ЛЕКЦИЯ 8
Кибертұрақтылық және кибершабуылдарға кешенді қарсы әрекет ету

Лекция мақсаты: Кибертұрақтылық және кибершабуылдарға кешенді қарсы әрекет ету тақырыбының негізгі ұғымдарын, процестерін және қолданылатын тәсілдерін кеңінен түсіндіру; олардың ерекшеліктері, артықшылықтары мен шектеулерін салыстыру және практикалық жағдайларда қолданылуын көрсету.

Кибертұрақтылық — кибероқиға кезінде ұйымның маңызды функцияларын сақтау, кибершабуылдың әсерін шектеу және ақпараттық жүйелерді қауіпсіз жұмыс күйіне қалпына келтіру қабілеті. Кибертұрақтылық шабуылдың алдын алумен ғана шектелмейді. Оның негізгі мақсаты — кибершабуыл толық тоқтатылмаған немесе қорғаныс құралдарының бір бөлігі істен шыққан жағдайда да ұйымның аса маңызды қызметтерінің жұмысын жалғастыру.

Кибертұрақтылық бірнеше өзара байланысты процесті қамтиды: *киберқауіптердің алдын алу, оларды дер кезінде анықтау, шабуылдың таралуын шектеу, инцидентке әрекет ету, зақымдалған жүйелерді қалпына келтіру және болған оқиғадан кейін қорғаныс жүйесін жетілдіру***.** Сондықтан кибертұрақтылықты қамтамасыз ету үшін тек антивирус, брандмауэр немесе IDS/IPS сияқты техникалық қорғаныс құралдарын пайдалану жеткіліксіз. Ұйымда резервтік көшіру, желіні сегментациялау, қолжетімділікті басқару, үздіксіз мониторинг, инциденттерге әрекет ету жоспары және қалпына келтіру рәсімдері де болуы қажет.

Кибертұрақтылықтың маңызды ерекшелігі — барлық ақпараттық ресурстарға бірдей талап қойылмайды**.** Алдымен ұйымның жұмыс істеуі үшін аса маңызды активтер мен бизнес-процестер анықталады. Мысалы, пайдаланушылардың аутентификация жүйесі, негізгі деректер қоры немесе ұйымның негізгі ақпараттық сервисі істен шықса, оның салдары қосалқы немесе тестілік сервердің істен шығуына қарағанда әлдеқайда жоғары болуы мүмкін. Сондықтан маңызды активтер үшін күшейтілген мониторинг, резервтеу және жедел қалпына келтіру шаралары қарастырылады.

Мысал. Егер кибершабуыл нәтижесінде ұйымның бір сервері зақымдалса, киберқауіпсіздік құралдары шабуылды анықтап, серверді оқшаулауға бағытталады. Ал кибертұрақтылық тұрғысынан бұған қоса серверде орналасқан қызметтің жұмысын қалай жалғастыруға болатыны, резервтік жүйеге ауысу мүмкіндігі, деректердің сақталуы және жүйені қанша уақытта қауіпсіз қалпына келтіруге болатыны қарастырылады.

Осылайша, киберқауіпсіздік «жүйені қалай қорғаймыз?» деген сұраққа жауап берсе, кибертұрақтылық «қорғаныс бұзылған жағдайда ұйым маңызды қызметтерін қалай сақтап, қалыпты жұмысқа қалай оралады?» деген сұраққа жауап береді.

Жүйенің немесе процестің құрылымы

Киберқауіпсіздік қорғаныс бақылауларын құрады, ал кибертұрақтылық инцидент болған жағдайда қызметтің жалғасуын да қарастырады. Сондықтан алдын алу, анықтау, оқшаулау, қалпына келтіру және сабақ алу бір цикл ретінде қарастырылады.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Кибертұрақтылықты қамтамасыз ету үшін ұйым өз қызметінің үздіксіздігін сақтауға және кибершабуыл салдарын барынша азайтуға бағытталған бірнеше өзара байланысты әдістерді қолданады. Бұл әдістер маңызды активтерді анықтау, тәуекелдерді бағалау, алдын алу, анықтау, оқшаулау, қалпына келтіру және тұрақты бақылау кезеңдерін қамтиды.

