ДӘРІС 2

Кибершабуылдардың жіктелуі, іске асыру механизмдері және шабуыл векторлары

Оқытушы: проф. Ахмедиярова А.Т.

Негізгі түсініктер

Негізгі түсініктер

Кибершабуыл ұғымын, кибершабуылдарды жіктеудің негізгі белгілерін, олардың іске асырылу механизмдерін және шабуыл векторларын жүйелі түрде қарастыру; фишинг, зиянды бағдарламалық қамтылым, ransomware, DDoS, веб-қосымшаларға және жеткізу тізбегіне бағытталған шабуылдардың ерекшеліктерін салыстыру; кибершабуылдың кезеңдері мен қорғаныс шараларының өзара байланысын түсіндіру.

Кибершабуыл және оны жіктеудің қажеттілігі

Кибершабуыл — ақпараттық жүйеге, желіге, бағдарламалық немесе аппараттық құралдарға, цифрлық сервистерге және деректерге қасақана әсер ету арқылы рұқсатсыз қол жеткізуге, ақпаратты ұрлауға, өзгертуге немесе жоюға, сондай-ақ жүйенің қалыпты жұмысын бұзуға бағытталған әрекет. Ақпараттық жүйеде осалдық болған жағдайда қауіп нақты шабуыл түрінде іске асуы мүмкін. Кибершабуылдарды жіктеу қорғаныс жүйесін дұрыс жобалау үшін қажет.

Кибершабуыл және оны жіктеудің қажеттілігі

Бір ғана «шабуыл түрі» ұғымы қауіптің барлық қасиетін ашпайды. Бір шабуыл бір мезгілде бірнеше белгі бойынша сипатталуы мүмкін: оның мақсаты, нысаны, қолданылатын механизмі, жүйе архитектурасындағы орны, бұзушының орналасуы және ықтимал салдары. Сондықтан жіктеу киберқауіпті әртүрлі қырынан бағалауға мүмкіндік береді. Жіктеудің практикалық маңызы — шабуылға сәйкес қорғаныс шарасын таңдау.

Кибершабуыл және оны жіктеудің қажеттілігі

Кибершабуыл және оны жіктеудің қажеттілігі

Мысалы, қолжетімділікті бұзуға бағытталған DDoS-шабуыл үшін трафикті сүзу мен резервтеу маңызды болса, тіркелгі деректерін алуға бағытталған фишинг үшін көпфакторлы аутентификация, пошта сүзгілері және пайдаланушыларды оқыту маңызды.

Мақсаты бойынша жіктеу

Кибершабуылдың мақсаты ақпараттық қауіпсіздіктің негізгі қасиеттерімен байланысты. Құпиялылыққа бағытталған шабуыл ақпаратты рұқсатсыз алуды көздейді. Тұтастыққа бағытталған шабуыл ақпаратты немесе жүйелік параметрлерді рұқсатсыз өзгертеді. Қолжетімділікке бағытталған шабуыл заңды пайдаланушының сервиске немесе дерекке қол жеткізуін шектейді.

Нысаны бойынша жіктеу

Шабуыл нысаны — шабуылдаушы әсер етуге тырысатын ақпараттық актив. Қазіргі ақпараттық инфрақұрылымда нысан ретінде тек компьютер немесе сервер ғана емес, пайдаланушы тіркелгісі, веб-қосымша, мобильді құрылғы, бұлттық сервис, API, желілік құрылғы және деректер қоры да қарастырылады. Нысанды дұрыс анықтау мониторинг деректерінің қай көздерін талдау керектігін көрсетеді.

Кибершабуылдардың іске асырылу механизмдері

Кибершабуылдардың іске асырылу механизмдері

Іске асыру механизмі — шабуылдаушының қауіп мақсатына жету үшін қолданатын негізгі тәсілі. Қазіргі кибершабуылдарда әлеуметтік манипуляция, бағдарламалық осалдықтарды пайдалану, зиянды бағдарламаларды енгізу, тіркелгі деректерін заңсыз қолдану және көптеген бұзылған құрылғыларды бір мезгілде пайдалану сияқты механизмдер кездеседі.

