Для того, щоб захистити себе, експерти з кібербезпеки пропонують почати зі встановлення якісної антивірусної програми, яка допомагатиме, наприклад, у спробах виявлення фішингу.

Також завжди слід бути пильним щодо джерела, яке запитує конфіденційні дані. Банк, наприклад, навряд чи буде телефонувати, щоб дізнатися код на зворотному боці картки.

Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей. Часто адреса відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд.

Якщо людину просять ввести особисті дані – краще окремо зайти на сайт компанії, наприклад, банку. Ще краще – зателефонувати на офіційний номер установи для уточнення інформації.

Варто також критично ставитися до отриманих повідомлень: наскільки правдоподібною може бути інформація про те, що принц із Саудівської Аравії міг залишити вам спадщину?

Не слід також забувати і про сповіщення про такі небезпеки інших членів сімей. Адже часто літні люди, наприклад, можуть не знати про те, що розголошення CVV-коду банківської картки може призвести до викрадення грошей.

Наскільки б банальний вигляд не мали методи соціальної інженерії у сучасному цифровому світі, люди все ще продовжують потрапляти на її «гачок».

Список використаних джерел

1.«Соціальна інженерія: як шахраї використовують людську психологію в інтернеті» - https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html

2.«Соціальна інженерія (безпека)» - https://uk.wikipedia.org/wiki/%D0%A1%D0% BE%D1%86%D1 %96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5 % D1%80%D1%96%D1%8F_(%D0%B1%D0%B5%D0% B7%D0%BF%D0%B5%D0%BA%D0%B0)

УДК 004.056.5

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРЗАХИСТУ

Кузьмина В. І., Стародубець І. О., студ.гр. КБ-171,
Ткач Ю. М., д.пед.н., доцент
Національний університет «Чернігівська політехніка»

Із широким впровадженням хмарних і мобільних технологій світ зробив об'єкт кібербезпеки нескінченно складним. Крім того, збільшення кількості точок доступу і удавана відсутність виснажливості сучасних хакерів означає, що потреба в створенні адекватних заходів безпеки мережі ніколи не була більш важливою. Утримати попит, як мінімум, складно. Штучний інтелект виявляється ідеальним рішенням.

В контексті інформаційної безпеки штучний інтелект (artificial intelligence, AI) - це ПЗ, здатне інтерпретувати стан середовища, розпізнавати події, які відбуваються в ньому, і самостійно вживати необхідні заходи. AI особливо добре справляється з розпізнаванням закономірностей і аномалій, тому може бути прекрасним інструментом виявлення загроз.

Одна з конкретних областей, в яких кібербезпека, заснована на AI, може збільшити людські IT-команди, - це використання аналітики передбачення. При цьому технологія використовує і старі, і нещодавно розроблені дані. По суті, це може полегшити активний, а не реактивний підхід до мережевої безпеки. Для тих неминучих випадків, коли загрозам вдається пройти, інтелектуальна автоматизація може допомогти у своєчасному та ефективному виявленні, викоріненні і усуненні порушень.

На сьогоднішній день в компаніях вже почали користуватися штучним інтелектом для розпізнавання загроз безпеки і реагування на них.

Зокрема, AI застосовують для виявлення ознак компрометації систем в локальній мережі і в хмарному середовищі. При цьому необхідна обробка гігантських обсягів даних, а в зв'язку з швидкою зміною світового ландшафту загроз, для протистояння їм необхідні найпередовіші технології та методи.

Із використанням систем постійного моніторингу загроз удосконалилася можливість захисту інтелектуальної власності. Адже щоденний трафік даних безпеки, що надходять від великої кількості користувачів та пристроїв, в компаніях зазвичай вимірюється десятками, а то й сотнями ГБайт, і проаналізувати їх повністю вручну, особливо зважаючи на частий дефіцит кадрів, майже неможливо.

Атаки змінюються і стають все складнішими: наприклад, протягом певного часу може мати місце малопомітна шкідлива активність, яка не одразу, але пізніше дасть зловмисникові можливість вкрасти великий обсяг даних. Приклад - SQL-ін'єкції. У жодній компанії світу немає можливості розглядати кожен такий інцендент окремо, щоб з'ясувати, чи вдалася спроба ін'єкції. Інструменти ж AI при накопиченні досить великих зрізів даних системи здатні виявляти дуже ранні ознаки появи нових загроз.

Автоматизовані засоби здатні помітити, коли хтось виконує сканування портів, переходячи від хосту до хосту, або, припустимо, незвичайним способом пересилає великі обсяги даних. Такий аналіз необхідно виконувати швидко, скоротивши до мінімуму час між розпізнаванням і реакцією. Штучний інтелект дозволяє прискорити розбір інцидентів і тим самим **с**прогнозувати серйозність витоку, швидше виявити інциденти і оперативно зреагувати на них, щоб мінімізувати можливі збитки.

Проблеми використання AI

З використанням AI час реакції на нові загрози може скоротитися до декількох хвилин, проте це не прогнозує кардинальних змін у співвідношенні сил між зловмисниками та потерпілими. Ті, хто атакують, теж навчають свої системи AI на атаках на системи захисту, мають повну інформацію про особливості роботи конкретних брендів і підлаштовують способи атаки, під час хибних атак знаходячи, чим саме захищаються ті, хто став ціллю атаки. Масові DDoS-атаки за допомогою автоматичного зараження або підбору паролів великої кількості об'єктів автоматизації, імітація поведінки людини на веб-сайті - це вже реалії сьогоднішнього дня.