Ең алдымен ұйымның ақпараттық активтері анықталып, олардың маңыздылығы бағаланады. Ақпараттық активтерге серверлер, деректер қорлары, ақпараттық жүйелер, желілік құрылғылар, бағдарламалық қамтамасыз ету, пайдаланушылардың есептік жазбалары және ұйым үшін құнды ақпарат жатады. Барлық активтердің маңыздылығы бірдей емес. Мысалы, негізгі деректер қорының немесе аутентификация серверінің тоқтауы тестілік сервердің уақытша істен шығуына қарағанда ұйым қызметіне едәуір үлкен әсер етуі мүмкін.

Активтер анықталғаннан кейін олар маңыздылық деңгейі бойынша жіктеледі. Жіктеу кезінде активтің ұйым қызметіне әсері, онда сақталатын ақпараттың құндылығы, басқа жүйелердің оған тәуелділігі және актив істен шыққан жағдайда туындайтын салдар ескеріледі. Осы бағалау нәтижесінде қандай жүйелердің бірінші кезекте қорғалуы және қандай жүйелер үшін резервтік ресурстар қарастырылуы қажеттігі анықталады.

Әдіс	**Мақсаты**	**Негізгі әрекеттер**	**Нәтижесі**
Активтерді анықтау	Қорғалатын ресурстарды белгілеу	Серверлерді, деректер қорларын, желілік құрылғыларды, ақпараттық жүйелерді түгендеу	Активтер тізімі қалыптасады
Активтерді жіктеу	Маңыздылық деңгейін анықтау	Активтің құндылығы мен ұйым қызметіне әсерін бағалау	Критикалық активтер анықталады
Тәуекелдерді бағалау	Ықтимал қауіп пен салдарды анықтау	Қауіптерді, осалдықтарды және ықтимал әсерді талдау	Қорғаныс басымдығы белгіленеді
Резервтеу	Қызметтің үздіксіздігін қамтамасыз ету	Деректер мен маңызды жүйелердің резервтік көшірмелерін жасау	Қалпына келтіру мүмкіндігі қамтамасыз етіледі
Сегментация	Шабуылдың таралуын шектеу	Желіні жеке қауіпсіздік аймақтарына бөлу	Бір сегменттегі инциденттің басқа жүйелерге таралуы азаяды
Мониторинг	Кибероқиғаны уақытында анықтау	Желілік трафикті, журналдарды және жүйелік оқиғаларды бақылау	Күдікті әрекеттер ерте анықталады

Тәуекелдерді бағалау барысында әрбір маңызды активке қандай қауіптер әсер етуі мүмкін екені және олардың ықтимал салдары анықталады. Мысалы, серверге рұқсатсыз қолжетімділік, зиянды бағдарламаның таралуы, деректердің өзгертілуі немесе сервистің қолжетімсіз болуы әртүрлі тәуекел туғызады. Осыған байланысты қорғаныс шаралары да активтің маңыздылығына сәйкес таңдалады.

Кибертұрақтылықтың келесі маңызды әдісі — ***резервтеу және қалпына келтіруге дайындық***. Маңызды деректердің резервтік көшірмелері жасалып қана қоймай, олардың жарамдылығы жүйелі түрде тексерілуі қажет. Егер кибершабуыл негізгі жүйенің жұмысын бұзса, резервтік көшірме ұйымға деректерді қалпына келтіруге және қызметтің тоқтап қалу уақытын қысқартуға мүмкіндік береді.

