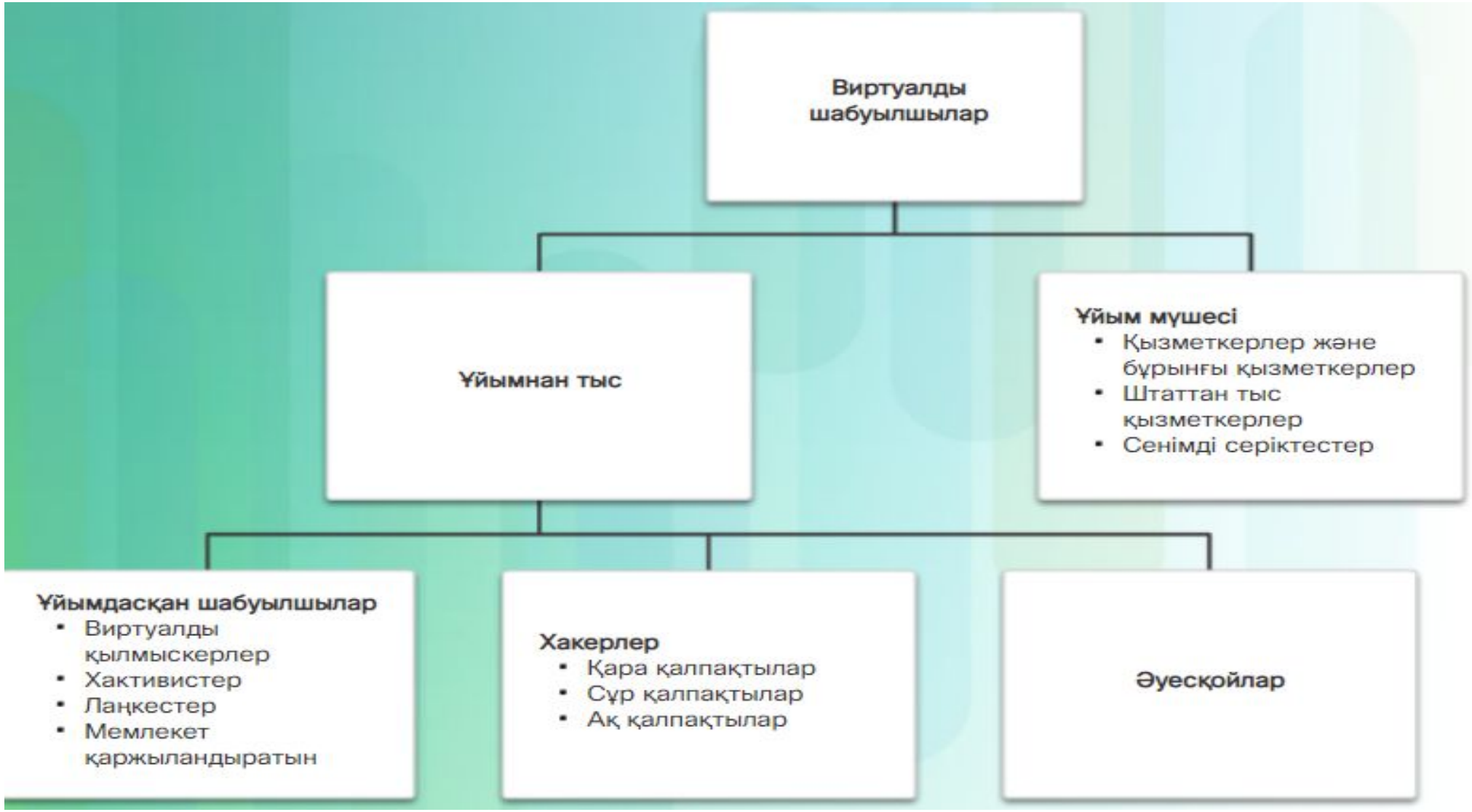
Шабуылдар, қағидаттар мен тәсілдер


Виртуалды шабуылшылар
Ұйымнан тыс
Ұйым мүшесі
• Қызметкерлер және бұрынғы қызметкерлер
• Штаттан тыс қызметкерлер
• Сенімді серіктестер
Ұйымдасқан шабуылшылар
• Виртуалды қылмыскерлер
• Хактивистер
• Лаңкестер
• Мемлекет қаржыландыратын
Хакерлер
• Қара қалпақтылар
• Сұр қалпақтылар
• Ақ қалпақтылар
Әуесқойлар

Ішкі және сыртқы қатерлер

Қауіпсіздікке төнетін ішкі қатерлер

Суретте көрсетілгендей, шабуылдар ұйымның ішінен не сыртынан ұйымдастырылуы мүмкін. Ішкі пайдаланушы (мысалы, қызметкер немесе мердігердің өкілі) шабуылды кездейсоқ немесе қасақана іске асыруы мүмкін:

- Құпия деректерді дұрыс пайдаланбау
- Ішкі серверлердің немесе желі инфрақұрылымының құрылғыларының жұмысына қатер төндіру
- Корпоративтік компьютерлік желіге зарарланған USB құрылғысын қосу арқылы сыртқы шабуылға жол ашу
- Зиянды электрондық хат немесе веб-сайттар арқылы байқаусызда желіге зиянды бағдарлама жұқтыру

Ішкі қатерлердің ықтимал әсері сыртқы қатерлерден асып кетуі мүмкін, себебі ішкі пайдаланушылар ғимарат пен оның инфрақұрылымдық құрылғыларына кіре алады. Оған қоса, қызметкерлер корпоративтік желі, оның ресурстары және құпия деректер, сондай-ақ пайдаланушы дәрежелері немесе әкімшілік басымдықтар туралы хабардар.

