ЛЕКЦИЯ 2

Кибершабуылдардың жіктелуі, іске асыру механизмдері және шабуыл векторлары

Лекция мақсаты

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. 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. 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.

Кибершабуылдарды жіктеудің негізгі белгілері

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
Әсер ету сипаты бойынша	Шабуылдың ақпарат пен жүйеге тигізетін нәтижесі бағаланады	Ақпараттың жария болуы, бұрмалануы, қолжетімсіздігі

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.

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

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.

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

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.

Механизм	**Анықтамасы**	**Ерекшелігі**	**Артықшылығы (шабуылдаушы үшін)**	**Кемшілігі/шектеуі**	**Қорғаныс бағыты**
Әлеуметтік инженерия	Адамның сенімі мен мінез-құлқын пайдалану арқылы қажетті әрекетті орындату	Техникалық осалдықтан гөрі адам факторына сүйенеді	Күрделі техникалық құралды қажет етпеуі мүмкін	Пайдаланушы күмәнді әрекетті таныса, шабуыл тоқтайды	Оқыту, пошта сүзгісі, MFA
Осалдықты пайдалану	Бағдарламадағы немесе конфигурациядағы әлсіздікті қолдану	Нақты техникалық әлсіздікке тәуелді	Жүйеге тікелей әсер етуі мүмкін	Патч орнатылса немесе осалдық жабылса тиімсіз	Patch management, vulnerability management
Зиянды БҚ	Зиянды код арқылы рұқсатсыз функцияларды орындау	Файлдық, процестік және желілік белгілер қалдыруы мүмкін	Бірнеше зиянды функцияны біріктіре алады	Антивирус/EDR және мінез-құлықтық талдау арқылы анықталуы мүмкін	EDR, allowlisting, сегментация
Тіркелгі деректерін пайдалану	Ұрланған немесе әлсіз логин/пароль арқылы заңды пайдаланушы атынан кіру	Қалыпты аутентификацияға ұқсас болуы мүмкін	Қорғанысты айналып өту ықтималдығы жоғары	MFA және мінез-құлықтық талдау әсерін төмендетеді	MFA, IAM, UEBA
Ботнет/тараты лған әсер	Көптеген бұзылған құрылғыны бір мақсатқа бағыттау	Көп көзден келетін трафик	Үлкен көлемді әсер қалыптастырады	Трафикті сүзу және DDoS-қорғаныс арқылы шектеледі	Rate limiting, anti-DDoS, резервтеу

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 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.

Шабуыл векторы	**Пайдаланылатын әлсіздік**	**Нысан**	**Бақылау/қорғаныс**
Электрондық пошта	Пайдаланушы сенімі, зиянды тіркеме немесе сілтеме	Пайдаланушы, жұмыс станциясы	Пошта сүзгісі, sandbox, awareness
Веб-интерфейс	Енгізуді тексерудің жеткіліксіздігі, қате конфигурация	Веб-қосымша, деректер	WAF, secure coding, тестілеу
Қашықтан қолжетімділік	Әлсіз пароль, артық ашық сервис	Сервер, тіркелгі	MFA, access control, журналдау
Үшінші тарап/жеткізу тізбегі	Сенімді компонент немесе жеткізушінің бұзылуы	Ұйым инфрақұрылымы	Жеткізуші тәуекелін бағалау, тұтастықты тексеру
Желілік сервис	Осал немесе дұрыс бапталмаған сервис	Желі, сервер	Сегментация, патчтау, IDS/IPS

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.

