ЛЕКЦИЯ 1
Киберқауіпсіздік, кибертұрақтылық және қазіргі кибершабуылдардың даму үрдістері

Лекция мақсаты

Киберқауіпсіздік, киберқауіп, осалдық, кибершабуыл және кибертұрақтылық ұғымдары туралы жүйелі түсінік қалыптастыру; қазіргі кибершабуылдардың негізгі түрлерін, мақсаттарын және даму үрдістерін қарастыру; кибершабуылдарды анықтау мен оларға қарсы әрекет етудің негізгі тәсілдерін және интеллектуалды технологиялардың киберқауіпсіздіктегі рөлін түсіндіру.

Киберқауіпсіздік туралы негізгі түсініктер

Қазіргі қоғамда ақпараттық жүйелер мемлекеттік басқару, өндіріс, қаржы, білім беру, медицина, көлік және басқа салалардың ажырамас бөлігіне айналды. Ақпараттық ресурстардың интернетпен, бұлттық сервистермен, мобильді құрылғылармен және сыртқы жүйелермен байланысуы олардың мүмкіндіктерін арттырады, бірақ сонымен бірге шабуыл бетінің кеңеюіне әкеледі.

Киберқауіпсіздік — ақпараттық жүйелерді, компьютерлік желілерді, бағдарламалық және аппараттық құралдарды, цифрлық сервистер мен деректерді киберкеңістікте туындайтын қауіптерден қорғауға бағытталған ұйымдастырушылық, техникалық және бағдарламалық шаралар жиынтығы. Киберқауіпсіздіктің міндеті шабуылдың алдын алумен ғана шектелмейді. Ол қауіпті анықтау, оқиғаны талдау, залалды шектеу, инцидентке әрекет ету және жүйенің қалыпты жұмысын қалпына келтіру процестерін де қамтиды.

Ақпараттық қауіпсіздіктің классикалық негізі құпиялылық, тұтастық және қолжетімділік қасиеттерімен сипатталады. Құпиялылық ақпаратқа тек тиісті рұқсаты бар тұлғалардың қол жеткізуін білдіреді. Тұтастық ақпараттың рұқсатсыз өзгертілмеуін және бұрмаланбауын қамтамасыз етеді. Қолжетімділік заңды пайдаланушының қажетті уақытта ақпараттық ресурсқа немесе сервиске қол жеткізу мүмкіндігін сипаттайды.

Киберқауіп, осалдық және кибершабуыл

Киберқауіп — ақпараттық жүйеге, желіге, деректерге немесе цифрлық инфрақұрылымға зиян келтіруі мүмкін ықтимал жағдай, оқиға немесе әрекет. Қауіптің болуы міндетті түрде шабуыл жасалды дегенді білдірмейді; ол зиян келтіру мүмкіндігін сипаттайды.

Осалдық — бағдарламалық немесе аппараттық құралдың, желілік архитектураның, конфигурацияның немесе ұйымдастырушылық процестің қауіп көзі пайдалана алатын әлсіз тұсы. Осалдық бағдарламалық кодтағы қателерден, ескірген бағдарламалық қамтылымнан, дұрыс емес конфигурациядан, әлсіз парольдерден, артық құқықтардан немесе қауіпсіздік жаңартуларының орнатылмауынан туындауы мүмкін.

Кибершабуыл — ақпараттық жүйенің немесе цифрлық ресурстың құпиялылығын, тұтастығын немесе қолжетімділігін бұзуға, рұқсатсыз қол жеткізуге, ақпаратты ұрлауға, өзгертуге, жоюға немесе жүйенің жұмысын бұзуға бағытталған қасақана әрекет. Киберинцидент — ақпараттық жүйенің қауіпсіздігіне нақты әсер еткен немесе әсер етуі мүмкін оқиға.

Бұл ұғымдардың өзара байланысын келесі логикалық тізбекпен көрсетуге болады: қауіп көзі → осалдық → шабуыл векторы → кибершабуыл → киберинцидент → салдар. Қорғаныс жүйесінің мақсаты — осы тізбектің мүмкіндігінше ерте кезеңінде қауіпті анықтап, оның әрі қарай дамуына жол бермеу.