Шабуыл векторы ұғымы

Шабуыл векторы — шабуылдаушының мақсатты жүйеге бастапқы қолжетімділік алуына немесе оған әсер етуіне мүмкіндік беретін жол. Векторды шабуыл түрімен шатастырмау керек. Мысалы, электрондық пошта шабуыл векторы болуы мүмкін, ал сол арна арқылы іске асырылатын әрекет фишинг немесе зиянды файлды тарату болуы мүмкін.

Шабуыл векторы ұғымы

Шабуыл векторын талдау кезінде үш сұрақ маңызды: шабуыл қай арнадан келеді, қандай осалдық немесе әлсіздік пайдаланылады және қандай активке әсер етеді. Осы байланыс қорғаныс құралдарын дұрыс орналастыруға мүмкіндік береді.

Кең таралған кибершабуыл түрлерін салыстыру

Кең таралған кибершабуыл түрлерін салыстыру

Қазіргі киберқауіпсіздік әдебиеттерінде фишинг, ransomware, DDoS, жеткізу тізбегіне бағытталған шабуылдар және зиянды бағдарламалық қамтылым кең таралған қауіптер ретінде қарастырылады. Олардың мақсаттары мен іске асырылу механизмдері әртүрлі болғандықтан, анықтау белгілері мен қорғаныс тәсілдері де өзгеше.

Кибершабуылдың кезеңдік моделі

Күрделі кибершабуыл көбінесе бір ғана әрекеттен тұрмайды. Ол өзара байланысты бірнеше кезеңнен құралады. Кезеңдік талдау қауіпсіздік маманына шабуылдың қай сатыда тұрғанын анықтауға және оны ертерек тоқтатуға мүмкіндік береді. Ақпарат жинау кезеңінде мақсатты ұйым, оның сервистері, пайдаланушылары және ықтимал кіру нүктелері туралы мәлімет жиналады.

Кибершабуылдың кезеңдік моделі

Бастапқы қолжетімділік кезеңінде фишинг, осал сервис немесе басқа вектор арқылы ортаға кіруге әрекет жасалады. Кейін шабуылдаушы қолжетімділікті сақтауға, құқықтарын кеңейтуге және желі ішінде басқа активтерге өтуге тырысуы мүмкін. Соңғы кезеңде деректерді ұрлау, өзгерту, жою немесе сервисті тоқтату сияқты мақсатты әсер орын алады.

Кибершабуылдың кезеңдік моделі

Кибершабуылдың кезеңдік моделі

Қорғаныс тұрғысынан әр кезеңде әртүрлі телеметрия маңызды: электрондық пошта журналдары, аутентификация оқиғалары, хост процестері, желілік қосылымдар, файл өзгерістері және деректерге қол жеткізу журналдары. Интеллектуалды анықтау жүйесі осы әртекті деректерді біріктіріп, жеке әлсіз сигналдардың арасындағы байланысты анықтауға мүмкіндік береді.

Кибершабуыл белгілері және анықтау индикаторлары

Шабуыл индикаторы — жүйеде күмәнді немесе зиянды белсенділіктің болуы мүмкін екенін көрсететін белгі. Бір индикатордың өзі әрқашан шабуылдың дәлелі бола бермейді. Сондықтан контекст, уақыт, активтің маңыздылығы және басқа оқиғалармен байланыс бірге қарастырылады.

Қорғаныс шараларын шабуыл түрімен сәйкестендіру

Тиімді қорғаныс «бір қауіп — бір құрал» қағидасына ғана сүйенбейді. Бір шабуылға бірнеше қорғаныс қабаты қарсы тұруы тиіс. Алдын алу шаралары бастапқы қолжетімділікті қиындатады, анықтау құралдары күмәнді белсенділікті байқайды, ал әрекет ету және қалпына келтіру шаралары шабуыл салдарын шектейді.