Шабуыл түрі	**Анықтамасы**	**Негізгі ерекшелігі**	**Артықшылығы (шабуылдаушы үшін)**	**Кемшілігі/ шектеуі**	**Негізгі қорғаныс**
Фишинг	Алдау арқылы құпия ақпаратты алуға немесе қауіпті әрекет орындатуға бағытталған шабуыл	Адам факторын пайдаланады	Техникалық осалдықсыз да нәтиже беруі мүмкін	Хабарламаның күмәнді белгілері анықталуы мүмкін	Awareness, MFA, email security
Ransomware	Деректерге/жүйеге қолжетімділікті шектеп, бопсалауға бағытталған зиянды шабуыл	Бизнес-процесті тоқтатуы мүмкін	Ұйымға жоғары қысым жасайды	Резервтік көшірме және сегментация әсерін төмендетеді	Backup, EDR, сегментация
DDoS	Көптеген көзден шамадан тыс трафик жіберіп, сервистің қолжетімділігін бұзу	Таратылған сипат	Үлкен трафик көлемін қалыптастырады	Anti-DDoS және масштабтау арқылы шектеледі	Фильтрация, rate limiting, резервтеу
Зиянды БҚ	Рұқсатсыз немесе зиянды әрекет	Әртүрлі функция	Жасырын әрекет пен	Файлдық және мінез-	EDR/антивирус, allowlisting

	орындайтын бағдарламалық код	атқара алады	автоматтандыру мүмкіндігі	құлықтық белгілер қалдырады	
Supply Chain	Сенімді жеткізуші немесе компонент арқылы мақсатты ортаға әсер ету	Сенім қатынасын пайдаланады	Бір компрометация көптеген ұйымға әсер етуі мүмкін	Жеткізу тізбегін бақылау мен тұтастық тексеруі тәуекелді азайтады	Third-party risk, integrity control

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	**Бастапқы қолжетімділік**	**Жүйеде орнығу**	**Құқықтарды кеңейту**	**Ішкі ортада қозғалу**	**Мақсатты активке әсер ету**

Ақпарат жинау кезеңінде мақсатты ұйым, оның сервистері, пайдаланушылары және ықтимал кіру нүктелері туралы мәлімет жиналады. 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.

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.

Индикатор тобы	**Мысал белгілер**	**Қандай шабуылмен байланысты болуы мүмкін**
Аутентификация	Көптеген сәтсіз кіру, жаңа геолокация, әдеттен тыс уақыт	Тіркелгі деректерін пайдалану, brute-force белгілері
Желілік трафик	Трафик көлемінің күрт өсуі, сирек порттар, көптеген қысқа қосылым	DDoS, сканерлеу, зиянды желілік белсенділік
Хост оқиғалары	Белгісіз процесс, күтпеген файл өзгерісі, құқықтардың өзгеруі	Malware, ransomware, privilege escalation
Веб-журналдар	Қалыптан тыс параметрлер, көп қате сұраныс, әдеттен тыс URI	Веб-шабуылдар, автоматтандырылған барлау
Деректермен жұмыс	Көп көлемді оқу/көшіру, ерекше уақытта экспорт	Деректердің сыртқа шығарылуы

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.

Шабуыл/тәуекел	**Алдын алу**	**Анықтау**	**Әрекет ету және қалпына келтіру**
Фишинг	Оқыту, MFA, пошта сүзгісі	Күмәнді хат/сілтеме талдауы, кіру аномалиялары	Тіркелгіні бұғаттау, парольді ауыстыру, сессияны тоқтату
DDoS	Архитектуралық резервтеу, лимиттер	Трафик көлемі мен ағын аномалияларын бақылау	Фильтрацияны күшейту, трафикті қайта бағыттау
Malware/Ransomware	Патчтау, allowlisting, сегментация	EDR, файл/процесс мінез-құлқын талдау	Хостты оқшаулау, қалпына келтіру, резервтік көшірме
Веб-шабуыл	Secure coding, конфигурацияны қатайту	WAF, веб-журналдарды талдау	Осал компонентті түзету, сессияларды қайта қарау
Supply Chain	Жеткізушілерді бағалау, компонент тұтастығы	Жаңарту мен компонент мінез-құлқын мониторингтеу	Компонентті оқшаулау/ауыстыру, тәуелділіктерді тексеру

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. 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. 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

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.

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.

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

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. 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. Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление. — 2025. — Т. 4, № 1. — С. 1001–1007. — DOI: 10.47813/2782-5280-2025-4-1-1001-1007.