Кибершабуылдың негізгі элементтері

Кибершабуылды жүйелі талдау үшін шабуыл субъектісі, шабуыл нысаны және шабуыл векторы қарастырылады. Шабуыл нысаны сервер, жұмыс станциясы, веб-қосымша, деректер қоры, желілік құрылғы, пайдаланушы тіркелгісі, мобильді құрылғы немесе бұлттық сервис болуы мүмкін.

Шабуыл векторы — шабуылдаушының мақсатты жүйеге қол жеткізу немесе оған әсер ету үшін пайдаланатын жолы немесе тәсілі. Фишингтік хабарлама, осал веб-қосымша, әлсіз пароль, дұрыс бапталмаған желілік сервис, зиянды файл немесе жеткізу тізбегіндегі осал компонент шабуыл векторы бола алады. Қазіргі күрделі кибершабуылдарда бірнеше вектор бір сценарийде қатар қолданылуы мүмкін.

Кибершабуылдардың негізгі мақсаттары

Қазіргі кибершабуылдардың мақсаттарына құпия ақпаратты ұрлау, ақпараттық жүйеге рұқсатсыз қол жеткізу, сервистің жұмысын тоқтату, деректерді өзгерту немесе жою, қаржылық пайда табу, бопсалау және барлау жатады. Сондықтан шабуылды оның техникалық механизмі бойынша ғана емес, көздеген мақсаты, нысаны және ықтимал салдары бойынша да бағалау қажет.

DDoS-шабуыл көбінесе сервистің қолжетімділігін бұзуға бағытталса, фишинг пайдаланушының тіркелгі деректерін алуға бағытталуы мүмкін. Ransomware деректерге қолжетімділікті шектеп, қаржылық талап қоюмен байланысты. Жеткізу тізбегіне бағытталған шабуыл сенімді бағдарламалық немесе сервистік компонент арқылы көптеген ұйымдарға бір мезгілде әсер етуі мүмкін.

Қазіргі кибершабуылдардың негізгі түрлері

Фишинг (Phishing) — пайдаланушыны алдау арқылы құпия ақпаратты алуға немесе белгілі бір қауіпті әрекетті орындатуға бағытталған әлеуметтік инженерия әдісі. Ол электрондық пошта, жалған веб-сайт, хабар алмасу жүйесі немесе басқа цифрлық байланыс арналары арқылы жүзеге асырылуы мүмкін. Фишингтің ерекшелігі — техникалық осалдықтан бұрын адам факторын пайдалану.

Зиянды бағдарламалық қамтылым (Malware) — ақпараттық жүйеге зиян келтіруге, рұқсатсыз әрекеттер орындауға, ақпаратты жинауға немесе жүйенің қалыпты жұмысын бұзуға арналған бағдарламалық код. Оны анықтау кезінде файл сипаттары, процестер, жүйелік оқиғалар, желілік белсенділік және бағдарламаның мінез-құлқы талданады.

Ransomware — деректерге немесе ақпараттық жүйенің ресурстарына қолжетімділікті шектеу арқылы бопсалауға бағытталған зиянды бағдарламалық шабуыл түрі. Мұндай шабуылдың салдары бір компьютермен шектелмей, ұйымның негізгі бизнес-процестерінің тоқтауына әкелуі мүмкін.

DDoS (Distributed Denial of Service) — көптеген көздерден мақсатты ресурсқа шамадан тыс сұраныс немесе трафик жіберу арқылы оның қолжетімділігін төмендетуге бағытталған таратылған шабуыл. Мұндай шабуылдарда жұқтырылған құрылғылардан құралған ботнеттер қолданылуы мүмкін.

Жеткізу тізбегіне бағытталған шабуыл (Supply Chain Attack) кезінде мақсатты ұйымға тікелей шабуыл жасаудың орнына оған бағдарламалық өнім, компонент, жаңарту немесе сервис жеткізетін сенімді тарап пайдаланылады. Мұндай шабуылдың қауіптілігі — бір компрометацияның көптеген тәуелді жүйелерге таралу мүмкіндігі.