Қауіпсіздікке төнетін сыртқы қатерлер

Әуесқойлардан немесе білікті шабуылшылардан төнетін сыртқы қатерлер кезінде желілердегі не компьютерлік құрылғылардағы осалдықтар не болмаса қатынау мүмкіндігіне ие болу үшін әлеуметтік инженерия пайдаланылуы мүмкін.

Дәстүрлі деректер

Корпоративтік деректер Кадрлық ақпаратты, зияткерлік меншікті және қаржылық деректерді қамтиды. Кадрлық ақпаратқа жұмысқа қабылдау туралы өтініштер, жалақы қоры, ұсыныс хаттары, еңбек шарттары және қызметкерлерді жалдау туралы шешім қабылдау кезінде қолданылатын кез-келген ақпарат кіреді. Патенттер, тауарлық белгілер және жаңа өнімді әзірлеу жоспарлары сияқты зияткерлік меншік компанияға бәсекелестерінен экономикалық артықшылық береді. Зияткерлік меншікті коммерциялық құпия ретінде қарастыруға болады; бұл ақпаратты жоғалту компанияның болашағы үшін апатты болуы мүмкін. Қаржылық деректер, мысалы, кірістер туралы декларациялар, баланстар және ақша ағындары туралы есептер компанияның әл-ауқаты туралы түсінік береді

Мобильді құрылғылардың осалдығы

Бұрын қызметкерлер әдетте корпоративті жергілікті желіге қосылған компанияның компьютерлерін қолданған. Жүйе әкімшілері осы компьютерлердің жұмысын үнемі қадағалап отырды және оларды қауіпсіздік талаптарын сақтау аясында жаңартты. Бүгінгі таңда планшеттер, iPhone және басқа смартфондар мен мобильді құрылғылар сияқты мобильді құрылғылар дәстүрлі компьютерлерді алмастыруда немесе толықтыруда. Корпоративтік ақпаратқа қол жеткізу үшін бұл құрылғыларды көбірек адамдар пайдаланады. BYOD моделі кең таралған. Корпоративтік желілік инфрақұрылымға кіру үшін қызметкерлер пайдаланатын мобильді құрылғыларды орталықтан басқара алмайтын және олардағы бағдарламалық жасақтаманы жаңарта алмайтын ұйымдар өздерін өсіп келе жатқан қауіпке душар етеді.

Интернет заттардың пайда болуы

Интернет заттары (IoT) — Интернетке әртүрлі құрылғыларды қосуға мүмкіндік беретін технологиялар жиынтығы. Заттар интернетінің пайда болуымен байланысты технологиялық эволюция коммерциялық және тұтынушылық ортаға өзгерістер енгізеді. Интернет заттары технологиясы Интернетке миллиардтаған құрылғыларды қосуға мүмкіндік береді. Олардың ішінде-бағдарламалық-аппараттық кешендер, құлыптар, қозғалтқыштар, ойын-сауық құрылғылары және т.б. Қорғауды қажет ететін деректер көлемі өсуде. Құрылғыларға қашықтан қол жеткізу қорғалуы керек желілік инфрақұрылымдардың санын көбейтеді.Интернеттің дамуымен басқару және қорғау өсіп келе жатқан деректер көлемін қажет етеді. Бұлттың және виртуализацияның арқасында қол жетімді болған дискілік кеңістіктің кеңейтілген өлшемдерімен және деректерді сақтау қызметтерімен бірге әртүрлі қосылымдар деректердің экспоненциалды өсуіне әкелді. Деректердің мұндай өсуі "деректердің үлкен көлемі"деп аталатын технологиялар мен бизнеске деген қызығушылықтың жаңа саласын тудырды.

Үлкен деректердің әсері

Үлкен деректер үлкен және күрделі мәліметтер жиынтығының нәтижесі болып табылады, оны өңдеу үшін дәстүрлі деректерді өңдеудің мүмкіндіктері жеткіліксіз болады. Үлкен деректермен байланысты мүмкіндіктер мен проблемалар үш факторға негізделген:

- Деректер көлемі
- Деректердің өсу және өңдеу жылдамдығы
- Деректер түрлері мен көздерінің әртүрлілігі

Жаңалықтар ірі корпорацияларға хакерлік шабуылдардың көптеген мысалдарына толы. Target, Home Depot және PayPal сияқты компаниялар ең көп жарияланған шабуылдардың нысаны болып табылады. Нәтижесінде қауіпсіздік саласындағы шешімдердің құрылымын айтарлықтай өзгерту және корпоративтік жүйелерді қорғаудың технологиялары мен әдістерін жетілдіру талап етіледі. Бұдан басқа, деректерді қорғауды және қауіпсіздікті бақылау құралдарын жақсартуды талап ететін үлкен деректерге қатысты жаңа мемлекеттік және салалық қағидалар мен нормалар пайда болады.