Рішення на основі AI сьогодні здатні розпізнавати вже існуючі атаки, а також багато нових їх видів. Проте хакери придумують нові способи злому інформаційних систем, таки само як і захисники розробляють нові засоби і технології захисту. І хто кого переможе - це питання якості розробки. Тут багато чого буде залежати як від швидкодії машин, так і від витонченості і якості алгоритмів.

Ще однією важливою проблемою є те, що недовіра до нововведень ускладнює перехід від традиційних процесів до автоматизації на основі штучного інтелекту - адже крім знання особливостей роботи вашого постачальника не завадять відомості про те, як саме AI приймає рішення. Принципи роботи експертних систем повинні бути зрозумілими, щоб їм можна було довіряти. Розуміючи, як діє система, клієнт дає свої коментарі та побажання, це допомагає вдосконалювати вже існуючі моделі.

Перспективи використання штучного інтелекту в світі кібербезпеки

Виявлення підозрілої активності користувачів і мережевого трафіку - найочевидніше застосування штучного інтелекту. Нинішні системи все успішніше справляються з виявленням незвичайних подій в великих потоках даних, рішенням стандартних завдань аналізу і розсилкою повідомлень.

Наступний крок – використання AI для боротьби з більш складними проблемами. Наприклад, рівень кіберризику для компанії в кожен конкретний момент залежить від безлічі факторів, у тому числі від наявності систем без латок, незахищених портів, надходження повідомлень спрямованого фішингу, рівня надійності паролів, обсягу незашифрованих конфіденційних даних, а також від того, чи є організація об'єктом атаки з боку спецслужб іншої держави.

Доступність точної картини ризиків дозволила б раціональніше використовувати ресурси і розробити більш детальний набір показників ефективності забезпечення безпеки. Сьогодні відповідні дані або не збираються, або не перетворюються на осмислені відомості.

Надалі штучний інтелект буде допомагати компаніям визначатися, в які нові технології безпеки слід вкладатися.

Є великий простір для розвитку. Сьогодні AI використовується в безпеки дуже обмежено. Можна говорити про відставання від інших галузей, і навіть разюче, що самоврядні автомобілі з'являються раніше, ніж мережі, що захищають самі себе. Нинішні платформи AI ще по суті не "розуміють" навколишній світ. Ці технології добре справляються з класифікацією даних, які схожі на зрізи і які використовувалися для навчання. Але штучний інтелект не є по-справжньому розумним - він не може зрозуміти ідею, що лежить в основі тієї чи іншої атаки. Тому людина, як і раніше, є ключовим елементом будь-якого рішення в області кіберзахисту.

І все ж прогрес в боротьбі з кіберзагрозами є. Існує такий напрямок досліджень, як генеративні змагальні мережі, - коли одночасно працюють дві моделі машинного навчання з протилежними цілями. Наприклад, одна намагається щось знайти, а інша - приховати те ж саме від виявлення. Цим принципом можна користуватися при створенні команд умовного противника, щоб з'ясовувати, якими можуть бути нові загрози.

Майбутнє інформаційної безпеки - за інтелектуальними системами, здатними забезпечити глибоку аналітику, прогнозування всього спектру ризиків і загроз. Впровадження таких систем створить необхідність перебудови бізнес-процесів підприємств з урахуванням використання сучасних інформаційних технологій.

Список використаних джерел

1. https://www.osp.ru/cio/2017/10/13053560/
2. https://www.osp.ru/cio/2017/10/13053565/
3. https://ayehu.com/role-artificial-intelligence-cybersecurity/
4. https://www.esecurityplanet.com/network-security/how-ai-is-redefining-cybersecurity.html
5. https://www.cio.ru/articles/181217-Gonka-vooruzheniy-iskusstvennyy-intellekt-i-kiberbezopasnost
6. https://www.cio.ru/articles/071217-Iskusstvennyy-intellekt-na-strazhe-kiberbezopasnosti

---

УДК 004.056.5

НЕЙРОМЕРЕЖА NVIDIA GAUGAN

Полевод О. М., Трощилов М. О., студ. гр. КБ-171

Науковий керівник: **Петренко Т. А.,** ст. викладач кафедри кібербезпеки та математичного моделювання

Національний університет «Чернігівська політехніка»

У 2019 році компанія Nvidia представила розробку нейромережі яка здатна із найпростіших замальовок (лінії та окружності) згенерувати детальні пейзажі природи. GauGAN дозволяє створювати віртуальні світи - і не тільки для розваги, але і для роботи. Так, архітектори, фахівці з ландшафтного дизайну, розробники ігор - всі вони можуть почерпнути щось корисне. Штучний інтелект відразу «розуміє», чого хоче людина і доповнює початкову ідею величезною кількістю деталей. Користувачі цього інструменту можуть змінювати початкову задумку, модифікувати пейзаж або інше зображення, додавати небо, піски, море і т.п., причому додавання відбувається всього за пару секунд. У цій роботі ми хочемо дослідити як саме працює дана технологія і що лежить в її основі.

Генерація зображень

Інструмент побудовано на технології генеративно-конкуруючих мереж (GAN), в основі яких лежить глибинне навчання. У більшості сучасних додатків глибинного навчання використовується нейронний дискримінантний тип (дискримінатор), а SPADE - це генеративна нейронна мережа (генератор).

Дискримінатор займається класифікацією даних, що вводяться. Наприклад, класифікатор зображення - це дискримінатор, який бере зображення і вибирає одну підходящу мітку класу, наприклад, визначає зображення як «собаку», «автомобіль» або «світлофор», тобто вибирає мітку, яка цілком описує зображення. Оскільки зв'язок між зображенням і його