Желіні сегментациялау да кибертұрақтылықты арттырады. Желіні бірнеше оқшауланған аймаққа бөлу шабуылдың бір жүйеден екіншісіне еркін таралуына кедергі жасайды. Мысалы, пайдаланушылар желісі, серверлік сегмент және аса маңызды ақпараттық жүйелер жеке қауіпсіздік аймақтарына бөлінуі мүмкін. Бір сегментте күмәнді белсенділік анықталған жағдайда оны уақытша оқшаулап, басқа жүйелердің жұмысын жалғастыруға болады.

Сонымен қатар **үздіксіз мониторинг** жүргізіледі. Желілік трафик, жүйелік журналдар, пайдаланушылардың әрекеттері және қауіпсіздік құралдарының ескертулері бақыланады. IDS/IPS, SIEM, EDR және интеллектуалды анықтау жүйелері күмәнді әрекеттерді ерте анықтауға көмектеседі. Бір ғана ескертуге сүйенбей, бірнеше дереккөзден алынған ақпаратты салыстыру инцидентті дәлірек бағалауға мүмкіндік береді.

Мысал. Ұйымның негізгі деректер қоры орналасқан серверде күмәнді белсенділік анықталды делік. Бұл сервер критикалық актив ретінде алдын ала жіктелген болса, оқиғаға жоғары басымдық беріледі. Қауіпсіздік жүйесі сервердегі әрекеттерді, желілік трафикті және аутентификация журналдарын талдайды. Қауіп расталған жағдайда сервер оқшауланып, шабуылдың басқа сегменттерге таралуы шектеледі. Егер оның жұмысы бұзылса, тексерілген резервтік көшірме арқылы деректер қалпына келтіріледі.

Осылайша, кибертұрақтылықты қамтамасыз етудің негізгі әдістері жеке-жеке емес, біртұтас цикл ретінде қолданылады:

Активтерді анықтау → маңыздылығын бағалау → тәуекелдерді анықтау → қорғаныс шараларын енгізу → мониторинг → инцидентті анықтау → оқшаулау → қалпына келтіру → нәтижелерді талдау және қорғаныстыжетілдіру.

Жұмыс істеу қағидасы

Алдын алу шараларына қауіпсіз конфигурация, жаңартуларды басқару, көпфакторлы аутентификация, ең аз құқық қағидасы, сегментация, резервтік көшіру және қызметкерлерді оқыту жатады.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Талдау және шешім қабылдау

Анықтау IDS/IPS, EDR, журналдар, желілік мониторинг және интеллектуалды талдау арқылы жүргізіледі. Бірнеше дереккөзден алынған белгілерді корреляциялау оқиғаның сенімділігін арттырады.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Қарсы әрекет ету

Оқшаулау шабуылдың таралуын шектеуге бағытталады. Әсер еткен активті бөлу кезінде техникалық қауіппен қатар бизнес-процестің тоқтау тәуекелі де бағаланады.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Тәуекелдер мен шектеулер

Қалпына келтіру кезінде тек резервтен көшіру жеткіліксіз. Алдымен бастапқы себептің жойылғаны, резервтің тұтастығы және жүйеде күмәнді компонент қалмағаны тексеріледі.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау

құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Жетілдіру және бақылау

Инциденттен кейін анықтау мен әрекет ету уақыты, бастапқы себеп және қорғаныс кемшіліктері талданып, мониторинг ережелері мен әрекет ету жоспары жаңартылады.

Бұл элементті жеке қарастыру жеткіліксіз. Киберқауіпсіздік жүйесінде оның нәтижесі қорғалатын активтің маңыздылығы, уақыттық контекст, басқа журналдар мен бақылау құралдарының нәтижелері және ұйымның қауіпсіздік саясаты арқылы нақтыланады. Осылайша автоматты белгі соңғы шешім емес, негізделген талдаудың бір бөлігі болып табылады.