Озық қаруды қолдану

Бүгінгі таңда бағдарламалық жасақтама осалдықтарының көзі программалау қателері, протокол осалдықтары немесе жүйенің дұрыс емес конфигурациясы болып табылады. Киберқылмыскерлер олардың біреуін ғана қолданады. Мысалы, әдеттегі шабуыл оны зақымдау және дұрыс жұмыс істемеу үшін программаға кіру үшін белгілі бір деректер ағынын құруды қамтиды. Бұл ақаулық программаны бұзудың кілті болып табылады немесе программадан ақпараттың ағып кетуіне әкеледі.

Бүгінгі кибершабуылдар күрделене түсуде. Күрделі мақсатты қауіп (APT) белгілі бір объектіге ұзақ мерзімді компьютерлік шабуыл болып табылады, ол байқаусыз жүзеге асырылады.

APT (ағылш. advanced persistent threat - "дамыған тұрақты қауіп"; сондай-ақ мақсатты кибершабуыл)

Қылмыскерлер әдетте коммерциялық немесе саяси себептермен шабуыл жасау мақсаттарын таңдайды. APT ұзақ уақыт бойы жетілдірілген зиянды программаларды қолдана отырып жүзеге асырылады және құпиялылықтың жоғары деңгейіне ие. Алгоритмдік шабуылдар жүйе автоматты түрде хабарлайтын деректерді, мысалы, компьютер тұтынатын энергияны бақылай алады және оларды мақсаттарды таңдау немесе жалған ескертулерді іске қосу үшін пайдалана алады.

Алгоритмдік шабуылдар компьютерді жадты қатты пайдалану немесе оның орталық процессорын шамадан тыс жүктеу арқылы өшіре алады. Алгоритмдік шабуылдар неғұрлым күрделі болып саналады, өйткені олар энергияны үнемдеу, жүйенің ақаулыққа төзімділігін және оның тиімділігін арттыру үшін қолданылатын эксплуатацияларды пайдаланады. Сонымен, жаңа ұрпақ шабуылдары құрбанды интеллектуалды таңдауды қолданады. Бұрын зиянкестер шабуыл жасау үшін жүйенің ең оңай қол жетімді немесе ең осал бөліктерін таңдаған. Алайда, қазір кибершабуылдарды анықтауға және оқшаулауға көп көңіл бөлінген кезде, киберқылмыскерлер өте абай болу керек. Егер шабуыл ерте анықталса, киберқауіпсіздік мамандары жүйеге кіруді жабады. Нәтижесінде, көптеген жетілдірілген шабуылдарды киберқылмыскердің мақсатты қолтаңбасы болған жағдайда ғана жасауға болады.

Кеңірек қамту және каскадты әсер

Федеративті сәйкестендіру деректерін басқару бірнеше кәсіпорындардың пайдаланушыларына топтың кез-келген кәсіпорнының желілік инфрақұрылымына қол жеткізу үшін бірыңғай тіркелгі деректерін пайдалануға мүмкіндік береді. Шабуыл болған жағдайда ол қамтуды кеңейтеді және каскадты әсер ету мүмкіндігін арттырады. Федералды сәйкестендіру менеджменті жеке жүйелер субъектілерінің электрондық сәйкестендіру деректерін байланыстырады. Мысалы, тақырып Yahoo! Google немесе Facebook тіркелгі деректерімен. Бұл әлеуметтік сәйкестендірудің мысалы.Федералды сәйкестендіруді басқарудың мақсаты-қорғалған топтың шекараларында сәйкестендіру ақпаратын автоматты түрде алмасу. Жеке пайдаланушының көзқарасы бойынша бұл Интернетке бірыңғай сәйкестендіру кірісін білдіреді.Ұйымдар серіктестермен бірге сәйкестендіру ақпаратына талдау жасауы керек. Зиянкес серіктестің желісінен әлеуметтік сақтандыру нөмірлері, атаулары мен мекенжайлары сияқты ақпаратты ұрлауға және оны алаяқтық жасау үшін пайдалануға мүмкіндігі бар. Федералды сәйкестендіру ақпаратын қорғаудың ең көп таралған әдісі-жүйеге кіруді уәкілетті құрылғыға байланыстыру.

Қауіпсіздік алғышарттары

АҚШ-тағы жедел жәрдем орталықтарының саны кибершабуылдарға осал болып табылады, олар жедел қызмет желілерін үзіп, қоғамдық қауіпсіздікке қауіп төндіруі мүмкін. Қызмет көрсетуден бас тарту (TDoS) телефон шабуылы мақсатты телефон желісіне қоңырауларды қолданады, жүйені бұғаттайды және қалаған қоңырауларға жол бермейді. Жедел жәрдем орталықтарының келесі буыны осал болып табылады, өйткені олар дәстүрлі сымды телефон желілерінің орнына Voice-over-IP (VoIP) жүйелерін пайдаланады. Tdos шабуылдарынан басқа, кол-орталықтар көптеген компьютерлерден жасалған және мақсатты ресурстарды шамадан тыс жүктейтін таратылған "қызмет көрсетуден бас тарту" (DDoS) шабуылдарына ұшырауы мүмкін. Осылайша, мақсатты нысан заңды пайдаланушылар үшін қол жетімді болмайды. Қазіргі уақытта смартфон қосымшаларын немесе үй қауіпсіздігі жүйелерін қолдана отырып, жедел қызметтерге жүгінудің көптеген жолдары бар.