Кибершабуылдарды іске асыру механизмдері

Әлеуметтік инженерия кезінде шабуылдаушы ақпараттық жүйенің техникалық осалдығын емес, адамның сенімін, абайсыздығын немесе қауіпсіздік туралы білімінің

жеткіліксіздігін пайдаланады. Сондықтан пайдаланушыларды оқыту киберқорғаныстың маңызды бөлігі болып табылады.

Осалдықтарды пайдалану бағдарламалық немесе аппараттық жүйелердегі әлсіздіктерді іздеуге және оларды шабуыл мақсатына қолдануға негізделеді. Осалдықтарды уақтылы анықтау, бағалау және жою шабуылдың ықтималдығын төмендетеді.

Кейбір шабуылдарда алдын ала бұзылған көптеген құрылғылар бір орталықтан басқарылып, бір мақсатқа бағытталады. Мұндай тәсіл таратылған шабуылдарда, әсіресе DDoS жағдайында кездеседі.

Қазіргі кибершабуылдардың даму үрдістері

Бірінші маңызды үрдіс — шабуылдардың күрделенуі және бірнеше әдістің бір сценарийде біріктірілуі. Шабуылдаушы әлеуметтік инженерия арқылы бастапқы қолжетімділік алып, кейін осалдықтарды пайдаланып артықшылықтарын жоғарылатуы, желі ішінде қозғалып, соңында деректерді сыртқа шығаруы немесе жүйенің жұмысын бұзуы мүмкін.

Екінші үрдіс — шабуыл бетінің кеңеюі. Бұлттық инфрақұрылым, қашықтан жұмыс істеу, мобильді және IoT құрылғылары, API және сыртқы сервистер ұйымның ақпараттық ортасына қосымша кіру нүктелерін қалыптастырады. Сондықтан тек желі периметрін қорғауға негізделген тәсіл жеткіліксіз.

Үшінші үрдіс — қауіпсіздік оқиғаларын өңдеуді автоматтандыру қажеттілігі. Үлкен көлемдегі журналдар мен желілік оқиғаларды тек қолмен талдау қиын. Осы себепті оқиғаларды автоматты корреляциялау, аномалияларды анықтау және қауіп деңгейін бағалау маңызды болуда.

Төртінші үрдіс — жасанды интеллект пен машиналық оқыту әдістерін киберқауіпсіздікке енгізу. Олар үлкен көлемдегі деректерден қалыпты мінез-құлықты үйренуге, одан ауытқуларды табуға және белгілі белгілерге ғана тәуелді емес анықтау модельдерін құруға мүмкіндік береді.

Кибертұрақтылық ұғымы

Кибертұрақтылық — кибершабуыл немесе басқа кибероқиға орын алған жағдайда ақпараттық жүйенің маңызды функцияларын сақтау, шабуылдың әсерін шектеу және қалыпты жұмыс режиміне қайта оралу қабілеті. Бұл ұғым киберқауіпсіздікпен тығыз байланысты, бірақ тек алдын алумен шектелмейді.

Абсолютті қорғалған жүйе құру іс жүзінде қиын болғандықтан, заманауи қорғаныс «шабуылға жол бермеу» қағидасына ғана сүйенбеуі тиіс. Ұйым шабуылды анықтауға, оқшаулауға, оған жауап беруге және қалпына келуге дайын болуы қажет.

Кибертұрақтылықты қамтамасыз етуге қауіптерді бағалау, резервтік көшіру, сегментация, қолжетімділікті басқару, тұрақты мониторинг, инциденттерге әрекет ету жоспары және қалпына келтіру рәсімдері кіреді. DevOps және DevSecOps орталарында қауіпсіздік талаптарын жүйенің өмірлік цикліне ерте енгізу де маңызды.

Кибершабуылдарды анықтаудың негізгі тәсілдері

Сигнатуралық анықтау белгілі шабуылға тән белгі немесе ережені іздеуге негізделеді. Егер желілік пакет, файл немесе оқиға белгілі сигнатураға сәйкес келсе, жүйе қауіп туралы хабарлама қалыптастырады. Бұл тәсіл белгілі шабуылдарды анықтауда тиімді, бірақ бұрын белгісіз немесе өзгертілген шабуылдарды өткізіп алуы мүмкін.