Жіктелуі және салыстырмалы сипаттамасы

Кезең	**Мақсаты**	**Нәтиже**
Алдын алу	Ықтималдықты азайту	Қорғаныс күшейеді
Анықтау	Оқиғаны табу	Ескерту
Оқшаулау	Таралуды шектеу	Әсер азаяды
Қалпына келтіру	Қызметті қайтару	Жұмыс қалпына келеді
Сабақ алу	Жетілдіру	Бақылаулар жаңарады

Процестің жалпы схемасы

Активтер → алдын алу → мониторинг → анықтау → оқшаулау → қалпына келтіру → сабақ алу

Схеманың түсіндірмесі

Схемада әр кезең алдыңғы кезеңнен алынған ақпаратқа сүйенеді. Бастапқы дерек толық немесе сапалы болмаса, кейінгі талдаудың сенімділігі төмендейді. Сондықтан деректерді жинаудан бастап әрекет етуге дейінгі барлық кезеңде бақылау, валидация және кері байланыс қажет. Кері байланыс жаңа ережелерді енгізуге, модельді қайта бағалауға және қорғаныс архитектурасын жетілдіруге мүмкіндік береді.

Практикалық мысалдар

Мысал 1

Файл серверінде күмәнді жаппай өзгерістер байқалды. Сервер оқшауланып, әсер көлемі анықталады; таза резерв тексерілгеннен кейін қызмет қалпына келтіріледі.

Бұл мысалда шешім бір ғана индикаторға сүйенбей қабылданады. Актив, уақыт, пайдаланушы, желілік байланыс және қосымша журналдар салыстырылған кезде жалған қорытынды ықтималдығы төмендейді және әрекет ету басымдығы дұрысырақ анықталады.

Мысал 2

Негізгі білім беру сервисі мен тест сервері бір уақытта қауіп белгісін берсе, маңызды сервиске қалпына келтіру басымдығы жоғары болады.

Бұл мысалда шешім бір ғана индикаторға сүйенбей қабылданады. Актив, уақыт, пайдаланушы, желілік байланыс және қосымша журналдар салыстырылған кезде жалған қорытынды ықтималдығы төмендейді және әрекет ету басымдығы дұрысырақ анықталады.

Артықшылықтары мен кемшіліктері

Қарастырылған тәсілдердің артықшылығы — қауіпсіздік оқиғаларын жүйелі талдау, үлкен көлемдегі деректерден маңызды белгілерді бөлу, белгілі және белгісіз қауіптерді салыстыру және әрекет ету уақытын қысқарту. Кемшіліктеріне деректердің толық болмауы, жалған оң және жалған теріс нәтижелер, қате конфигурация, ескірген ережелер немесе модельдер, интеграцияның күрделілігі және автоматты әрекеттің заңды бизнес-процеске әсер ету ықтималдығы жатады.

Қорытынды

Кибертұрақтылық және кибершабуылдарға кешенді қарсы әрекет ету кибершабуылдарды анықтау және оларға қарсы әрекет етудің кешенді жүйесіндегі маңызды бағыт болып табылады. Нәтиженің сапасы жеке құралмен ғана емес, деректердің сапасымен, бірнеше қорғаныс механизмінің өзара байланысымен, тұрақты мониторингпен және алынған белгілерді контекстпен тексерумен анықталады.

Бақылау сұрақтары

1. Негізгі ұғымға анықтама беріңіз.
2. Қарастырылған процестің негізгі кезеңдерін түсіндіріңіз.
3. Кестеде берілген тәсілдердің айырмашылығы қандай?
4. Негізгі артықшылықтарды атаңыз.
5. Негізгі кемшіліктер мен шектеулер қандай?
6. Қандай деректер талдау үшін маңызды?
7. Интеллектуалды әдістердің рөлі қандай?
8. Автоматтандыру кезінде адам бақылауы не үшін қажет?
9. Практикалық мысалдағы шешім қабылдау логикасын түсіндіріңіз.
10. Бұл тақырып кешенді киберқорғаныспен қалай байланысады?

Әдебиеттер тізімі:

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.