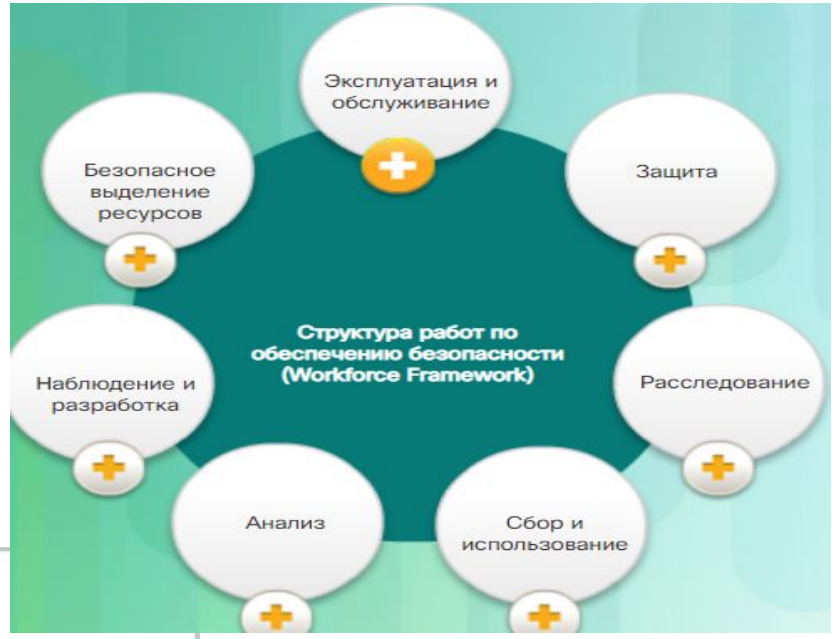
TDOS-бұл телекоммуникациялық желілерге қызмет көрсетуден бас тартуға жасалған шабуылдар.

Дауысты Интернет протоколы (VoIP) арқылы беру, IP телефония деп те аталады, Интернет сияқты Интернет протоколы (IP) арқылы дауыстық байланыс пен мультимедиялық сеанстарды жеткізуге арналған әдіс пен технологиялар тобы.

Киберқауіпсіздік қатерлерін жоғары тану

Кибер әуе шабуылынан қорғаныс әлсіз болды. Тіпті ақылды орта мектеп оқушысы немесе әуесқой хакер жүйелерге қол жеткізе алады. Уақыт өте келе бүкіл әлемдегі елдер кибершабуылдардың қауіптілігін жақсы түсіне бастады. Кибершабуылдар қазір көптеген елдердегі ұлттық және экономикалық қауіпсіздікке төнетін ең үлкен қауіптердің тізімінде.

Киберқауіпсіздік саласындағы қызметкерлерді кәсіби даярлаудың ұлттық тұжырымдамасы (The National Cybersecurity Workforce Framework)



Эксплуатация и обслуживание

Специалисты в этой области отвечают за оказание поддержки, администрирование и обслуживание, необходимые для обеспечения эффективной и действенной работы и безопасности ИТ-систем.

Защита

Сотрудники, специализирующиеся в этой области, отвечают за определение, анализ и устранение угроз для внутренних ИТ-систем или сетевых инфраструктур.

Расследование

Сотрудники, специализирующиеся в этой области, отвечают за расследование киберсобытий и/или преступлений, совершенных в ИТ-системах или сетевых инфраструктурах, и изучение цифровых доказательств.

Сбор и использование

Специалисты в этой области отвечают за проведение операций по сокрытию данных и дезинформации, а также сбор информации о кибербезопасности для разведки.

Анализ

Специалисты в этой области отвечают за детальную проверку и оценку поступающей информации о кибербезопасности для определения ее полезности для разведки.

Наблюдение и разработка

Специалисты в этой области отвечают за руководство, управление, направление и/или развитие и информационную поддержку, чтобы отдельные лица и организации могли эффективно обеспечивать кибербезопасность.

Безопасное выделение ресурсов

Специалисты в этой области отвечают за разработку, проектирование и создание безопасных ИТ-систем, т. е. несут ответственность за те или иные аспекты их развития.

Национальная концепция профессиональной подготовки сотрудников в сфере кибербезопасности (The National Cybersecurity Workforce Framework)

Структура работ по обеспечению безопасности (Workforce Framework) выделяет семь категорий задач в области кибербезопасности.

Эксплуатация и обслуживание включают в себя техническую поддержку, администрирование и обслуживание, необходимые для обеспечения производительности и безопасности ИТ-системы.

Защита включает идентификацию, анализ и устранение угроз для внутренних систем и сетевых инфраструктур.