Интеллектуалды құралдардың жіктеу мен анықтаудағы рөлі

Интеллектуалды құралдардың жіктеу мен анықтаудағы рөлі

Кибершабуылдарды жіктеу интеллектуалды анықтау жүйелерін құру кезінде де маңызды. Машиналық оқыту моделіне берілетін класс белгілері шабуылдардың таңдалған жіктеуіне тәуелді. Екі класты модель «қалыпты/шабуыл» деп ажыратса, көпкласты модель фишинг, DDoS, malware немесе басқа санаттарды бөлек анықтауға бағытталуы мүмкін. Интеллектуалды жүйе үшін деректердің сапасы шешуші мәнге ие.

Интеллектуалды құралдардың жіктеу мен анықтаудағы рөлі

Егер оқыту жиынында шабуыл түрлері теңгерімсіз болса немесе бір класқа әртүрлі механизмдер ретсіз біріктірілсе, модельдің нәтижесі бұрмалануы мүмкін. Сондықтан кибершабуыл таксономиясы тек теориялық жіктеу емес, деректерді белгілеу, модельді оқыту және нәтижелерді түсіндіру үшін қолданылатын практикалық негіз болып табылады. Интеллектуалды талдау дәстүрлі қорғаныс құралдарын алмастырмайды.

Интеллектуалды құралдардың жіктеу мен анықтаудағы рөлі

Ол сигнатуралық ережелер, IDS/IPS, журналдау, желілік мониторинг және қауіпсіздік маманының талдауымен бірге қолданылғанда тиімді. Бұл пәннің келесі лекцияларында сигнатуралық және аномалиялық анықтау, желілік трафикті талдау және машиналық оқыту модельдері жеке қарастырылады.

Қорытынды

Қорытынды

Кибершабуылдарды жіктеу олардың мақсатын, нысанын, іске асыру механизмін, шабуыл векторын және ықтимал салдарын жүйелі түрде сипаттауға мүмкіндік береді. Бір шабуыл бірнеше жіктеу белгісіне бір мезгілде сәйкес келуі мүмкін, сондықтан қорғаныс кезінде тек шабуыл атауын емес, оның нақты контекстін талдау қажет.

Қорытынды

Фишинг, ransomware, DDoS, зиянды бағдарламалық қамтылым және жеткізу тізбегіне бағытталған шабуылдар іске асырылу тәсілі, анықтау белгілері және қорғаныс шаралары бойынша ерекшеленеді. Кибершабуылды кезеңдерге бөлу және шабуыл векторларын анықтау қауіптің ерте сатысында қорғаныс шараларын қолдануға мүмкіндік береді.

Қорытынды

Интеллектуалды киберқорғаныс жүйелерінде шабуылдардың дұрыс жіктелуі деректерді белгілеу, модель класын анықтау, аномалияларды түсіндіру және автоматтандырылған әрекет ету шешімдерін қалыптастыру үшін негіз болады.

Бақылау сұрақтары

Бақылау сұрақтары

1. Кибершабуыл дегеніміз не және оны жіктеу не үшін қажет? 2. Кибершабуылдар қандай негізгі белгілер бойынша жіктеледі? 3. Құпиялылыққа, тұтастыққа және қолжетімділікке бағытталған шабуылдардың айырмашылығы қандай? 4. Шабуыл механизмі мен шабуыл векторының айырмашылығын түсіндіріңіз. 5. Әлеуметтік инженерия мен осалдықты пайдалануға негізделген шабуылдардың ерекшеліктері қандай? 6.

Бақылау сұрақтары

Фишинг, ransomware және DDoS шабуылдарын негізгі белгілері бойынша салыстырыңыз. 7. Жеткізу тізбегіне бағытталған шабуылдың ерекшелігі неде? 8. Кибершабуылдың кезеңдік моделінің қорғаныс үшін маңызы қандай? 9. Шабуыл индикаторлары қандай дерек көздерінен анықталуы мүмкін? 10. Кибершабуылдарды жіктеу интеллектуалды анықтау жүйелерін құруға қалай әсер етеді?

