KPMG

Питання кібербезпеки в умовах воєнного часу в Україні

Як підготуватися у кіберпросторі

Після місяця військового тиску Росії на Україну в організаціях підвищується рівень занепокоєння щодо можливих кіберінцидентів та стосовно стійкості важливих бізнес функцій. Окрім захисту своїх співробітників і підтримки українського народу, бізнес також оцінює схильність та вразливість своїх критичних сервісів до інцидентів кібербезпеки, технологічних збоїв та впливів з боку ланцюгів постачання. Ці загрози можуть виникати внаслідок атак на системи та інфраструктуру, можуть бути прямим або побічним наслідком воєнних дій. До сих пір залишається багато невизначеностей навколо вторгнення, включаючи його тривалість, масштаби та ступінь ураження. У зв'язку з цим ми підготували рекомендації, що можуть допомогти оцінити рівень готовності вашої кібербезпеки.

Загроза

Спостерігається значне збільшення загроз у кіберпросторі проти українських стратегічних цілей, що доволі очікувано може розповсюдитися на прибічників та союзників України[1]. Уряд Росії зробив рішучі заяви щодо дій, які він збирається вживати проти суб'єктів підприємницької діяльності, які намагаються вийти з країни, включаючи націоналізацію активів[2]. Організації повинні бути готові до потенційного збільшення кібератак у відповідь на такі рішення. Крім того, ті підприємства, які є частиною критичної інфраструктури, включаючи енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни. Незалежно від того, чи локалізована бізнес діяльність компаній в Україні чи інших країнах, вони повинні оцінити свою готовність до кіберінцидентів і свою здатність відновитися після кібератак.

Стійкість і готовність до інцидентів

Необхідно провести огляд наявних планів реагування, щоб краще зрозуміти ризики поточних сценаріїв загроз, які з великою ймовірністю можуть відбутися, враховуючи такі фактори, як профіль компанії, її географію тощо.

Що ви можете зробити

— Перегляньте ландшафт потенційних загроз для вашого бізнесу, налагодьте зв'язок з організаціями, які надають інформацію щодо загроз кібербезпеки аби краще зрозуміти бізнес ризики та заходи, які необхідно вжити.

— Врахуйте імовірність призупинення діяльності в регіонах, де вже відбуваються бойові дії або велика імовірність того, що це може відбутися найближчим часом, і те, як мінімізувати ці ризики для бізнесу, що може включати відключення деяких функцій (наприклад, недоступність частково або повністю IT-інфраструктури або телефонного зв'язку) або впровадження додаткових контролів захисту.

— Перегляньте плани реагування на інциденти та плани неперервності, поставте собі наступні запитання: Як часто ви тестували свої плани? Чи спрацюють тестові сценарії під час поточних загроз?

— Оновіть плани реагування на інциденти безпеки та створіть конкретні плани реагування на програми-вимагачі.

— Перегляньте свої політики страхування в сфері кібербезпеки, в т.ч. умови покриття та будь-які винятки, які можуть бути застосовні у поточній ситуації.

— Переконайтеся, що ваші договори з постачальниками послуг з реагування та стримування атак є актуальними.

— Перегляньте всі нормативні вимоги щодо необхідності звітування про інциденти кібербезпеки.

— Розгляньте можливість проактивного налагодження зв'язків з правоохоронними та державними органами, які мають бути залучені у разі масштабного інциденту кібербезпеки.

— Подумайте про проведення симуляцій реагування на кібератаки, якщо ви не виконували такі вправи протягом останніх 6 місяців.

Кіберзахист

Враховуючи підвищену стурбованість кіберзагрозами, є сенс переглянути ключові набори контролів кібербезпеки, які можуть допомогти знизити імовірність успішності атак — зокрема тих, які допомагають захиститися від загроз від держави-агресора або організованих угруповань, які активізували свою діяльність під час війни.