Аномалиялық анықтау қалыпты мінез-құлықтан ауытқуды іздеуге негізделеді. Пайдаланушының әдеттегіден өзгеше уақытта жүйеге кіруі, желілік трафик көлемінің күрт

өсуі, қысқа уақыт ішінде көптеген сәтсіз авторизация әрекеттері немесе серверге тән емес сұраныстар аномалия ретінде қарастырылуы мүмкін.

Аномалиялық тәсіл жаңа немесе бұрын белгісіз қауіптерді анықтауға мүмкіндік береді, бірақ қалыпты, сирек кездесетін әрекеттерді де шабуыл деп белгілеуі мүмкін. Бұл жалған оң нәтиже мәселесін туғызады. Сондықтан қазіргі жүйелерде сигнатуралық және аномалиялық әдістерді біріктіретін гибридті тәсілдер кеңінен қарастырылады.

Интеллектуалды кибершабуыл анықтау жүйелері

Дәстүрлі сигнатуралық әдістер белгілі шабуылдарға тиімді болғанымен, жаңа және өзгертілген шабуылдарды анықтау үшін интеллектуалды әдістер қажет. Интеллектуалды анықтау жүйесі желілік трафик, жүйелік журналдар, пайдаланушы әрекеттері, файл сипаттары және қауіпсіздік оқиғалары сияқты деректерді талдайды.

Интеллектуалды жүйенің жалпы жұмыс логикасын келесі тізбекпен көрсетуге болады: деректерді жинау → алдын ала өңдеу → белгілерді қалыптастыру → интеллектуалды талдау → шабуылды анықтау → шешім қабылдау → қарсы әрекет ету.

Гибридті архитектурада сигнатуралық компонент белгілі шабуылдарды жылдам анықтайды, ал машиналық оқыту моделі қалыпты мінез-құлықтан ауытқуларды іздейді. Бұл тәсіл бір әдістің шектеулерін екінші әдіспен толықтыруға мүмкіндік береді.

Машиналық оқытудың киберқауіпсіздіктегі рөлі

Ақпараттық қауіпсіздік құралдары желілік трафик, жүйелік журналдар, қауіпсіздік оқиғалары, пайдаланушы әрекеттері және файл сипаттары түрінде үлкен көлемдегі деректер қалыптастырады. Машиналық оқыту осы деректерден шабуылға тән заңдылықтарды автоматты түрде анықтауға мүмкіндік береді.

Бақыланатын машиналық оқытуда модель алдын ала белгіленген мысалдар бойынша қалыпты және шабуыл кластарын ажыратуды үйренеді. Бақыланбайтын оқытуда алдын ала берілген класс белгілері болмайды; модель деректер құрылымын, топтарды және қалыпты мінез-құлықтан ауытқуларды іздейді.

Уақыттық тізбектерді талдау кезінде тізбекті деректермен жұмыс істейтін нейрондық желілер қолданылуы мүмкін. Мысалы, LSTM архитектурасы оқиғалардың уақыт бойынша өзгерісін ескеруге мүмкіндік береді. Мұндай модельдер желілік белсенділіктің қалыпты үлгісін үйреніп, күмәнді ауытқуларды белгілеу үшін пайдаланылуы мүмкін.

Интеллектуалды модельдердің нәтижелерін бағалау

Кибершабуылды анықтайтын модельдің сапасын тек жалпы дәлдікпен бағалау жеткіліксіз. Қауіпсіздік міндеттерінде True Positive, True Negative, False Positive және False Negative жағдайларын бөлек талдау маңызды. False Positive қалыпты әрекетті шабуыл деп қате белгілеуді, ал False Negative нақты шабуылдың анықталмай қалуын білдіреді.

Precision көрсеткіші модель шабуыл деп белгілеген оқиғалардың қаншасы шын мәнінде шабуыл болғанын сипаттайды: Precision = TP / (TP + FP). Recall нақты шабуылдардың қаншасын модель анықтай алғанын көрсетеді: Recall = TP / (TP + FN). F1-score Precision және Recall арасындағы теңгерімді бағалайды: F1 = 2 × Precision × Recall / (Precision + Recall).