Список источников

1. Менщиков А.А., Заколдаев Д.А., Воробьева А.А. Введение в кибербезопасность и киберустойчивость: учебно-методическое пособие. — Санкт-Петербург: Университет ИТМО, 2024. — 72 с. 2. Вострецова Е.В. Основы информационной безопасности: учебное пособие. — Екатеринбург: Издательство Уральского университета, 2019. — 204 с. — ISBN 978-5-7996-2677-8. 3. Назарян А.К., Карцан И.Н.

Негізгі әдістер мен сипаттамаларды салыстыру

Жіктеу белгісі	Сипаттамасы	Мысал
Мақсаты бойынша	Шабуыл нәтижесінде қандай қауіпсіздік қасиетін немесе бизнес-процесті бұзу көзделетінін көрсетеді	Деректерді ұрлау, өзгерту, сервисті тоқтату
Нысаны бойынша	Шабуыл бағытталған актив немесе ақпараттық ресурс анықталады	Пайдаланушы, сервер, желі, веб-қосымша, деректер қоры
Іске асыру механизмі бойынша	Шабуылдаушы қолданатын негізгі әдіс немесе техникалық тәсіл сипатталады	Әлеуметтік инженерия, осалдықты пайдалану, зиянды БҚ
Шабуыл векторы бойынша	Мақсатты жүйеге әсер ету немесе бастапқы қолжетімділік алу жолы көрсетіледі	Электрондық пошта, веб-интерфейс, қашықтан қолжетімділік сервисі
Бұзушының орналасуы бойынша	Шабуыл көзінің қорғалатын жүйеге қатысты орны анықталады	Сыртқы немесе ішкі бұзушы

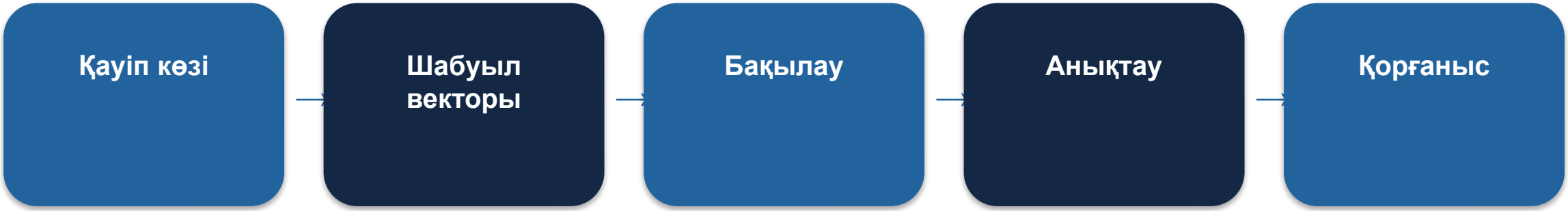
Негізгі әдістер мен сипаттамаларды салыстыру

Мақсат	Анықтамасы	Негізгі белгісі	Ықтимал салдары
Құпиялылықты бұзу	Қорғалған ақпаратқа рұқсатсыз қол жеткізу	Деректердің сыртқа шығуы немесе есептік жазбаның бұзылуы	Құпия ақпараттың жария болуы, қаржылық және беделдік шығын
Тұтастықты бұзу	Ақпаратты немесе жүйе күйін рұқсатсыз өзгерту	Файлдар, жазбалар немесе конфигурациялардың өзгеруі	Қате шешімдер, деректерге сенімнің жоғалуы
Қолжетімділікті бұзу	Ресурсты заңды пайдаланушы үшін қолжетімсіз ету	Сервис өнімділігінің төмендеуі немесе тоқтауы	Бизнес-процестің үзілуі, қызмет көрсетудің тоқтауы