Расследование включает в себя расследование кибернарушений и/или киберпреступлений, связанных с ИТ-ресурсами.

Сбор и управление включают в себя специализированные операции по сокрытию данных и дезинформации и сбор информации для обеспечения кибербезопасности.

Анализ включает в себя высококвалифицированный обзор и оценку поступающей информации по кибербезопасности, чтобы определить, является ли она полезной.

Контроль и развитие предлагают инструкции, указания и руководство для эффективной работы в сфере кибербезопасности.

Безопасность и выделение ресурсов включают в себя разработку концепций, проектирование и внедрение безопасных ИТ-систем.

В каждой категории есть несколько областей специализации. Области специализации определяют стандартные типы работ по кибербезопасности.

На рисунке показаны все категории и приведено их краткое описание.

Стакснет шабуылды жүйеге заңды етіп көрсету үшін ұрланған цифрлық сертификаттарды пайдаланған.

Стакснет. Яғни, маңызы?

Барлық күшті қатерлер сияқты мұның тәптіштелуі жалғасуда, бірақ осы жерде назар аударуға тұрарлық **бес жайт** бар деп ойлаймын.

Киберсоғыстың мақсаты

Киберсоғыстың басты мақсаты – қарсыластардан (мемлекеттер немесе бәсекелестер) асып түсу.

Бір ел басқа елдің инфрақұрылымына тұрақты түрде шабуыл жасауы, қорғаныс деректерін ұрлауы және өз өнеркәсібі мен әскери күшіндегі кемшілікті азайту үшін технологиялар туралы ақпаратты жинауы мүмкін. Өнеркәсіптік және әскери тыңшылықтан бөлек, киберсоғыс барысында елдердің инфрақұрылымына іріткі салу әрекеттері жасалып, ол мақсатты елдердегі тұрғындардың өліміне алып келуі мүмкін. Мысалы, шабуыл кезінде ірі қаладағы қуат желісі ажыратылуы мүмкін. Жол қозғалысы үзіледі. Тауарлар мен қызметтер алмасу тоқтайды. Төтенше жағдайларда емделушілер медициналық жәрдем ала алмайды. Интернет байланысы үзілуі мүмкін. Қуат желісін ажырату бейбіт тұрғындардың күнделікті өміріне кері әсерін тигізуі мүмкін.

Киберсоғыс деген не?

Киберкеңістік елдердің арасында үйреншікті әскер мен соғыс машиналарынсыз шайқас жүргізілетін маңызды алаңға айналды. Бұл кей елдерге барынша аз әскери күш қолданып, киберкеңістікте басқа елдермен теңесу мүмкіндігін береді. Киберсоғыс дегеніміз – басқа елдердің компьютерлік жүйелері мен желілеріне кірумен сипатталатын интернеттегі шайқас. Мұндай шабуылшылардың интернет арқылы басқа елдерге жаппай шабуыл жасап, зиян келтіру немесе қуат желісін сөндіру сияқты қызметтерді ажыратуға жеткілікті ресурстары мен тәжірибесі бар.
Мемлекет демеушілік еткен шабуылдардың бірінде Иранның ядролық байыту зауытына зиян тигізу үшін жасалған Стакснет зиянды бағдарламасы пайдаланылған. Стакснет зиянды бағдарламасы ақпарат ұрлау үшін жасалмады.
Оның мақсаты компьютерлермен басқарылатын нақты жабдықтарға зиян келтіру болған. Онда зиянды бағдарлама ішінде арнайы тапсырма орындауға бағдарламаланған модульді код пайдаланылған.

Одан бөлек, ұрланған құпия деректер шабуылшыларға үкіметте жұмыс істейтін адамдарды бопсалау мүмкіндігін беруі мүмкін. Алынған ақпарат негізінде шабуылшы өзін құпия ақпаратқа немесе жабдыққа жетуге рұқсаты бар пайдаланушы ретінде таныстыруы мүмкін.

Егер үкімет кибершабуылдардан қорғана алмаса, азаматтар үкіметтің оларды қорғай алатынына күмандана бастауы мүмкін. Киберсоғыс елге кірмей-ақ ондағы тұрақтылықты жоюға, сауданы тоқтатуға және азаматтардың үкіметке деген сенімін жоюға мүмкіндік береді.

Қауіпсіздікті қамтамасыз етудің осал тұстарын анықтау

Бағдарламалық құралдың не жабдықтың кез келген ақауы қауіпсіздікті қамтамасыз етудің осал тұсы болып табылады. Зиянды бағдарламаларды пайдаланушылар осал тұстарды анықтағаннан кейін осалдықты пайдалануға әрекет жасайды. Осалдықты *пайдалану құралы* - анықталған осалдықты пайдалану мақсатында жазылған бағдарламаны сипаттау үшін қолданылатын термин. Осал тұсқа қатысты осалдықты пайдалану құралын қолдану әрекеті шабуыл деп аталады. Шабуылдың мақсаты – жүйеге, онда орналастырылған деректерге немесе белгілі бір ресурстарға кіру мүмкіндігіне ие болу.