Киберқауіпсіздік жүйесінде False Negative ерекше маңызды болуы мүмкін, себебі бұл жағдайда нақты шабуыл анықталмай қалады. Сонымен қатар False Positive санының шамадан тыс болуы қауіпсіздік мамандарының уақытын тиімсіз жұмсауға және маңызды хабарламалардың назардан тыс қалуына әкелуі мүмкін.

Кибершабуылдарға қарсы кешенді әрекет ету

Кибершабуылдарға қарсы тиімді қорғаныс бір ғана технологияға негізделмеуі тиіс. Кешенді киберқорғаныс техникалық, ұйымдастырушылық және білім беру шараларын біріктіреді.

Техникалық шараларға желіаралық экрандар, IDS/IPS, шифрлау, мониторинг, қолжетімділікті басқару, осалдықтарды анықтау және резервтік көшіру жатады. Ұйымдастырушылық шараларға ақпараттық қауіпсіздік саясаты, пайдаланушы құқықтарын басқару, инциденттерге әрекет ету жоспары, қауіпсіздік аудиті және тәуекелдерді бағалау кіреді.

Адам факторы да маңызды. Қызметкерлерді фишингті тануға, құпия деректермен дұрыс жұмыс істеуге және күмәнді оқиғалар туралы хабарлауға үйрету техникалық қорғанысты толықтырады. Қазіргі киберқауіпсіздік тұрақты мониторингті, оқиғаларды талдауды және қорғаныс механизмдерін үздіксіз жетілдіруді талап етеді.

Қорытынды

Киберқауіпсіздік ақпараттық жүйелердің, желілердің, бағдарламалық құралдардың және деректердің киберқауіптерден қорғалуын қамтамасыз ететін кешенді сала. Киберқауіп, осалдық, кибершабуыл және киберинцидент өзара байланысты болғанымен, мағынасы әртүрлі ұғымдар.

Қазіргі кибершабуылдардың кең таралған түрлеріне фишинг, зиянды бағдарламалық қамтылым, ransomware, DDoS және жеткізу тізбегіне бағытталған шабуылдар жатады. Олардың күрделенуі, шабуыл бетінің кеңеюі және оқиғалар көлемінің артуы дәстүрлі қорғаныс әдістерін интеллектуалды талдау құралдарымен толықтыруды талап етеді.

Кибертұрақтылық қағидасы ақпараттық жүйені тек шабуылдан қорғауды емес, шабуыл орын алған жағдайда маңызды функцияларды сақтау, әсерді шектеу, инцидентке әрекет ету және жүйені қалпына келтіру қабілетін қамтиды. Сондықтан қазіргі киберқорғаныс алдын алу, анықтау, әрекет ету және қалпына келтіру кезеңдерін біртұтас процесс ретінде қарастырады.

Бақылау сұрақтары

1. Киберқауіпсіздік ұғымы нені білдіреді?
2. Киберқауіп, осалдық, кибершабуыл және киберинцидент ұғымдарының айырмашылығы қандай?
3. Құпиялылық, тұтастық және қолжетімділік қағидаларын түсіндіріңіз.
4. Кибершабуылдардың негізгі мақсаттары қандай?
5. Фишинг, ransomware және DDoS шабуылдарының ерекшеліктері қандай?
6. Жеткізу тізбегіне бағытталған шабуылдардың қауіптілігі неде?
7. Кибертұрақтылық дегеніміз не және оның киберқауіпсіздікпен байланысы қандай?
8. Сигнатуралық және аномалиялық анықтау тәсілдерінің айырмашылығы қандай?
9. Машиналық оқыту кибершабуылдарды анықтауда қандай міндеттерді орындайды?
10. Неліктен кибершабуылдарға қарсы қорғаныс кешенді болуы тиіс?

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.

4. Кривчун Н.А., Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И. Кибератаки и методы их предотвращения в информационных системах // Дискуссия. — 2024. — Вып. 128. — С. 120–126.