

Въздействие на генеративния изкуствен интелект върху концепцията за киберсигурност

ВЪВЕДЕНИЕ / 8

ГЛАВА I / 15

КОНЦЕПЦИИ ЗА КИБЕРСИГУРНОСТ И РОЛЯТА НА ГЕНЕРАТИВНИЯ ИЗКУСТВЕН ИНТЕЛЕКТ

1. Фундаменти на съвременната концепция за киберсигурност / 15

1.1. Триадата КИН като основополагащ принцип / 16

1.2. „Защита в дълбочина“ като стратегически принцип / 17

1.3. Принципът на „Нулево доверие“ като оперативен принцип / 19

1.4. Принципите на „минималните привилегии“ и

„отграничаване на задълженията“ / 21

1.5. Значение на принципите „сигурност по дизайн“ и „поддържане на опростеност и сигурност“ (KISS) / 22

1.6. Отговор при инциденти, непрекъснатост на бизнеса и възстановяване от бедствия / 24

1.7. Връзка на законите, стандартите, политиките и базовите линии с киберсигурността / 26

1.8. Преход от реакционната същност на киберсигурността към проактивност чрез употребата на генеративен ИИ / 28

2. Изкуствен интелект - същност, функционалност, внедряване и рискове / 30

2.1. Определение за изкуствен интелект / 31

2.2. Етични принципи при разработването на ИИ / 33

2.3. Сигурност на ИИ моделите- нов елемент към класическите принципи на киберсигурността / 37

2.4. Проследимост, прозрачност и доверие, като нови елементи на Триадата КИН в контекста на ИИ / 40

3. Стратегически причини за масовото разпространение на генеративния ИИ / 42

3.1. Широка достъпност и демократизация на изчислителните мощности / 42

3.2. Интеграция в корпоративни и публични платформи / 44

3.3. Технологична надпревара между държави и корпорации / 46

3.4. Генеративен ИИ и автоматизацията на технологичните процеси / 48

3.5. Регулаторно изоставане и правна несъгласуваност / 49

4. Позициониране на генеративния ИИ в динамичната среда на

киберсигурността / 51

- 4.1. Генеративният ИИ като фактор при измененията на дигиталната среда / 51
- 4.2. Двойствения характер на генеративния ИИ като инструмент за защита и вектор на заплахата / 52
- 4.3. Устойчивост на критичната инфраструктура в контекста на ИИ / 54
- 5. Рискове и ограничения при използването на генеративен ИИ / 56
 - 5.1. Халюцинации и генериране на фалшиво или невярно съдържание / 57
 - 5.2. Трудности при проверка достоверността на информацията / 58
 - 5.3. Предубеденост, липса на прозрачност и етични рискове / 59
 - 5.4. ИИ като атакуема повърхност / 60
 - 5.5. Безконтролен ИИ и организационни дефицити / 62
- 6. Обобщение и изводи / 63

ГЛАВА II / 68

ГЕНЕРАТИВНИЯТ ИЗКУСТВЕН ИНТЕЛЕКТ И ВЪЗХОДЪТ НА КИБЕРПРЕСТЪПЛЕНИЯТА ОТ НОВО ПОКОЛЕНИЕ

- 1. Генеративният изкуствен интелект като стратегическо предимство за киберпрестъпниците / 68
 - 1.1. Висока адаптивност и динамично самообучение / 68
 - 1.2. Автоматизация и повишена оперативна ефективност / 71
 - 1.3. Снизен праг за достъпност / 73
 - 1.4. Избягване на засичане и подобрени стратегии за целеполагане / 74
- 2. Технологии и методи за атаки с генеративен ИИ / 77
 - 2.1. Фишинг и социално инженерство / 77
 - 2.2. Генериране и оптимизиране на зловреден софтуер / 81
 - 2.3. Дълбоки фалшификати и синтетични личности като вектор на измама / 82
 - 2.4. Разузнаване и сканиране, базирани на ИИ / 84
 - 2.5. Атаки за удостоверяване и CAPTCHA системи / 84
- 3. Сложни настойчиви заплахы и използването на генеративен ИИ / 85
 - 3.1. Еволюция на тактиките на сложните настойчиви заплахы / 86
 - 3.2. Държавно спонсорираны киберпрестъпны екосистемы / 87
 - 3.3. Сътрудничество между държавно спонсорираны хакерски групи и криминални синдикаты / 89
 - 3.4. Престъпны киберсиндикаты, хакерски общности и ролята на генеративния ИИ / 90

4. Генеративен ИИ и тъмната мрежа / 91

4.1. Пазари за инструменти и AlaaS / 92

4.2. Генеративен ИИ при създаване на фалшиво съдържание / 93

4.3. Прикриване на самоличност, фалшифициране и персонализирани модели за нелегални цели / 94

5. Обобщение и изводи / 95

ГЛАВА III / 103

ГЕНЕРАТИВНИЯТ ИЗКУСТВЕН ИНТЕЛЕКТ В ПРАКТИКИТЕ ПО КИБЕРСИГУРНОСТ

1. Възможни приложения на генеративния изкуствен интелект / 103

1.1. Автоматизация на аналитичната дейност и оперативния цикъл / 104

1.2. Автономна интерпретация и вземане на решения / 106

1.3. „Лов на заплахи“ и индикатори на компрометиране / 107

1.4. Анализ на аномалии и роля на човешкия надзор / 109

2. Генеративен изкуствен интелект в архитектурата на модерната

Киберотбрана / 111

2.1. Генеративен ИИ в предиктивно и симулационно моделиране / 112

2.2. Интеграция с SIEM и SOAR системи / 114

2.3. Екип по киберсигурност, подпомаган от генеративен ИИ / 117

3. Стратегически и организационни измерения на генеративния изкуствен
Интелект / 119

3.1. Интегрирано управление на сигурността, риска и съответствието (GRC) / 119

3.2. Обучение, квалификация и адаптация на експертния състав / 121

3.3. Стратегическа позиция спрямо ИИ и институционална готовност / 124

3.4. Етика, отчетност и алгоритмична прозрачност / 127

4. Рамка за автоматизирано асоцииране на зловредна дейност с известни субекти, извършващи
киберпрестъпления / 129

4.1. Теоретични основи на рамката / 130

4.2. Функционални стъпки на автоматизираната рамка / 133

4.3. Симулационен казус: DarkMist рансъмуер / 138

4.4. Предимства и ограничения на автоматизираната рамка / 139

5. Обобщение и изводи / 141

ЗАКЛЮЧЕНИЕ / 144