Що ви можете зробити

— Надайте пріоритет задачам з встановлення виправлень (патчів) усіх критичних вразливостей у системах – особливо для тих, які зараз активно використовуються зловмисниками. Агентство з кібербезпеки та безпеки інфраструктури США (CISA) веде базу даних таких вразливостей, а деякі центри кібербезпеки надають поради щодо того, на які з них слід звернути першочергову увагу.

— Перегляньте контролі доступу до ключових систем, зосереджуючи увагу на багатофакторній аутентифікації, видаленні облікових записів, що не використовуються або термін дії яких закінчився, а також необхідності ізоляції систем, що мають високий ризик.

— Переконайтеся, що захист від шкідливого ПЗ встановлений, ліцензії актуальні і програми регулярно оновлюються.

— Виконуйте зовнішнє сканування вразливостей для систем, що мають доступ до інтернету, і усуньте найбільш важливі недоліки.

— Переконайтеся, що для критичних систем налаштовані процеси резервного копіювання і регулярно створюються офлайн копії важливих бізнес-даних.

[1] Alert: Destructive Malware Targeting Organizations in Ukraine, CISA, March 01, 2022.

[2] Mauro Orru, "Russian Commission Backs Nationalization of Exited Western Businesses" The Wall Street Journal, March 9, 2022.

Моніторинг кібербезпеки

Разом із вживанням заходів превентивного захисту, ефективний моніторинг безпеки є також важливим з огляду на своєчасне виявлення та реагування на вторгнення. Середній час між початковою компрометацією і запуском деструктивного шкідливого ПЗ тепер вимірюється днями, а не тижнями або місяцями, як було раніше.

Що ви можете зробити

— Зрозумійте поточні можливості з моніторингу кібербезпеки у вашій мережевій інфраструктурі, щоб переконатися в існуванні можливостей з виявлення та запобігання інцидентів кібербезпеки та охопленні ними бізнес послуг, систем та даних.

— Якщо у вас є команда з полювання на загрози, доручіть їм пошук індикаторів компрометації (IOC), заснованих на тактиках, техніках та процедурах (TTP's), пов'язаних з групами, що асоціюються з державою-агресором або її партнерами, або організованими злочинними групами, які залучені до війни на кібер-фронті.

— Подумайте про залучення зовнішніх вендорів, що надають послуги керованого виявлення та реагування, з метою розширення ваших можливостей та отримання кваліфікованої підтримки у разі потреби.

Люди

Багато людей зараз перебувають у стані занепокоєння та невизначеності. Підприємствам слід планувати можливу зупинку своєї діяльності в регіонах бойових дій та у деяких випадках організовувати тимчасову кадрову підтримку для забезпечення функціонування своїх критичних сервісів, допоки їхні співробітники не зможуть повернутися до офісу або в країну. Окрім підтримки співробітників та їхніх сімей, організації також повинні знати про ризики організованих злочинних груп. Ці групи намагаються скористатися кризою на свою користь, створюючи підроблені вебсайти, які нібито пропонують допомогу чи корисну інформацію, або приймають пожертвування. Велика ймовірність фішингових кампаній, орієнтованих на тематику війни в Україні і спрямованих на високопоставлених осіб, які відкрито висловлюють свою позицію стосовно війни.

Що ви можете зробити

— Пересвідчитись, що співробітники мають доступ до надійних та перевірених джерел інформації щодо поточної ситуації і є обізнаними щодо ризиків фішингу і шахрайських веб сайтів з тематики війни в Україні.

— Надавати поради з кібербезпеки для співробітників, що знаходяться в місцях потенційного ризику або працюють на високих позиціях.

— Надавати психологічну підтримку співробітникам та їх сім'ям, включаючи проведення тренінгів або семінарів щодо дій в непередбачуваних або кризових ситуаціях.

— Подумайте про термінову додаткову підтримку в управлінні звичайними функціями безпеки, аналізу збільшеного обсягу сповіщень безпеки та реалізації термінових покращень щодо безпеки.

