CYBER INSURANCE

СТРАХУВАННЯ КІБЕРРИЗИКІВ

м. ОДЕСА 2020

НАПРЯМКИ ДІЯЛЬНОСТІ

LEGAL OFFICE

Офіс сприяння формуванню державної політики у сфері кібербезпеки:

нормотворча діяльність

ліцензійно – сертифікована діяльність

експертно – оціночна діяльність

ведення реєстрів

COLLABORATION HUB

Платформа взаємодії та обміну:

популяризація, підвищення рівня обізнаності суспільства про кібербезпеку через засоби маркетингової комунікації:

організація та проведення тематичних заходів та зустрічей, хакатонів тощо

організація електронної платформи обміну технічною інформацією

забезпечення обміну досвідом і вирішення комплексних питань

R&D CENTER

Науково – дослідний центр, діяльності якого спрямована на створення умов для впровадження в Україні сучасних технологій кіберзахисту та кібербезпеки:

проведення досліджень

навчання та підвищення кваліфікації

розробка вимог, стандартів та критеріїв сертифікації

науково – дослідницька діяльність із розробки нових продуктів забезпечення кібербезпеки

ГЛОБАЛЬНИЙ РИНОК КІБЕРРИЗИКІВ

Вперше за весь час кіберінциденти (39% відповідей) вважаються найважливішим бізнес-ризиком у всьому світі*, виводячи багаторічні перешкоди бізнесу (37% відповідей) на друге місце.

В 2013 р. ризик кіберзагроз посів лише 15-е місце із лише 6% відповідей.

* - згідно дев'ятого барометру ризику Allianz 2020

CYBER INSURANCE

Кіберстрахування – це страховий продукт для захисту бізнесу і фізичних осіб від ризиків, пов'язаних з користуванням інтернетом, зберіганням і обробкою даних в електронному вигляді, роботою з IT-інфраструктурою.

Кіберстрахування поєднується з іншими інструментами кібербезпеки і дає додатковий захист компаніям з фінансового боку

ГЛОБАЛЬНИЙ РИНОК КІБЕРСТРАХУВАННЯ

В 2020 році розмір глобального ринку кіберстрахування складе 7-8 млрд. $

До 2025 року. очікується, що обсяг глобального ринку кіберстрахування досягне 21,4 млрд. $

ГЛОБАЛЬНИЙ РИНОК КІБЕРСТРАХУВАННЯ

Кіберстрахування має допомогти пом'якшити ризик, компенсуючи витрати на відшкодування наслідків порушення кібербезпеки.

Кібератаки, які здійснюються хакерами, терористами, інсайдерами чи навіть національними державами, можуть спричинити помірні та серйозні збитки.

СЛАБКІ МІСЦЯ

Брак кваліфікованих кадрів у сфері ІБ та брак коштів на постійне підвищення кваліфікації існуючих спеціалістів

Куди звертатись, якщо наслідки кіберінциденту виходять за межі можливостей спеціалістів?

Швидкі гроші на ліквідацію і зупинку наслідків кіберінциденту

Швидка узгодженість виділення коштів з фондів без втрати часу

СЛАБКІ МІСЦЯ

Брак коштів на усунення наслідків кіберінцидентів (відновлення даних, проведення розслідування, судові позови, тощо)

Відповідальність перед третіми особами, клієнтами, партнерами, державою.

Відповідальність за персонал (фішинг, фрод, антикібергініена і т.д.).

0-day атаки

ЩО ПОКРИВАЄ КІБЕРСТРАХУВАННЯ

РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТ

Витрати на послуги експертів в сфері кібербезпеки.
Покриття інцидентів:
DDoS атаки,
фішинг,
вимагачі,
крадіжка даних,
хакерська атака,
комп'ютерний вірус,
хактивізм та ін.

ПЕРЕРВА У ВИРОБНИЦТВІ

Відшкодування втраченого прибутку в результаті порушення роботи IT – систем через кібератаку.

Обсяг прибутку розраховується на основі даних про обіг Компанії.

ВИМАГАЧІ

Відшкодування викупної суми, сплаченої вимагачам, за дешифрування заблокованої інформації, а також, у разі погроз про знищення / пошкодження IT –інфраструктури і даних

ВІДПОВІДАЛЬНІСТЬ ПЕРЕД ТРЕТІМИ ОСОБАМИ

Відшкодування збитків, завданих третім особам внаслідок вчинення кібератаки, відповідно до їх вимог та/або згідно с рішення суду

СОЦІАЛЬНА ІНЖЕНЕРІЯ

Покриває втрату грошових коштів і активів Страхувальника, яка сталася за допомогою застосування технологій соціальної комп'ютерної інженерії

ДОДАТКОВЕ ПОКРИТТЯ

Розслідування інциденту (форензік)
Кризова комунікація (послуги з відбілювання репутації)
Витрати на відновлення даних
Покриття штрафних санкцій

ЩО НЕОБХІДНО ДЛЯ КІБЕРСТРАХУВАННЯ

- заповнена анкета
- оборот організації
- обсяг персональних даних
- сфера діяльності
- необхідний ліміт відповідальності
- необхідне покриття

КІБЕРІНЦИДЕНТ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ 2020рр.

Влада Ізраїлю запідозрені в здійсненні кібератаки на один з ядерних об'єктів Ірану.

Інцидент стався 2 липня 2020р. і спричинив пожежу і потім вибух на підземному об'єкті зі збагачення урану в Натанзі, повідомив іранський високопоставлений чиновник газеті Al-Jareeda.

500 млн. $.
вірус Petya завдав шкоди українській економіці 0,4-0,5% від ВВП

5 млн. $./рік
вартість страхування
від умовних інцидентів,
в т.ч. Petya, які можуть
завдати шкоди в 500 млн. $

Ознака сучасного та ефективного суспільства - це те, що
всі збитки мають сплачуватись Страховими Компаніями.

Отже, пропонуємо разом привести енергетичну сферу України до сучасності та ефективності!

ICU

Non-government organization
INTERNATIONAL CYBERSECURITY UNIVERSITY

OLEKSII KHOMENKO
+380 50 416 57 98
| info@icu-ng.org
| www.icu-ng.org
| oleksii.khomenko@icu-ng.org