Негізгі әдістер мен сипаттамаларды салыстыру

Шабуыл нысаны	Ерекшелігі	Бақыланатын белгілер	Негізгі қорғаныс
Пайдаланушы	Адам факторы мен тіркелгі деректері нысана болады	Күмәнді хаттар, әдеттен тыс кіру, көптеген аутентификация әрекеті	MFA, awareness, қолжетімділікті басқару
Желі	Желілік байланыстар мен сервистерге әсер етеді	Трафик көлемі, порттар, қосылым жиілігі, аномалиялық ағындар	Firewall, IDS/IPS, сегментация
Сервер/хост	ОЖ, қызметтер және файлдық жүйе нысана болады	Процестер, журналдар, файл өзгерістері, құқықтардың өзгеруі	EDR, жаңарту, least privilege
Веб-қосымша	HTTP/HTTPS арқылы қолжетімді функциялар нысана болады	Күмәнді параметрлер, қате сұраныстар, аномалиялық сессиялар	Қауіпсіз әзірлеу, WAF, тестілеу
Деректер	Ақпаратты ұрлау, өзгерту немесе жою көзделеді	Көп көлемді оқу/көшіру, рұқсат өзгерістері	Шифрлау, DLP, резервтік көшіру

Жүйенің жалпы жұмыс істеу архитектурасы



Әр кезеңнің нәтижесі келесі кезеңнің кіріс дерегі болады. Мониторинг пен тексеру нәтижелері қорғаныс шешімін нақтылауға мүмкіндік береді.

Түйінді ұғымдар және қолданылуы

Негізгі түсініктер

Кибершабуыл ұғымын, кибершабуылдарды жіктеудің негізгі белгілерін, олардың іске асырылу механизмдерін және шабуыл векторларын жүйелі түрде қарастыру; фишинг, зиянды бағдарламалық қамтылым, ransomware, DDoS, веб-қосымшаларға және жеткізу тізбегіне бағытталған шабуылдардың ерекшеліктерін салыстыру; ки

Кибершабуыл және оны жіктеудің қажеттілігі

Кибершабуыл — ақпараттық жүйеге, желіге, бағдарламалық немесе аппараттық құралдарға, цифрлық сервистерге және деректерге қасақана әсер ету арқылы рұқсатсыз қол жеткізуге, ақпаратты ұрлауға, өзгертуге немесе жоюға, сондай-ақ жүйенің қалыпты жұмысын бұзуға бағытталған әрекет. Ақпараттық жүйеде осалдық

Кибершабуыл және оны жіктеудің қажеттілігі

Бір ғана «шабуыл түрі» ұғымы қауіптің барлық қасиетін ашпайды. Бір шабуыл бір мезгілде бірнеше белгі бойынша сипатталуы мүмкін: оның мақсаты, нысаны, қолданылатын механизмі, жүйе архитектурасындағы орны, бұзушының орналасуы және ықтимал салдары. Сондықтан жіктеу киберқауіпті әртүрлі қырынан бағалауғ

Кибершабуыл және оны жіктеудің қажеттілігі

Мысалы, қолжетімділікті бұзуға бағытталған DDoS-шабуыл үшін трафикті сүзу мен резервтеу маңызды болса, тіркелгі деректерін алуға бағытталған фишинг үшін көпфакторлы аутентификация, пошта сүзгілері және пайдаланушыларды оқыту маңызды.

Қорытынды және талдау сұрақтары

Негізгі қорытынды

Кибершабуылдардың жіктелуі, іске асыру механизмдері және шабуыл векторлары. Қорғаныс шешімін қабылдағанда деректер сапасы, жүйенің контексті және тәуекел деңгейі бірге бағаланады.

Талдау тапсырмасы

Берілген жүйе үшін негізгі активтерді, қауіп белгілерін, анықтау әдісін және қорғаныс шараларын бір сызбада көрсетіңіз.

Салыстыру

Қарастырылған тәсілдердің артықшылықтары мен шектеулерін нақты мысал арқылы түсіндіріңіз.