Бағдарламалық құралдың осал тұстары

Бағдарламалық құралдың осал тұстары әдетте операциялық жүйедегі не қолданба кодындағы қателер түрінде көрініс табады, компаниялардың бағдарламалық құралдардың осал тұстарын анықтауға және түзетуге бағыттаған орасан зор күшіне қарамастан, жаңа осалдықтар орын ала беруде. Microsoft, Apple және өзге де операциялық жүйе жетілдірушілері күн сайын дерлік түзетулер мен жаңартулар шығарып отырады. Қолданба жаңартулары да жиі-жиі ұсынылады. Жауапты компаниялар не ұйымдар веб-браузерлер, мобильді қолданбалар және веб-серверлер секілді қолданбаларды жаңартып отырады.

2015 жылы Cisco IOS жүйесінде SYNful Knock деп аталатын ірі осалдық анықталды. Бұл осалдық шабуыл жасаушыларға legacy Cisco 1841, 2811 және 3825 маршрутизаторлары секілді корпоративтік деңгейдегі маршрутизаторларды басқаруға мүмкіндік берді. Шабуыл жасаушылар желідегі барлық қарым-қатынасты бақылау және өзге желілік құралдарды бүлдіру мүмкіндігіне ие болды. Бұл осалдық маршрутизаторларда бүлінген IOS нұсқасы орнатылған кезде жүйеге енгізілді. Мұның алдын алу үшін әрдайым жүктелген IOS кескінінің тұтастығына назар аударып, құралды тек өкілетті қызметкерлердің пайдалануына рұқсат беру қажет.

Бағдарламалық құрал жаңартуларының мақсаты – даму қарқынына сәйкес келу және осалдықтарды қолданудың алдын алу. Көптеген компаниялардың бағдарламалық осалдықтарын пайдаланбас бұрын оларды іздеу, табу және түзету әрекеттерін орындайтын арнайы сынау топтары өз жұмыстарын іске асырса, үшінші тараптық қауіпсіздікті қамтамасыз ету саласындағы зерттеушілер де бағдарламалық құралдағы осал тұстарды анықтауға маманданады.

Google тобының Project Zero жобасы – осындай тәжірибенің айқын мысалы. Түпкі пайдаланушылар қолданатын түрлі бағдарламалық құралдардағы бірнеше осалдықты анықтағаннан кейін Google бағдарламалық құрал осалдықтарын анықтайтын арнайы тұрақты топты жасақтады. Қауіпсіздікті қамтамасыз ету саласындағы Google зерттеулерін мына жерден табуға болады.

Жабдықтың осал тұстары

Жабдықтың осал тұстары әдетте жабдықтың құрылымдық ақаулары түрінде көрініс табады. Мысалы, ЖЖҚ жады бір-біріне жақын орналасқан маңызды конденсаторлардан құралады. Олардың жақын орналасуына байланысты осы конденсаторлардың біріне жасалған тұрақты өзгертулердің көршілес орналасқан конденсаторларға әсер ететіні анықталды. Осы құрылымдық ақаудың негізінде Rowhammer деп аталатын осалдықты пайдалану құралы жасалды. Бір мекенжайда жадыны қайталап жазу арқылы Rowhammer осалдықты пайдалану құралы ұяшықтардың қорғалғанына қарамастан жақын маңдағы мекенжайдың жады ұяшықтарынан деректерді алуға мүмкіндік береді.

Жабдықтың осал тұстары белгілі бір құрал үлгілері үшін қолданылады және кездейсоқ бүлдіру әрекеттері арқылы іске аспайды. Жабдықтың осалдықтарын пайдалану құралдары мақсатты шабуылдарда жиі қолданылса, дәстүрлі зиянды бағдарламалардан қорғау және физикалық қорғау әрекеттері күнделікті пайдаланушылар үшін маңызды қорғау әдістері болып табылады.

Қауіпсіздікті қамтамасыз етудегі осалдықтарды санаттарға бөлу

Бағдарламалық құралдың қауіпсіздігін қамтамасыз етудегі осалдықтар келесі санаттардың біріне жатады:

Буфер жадының толып кетуі – Деректер буфердің шекті мөлшеріне жететін көлемде жазылғанда осы осалдық орын алады. Буферлер – қолданба үшін тағайындалған жады аумақтары. Буфер шекарасынан тыс аймақта деректерді өзгерту арқылы қолданба өзге процестер үшін тағайындалған жадыны қолданады. Бұл жүйенің істен шығуына, деректердің бүлінуіне әкелуі немесе айрықша құқықтарды беруі мүмкін.

Бағаламастан енгізу – Бағдарламалар әдетте деректерді енгізумен жұмыс істейді. Бағдарламаға енгізілген бұл деректерде бағдарламаны мақсатынан тыс жұмыс істеуге итермелейтін етіп жасалған зиянды мазмұн болуы мүмкін. Өңделетін кескінді қабылдайтын бағдарламаны қарастырайық. Зиянды бағдарлама пайдаланушы кескін файлын жарамсыз кескін өлшемдерімен бүлдіруі мүмкін. Зиянды бағдарлама арқылы бүлінген өлшемдер бағдарламаның дұрыс емес әрі күтпеген өлшемдегі буферлерді таратуына әкелуі мүмкін.