Ризики партнерів, вендорів і ланцюгів поставок

На початку пандемії COVID-19, коли підприємства припиняли свою роботу, а співробітників відправили додому, організації швидко зрозуміли, наскільки залежними вони стали від складної екосистеми третіх сторін, що надають критичні системи, послуги та дані. Воєнний стан в Україні знову підкреслює важливість розуміння безпеки та стійкості усіх партнерів у важливих напрямках ланцюгів поставок.

Що ви можете зробити

— Ідентифікувати залежності від вендорів і партнерів, що знаходяться в України, Росії та сусідніх країнах, та створити резервний план, якщо раптом за певних умов вони будуть виключені з ланцюгів постачання.

— Для критичних постачальників (щонайменше) налаштувати посилений моніторинг вхідного мережевого трафіку, оскільки кіберзлочинність може стати більш витонченою та складною через дії численних хакерських груп, у яких розв'язані руки в поточній ситуації.

— Для критичних постачальників (щонайменше), перевірити наявність та актуальність планів реагування на інциденти та планів забезпечення стійкості.

— Зрозуміти вплив на вашу організацію потенційних інцидентів у ваших ланцюгах поставок, щоб визначити, де саме зосередити посилений моніторинг та підвищити готовність до реагування.

Міграція у хмару

Воєнний стан в Україні викликає занепокоєння компаній також через нові виклики у забезпеченні безперебійної роботи критичних сервісів та систем, які можуть бути пошкоджені або виведені з ладу внаслідок бойових дій. Перенесення IT-інфраструктури в хмару або створення сайтів аварійного відновлення у глобальних хмарних ЦОД дозволить гарантувати необхідний рівень доступності.

Що ви можете зробити

— Проаналізувати наявну IT-архітектуру на предмет можливості та доцільності міграції в хмару, враховуючи технічні (можливість/складність перенесення в хмару), фінансові, регуляторні та питання безпеки

— Обрати провайдера хмарних сервісів, враховуючи наявні компетенції IT-спеціалістів

— Визначити черговість та критичність перенесення тих чи інших елементів IT-архітектури в хмару

— Розглянути та обрати наявні на ринку хмарні сервіси, зокрема для забезпечення віддаленої роботи (проведення відеодзвінків, офісне програмне забезпечення тощо)

— Організувати збереження резервних копій інформації в хмарі

— Організувати сайти аварійного відновлення в публічній хмарі

Наступні кроки

Війна в Україні викликає зростання занепокоєння щодо інцидентів кібербезпеки та стійкості критичних бізнес функцій та послуг. Хоча ситуація сьогодні доволі непередбачувана, постійно аналізуйте, як вона може розвиватися далі, та які сценарії можуть виникнути. Для кожного сценарію оцініть їхній вплив на вашу організацію з огляду на людей, бізнес, ланцюги поставок і технології. При цьому деякі розглянуті рекомендації можна впровадити вже зараз, щоб підготуватися до таких випадків, підвищити стійкість, зменшити вплив і скоротити тривалість інцидентів, якщо вони відбудуться.

Зв’язатися з нами

Олексій Янковський

Партнер, керівник практики з надання консультаційних послуг у сфері IT та кібербезпеки KPMG в Україні

T: +380 (50) 3157995

E: ayankovski@kpmg.ua

Генадій Резниченко

Заступник директора, консультаційні послуги у сфері IT та кібербезпеки

T: +380 (44) 4905507

E: greznichenko@kpmg.ua

Максим Батуренко

Менеджер, консультаційні послуги у сфері IT та кібербезпеки

T: +380 (44) 4905507

E: mbaturenko@kpmg.ua

Артем Кобец

Менеджер, консультаційні послуги у сфері IT та кібербезпеки

T: +380 (44) 4905507

E: artemkobets@kpmg.ua

kpmg.ua