструктури віддаленого доступу

Надання віддаленого доступу до корпоративної мережі та додатків клієнтам, працівникам, партнерам, постачальникам стало необхідністю бізнесу в поточних умовах. Однак некоректно налаштований віддалений доступ може призвести до несанкціонованого доступу зловмисників до вашої внутрішньої інфраструктури та корпоративних даних. KPMG може протестувати захищеність мережевої інфраструктури, задіяної в забезпеченні віддаленої роботи, виявити вразливості в її компонентах та розробити рекомендації щодо їх оперативного усунення.

Оцінка контролів безпеки у процесах, пов'язаних з управлінням віддаленим доступом

KPMG зробить огляд контролів безпеки у процесі організації віддаленої роботи компанії, оцінить їхню відповідність провідним практикам та загальноприйнятим стандартам, запропонує рекомендації щодо їхнього покращення. Це допоможе керівництву компанії зрозуміти, чи правильно функціонують відповідні процеси та чи готова компанія зустрітися з потенційними викликами.

Незалежний радник у складі команди по виходу з кризових ситуацій

Експерти KPMG мають досвід управління кризовою командою реагування на масштабний інцидент кібербезпеки в банку, стримування та очищення систем від зловмисників, проведення розслідування. Експерти KPMG готові виступити незалежними радниками у складі команди компанії з виходу з кризових ситуацій, що можуть бути наслідками інцидентів IT/ІБ, недоступності та переривання ключових сервісів та процесів компанії, недоступності ключового IT-персоналу на робочих місцях або в умовах віддаленого доступу.

Проведення навчального тренінгу з інформаційної безпеки по роботі компанії у період карантину

Проведення навчального тренінгу для керівництва та співробітників з питань безпеки, які мають бути враховані компанією при організації роботи в період карантину. Перелік запропонованих тем для висвітлення може включати, але не обмежуватися наступними: безперервність ведення бізнесу, уникнення вразливостей та слабких місць в інфраструктурі віддаленого доступу, захист від фішингових атак, забезпечення конфіденційності та надійності каналів зв'язку, реагування на кіберінциденти тощо.

Оцінка стійкості співробітників компанії до фішингових атак

З огляду на те, що громадяни усіх країн світу сьогодні зіштовхуються зі страхами та побоюваннями щодо вірусу COVID-19, злочинці також беруть це до уваги. Вони використовують стресовий стан як можливість заволодіти особистою або корпоративною інформацією своїх жертв, спробувати вкрасти в них гроші або паролі від облікових записів. KPMG може провести тестування реакції співробітників вашої компанії на атаки такого типу. Це дозволить оцінити ефективність діючих політик безпеки, існуючих засобів захисту та програм навчання персоналу.

Проведення оцінки щодо готовності до тривалої віддаленої роботи

Експерти KPMG розробили чек-лист для оцінки рівня готовності компанії до тривалої віддаленої роботи та підтримки бізнес процесів. Чек-лист дозволяє критично оцінити готовність IT інфраструктури (наявність VPN каналів, необхідної кількості техніки, засобів аудіо- та відеоконференцій), залежність від зовнішніх постачальників, підрядників, контакт-центрів, ключових IT-спеціалістів. Чек-лист також включає, але не обмежується оцінкою доступності ЦОДів, хмарних сервісів, дозволяє відповісти на питання, чи має компанія план дій на випадок реалізації інциденту IT або інформаційної безпеки. Ми готові виконати таку оцінку та на основі її результатів розробити комплекс коригуючих заходів.

Зв'яжіться з нами

Олексій Янковський

Партнер, керівник практики з
надання консультаційних
послуг у сфері
інформаційних технологій і
кібербезпеки
KPMG в Україні

ayankovski@kpmg.ua

kpmg.ua