Ағындар бәйгесі – Бұл осалдық тапсырыс берілген немесе жоспарланған оқиғаны шығаруға байланысты орын алады. Ағындар бәйгесі қажетті жүйелі не жоспарланған оқиғалар дұрыс тәртіпте не керекті уақытта іске асырылмағанда осалдық көзіне айналады.

Қауіпсіздікті қамтамасыз ету әдістерінің әлсіз тұстары – Жүйелер мен сезімтал деректерді аутентификация, растау және шифрлау секілді әдістер арқылы қорғауға болады. Жетілдірушілер өздерінің жеке қауіпсіздік алгоритмдерін жасауға әрекет жасамауы тиіс, өйткені мұның нәтижесінде осалдықтар пайда болуы мүмкін. Жетілдірушілерге бұған дейін жасалған, сыналған және расталған қауіпсіздік кітапханаларын пайдалануға кеңес беріледі.

Кіруді бақылау мәселелері – Кіруді басқару – кімнің қандай әрекетті орындағанын және физикалық кіру әрекетінен файл секілді ресурсты кімнің пайдаланғанын және олардың бұл ресурстың көмегімен файлды оқу не өзгерту секілді әрекеттердің қайсысысын орындағанын бақылауға дейінгі ауқымды қамтитын процесс. Қауіпсіздікті қамтамасыз етудегі көптеген осалдықтар кіруді бақылау құралдарын дұрыс пайдаланбау нәтижесінде орын алады.

Егер шабуылшы нысанадағы жабдыққа физикалық түрде қатынаса алса, барлық дерлік кіруді бақылау құралдары мен қауіпсіздік шараларын жеңіп өтуге болады. Мысалы, файлға қандай рұқсат параметрлерінің орнатылғанына қарамастан, операциялық жүйе шабуылшының деректерді дискіден тікелей алуына тосқауыл бола алмайды. Жабдық пен онда сақталатын деректерді қорғау үшін физикалық қатынасты шектеу керек және деректердің ұрлануының не бұзылуының алдын алу үшін оларды шифрлау әдістерін қолдану керек.

Зиянды бағдарламалардың түрлері

Зиянды бағдарламалық құрал, қысқаша айтқанда зиянды бағдарлама, – деректерді ұрлау, кіруді басқару элементтерін айналып өту немесе жүйеге зиян тигізу не қауіп төндіру үшін қолдануға болатын кез келген код. Зиянды бағдарламалардың жиі кездесетін бірнеше түрі:

Тыңшылық бағдарлама пайдаланушыны іздеуге және тыңшылық жасауға арналған. Тыңшылық бағдарламаның құрамында көбіне іс-әрекетті бақылау құралдары, перне басу жинағы және деректерді аулау құралдары болады. Қауіпсіздік шараларынан құтылу үшін тыңшылық бағдарлама көбіне қауіпсіздік параметрлерін өзгертеді. Тыңшылық бағдарлама көп жағдайда өзін зиянсыз бағдарламаға немесе Троян аттарына байлайды.

Жарнамалық бағдарламалар – автоматты түрде жарнамаларды жеткізу үшін жасалған, жарнаманы қолдайтын бағдарлама. Көбінесе жарнамалық бағдарлама бағдарламалардың кейбір нұсқаларымен бірге орнатылады. Кейбір жарнамалық бағдарламалар тек жарнама жеткізуге арналады, алайда жарнамалық бағдарламамен бірге тыңшылық бағдарламаның да қатар орнатылуы жиі кездеседі.

Бот – робот сөзінен шыққан; әрекетті, әсіресе желідегі әрекетті, автоматты түрде орындау үшін жасалған зиянды бағдарлама. Боттардың басым бөлігі зиянсыз болғанмен, ботнеттер зиянды боттардың қолданылуын арттыруда. Тыныш қана шабуылшының пәрменін күтіп отыруға бағдарламаланған боттар бірнеше компьютерге жұқтырылады.

Бопсалаушы бағдарлама – компьютерді немесе ондағы деректерді төлем жасалғанша босатпай ұстап тұру үшін жасалған. Бопсалаушы бағдарлама әдетте компьютердегі деректерді пайдаланушыға беймәлім кілтпен шифрлау арқылы жұмыс істейді. Ал кейбір нұсқалары жүйенің белгілі бір осал тұстарының арқасында жүйені кілттейді. Бопсалаушы бағдарлама жүктеп алынған файл не кейбір бағдарламалардың осал тұстары арқылы таралады.

Қорқытушы бағдарлама – пайдаланушыны қорқыту арқылы оны белгілі бір әрекет жасауға итермелеу үшін қолданылады. Қорқытушы бағдарлама операциялық жүйенің терезелеріне ұқсайтын жалған ашпалы терезелер жасайды. Бұл терезелерде жүйеге қатер төніп тұрғаны немесе жүйені қалыпты жұмысқа қайтару үшін нақты бір бағдарламаны іске қосу керектігі айтылған жалған хабарлама көрсетіледі. Ал шындығында, ешқандай проблема анықталмаған, сондықтан егер пайдаланушы келісім беріп, бағдарламаны іске қосуға рұқсат етсе, оның жүйесі зиянды бағдарламаны жұқтырады.

Руткит – қосымша кіру жолын ашу үшін операциялық жүйені өзгертетін зиянды бағдарлама. Содан соң шабуыл жасаушылар компьютерге қашықтан кіру үшін сол қосымша жолды пайдаланады. Көп руткиттер бағдарламаның осал тұстарын пайдаланып, айрықша құқықтарды іске асырады және жүйенің файлдарын өзгертеді. Сонымен қатар руткиттер жүйе сараптамаларын және мониторинг құралдарын өзгертіп, өздерін табуды өте қиындатады. Көп жағдайда руткит бүлдірген компьютерді тазалап, қайта орнату қажет.

Вирус – орындалатын өзге файлдарға, көбінесе рұқсат етілген бағдарламаларға тіркеліп келетін зиянды, орындалатын код. Көп вирустар түпкі пайдаланушының іске қосуын қажет етеді және белгілі уақытта немесе белгілі бір күні іске қосыла алады. Вирустар зиянсыз болуы және жай ғана сурет көрсетуі мүмкін немесе деректерді өзгерту не жою арқылы аса зиянды болуы мүмкін. Сондай-ақ анықталудың алдын алу үшін вирустар мутацияға ұшырауға бағдарламалануы мүмкін. Көптеген вирустар қазіргі таңда USB диск жетегі, оптикалық дискілер, желідегі жалпы ресурстар немесе электрондық пошта арқылы таралады.

Трояндық ат – қажетті операция кейпінде жасырылған зиянды операцияларды орындайтын зиянды бағдарлама. Бұл зиянды код өзін іске қосқан пайдаланушының айрықша құқықтарын қолданады. Көп жағдайда, Трояндар кескін файлдарында, аудио файлдарда немесе ойындарда кездеседі. Трояндық аттың вирустан айырмашылығы – оның орындалмайтын файлдарға байланатыны.

Құрттар – желілердің осал тұстарын еркін пайдалану арқылы өздерінің көшірмелерін жасайтын зиянды бағдарламалар. Құрттар әдетте желілердің жұмысын баяулатады. Егер вирус үшін өзі жұққан бағдарламаның жұмыс істегені қажет болса, ал құрттар өз беттерімен жұмыс істей алады. Алғашқы жұқтырудан кейін оларға пайдаланушының қатысуы қажет емес. Қабылдаушыға жұққаннан кейін құрт желі аясында өте жылдам тарала алады. Құрттардың сипаттары ұқсас. Олардың барлығын іске қосатын осал тұс, өздерін көбейту жолы және барлығының пайдалы жүктемесі бар.

Интернеттегі аса жойқын шабуылдардың кейбіріне құрттар жауапты. 1-суретте көрсетілгендей, 2001 жылы Қызыл код құрты 658 серверге жұққан. 2-суретке сүйенсек, 19 сағаттан кейін құрт 300 000-нан астам серверге жұққан.

Ортадағы адам (Man-in-the-Middle, MitM) – шабуылшының пайдаланушыға білдірместен құрылғыны басқаруына мүмкіндік береді. Қосылудың осындай деңгейімен шабуылшы пайдаланушының ақпаратын тиісті орнына жетпей жатып ұстап ала алады. MitM шабуылдары қаржы ақпаратын ұрлауда кеңінен қолданылады. Шабуылшыларға MitM мүмкіндіктерін беретін көптеген зиянды бағдарламалар мен әдістер бар.

Мобильді құрылғыдағы адам (Man-in-the-Mobile, MitMo) – ортадағы адам шабуылының бір түрі болып табылатын MitMo мобильді құрылғының басшылығын тартып алуға бағытталған шабуыл. Жұқтырылған кезде мобильді құрылғыға пайдаланушының құпия ақпаратын шығарып, шабуылшыларға жіберу туралы нұсқаулар берілуі мүмкін. ZeuS – MitMo мүмкіндіктері бар пайдалану құралының мысалы. Ол пайдаланушыларға жіберілген 2 қадамдық SMS растамаларын білдірмей ұстап алуға мүмкіндік береді.

1-сурет. Бастапқы кодтың қызыл құрт жұқпасы

2-сурет. Қызыл құрт жұқпасы – 19 сағаттан кейін

Зиянды бағдарламалардың белгілері

Жүйеге нұқсан келтірген зиянды бағдарламаның түрінен тәуелсіз, төмендегі белгілер зиянды бағдарламалардың жалпы белгілері болып табылады:

- Орталық процессорды қолдану көлемінің артуы.
- Компьютер жылдамдығының баяулауы.
- Компьютердің жиі қатып қалуы не жұмыс істемей қалуы.

Интернетте веб-шолу жылдамдығының төмендеуі.

- Желі байланыстарында түсініксіз мәселелердің орын алуы.
- Файлдарға өзгерту енгізілуі.
- Файлдардың жойылуы.
- Белгісіз файлдардың, бағдарламалардың не жұмыс үстелі белгішелерінің пайда болуы.
- Белгісіз процестердің іске қосылуы.
- Бағдарламалардың өздігінен өшіп қалуы не қайта реттелуі.
- Пайдаланушыға хабарламастан не оның келісімін алмастан электрондық хабарлама жіберілуі.